A Quantum Hub for Star-Shaped Quantum Key Distribution Networks

Ein Quanten-Hub für sternförmige Quantenschlüsselaustausch-Netze
Zur Erlangung des Grades eines Doktors der Naturwissenschaften (Dr. rer. nat.)
Genehmigte Dissertation von Erik Fitzke aus Berlin-Pankow
Tag der Einreichung: 17. Oktober 2023, Tag der Prüfung: 13. Dezember 2023

1. Gutachten: Prof. Dr. Thomas Walther
2. Gutachten: Prof. Dr. Gerhard Birkl
Darmstadt, Technical University of Darmstadt

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Physics Department
Institute for Applied Physics
Laser and Quantum Optics

A Quantum Hub for Star-Shaped Quantum Key Distribution Networks
Ein Quanten-Hub für sternförmige Quantenschlüsselaustausch-Netze

Accepted doctoral thesis by Erik Fitzke

Date of submission: October 17, 2023
Date of thesis defense: December 13, 2023

Darmstadt, Technical University of Darmstadt

This thesis is dedicated to my parents, who have always supported me.

Abstract

Recent advances in the field of classical computing and quantum computing enable new attacks on today's public-key cryptography. Therefore, an essential goal of cybersecurity research is to develop new, future-proof cybersecurity solutions.

Quantum key distribution (QKD) is a method to distribute symmetric digital cryptographic keys between two users by using principles of quantum physics, enabling the information-theoretically secure exchange of encrypted messages. Fundamental principles of quantum physics ensure that the QKD users detect every attempt by a third party to obtain a copy of the key. However, for many applications, secure connections between two users are insufficient, so larger networks for multiple users are required. On the way to the widespread use of QKD, laboratory experiments under controllable environmental conditions are only the first step, and tests under realistic operating conditions are required to demonstrate the reliability of the systems.

Therefore, the goals of the research presented in this thesis are to develop a multi-user QKD network, to demonstrate its reliability and flexibility in a field test, and to develop detailed models of this system taking the relevant setup imperfections into account.

The multi-user QKD network is implemented as a star-shaped network with a central *quantum key hub* (q-hub), enabling simultaneous and independent distribution of quantum keys to multiple pairs of users with distances up to 100 km between the users. In contrast to other QKD networks, the q-hub system uses a polarization-insensitive QKD protocol based on quantum-entangled photon pairs in combination with wavelength demultiplexing to enable robust key transmissions. Therefore, the q-hub system is well suited to implement QKD networks in urban areas or for other applications where the optical fiber transmission links are exposed to the weather or vibrations which may lead to polarization instabilities.

The first part of this thesis presents the implementation and performance evaluation of a q-hub network with four users. The QKD receivers of the users are synchronized with a precision better than 100 ps by using a new method for clock recovery from the arrival times of the photons for which a patent is pending. The compactness and flexibility of the QKD system required for real-world applications are proven in a field test at a facility of the *Deutsche Telekom* company. This field test was the first field test of a multi-user QKD network based on the Bennett-Brassard-Mermin 1992 (BBM92) time bin QKD protocol. Stable key distribution over more than three days is demonstrated for fiber lengths of more than 100 km between two users, including 27 km of fiber deployed in the field. Dozens of users could be readily connected to the network if the required number of QKD receivers were built. Finally, a photonic integrated circuit is designed as a first step towards an even more compact q-hub, and on-chip photon pair generation is demonstrated.

The second part of this thesis presents detailed numerical models of the q-hub system. A new method for the time-dependent tomographic characterization of single-photon detectors in terms of positive operator-valued measures (POVMs) is presented and applied to characterize the detectors employed in the QKD system.

Furthermore, a general method for the photon-number-resolved simulation of multi-mode quantum-optical setups with Gaussian states is developed. A key result is the derivation of the generating function for the photon statistics, from which the photon number distribution and its moments and factorial moments are computed by automatic differentiation. One of the strengths of this simulation method is the flexibility to include effects from various kinds of setup imperfections in simulations of quantum-optical setups.

Finally, a frequency-resolved simulation of the QKD system is developed by generalizing the covariance formalism of Gaussian states to a continuum of frequencies. The simulation results match the measurements to a high degree, allowing for a realistic prediction of the setup performance. The simulation will enable performance optimizations and cost reductions for the development of future QKD networks.

Kurzfassung

Durch Fortschritte im Bereich der klassischen Computer und der Quantencomputer werden neue Angriffe auf die heute genutzten Verfahren der asymmetrischen Kryptographie möglich. Ein wichtiges Ziel der Cybersicherheitsforschung ist es daher, neue, zukunftsfähige Sicherheitslösungen zu entwickeln.

Quantenschlüsselaustausch (eng.: *quantum key distribution*, kurz QKD) ist eine Methode zur Verteilung symmetrischer digitaler kryptographischer Schlüssel zwischen zwei Nutzern basierend auf Prinzipien der Quantenphysik, welche den informationstheoretisch sicheren Austausch verschlüsselter Nachrichten ermöglicht. Grundlegende quantenphysikalische Prinzipien gewährleisten, dass jeder Versuch eines Dritten, eine Kopie des Schlüssels zu erhalten, von den QKD-Nutzern erkannt wird. Für viele Anwendungen sind sichere Verbindungen zwischen zwei Nutzern nicht ausreichend und es werden stattdessen größere QKD Netze für mehrere Nutzer benötigt. Auf dem Weg zu einem großflächigen Einsatz von QKD sind Laborexperimente unter kontrollierbaren Umgebungsbedingungen immer nur der erste Schritt. Tests der Systeme unter realistischen Betriebsbedingungen sind erforderlich, um ihre Zuverlässigkeit unter realistischen Einsatzbedingungen zu demonstrieren. Daher sind die Ziele der in dieser Arbeit vorgestellten Forschung die Entwicklung eines Multi-User-QKD-Netzwerks, die Demonstration seiner Zuverlässigkeit und Flexibilität in einem Feldtest und sowie die Entwicklung detaillierter Modelle dieses Systems, welche die relevanten Imperfektionen des Aufbaus berücksichtigen.

Das Multi-User-QKD-Netzwerk wurde als sternförmiges Netzwerk mit einem zentralen *quantum key hub* (q-hub) implementiert, der die gleichzeitige und unabhängige Verteilung von Quantenschlüsseln an mehrere Nutzerpaare über optische Fasern über Distanzen bis zu 100 km zwischen den Nutzern ermöglicht. Im Gegensatz zu anderen QKD-Netzwerken verwendet das *q-hub* System ein polarisationsunabhängiges QKD-Protokoll basierend auf quantenverschränkten Photonenpaaren in Kombination mit Wellenlängen-Demultiplexing, um robuste Schlüsselübertragungen zu ermöglichen. Das *q-hub* System ist daher gut zur Implementierung von QKD-Netzwerken in städtischen Gebieten oder für andere Anwendungsszenarien geeignet, bei denen die Glasfaserübertragungsstrecken dem Wetter oder Vibrationen ausgesetzt sind, was zu Polarisationsänderungen führen kann.

Im ersten Teil dieser Arbeit wird die Implementierung eines QKD-Netzwerks mit vier Nutzern vorgestellt und seine Leistungsfähigkeit evaluiert. Die QKD-Empfänger der Nutzer werden mit Hilfe einer neuen Methode zur Taktrückgewinnung aus den Ankunftszeiten der Photonen synchronisiert, wobei Genauigkeiten besser als 100 ps erzielt werden. Diese Methode ist zum Patent eingereicht. Die Kompaktheit und Flexibilität des QKD-Systems für reale Anwendungen wurden in einem Feldtest an einem Standort der Deutschen Telekom demonstriert. Dieser Feldtest war der erste Feldtest eines Multi-User-QKD-Netzwerks, das auf dem Bennett-Brassard-Mermin 1992 (BBM92) Time-Bin-QKD-Protokoll basiert. Ein mehr als drei Tage dauernder stabiler Schlüsselaustausch über Glasfaserlängen von mehr als 100 km zwischen zwei Nutzern wurde demonstriert. Von der Faserstrecke sind ca. 27 km im Feld verlegt. Dutzende von Nutzern könnten ohne weiteres an das Netzwerk angeschlossen werden, wenn die entsprechende Anzahl and QKD-Empfängern gebaut würde. Als erster Schritt zu einem noch kompakteren *q-hub* wurde ein integrierter photonischer Chip entworfen und die Erzeugung von Photonenpaaren mittels dieses Chips wurde demonstriert.

Im zweiten Teil dieser Arbeit werden detaillierte numerische Modellierungen des *q-hub* Systems vorgestellt. Eine neue Methode zur zeitabhängigen Detektortomographie mittels sogenannter *positive operator-valued measures* (POVMs) wird vorgestellt und zur Charakterisierung der im QKD-System verwendeten Detektoren verwendet.

Darüber hinaus wird eine allgemeine Methode für die photonenzahlaufgelöste Simulation von quantenoptischen Experimenten mit Gaußschen Multimode-Zuständen entwickelt. Ein wesentliches Ergebnis ist die Herleitung der erzeugenden Funktion für die Photonenstatistik, aus der die Photonenzahlverteilung sowie deren Momente und faktorielle Momente durch sogenanntes automatisches Differenzieren berechnet werden. Eine der Stärken dieser Simulationsmethode ist die Flexibilität, die es erlaubt, Effekte von verschiedenen Arten von Imperfektionen bei der Simulation verschiedenster quantenoptischer Aufbauten zu berücksichtigen.

Schließlich wird eine frequenzaufgelöste Simulation des QKD-Systems entwickelt, indem der Kovarianzformalismus der Gaußschen Zustände auf ein Kontinuum von Frequenzen verallgemeinert wird. Die Simulationsergebnisse stimmen in hohem Maße mit den Messungen überein und erlauben damit realistische Vorhersagen zur Leistungsfähigkeit des Systems. Die Simulation wird die Optimierung der Leistungsfähigkeit und die Reduktion der Kosten bei der Entwicklung zukünftiger QKD Systeme ermöglichen.

Contents

List of Abbreviations

AD	Automatic Differentiation
ASE	Amplified Spontaneous Emission
AWG	Arrayed-Waveguide Grating
BB84	Bennett and Brassard 1984 (QKD protocol)
BBM92	Bennett, Brassard, and Mermin 1992 (QKD protocol)
BPF	Bandpass Filter
BS	Beam Splitter
CAR	Coincidenc-to-Accidental Ratio
CD	Chromatic Dispersion
CR	Clock Recovery
CW	Continuous Wave (laser)
DCF	Dispersion-Compensating Fiber
DIMITRI	Dual Imbalanced Mach-Zehnder Interferometer Ring
DWDM	Dense Wavelength-Division Multiplexing
EDFA	Erbium-Doped Fiber Amplifier
EOAM	Electro-Optic Amplitude Modulator
EOPM	Electro-Optic Phase Modulator
FBG	Fiber Bragg Grating
FFT	Fast Fourier Transformation
FRM	Faraday Rotator Mirror
FT	Fourier Transform
FWHM	Full Width at Half Maximum
GBS	Gaussian Boson Sampling
GS	Gaussian State
IF	Interferometer
IFT	Inverse Fourier Transform
ITU	International Telecommunication Union
JSA	Joint Spectral Amplitude

LDPC	Low-Density Parity Check (error correction code)
MRR	Microring Resonator
non-PNR	non-photon-number-resolving (single photon detector)
OPD	Optical Path Difference
OTDR	Optical Time-Domain Reflectometer
PDH	Pound-Drever-Hall (resonator stabilization technique)
PGF	Probability-Generating Function
PIC	Photonic Integrated Circuit
PID	Proportional-Integral-Derivative (control loop)
PM	Polarization-Maintaining (fiber)
PMD	Polarization-Mode Dispersion
PND	Photon Number Distribution
PNR	Photon-Number-Resolving (single photon detector)
POVM	Positive Operator-Valued Measure
PPLN	Periodically Poled Lithium Niobate
PPS	Photon Pair Source
PQC	Post-Quantum Cryptography
q-hub	Quantum Key Hub
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
SFWM	Spontaneous Four-Wave Mixing
SHG	Second Harmonic Generation
SM	Single-Mode
SMF	(Standard) Single-Mode Fiber
SPD	Single-Photon Detector
SPDC	Spontaneous Parametric Down-Conversion
SVD	Singular Value Decomposition
TC	Time Controller
TCU	Temperature Control Unit
TEC	Thermoelectric Cooler
TMSV	Two-Mode Squeezed Vacuum
VOA	Variable Optical Attenuator
WDM	Wavelength-Division (De-) Multiplexer
WSS	Wavelength-Selective Switch

Introduction

Quantum technologies are an active field of research. Two of the major research areas are quantum computing and quantum communications. One of the most important goals of quantum computing research is to use effects from quantum physics to solve mathematical problems that cannot be tackled efficiently with classical computers. Therefore, the development of quantum computers has far-reaching consequences for complexity-based cryptography, as it is used in today's digital communication [1]. Considering the recent advancements, quantum computers powerful enough to render large parts of nowadays's cryptography insecure are feasible within the next couple of years. The IT security community and national cybersecurity agencies such as the NSA in the United States [2], the ANSSI [3] in France, the NCSC in the United Kingdom [4] or the Federal Office for Information Security (BSI) in Germany [5] are therefore closely monitoring the advancements in quantum computing and advise to prepare for a transition to quantum-secure cryptography. The BSI works with the following timeline for risk assessment [5]:

> *"For high security systems, BSI acts on the working hypothesis that cryptographically relevant quantum computers will be available in the early 2030s."*

In a national security memorandum from May 2022, the White House calls for action [6]:

> *"To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035."*

These statements corroborate that quantum-resistant cybersecurity solutions are urgently required within the next decade.

Fortunately, quantum physics can also be used to re-establish security. *Quantum key distribution* (QKD) is a subfield of quantum communications concerned with distributing symmetric keys for encrypting digital messages. The security of QKD relies on fundamental laws of quantum physics and information theory. The great advantage of QKD is that it remains secure even when powerful quantum computers become available. Importantly, QKD does not require quantum computing. Therefore, QKD can already be implemented before cryptographically relevant quantum computers become available. The general idea of QKD is almost 40 years old and was introduced by Charles H. Bennett and Gilles Brassard, who proposed the BB84 QKD protocol [7, 8]. Since these days, the field of QKD research has consistently evolved. Today, numerous companies offer commercial QKD solutions [9–16].

One of the major directions in experimental QKD research has been the demonstration of increasingly higher key rates and increasingly longer transmission distances. Key rates of more than 110 Mbit/s over a transmission distance of 10 km have recently been demonstrated [17]. QKD over optical fibers with lengths of hundreds of kilometers has been demonstrated using state-of-the-art QKD systems [18, 19], and the mark of 1000 km transmission distance through optical fibers has been reached recently [20]. QKD over thousands of kilometers has been demonstrated employing satellites [21, 22].

Another important research direction is the implementation of QKD networks for multiple users. A common approach to realizing QKD networks is to use *trusted nodes*. Trusted nodes are stations between the users where the keys are relayed and processed as classical information. Therefore, network users must trust the operator of the node, because he knows the keys. The world's largest QKD network is located in China, connecting Beijing, Shanghai, and other cities via trusted nodes to a 2000 km long backbone link and including multiple metropolitan-area QKD networks [23]. A crucial disadvantage of the trusted-node approach is that the users need to trust the network provider. To achieve end-to-end quantum security between the users, trusted-node-free QKD networks are required. Two of the most important topologies for such networks are ring-shaped networks [24] and star-shaped networks [25–27]. In a ring-shaped network, all users are connected via a single fiber ring. The quantum signals have to pass all users before they are detected, which limits the scalability of this approach. In star-shaped networks, all users are connected to a central element, which can be either the measurement station of a measurement-device-independent QKD network [25] or the source of entangled photons in an entanglement-based network [26, 27].

One of the major goals of the research presented in this thesis is to develop a *quantum key hub* (q-hub), that is a central device allowing to connect more than two users to each other in a QKD network with a star-shaped topology. Such networks could be used to connect tens or hundreds of users in metropolitan areas, with possible applications in the healthcare and financial sectors as well as for law enforcement and government organizations. An important difference between the q-hub and trusted nodes in QKD networks is that two users sharing a quantum key only need to trust each other but do not need to trust the q-hub or other users in the q-hub network.

Outline

This thesis contains both experimental results and results from numerical simulations of the q-hub QKD network, which is the successor of an entanglement-based QKD system for two users developed by Oleg Nikiforov during his Ph.D. [28]. The first part describes the experimental realization of the network and its field test at a facility of *Deutsche Telekom* with key transmissions over a fiber deployed underground. The second part presents theoretical models and numerical simulations of the q-hub QKD system. For the simulation to correctly reproduce the experiment, several parameters of the system need to be determined by characterization experiments. Therefore, thorough characterizations of various parts of the QKD system are presented.

Many results presented in this thesis have been obtained in close collaboration with students working on their bachelor's theses (refs. [B1–B7]) or master's theses (refs. [M1–M9]). Some of the following results have been published or are submitted for publication as refs. [I–IX]). Two patents for inventions related to the q-hub system are pending.

Chapter 1 introduces the basic concepts of quantum key distribution and of photon pair generation by spontaneous parametric down-conversion as well as properties of single mode optical fibers that are relevant for the following chapters.

Chapter 2 describes the setup of the q-hub network, consisting of a source of quantum-entangled photon pairs and four receivers for the QKD users. Characterizations of the photon pair source are presented, and the requirements on the interferometers in the receivers are derived. The timing synchronization of the receivers is achieved by recovering the clock frequency of the photon pair source from the arrival times of the photons at the receivers, and the performance of this method is analyzed. Two patents of O. Nikiforov, E. Fitzke, and Th. Walther for the method to build and align fiber interferometers fast and with high accuracy and of E. Fitzke and Th. Walther for the clock recovery method are pending. An analysis of some of the photon spectra has been published in ref. [I]:

> *"Spectral characterization of SPDC-based single-photon sources for quantum key distribution"*, S. Euler, E. Fitzke, O. Nikiforov, D. Hofmann, and Th. Walther, The European Physical Journal Special Topics **230** 1073-1080 (2021).

Further details about the photon pair source of the q-hub will be published in ref. [VIII]:

> *"A flexible modular all-fiber based single-photon source for quantum key distribution in a network"*,
> M. Tippmann, E. Fitzke, O. Nikiforov, P. Kleinpass, T. Dolejsky, M. Mengler, and Th. Walther, Manuscript submitted for publication.

The complete q-hub QKD network has been published in ref. [II]:

> *"Scalable Network for Simultaneous Pairwise Quantum Key Distribution via Entanglement-Based Time-Bin Coding"*,
> E. Fitzke, L. Bialowons, T. Dolejsky, M. Tippmann, O. Nikiforov, Th. Walther, F. Wissel, and M. Gunkel, PRX Quantum **3** 020341 (2022).

Chapter 3 presents results from the field test, for which the q-hub and the receiver modules were placed at a facility of the *Deutsche Telekom* company in Darmstadt. Simultaneous pairwise QKD between the users over a fiber deployed underground and over spooled fibers in the laboratory was demonstrated for fiber lengths up to more than 100 km between two users. A part of the results from the field test has been published in ref. [II]. Most of the field test results have been published in ref. [V]:

> *"Flexible reconfigurable entanglement-based quantum key distribution network"*,
> T. Dolejsky, E. Fitzke, L. Bialowons, M. Tippmann, O. Nikiforov, and Th. Walther, The European Physical Journal Special Topics (2023).

Chapter 4 presents first results of experiments with photonic integrated circuits for the q-hub. Photon pairs are generated by spontaneous four-wave mixing in integrated microring resonators. A setup for gigahertz-modulated Pound-Drever-Hall locking is developed to stabilize the microring resonators to the laser frequency. Furthermore, a dedicated photonic integrated circuit for photon pair generation is designed and tested.

Chapter 5 presents a thorough characterization of the single-photon avalanche detectors of the QKD receivers. A new method for reconstructing time-dependent positive operator-valued measures (POVMs) describing the detectors is introduced, adapting the weight of the regularization term to the statistical quality of the data. Furthermore, a model from the literature constructing theoretical time-dependent detectors POVM based on the detector timing jitter distribution and dead time is compared to measurements. The results have been published in ref. [III]:

> *"Time-dependent POVM reconstruction for single-photon avalanche photo diodes using adaptive regularization"*,
> E. Fitzke, R. Krebs, T. Haase, M. Mengler, G. Alber, and Th. Walther, New Journal of Physics **24** 023025 (2022).

Chapter 6 presents a new method to simulate the photon statistics of multimode Gaussian states as well as photon-added and photon-subtracted Gaussian states. The key results of this chapter are the generating functions for the photon number distribution, moments, and factorial moments. The method is applied to simulate the q-hub QKD system. The simulated QKD performance is compared to measurements, and the simulation is used to demonstrate the relevance of multi-photon-pair emission for the quantum bit error rate. The simulation method has been published in ref. [VI]:

> *"Simulating the photon statistics of multimode Gaussian states by automatic differentiation of generating functions"*,
> E. Fitzke, F. Niederschuh, and Th. Walther, APL Photonics **8** 026106 (2022).

The application of the framework *PyTorch* [29] for the evaluation of the multivariate higher-order derivatives of the generating functions is demonstrated in a technical report [IV]:

> *"Simulating the Photon Statistics of Gaussian States Employing Automatic Differentiation from PyTorch"*,
> E. Fitzke, F. Niederschuh, and Th. Walther,
> Technical Report, DOI: 10.26083/tuprints-00023061 (2022).

Chapter 7 presents a time- and frequency-resolved simulation of the q-hub QKD system. The frequency resolution allows considering effects such as frequency-dependent losses or chromatic dispersion in the fiber links. For the simulation, the covariance formalism of Gaussian states is extended to a continuum of frequencies and times, and the relevant matrix transformations of the covariance in the discrete-mode formalism are replaced by integral operators. Systematic approximations for strongly entangled biphoton states, as they are used in the q-hub QKD system, are derived, and error bounds for the approximations are provided. The QKD system is modeled, and simulation results for the QKD performance are compared to measurements. A manuscript presenting the results is to be submitted for publication as ref. [VII]:

> *"Frequency-Resolved Simulations of Highly Entangled Biphoton States beyond the Single-Pair Approximation"*,
> P. Kleinpass, E. Fitzke, and Th. Walther, Manuscript to be submitted for publication.

Part I

Development and Field Test of a Multi-User QKD System

1 Basic Concepts

Suppose two users want to exchange a digital message in such a way that no one else can read it. In that case, they can use a symmetric encryption algorithm such as the *Advanced Encryption Standard* (AES) to encrypt their message [30]. Furthermore, a symmetric encryption method called *one-time pad* encryption exists, which has been proven to be information-theoretically secure, meaning that it cannot be broken even with infinite computational resources [31]. The one-time pad encryption requires that the users, who are commonly called *Alice* and *Bob*, share the same secret key. The secret key must be completely random, at least as long as the message, and it can be used only once [31]. Alice encrypts her plain text message to be sent to Bob symbol by symbol with the key, for example, by using bitwise addition modulo two. She sends the resulting ciphertext to Bob, who decrypts the message by subtracting the key from the ciphertext. If the eavesdropper *Eve* can only obtain a copy of the ciphertext but not a copy of the key, Eve cannot decrypt the message. In principle, Eve can try out all possible keys and subtract them from the ciphertext. But as the key is random, the ciphertext is also random, such that Eve recovers all possible plain text messages with equal probability. It is, therefore, impossible for Eve to decide which of the recovered messages is the plain text Alice sent to Bob, meaning that Eve cannot break the encryption. A disadvantage of the one-time pad is that individual bits of the plain text can be easily reconstructed if the corresponding key bits are known. Therefore, the BSI recommends using the one-time pad only in combination with different algorithms [5].

In any case, symmetric encryption algorithms require that Alice and Bob share a digital, identical secret key. To exchange such a key, Alice and Bob can use a protocol called *Diffie-Hellman key exchange*. The security of the Diffie-Hellman method and of the widely used RSA public-key cryptosystem relies on the assumption that computing the discrete logarithm and prime factorizations of large enough numbers is unfeasible even with the most powerful classical computers [32]. In 1994, Peter Shor proposed algorithms for solving both problems efficiently on quantum computers, meaning that the run time of the algorithms grows not significantly faster than a polynomial of the number of digits of the input [33, 34]. In the limit of large input numbers, the runtime of these algorithms is significantly shorter than for the best known algorithms for classical computers. Once quantum computers are advanced enough to run Shor's algorithms for the input lengths used in cryptography, protocols based on these mathematical problems will become insecure. Therefore, new methods are required to replace cryptographic protocols based on the vulnerable methods.

The efforts to develop new, quantum-safe cryptography solutions can be grouped into two approaches. The idea of the first approach, called *post-quantum cryptography* (PQC), is to use different algorithms for cryptography based on mathematical problems that are believed to be resistant to attacks with quantum computers. Several different PQC algorithms have been proposed. Since 2016, the National Institute of Standards and Technology (NIST) has been running a competition to select and standardize PQC algorithms [35]. PQC is considered one of the most promising solutions to the security threat from quantum computers [2–5]. However, establishing new cryptographic algorithms within a relatively short time also comes at the risk that new, unexpected attack methods may soon be discovered. Examples are attacks on the two candidate algorithms RAINBOW and SIKE in late rounds of the NIST competition. Spectacular attacks on both algorithms were discovered in 2022, allowing to break the encryption based on these algorithms within a couple of hours of computing time on a laptop [36, 37].

1.1 Basic Principles of Quantum Key Distribution

Another possible solution to distributing symmetric keys to different users is *quantum key distribution* (QKD). For QKD, Alice and Bob exchange quantum signals and derive the key bits from the results of quantum-mechanical measurements of the transmitted signal. Typically, light signals at the single photon level are used because they can be transmitted with relatively low losses through optical fibers or via free-space links. The reviews [31, 38–40] provide overviews of various aspects of QKD.

The Bennett and Brassard 1984 (BB84) QKD Protocol

In 1984, Bennett and Brassard developed the BB84 QKD protocol [7, 8]. It is one of the most famous QKD protocols and well suitable to explain the general idea of QKD.

The classic BB84 QKD requires the following steps [7, 8, 31]: Alice prepares a *quantum bit* represented by a photon in one of the four polarization states "horizontal", "vertical", "diagonal" or "antidiagonal" and sends it to Bob. If Alice sends a horizontal or diagonal photon, she notes a bit "0". For the other two states, she notes a bit "1". Bob's receiver consists of a polarizing beam splitter and two single-photon detectors labeled "0" and "1" placed at its outputs. Horizontal photons are guided to detector 0, and vertical photons are guided to detector 1. Bob notes down the bit value of the detector registering the photon. Furthermore, he can rotate his setup by 45°, such that diagonal photons are guided to detector 0, and antidiagonal photons are guided to detector 1. Before he receives Alice's photon, Bob randomly decides whether he wants to measure the polarization state of the incoming photon in the rectilinear +-basis or whether he rotates his setup by 45° and to measure the polarization in the diagonal ×-basis. Alice sends several photons to Bob, and Bob decides for each photon individually and randomly in which basis he measures the polarization. When he measures in the +-basis, Bob always registers horizontal photons in detector 0 and vertical photons in detector 1. When he measures in the ×-basis, he always registers diagonal or antidiagonal photons in detector 0 or 1, respectively. However, when Alice's and Bob's bases do not match, he randomly registers the photon in the first or second detector with 50 % probability.

In the next step, called *key sifting*, Alice shares her bases choices with Bob over an authenticated channel while keeping the bit values secret [7, 8, 31, 38, 40]. If her basis matches Bob's basis, they keep their bit, knowing that the bit values will be the same. If they chose different bases, Bob's bit value is random, and Alice and Bob discard their bit values, which is called *postselection*.

A simple attack strategy for Eve, called *intercept-resend attack*, would be to intercept the photon from Alice, measure the polarization, store the bit value, and send a new photon with the same polarization to Bob [7, 8, 31, 38, 40]. However, Eve does not know in which basis Alice prepared the photon and therefore measures and prepares the new photon in the wrong basis with 50 % probability. As Alice and Bob only keep bits from photons where they chose the same basis, a photon prepared by Eve in the wrong basis generates a random bit value in Bob's measurement station. Therefore, Eve's attack leads with a probability of 25 % to a *quantum bit error*, that is a deviation of Alice's and Bob's key bit.

To check if Eve intercepted the photons, Alice and Bob compare after the QKD session a random sample of 10 % of their key bits over an authenticated channel and calculate the *quantum bit error rate* (QBER), given by the ratio of quantum bit errors to the total number of sifted key bits [31, 38, 40]. The bits they compared are not secure anymore and are therefore discarded. When the QBER is zero, Alice and Bob can be sure that Eve does not know the key, and they can use the remaining bits to encrypt and exchange their message. However, when Eve applies the intercept-resend strategy to all quantum bits, Alice and Bob will observe a QBER of 25 % in their sample. The high QBER reveals the presence of Eve to Alice and Bob, so they do not use the key to encrypt their message. They can try to establish a new key in another QKD session, and if Eve again intercepts the photons, this key cannot be either. Alice and Bob always notice when Eve intercepts the photons because Eve inevitably introduces quantum bit errors. Therefore, the worst Eve can do is to launch a denial-of-service attack, preventing a successful key exchange. However, she can never obtain the key used to encrypt the message.

Key Postprocessing: Error Correction and Privacy Amplification

After key sifting, Alice and Bob obtain bit strings $\boldsymbol{a}$ and $\boldsymbol{b}$. In practice, these bit strings generally differ due to detection noise or Eve's interception of some bits. To obtain identical, error-free bit strings, Alice and Bob execute an *error correction* algorithm. Two common algorithms are the *Cascade* algorithm [41, 42] and *low-density parity-check* (LDPC) codes [43, 44]. Both approaches are fundamentally different: Cascade is an interactive protocol requiring multiple rounds of message exchanges between Alice and Bob, while LDPC is a forward error correction method requiring only a single round. LDPC codes are also used, for example, for error correction in Wi-Fi communication [45]. In QKD, LDPC codes can be used as follows [44]: Alice and Bob agree on a parity-check matrix $\boldsymbol{G}$, which is sparsely populated with ones and which is zero everywhere else. Alice computes the checksum bit vector $\boldsymbol{c}_\mathrm{A} = \boldsymbol{G}\boldsymbol{a}$ in modulo-2 arithmetics and a hash value $\mathrm{hash}(\boldsymbol{a})$ and sends both to Bob. Bob computes $\boldsymbol{c}_\mathrm{B} = \boldsymbol{G}\boldsymbol{b}$ and compares his checksum vector to Alice's. In general, when Alice's and Bob's bit strings are different, the checksum vectors $\boldsymbol{c}_\mathrm{B}$ and $\boldsymbol{c}_\mathrm{A}$ are different. Bob then iteratively corrects the bits and updates $\boldsymbol{c}_\mathrm{B}$ until the checksum vectors are identical [44]. To verify the successful reconstruction of the correct bit string, he checks that $\mathrm{hash}(\boldsymbol{b}) = \mathrm{hash}(\boldsymbol{a})$.

Alice and Bob have to assume that all bit errors were caused by Eve, meaning Eve has partial information about the key. Furthermore, Eve gained additional information about the key from the checksum bits exchanged for the error correction. Therefore, Alice and Bob have to distill a secure key from the corrected key such that Eve has almost no information about the secure key [46]. For that, Alice and Bob must estimate, based on the number of error bits and checksum bits, how much information Eve may have obtained about the key. Then, they execute a procedure called *privacy amplification*, during which they apply a suitable hash function to the corrected key to extract a shorter secure key [46]. The more information Eve is assumed to possess about the key, the shorter the secure key after privacy amplification. A commonly used hash function is the multiplication with a Toeplitz matrix, which can be efficiently implemented by using the fast Fourier transformation [40].

Security of QKD

The example of the BB84 protocol and Eve's intercept-resend attack well illustrates the general idea of QKD, but the situation is more complicated in practice. For example, Eve could intercept only some of the photons to keep the QBER low at the price of obtaining less information about the key. Or Eve could create entangled photon pairs, send one of the photons to Bob, and store the other photon in a quantum memory for a delayed analysis after the key sifting in the correct basis. Formal security proofs exist for BB84 and other QKD protocols, which provide upper bounds for the information Eve may obtain about the key as a function of the observed QBER and the capabilities of Eve [47, 48]. Reference [49] provides a detailed overview of approaches to QKD security proofs. The most general type of attacks considered in such proofs are called *coherent attacks*, which assume that Eve has unlimited resources and can perform any possible operation based on classical physics or quantum physics [40].

Theoretically, Alice and Bob can obtain a secure key from the BB894 protocol as long as the QBER is below 11 % [50]. In practice, the achievable secure key rate depends not only on the QBER but also on the efficiency of the error correction algorithms and the lengths of the keys. Stronger error correction and privacy amplification lead to lower secure key rates, such that the ratio of the secret key rate to the sifted key rate is lower when the QBER is higher. In this thesis, the secure key rate r_{sec} is calculated from the sifted key rate r_{sif} and the QBER q by [51]

$$r_{\text{sec}} = r_{\text{sif}} \left\{1 - (1+f)\left[-q\log_2(q) - (1-q)\log_2(1-q)\right]\right\}. \tag{1.1}$$

Equation (1.1) does not take effects from the finite key lengths into account, but it uses a conservative estimate of $f = 1.5$ for the reconciliation efficiency of the error correction [51]. Figure 1.1 shows the ratio of the $r_{\text{sec}}/r_{\text{sif}}$ obtained from eq. (1.1) as a function of the QBER. With $f = 1.5$, secure keys can be obtained for QBERs up to 8 %. For a relatively low QBER of 1 %, the secure key rate is about 80 % of the sifted key rate, and for a QBER of 4 % the ratio drops to 40 %. Therefore, QKD setups must be designed carefully, allowing for low QBERs and high secure key rates. The dependency of the secure key rate on the QBER ultimately limits the maximum transmission distance achievable with QKD systems: the lower the photon rate arriving at the receiver, the higher the relative noise level and the higher the QBER. If the distance is too long such that the QBER is too high, Alice and Bob cannot establish secure keys.

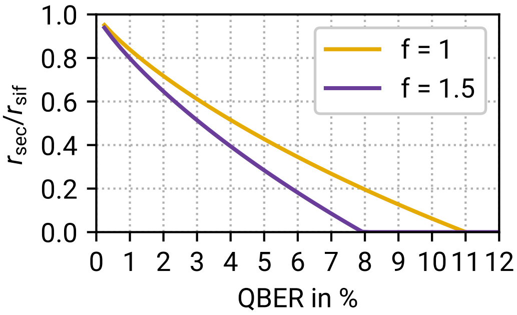


Figure 1.1: Ratio of the secure rate r_{sec} to the sifted key rate r_{sif} as a function of the QBER according to eq. (1.1) for an ideal efficiency of the error correction $f = 1$ and for the conservative value of $f = 1.5$ used to calculate the secure key rates in the experiments.

The theoretical security of QKD systems can be impaired by hardware imperfections in practical systems. Especially single-photon detectors are vulnerable to attacks [39, 40, 52, 53]. An overview of different attack strategies and countermeasures can be found in refs. [39, 40]. In many of these attack strategies, Eve prepares special light pulses and sends them into the receiver to manipulate it or to obtain information about its inner state. In 2010, this strategy was used to hack commercially available QKD systems [52].

A whole new family of protocols called *measurement-device-independent QKD* has been developed to overcome the weaknesses of QKD introduced by detectors [40, 54]. However, these protocols are, in principle, still vulnerable to attacks against the photon source. Device-independent QKD protocols have been designed to avoid side channel attacks against the quantum-optical devices, but they are challenging to implement, requiring high overall transmission and detection efficiencies. So far, only key transmissions over very short distances, up to a few hundred meters, could be realized [40, 55]. However, even for device-independent QKD, further security threats remain. Insecure implementations of the post-processing, for example, can make the protocol vulnerable to cache-side-channel attacks [56]. Another example are so-called memory attacks. Assuming that Eve may have manufactured the QKD system, she could integrate memories in the devices to which the keys are copied. At a later time, the device could leak the stored keys to Eve over a classical communication channel [57, 58].

In conclusion, it can be noted that from a theoretical point of view, QKD can provide information-theoretic security based on fundamental laws of quantum physics [38–40, 47]. In comparison, the security of classical cryptography is based on assumptions about the computational resources that are required to solve certain mathematical problems. An advantage of QKD is that, in theory, its security is independent of mathematical and technical advancements. However, side channels in QKD implementations can undermine the security. Therefore, the BSI recommends to use QKD only in combination with classical encryption methods and PQC [5].

1.2 The Bennett-Brassard-Mermin 1992 (BBM92) Time Bin QKD Protocol

In entanglement-based QKD systems, a *photon pair source* (PPS) is placed in between the users. The entangled photons are distributed to the users, which analyze the quantum states using receiver modules. The multi-user QKD network developed in this thesis uses the entanglement-based BBM92 QKD protocol. Therefore, this section describes this protocol in detail.

After Bennett, Brassard, and Mermin proposed the protocol in 1992 [59], the first implementations using time-bin entanglement followed a few years later [60, 61]. Afterwards, the distribution of time-bin entangled photons was demonstrated for increasingly long distances between the users up to 300 km [62–65]. Security proofs for the protocol were derived in refs. [66, 67], and an attack strategy exploiting detector vulnerabilities was presented in ref. [53]. The schematic setup for the protocol is shown in fig. 1.2 (a). A central source of entangled photon pairs is set up to send one photon of each pair to Alice and the other to Bob. Both users are equipped with receivers to measure the photon state. The protocol works as follows [31]: In the *photon pair source* (PPS), laser pulses are sent through an *interferometer* (IF) with arms of different lengths. The *optical path difference* (OPD) of the IF is so large that the delay between the two halves of the pulse in the arms is larger than the pulse duration. Therefore, the two half-pulses do not interfere at the second beam splitter, such that double pulses with a delay and phase determined by

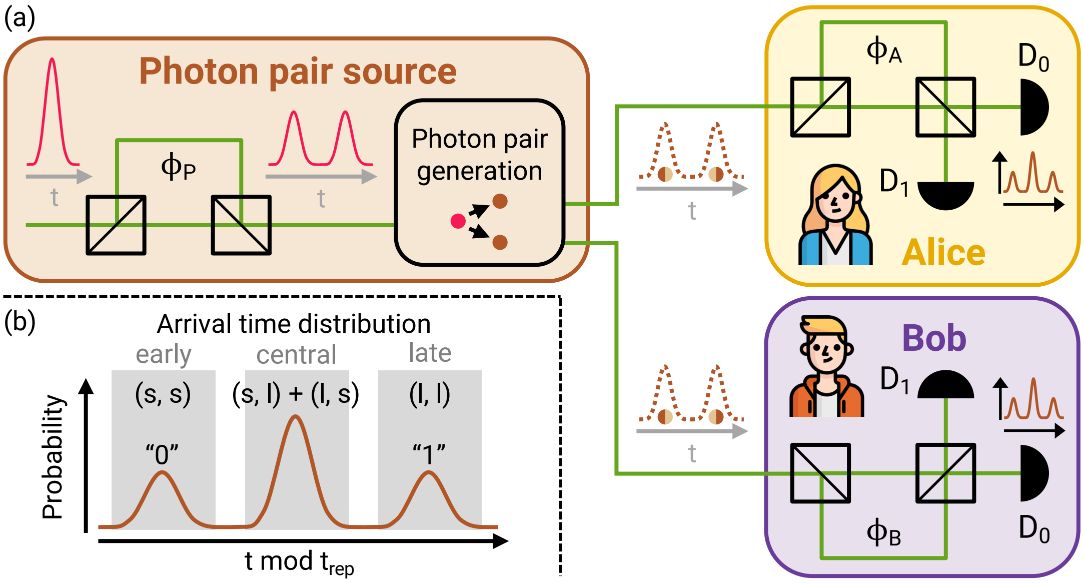


Figure 1.2: Schematic setup for BBM92 QKD with time bins. (a) Setup consisting of a photon pair source and two receivers for Alice and Bob. The pump pulses in the source and the photons in the receivers travel through imbalanced interferometers with phases ϕ_P, ϕ_A, and ϕ_B. The detectors at the receiver outputs are labeled with the bit values "0" and "1" for the phase basis. (b) Arrival time histogram of the photons in one of the detectors, modulo the repetition time t_rep. Photons arrive in three time bins "early", "central" and "late". The early time bin corresponds to time basis bits "0" and the late time bin to time basis bits "1".

the OPD leave the IF. These double pulses pump a nonlinear optical process to generate entangled photon pairs. The energy of the laser pulses is chosen such that the probability of generating more than one photon pair per pulse is much less than one. Each photo pair is split such that one photon is sent to Alice and the other photon is sent to Bob, for example through optical fibers. Both users have a receiver consisting of one IF and two *single-photon detectors* (SPDs), D_0 and D_1. The OPD of the IFs precisely matches the OPD of the IF in the PPS. When one of the detectors registers a photon, it produces a *count*, that is an electrical output pulse indicating the presence of the photon. Alice and Bob record the times of their detector counts and the detector labels.

The arrival time distribution of the photons in each detector with respect to the emission time of the laser pulse in the PPS consisting of three peaks is shown in fig. 1.2 (b). The early peak is caused by photons traveling through the short IF arm when they were generated by the pump pulse taking the short path in the PPS (s, s). Analogously, the late peak is caused by photons traveling through the long IF arm when they were generated by the pump pulse taking the long path in the PPS (l, l). The central peak contains as many photons as the other two peaks combined. It is caused by photons from the (s, l) and (l, s) path combinations, respectively.

The arrival time of each photon is assigned to one of three time bins: early, central, and late, comprising the three peaks, respectively. During the key sifting, Alice and Bob only reveal whether they detected their photons in one of the outer time bins or in the central time bin. Pulse cycles in which Alice or Bob detected the photon in the central time bin and the other one detected it in one of the outer time bins are discarded in the postselection. The information in which detector and in which of the outer time bins a photon was detected is kept secret.

Time Basis and Phase Basis

The photon arrival time constitutes the first basis of the QKD protocol. Alice and Bob assign bit values to the early and late time bins, for example “0” for early and “1” for late photons. When a photon pair is produced by the first pump pulse, Alice and Bob can detect their photons either in the same time bin or in different time bins (early or central). However, it is not possible for one of them to detect the photon in the late time bin. Analogously, when the second pump pulse produces the photon pair, Alice and Bob cannot detect a photon in the early time bin. When at most one photon pair is produced per pulse repetition, Alice and Bob never detect their photons in an early-late combination. Therefore, in repetitions in which they detect their photon in outer time bins, they know that they both detected the photon either in the early or late time bin and the value “0” or “1” assigned to these time bins is their shared key bit.

The second basis of the QKD protocol is the phase basis. When Alice and Bob both detect their photons in the central time bin, the labels of the detectors in which the photons are detected are correlated due to a nonlocal two-photon interference effect called Franson interference [31, 61, 62, 68]. The probability amplitudes of the biphoton wave packet corresponding to the path combinations (s, l, l) and (l, s, s) in the pump IF and the receiver IFs interfere at the outer beam splitters of the receiver IFs. For a setup without losses and with perfect 50/50 beam splitters, the coincidence probability to obtain counts in the central time bin (C) in the detectors $i, j \in \{0, 1\}$ of Alice (A) and Bob (B) is given by [60–62]

$$P(A_{i,\mathrm{C}}, B_{j,\mathrm{C}}) = \frac{1}{16}\big(1 + (-1)^{i+j}\cos(\phi_\mathrm{A} + \phi_\mathrm{B} - \phi_\mathrm{P})\big)\,. \tag{1.2}$$

For $\phi_\mathrm{A} + \phi_\mathrm{B} - \phi_\mathrm{P} = 2n\pi$ with $n \in \mathbb{Z}$, the probabilites $P(A_{0,\mathrm{C}}, B_{0,\mathrm{C}}) = P(A_{1,\mathrm{C}}, B_{1,\mathrm{C}}) = 1/8$ are maximal and $P(A_{0,\mathrm{C}}, B_{1,\mathrm{C}}) = P(A_{1,\mathrm{C}}, B_{0,\mathrm{C}}) = 0$ vanish. The sum of all four coincidence probabilities in the central time bin is 1/4 because 50 % of all photon pairs are detected in different bases such that they are postselected. Furthermore, 50 % of the remaining photon pairs are detected in the time basis. Due to noise and imperfections in real setup, the QBER is generally non-zero even when Eve is not present. The average QBER in the time basis, $\mathrm{QBER_t}$, and in the phase basis, $\mathrm{QBER_p}$, are defined as

$$\mathrm{QBER_t} = \frac{e_\mathrm{t}}{b_\mathrm{t} + e_\mathrm{t}} \quad \text{and} \quad \mathrm{QBER_p} = \frac{e_\mathrm{p}}{b_\mathrm{p} + e_\mathrm{p}}\,. \tag{1.3}$$

Here, b_t and e_t are the numbers of correct bits and error bits in the time basis obtained over some time interval, respectively, and b_p and e_p are the numbers of correct bits and errors in the phase basis. The overall QBER is given by

$$\mathrm{QBER} = \frac{e_\mathrm{t} + e_\mathrm{p}}{b_\mathrm{t} + b_\mathrm{p} + e_\mathrm{t} + e_\mathrm{p}}\,. \tag{1.4}$$

1.3 Properties of Single-Mode Fibers

The QKD system described in this thesis consists of fiber-optical components, and the photons are transmitted to the users through single-mode optical fiber links. Therefore, some of the most relevant properties of optical single-mode fibers are briefly discussed.

Typically, optical fibers consist of SiO_2 glass and are highly transparent for near-infrared light [69]. Fibers for long-range telecommunication are designed such that they guide only a single spatial mode in the desired wavelength range, and they are therefore called *single-mode* (SM) fibers. The most widely used type of SM fiber is specified by the International Telecommunication Union (ITU) in the recommendations ITU-T G.652 [70] and fibers following this recommendation are therefore often called *(standard) single-mode fibers* (SMF). A widely-used SMF is the SMF-28 fiber from Corning. SMF-28 guides only a single-mode for wavelengths longer than 1260 nm [71, 72]. Relevant parameters of this fiber are listed in table 1.1.

A cross-section of an SMF is shown in fig. 1.3 (a). It consists of a circular core with a diameter of 8.2 µm, embedded in a 125 µm diameter cladding with a slightly lower refractive index [71]. Such fibers are often protected by a 250 µm diameter polymer coating and embedded in further layers of different materials for mechanical protection. Long-range telecommunication is typically realized in the optical C-band, with wavelengths between 1530 and 1565 nm, because the attenuation is minimal in this wavelength range, as shown in fig. 1.5. Frequency channels in the C-band are specified by the ITU *dense wavelength division multiplexing* (DWDM) grid. The n-th channels center frequency is

Table 1.1: Properties of standard single-mode fiber at a wavelength of 1550 nm [69, 71–73].

Transmission losses	$\leq$ 0.22 dB/km
Effective group index of refraction	$n_g = 1.4682$
Mode field diameter	10.4 µm
Polarization-mode dispersion coefficient	$\leq$ 0.2 ps/$\sqrt{\text{km}}$
Chromatic dispersion	$D = 17$ ps/(nm · km) $\beta = -21.7$ ps^2/km
Typical losses of fiber splices	0.05 to 0.2 dB
Typical losses of pluggable fiber connectors	0.2 to 1 dB

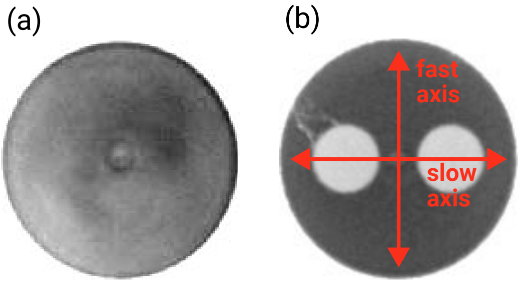


Figure 1.4: Cross section of (a) standard single-mode fiber with 8 µm core diameter and 125 µm cladding and (b) a polarization-maintaining PANDA-fiber with two round stress members embedded in the cladding.

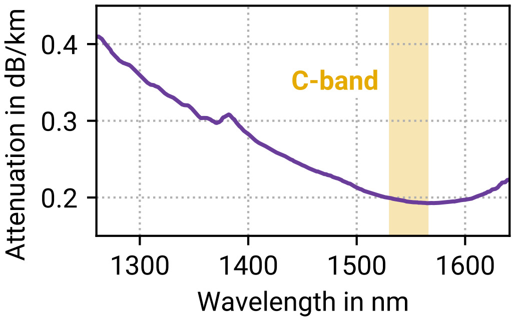


Figure 1.5: Spectral attenuation of standard single-mode fiber. The figure was created with data from ref. [28], showing the attenuation of the QKD field test link (cf. section 3.1).

given by $f_n = 193.1\,\text{THz} + n\Delta f$, with typical channel widths Δf of 12.5, 25, 50, 100 or 200 GHz [74].

SMFs can be connected with relatively low losses, for example, with pluggable connectors, or they can be joined permanently by *splicing* the fibers together. For that, the glass is melted in an electrical arc, and the fibers are attached with the cores aligned. Deployed fiber links often consist of multiple fiber sections, and the connections introduce additional losses. Typical insertion losses are 0.2 to 1 dB for fiber connectors and 0.05 to 0.2 dB for splices [73].

1.3.1 Polarization-Mode Dispersion and Polarization Stability

In general, SMFs do not preserve the polarization state of the transmitted light. Asymmetries of the fiber core, internal mechanical tension, or external mechanical stress introduce a small amount of birefringence. For some fixed wavelength, two orthogonal *principal states of polarization* can be found which are not changed when launched into the birefringent fiber and which travel with different speeds [75, 76]. This effect is called *polarization-mode dispersion* (PMD), and the difference in the travel time of the two states is called *differential group delay*. The birefringence changes over time for deployed fibers exposed to temperature changes and varying mechanical stress. As a result, the polarization of polarized light launched into an SMF is generally transformed into an unknown polarization state. The birefringence introduced by effects such as bending, torsion, and applied pressure is typically stronger than the intrinsical birefringence [69]. Therefore, a long deployed fiber can be envisioned as the concatenation of multiple smaller segments, with randomly distributed birefrigence [69, 75]. The polarization transformation and the differential group delay are therefore given by probability distributions [77] and the expectation value of the differential group delay scales proportionally with the square root of the fiber lengths [69, 77, 78]. The proportionality constant is called *PMD coefficient* and for SMF its values is less than $0.2\,\text{ps}/\sqrt{\text{km}}$ [70]. This value is so small that for many QKD systems, the elongation of the photon wave packets due to the differential group delay can be neglected. However, environmental conditions can affect the birefringence and, thereby, the polarization state in the fiber link, which is highly relevant for QKD.

Some QKD protocols, such as the BB84 QKD protocol explained in section 1.1, use the polarization of the photons to encode the quantum bits, which has the advantage that the polarization analyzers in the receivers are relatively robust and simple to set up. For long-term operation, polarization-sensitive QKD systems require active polarization stabilization to compensate for changing birefringence in the transmission fibers. Some publications report relatively slow polarization changes in the fiber at the time scale of hours to days [79–81], for example, when the transmission fibers are submarine fibers or when they are deployed underground [79, 82]. However, significantly faster polarization changes have been observed for fiber links in urban areas [83]. The impact of polarization variations on polarization-sensitive QKD systems was systematically analyzed in ref. [84]: the required polarization tracking speed was measured to be in the range of multiple rad/s for inter-city and aerial links. A field experiment with a 68 km long aerial fiber link showed that polarization adjustments on the millisecond timescale are necessary for stable QKD over this link [84].

One option to realize polarization realignment is to compensate for the polarization change with polarization controllers such that the QBER is minimized. This method was used recently to demonstrate QKD with polarization-entangled photons over a 248 km long fiber link for over 110 hours [80]. When the QBER exceeded a threshold, an automatic polarization realignment algorithm was used to scan polarization controllers to find a better alignment, which took 57 min on average. In total, 25 % of the measurement time were used for recalibrations.

An advantage of this method is that it does not require additional hardware, such as alignment lasers. The key rate limits the minimum time required for a realignment because a sufficient number of key bits and error bits need to be acquired to estimate the QBER in each alignment step. The method is, therefore, limited to fiber links and QKD systems for which the time between significant polarization changes is considerably longer than the time it takes to complete the realignment. Other stabilization schemes that do not rely on the QBER have been proposed, but they require additional components and increase the complexity of the QKD system [85–87].

Impairments due to polarization instabilities are avoided when QKD protocols with phase- or time-bin encoding are used, such as in the BBM92 protocol described in section 1.2. Instead of polarization stabilization, such systems require phase stabilization of the IFs. However, the IF phases are only sensitive to the local environment of the receivers and unaffected by temperature changes or vibrations of the transmission links. The environments of the receivers are generally better controllable than the fiber links exposed to environmental influences. Therefore, the QKD transmission with time bin QKD systems is stable even when the fiber link is exposed to harsh environmental conditions. Due to these advantages, a time bin QKD protocol was chosen for the q-hub system presented in this thesis.

Polarization-Maintaining Fibers

Parts of the PPS are set up with special *polarization-maintaining* (PM) fibers, which are designed such that they preserve the polarization state of linearly polarized light coupled into the fiber in parallel to the *slow axis* or *fast axis*. Light polarized along the slow axis travels slower through the fiber than light polarized along the fast axis, so cross-talk between the two polarization directions is minimized. The fast and slow axes are defined by introducing a strong birefringence in a particular direction across the core during the manufacturing process [69]. A common variant of PM fiber is the so-called PANDA fiber, where stress-induced birefringence is generated by introducing two cylindrical *stress members* consisting of a material with a different thermal expansion coefficient parallel to the core [69]. The cross-section of a PANDA fiber is shown in fig. 1.3 (b).

1.3.2 Chromatic Dispersion

The field of a coherent optical pulse with an amplitude envelope $A(t)$ varying slowly compared to the period of the angular center frequency ω_0 can be written as

$$\alpha(t) = A(t)\,\mathrm{e}^{-\mathrm{i}\omega_0 t}\,. \tag{1.5}$$

The complex spectra $\tilde{\alpha}(\omega) = \mathcal{F}_t[\alpha(t)](\omega)$ and $\tilde{A}(\omega) = \mathcal{F}_t[A(t)](\omega)$ of the wave packet and its envelope are related by the shift rule of the *Fourier transform* (FT)[1] (cf. eq. (A.6)):

$$\tilde{\alpha}(\omega) = \mathcal{F}_t\big(A(t)\,\mathrm{e}^{-\mathrm{i}\omega_0 t}\big)(\omega) = \tilde{A}(\omega - \omega_0) \tag{1.6}$$

The shape of the temporal power distribution of the wave packet is proportional to $|\alpha(t)|^2$ and the spectral power distribution is proportional to the *spectral density* $|\tilde{\alpha}(\omega)|^2$.

When the wave packet travels through a medium such as an optical fiber, the field after the medium can be expressed in the time domain by using the *impulse response* $h(t)$ or in the frequency domain by using the *frequency response* $\tilde{h}(\omega) = \mathcal{F}_t[h(t)](\omega)$ of the medium, and both expressions are related by the convolution theorem (cf. eq. (A.11))[2]:

$$\tilde{\alpha}_{\text{out}}(\omega) = \tilde{h}(\omega)\tilde{\alpha}(\omega) \quad \text{and} \tag{1.7}$$

$$\alpha_{\text{out}}(t) = \frac{1}{\sqrt{2\pi}}(\alpha * h)(t) = \frac{1}{\sqrt{2\pi}}\int \alpha(\tau)h(t-\tau)\,\mathrm{d}\tau\,. \tag{1.8}$$

The frequency response for the propagation through a medium such as a fiber of length L is given by

$$\tilde{h}_{\text{prop}}(\omega) = \mathrm{e}^{\mathrm{i}k(\omega)L} \tag{1.9}$$

with the frequency-dependent wave number $k(\omega) = n(\omega)\omega/c_0$, the refractive index $n(\omega)$ and the speed of light c_0. For wave packets with a narrow bandwidth, it is usually sufficient

[1] The Fourier transform and the inverse Fourier transform are denoted by $\mathcal{F}$ and $\mathcal{F}^{-1}$. Multiple definitions of the Fourier transform with different prefactors and sign conventions exist in the literature. The definitions used in this thesis and some other mathematical relations are listed in appendix A.

[2] For integrals from $-\infty$ to ∞ the bounds are omitted for brevity.

to consider a Taylor expansion of the frequency-dependent wave number up to the quadratic term around ω_0 [69, 88]:

$$k(\omega) = k_0 + \left.\frac{\partial k}{\partial \omega}\right|_{\omega_0} (\omega - \omega_0) + \frac{1}{2}\left.\frac{\partial^2 k}{\partial \omega^2}\right|_{\omega_0} (\omega - \omega_0)^2 + \mathcal{O}\big((\omega - \omega_0)^3\big) \tag{1.10}$$

$$\approx k_0 + \frac{1}{v_g}\Omega + \frac{\beta}{2}\Omega^2 \tag{1.11}$$

Here, the abbreviation $\Omega = \omega - \omega_0$ is used, and the $\mathcal{O}(\Omega^3)$ term will be neglected in the following. The quantity v_g is the *group velocity* and β is the *group velocity dispersion*[3]. These parameters are related to the frequency derivatives of the refractive index [69]:

$$\frac{1}{v_g} = \frac{n_g}{c_0} = \frac{1}{c_0}\left(n(\omega) + \omega\frac{\partial n}{\partial \omega}\right)\Bigg|_{\omega_0} \quad \text{and} \quad \beta = -\frac{\lambda_0^2}{2\pi c_0}D = \frac{1}{c_0}\left(2\frac{\partial n}{\partial \omega} + \omega\frac{\partial^2 n}{\partial \omega^2}\right)\Bigg|_{\omega_0} \tag{1.12}$$

For $\partial n/\partial \omega|_{\omega_0} \neq 0$, the *group index* n_g and the group velocity are different from $n(\omega_0)$ and from the phase velocity $c_0/n(\omega_0)$. The center of the wave packet travels with v_g through the medium. The dependence of v_g on the wavelength is called *chromatic dispersion* (CD) and quantified by β. In optical fiber communications, often the *dispersion parameter D* in units of ps/(nm · km) with an intuitive meaning is used instead of β: When two light pulses with center frequencies separated by a small wavelength difference $\Delta\lambda$ are launched into an optical fiber of length L, they arrive at the end of the fiber with a time difference of [69]

$$\Delta t = DL\,\Delta\lambda\,. \tag{1.13}$$

Typical values for SMFs at 1550 nm are $n_g \approx 1.47$ and $D = 17\,\text{ps}/(\text{nm}\cdot\text{km})$. The sign of D is positive, meaning that a wave packet at shorter wavelengths travels faster than a wave packet at longer wavelengths, which is called anomalous dispersion [69]. Around 1310 nm, the dispersion parameter of SMF crosses zero and becomes negative for even shorter wavelengths.

Effects of Chromatic Dispersion on a Traveling Wave Packet

The impulse response for the propagation through a medium with wave number k is obtained by the *inverse Fourier transformation* (IFT) $h_{\text{prop}}(t) = \mathcal{F}_\omega^{-1}\{\exp[\mathrm{i}k(\omega)L]\}$. Using

[3] In the literature, this value is often denoted β_2, but here the index is dropped for brevity.

the second-order approximation for $k(\omega)$ from eq. (1.11) and the complex Gaussian integrals from eqs. (A.1) and (A.2) yields [89, 90]

$$h_{\text{prop}}(t) = \begin{cases} \exp[\mathrm{i}(k_0 L - \omega_0 t)]\sqrt{2\pi}\,\delta(T) & \text{for} \quad \beta = 0 \quad \text{and} \\ \exp[\mathrm{i}(k_0 L - \omega_0 t)]\sqrt{\dfrac{\mathrm{i}}{\beta L}}\exp\left(-\dfrac{\mathrm{i}T^2}{2\beta L}\right) & \text{for} \quad \beta \neq 0 \end{cases} \tag{1.14}$$

with $T = t - L/v_\mathrm{g}$ and the Dirac delta distribution $\delta(T)$.

When $\beta = 0$, the pulse shape is unchanged by the propagation through the medium, and the pulse is shifted by the time L/v_g. For $\beta \neq 0$, using the time-domain or the frequency-domain approach from eqs. (1.7) and (1.8) yields

$$\begin{aligned} \alpha_{\text{out}}(t) &= \mathcal{F}_\omega^{-1}\big(\tilde{h}_{\text{prop}}(\omega)\mathcal{F}_\tau[\alpha(\tau)](\omega)\big)(t) \\ &= \exp[\mathrm{i}(k_0 L - \omega_0 t)]\,\mathcal{F}_\Omega^{-1}\left[\exp\left(\mathrm{i}\frac{\beta L}{2}\Omega^2\right)\mathcal{F}_\tau[A(\tau)](\Omega)\right](T) \quad \text{or} \end{aligned} \tag{1.15}$$

$$\begin{aligned} \alpha_{\text{out}}(t) &= \frac{1}{\sqrt{2\pi}}(a * h_{\text{prop}})(t) \\ &= \exp[\mathrm{i}(k_0 L - \omega_0 t)]\sqrt{\frac{\mathrm{i}}{\beta L}}\exp\left(-\frac{\mathrm{i}T^2}{2\beta L}\right)\mathcal{F}_\tau\left[A(\tau)\exp\left(-\frac{\mathrm{i}\tau^2}{2\beta L}\right)\right]\left(\frac{T}{\beta L}\right) \end{aligned} \tag{1.16}$$

An essential step in the derivation of eq. (1.16) is the separation of the square in the exponential that is obtained by convolving eq. (1.14) with $A(t)$ and recognizing the term proportional to $\tau T/(\beta L)$ as a FT with respect to τ, evaluated at $T/\beta L$. Equations (1.15) and (1.16) both map $A(t)$ to $\alpha_{\text{out}}(t)$. They are analytically equivalent but conceptually different. Equation (1.15) is the standard approach, requiring an FT of the pulse envelope, the multiplication by the phase factor with quadratic Ω-dependence, and an IFT back into the time domain. When βL is relatively large, the quadratic phase term in eq. (1.15) oscillates rapidly. For a numerical computation using the *fast Fourier transformation* (FFT), a fine frequency resolution is necessary to resolve these oscillations and avoid aliasing.

Andrianov's Method for Computing the Shape of Wave Packets with Large Dispersion

Equation (1.16) requires, in contrast to eq. (1.15), only a single FT and its structure reveals some additional properties of $\alpha_{\text{out}}(t)$ in the limit of large dispersions. The exponential with a quadratic argument in T shows that CD introduces a chirp, that is a dependence $\partial^2\phi(t)/\partial t^2 \neq 0$ of the signal phase $\phi(t)$. Andrianov et al. recognized in ref. [91] that evaluating eq. (1.16) by using the FFT can be computationally much more efficient than evaluating eq. (1.15) when the dispersion is large. This approach to computing the wave packet after a dispersive element will therefore be referred to as *Andrianov's method* in the following. When the dispersion βL is large, the complex exponential in the FT is almost constant over the times where $A(t)$ is nonzero, such that the pulse shape attains the shape of the spectral density of the initial pulse envelope, which is known as *wavelength-to-time mapping* or *frequency-to-time mapping* [90, 92–95]:

Mapping of the spectral density to the time domain due to chromatic dispersion

$$|\alpha_{\text{out}}(t)|^2 \underset{\beta L\to\infty}{\propto} \left|\tilde{A}\left(\frac{t - L/v_{\text{g}}}{\beta L}\right)\right|^2 . \tag{1.17}$$

Equation (1.17) shows that large values of βL elongate the wave packet proportional to βL. When Andrianov's method is used, the FT in eq. (1.16) is evaluated at $T/(\beta L)$, meaning that the grid of time values scales automatically with the elongation.

The dispersion-induced elongation can be compensated by introducing *dispersion-compensating fibers* (DCFs) into a fiber link [96]. When the values β_{DCF} and L_{DCF} of such a fiber are chosen such that $\beta L + \beta_{\text{DCF}} L_{\text{DCF}} = 0$, the DCF compensates the dispersion of the regular fiber, such that the pulses are not elongated. Figure 1.6 shows D for the deployed fiber link used during the QKD field test and for two DCF modules. The values for the fiber length and dispersion parameter were measured using an *optical time-domain reflectometer* (OTDR)[4] and a chromatic dispersion test set[5].

To compute the shape of a dispersed wave packet numerically by using the FFT, $A(t)$ is discretized on an interval I_τ centered around $\tau = 0$ with a resolution $\Delta\tau$. Of course, $\Delta\tau$ must be chosen small enough such that all relevant details of $A(\tau)$ are resolved, and I_τ must be chosen large enough such that it covers the complete range where $A(\tau)$ attains non-negligible values. Furthermore, by using the Nyquist-Shannon sampling theorem[6], a condition for $\Delta\tau$ and I_τ can be derived which must be fulfilled to avoid aliasing from the quadratic phase terms in the FTs. The phase between adjacent data points needs to be less than π, which means that $\Delta\tau$ and I_τ need to be chosen such that

$$I_\tau \Delta\tau \begin{cases} > |2\pi\beta L| & \text{for the standard method (eq. (1.15)) and} \\ < |2\pi\beta L| & \text{for Andrianov's method (eq. (1.16)).} \end{cases} \tag{1.18}$$

A slightly different threshold is provided in ref. [91]. Due to eq. (1.18), one of the methods may require much less discretization points and much less computational resources than the

[4] OTDR device: FTB-7400E from *EXFO*.

[5] Chromatic dispersion test set: FD440 from *Perkin Elmer*.

[6] The Nyquist-Shannon sampling theorem state that a signal with frequency components up to frequency f can be reconstructed from samples of the signal when the sample spacing in time is $1/(2f)$ or less [97].

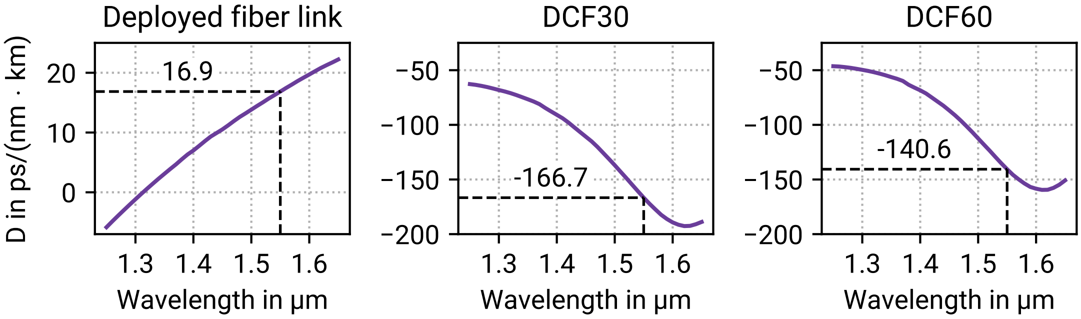


Figure 1.6: Measured wavelength-dependent group velocity dispersion parameter D for the SMF of the QKD field test link (cf. section 3.1) and for two dispersion compensation modules, DCF30 and DCF60, compensating 30 or 60 km of SMF, respectively. The lengths of the DCFs measured by OTDR were 3.1 km for DCF30 and 7.35 km for DCF60, assuming the same group velocity as for SMF. The dashed line marks the value of D at a wavelength of 1550 nm.

other. The standard method is better suited when the dispersion is small, and Andrianov's method is better suited when the dispersion is large. Equation (1.18) does not take the phase of $\mathcal{F}_\tau[A(\tau)](\Omega)$ in eq. (1.15) or of $A(\tau)$ in eq. (1.16) into account, such that for practical implementation, $I_\tau \Delta\tau$ should not be chosen too close to $|2\pi\beta L|$. Depending on the values of βL, one method or the other is used in the simulations of the QKD system in chapter 7 to compute dispersed entangled biphoton wave packets.

1.4 Spontaneous Parametric Down-Conversion

The central element of QKD network presented in this thesis is the quantum key hub comprising a source of entangled photon pairs and a *wavelength-division demultiplexer* (WDM). The photon pairs are generated by *spontaneous parametric down-conversion* (SPDC). In SPDC, a medium with an optical second-order nonlinear susceptibility $\chi^{(2)}$ moderates a three-wave mixing process in which a pump photon is spontaneously converted with low probability into two photons called *signal* and *idler* [98]. Due to energy conservation, the sum of the signal and idler photon energies equals the pump photon energy [98]:

Energy conservation in spontaneous parametric down-conversion

$$\underbrace{\hbar\omega_\mathrm{s}}_{\text{Signal energy}} + \underbrace{\hbar\omega_\mathrm{i}}_{\text{Idler energy}} = \underbrace{\hbar\omega_\mathrm{p}}_{\text{Pump photon energy}} \qquad (1.19)$$

A SPDC process must therefore be pumped with light at 775 nm to obtain two photons in the C-band at 1550 nm. In the simplest case, the production of photon pairs in one signal mode and one idler mode is described by the operator $\hat{U} = \exp(-\mathrm{i}\hat{H}/\hbar)$ with $\hat{H} = \mathrm{i}\chi\hbar\,\hat{a}_\mathrm{p}\hat{a}_\mathrm{s}^\dagger\hat{a}_\mathrm{i}^\dagger + \mathrm{H.c.}$ [99]. The operator $\hat{H}$ converts one pump photon into a signal-idler pair: $\hat{H}|1\rangle_\mathrm{p}|0\rangle_\mathrm{s}|0\rangle_\mathrm{i} = \mathrm{i}\chi\hbar\,|0\rangle_\mathrm{p}|1\rangle_\mathrm{s}|1\rangle_\mathrm{i}$. Here, the coefficient χ incorporates all constants determining the strengths of the interaction and depends on the properties of the nonlinear medium. As the nonlinearity is typically small, the conversion probability is low, and strong pump fields are required to generate a significant amount of photon pairs. Therefore, the strong pump light can be assumed to be classical coherent laser light, allowing to replace the annihilation operator by the pump field amplitude α. Writing $\alpha\chi = r\,\mathrm{e}^{\mathrm{i}\theta}$ with $r, \theta \in \mathbb{R}$ yields the SPDC state [99, 100]

$$|\psi\rangle_\mathrm{TMSV} = \exp\!\big(r\,\mathrm{e}^{\mathrm{i}\theta}\hat{a}_\mathrm{s}^\dagger\hat{a}_\mathrm{i}^\dagger - r\,\mathrm{e}^{-\mathrm{i}\theta}\hat{a}_\mathrm{s}\hat{a}_\mathrm{i}\big)|0\rangle = \frac{1}{\cosh r}\sum_{n=0}^{\infty}(\mathrm{e}^{\mathrm{i}\theta}\tanh r)^n|n_\mathrm{s}\rangle|n_\mathrm{i}\rangle\,. \tag{1.20}$$

Here, $|n_\mathrm{s}\rangle = \big(\hat{a}_\mathrm{s}^\dagger\big)^n|0\rangle/\sqrt{n}$ and $|n_\mathrm{i}\rangle = \big(\hat{a}_\mathrm{i}^\dagger\big)^n|0\rangle/\sqrt{n}$ are the n-photon signal and idler Fock states. The state is called *two-mode squeezed vacuum* (TMSV) state because it is similar to the single-mode squeezed state $\exp\!\big(-\chi\hat{a}^{\dagger 2}/2 + \chi^*\hat{a}^2/2\big)|0\rangle$, but involves two different modes for signals and idlers. In each term of the series expansion in eq. (1.20), the number of the signal and idler photons are the same, meaning that zero to infinitely many signal-idler pairs are produced with decreasing probability. The probability to find N photon pairs in the state is given by [101]

$$p(n\text{ pairs}) = \frac{\mu_\mathrm{p}^n}{(1+\mu_\mathrm{p})^{n+1}}\,, \tag{1.21}$$

with the *mean photon pair number* $\mu_\mathrm{p} = \sinh^2(r)$. The photon pair probability distribution in eq. (1.21) is the same probability distribution that describes the photon number distribution of a single-mode thermal light source [99].

In entanglement-based QKD, the generation of multiple photon pairs can lead to quantum bit errors when Alice and Bob detect photons from different pairs because these photons are not entangled. The effect of the generation of two pairs on time-bin entanglement experiments was analyzed in ref. [102]. The simulations of the q-hub system in chapters 6 and 7 consider effects from multi-photon-pair emission of all orders systematically.

Broadband SPDC

SPDC generally produces photon pairs in wave packets with a broader spectrum and some spatial distribution. As the nonlinear crystals employed in the q-hub QKD system only guide a single spatial mode, spatial dependencies are irrelevant. For the wave packets, wave packet creation operators and annihilation operators are introduced. A single photon wave packet ξ, for example, can be described by the state $|1_\xi\rangle = \hat{a}_\xi^\dagger|0\rangle$. Assuming that the bandwidth of the field excitation is much smaller than the optical center frequency, the wave packet creation operator can be represented as [103, 104]

$$\hat{a}_\xi^\dagger = \int \xi(t)\hat{a}^\dagger(t)\,\mathrm{d}t = \int \tilde{\xi}(\omega)\hat{a}^\dagger(\omega)\,\mathrm{d}\omega\,. \tag{1.22}$$

Here, $\hat{a}^\dagger(t)$ and $\hat{a}^\dagger(\omega)$ describe the creation of a photon at time t or at frequency ω, respectively. The functions $\xi(t)$ and $\tilde{\xi}(\omega)$ are related by $\tilde{\xi}(\omega) = \mathcal{F}_t[\xi(t)](\omega)$ and similarly, $\hat{a}^\dagger(t)$ and $\hat{a}^\dagger(\omega)$ are related by [103]

$$\hat{a}(t) = \mathcal{F}_\omega^{-1}(\hat{a}(\omega))(t) = \frac{1}{\sqrt{2\pi}}\int \hat{a}(\omega)\,\mathrm{e}^{-\mathrm{i}\omega t}\,\mathrm{d}\omega \quad \text{and} \tag{1.23}$$

$$\hat{a}^\dagger(t) = \left(\mathcal{F}_\omega^{-1}\right)^*\left(\hat{a}^\dagger(\omega)\right)(t) = \frac{1}{\sqrt{2\pi}}\int \hat{a}^\dagger(\omega)\,\mathrm{e}^{\mathrm{i}\omega t}\,\mathrm{d}\omega \tag{1.24}$$

with the commutators $\left[\hat{a}(t), \hat{a}^\dagger(t')\right] = \delta(t-t')$ and $\left[\hat{a}(\omega), \hat{a}^\dagger(\omega')\right] = \delta(\omega-\omega')$ [103]. Using these continuous-mode operators, a broadband SPDC state can be written as[7] [98]

Broadband biphoton state generated by spontaneous parametric down-conversion

$$|\psi_{\mathrm{SPDC}}\rangle = \exp\!\left(\frac{\chi}{2}\iint \tilde{\psi}(\omega_\mathrm{s},\omega_\mathrm{i})\hat{a}^\dagger(\omega_\mathrm{s})\hat{a}^\dagger(\omega_\mathrm{i})\,\mathrm{d}\omega_\mathrm{s}\,\mathrm{d}\omega_\mathrm{i} - \mathrm{H.c.}\right)|0\rangle \tag{1.25}$$

$$= \exp\!\left(\frac{\chi}{2}\iint \psi(t_\mathrm{s},t_\mathrm{i})\hat{a}^\dagger(t_\mathrm{s})\hat{a}^\dagger(t_\mathrm{i})\,\mathrm{d}t_\mathrm{s}\,\mathrm{d}t_\mathrm{i} - \mathrm{H.c.}\right)|0\rangle \tag{1.26}$$

with the biphoton wave packet $\psi(t_\mathrm{s}, t_\mathrm{i})$. It is convenient to absorb all constant amplitudes into the real coefficient χ and complex phases into $\tilde{\psi}$ and to normalize the *joint spectral amplitude* (JSA) $\tilde{\psi}(\omega_\mathrm{s}, \omega_\mathrm{i}) = \mathcal{F}_{t_\mathrm{s},t_\mathrm{i}}\big(\psi(t_\mathrm{s}, t_\mathrm{i})\big)(\omega_\mathrm{s}, \omega_\mathrm{i})$ to

$$\iint \left|\tilde{\psi}(\omega_\mathrm{s},\omega_\mathrm{i})\right|^2 \mathrm{d}\omega_\mathrm{s}\,\mathrm{d}\omega_\mathrm{i} = 1\,. \tag{1.27}$$

[7] The derivation of eq. (1.25) involves multiple assumptions [98]: The pump is assumed to be classical undepleted coherent light. The nonlinear medium is assumed to be lossless, much longer than the wavelengths, and to have a frequency-independent nonlinear susceptibility. Effects from time ordering [105] are ignored. The pump, signal, and idler fields are assumed to have a bandwidth much narrower than the optical center frequency.

First-Order Approximation of the Generated Biphoton State

When the SPDC interaction is weak, such that $\chi \ll 1$, the SPDC state can be approximated by the first order expansion of eq. (1.25):

$$|\psi_{\mathrm{SPDC}}\rangle \approx |0\rangle + \frac{\chi}{2} \iint \tilde{\psi}(\omega_{\mathrm{s}}, \omega_{\mathrm{i}}) \hat{a}_s^\dagger(\omega_{\mathrm{s}}) \hat{a}_i^\dagger(\omega_{\mathrm{i}})\, \mathrm{d}\omega_{\mathrm{s}}\, \mathrm{d}\omega_{\mathrm{i}} |0\rangle \,. \tag{1.28}$$

To facilitate some of the following considerations, it is convenient to drop the vacuum part and to consider only the wave packet containing exactly one photon pair,

$$|\psi\rangle = \iint \tilde{\psi}(\omega_{\mathrm{s}}, \omega_{\mathrm{i}}) \hat{a}_s^\dagger(\omega_{\mathrm{s}}) \hat{a}_i^\dagger(\omega_{\mathrm{i}})\, \mathrm{d}\omega_{\mathrm{s}}\, \mathrm{d}\omega_{\mathrm{i}} |0\rangle \,. \tag{1.29}$$

For this state, the two-dimensional probability density to detect the signal and idler photons at times t_{s} and t_{i} is given by $|\psi(t_{\mathrm{s}}, t_{\mathrm{i}})|^2$ and the joint spectral density is given by $|\tilde{\psi}(\omega_{\mathrm{s}}, \omega_{\mathrm{i}})|^2$. The coefficient $\chi/2$ has been dropped and the state is normalized to $|\langle\psi|\psi\rangle|^2 = 1$ according to eq. (1.27). The probability to jointly detect the signal photon in time interval I_{A} and the idler photon in I_{B} is given by

$$p[(\text{signal in } I_{\mathrm{A}}) \cap (\text{idler in } I_{\mathrm{B}})] = \int_{I_{\mathrm{A}}} \int_{I_{\mathrm{B}}} |\psi(t_{\mathrm{s}}, t_{\mathrm{i}})|^2\, \mathrm{d}t_{\mathrm{s}}\, \mathrm{d}t_{\mathrm{i}} \,. \tag{1.30}$$

The probability density $p_{\mathrm{s}}(t_{\mathrm{s}})$ for the detection of a signal photon (and, analogously, for an idler photon) at time t_{s} and the spectral density S_{s} to detect it at the frequency ω_{s} are given by the marginal distributions

$$p_{\mathrm{s}}(t_{\mathrm{s}}) = \int |\psi(t_{\mathrm{s}}, t_{\mathrm{i}})|^2\, \mathrm{d}t_{\mathrm{i}} \quad \text{and} \quad S_{\mathrm{s}}(\omega_{\mathrm{s}}) = \int |\tilde{\psi}(\omega_{\mathrm{s}}, \omega_{\mathrm{i}})|^2\, \mathrm{d}\omega_{\mathrm{i}} \,. \tag{1.31}$$

The JSA can be factored into the pump pulse spectrum $\tilde{\alpha}(\omega)$ and the *phase matching function* $\tilde{\Phi}$ determined by the properties of the nonlinear medium [98]. Due to energy conservation, signal and idler fields at ω_{s} and ω_{i} are produced by pump light at the sum frequency $\omega_{\mathrm{p}} = \omega_{\mathrm{s}} + \omega_{\mathrm{i}}$:

$$\tilde{\psi}(\omega_{\mathrm{s}}, \omega_{\mathrm{i}}) = \tilde{\Phi}(\omega_{\mathrm{s}}, \omega_{\mathrm{i}})\, \tilde{\alpha}(\omega_{\mathrm{s}} + \omega_{\mathrm{i}}) \tag{1.32}$$

For further considerations, it is convenient to normalize the pump pulse to

$$\int |\tilde{\alpha}(\omega)|^2\, \mathrm{d}\omega = 1 \,. \tag{1.33}$$

The Phase Matching Function

The shape of the phase-matching function depends on the properties of the nonlinear medium. For a crystal waveguide of length L centered at $z = 0$ it is given by [106–108]

$$\tilde{\Phi}(\omega_\mathrm{s}, \omega_\mathrm{i}) = \int_{-L/2}^{L/2} s(z) \exp\left(\mathrm{i} \int_{-L/2}^{z} \Delta k(\omega_\mathrm{s}, \omega_\mathrm{i}, \xi)\, \mathrm{d}\xi \right) \mathrm{d}z\,. \tag{1.34}$$

The function $s(z)$ is proportional to the nonlinear susceptibility and the *phase mismatch* is

$$\Delta k(\omega_\mathrm{s}, \omega_\mathrm{i}, \xi) = \frac{1}{c_0}\big[n_\mathrm{p}(\omega_\mathrm{s} + \omega_\mathrm{i}, \xi)(\omega_\mathrm{s} + \omega_\mathrm{i}) - n_\mathrm{s}(\omega_\mathrm{s}, \xi)\omega_\mathrm{s} - n_\mathrm{i}(\omega_\mathrm{i}, \xi)\omega_\mathrm{i}\big]\,. \tag{1.35}$$

The subscripts “p”, “s”, and “i” indicate the refractive index of pump, signal, and idler. When signal and idler photons are parallel polarized, $n_\mathrm{s}(\omega)$ and $n_\mathrm{i}(\omega)$ are equal.

The SPDC processes are distinguished based on the polarization of the photons. When the photons are parallel polarized to the pump light, the process is called *type-0 SPDC*. When they are orthogonally polarized to each other, the process is called *type-II SPDC*.

For a nonlinear susceptibility independent of z, the integral in eq. (1.34) becomes maximal for the frequencies where the phase matching condition $\Delta k = 0$ is fulfilled, which is, in general, the case at frequencies outside of the desired frequency range. To realize phase matching at a specific frequency, the orientation of the susceptibility and thereby $s(z)$ is periodically inverted during the crystal manufacturing, which is called *periodic poling*. A periodic function $s(z)$ can be written as a complex Fourier series $s(z) = \sum_{m=-M}^{M} s_m\, \mathrm{e}^{-\mathrm{i}2\pi m z/\Lambda}$. By choosing a poling period of $\Lambda = 2\pi/\Delta k(2\omega_0, \omega_0, \omega_0)$, phase matching for $m = 1$ at $\omega_\mathrm{s} = \omega_\mathrm{i} = \omega_0$ is achieved, such that $\Delta k - 2\pi/\Lambda \approx 0$ around these frequencies. For different m, the phase matching condition $\Delta k = 0$ is fulfilled at wavelengths far away from the spectral region of interest, such that typically, only one term of the Fourier series contributes. By including the periodic poling, eq. (1.34) becomes [106–108]

$$\tilde{\Phi}(\omega_\mathrm{s}, \omega_\mathrm{i}) \propto \int_{-L/2}^{L/2} \exp\left[-\mathrm{i}\left(\frac{2\pi z}{\Lambda} - \int_{-L/2}^{z} \Delta k(\omega_\mathrm{p}, \omega_\mathrm{s}, \omega_\mathrm{i}, \xi)\, \mathrm{d}\xi \right) \right] \mathrm{d}z\,, \tag{1.36}$$

which can be simplified for an ideal crystal with Δk independent of z to[8]

$$\tilde{\Phi}(\omega_\mathrm{s}, \omega_\mathrm{i}) \propto \mathrm{sinc}\left[\left(\frac{\Delta k(\omega_\mathrm{s}, \omega_\mathrm{i})}{2} - \frac{\pi}{\Lambda} \right) L \right]. \tag{1.37}$$

By using periodic poling, photon pairs around 1550 nm can be generated by type-0 SPDC and type-II SPDC in *periodically poled lithium niobate* (PPLN) crystals.

[8] Following ref. [98], in this thesis the definition $\mathrm{sinc}(x) = \sin(x)/x$ is used (cf. eq. (A.22)), in contrast to other literature such as ref. [109] defining $\mathrm{sinc}(x) = \sin(\pi x)/(\pi x)$.

2 Development of a Multi-User QKD Network with a Central Quantum Key Hub

One of the central research goals of this doctoral thesis is to develop a *quantum key hub* (q-hub), which is the central element of a star-shaped multi-user QKD network comprising a source of entangled photon pairs and a demultiplexer to distribute the photons to the network users. The q-hub QKD system presented in this chapter is the successor of a QKD system for two users, presented in the Ph.D. thesis of Oleg Nikiforov [28]. For the first tests, a free-space photon pair source generating orthogonally polarized photons for the two-user QKD system was realized in close collaboration with Oleg Nikiforov and Daniel Hofmann during Hofmann's master's thesis [M1]. Experiments showed that a fiber-based PPS would be more suitable for the q-hub because it would be more robust and more flexible. Therefore, a fiber-based PPS was designed to meet the specific requirements and laser safety regulations for the on-site field test of the q-hub network at a facility of *Deutsche Telekom*. It was then realized with Oleg Nikiforov and Maximilian Tippmann during Tippmann's master's thesis [M4].

Another major research challenge of the project was the development of the IFs required to implement the time bin BBM92 QKD protocol. Setting up the IFs requires only a few off-the-shelf fiber-optic components, but to achieve low QBERs, the OPDs of the IFs must be precisely matched. The high requirements on the IF quality may be one reason why, so far, the time bin BBM92 protocol has not been used to implement multi-user QKD networks. A new method to build multiple IFs quickly and reliably has been developed. The IFs for the two-user QKD system and the q-hub system were built using this method, and a patent of O. Nikiforov, E. Fitzke, and Th. Walther for the method is pending.

An important advancement compared to the two-user system is the synchronization of the QKD receiver clocks. While synchronization for the two-user system was achieved by using electrical cables, for the q-hub system, a method using *clock recovery* from the arrival time of the photons was developed. A patent of E. Fitzke and Th. Walther for the clock-recovery method is pending.

Section 2.1 describes the general concept of the q-hub and the realized setup consisting of a PPS and a WDM in detail. The PPS comprises several in-house-made modules that can be combined in different arrangements, providing flexibility for experiments.

Section 2.2 presents setups for measuring photon pair spectra: a dispersion-based spectrometer setup and a commercial grating spectrograph placed in a controlled environment, allowing for cooling to 8 °C. A model is developed to explain the asymmetry of the type-II spectra, enabling the reconstruction of the complex-valued spectrum required for the QKD simulation in chapter 7. Furthermore, a model for calculating the generated photon pair rate from measured photon timestamps is developed, taking into account effects from the detector dead times, afterpulses, dark counts, and frequency-dependent losses. The model is applied to determine the SPDC conversion efficiencies of the wavelength converters employed in the q-hub.

In section 2.3, the requirements on the OPD accuracy and IF delays are calculated. The optical setup of the in-house-made IFs is described.

Section 2.4 presents further parts of the QKD receivers, such as the timing acquisition and the temperature-stabilized interferometer containers. A brief overview of the largely automated network operation is provided.

Section 2.5 describes the synchronization of the receivers using a new method for clock recovery from the arrival times of the photons. The stability of the receiver clocks is analyzed, and the performance of the clock recovery is investigated.

Details about this PPS will be published in ref. [VIII]. The whole q-hub network and first results of the field test are presented in publication [II].

2.1 Setup of the Quantum Key Hub

A star-shaped QKD network with a central q-hub is schematically shown in fig. 2.1 (a). The q-hub enables simultaneous, pairwise, independent QKD in the network and implements the BBM92 QKD protocol described in section 1.2. The essential element of the q-hub is a PPS generating photon pairs with a spectrum much broader than the spectrum of the pump light. The photon pairs are generated by SPDC, and the energy conservation condition from eq. (1.19) ensures that the sum of the signal and idler frequencies ω_s and ω_i equals the frequency ω_p of the light pumping the SPDC process. This means that the frequencies of each of the photons can vary in a wide range determined by the phase-matching bandwidth, but the sum of the frequencies of both photons from a pair can only vary in the narrow spectral range of the pump light. As a consequence, the frequencies of the photons are anti-correlated. Multiple pairs of users can, therefore, be addressed by demultiplexing the photon spectrum into multiple frequency channels and assigning channels with symmetric

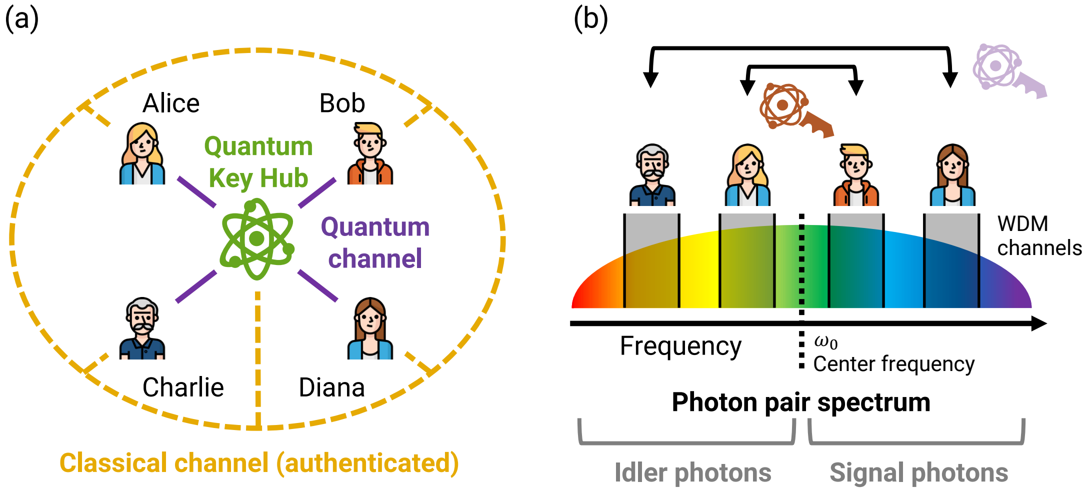


Figure 2.1: Concept of the quantum key hub (q-hub). (a) Star-shaped QKD network with four users *Alice*, *Bob*, *Charlie*, and *Diana* receiving photon pairs from the q-hub through a quantum channel. A classical channel enables communication for network management and key postprocessing. (b) Distribution of photon pairs to the users using a wavelength-division demultiplexer (WDM). Energy conservation ensures that the frequencies of signal and idler photons are symmetric around the center frequency, such that Alice and Bob obtain a quantum key and Charlie and Diana simultaneously obtain a different one.

spacing around the center frequency to pairs of users that want to exchange quantum keys (cf. fig. 2.1 (b)) [110]. Using this principle, $2N$ users in N pairs can exchange quantum keys simultaneously. The maximum number of usable channel pairs depends on the width of the photon pair spectrum as well as the width and spacing of the WDM channels.

The distribution of quantum keys between all possible user combinations in star-shaped QKD networks with more than two users have been realized by using *wavelength-division demultiplexers* (WDM) and time-division demultiplexing [26, 111, 112]. Instead of using fixed WDM channel configurations for such networks, the channel assigned can also be switched dynamically based on the key demands in the network. Dynamic networks have been demonstrated by combining a WDM with an optical switch [113] or by using a *wavelength-selective switch* (WSS) as a WDM [27, 114, 115].

A number of publications about entanglement-based multi-user QKD networks were released in the same year as ref. [II], demonstrating that developing such networks is an active field of research:

- A laboratory network with three users equipped with unbalanced Mach-Zehnder IFs and a similar PPS as the one used in the q-hub was demonstrated in ref. [116]. The system uses a protocol with active basis choice in the receivers and requires polarization re-adjustments for stable long-term operation.

- In ref. [117], entanglement distribution between four users and QKD between two users are demonstrated with photon pairs generated in a microring resonator operated in CW (continuous-wave) mode. The two bases are realized by setting up two IFs for each user with different phases. To achieve long-term stability, laser light is injected into the IFs, and the phases are adjusted with a control loop monitoring the interference with a photodiode.

- A fully-connected network for 40 users using a QKD protocol based on chromatic dispersion was presented in ref. [118]. The dispersive elements map the frequency entanglement to the time domain [119, 120], such that the network is polarization-insensitive and does not require IFs. QKD over a partially deployed fiber link using this protocol was demonstrated in ref. [121].

Compared to other entanglement-based QKD systems, the q-hub network combines several unique features. The field test presented in chapter 3 is the first field test of a QKD system with four users using the time bin BBM92 protocol. An advantage of this protocol is its insensitivity to polarization changes in the transmission fiber. The receiver modules are kept very simple to improve the scalability of the number of users. Neither phase shifters nor a classical interference signal are required for the phase stabilization of the IFs, which is solely achieved by temperature adjustments minimizing the QBER [28]. The synchronization of the receivers is achieved by clock recovery from the arrival time of the photons, such that neither an additional synchronization channel nor particularly stable local clocks nor synchronization to a GPS signal are required. Instead of a fully-connected network, a reconfigurable network is implemented. The advantage of reconfigurable networks is that the available resources can be efficiently used to generate keys between the users based on the actual key demands.

The network and the modules were designed according to the following criteria, taking into account experiences from Nikiforov's field test of the two-user QKD system [28]:

Flexibility During development, various experiments beyond the usual QKD operation were necessary. Therefore, the software and hardware are designed to provide the required flexibility. The PPS is designed such that the individual modules can be operated as stand-alone devices. They can be used together for QKD but also individually or in different arrangements for other experiments. Furthermore, future upgrades of the PPS, enabling the implementation of different QKD protocols or photonic integrated circuits for photon pair generation, are easily possible.

Robustness and Compactness The hardware was designed to enable stable QKD during the field test in a server room of *Deutsche Telekom*. The optical setup was built compactly using fiber components to avoid cleaning and re-aligning free-space optics and meet space constraints known from the first field test.

Scalability Photon losses were minimized to enable high key rates and long transmission distances. Although only four receivers were implemented, the q-hub was designed so that a higher number of receivers can be connected.

Compatibility Whenever possible, cost-effective, off-the-shelf components were used to maximize the compatibility with regular optical telecom networks. The center frequency was aligned to the ITU-T DWDM grid [74], so commercial WDMs aligned to this grid can be used to distribute the photons to the users. The receiver modules and the PPS were built to fit into typical 19 inch wide electronics racks.

The general, simplified concept of the PPS of the q-hub is shown in fig. 2.2. Nearly Fourier-

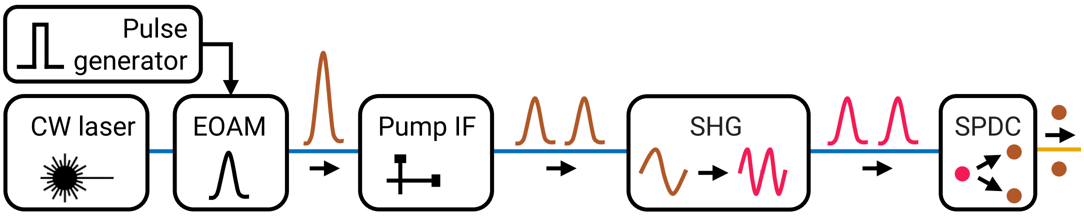


Figure 2.2: Simplified concept of the photon pair source. An electro-optic amplitude modulator (EOAM) shapes CW laser light into pulses, which are split into two half-pulses by the pump interferometer (IF). The pulses are then frequency-doubled in a second-harmonic generation (SHG) stage. Photon pairs are generated by spontaneous parametric down-conversion (SPDC). Polarization-maintaining (PM) fibers are shown in blue, and the single-mode (SM) fiber behind the SPDC is shown in yellow.

limited laser pulses are created by sending CW laser light at the center frequency ω_0 through an *electro-optic amplitude modulator* (EOAM). In the *pump interferometer*, the pulses are split into two half-pulses with a fixed phase relation. Both halves of the pulse pump a *second-harmonic generation* (SHG) process in a nonlinear optical crystal, doubling the center frequency of the pulses to $2\omega_0$. The SHG pulses are then sent into a second nonlinear optical crystal to produce photon pairs by SPDC. This concept has the advantage that widely available fiber components for light around 1550 nm can be used for all parts of the setup except for the connection of the SHG and SPDC stages. Furthermore, using components identical to those installed in the receiver IFs makes it easier to match the OPD precisely to that of the receivers.

For the realization of the PPS according to this scheme, additional components such as amplifiers and optical filters are required. To achieve maximum flexibility, the q-hub is split up into different modules, each comprising all components required to realize one of the core functionalities: a frequency-stabilized seed laser, two inhouse-made *erbium-doped fiber amplifiers* (EDFAs), a pulse generation module, the pump IF, an SHG module, two SPDC modules, and three different WDMs. The modules can be combined in different configurations to realize various experiments. Three arrangements of the modules that are used to generate time-bin entangled photon pairs via type-II SPDC are shown in fig. 2.3. The first group of modules for generating the laser pump pulses is described in section 2.1.1.

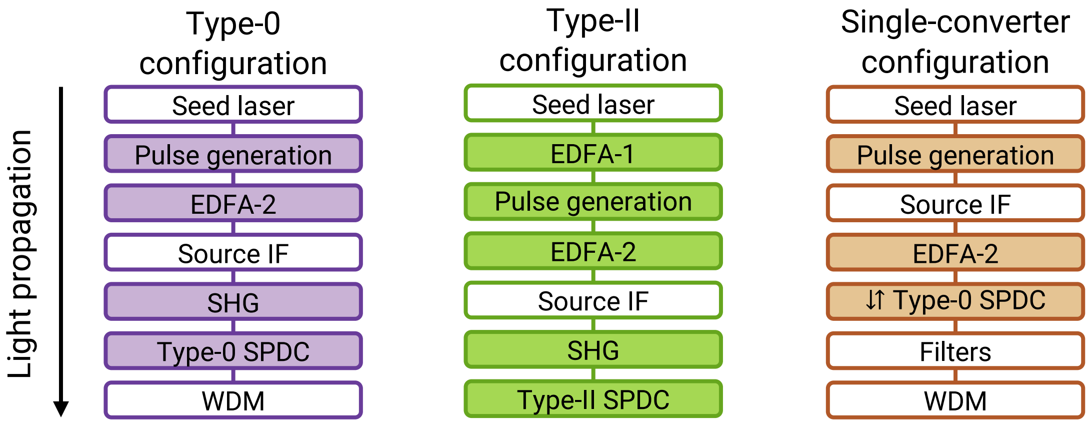


Figure 2.3: Module configuration of the photon pair source for three operation modes. Modules represented by filled boxes can be integrated into a mounting frame for 19 inch wide electronics racks (cf. fig. 2.4). In the single-converter configuration described in detail in section 3.2, the type-0 SPDC module is extended by further components such that it generates SHG light in the forward pass and photon pairs in the backward pass.

Modules for photon pair generation and WDM are described in section 2.1.2. The source interferometer is described together with the receiver interferometers in section 2.3.

A welded steel mounting frame with a height of four standard rack height units holds the EDFAs, the pulse generation state, the SHG module and one of the SPDC modules at a time. Two vertical rows of through-holes at the sides allow mounting the frame in standard 19 inch wide electronics racks. The frame-mountable modules contain most of the optics of the PPS. The module cases are constructed from black anodized aluminum plates. The walls and the top covers are fixed by screws and can be easily removed. All optical connectors are placed at the front panels (cf. fig. 2.4 (a)), and all electrical connections are placed at the rear panels (cf. fig. 2.4 (b)). The EDFA modules and the pulse generation module feature ventilation grids in the front panel and 80 mm fans installed at the rear panels to provide ventilation and remove the heat generated inside the module boxes. Dividing walls are installed inside the box for laser safety, preventing a direct line of sight into the modules. Therefore, direct laser light cannot leave the box via the ventilation openings. Both EDFA modules feature a key switch in the front panel connected to an interlock circuit, so the laser drivers cannot be activated without the keys.

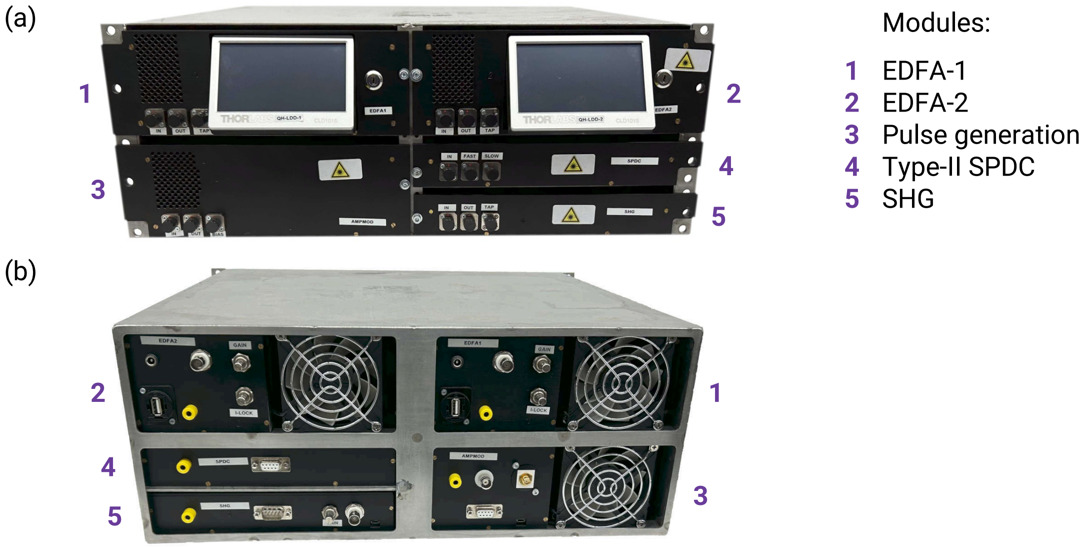


Figure 2.4: Photon pair source consisting of multiple modules in a mounting frame for 19 inch wide electronics racks with a size of 48 cm × 18 cm × 44 cm (width × height × length). (a) Front panels of the modules with connectors for optical fibers. (b) Rear panels with electrical connections and fans.

2.1.1 Laser Pulse Generation

Seed Laser

The seed laser for the PPS is a CW diode laser[1] emitting approximately 25 mW linear polarized light. The seed laser is always operated with a subsequent optical isolator to protect it from possible reflections at subsequent components. The laser has a built-in gas cell filled with the NIST standard reference material 2519a, hydrogen cyanide $\mathrm{H\,^{13}C\,^{14}N}$ [122]. The laser wavelength is locked to an absorption line of the gas cell, providing a precise frequency reference for the q-hub. The center frequency ν_0, angular center frequency ω_0, and the corresponding center wavelength λ_0 of the seed laser are

The center frequency of the q-hub QKD network

$$\omega_0 = 2\pi\nu_0, \quad \nu_0 = 193.350\,171(5)\,\mathrm{THz}\,, \quad \text{and} \quad \lambda_0 = 1550.515\,61(4)\,\mathrm{nm}\,. \tag{2.1}$$

The uncertainty of 5 MHz is determined by the accuracy of the frequency locking and by the linewidth of 1 MHz. While the width of optical spectra, for example, for filters, is often specified in nanometer, the ITU-T DWDM channels are specified in the frequency domain, and a common channel width is 100 GHz [74]. A handy rule of thumb for conversions between wavelength intervals and frequency intervals around 1550 nm is the following scaling factor:

$$\left|\left.\frac{\mathrm{d}\,\lambda(\nu)}{\mathrm{d}\,\nu}\right|_{\nu_0}\right| \approx \frac{0.80\,\mathrm{nm}}{100\,\mathrm{GHz}}\,. \tag{2.2}$$

Pulse Generation Module

The pulse generation module is shown in fig. 2.5. It contains a lithium-niobate-based EOAM[2], a fiber-optic beam splitter, and an electronic high-frequency amplifier[3] amplifying the modulation signal to the voltage of about 5.6 V required to switch the modulator from the completely closed state to the completely open state. The specified bandwidths of the modulator and the amplifier are 10 and 8 GHz.

The modulator must be aligned to completely block incoming light when no electrical signal is applied to the high-frequency input. This is achieved by using a bias controller[4] applying a constant voltage plus a small dither signal at a frequency of 1040 Hz to the electrical bias input of the modulator. A fraction of 10 % of the light after the modulator is split off by the beam splitter and fed into the optical input of the bias controller, and the

[1] Seed laser: Clarity NLL-1550-HP from *Wavelength References, Inc.*

[2] Electro-optic amplitude modulator: MXAN-LN-10 from *iXblue*.

[3] Electronic high-frequency amplifier: DR-DG-10-HO from *iXblue*.

[4] Modulator bias controller: MBC-DG-LAB-A1 from *iXblue*.

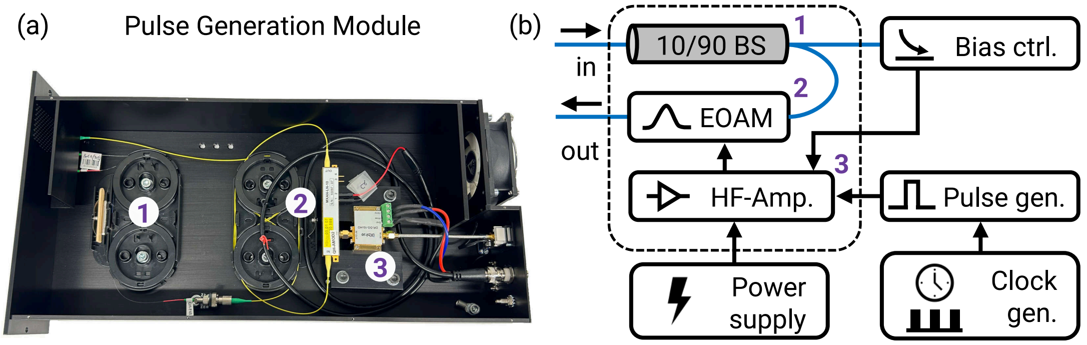


Figure 2.5: Pulse generation module. (a) Photo of the module interior. (b) Scheme of the components. The bias controller, the laboratory power supply, and the pulse generator are not integrated into the module container (dashed line). BS – Beam splitter (10/90 tap coupler), EOAM – Electro-optic amplitude modulator, HF-Amp. – High frequency amplifier. The numbers indicate the location of the components in the container.

controller automatically locks the IF phase to zero by adjusting the bias voltage based on the optical input signal. The optical input for the modulator and the two outputs of the tap coupler are guided to connectors at the front panel. At the rear panel, the electronic signal for the amplifier is supplied through an SMA connector, and the modulator bias voltage is supplied through a BNC connector. The supply voltage for the high-frequency amplifier and a constant voltage to control its gain are generated by an external laboratory power supply[5] and provided through a DE-9 D-sub connector.

Two pulse generators from Hewlett Packard are available to generate the electronic pulses to be applied to the modulator: model *HP 8131A* for repetition frequencies up to 500 MHz and pulse durations down to 380 ps and model *HP 8133A* for repetition frequencies between 33 MHz and 3 GHz and pulse durations between 150 ps and 10 ns. The clocks of the pulse generators are relatively unstable, and therefore, the generators are triggered by a stable clock generator[6].

EDFA-1 Module

The EDFA-1 module is designed to amplify the seed laser light before it is chopped into pulses by the pulse generation module. The EDFA is set up so that the seed and pump light are co-propagating, minimizing the number of required components. The setup is shown in fig. 2.6. It comprises a pump laser, a Faraday isolator, a wavelength combiner, 104 cm of erbium-doped fiber, a pump filter, a bandpass filter, and a 1/99 beam splitter. The pump

[5] Laboratory power supply: 2231A-30-3 from *Keithley*.
[6] Clock Generator: CG635 from *Stanford Research Systems*.

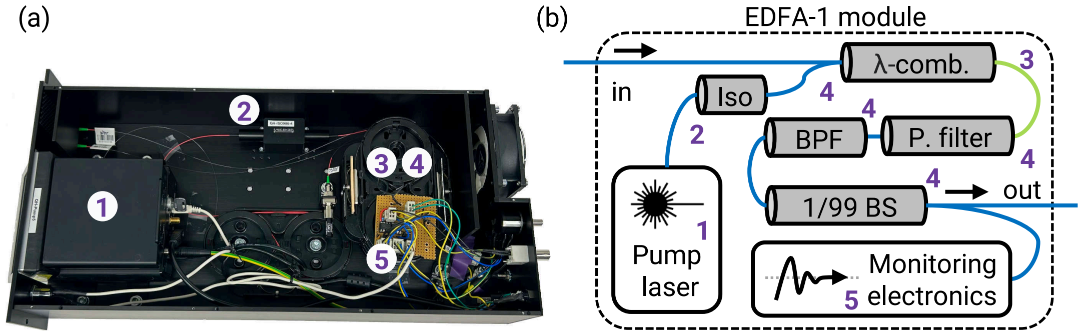


Figure 2.6: EDFA-1 module. (a) Photo of the module interior. (b) Scheme of the components. Iso – Optical Isolator, λ-comb. – Wavelength combiner, P. filter – Pump filter, BPF – Band pass filter, BS – Beam splitter (1/99 tap coupler). The doped amplifier fiber is shown in green.

laser diode[7] emitting pump light at a wavelength of 976 nm is mounted on a laser driver[8]. The Faraday isolator protects the pump laser from reflected light. Seed light at 1550 nm and pump light are combined in the wavelength combiner into the core of the doped PM fiber[9] and remaining pump light is filtered out by the pump filter after the doped fiber. The length of the doped fiber was optimized by repeatedly measuring the power at 1550 nm and clipping a longer piece of the doped fiber until a maximum output power was reached. The 6.5 nm wide bandpass filter suppresses light from *amplified spontaneous emission* (ASE) around 1530 nm and the tap coupler splits off one percent of the output for the internal power monitoring electronics.

The power monitoring electronics developed by Oleg Nikorov is described in detail in ref. [M4]. It features a photodiode receiving a small fraction of the output power. The electrical signal of the photodiode is amplified and low-pass filtered. When the EDFA is seeded with CW light or pulses at Megahertz repetition rates, the voltage level is proportional to the average optical output power of the module. This electrical signal is directly accessible from outside the module via a BNC connector at the rear panel and can be used as a feedback signal for output power stabilization. Furthermore, the voltage is provided to a threshold detection circuit connected to the interlock of the laser driver. The interlock is only released if the key in the module's front panel is turned to activate the driver. The photodiode detects optical powers above a certain threshold, indicating that seed light is present. If the driver is running and the circuit notices a drop of the output

[7] Laser diode: 1999CVB from *3SP Technologies*.
[8] Laser driver: CLD1015 from *Thorlabs*.
[9] Erbium-doped fiber: ESF-7/125 from *Nufern*.

power below the threshold, the interlock is activated within less than 32 µs to prevent damage to the EDFA, which could occur when the doped fiber is pumped but not seeded.

The front panel of the module provides fiber connections for the optical input and output. The touchscreen display of the pump driver is integrated into the front panel. The rear panel features a USB port allowing for remote control of the driver as well as two potentiometers to adjust the photodiode amplifier gain and the interlock threshold value of the power monitoring electronics.

Figure 2.7 (a) shows the output power as a function of the pump current. The maximum output power at the highest pump current of 1471 mA is 173.8(87) mW. This power is well above the 100 mW maximum allowed input power of the EOAM in the pulse generation module, so the amplitude modulator's input power range can be fully used.

A clean output spectrum of the EDFA is important to avoid the contamination of the photon pair spectra with noise. The output spectrum is shown in fig. 2.7 (b), featuring only the peak at the seed wavelength. The pump light at 976 nm and the ASE around 1530 nm are suppressed by more than 70 dB.

EDFA-2 Module

The EDFA-2 module is designed to amplify the light pulses generated by the pulse generation module. It contains an inhouse-made EDFA using the doped PM fiber and pump laser of the same type as EDFA-1. A bidirectional configuration was chosen to optimize pulsed operation. The EDFA-2 consists of a four-port optical circulator, a wavelength combiner, a pump laser protected by an isolator, 82 cm of erbium-doped fiber, two *fiber Bragg gratings* (FBGs) and a 1/99 beam splitter. The length of the doped fiber was optimized by repeatedly measuring

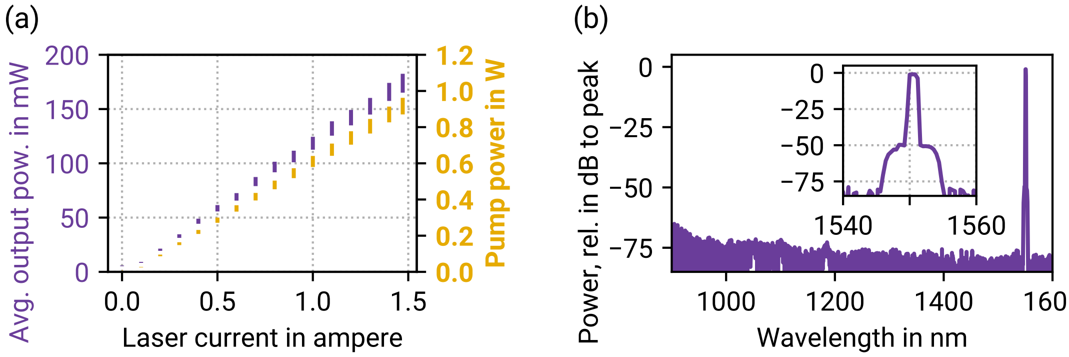


Figure 2.7: Performance of EDFA-1 when seeded with the seed laser (cf. section 2.1.1). (a) Output power (left) and pump power (right) as a function of the pump driver current. (b) Optical output spectrum showing a clean peak at the seed wavelength λ_0.

the power at 1550 nm, clipping the doped fiber, and splicing the FBG to the end until the maximum output power was reached.

The setup of EDFA-2 is shown in fig. 2.8. The front and rear panels of the EDFA-2 module have the same connections as the EDFA-1 module. The seed light enters the EDFA-2 via the first port of a circulator and leaves it at the second port before it is combined with the pump light in the wavelength combiner. In the first pass, seed and pump light co-propagate along the doped fiber. The amplified light is then reflected by the FBG with a reflection bandwidth of 50 GHz centered at λ_0. Thereby, the spectrum is cleaned from other unwanted wavelengths. The reflected light travels backward through the doped fiber and is further amplified. The light re-enters the circulator and leaves it at port 3, where a second FBG cleans the spectrum. One percent of the power leaving the circulator at port 4 is split for the power monitoring electronics.

The pulse energy after the pulse generation module is limited by the maximum input power of the EOAM. Amplifying these pulses to the desired output energy requires a high gain, which comes at the price of stronger ASE. The advantage of the bidirectional design is that the first FBG filters out the ASE light from the forward pass, and only the desired light at 1550 nm is further amplified in the second pass before being filtered again. This allows for a relatively high gain in combination with a high ASE suppression.

Figure 2.9 (a) shows the output power as a function of the pump driver current for three different pulse repetition rates. The optical output power increases approximately linearly with the current of the pump laser. An important figure characterizing EDFA-2 is the maximum achievable peak power of the output pulses. The maximum peak powers

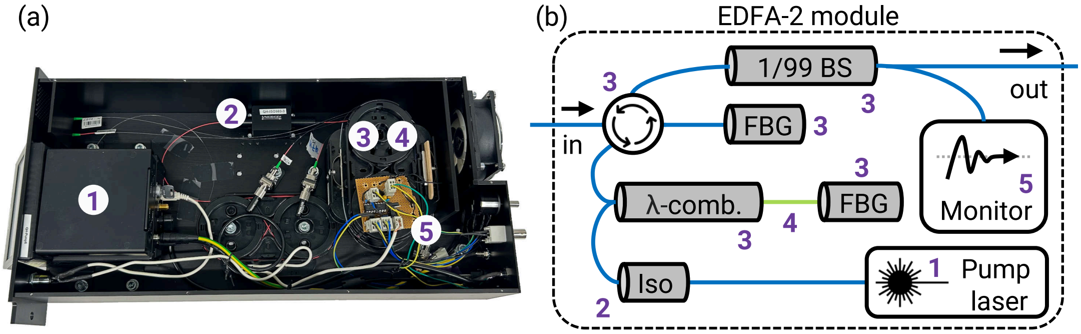


Figure 2.8: EDFA-2 module. (a) Photo of the module interior. (b) Scheme of the components. PM fibers are shown in blue, and the doped fiber is shown in green. BS – Beam splitter (1/99 tap coupler), FBG – Fiber Bragg grating, Iso – Optical Isolator, λ-comb. – Wavelength combiner, Monitor – Power monitoring electronics.

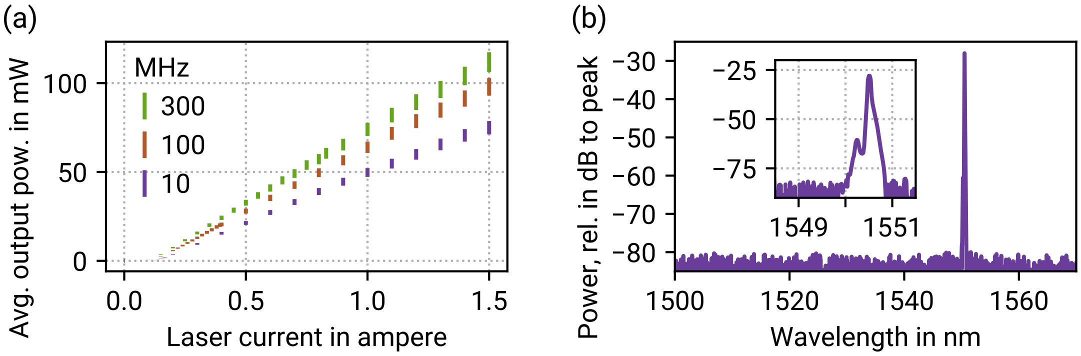


Figure 2.9: Performance of EDFA-2 when seeded with EDFA-1. (a) Average output power as a function of the pump driver current for different repetition frequencies. (b) Output spectrum at a pulse repetition frequency of 10 MHz and at the maximal pump driver current of 1500 mA. The light is transmitted through an FBG attached to an additional circulator, suppressing the seed wavelength by 28 dB.

are 17.3 W at 10 MHz, 2.47 W at 100 MHz and 0.74 W at 300 MHz and pulse lengths of roughly 400 ps. The maximum average input power for the wavelength converter in the SHG module is 500 mW. The input peak power is kept below this value for pulsed operation to avoid damaging the crystal. For typical repetition rates of 110 to 220 MHz at which the PPS is operated for QKD, this means that peak powers close to the maximum input power of the SHG module can be generated with EDFA-2, even when the insertion losses introduced by the pump IF are taken into account.

Figure 2.9 (b) shows the output spectrum of EDFA-2. The ASE suppression in the main output after the second FBG is so high that ASE was not directly measurable with the optical spectrum analyzer. To estimate the suppression, a circulator with an FBG at the second port was connected to the EDFA-2 output. The FBG reflected most of the light at the seed wavelength, while the rest of the spectrum was transmitted to an optical spectrum analyzer. Even at the lowest repetition frequency of 10 MHz and at the highest pump driver current of 1500 mA, no ASE was measurable with a noise floor around −52 dB. The extinction ratio of the pump light in transmission of the FBG was measured to 28 dB, such that the ASE suppression in the main output can be estimated to be better than 80 dB.

SHG Module

The SHG module, shown in fig. 2.10, doubles the optical frequency of the pump light pulses to a wavelength of 775 nm. The module contains a wavelength converter, a shortpass filter removing remaining light at 1550 nm after the conversion, a 1/99 fiber beam splitter,

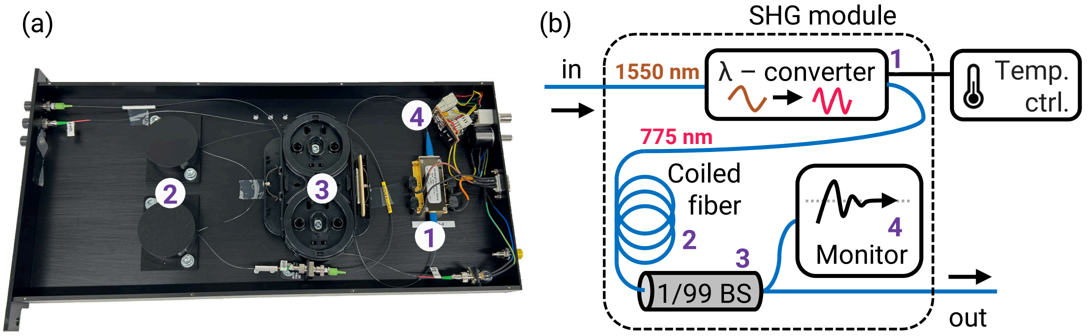


Figure 2.10: SHG module. (a) Photo of the module interior. (b) Scheme of the components. λ-converter – fiber-coupled type-0 nonlinear wavelength converter, BS – Beam splitter (1/99 tap coupler), Temp. ctrl. – Temperature controller, Monitor – Power monitoring electronics.

and power monitoring electronics. The wavelength converter[10] contains a fiber-coupled *periodically-poled lithium niobate* (PPLN) waveguide with a length of 34 mm and angle-cut anti-reflection-coated end facets. The converter used in the SHG module is the one of two identical models, and the other one is used in the type-0 SPDC module. The crystal is quasi-phase matched for SHG from 1550 to 775 nm at a temperature of 43.5 °C. A thermistor and a *thermoelectric cooler* (TEC) for temperature control are integrated into the wavelength converter. The crystal temperature can be controlled by connecting an external temperature controller[11] to a D-sub connector at the rear panel of the SHG module. The shortpass filter consists of two fiber spools with a diameter of 31 mm, around which more than 4 m of PM fiber[12] specified for 780 nm are wound. At this bending diameter, the light at 775 nm is guided without significant loss, and the polarization is maintained, while light around 1550 nm is coupled out, experiencing high losses. In a test with two meters of such spooled fiber, a suppression of more than 79 dB was observed for light at 1550 nm. Both fiber spools are covered by black anodized aluminum hoods absorbing the out-coupled light. The 1/99 coupler splits off one percent of the SHG light for the power monitoring electronics, which is similar to the electronics integrated into the EDFA modules. However, in the SHG module, neither a key switch nor an interlock is implemented.

Figure 2.11 (a) shows the measured average SHG power as a function of the average fundamental power at a repetition frequency of 100 MHz. The curve slightly deviates from a purely quadratic dependency due to non-negligible pump depletion. Figure 2.11 (b)

[10] Wavelength converter (purchased in 2020): WH-0775-000-F-B-C from *NTT Electronics*.
[11] All three temperature controllers for the SHG module and the SPDC modules are TED200C from *Thorlabs*.
[12] PM fiber for 780 nm: PM 780-HP from *Nufern*.

shows the pulse shape of the SHG pulses for different repetition frequencies, measured with a fast photodetector[13] and a broadband oscilloscope[14]. The pulses are almost rectangular, but the falling edges show tails. Furthermore, although the width was always set to 400 ps, the *full width at half maximum* (FWHM) depends non-monotonously on the repetition frequency. This variation is also present in the fundamental pulses and can be attributed to an imperfect realization of the desired pulse duration by the *HP 8131A* pulse generator.

2.1.2 Generation and Separation of Photon Pairs

Two SPDC modules were built to generate orthogonally or parallel polarized photon pairs. Two *arrayed-waveguide gratings* (AWGs) and a *wavelength-selective switch* (WSS) are available as WDMs.

Type-II SPDC Module

The type-II SPDC module is shown in fig. 2.12. It generates orthogonally polarized photon pairs around the center frequency λ_0 and separates the photons by their polarization. The module contains a fiber-coupled wavelength converter, two longpass filters, a bandpass filter, and a polarization beam splitter. The wavelength converter[15] features a 24 mm long PPLN crystal waveguide quasi-phase-matched for type-II SPDC from 775 to 1550 nm. This

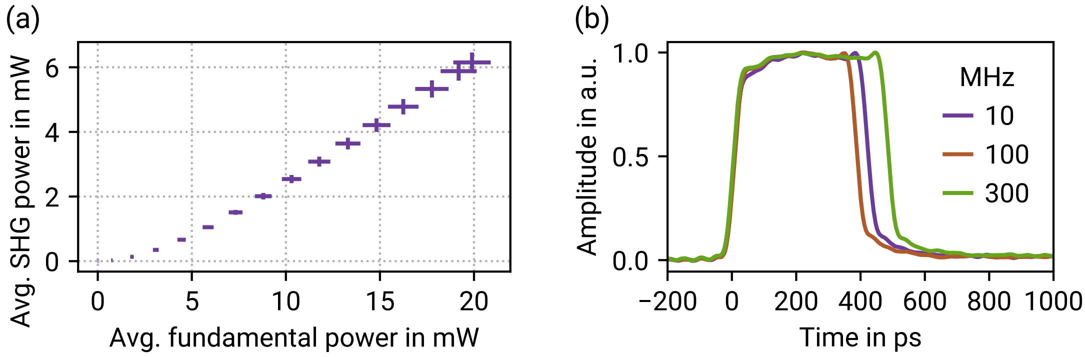


Figure 2.11: Performance of the SHG module. (a) Average second-harmonic output power as a function of the average fundamental light power at a repetition frequency of 100 MHz. (b) SHG pulse shapes at different repetition frequencies for a set pulse width of 400 ps. The FWHM of the pulse varies between 381 ps at 100 MHz over 418 ps at 10 MHz up to 482 ps at 300 MHz.

[13] Photodetector module: New Focus 1454 from *Newport* with a rise time of 18.5 ps.

[14] Oscilloscope: MSO72004C from *Tektronix* with a bandwidth of 20 GHz.

[15] Type-II wavelength converter: WDC-K0775-P15P78AL0 from *AdvR*.

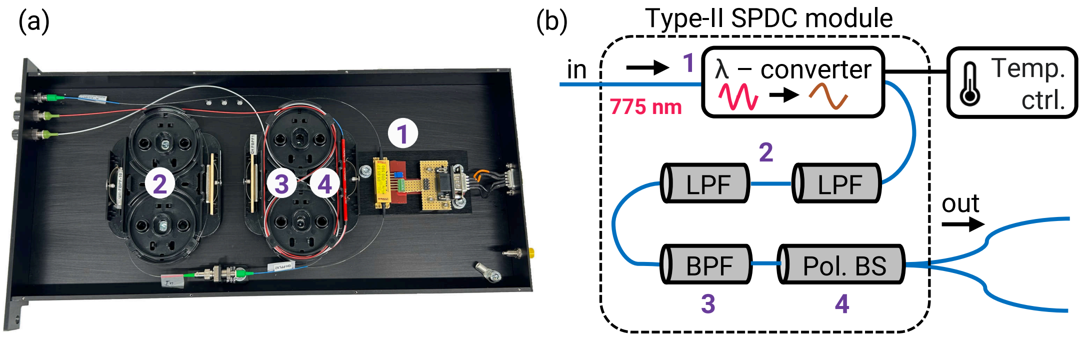


Figure 2.12: Type-II SPDC module. (a) Photo of the module interior. (b) Scheme of the components. λ-converter – fiber-coupled type-II nonlinear wavelength converter, LPF – Longpass filter, BPF – 5 nm Band pass filter, Pol. BS – Polarization beam splitter.

converter was used to generate photon pairs during Nikiforov's field test of the two-user QKD system [28]. Similar to the SHG module, the crystal temperature is controlled by a temperature controller. The longpass filters remove the SHG light from the photon pairs with a suppression of more than 60 dB per filter, and the bandpass filter suppresses wavelengths outside of a 5 nm wide window around the center wavelength of the photon pairs.

Type-0 SPDC Module

The type-0 SPDC module generates parallel polarized photon pairs with a broad spectrum. The module contains a wavelength converter, two longpass filters, and a bandpass filter transmitting only the optical C-band from 1525 to 1572 nm. Figure 2.13 shows the setup of the module. The wavelength converter is the same model as in the SHG module[16], and the longpass filters are of the same type as those in the type-II SPDC module.

Wavelegth Division Demultiplexers

Three different WDMs are available for demultiplexing the type-0 SPDC spectrum: an AWG with 96 channels and a channel width of 50 GHz, an AWG with 44 channels and a channel width of 100 GHz, and a WSS with nine outputs. The channel width of the WSS can be set between 6.25 GHz and the whole operating wavelength range in steps of 3.125 GHz.

Figure 2.14 shows the expected spectrum for the type-0 SPDC module, the spectrum of the C-band filter, and the wavelength ranges accessible with the different WDMs. The sinc^2-shaped SPDC spectrum was calculated based on eq. (1.37) using the properties of the type-0 wavelength converter. It is almost constant over the pass band of the C-band

[16] Wavelength converter (purchased in 2018): WH-0775-000-F-B-C from *NTT Electronics*.

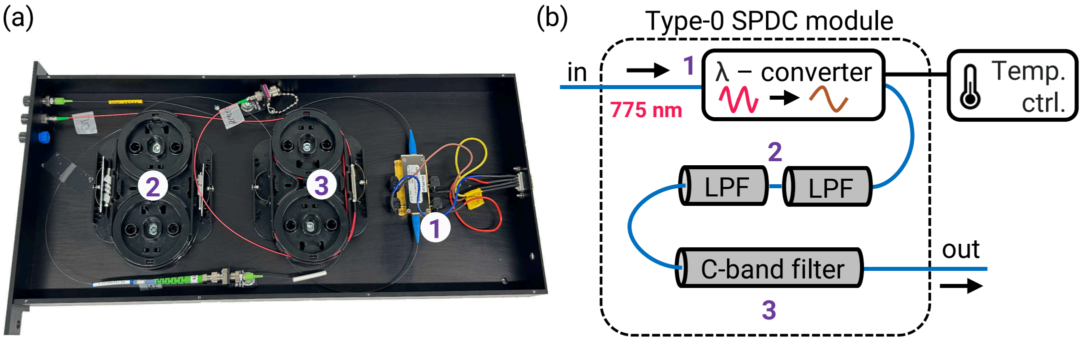
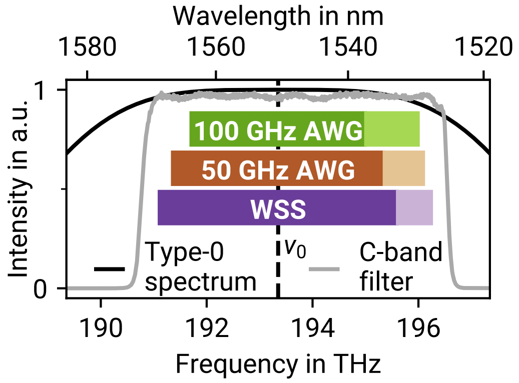


Figure 2.13: Type-0 SPDC module. (a) Photo of the module interior. (b) Scheme of the components. LPF – Longpass filter, λ-converter – fiber-coupled type-0 nonlinear wavelength converter, Temp. ctrl. – Temperature controller. For all measurements presented in this thesis, the C-band filter was connected with fiber connectors. Afterwards, it was permanently spliced to the LPFs, so the insertion loss observed in future experiments may be slightly lower.



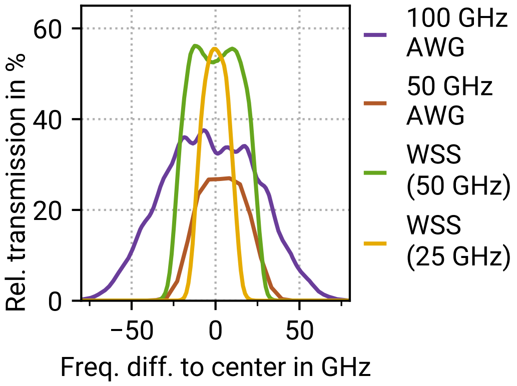


Figure 2.14: Spectra of the WDMs with usable (saturated bars) and unusable (light bars) bandwidths as well as the expected type-0 SPDC spectrum and C-band filter spectrum.

Figure 2.15: Typical transmission spectra for channels of the AWGs and for the WSS with 25 and 50 GHz wide channels. A transmission of 100 % means no loss.

filter. The spectral ranges accessible with the WDMs are narrower than the spectra of the wavelength converter and the C-band filter, so the bandwidth available for QKD is limited by the WDMs. For signal photons produced in the light-colored frequency ranges, the idler photon is already outside of the wavelength range of the WDM. This means only the symmetric part (saturated bars in fig. 2.14) of the technically accessible frequency range around ν_0 can be used for QKD. With the current choice of ν_0 (cf. eq. (2.1)), the practically usable wavelength ranges around ν_0 are ±1.65 THz for the 100 GHz AWG, ±2 THz for the 50 GHz AWG and ±2.25 THz for the WSS. Theoretically, this enables QKD between 34 users with the 100 GHz AWG or between 78 users with the 50 GHz AWG. Although the WSS has the widest usable spectral range, only nine users can be connected due to the limited number of outputs. By shifting the center frequency to the center of the WDM spectra, the number of users that can simultaneously be connected to the q-hub could be slightly increased. However, because the filters and FBGs used in the different modules are tailored to the center frequency, using a different center frequency would require different components.

Figure 2.15 shows transmission spectra for typical channels of the WDMs. The relative transmission at the top of the peak is for the AWGs lower than for the WSS, meaning that the AWGs introduce higher losses, resulting in lower key rates. For the WSS, the edges of the transmission peaks are very steep. In fact, the resolution of the optical spectrum analyzer limits the measured slope for the WSS. In comparison, the spectra of the AWGs have considerably shallower edges. At the base, the shapes of these peaks are broader than the nominal channel width, meaning that adjacent AWG channels will show some spectral cross-talk due to the overlapping foothills of the transmission peaks.

2.2 Characterization of the Photon Pair Source

In this section, the performance of the PPS is characterized. Section 2.2.1 presents the methodology and results of conversion efficiency measurements for the SPDC modules. Measured photon spectra for both SPDC modules are presented in section 2.2.2. Further details about the performance of the PSS are presented in ref. [VIII].

2.2.1 Conversion Efficiency Measurements

The strength of SPDC fields depends on multiple parameters characterizing the nonlinear crystal. The signal power is proportional to the pump power as well as to the squares of the crystal length and of the coefficient of the nonlinear interaction [123]. Further quantities determining the signal power, such as the exact effective cross-section area of the waveguide and the coupling losses into and out of the waveguide, are not precisely known for the wavelength converters. However, a precise value for the efficiency of conversion of SHG photons into photon pairs is required to calculate the mean photon pair number per pulse μ_P for the simulations of the QKD system in chapters 6 and 7. Therefore, the conversion efficiency was measured.

One way to quantify the conversion efficiency is to define the dimensionless parameter ϵ as the probability that a SHG photon is converted into a photon pair. The produced photon pair rate is then given by

$$R_\mathrm{pair} = \epsilon \, \frac{P_\mathrm{SHG}}{2\hbar\omega_0}\,, \tag{2.3}$$

with the SHG pump power P_SHG and the energy $2\hbar\omega_0$ of the pump photons. To measure R_pair, the crystal is pumped with a known SHG power, signal and idler photons are separated and guided into two detectors, and R_pair is obtained from the coincidence rate of the signal and idler counts. The type-II photon pairs are separated by using a polarization beam splitter. The type-0 photons can be probabilistically separated by using a 50/50 beam splitter, or they can be separated by using a WDM.

However, many photons are lost, and detector imperfections such as dark counts, the dead time, and afterpulses (cf. chapter 5) further complicate the calculation of R_pair from the measurements. The directly measurable data are the average SHG pump power and the timestamps of the detector counts of the signal and idler detector, from which three rates are calculated: the signal count rate r_s, the idler count rate r_i, and the coincidence count rate R. The conversion efficiency ϵ and the unknown transmission probabilities for signal and idler photons can be calculated from these values. A model has been developed for this calculation, correcting for detector dark counts, afterpulses, and dead times. The first version of the model was developed during the master's thesis of Daniel Hofmann [M1]. It was then extended to incorporate afterpulses, frequency-dependent losses, and probabilistic separation of parallel polarized photon pairs during the master's thesis of Lucas Bialowons [M5]. An improved method to treat the detector dead time and afterpulses by data postselection was integrated during the master's thesis of Maximilian Mengler [M8]. The model is described in detail in appendix B, where its correctness is verified with simulated timestamps. The simulation also shows that all the considered effects need to be taken into account in the efficiency calculation to obtain correct results.

For the conversion efficiency measurements, the SPDC modules were pumped with CW laser light, and a beam splitter was inserted after the SHG module to split off ten percent of the SHG power for monitoring P_SHG. For the type-II measurement, the photon pairs are separated with a polarization beam splitter. For the type-0 measurements, the central region of the spectrum was selected with a 7 nm wide bandpass filter, and the photon pairs were probabilistically split by a 50/50 beam splitter. Timestamp values from both detectors are saved over 120 seconds for several different SHG powers, and the conversion efficiency model is applied to each measurement. The conversion efficiency and transmission values are then obtained by averaging the results for the different SHG powers.

For the different converters, the calculated values for ϵ as well as t_s and t_i are tabulated in table 2.1. For convenience, the conversion efficiency is given both in photon pairs per SHG photon and in pairs per second per milliwatt SHG pump power. For QKD, not the complete spectrum of the type-0 converter is used, but instead, narrower channels are selected, and therefore, a spectral efficiency density ϵ_ν per frequency interval is introduced. The type-0 spectrum is so broad that the spectral density is essentially constant over the typical channel width (cf. fig. 2.14), such that the efficiency for a specific channel width is obtained by multiplying ϵ_ν with the channel width. Assuming a channel width of 100 GHz, the type-0 converters are roughly two orders of magnitude more efficient than the type-II converter. As the wavelength converters in the SHG and type-0 SPDC modules are identical, SPDC was tested with both converters. The converter purchased in 2018 was then selected for the type-0 SPDC module due to its higher conversion efficiency density ϵ_ν and lower insertion losses. The converter purchased in 2020 was built into the SHG module.

Frequency-Dependent Losses in the WDMs

When WDMs are used for separating the photons, it is important to consider their frequency-dependent transmission functions because they lead to correlations between the signal and idler photons. This aspect is relevant for the crystal efficiency calculation and the simulation of the QKD system in chapter 6.

It is convenient to split the transmission probabilities for signals and idlers into the frequency-independent transmissions t_s and t_i and into ζ_s and ζ_i, which contain all

Table 2.1: SPDC performance of the wavelength converters. The type-0 converters are distinguished by the year in which they were purchased. The largest contribution to the uncertainty of the efficiency is the coupling ratio of the beam splitter for tracking the SHG power, which varies over time. The efficiency is given as ϵ for the type-II converter and as efficiency density ϵ_ν in the center of the spectrum for the type-0 converters.

Wavelength converter	Efficiency in pairs per SHG photon	Efficiency in pairs per second per μW	Coupling efficiencies t_s and t_i
Type-II	$7.6(4) \times 10^{-10}$	$3.0(2) \times 10^{3}$	28(1) %
Type-0 (2018)	$6.7(7) \times 10^{-10}$/GHz	$2.6(3) \times 10^{3}$/GHz	36(4) %
Type-0 (2020)	$4.3(4) \times 10^{-10}$/GHz	$1.7(2) \times 10^{3}$/GHz	34(3) %

frequency-dependent losses. The total transmission probabilities through the WDM for signal and idler photons are then $t_\mathrm{s}\zeta_\mathrm{s}$ and $t_\mathrm{i}\zeta_\mathrm{i}$ with

$$\zeta_\mathrm{s} = \frac{1}{\Delta I}\int_I \tau_\mathrm{s}(\nu_0+\nu)\,\mathrm{d}\,\nu \quad \text{and} \quad \zeta_\mathrm{i} = \frac{1}{\Delta I}\int_I \tau_\mathrm{i}(\nu_0-\nu)\,\mathrm{d}\,\nu\,. \tag{2.4}$$

The functions $\tau_\mathrm{s}(\nu)$ and $\tau_\mathrm{i}(\nu)$ with $0 \le \tau_{\mathrm{s/i}}(\nu) \le 1$ and $\max_{\nu\in I}(\tau_{\mathrm{s/i}}(\nu)) = 1$ describe the frequency dependence of the transmission. To take all transmitted photons into account, the integration interval $I = [I_\mathrm{min}, I_\mathrm{max}]$ with $\nu_0 \le I_\mathrm{min} \le I_\mathrm{max}$ and width $\Delta I = I_\mathrm{max} - I_\mathrm{min}$ must be chosen to be large enough such that the spectral regions where τ_s and τ_i attain non-negligible values are entirely covered.

For strongly frequency-entangled photon pairs, the width of the pump light spectrum is negligible compared to the width of the photon spectrum. The frequencies of signals and idlers are anticorrelated due to energy conservation, such that $\nu_\mathrm{s} = \nu_\mathrm{p} - \nu_\mathrm{i}$ (cf. eq. (1.19)). Therefore, the average transmission probability for a photon pair with center frequency $\nu_0 = \nu_\mathrm{p}/2$ is given by $t_\mathrm{s}t_\mathrm{i}\zeta_\mathrm{pair}$ with

$$\zeta_\mathrm{pair} = \frac{1}{\Delta I}\int_I \tau_\mathrm{s}(\nu_0+\nu)\tau_\mathrm{i}(\nu_0-\nu)\,\mathrm{d}\,\nu\,. \tag{2.5}$$

In general, $\zeta_\mathrm{pair} \neq \zeta_\mathrm{s}\zeta_\mathrm{i}$, which means that the transmission probabilities for signals and idlers are not independent. To quantify the correlation, it is convenient to define the *spectral correlation factor*

$$c_{\Delta I} = \frac{\zeta_\mathrm{pair}}{\zeta_\mathrm{s}\zeta_\mathrm{i}}\,. \tag{2.6}$$

For frequency-independent transmission losses, the factor becomes $c_{\Delta I} = 1$. Table 2.2 lists the values for ζ_pair, $\zeta_\mathrm{s/i}$ and $c_{\Delta I}$ for the 100 GHz AWG and the WSS channels used in the QKD field test. For the 7 nm wide bandpass filter used in the type-0 crystal conversion efficiency measurements, $c_{\Delta I} = 1.38$ is obtained for $\Delta I = 700\,\mathrm{GHz}$. The values for $c_{\Delta I}$ for the WDMs, WSS, and bandpass filter significantly deviate from one, which shows that the correlation introduced by the frequency-dependent losses cannot be neglected. Taking $c_{\Delta I}$ into account is therefore important to obtain correct results for the conversion efficiencies and QKD simulations.

2.2.2 Photon Spectra

The spectra of the photon pairs are highly relevant for the QKD system. The type-0 photon pairs are separated by WDMs, and the width of their spectrum determines, together with the WDM channel width, the maximum number of user pairs that can be connected.

Table 2.2: Spectral correlation factors and insertion losses for the 100 GHz AWG and the WSS. During the field test, Alice and Bob are connected to the WSS ports 5 and 2, and Charlie and Diana are connected to 4 and 7 (cf. table 3.2).

WDM	Ports	ΔI	$c_{\Delta I}$	$t_\mathrm{s}, t_\mathrm{i}$	$\zeta_\mathrm{s}, \zeta_\mathrm{i}$
100 GHz AWG	C32, C35	150 GHz	1.72	-3.5 dB	-3.7 dB
WSS, 50 GHz channels	5, 2	75 GHz	1.48	-2.3 dB	-2.4 dB
WSS, 25 GHz channels	4, 7	50 GHz	1.88	-3.7 dB	-2.5 dB

Furthermore, for both type-0 and type-II photon pairs, the shape of the spectrum is relevant because the broadening of the photon wave packets due to chromatic dispersion can lead to quantum bit errors. Details about the type-II and type-0 photon spectra have been published in refs. [I, VIII].

Expected Photon Spectra for Ideal SPDC Crystals

Figure 2.16 shows the type-II joint spectral density $|\tilde{\psi}(\omega_\mathrm{s}, \omega_\mathrm{i})|^2$ for an ideal 24 mm long PPLN crystal. The bivariate phase matching function $\tilde{\Phi}(\omega_\mathrm{s}, \omega_\mathrm{i})$ is almost constant across the narrow stripe where $|\tilde{\alpha}(\omega_\mathrm{s} + \omega_\mathrm{i})|^2$ attains non-negligible values. It can therefore be approximated by the univariate function $\tilde{\Phi}(\omega_\mathrm{s} - \omega_\mathrm{i}) \approx \tilde{\Phi}(\omega_\mathrm{s}, \omega_\mathrm{i})$, which allows to factorize the JSA:

Factorization of the joint spectral amplitude in diagonal coordinates

$$\tilde{\psi}(\omega_\mathrm{s}, \omega_\mathrm{i}) \approx \tilde{\alpha}(\omega_\mathrm{s} + \omega_\mathrm{i})\, \tilde{\Phi}(\omega_\mathrm{s} - \omega_\mathrm{i})\,. \tag{2.7}$$

Working with eq. (2.7) is facilitated by introducing diagonal coordinates $\omega_\pm$ and $t_\pm$:

$$\begin{array}{rcl|rcl} \begin{aligned} \omega_+ &= \omega_\mathrm{s} + \omega_\mathrm{i} \\ \omega_- &= \omega_\mathrm{s} - \omega_\mathrm{i} \end{aligned} & \Leftrightarrow & \begin{aligned} \omega_\mathrm{s} &= (\omega_+ + \omega_-)/2 \\ \omega_\mathrm{i} &= (\omega_+ - \omega_-)/2 \end{aligned} & \begin{aligned} t_+ &= t_\mathrm{s} + t_\mathrm{i} \\ t_- &= t_\mathrm{s} - t_\mathrm{i} \end{aligned} & \Leftrightarrow & \begin{aligned} t_\mathrm{s} &= (t_+ + t_-)/2 \\ t_\mathrm{i} &= (t_+ - t_-)/2 \end{aligned} \end{array}. \tag{2.8}$$

The photon spectra are the marginal distributions of the joint spectral density $|\tilde{\psi}(\omega_\mathrm{s}, \omega_\mathrm{i})|^2 = |\tilde{\Phi}(\omega_\mathrm{s}, \omega_\mathrm{i})|^2 |\tilde{\alpha}(\omega_\mathrm{s} + \omega_\mathrm{i})|^2$. To separate the contributions of the pump pulse and phase matching function, the SPDC process can be pumped with a narrow CW laser, such that $|\alpha(\omega)|^2 \approx \delta(\omega_\mathrm{s} + \omega_\mathrm{i} - 2\omega_0)$. Thereby, the spectral densities for signals and idlers from eq. (1.31) become

$$S_\mathrm{s}(\omega_\mathrm{s}) = \left|\tilde{\Phi}[2(\omega_\mathrm{s} - \omega_0)]\right|^2 \quad \text{and} \quad S_\mathrm{i}(\omega_\mathrm{i}) = \left|\tilde{\Phi}[2(\omega_0 - \omega_\mathrm{i})]\right|^2, \tag{2.9}$$

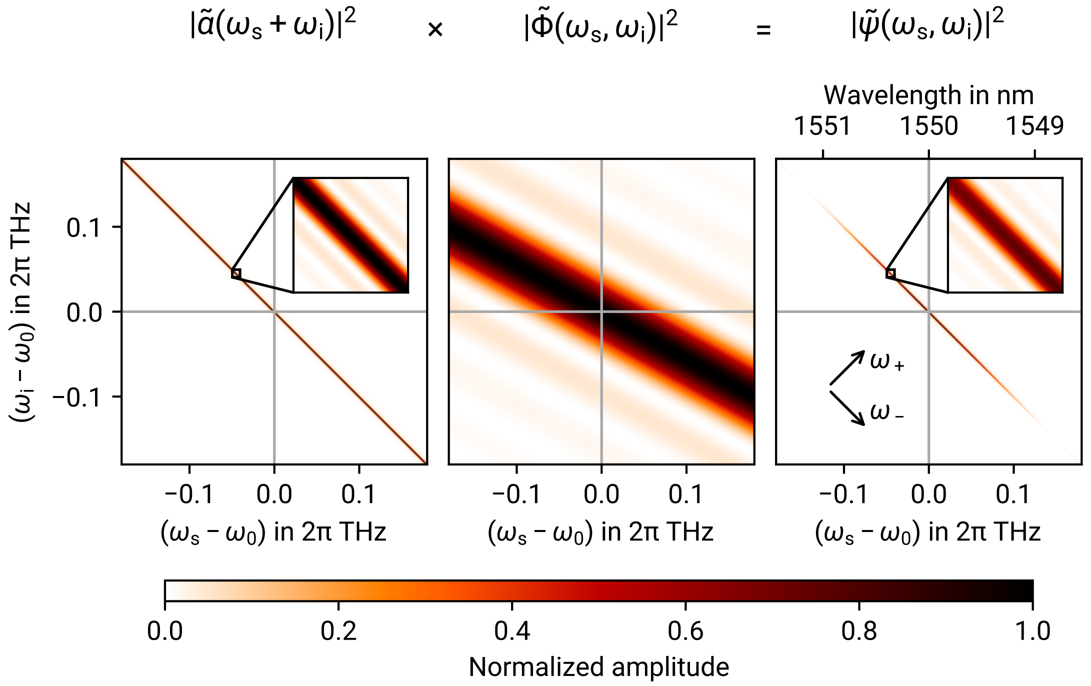


Figure 2.16: Joint spectral density $|\tilde{\psi}(\omega_s, \omega_i)|^2$ for an ideal 24 mm long type-II crystal phase-matched at ω_0, for a 400 ps long rectangular pump pulse. The phase matching function $|\tilde{\Phi}(\omega_s, \omega_i)|^2$ is calculated based on the refractive index data for lithium niobate from ref. [124]. The arrows in the plot of $|\tilde{\psi}|^2$ indicate the directions of the diagonal coordinates ω_+ and ω_-.

such that measuring the photon spectrum directly yields the squared absolute value of the phase-matching function. The spectral density of the signal and idler photons are the same functions mirrored at ω_0 due to energy conservation. By using eq. (1.37) and calculating Δk via eq. (1.35) from refractive index data for lithium niobate from ref. [124], the photon spectra expected for ideal crystals were calculated. Figure 2.17 shows the expected spectral densities of the signal photons for the type-II and type-0 converters. Although the type-0 crystal is longer than the type-II crystal and both crystals consist of lithium niobate, the type-0 spectrum is almost two orders of magnitude broader than the type-II spectrum. This can be understood by considering the expansion of the phase mismatch Δk from eq. (1.35) around the center frequency [98]: When the pump light spectrum is so narrow that the change of Δk over the frequency interval of the pump light can be neglected, the

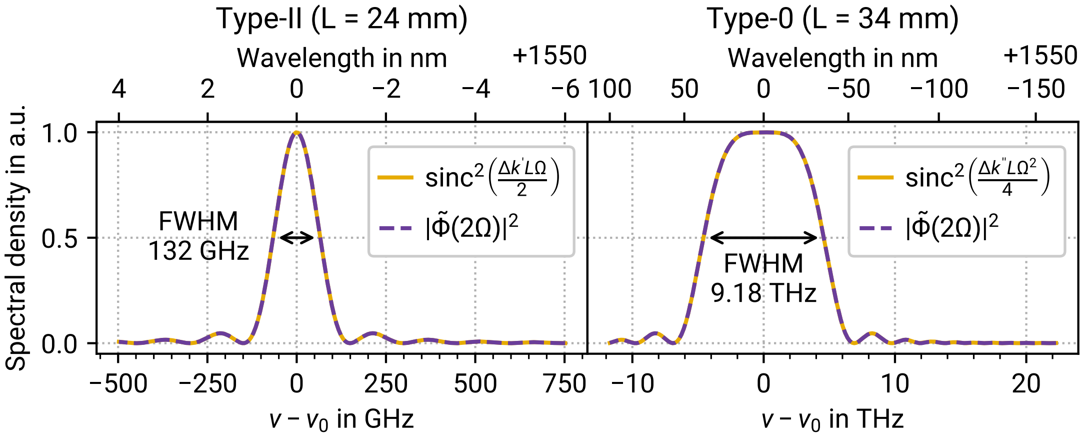


Figure 2.17: Theoretical spectral densities of the signal photons from the PPLN crystals in the SPDC modules with phase matching at λ_0. The values for $\Delta k'$ and $\Delta k''$ were calculated via eq. (1.35) based on refractive index data for lithium niobate from ref. [124].

approximations $\omega_p \approx 2\omega_0$, $\omega_s = \omega_0 + \Omega$ and $\omega_i = \omega_0 - \Omega$ yield the following expansion of Δk around ω_0:

$$\Delta k(\omega_s, \omega_i) = \Delta k(\Omega) = \Delta k_0 + \Delta k' \Omega + \frac{\Delta k''}{2} \Omega^2 + \mathcal{O}\big(\Omega^3\big) \quad \text{with} \tag{2.10}$$

$$\Delta k_0 = \Delta k(\omega_0, \omega_0)\,, \quad \Delta k' = \left(\frac{\partial\, k_i}{\partial\, \omega} - \frac{\partial\, k_s}{\partial\, \omega} \right)\bigg|_{\omega_0} \quad \text{and} \quad \Delta k'' = \left(\frac{\partial^2 k_i}{\partial\, \omega^2} + \frac{\partial^2 k_s}{\partial\, \omega^2} \right)\bigg|_{\omega_0} . \tag{2.11}$$

In the experiment, the temperatures of the converter crystals are tuned to achieve a precise compensation of Δk_0 by the poling period $\Lambda = 2\pi/\Delta k$. For parallel polarized photons, the term $\Delta k'$ vanishes as well, such that the first contributing term is $\Delta k''$, leading to a broad phase matching function [98]. The plots in fig. 2.17 show that truncating Δk to the first contributing order, that is, to $\Delta k'$ for type-II SPDC and to $\Delta k''$ for type-0 SPDC, yields an excellent approximation of the phase matching function calculated from the refractive indices. Therefore, the photon spectrum expected for ideal crystals is shaped as $\mathrm{sinc}^2(x)$ for type-II SPDC and as $\mathrm{sinc}^2(x^2)$ for type-0 SPDC.

Two methods to measure the spectra were developed during the master's thesis of Daniel Hofmann [M1]. First, an insulated housing for a commercial single-photon spectrograph was built, enabling operation at a lower temperature to improve the noise floor. Furthermore, a single-photon spectrometer based on chromatic dispersion was developed. Both methods were presented in publication [I] and are described below.

Spectrograph Setup for Measuring the SPDC Spectra

The spectrograph[17] uses a grating with 600 lines per mm and an indium gallium arsenide detector array[18] with 512 pixels, achieving a resolution of 0.07 nm for wavelengths around 1550 nm. Internal thermoelectric coolers cool the detector array to −90 °C. The warm side of the thermoelectric coolers requires water cooling. The manufacturer recommends a coolant temperature of 10 °C to reach a low noise level. The laboratory at the university is not air-conditioned, the humidity cannot be controlled, and the dew point is above 10 °C during summer. To avoid water condensation inside the detector when cooling it to 10 °C, the whole spectrograph setup is placed in a self-made insulating box constructed from extruded polystyrene boards. The spectrograph setup inside the insulating box is shown in fig. 2.18. Silica beads are placed inside the box to reduce the humidity of the air. An air-coolant heat exchanger is integrated into the cooling circuit and placed inside the box, such that the air inside the box is cooled as well to reduce the noise further. The coolant temperature is set to 1 °C to avoid theformation of ice from condensed water, resulting in an air temperature of about 8 °C inside the box. At this temperature, the noise background is approximately four times lower than at an ambient temperature of 25 °C. The box features a window made of transparent acrylic glass. It is covered by an insulating cover when the box is cooled. Humidity and temperature inside the box are monitored with sensors. To

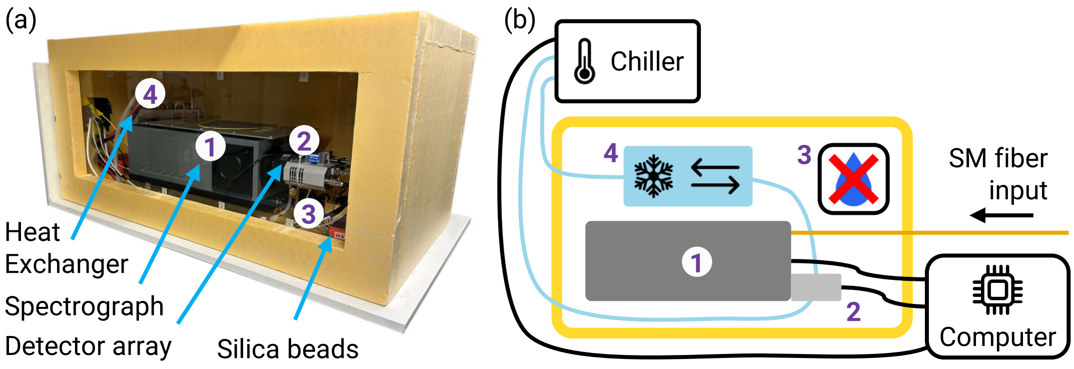


Figure 2.18: Spectrograph setup. (a) View through the acrylic glass window into the insulating box. (b) Schematic setup of the spectrograph inside the insulating box. The coolant circuit is shown in light blue.

[17] Spectrograph: Shamrock 500i from *Oxford Instruments*.
[18] Detector array: iDus DU490A from *Oxford Instruments*.

avoid condensation, Daniel Hofmann developed a *LabVIEW* program during his master's thesis for monitoring the conditions inside the box, restricting the coolant temperature to values above the dew point [M1]. When the program detects a sudden increase in the humidity at low temperatures, for example, due to a leak in the coolant circuit or because the box is opened when cooled, it automatically shuts down the setup and disconnects the line voltage to avoid any damage to the electronics of the spectrograph or detector array due to water condensation.

The spectrum of the type-II module measured for multiple converter crystal temperatures is shown in fig. 2.19. At a crystal temperature of 41.64 °C, the maxima for both polarization directions are located at the center frequency. For lower temperatures, the photons polarized along the slow axes of the PM fiber are shifted to longer wavelengths, and the photons polarized along the fast axis are shifted to shorter wavelengths.

The temperature-dependent spectrum of the type-0 module was also measured with the spectrograph and is shown in fig. 2.20. The spectrum splits into two peaks above approximately 44.5 °C. At temperatures below 43 °C, the spectrum gets narrower and

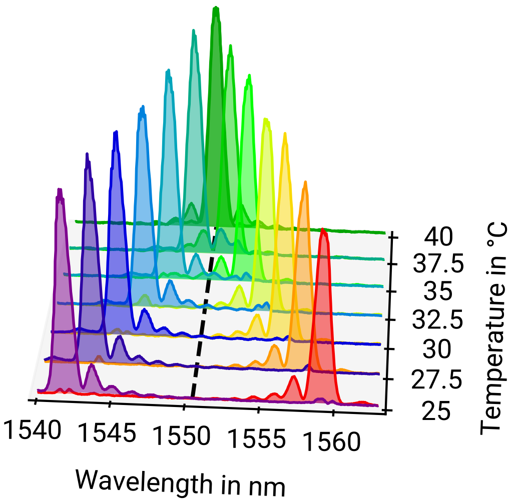


Figure 2.19: Photon spectrum of the type-II SPDC module for different converter crystal temperatures. Tuning the temperature shifts the peaks for the slow axis (right peak) and fast (left peak) axis. The overall spectrum is symmetric around the center wavelength λ_0 (dashed line).

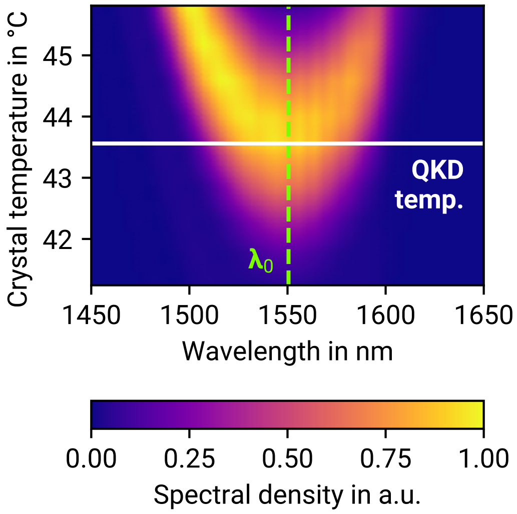


Figure 2.20: Photon spectrum of the type-0 SPDC module for different crystal temperatures. The asymmetry with respect to the center wavelength λ_0 is due to the drop in the sensitivity of the detector for wavelengths above 1600 nm. The horizontal line marks the temperature of 43.56 °C used for QKD.

weaker because the phase matching is not optimal anymore. For the QKD experiments, the type-0 module is operated at a crystal temperature of 43.56 °C.

Dispersion-Based Single-Photon Spectrometer

The setup of the spectrograph is rather large and not portable. To be able to measure photon spectra during the QKD field test at the facility of *Deutsche Telekom*, a portable single-photon spectrometer was implemented by using the dispersion-compensating fibers and single-photon detectors. Similar setups have been presented in refs. [95, 125, 126].

Figure 2.21 shows the setup of the spectrometer. One photon of each pair is directly detected as a herald, and the other photon is sent through the DCFs before being detected. Due to the group velocity dispersion, the travel time of the idlers in the DCF depends on their wavelength, so the arrival time difference distribution between signals and idlers resembles the shape of the idler spectrum (cf. eq. (1.17)). To enhance the signal-to-noise ratio, only those signal-idler coincidences are evaluated that are additionally coincident with the trigger pulse of the PPS. The time axis can be directly converted into a wavelength axis by using eq. (1.13). A double-pass variant of the spectrometer was set up as well to enhance the spectral resolution. In this configuration, the DCF modules are connected via a circulator, and a retroreflector is connected to the end, such that the idlers are reflected, travel backward through the DCFs, and leave the circulator at the third port where they are detected. The spectral resolution is determined by the timing resolution of the photon detection limited by the detector timing jitter of approximately 200 to 300 ps (cf. sec-

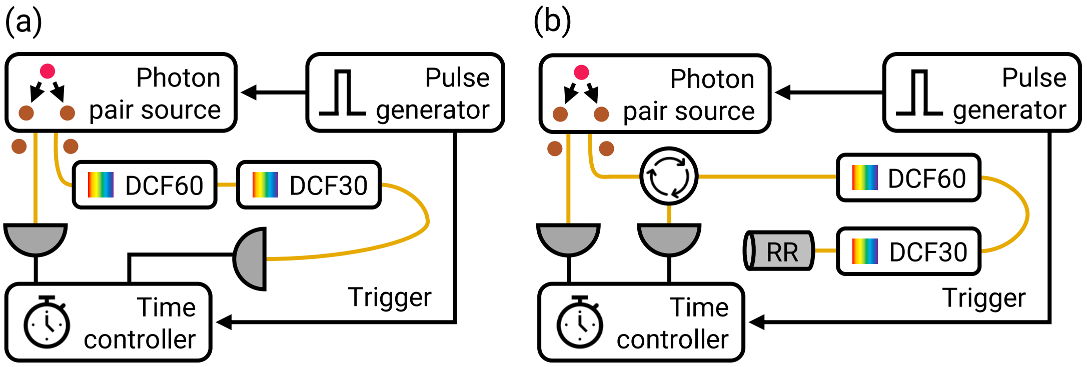


Figure 2.21: Dispersion-based single-photon spectrometer using two dispersion compensation fibers (DCFs) (cf. fig. 1.6) for compensating the dispersion in 30 and 60 km long SMFs. The time controllers measure the times at which the single-photon detectors (SPDs) yield counts. Sections 2.4 and 5.2 provide more details about the SPDs and time controllers. (a) Single-pass configuration. (b) Double-pass configuration. RR – Retro reflector.

tion 5.4). The resolution of the double-pass setup is below 0.1 nm, which is comparable to the resolution of the spectrograph. Figure 2.22 shows that the spectra acquired with the dispersion spectrometers match the spectrum acquired with the spectrograph.

Asymmetry of the Type-II Spectrum

The simulation of the QKD system in chapter 7 requires as an input the complex-valued spectrum of the photons, which is then Fourier-transformed to the time domain. However, only the squared absolute value of the amplitude is directly measured. Therefore, a model describing the spectrum is required. The squared absolute value from the model can then be fitted to the measured spectral density to determine the model parameters.

The type-II spectrum in fig. 2.22 shows a strong asymmetry of the side lobes and is not well approximated by the sinc^2-function expected for an ideal crystal (cf. eq. (1.37)). Therefore, a different model describing the spectrum was developed.

The asymmetry is due to fabrication imperfections introducing small changes of the phase mismatch Δk along the waveguide [106, 127, 128]. To model this z-dependence, the decoupling approximation [107, 108]

$$\Delta k(\Omega, z) \approx \Delta k(\Omega) + \epsilon_k(z) \tag{2.12}$$

is used, separating the uniform $\Delta k(\Omega)$ from a small frequency-independent spatial perturbation $\epsilon_k(z)$ [108]. By inserting the approximation into eq. (1.36) and writing the integral

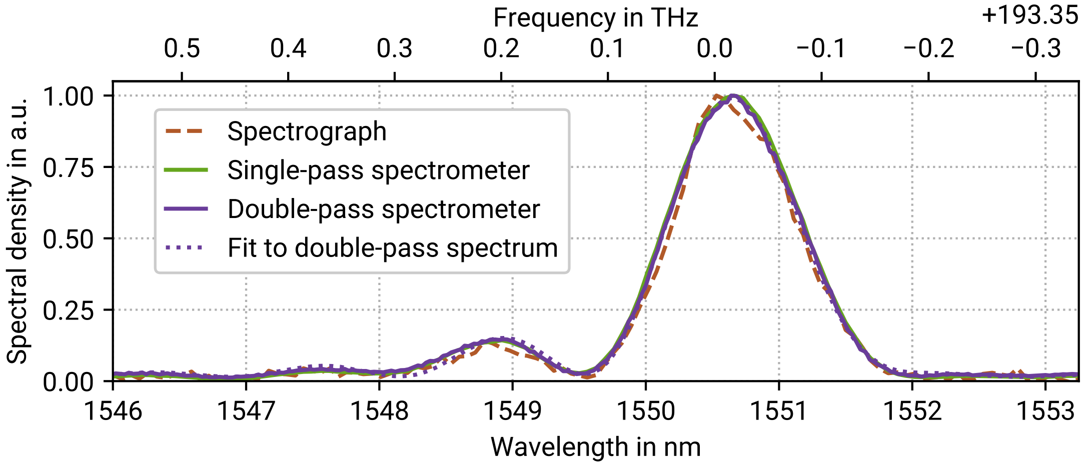


Figure 2.22: Type-II SPDC spectra measured with the dispersion-based single-photon spectrometer in single-pass and double-pass configuration and with the spectrograph. A fit of eq. (2.14) over ϵ_k' and ϵ_k'' to the double-pass data is shown for comparison.

over the crystal length as an FT of the phase term multiplied by a rectangle function (cf. eq. (A.21)), the shape of the phase matching function becomes

$$\tilde{\Phi}(\Omega) \propto \mathcal{F}_z\left[\exp\left(\mathrm{i}\int_{-L/2}^{z} \epsilon_k(\xi)\,\mathrm{d}\xi\right)\mathrm{rect}_L(z)\right]\left(\Delta k(\Omega) - \frac{2\pi}{\Lambda}\right). \tag{2.13}$$

As the perturbation is small, it can be expanded around the crystal center up to the second order as $\epsilon_k(\xi) = \epsilon_k'\xi + \epsilon_k''\xi^2/2$, with the constant order being absorbed into $\Delta k(\Omega)$. Such smooth variations of ϵ_k along the crystal can be caused, for example, by a variation of the waveguide width [127]. The spectral density for the signal photons thereby becomes

$$|\tilde{\Phi}(\Omega)|^2 \propto \left|\mathcal{F}_z\left[\exp\left(\mathrm{i}\frac{\epsilon_k'}{2}z^2 + \mathrm{i}\frac{\epsilon_k''}{6}z^3\right)\right]\mathrm{rect}_L(z)\right|^2\left(\Delta k(\Omega) - \frac{2\pi}{\Lambda}\right). \tag{2.14}$$

The term $\exp\left(\mathrm{i}\epsilon_k' z^2/2\right)$ and the rectangle function are even functions in z such that their FT is also even. Therefore, the lowest expansion order of ϵ_k that can lead to an asymmetry of the spectrum is the z^3-term. Figure 2.22 shows a fit of eq. (2.14) over ϵ_k' and ϵ_k'' to the data measured with the double-pass dispersion spectrometer. It shows that the model reproduces the measured spectral density. Therefore, the model is used in chapter 7 to obtain the complex-valued type-II photon spectrum for the QKD simulation.

2.3 Interferometers

An advantage of phase-time-encoded quantum bits is that the key transmission is independent of the polarization changes in the fiber link, so polarization control is not required. However, because the photons can arrive with an arbitrary polarization at the receivers, the IFs must allow for polarization-independent interference. They are therefore set up in a Michelson configuration with two *Faraday rotator mirrors* (FRMs) consisting of 45° Faraday rotators in front of retroreflectors, as shown in fig. 2.23. The photons enter the

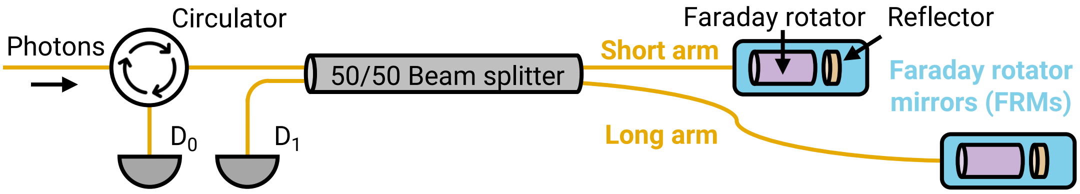


Figure 2.23: Schematic setup of an imbalanced Michelson interferometer with FRMs.

IF through a circulator. This circulator guides photons returning from the IF to the first Detector D_0. Detector D_1 is connected to the fourth port of the beam splitter.

An FRM maps an incoming linear polarization to the orthogonal linear polarization, and it maps left- to right-circular polarization and vice versa [129, 130]. When light with a particular polarization state is sent through a birefringent fiber and reflected by an FRM such that it travels back through the same fiber, the resulting polarization state is always orthogonal to the input state [129]. Thereby, a FRM compensates any reciprocal[19] birefringence in the fiber. Incoming photons experience different polarization transformations when traveling forward through the IF arms, but after traveling back, the polarization of the light returning from both arms is the same polarization, orthogonal to the input state. As Michelson IFs with Faraday mirrors enable interference for arbitrary input polarizations, they are used in various QKD setups, for example in refs. [60, 61, 112, 117, 133].

The pump IF is identical to the receiver IFs up to the circulator, which is polarization-maintaining and optimized for higher optical input powers. Light launched into port 1 with linear polarization along the slow axis leaves port 3 polarized along the fast axis due to the FRMs. A PM fiber with a 90° offset is spliced to port 3 to realign the polarization to the slow axes.

The effect of the IFs can be visualized by considering the probability density of the biphoton wave packet $|\psi_{\mathrm{IF}}(t_{\mathrm{A}}, t_{\mathrm{B}})|^2$ after the receiver IFs, as shown in fig. 2.24 for the detector combination A_0-B_0. For short fiber length, $|\psi_{\mathrm{IF}}(t_{\mathrm{A}}, t_{\mathrm{B}})|^2$ is given by seven narrow stripes and the shape of each stripe is determined by $|\psi(t_{\mathrm{A}}, t_{\mathrm{B}})|^2$. The probability in the central-central time bin combinations is twice as high as in other time bin combinations because the IF phases are aligned for constructive interference. If, for example, the delay of Alice's IF would not match the delay of the other two IFs, two narrow stripes with a horizontal offset would appear in the central-central combination, and no two-photon interference would be observed. Therefore, the width of the stripe is related to the required accuracy of the *optical path differences* (OPDs) in the IFs.

For long fiber links, CD elongates the wave packet such that photons leak out of the time bins. For very long fibers, the photons may leak into adjacent time bins, leading for example in fig. 2.24 for $L_{\mathrm{A}} = L_{\mathrm{B}} = 100\,\mathrm{km}$ to a nonzero detection probability of time basis errors. Therefore, the width and the separation of the time bins must be chosen to avoid photon leakage into adjacent time bins even for the maximum link length for which the QKD system is designed. Based on these considerations, the required accuracy of the OPDs and the choice of the IF delays are discussed in more detail in the following.

[19] A FRM does not compensate for non-reciprocal birefringence introduced by the Faraday effect [131, 132]. However, the Faraday effect in the IF fibers is negligible.

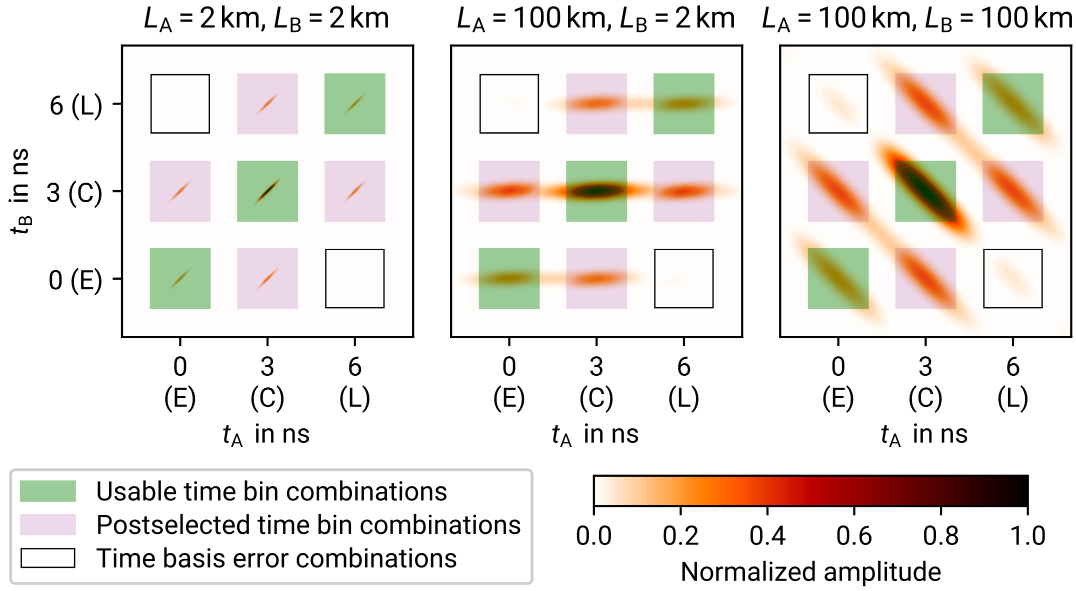


Figure 2.24: Example of a probability density $|\psi_{\mathrm{IF}}(t_\mathrm{A}, t_\mathrm{B})|^2$ after the IFs for the detector combination A_0-B_0 with different fiber link lengths L_A and L_B to Alice and Bob. The initial shape of the pump pulse is given by a Gaussian pump pulse with a FWHM of 400 ps and a sinc^2-shaped phase matching function for a 24 mm long type-II PPLN crystal. The early (E), central (C), and late (L) time bins are 2 ns wide, and the IF delay is 3 ns. The time bin combinations EE, CC, and LL yield quantum key bits. Detections in the EL and LE time bin combinations yield errors in the time basis, and detections in the combinations EC, LC, CE, and CL are postselected. In the combinations EL and LE, the probability density becomes nonzero for $L_\mathrm{A} = L_\mathrm{B} = 100$ km because photons from the side lobes of the sinc^2-shaped JSA leak into these time bin combinations.

2.3.1 Required Accuracy of the Optical Path Differences

The minimal $\mathrm{QBER_p}$ is obtained when the OPDs in the IFs are precisely matched and the phases are perfectly aligned. When the OPDs are different, imperfect two-photon interference increases the $\mathrm{QBER_p}$. The minimal $\mathrm{QBER_p}$ that can be obtained when the IF phases are scanned over 2π, $\mathrm{QBER_{p,\,min}}$, depends on the accuracy of the OPDs in relation to the shape of the biphoton wave packet $\psi(t_\mathrm{A}, t_\mathrm{B})$. A rule of thumb estimation for the required accuracy is that the difference between the OPDs of different IFs should be much smaller than the coherence length of the photons, enabling two-photon interference. For the type-II photons, the coherence length $L_\mathrm{c} = c_0\tau_\mathrm{c}$ can be directly calculated via the coherence time τ_c from the measured spectrum by using eq. (A.15), which yields $L_\mathrm{c} = 0.88$ mm. On the one hand, the deviation of the OPDs of different IFs must be much smaller than this value to obtain a high two-photon interference contrast and a low $\mathrm{QBER}_{\mathrm{p,\,min}}$. On the other hand, this value provides a minimum for the OPD. The IF delay must be much larger than τ_c such that single-photon interference in the IFs is suppressed.

A more precise estimate for the required OPD precision is needed to specify the required accuracy for the building method because manufacturing the IFs with very precise OPDs is technically challenging. Based on the required accuracy, the building method can be optimized to be as simple and fast as possible so that higher numbers of receiver modules can be built for large QKD networks with reasonable efforts. The required accuracy can be obtained by considering the achievable $\mathrm{QBER}_{\mathrm{p,\,min}}$ as a function of the OPD mismatch.

Calculation of the Required OPD Accuracy for a Joint Spectral Amplitude Factorized in Diagonal Coordinates

The factorization of the JSA in rotated coordinates from eq. (2.7) allows to express $\mathrm{QBER}_{\mathrm{p,\,min}}$ in terms of the autocorrelation functions of $\alpha(t_+)$ and $\Phi(t_-)$. To simplify this analysis and to isolate the QBER contribution caused by mismatched OPDs, the beam splitters are assumed to be perfect 50/50 splitters. All losses and the chromatic dispersions in the IFs are neglected, meaning that the expansion of $k(\omega)$ from eq. (1.11) is truncated after the linear order in Ω for the interferometer fibers.

When a wave packet $\alpha_\mathrm{fund}(t)$ centered around the fundamental frequency ω_0 is sent through the pump IF with OPD ΔL_P, the field after the IF is given by $\tilde{\alpha}_\mathrm{fund}(\omega)\big(1+\mathrm{e}^{\mathrm{i}\Delta L_\mathrm{P}(k_0+\Omega/v_\mathrm{g})}\big)/2$, up to a phase reference factor for the short path that is of no further relevance. After second-harmonic generation, the spectrum $\tilde{\alpha}(\omega)$ of the pump field guided into the SPDC crystal is centered around $2\omega_0$, such that the field can be expressed as $\alpha(t) = A(t)\,\mathrm{e}^{-2\mathrm{i}\omega_0 t}$ with a slowly varying envelope $A(t)$. The JSA, after transmission through the fiber links and receivers, is given by

$$\tilde{\psi}_\mathrm{IF}(\omega_\mathrm{s},\omega_\mathrm{i}) = \frac{1}{4\sqrt{2}}\iint \mathrm{d}\omega_\mathrm{s}\,\mathrm{d}\omega_\mathrm{i}\,\overbrace{\Big(1+\mathrm{e}^{\mathrm{i}[2k_0\Delta L_\mathrm{P}+[\omega_\mathrm{s}+\omega_\mathrm{i}-2\omega_0]\tau_\mathrm{P}]}\Big)}^{\text{Source interferometer}}\,\overbrace{\tilde{\alpha}(\omega_\mathrm{s}+\omega_\mathrm{i})\tilde{\Phi}(\omega_\mathrm{s}-\omega_\mathrm{i})}^{\tilde{\psi}(\omega_\mathrm{s},\omega_\mathrm{i})}$$
$$\times\,\underbrace{\mathrm{e}^{\mathrm{i}[k(\omega_s)L_A+k(\omega_i)L_B]}}_{\text{Fiber links}}\,\underbrace{\Big(1+\mathrm{e}^{\mathrm{i}\Delta L_\mathrm{A}[k_0+(\omega_\mathrm{s}-\omega_0)/v]}\Big)}_{\text{Alice's IF}}\,\underbrace{\Big(1+\mathrm{e}^{\mathrm{i}\Delta L_\mathrm{B}[k_0+(\omega_\mathrm{i}-\omega_0)/v_\mathrm{g}]}\Big)}_{\text{Bob's IF}}. \tag{2.15}$$

Here, the lengths of the fiber links to Alice and Bob are L_A and L_B, and the path length differences of the IFs are ΔL_A for Alice, ΔL_B for Bob and ΔL_P for the pump IF. The probability $P(A_{0,\mathrm{C}}, B_{0,\mathrm{C}})$ of obtaining a coincident count in the detectors A_0 and B_0 in the central time bin is given by the integral over the joint spectral density, taking only the path combinations (s, l, l) and (l, s, s) (cf. section 1.2) into account. The expression can be evaluated in the rotated $\omega_\pm$ coordinate system and depends on the deviation of Alice's and Bob's path differences $d_{\mathrm{A/B}} = \Delta L_{\mathrm{B}} - \Delta L_{\mathrm{A}}$ and on the deviation of the path difference of the pump IF from the mean of the receivers, $d_{\mathrm{P}} = \Delta L_{\mathrm{P}} - (\Delta L_{\mathrm{A}} + \Delta L_{\mathrm{B}})/2$:

$$P(A_{0,\mathrm{C}}, B_{0,\mathrm{C}}) = \frac{1}{16}\,\mathrm{Re}\left[1 + \exp(2ik_0 d_{\mathrm{P}})\, g_A^{(1)}\!\left(\frac{d_{\mathrm{P}}}{v_{\mathrm{g}}}\right) g_\Phi^{(1)}\!\left(\frac{d_{\mathrm{A/B}}}{2v_{\mathrm{g}}}\right)\right]. \tag{2.16}$$

Here, $g_\Phi^{(1)}$ and $g_A^{(1)}$ are the normalized autocorrelation functions (cf. eq. (A.12)) of $\Phi(t)$ and $A(t)$. The oscillation period of the complex exponential is π/k_0, meaning that the oscillation is much faster than variations in the autocorrelation functions. Therefore, the autocorrelations can be assumed to be almost constant over one oscillation period. $\mathrm{QBER}_{\mathrm{p,\,min}}$ is therefore approximately given by

$$\mathrm{QBER}_{\mathrm{p,\,min}}(d_{\mathrm{P}}, d_{\mathrm{A/B}}) \approx \frac{1}{2}\left[1 - \left|g_A^{(1)}\!\left(\frac{d_{\mathrm{P}}}{v_{\mathrm{g}}}\right) g_\Phi^{(1)}\!\left(\frac{d_{\mathrm{A/B}}}{2v_{\mathrm{g}}}\right)\right|\right]. \tag{2.17}$$

When the pump IF is aligned such that $d_{\mathrm{P}} = 0$, the dependence on $d_{\mathrm{A/B}}$ is given by $\mathrm{QBER}_{\mathrm{p,\,min}}(0, d_{\mathrm{A/B}}) = \big(1 - \big|g_\Phi^{(1)}[d_{\mathrm{A/B}}/(2v_{\mathrm{g}})]\big|\big)/2$. When instead Alice's and Bob's IFs are aligned to $d_{\mathrm{A/B}} = 0$, the dependence on d_{P} is $\mathrm{QBER}_{\mathrm{p,\,min}}(d_{\mathrm{P}}, 0) = \big(1 - \big|g_A^{(1)}(d_{\mathrm{P}}/v_{\mathrm{g}})\big|\big)/2$. Figure 2.25 shows the influence of the misalignments $d_{\mathrm{A/B}}$ and d_{P} on $\mathrm{QBER}_{\mathrm{p,\,min}}$. Assuming an ideal crystal of length L and a rectangular pump pulse of duration T, the autocorrelations attain a triangular shape because A and Φ become rectangle functions. The $\mathrm{QBER}_{\mathrm{p,\,min}}$ then simplifies to

$$\mathrm{QBER}_{\mathrm{p,\,min}}(d_{\mathrm{P}}, 0) = \frac{1}{2}\min\!\left(\left|\frac{d_{\mathrm{P}}}{Tv_{\mathrm{g}}}\right|, 1\right) \quad \text{and} \quad \mathrm{QBER}_{\mathrm{p,\,min}}(0, d_{\mathrm{A/B}}) = \frac{1}{2}\min\!\left(\left|\frac{d_{\mathrm{A/B}}}{2L\Delta k' v_{\mathrm{g}}}\right|, 1\right). \tag{2.18}$$

The QKD system is operated in the range of low QBERs up to around 2 % displayed in the inset plots of fig. 2.25. In this range, the curve for $\mathrm{QBER}_{\mathrm{p,\,min}}(d_{\mathrm{P}}, 0)$ calculated from the measured data is much shallower than the curve for an ideal rectangle pulse, which can be attributed to the limited data resolution. To obtain a $\mathrm{QBER}_{\mathrm{p,\,min}}$ below 1 %, a deviation d_{P} of less than 2 mm is acceptable according to the curve for an ideal pulse. For $|d_{\mathrm{P}}| > 100\,\mathrm{mm}$, the curve calculated from the measured data slowly increases until it reaches 50 % around $|d_{\mathrm{P}}| \approx 400\,\mathrm{mm}$. This deviation from the ideal curve is due to the relatively long tail of the falling edge of the pump pulse (cf. fig. 2.11 (b)) introducing long-range correlations.

Although the measured crystal spectrum is not well approximated by a sinc^2 function due to its asymmetry, the curve for $\mathrm{QBER}_{\mathrm{p,\,min}}(0, d_{\mathrm{A/B}})$ of an ideal crystal deviates only slightly

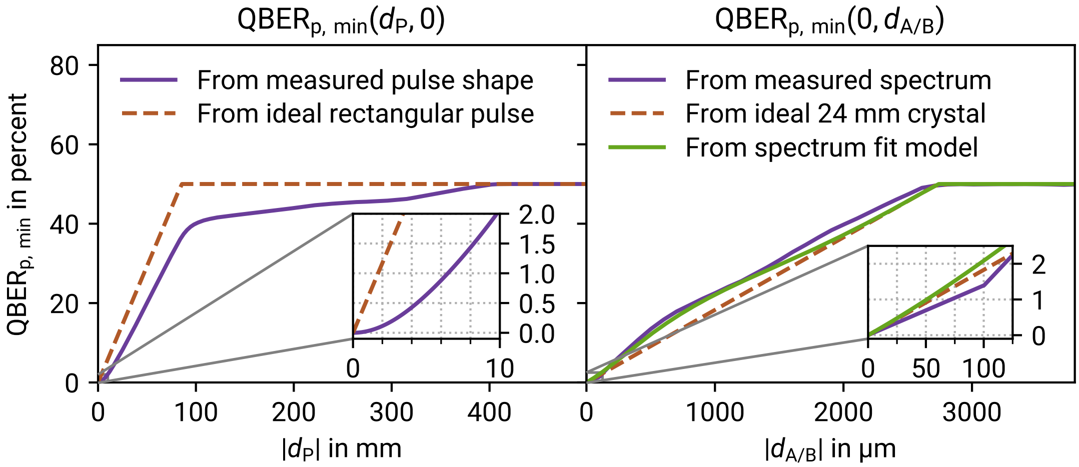


Figure 2.25: Estimated QBER$_{\text{p, min}}$ due to OPD misalignment of the IFs. Left: Influence of the pump IF misalignment d_P when Alice's and Bob's OPDs are matched. The curve for the measured pump pulse shape was calculated for the pulse shape from fig. 2.11 with an FWHM of 418 ps. Right: Influence of the pump IF misalignment $d_\text{A/B}$. The function $g_\Phi^{(1)}$ for the measured spectrum was calculated from the spectrograph data shown in fig. 2.22 via the Wiener-Khinchine theorem and for the fit model from eq. (2.14). The curves for the ideal rectangular pump pulse and the ideal crystal are given by eq. (2.18).

from the curves for the measured spectrum or for the fit model. In the inset, the kink in the curve for the measured spectrum shows that the data resolution limits the accuracy in this range. However, all three curves are relatively close together, showing that d_AB should not exceed 50 µm to keep QBER$_{\text{p, min}}$ below 1 %. It is important to note that the allowed tolerance in the fiber lengths is only half of the deviations d_P and d_AB because the light passes each fiber section twice in the Michelson configuration.

A multi-step building method was developed in close collaboration with Oleg Nikiforov to build the IFs with an accuracy better than 25 µm. This method allows multiple IFs to be built quickly and reproducibly with a precise OPD, which is an essential step towards realizing larger QKD networks with tens or hundreds of users. The method was used to build the IFs for the two-user QKD system and was further improved to build the IFs for the q-hub QKD network. The interference quality was confirmed by setting up a QKD session with a very low mean photon pair number to reduce the contribution of multi-photon-pair emission to the QBER. QBERs below 0.5 % were observed, indicating a high interference contrast [II]. At the time of submission of this thesis, a patent is pending on the building method, so further details cannot be disclosed here.

2.3.2 Choice of the Optical Path Difference Between Long and Short Arms

An important parameter that must be chosen before the IFs are built is the value for the OPD between the long and short arms. The OPD determines the repetition cycle time. Equally-spaced time bins are obtained when the pump pulse repetition time is chosen to three times the time bin separation. On the one hand, short OPDs are generally preferred because they allow operating the system at high pulse repetition rates. On the other hand, the OPD must be chosen large enough such that the peaks in the arrival time histogram (cf. fig. 1.2) of the photons are well separated. If the peaks overlap, photons are sometimes assigned to the wrong time bin, resulting in additional quantum bit errors and reduced secure key rate. The width of the peaks in the arrival time histogram depends on the duration of the pump pulse, on the timing jitters of the pulse generation electronics, SPDs, and timing electronics in the receivers, and on the elongation of the photon wave packets due to CD in the fiber links. While the timing jitter distributions and pulse duration are fixed, the wave packet elongation depends on the photon spectrum and the length of the transmission link.

Elongation of the Photon Wave Packets Due to Chromatic Dispersion

In fig. 2.24, it was shown for an exemplary JSA how CD affects the shape of the wave packet. For the QKD experiments, the range of dispersion values is the most important where CD leads to an elongation of the distributions $p_{\mathrm{s/i}}(t_{\mathrm{s/i}})$ that is in the same order of magnitude as the pump pulse duration. In this parameter range, most of the photons are still detected within the time bins, but the elongation leads to a leakage of photons out of the time bins. For even larger dispersions, the photons eventually leak into adjacent time bins. When the wavelength of the photon sent to Alice is longer than the center wavelength, the wavelength of the photon sent to Bob is automatically shorter than the center wavelength. Around 1550 nm, the dispersion in the SMF is anomalous, meaning that the photon sent to Alice travels slower than the photon sent to Bob. If the chromatic dispersion is large, Alice may register the photon in the late time bin, while Bob registers it in the early time bin, leading to an error bit in the time basis.

At the parameters used in the experiments, the phase matching function is much broader than the spectrum of the pump pulse. Conversely, $\Phi(t) = \mathcal{F}_{\omega}^{-1}\big(\tilde{\Phi}(\omega)\big)$ is shorter than the duration of the pump pulse due to the uncertainty principle. Therefore, CD elongates $\Phi(t)$ much more than the pulse envelope $A(t)$.

The pulse shape $|\alpha(t)|^2$ determines the probability density for creating the photon pair. For small dispersions βL, the arrival time distributions of the signal photons $p_{\mathrm{s}}(t_{\mathrm{s}})$ is therefore determined by the pump pulse shape $|\alpha(t)|^2$. When the dispersion is larger, the spectral density of the phase matching function is mapped to the time domain (cf. eq. (1.17)), such that the distribution relative to the time where the photon was created attains the shape of $|\tilde{\Phi}(\Omega)|^2$ in time. Neglecting the dispersion of the pump pulse, the resulting probability density $p_\mathrm{s}(t_\mathrm{s})$ would become the convolution of $|\alpha(t)|^2$ and $|\tilde{\Phi}(\Omega)|^2$.

To obtain a quantitative estimate for the elongation of the wave packets, $p_\mathrm{s}(t_\mathrm{s})$ can be calculated. For simplicity, only a single time bin is considered, such that $p_\mathrm{s}(t_\mathrm{s})$ is given by the marginal distribution of the joint spectral density (cf. eq. (1.31)) multiplied by the phase factor for the propagation through fibers of lengths L_s and L_i:

$$p_\mathrm{s}(t_\mathrm{s}) = \int \left| \mathcal{F}^{-1}_{\omega_\mathrm{s},\omega_\mathrm{i}}\Big(\tilde{\alpha}(\omega_\mathrm{s}+\omega_\mathrm{i})\tilde{\Phi}(\omega_\mathrm{s}-\omega_\mathrm{i})\, \mathrm{e}^{\mathrm{i}[k(\omega_\mathrm{s})L_\mathrm{s}+k(\omega_\mathrm{i})L_\mathrm{s}]}(t_\mathrm{s},t_\mathrm{i})\Big)\right|^2 \mathrm{d}t_\mathrm{i}\,. \tag{2.19}$$

The phase matching function is much broader than the pump pulse spectrum, such that similar as in eq. (2.10), the approximation $\omega_\mathrm{s}+\omega_\mathrm{i} \approx 2\omega_0$ can be used in the argument of $\tilde{\Phi}$ to approximate $\tilde{\Phi}(\omega_\mathrm{s}-\omega_\mathrm{i}) \approx \tilde{\Phi}[2(\omega_\mathrm{s}-\omega_0)]$, which allows simplifying eq. (2.19) to

$$p_\mathrm{s}(t_\mathrm{s}) \approx \left(|\alpha|^2 * \left|\mathcal{F}^{-1}_{\omega_\mathrm{s}}\Big(\tilde{\Phi}[2(\omega_\mathrm{s}-\omega_0)]\,\mathrm{e}^{\mathrm{i}k(\omega_\mathrm{s})L_\mathrm{s}}\Big)\right|^2\right)(t_\mathrm{s})\,. \tag{2.20}$$

Using the second-order approximation for $k(\Omega)$ from eq. (1.11) and eq. (1.17) yields

$$p_\mathrm{s}(t_\mathrm{s}) \approx \frac{1}{|\beta L|}\Big(|\alpha|^2 * \big|\tilde{\Phi}_\mathrm{CD}\big|^2\Big)(t_\mathrm{s}-L_\mathrm{s}/v_\mathrm{g}) \quad \text{with} \quad \tilde{\Phi}_\mathrm{CD}(t) = \tilde{\Phi}\left(\frac{2t}{\beta L}\right). \tag{2.21}$$

Equation (2.21) is valid when the dispersion is so large that the factor $\exp[-\mathrm{i}\tau^2/(2\beta L)]$ appearing within the FT in Andrianov's expression, eq. (1.16), is almost constant over the range of τ values for which the IFT of $\tilde{\Phi}[2(\omega_\mathrm{s}-\omega_0)]$ from eq. (2.20) attains non-negligible values. Assuming that for a phase tolerance below $\Delta\phi = 0.1$ the phase term can be neglected, the approximation is valid for the type-II crystal with $L_\mathrm{crystal} = 24\,\mathrm{mm}$ for fiber lengths longer than $(L_\mathrm{crystal}/\Delta k')^2/(2|\beta|\Delta\phi) \approx 10\,\mathrm{km}$. Therefore, eq. (2.21) can be used to estimate the arrival time distribution for the fiber lengths used in the QKD field test.

Figure 2.26 (a) shows $p_\mathrm{s}(t_\mathrm{s})$ computed from eq. (2.21) for two different fiber lengths. For the type-II photons, the side lobe of the spectrum introduces a pronounced foothill. The base of the distribution is approximately 1.5 ns long for the fiber length of 26.8 km used in the QKD field test and 3 ns long for a 50 km long fiber. This means that the time bin separation necessary to avoid the leakage of photons into adjacent time bins for fiber lengths up to 50 km is 3 ns. Figure 2.26 (b) shows measured arrival time distributions for type-0 photons demultiplexed by the 100 GHz AWG. The distributions were measured by connecting Bob via the DCFs to the source, introducing a dispersion equivalent to 30, 60, or 90 km of optical fiber, but with the opposite sign. The DCFs were chosen because the sign of the dispersion is not important to investigate the magnitude of the elongation, and the losses are significantly lower than for the length of SMF with the same dispersion. Using the DCFs instead of SMFs, therefore, improves the signal-to-noise ratio in the measurement. It can be seen that the type-0 photons are not elongated as much as the type-II photons. The reason is that the transmission spectrum of the 100 GHz AWG channels (cf. fig. 2.15) is narrower and does not show side lobes.

The OPD of the IFs should be suitable for QKD with both type-0 and type-II photons. The timing jitter distribution of the SPDs and timing electronics with a width of around 250 ps (cf. fig. 5.8) do not broaden the count distribution significantly. Based on these considerations, the delay between the long and short IF paths and the resulting pulse repetition frequency f_rep were chosen to

Interferometer delay and fundamental pulse repetition frequency of the q-hub system

$$T = \frac{\Delta L}{v_\mathrm{g}} = 3.03\,\mathrm{ns} \quad \text{and} \quad f_\mathrm{rep} = \frac{1}{3T} = 110\,\mathrm{MHz}\,. \tag{2.22}$$

The width of the time bins is set to 1 ns. For the q-hub system, five IFs with this delay were built during Lucas Bialowons's master's thesis [M5] for the source and four receivers.

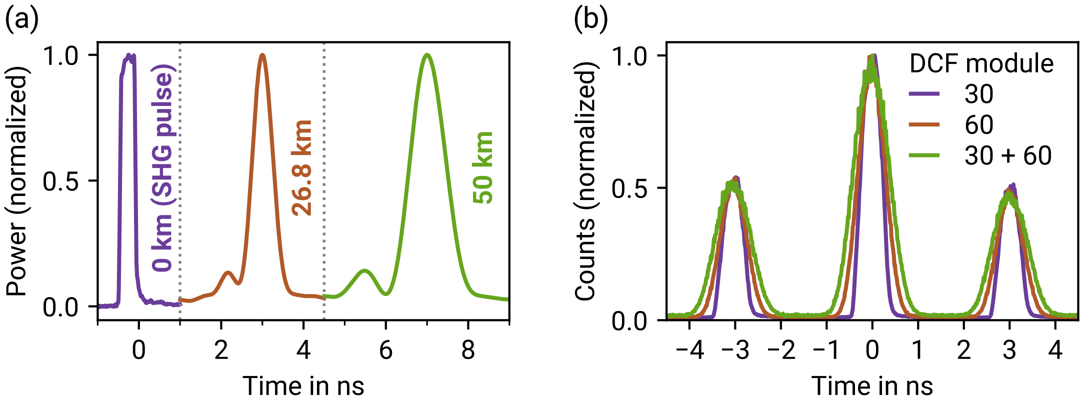


Figure 2.26: Elongation of the photon arrival time distribution due to chromatic dispersion in the transmission fibers. (a) Expected photon arrival time distribution $p(t)$ for type-II photons after typical fiber lengths used in the QKD field test. Without a transmission fiber, $p(t)$ attains the shape of the SHG pump pulse from fig. 2.11 (b). For the fiber lengths of 26.8 and 50 km, $p(t)$ is calculated according to eq. (2.21) by convolving the pump pulse with the photon spectrum (cf. fig. 2.22). For better comparability, the distributions are shifted in time. (b) Measured arrival time histogram $p(t)$ for type-0 photons demultiplexed with the 100 GHz AWG after traveling through the DCFs, introducing a dispersion equivalent to 30, 60, and 90 km of SMF.

2.4 QKD Receivers and Setup Operation

For QKD, the phase relation from eq. (1.2) must be fulfilled to observe two-photon interference. To obtain a low $\mathrm{QBER_p}$, the phase of the IFs must be kept stable. In this section, the requirements for the stability of phase and temperature are discussed, and the setup of the receivers and the methods to meet these requirements are described.

Required Stability of Phase and Temperature

The phase of an IF depends on the *optical path difference* (OPD) $n\Delta L$ with the refractive index n and the path length difference ΔL. When the fiber is heated, it becomes longer due to thermal expansion. Furthermore, its refractive index changes. Both effects lead to a dependence of the phase on the temperature. The phase difference $\Delta\phi$ at frequency ω introduced by a small temperature change ΔT of the fibers depends on the derivatives of n and ΔL with respect to the temperature:

$$\Delta\phi = \Delta T \frac{\omega}{c_0} \frac{\partial}{\partial T} n\Delta L = \omega \Delta L \Delta T \left(\frac{1}{c_0} \frac{\partial n}{\partial T} + \frac{n}{c_0 \Delta L} \frac{\partial \Delta L}{\partial T} \right). \tag{2.23}$$

For SMF, the refractive index change $c_0^{-1} \partial n / \partial T \approx 37\,\mathrm{ps/(km \cdot K)}$ contributes much more to the phase change than the thermal expansion $n/(c_0 L) \times \partial L / \partial T \approx 2\,\mathrm{ps/(km \cdot K)}$ [134]. The total temperature tuning coefficient is about [134–136]

$$\frac{1}{c_0 L} \frac{\partial nL}{\partial T} \approx 40 \frac{\mathrm{ps}}{\mathrm{km \cdot K}}. \tag{2.24}$$

The temperature sensitivity of the IFs calculated from eq. (2.23) thereby becomes $\partial \phi / \partial T \approx 9\,\pi/\mathrm{K}$. For perfect IFs, the maximal phase deviation that is allowed to keep the $\mathrm{QBER_p}$ below a certain threshold can be calculated from eqs. (1.2) and (1.3) by

$$\Delta\phi = \arccos(1 - 2\,\mathrm{QBER_p}). \tag{2.25}$$

To keep $\mathrm{QBER_p}$ below 1 %, the phase deviation must be kept below $\Delta\phi = 0.2$, meaning that the temperature deviation needs to be kept below $\Delta T \approx 7\,\mathrm{mK}$.

In principle, multiple approaches can be used to keep the phases aligned. For example, phase modulators [137] or tunable delay lines [138] can be inserted into one of the IF arms, but these components would introduce additional insertion losses, leading to lower key rates. Another option to adjust the phase is to use piezo-electric fiber stretchers to apply a variable mechanical tension to the IF fibers for realigning the phases [61, 62, 133]. However, this approach requires an error signal, according to which the stretcher re-adjusts the phase. Such an error signal could be provided, for example, by probing the IF phase with light at a different wavelength. Such an active stabilization would require additional components and complicate the setup [62, 138]. These disadvantages can be avoided by using the QBER_p as an error signal for the stabilization. If the IF is exposed to fast temperature variations and the key rate is low, the phase may already be misaligned before a sufficient number of key bits and error bits have been obtained to calculate QBER_p with the required accuracy. Therefore, if the stabilization is based on the QBER_p, the IFs need to be stabilized in temperature to prevent fast phase fluctuations due to temperature changes. The phases are then realigned to minimize the QBER_p, which can be realized with a piezo stretcher adjusting the path length of an IF arm or by slightly adjusting the IF temperature. The latter approach has the advantage that temperature control is already implemented for stabilization, so no additional components are needed. This approach has been chosen for the QKD network because the reduction of the complexity of the receiver module benefits the scalability of the multi-user QKD network.

Setup of the Receiver Modules

Each receiver consists of a fiber-optic IF in a temperature-controllable metal container, an electronic *temperature control unit* (TCU), two *single-photon detectors*[20] (SPDs) connected to the IF outputs and a *time controller*[21] (TC). The SPDs are characterized in detail in chapter 5. The TCs register the detector counts with a resolution of approximately 13 ps[22] and save a *timestamp* for each count. The timestamps are integers counting the picoseconds since the last reset of the TC clock. A schematic setup of a receiver is shown in fig. 2.27 (a). The TCUs and the design of the IF containers were developed by Oleg Nikiforov for the two-user QKD system during his Ph.D. [28]. Although the two-user QKD system only requires three TCUs for the two users and for the IF in the source, Nikiforov built a total of five TCUs named *Alice*, *Bob*, *Charlie*, *Diana* and *Source*.

Each temperature-controllable IF container consists of an outer container made of aluminum and an inner container consisting of an aluminum ground plate and a copper cover cap as shown in figs. 2.27 (b) and 2.27 (c). The outer container is covered by an insulating silicone cap. The ground plate of the inner container is temperature-stabilized against the ground plate of the outer container by four TECs. The ground plate of the outer container is temperature-stabilized by four TECs against a copper plate acting as a thermal reservoir. Two milled grooves in the ground plate of the inner container hold the Faraday rotator mirrors and beam splitter of the IF. A recess in the ground plate and an inset plate are prepared to hold fixtures for *electro-optic phase modulators* (EOPMs), which may be used in

[20] Single-photon detectors: ID220 from *IDQuantique*.

[21] Time controllers: ID900 Time Controller from *ID Quantique*.

[22] The distances between timestamps are not always multiples of 13 ps but follow a more complex scheme with a super-cycle of 625 ps = 47 × 13 ps + 14 ps [B2].

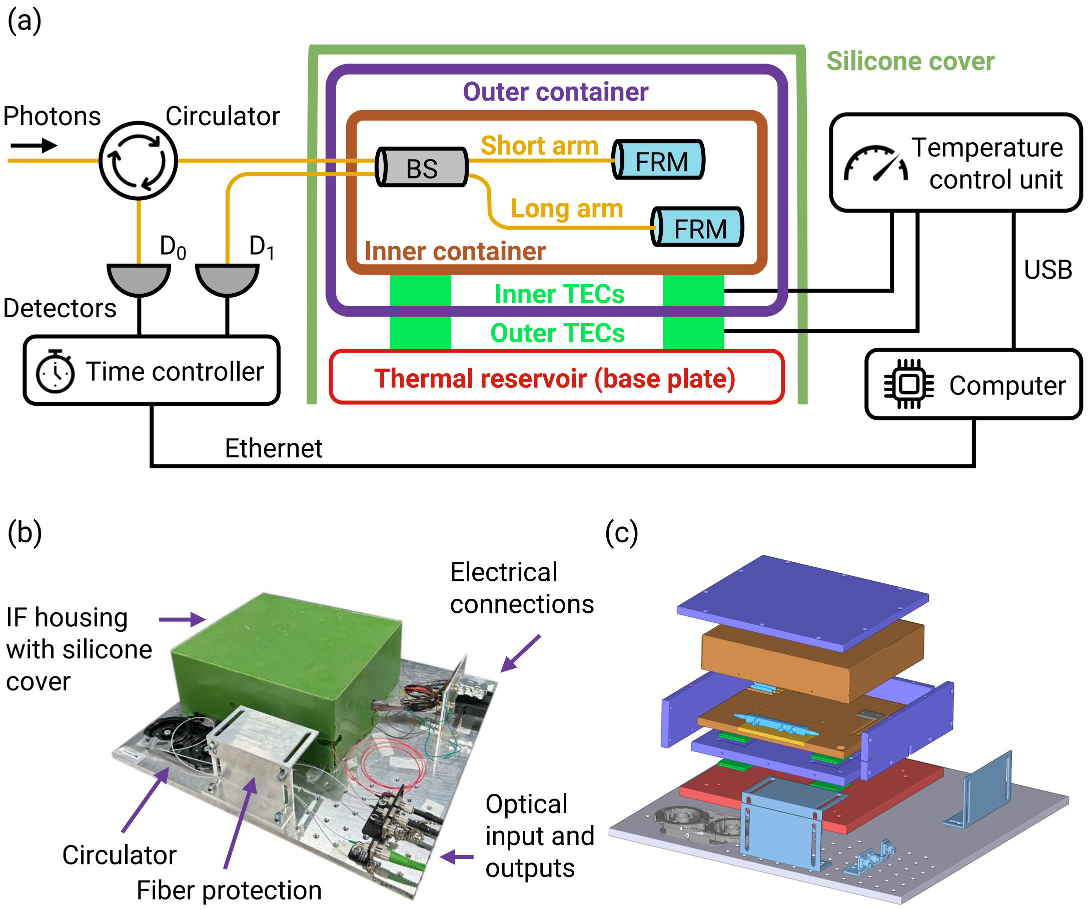


Figure 2.27: Setup of the QKD receivers. (a) Schematic setup. The interferometer consisting of a 50/50 beam splitter (BS) and two Faraday rotator mirrors (FRMs) is installed in an inner temperature stabilization container surrounded by an outer temperature stabilization container. The container temperatures are adjusted by a temperature control unit (TCU) via thermoelectric coolers (TECs). The photons are detected by two single-photon detectors D_0 and D_1, and the detector counts are time-stamped by a time controller. (b) Photo of the receiver *Eta*, typically used with the TCU *Charlie*. A green silicone cap covers the outer metal container to improve the temperature stability. (c) Exploded view of the containers. Light gray – base plate, red – thermal reservoir (copper base plate), green – TECs, violet — outer container, brown – ground plate and copper cap of inner container, light blue – FRMs and (optional) phase modulator, gold – base plate for phase modulator, blue-gray – fixtures for optical and electrical connections and fiber protectors, black – fiber component tray for the circulator.

future IFs for QKD protocols with active phase choice. Two further grooves for Faraday rotator mirrors, another groove for a beam splitter, and threaded mounting holes have been prepared. Thereby, in the future, a second IF with an EOPM can be easily installed in each container together with the current IF. Thermistors sensing the container temperatures and providing them to the control loops are positioned in holes in the ground plates of the inner and outer container. Additional thermistors allow for monitoring the temperatures of different parts of the inner and outer containers. The IF containers, fixtures for the optical and electrical connections, and component trays holding the circulators are mounted on aluminum base plates as shown in fig. 2.27 (b), fitting into 19 inch wide electronics racks. The receivers are named according to the Greek alphabet *Zeta*, *Eta*, *Theta*, *Iota* and *Kappa* for identification [M5].

Each TCU comprises a microcontroller board[23] managing two proportional-integral (PI) control loops controlling the temperature of the outer and inner metal container. The settings can be adjusted manually via a display and a rotary encoder in the front panel of the TCU or remotely via a USB connection. Figure 2.28 shows the front panel of the TCU *Alice*. The temperature resolution of the control loops is 0.5 mK around room temperature, and the specified long-term stability of the controller is 2 mK throughout one day [28]. The temperature for the inner container is chosen to 0.5 K above the temperature of the outer container, which itself is chosen to be a few kelvin above the room temperature. Thereby, frequent switching between the heating and cooling operation of the TECs is avoided, prolonging the lifetime of the TECs [139]. High-precision temperature measurements showed that the container temperatures can be kept stable with a precision of 1 mK over several hours when the room temperature changes only moderately [28, M5].

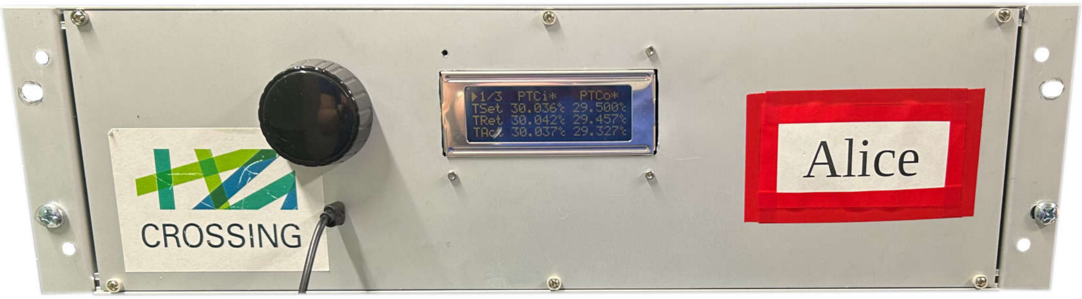


Figure 2.28: Front panel of the rack-mountable temperature control unit *Alice* with integrated display, rotary encoder knob for manual operation and USB connection for remote control.

[23] Microcontroller board: Arduino Micro from *Arduino*.

For the four users and for the q-hub, five new IF containers were built based on Nikiforov's design during the master's thesis of Lucas Bialowons [M5]. Nikiforov showed that the general design of the receivers is robust and achieves a temperature stability sufficient for stable QKD [28] with the two-user QKD system. Therefore, only a few minor adjustments were made compared to the containers of the two-user QKD system. The most relevant changes are the new design for the ground plate of the outer container, improving the cable management, and the change of the material for the ground plates for the inner and outer container, simplifying manufacturing. In Nikiforov's design, only the ground plate of the inner container was present. For the new containers, the copper cover cap has been added, completing the inner ground plate to an inner container to improve the phase stability of the IFs further.

Setup Operation

For the QKD tests in the laboratory at the university and during the field test at the facility of *Deutsche Telekom*, the q-hub and all receiver modules were located in one room. Fully functional key postprocessing software was not yet available during the experiments. Instead, the timestamps of all users were transferred from the TCs to one local computer for processing. The key rates and QBERs were then derived by directly comparing the raw keys. Large parts of the setup operation are automated to enable safe and robust QKD operation. The structure of the software and the remote control of the PPS were developed during the master's thesis of Lucas Bialowons [M5]. The software is written in the *Python* programming language and uses multiprocessing and multithreading to parallelize the data acquisition and to avoid unnecessary idle times of the system. Fast functions from the *NumPy* package and the *Numba* compiler are used to speed up time-consuming computations in the data processing. The software controls the setup, including the PPS, all TCUs, TCs, and the clock generator. It ensures that the devices are turned on in the correct order during startup. When it detects a system malfunction during startup or measurement, it automatically shuts down the system. The software processes the timestamps, reads and sets the IF temperatures, reads the SHG power from a power meter receiving 10 % of the SHG light, and logs the temperatures and pump powers. Furthermore, it features a control loop that automatically stabilizes the SHG power by adjusting the EDFA-2 pump current based on the reading of the SHG power. A graphical user interface shows diagrams of the key rates, QBERs, and IF temperatures.

During a QKD session, the TCs continuously record the counts of the SPDs and transfer blocks of timestamps every 4 seconds via Ethernet to the computer for evaluation. The timestamps are split into runs of 90 seconds for further processing. To evaluate a run, a clock recovery algorithm is applied to the timestamps of each receiver individually, identifying and correcting the deviation of the receiver time to the source time as described in section 2.5. The timestamps are then sorted into the time bins, the key bits and bit errors are obtained by matching the detection results of the users, and the sifted key rate, QBER_p, and QBER_t are calculated.

Based on the QBER_p from the current and previous runs, a phase adjustment algorithm decides whether the IF temperatures need to be adjusted. The algorithm aims for a minimal value of the correlation[24]. Due to noise and other imperfections, the QBER_p will, in practice, attain a value larger than zero even when the phases are perfectly aligned. To avoid oscillations around the minimum, the phase adjustment algorithm does not aim for $\mathrm{QBER}_\mathrm{p} = 0$. Instead, it stops to adjust the phase when a value close to a slightly higher target value calculated from QBER_t is reached.

The duration of 90 seconds for a run was found to be the optimal time to update the estimate of QBER_p. When longer times are chosen, the phase can drift significantly during a single run. When shorter times are chosen, the estimate of QBER_p is not precise enough to reliably determine if the phase needs to be adjusted because the number of error bits is low and the statistical uncertainty is high. From the value of QBER_p for a single run, it is unclear if the temperature needs to be increased or decreased to optimize QBER_p because QBER_p is a symmetric function of the phases around its minimum. Therefore, the algorithm remembers the previous adjustments and considers them to determine the direction of the required temperature change. The algorithm automatically corrects the decision in the next run when it notices that the previous adjustment has led in the wrong direction.

2.5 Receiver Synchronization using Clock Recovery

For the evaluation of the quantum keys, the photon arrival times must be assigned to the correct repetition cycle numbers and time bins. For that, the receiver modules need to be synchronized. In general, the clocks of the receivers and the source run with different clock frequencies, and there may be an initial timing offset. In the q-hub network, the q-hub clock is considered the main clock to which the receivers are synchronized.

The time error $\mathrm{TE}(t)$ is the deviation of the time t indicating when a photon is detected from the time t_q at the q-hub clock when the photon pair was generated:

$$\mathrm{TE}(t) = t - t_\mathrm{q} = \varDelta t_0 + \varDelta T(t)\,. \tag{2.26}$$

[24] The insertion losses of the circulators (cf. fig. 2.27 (a)) reduce the detection probabilities of the D_0 detectors compared to the D_1 detectors. When the phases are aligned to maximize the coincidence rates in the D_0-D_0 and D_1-D_1 combinations, these insertion losses lead to an imbalance between the zero and one bits in the phase basis. Therefore, the anticorrelated D_0-D_1 and D_1-D_0 coincidences are used as key bits to reduce the imbalance.

The time error can be separated into the initial time deviation Δt_0 at the beginning of the QKD session and the time-dependent deviation $\Delta T(t)$. The offset Δt_0 comprises constant electronic and optical delays introduced by the fiber links, and $\Delta T(t)$ comprises varying clock speeds in the q-hub and the receivers.

Even if the clocks themselves run with the same frequency, $\Delta T(t)$ can vary over time due to environmental effects changing the optical path length of the fiber link. While fibers deployed underground can be expected to have a relatively stable temperature, aerial fibers are exposed to the weather, so their temperature may change rapidly. To make an example demonstrating the relevance of the effect, a 50 km long aerial fiber is assumed to be heated by the sun with a rate of 1 mK/s. The propagation delay would then change by 39 ps every 20 seconds according to eq. (2.24). After 10 min, the delay has changed by more than 1 ns, which is more than the width of a time bin.

To keep the clocks synchronized, a method enabling sub-nanosecond precision is required. Typical synchronization signals used for network communication, such as the network time protocol (NTP), achieve millisecond precision [140], which is not precise enough for this application. One option to realize the synchronization is to establish a dedicated synchronization channel, for example, by sending optical signals through a parallel optical fiber or by wavelength- or time-multiplexing of synchronization signals with the QKD photons in the same fiber [141–145]. Another option is to set up a stable clock at each receiver and synchronize these clocks to an external high-precision time reference such as the GPS signal [146–148]. Using the *White Rabbit* protocol, sub-nanosecond timing synchronization can also be achieved via Ethernet [149, 150]. For *White Rabbit*, special *White Rabbit* switches and nodes are required. The synchronization of QKD systems based on *White Rabbit* has been demonstrated in refs. [151–153].

A disadvantage of all these synchronization methods is that they require additional resources, such as a dedicated channel or specialized hardware. They complicate the setup or reduce the achievable key rate because they block time slots for frequency channels that could otherwise be used for transmitting quantum bits.

The disadvantage can be overcome by using the photon arrival times for the synchronization. A common method is to evaluate the cross-correlation of the arrival times of entangled photons at two stations [154–156]. Another option to synchronize QKD systems with non-entangled photons is to use *clock recovery* (CR) based on the arrival times of the photons. Examples for such methods are a method for satellite-based QKD presented in ref. [157] and the method *Qubit4Sync* [158, 159].

One of the design criteria for the QKD network is the scalability in the number of users, which benefits from a simple hardware setup of the receivers. As CR is simply another step in the processing of the timestamps and does not require additional hardware resources, it was chosen as the synchronization method for the q-hub network. Therefore, a new efficient method for CR from the photon arrival times was developed. In the following, a brief analysis of the stability of the TC clocks is presented, requirements on the CR algorithm are derived, and the performance of the method is discussed.

The clock synchronization is implemented in two steps. In the first step, each user processes the timestamps from both detectors by the CR algorithm to obtain an estimate $\Delta T'(t_i)$ for the deviation for each timestamp t_i. Subsequently, the users subtract $\Delta T'(t_i)$ from their timestamps. In the second step, the constant offset between the timestamps due to Δt_0 is corrected (cf. eq. (2.26)). Details of the method to estimate $\Delta T'(t_i)$ are not presented because a patent on this method is pending.

Clock Stability of the Time Controllers

The requirements on the synchronization method depend on the stability of the clocks to synchronize. Therefore, the clock stability of all four TCs was analyzed during the bachelor's thesis of Christian Schaub [B7]. For the measurement, a function generator[25] was set up to produce reference pulses with a frequency of 1 MHz and its clock was synchronized to the 10 MHz reference of a stable rubidium frequency standard[26]. The pulses produced by the function generator were sent into the TCs. The time error TE(t) was obtained as the deviation of the n-th timestamp to the reference time of n µs. Figure 2.29 (a) shows the time error as a function of the reference clock time. It scales almost linearly with the time, with a rate between 1.04 µs/s for Diana and 1.35 µs/s for Charlie, meaning that the ID900 clock

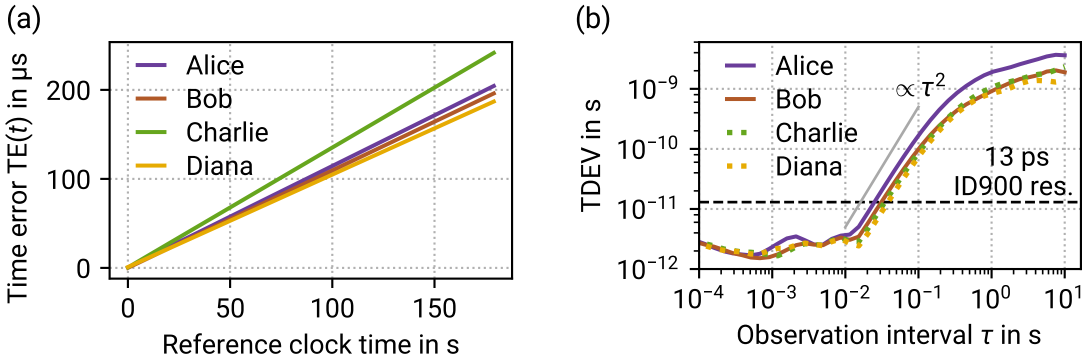


Figure 2.29: Clock stability of the time controllers. (a) Time error TE(t) as a function of the rubidium reference clock time. (b) Time deviation (TDEV) as a function of the clock observation interval. For comparison, the time resolution of the time controllers of 13 ps and a quadratic dependence of the TDEV on τ are shown.

[25] Function generator: AFG3052C from *Tektronix*.

[26] Rubidium frequency standard: FE-5650A from *FEI Communications, Inc.*

frequencies have a relative frequency offset of about 10^{-6} to the reference clock and of up to 0.31×10^{-6} among each other. This deviation shows that synchronizing the receivers is necessary even at short time scales. If Alice's and Charlie's clocks are not synchronized, their clocks deviate after 3 ms by the time bin width of 1 ns. However, a linear increase of $\mathrm{TE}(t)$ due to a constant frequency offset can be easily compensated in the data processing. More important are the nonlinear contributions to the time error, which can be quantified by the *time deviation* (TDEV)[27] commonly used in telecommunications. It is related to a modified version of the Allan variance often used in the field of clock frequency stability analysis [160, 161]. The TDEV is insensitive to constant frequency offsets and scales with the square of the observation time interval when a linear frequency drift dominates the clock error [161]. Figure 2.29 (b) shows the TDEV as a function of the clock observation interval for the TCs, computed with the Python library *Allantools*. The course of the TDEV is similar for all TCs, indicating that the clocks are of similar quality. For time intervals τ shorter than approximately 10 ms, the TDEV is almost constant and below the time resolution of the TCs. It grows for τ between 10 and 100 ms almost quadratically with τ. This means that the TDEV is limited for time intervals up to approximately 10 ms by the time resolution of the measurement. For time intervals up to approximately 100 ms, it is limited by the linear frequency drifts of the clocks.

Performance of the Clock Recovery Algorithm

Due to the statistical generation of photon pairs by SPDC and due to losses, the arrival of photons at a receiver is a probabilistic process. Furthermore, dark counts and afterpulses lead to detection noise. Therefore, deducing the q-hub clock time from a single count is impossible. Instead, it is necessary to accumulate several counts to compute the estimate $\Delta T'(t)$. The characterization of the clock stability in fig. 2.29 (b) showed that counts can at least be accumulated over times in the order of magnitude of 10 ms before clock instabilities become relevant and that for time intervals up to 100 ms the variation of $\Delta T(t)$ is mainly determined by smooth frequency drifts. To achieve stable CR based on these values, the algorithm accepts two parameters T_{acc} and T_{sm}, indicating over which time spans counts can be accumulated and over which time spans the clock frequency smoothly drifts. The performance of the CR algorithm can be tuned by adjusting these parameters,

[27] The time deviation is given by $\mathrm{TDEV}(\tau) = \tau \sigma_y(\tau)/\sqrt{3}$, with the *modified Allan variance* [160]

$$\sigma_y^2(\tau) = \frac{1}{2m^2\tau^2(N-3m+1)} \sum_{j=1}^{N-3m+1} \left(\sum_{i=j}^{j+m-1} x_{i+2m} - 2x_{i+m} + x_i \right)^2 .$$

The time interval is $\tau = m\tau_0$, the sampling interval is τ_0, the total number of samples is N, and the measured times are $x_1, \ldots, x_N$.

and the optimal values are expected to be in the orders of magnitude of 10 and 100 ms, respectively.

To assess the performance of the CR, a measurement was set up as shown in fig. 2.30 (a). The photon source is operated with the default settings used during the QKD field test (cf. table 3.1), and Bob's receiver is connected via a 81.2 km long fiber. Additionally, the function generator producing reference pulses with a frequency of 1 kHz is synced to the 10 MHz clock of the clock generator of the q-hub as shown in fig. 2.30 (a). The reference pulses are sent into one of the TC inputs, producing the timestamps $t_{\text{ref},\,i}$. They indicate the reference times $t_{\text{q},\,i} = n \times 1\,\text{ms}$ with $n \in \mathbb{N}$. The course of $\varDelta T'(t)$ is reconstructed by applying the CR algorithm to the photon timestamps and the corrected reference timestamps $t_{\text{ref},\,i} - \varDelta T'(t_{\text{ref},\,i})$ are compared to the reference times $t_{\text{q},\,i}$.

The longer the transmission distance, the lower the photon rate arriving at a receiver module. The CR algorithm becomes unstable for low photon rates when it cannot accurately track the clock deviation. The most frequent type of instability is the erroneous slip by one time bin separation of $(3f_{\text{rep}})^{-1}$. Figure 2.30 (b) shows such a slip as a jump in the difference between the estimate $\varDelta T'(t)$ and the actual deviation $\varDelta T(t)$. When a slip occurs during a QKD session, the QBER$_\text{t}$ suddenly jumps to high values, interrupting key exchange.

Timestamps were acquired over one hour with the setup in fig. 2.30 (a) with a fiber length of 81.2 km to Bob. To analyze the stability for lower count rates corresponding to longer transmission fibers, the measured count rate was artificially reduced, and it was analyzed if the estimate $\varDelta T'(t)$ exhibits a time bin slip. For that, random subsets of the measured timestamps were selected according to the damping in a SMF of the considered length, before the CR algorithm was applied. The random selection and analysis were repeated 10 times. The CR is considered stable if no time bin slip occurred in any of the 10 repetitions. If at least one slip occurred, it is considered partly stable, and if none of the repetitions was free of slips, it is considered unstable.

Figure 2.30 (c) shows that for values around $T_{\text{acc}} \approx 20$ to 25 ms, the CR is stable for transmission distances up to 120 km between the q-hub and one receiver or, equivalently, for a sum of the count rates in both detectors D_0 and D_1 down to 2 kcps. The longest distance between the q-hub and a user for which QKD was tested was 81.2 km (cf. chapter 3). This means the CR algorithm works stably for the practically relevant range of transmission link lengths. However, as the photon loss and the clock deviations are statistical processes, it is nevertheless, in rare cases, possible that the clock recovery algorithm slips. To avoid the abortion of the QKD session in these cases, automatic resynchronization is implemented in the evaluation software. Sudden jumps in the QBER$_\text{t}$ from one run to the next one are automatically detected. In the following run, a resynchronization is triggered, as executed

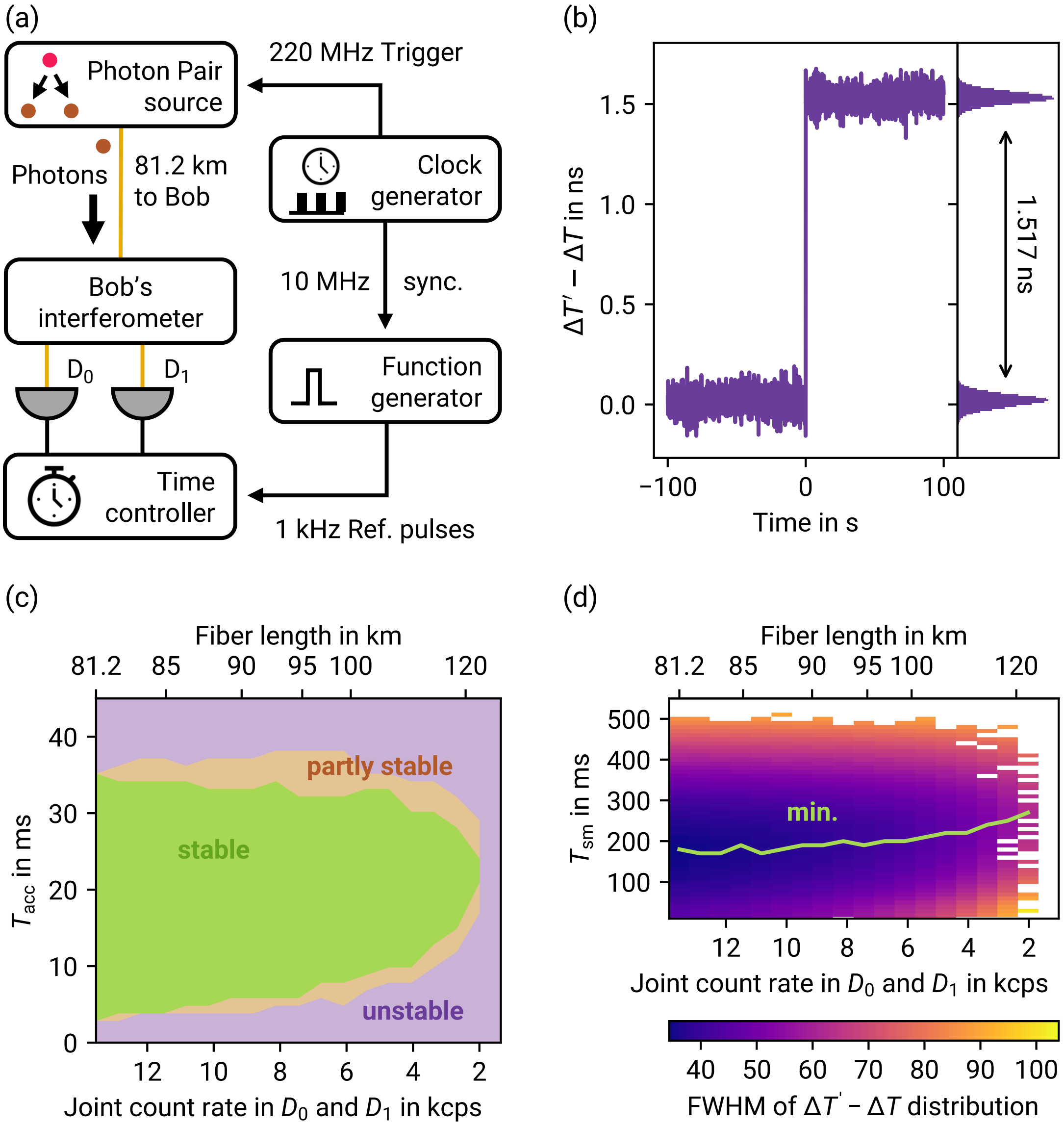


Figure 2.30: Performance of the clock recovery (CR) algorithm, measured with Bob's receiver over one hour with the standard settings (cf. table 3.1). (a) Setup for the CR performance evaluation. Bob is connected via 81.2 km of optical fiber. (b) Deviation $\Delta T' - \Delta T$ around a time when the CR failed. The CR slips by one time bin separation of $(3f_{\mathrm{rep}})^{-1} = 1.517$ ns. (c) Stability of the clock recovery as a function of the count rate or distance and of T_{acc} with fixed T_{sm} = 200 ms. (d) FWHM of the distribution $\Delta T' - \Delta T$ quantifying the precision of the CR, for fixed T_{acc} = 25 ms. In the colorless area, the clock recovery failed. The line "min." indicates for which T_{sm} the minimum FWHM for a given count rate was reached.

at the beginning of each QKD session. During the measurements presented in fig. 9 of publication [II], the automatic resynchronization was triggered a few times. The stability of the algorithm was then improved, and the performance results shown in fig. 2.30 (c) were obtained with the improved algorithm fig. 2.30.

If the CR algorithm does not slip, the distribution of $\Delta T' - \Delta T$ will show a single peak around $t = 0$. The second parameter ΔT_{sm} mainly determines the width of the distribution of $\Delta T' - \Delta T$. The FWHM of the peak characterizes the precision of the estimate $\Delta T'(t)$ obtained from the algorithm. Figure 2.30 (d) shows the FWHM of the peak as a function of the parameter T_{sm}. For each count rate, the minimum of the FWHM over T_{sm} is reached for values of T_{sm} between 170 and 270 ms. When the best value of T_{sm} is chosen for each rate, as indicated by the green line in fig. 2.30 (d), FWHMs between 61.7 ps for the lowest count rate and 34.3 ps for the highest count rate are obtained. These values show that the estimate $\Delta T'$ is very accurate. It is less than a factor of five worse than the resolution of the TCs of 13 ps and a factor of 16 smaller than the time bin width of 1 ns. This means that the broadening of the photon detection histograms in the time bins due to the limited accuracy of the synchronization by CR can be neglected.

Clock Offset Correction Based on the Arrival Time Cross-Correlation

To compensate for constant delays in their timestamps lists after clock recovery, Alice and Bob determine $\Delta T_{\mathrm{BA}} = \Delta t_0(\mathrm{Bob}) - \Delta t_0(\mathrm{Alice})$ and Bob subtracts it from his timestamps. They obtain the time difference ΔT_{BA} by computing the cross-correlation between their corrected timestamps $t_i - \Delta T'(t_i)$ for a fraction of the first run of a QKD session. The calculation of ΔT_{BA} requires that Alice sends her corrected timestamps to Bob so that he can compute the cross-correlation with his timestamps. The timestamps sent by Alice are then possibly known to Eve and can not be used to generate key bits anymore. However, in general, the first few runs of a QKD session cannot be used to generate key bits anyway because the IF phases still need to be aligned. Therefore, calculating ΔT_{BA} does not reduce the number of usable key bits.

An essential advantage of this synchronization scheme compared to schemes evaluating the cross-correlations continuously, such as in refs. [155, 156], is that the cross-correlation is only evaluated during the initial phase and the value ΔT_{BA} is reused in subsequent runs. Other algorithms achieving synchronization based on the arrival time of entangled photon pairs by evaluating the cross-correlation continuously often require that a fraction of the timestamps is sacrificed to calculate the cross-correlation. However, for some QKD protocols, continuously tracking the cross-correlation can also be realized without sacrificing quantum bits [162].

Summary of Chapter 2

A *quantum key hub* (q-hub) consisting of a photon pair source and a wavelength-division demultiplexer was developed, enabling simultaneous QKD between multiple pairs of users in a star-shaped network without a trusted node. The photon pair source generates time-bin entangled photon pairs for QKD based on the Bennett-Brassard-Mermin 1992 (BBM92) protocol and was built to be modular and portable in anticipation of field testing the system. Details about the photon pair source will be published in ref. [VIII], and details about measurements of the photon spectra have been published in ref. [I].

Four receivers were built to demonstrate simultaneous pairwise QKD with four users *Alice*, *Bob*, *Charlie*, and *Diana* via the q-hub. Calculations showed that the receiver interferometers must be manufactured with an accuracy of the optical path differences of a few micrometers to keep the quantum bit error rate in the phase basis low. A patent for a method to build fiber-based interferometers quickly and simply with the required accuracy is pending.

A synchronization method based on clock recovery from the arrival times of the photons was developed to synchronize the receiver clocks. The method only requires data processing and no additional hardware. It enables a stable synchronization for distances up to 120 km with an accuracy better than 100 ps for all tested fiber distances. A patent for the clock recovery method is pending.

The whole q-hub QKD network is presented in ref. [II].

3 Field Test of the Multi-User QKD System

One of the most important goals of the research presented in this thesis was to demonstrate QKD with the q-hub network at a facility of *Deutsche Telekom* in Darmstadt over a fiber link deployed underground. The field test of the system was the first demonstration of a multi-user QKD network using the time bin BBM92 protocol. Alice is connected via the deployed fiber link, and the other users are connected via spooled fibers. The goals of the field test were to show that the hardware of the q-hub network is robust enough to be operated in a typical telecom environment and to demonstrate the flexibility of the network.

Results of QKD experiments at the Technical University of Darmstadt and first results of the field test have been published in ref. [II]. Multiple further field test experiments demonstrating the flexibility of the q-hub network have been published in ref. [V]. Most of the results presented in this section were obtained during the master's thesis of Till Dolejsky [M6], and some were obtained during the master's thesis of Lucas Bialowons [M5].

In section 3.1, the 27 km long deployed fiber link is characterized and the default settings of the q-hub network for the field test are described. The PPS and the receivers are all located in the same room. The optimal parameters for the dead times and efficiencies of the detector and the optimal pump power are determined.

In section 3.2, the most important results of the field test are presented, and the versatility of the q-hub QKD network is demonstrated in various experiments. The operation of the system with twofold and fourfold time bin interlacing is demonstrated. The stability of the system is proven in a long-term QKD session over more than three days and for fiber length up to 108 km between two users. The scalability of the number of QKD users is tested with three different WDMs. Furthermore, QKD is demonstrated between all combinations of users, with dynamic switching of the user configurations, in sub-networks, and in a fully-connected network. Finally, a modified setup of the PPS is tested using the same nonlinear wavelength converter for SHG and SPDC.

3.1 Field Test Preparations

Characterization of the Deployed Fiber Link

For the field test, the four receivers and the q-hub were set up at the facility of *Deutsche Telekom* in the Heinrich-Hertz-Straße 3-7 building in Darmstadt. For the field test, *Deutsche Telekom* granted access to two fibers deployed underground between Darmstadt and the nearby village of Griesheim. The fibers are *dark fibers*, which means that *Deutsche Telekom* does not send any other light signals through these fibers during the field test. In Griesheim, the two fibers are connected to form a loop starting and ending in Darmstadt. This fiber loop was already used for the field test of the QKD system for two users during Nikiforov's Ph.D. [28]. Figure 3.1 shows the approximate path of the fiber link. The total link length measured by using a *optical time-domain reflectometer* (OTDR)[1] is 26.8 km, and the overall attenuation introduced by the link is 6.8 dB, corresponding to an average loss of 0.25 dB/km. While the attenuation for SMF is typically below 0.22 dB/km (cf. table 1.1), for deployed fiber cables up to 0.3 dB/km are allowed between 1530 to 1565 nm according to the ITU-T specification G.652.D [70]. Therefore, the attenuation coefficient of the field test link can be considered as typical for such a link.

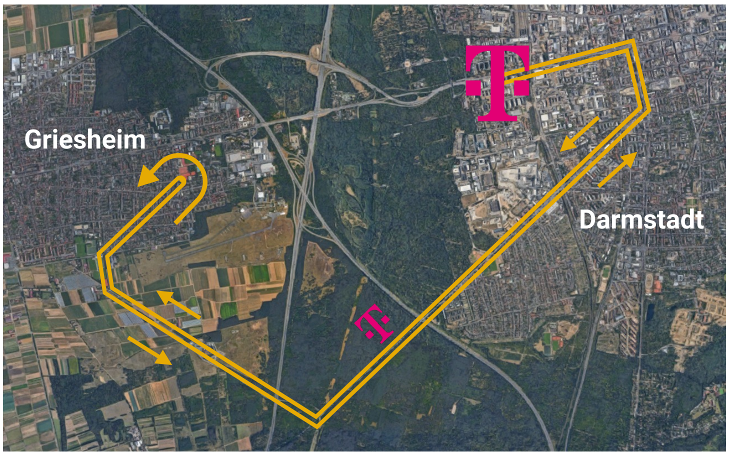


Figure 3.1: Approximate route of the deployed dark fibers between Darmstadt and Griesheim before July 12, 2022 (Map source: Google Maps 2023). The total length of the link is 26.8 km, introducing an attenuation of 6.8 dB. In July 2022, the link was rerouted in the city of Darmstadt to allow for service work required by *Deutsche Telekom*. After the rerouting, the link length is 27.3 km and the attenuation is 7.0 dB.

[1] OTDR device: FTB-7400E from *EXFO*.

Default Configuration of the Q-Hub Network

The default configuration of the q-hub network for the field test is shown in fig. 3.2. The q-hub and all receivers are set up at the *Deutsche Telekom* facility in Darmstadt. Alice is connected via the deployed fiber link, and the other receivers are connected via fiber spools. The default settings of the q-hub and the receives are tabulated in tables 3.1 and 3.2. By default, the WSS is used as WDM, the channel width is set to 50 GHz, and the channels are configured for the connections Alice-Bob and Charlie-Diana. Clock recovery is used to synchronize the receivers.

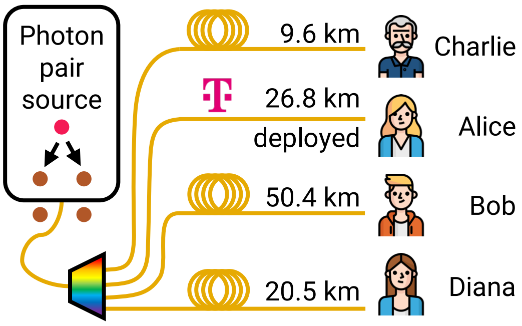


Figure 3.2: Default setup for the field test. The q-hub, receivers, and fiber spools for Bob, Charlie and Diana are located at the facility of *Deutsche Telekom* in Darmstadt.

Q-Hub Settings	
Interferometer name	Theta
IF temperature reading	29.65 °C
WSS channel width	50 GHz
Average SHG power	60 μW
Pulse repetition frequency	220 MHz

Table 3.1: Default configuration of the q-hub during the field test. The source is, by default, operated with twofold pulse interlacing at a repetition frequency of 220 MHz. The default WDM is the WSS with 50 GHz wide channels.

Table 3.2: Default configuration of the receivers for the field test. The detector connected to the third port of the circulator is D_0, and the detector connected to the beam splitter is D_1 (cf. fig. 2.27 (a)). The fiber to Alice is the deployed field test link (cf. fig. 3.1). The fiber lengths and attenuation values were measured by OTDR. The temperature references are uncalibrated because only temperature differences are relevant for the phase adjustments. The readings of the TCUs may deviate up to a few kelvins from the actual temperatures of the IFs.

TCU	IF temp. reading	Receiver name	WSS port	Channel center freq.	D_0 SPD	D_1 SPD	Fiber length	Link loss
Alice	30.00 °C	Kappa	5	193.325 THz	7	6	26.8 km	−6.8 dB
Bob	31.64 °C	Zeta	2	193.375 THz	8	1	50.4 km	−15.7 dB
Charlie	39.50 °C	Eta	4	193.250 THz	3	2	9.6 km	−1.9 dB
Diana	35.76 °C	Iota	7	193.550 THz	5	4	20.5 km	−3.9 dB

Choice of the Detector Efficiency and Dead Time

The SPDs have a variable dead time and efficiency. The dead time can be set in the range from 1 to 25 µs and the efficiency can be set to 10, 15, or 20 %. In general, the higher the efficiency and the shorter the dead time, the higher the achievable key rate. However, these settings come with a trade-off: Higher efficiencies lead to a higher afterpulse probability and a higher dark count rate for the same dead time setting. The resulting unwanted noise can be reduced by choosing higher values for the dead time. However, a long dead time can significantly reduce the achievable key rate because it leads to a high probability that the detector is deactivated when the next photon arrives. A detailed characterization of these detector effects is presented in section 5.2. To choose suitable parameters for the field test, QKD sessions were recorded for different combinations of the dead time and efficiency. For the first measurement, Alice and Bob were directly connected to the source, and for the second one, they were connected via the default fiber links. The measured sifted key rates, the QBER$_t$, and the resulting secure key rates calculated by using eq. (1.1) are shown in fig. 3.3. Here, the QBER$_t$ instead of the total QBER was used to calculate the

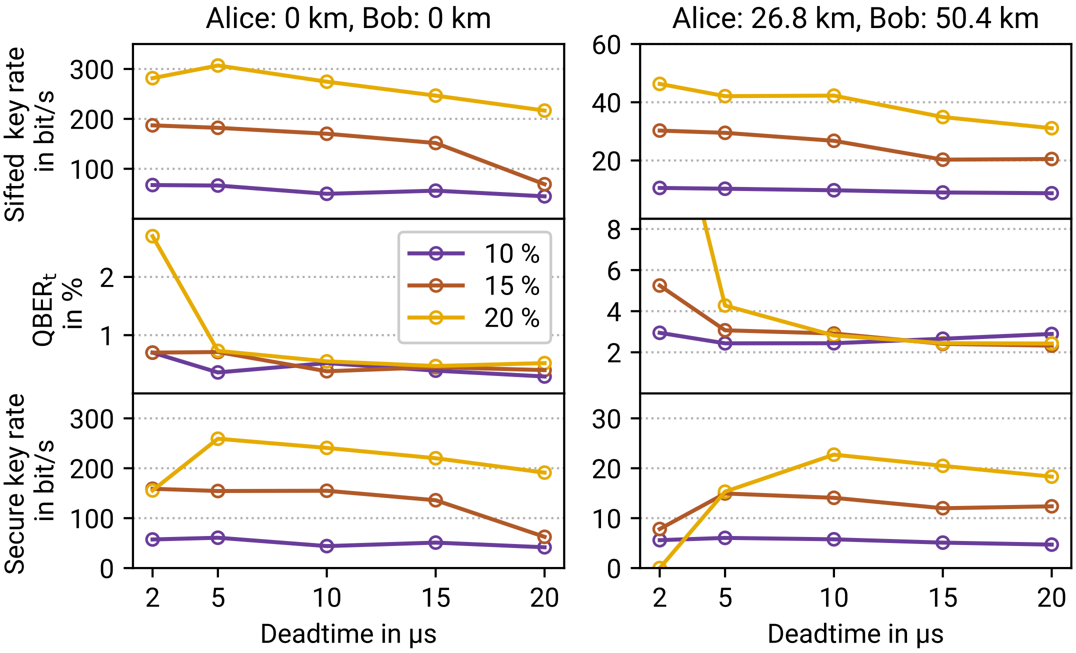


Figure 3.3: Sifted key rates, QBER$_t$ and secure key rates for different dead times and efficiency settings of 10, 15, and 20 %, measured at a source repetition frequency of 100 MHz.

secure key rate to remove the influence of the phase alignment, meaning that the QBER_t is used as an estimate for the total QBER. Due to the transmission losses, the sifted key rates measured with fiber links are significantly lower than without the links. Without the links, the maximum of the secure key rates is reached for an efficiency of 20 % and a dead time of 5 µs. With the links, the maximum is reached at 10 µs, and the secure key rate obtained for 5 µs is significantly lower. Based on these results, the settings were chosen to 10 µs dead time and 20 % efficiency for all field test measurements.

Dead Time Postselection

The dead time affects not only the count rates but also the security of the key exchange. A simple attack strategy for Eve would be to send intense light pulses between the time bins into a receiver station [163]. Thereby, Eve can switch off one of the detectors in the receiver so that she knows which detector is still active and can yield the next key bit. Such attacks are impossible when only key bits derived from pulse cycles are accepted in which all detectors are active. This postselection of key bits can easily be implemented in the data processing software. If the difference between the count time of any detector and the count generating the key bit is less than a threshold time given by the dead time of $\tau_{\mathrm{dead}} = 10\,\mu\mathrm{s}$, the key bit is discarded.

To analyze the effect of the dead time postselection, three different methods were implemented to evaluate the key bits: “None”, “All”, and “Others”. In mode “None”, no dead time postselection is applied. In mode “All”, postselection is applied to all detectors. A key bit or error bit is only kept when all detectors were active during the time span τ_{dead} before the beginning of the first time bin of the pulse cycle. Mode “Others” is similar to mode “All”, but only those detectors are considered for the postselection, which did not yield the key bit or error bit. The idea behind this postselection mode is that a detector may have already recovered from the dead time in a time slightly shorter than τ_{dead}, such that it can register a photon yielding the key bit or error bit. The fact that the detector registered a count implies that it was active, and the key bit does not need to be discarded, although the time difference to the previous count of this detector is less than the specified value of τ_{dead}.

Choice of the SHG Pump Power

An important parameter allowing the optimization of the secure key rate is the SHG pump power. Figure 3.4 shows the sifted key rate and QBER of Alice and Bob as well as the resulting secure key rate for 50 GHz wide AWG channels as a function of the average pump power for the different dead time postselection methods. The secure key rate shows a relatively flat maximum around 40 to 70 µW. As the slope towards higher pump powers is shallower than towards lower pump powers, the value of 60 µW was chosen as the default

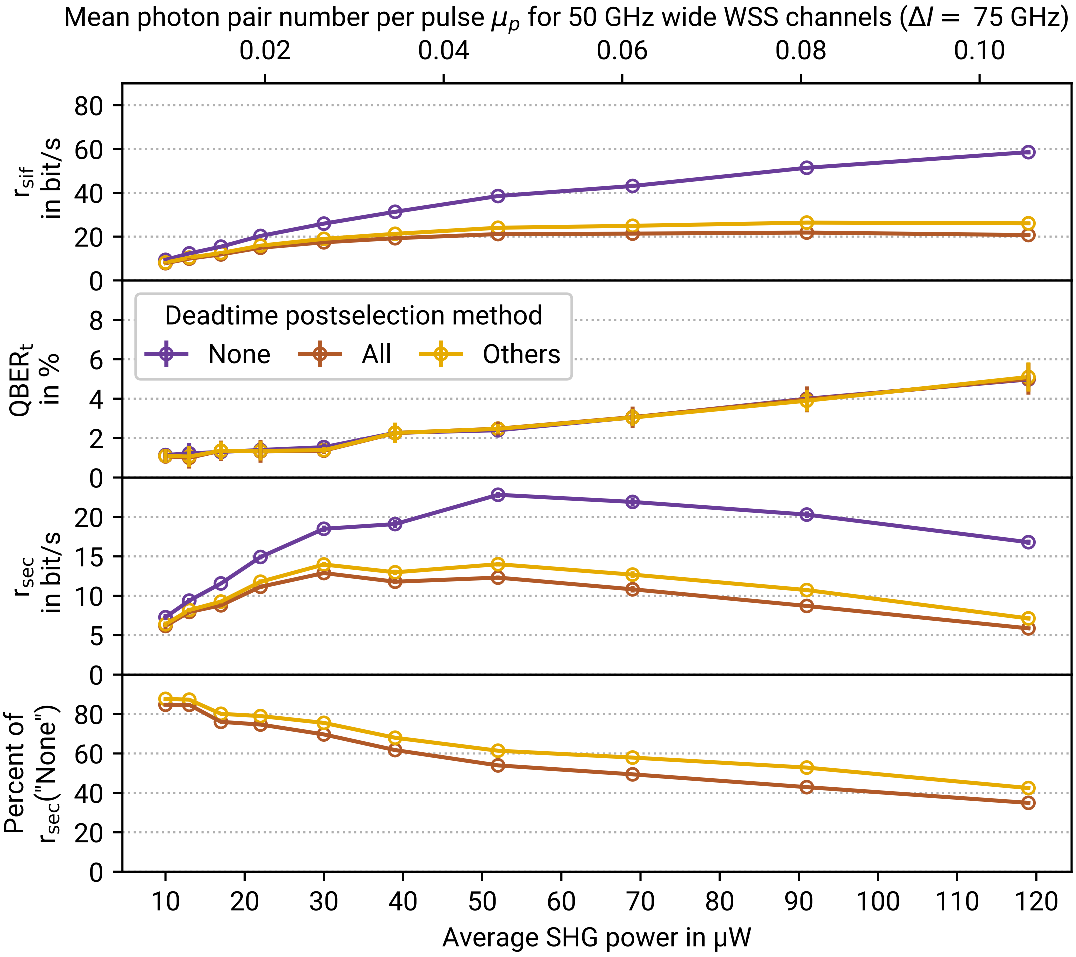


Figure 3.4: Sifted key rates r_{sif}, QBER$_{\mathrm{t}}$, and secure key rate r_{sec} of Alice and Bob as a function of the average SHG pump power for the default field test setup (cf. tables 3.1 and 3.2). The upper horizontal axis shows the corresponding mean photon number per pulse μ_{p}. The data are evaluated using three different methods: without considering the dead times (”None”), checking if the time since the last count is longer than the dead time of 10 μs for all detectors (”All”), and checking this condition only for the other detectors that have not registered a photon in the pulse cycle yielding the key bit or error bit (”Others”). The lowermost plot shows the ratios r_{sec}(”All”)/r_{sec}(”None”) and r_{sec}(”Others”)/r_{sec}(”None”).

value for the field test. At this SHG power, the mean photon pair number over a frequency interval $\varDelta I = 75\,\text{GHz}$ for 50 GHz wide WSS channels (cf. table 2.2) is $\mu_\text{p} = 0.053$. The dead time postselection reduces the sifted and secure key rates significantly. For pump powers around 60 µW, the remaining fraction of key bits is about 60 % when only the postselection for other detectors is applied, and it is even lower when the postselection is applied to all detectors.

For the results presented in the next section, the dead time postselection is not applied to keep the comparability to the results published in ref. [II], which were obtained before the dead time postselection was implemented. The simulation results in chapter 7 are compared to measured results with dead time postselection applied to all detectors.

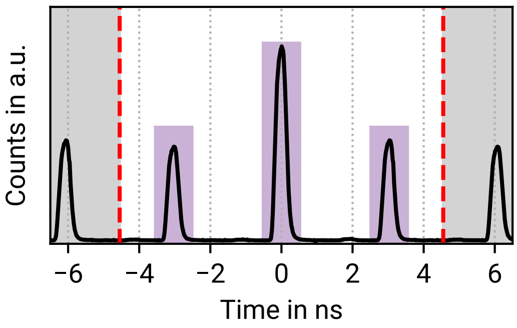
3.2 Field Test Results

Repetition Cycle Interlacing

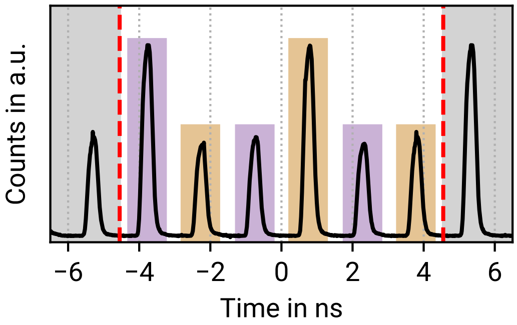
The IF delay of about 3 ns (cf. eq. (2.22)) was chosen such that the leakage of photons into adjacent time bins due to chromatic dispersion is avoided, even when the relatively broad type-II photons and long transmission links are used (cf. section 2.3.2). When type-0 photons are demultiplexed into 50 GHz wide channels or when the transmission links are relatively short, the peaks in the photon arrival time histogram are relatively narrow. Due to the comparatively long IF delay, no photons are registered in long time intervals between the peaks. These time intervals can be used by interlacing repetition cycles, enabling a more efficient key transmission. This concept of repetition cycle interlacing was introduced by Nikiforov during his Ph.D. [28]. By setting up the electronic pulse generator to create sequences of two electrical pulses with a time difference equal to half the IF delay, Nikiforov interlaced the three time bins with a second triplet of arrival time peaks and time bins. A similar interlacing of two repetition cycles can be achieved by doubling the pulse repetition frequency [M5]. Compared to Nikiforov's method, the time shift between the two interlaced time bin triplets is not half of the IF delay but one and a half delays. An advantage of this method is that it does not require electrical double-pulses and can be implemented with any pulse generator capable of generating pulses at twice the repetition frequency. By setting the repetition frequency to 2^N times the fundamental repetition frequency, 2^N time bin triplets can be interlaced.

Table 3.3 shows the photon arrival histograms without interlacing, with twofold, and with fourfold interlacing. For the fourfold interlacing, the pump pulse duration was shortened from 300 to 160 ps and the time bin width was reduced from 1 to 0.5 ns. The CR parameters T_acc and T_sm were optimized for each interlacing level. With fourfold interlacing, stable CR was possible for fiber lengths up to around 50 km. For single- and double interlacing, the

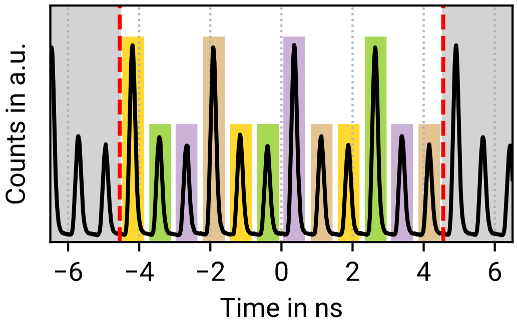
Table 3.3: Overview over the pump pulse interlacing measurements. The setup is operated in the default configuration, with an average SHG power of 60 µW and with 50 GHz wide WSS channels. The histograms show Charlie's photon arrival time distribution. The maximal stable fiber distance is the fiber length between the source and a receiver for which the clock recovery (CR) works stably.



Single/No interlacing	
Repetition frequency	110 MHz
Pulse duration	300 ps
Time bin width	1 ns
CR parameter T_{acc}	45 ms
CR parameter T_{sm}	350 ms
Max. stable fiber distance	$\approx$ 100 km
QBER$_{\mathrm{t}}$ for Charlie-Diana	4.9(3) %



Twofold interlacing	
Repetition frequency	220 MHz
Pulse duration	300 ps
Time bin width	1 ns
CR parameter T_{acc}	25 ms
CR parameter T_{sm}	200 ms
Max. stable fiber distance	$\approx$ 100 km
QBER$_{\mathrm{t}}$ for Charlie-Diana	2.6(2) %



Fourfold interlacing	
Repetition frequency	440 MHz
Pulse duration	160 ps
Time bin width	0.5 ns
CR parameter T_{acc}	15 ms
CR parameter T_{sm}	200 ms
Max. stable fiber distance	$\approx$ 50 km
QBER$_{\mathrm{t}}$ for Charlie-Diana	1.3(1) %

CR was stable for fiber lengths of up to approximately 100 km because the larger time bin separation helps to avoid slips by one time bin (cf. fig. 2.30 (b)).

When the average pump power is doubled, and twofold interlacing is used, the sifted key rate increases and the QBER remains approximately constant because the contribution of multi-photon-pair emission to the QBER is unchanged. Conversely, if the pump power is not changed, the sifted key rate will be approximately the same, and the lower mean photon pair number per pulse μ_p results in a lower QBER. To demonstrate both effects, two measurement series were set up. For the first series, the system was operated in the default configuration with 60 µW average SHG power and with three different interlacing levels. For the second series, the SHG power was scaled proportionally to the interlacing level. The QBERs obtained from the first series are given in table 3.3. Each interlacing level reduces the QBER_t approximately by a factor of two, which shows that multi-photon-pair emission significantly contributes to the QBER.

The results of the second measurement series are shown in fig. 3.5. The QBER is approximately constant, but the key rate increases with the interlacing level. However, the sifted key rate and the secure key rate do not scale proportionally with the SHG pump power and interlacing level because with an increase of the count rate, the probability that the detector is in the dead time when the next photon arrives scales up as well. Therefore, when the fourfold pump power and fourfold nesting are used, the key rate is only approximately twice as high as the key rate obtained without interlacing.

Long-Range and Long-Term QKD

An important performance indicator for QKD systems is the maximum distance over which quantum keys can be distributed. Figure 3.6 shows a long-term measurement, demonstrating the continuous, stable operation of the system over more than three days, with a total fiber link length of 108 km between Alice and Bob. Alice was connected via the

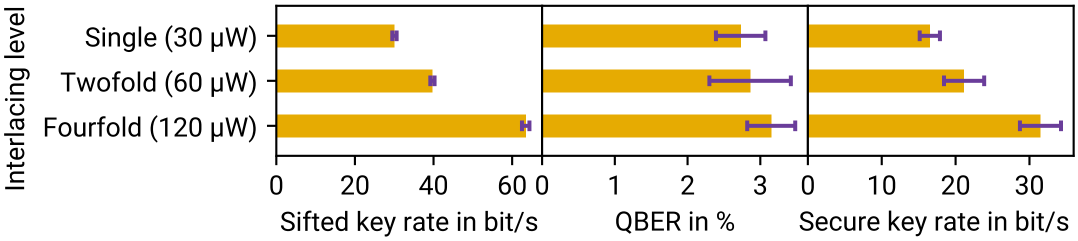
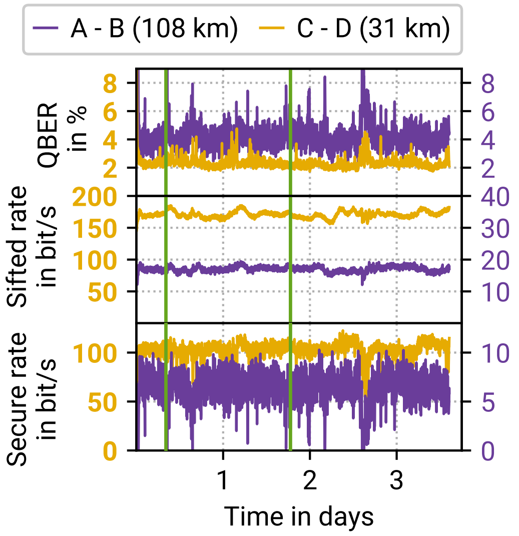


Figure 3.5: QKD performance between Alice and Bob in default configuration with different pump pulse interlacing levels. The average SHG power was set to 30, 60, and 120 µW for single, twofold, and fourfold interlacing.



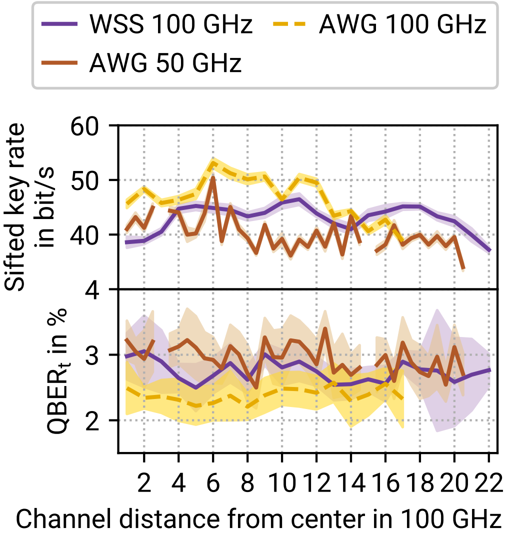


Figure 3.6: Long-term QKD demonstration with Bob connected via a 81.2 km long fiber. The average SHG power was 90 µW, and Charlie's and Diana's WDM channel widths were reduced to 25 GHz. The data link connection to the TCs was lost twice for a short time (green intervals), and the connection was automatically re-established.

Figure 3.7: QKD performance for different channel pairs. Bob and Charlie were connected via 50 and 10.5 km to test the 100 GHz AWG. The 50 GHz AWG and the WSS were tested with Alice and Bob in the default configuration. The gaps at 300 and 1500 GHz in the curve for the 50 GHz AWG are due to defective fiber connectors.

deployed fiber, and Bob was connected via 81 km of spooled fiber. Charlie and Diana were connected via their standard fiber links. The average SHG power was set to 90 µW, and the WSS channel width was set to 50 GHz for Alice and Bob to facilitate the clock recovery. For Charlie and Diana, the channel width was reduced to 25 GHz, resulting in a lower value of μ_p, avoiding unnecessarily high QBERs due to multi-photon-pair emission. After the initial phase-alignment, taking roughly 40 min, average secure key rates of 6(2) bit/s and 4.3(26) % QBER were measured between Alice and Bob and 102(11) bit/s and 2.4(5) % QBER were measured between Charlie and Diana.

For the two-user system, the measurement time was limited to approximately 5 hours due to frequent interruptions of the data transfer from the TCs to the computer [28]. To achieve a more stable operation, the data communication between the computer and the TCs was revised, enabling the operation of the q-hub network over more than three days. However, the stability of these connections still needs improvement. The software operating the setup was implemented such that connections are automatically reestablished when they are lost during a QKD session. During the long-term QKD session, the connection was lost twice for a few runs.

Scalability of the Number of Users in the Q-Hub Network

From fig. 2.14, it is expected that the bandwidth of the photon pairs that can be used to distribute quantum keys is limited by the WDMs. To demonstrate that the type-0 photon pair spectrum is broad enough such that the entire wavelength range of the WDM can be used, quantum keys were distributed with the three available WDMs for several different wavelength channel pairs. The QKD results are shown in fig. 3.7. The key rates and QBERs obtained with all WDMs vary slightly from channel to channel, but the whole bandwidth of the WDMs can be used for QKD. This means that, if sufficiently many receiver modules were available, up to 34 users could be readily connected to the q-hub via the 100 GHz AWG, and 78 users could be connected via the 50 GHz AWG.

One of the major advantages of the q-hub network over fixed point-to-point connections between the users is the possibility to reconfigure the combinations of users to which keys are distributed. For the q-hub network, it is important to show that the OPD of all receivers are matched so precisely that all combinations of users can exchange quantum keys. Figure 3.8 shows the QKD performance for three measurements with different user pairings, using the 100 GHz AWG as WDM. The QBERs are similar for all combinations, indicating that all OPDs are well-matched. The key rates of different pairs differ due to the individual link lengths.

The channel assignment of the AWGs is fixed, and manual reconfiguration is required to change the user pairing in the network. For practical applications, a reconfigurable WDM allowing the remote reconfiguration of the network based on the key demands would be more desirable. One option to realize such a network would be to use an optical switch after the AWG, enabling the routing of any AWG output channel to any fiber link. Switches with port counts up to 576 outputs are commercially available [164].

Another option to realize reconfigurable QKD networks with the q-hub is to use a WSS as WDM. Compared to the available AWGs, the tested WSS has a lower insertion loss. It allows to freely choose the frequency channel center frequencies and to set channels with a width as narrow as 6.25 GHz. QKD results for a measurement demonstrating dynamic network reconfiguration with the WSS are shown in fig. 3.9. QKD sessions with different user pairings are automatically executed in a sequence, with the WSS switching the configurations every 6 hours. After switching, the phases are automatically optimized by the alignment algorithm to minimize the QBERs of the new configuration. The alignment typically takes less than 40 min and is completed faster when the phases are well pre-

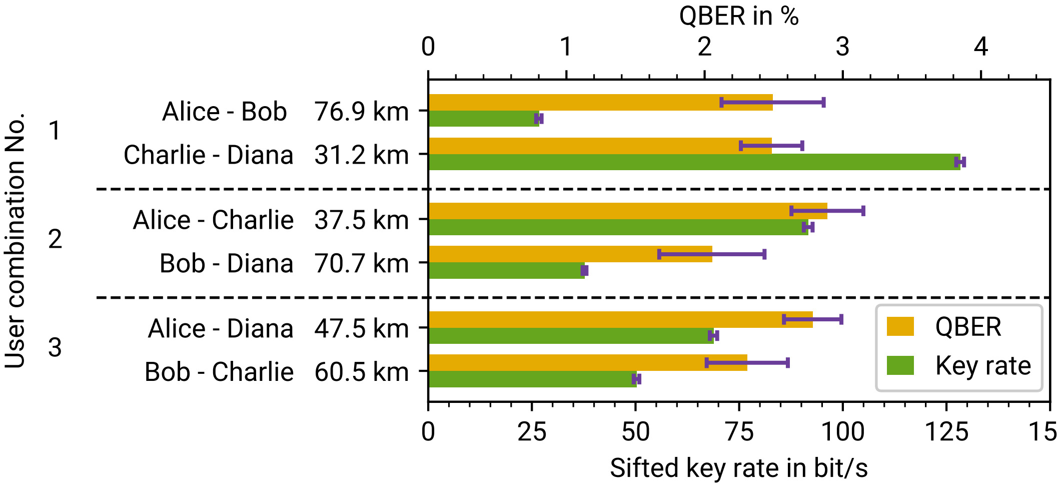


Figure 3.8: QKD performance for different combinations of users obtained with the 100 GHz AWG. Data were obtained over 20 runs, each taking 90 seconds. The standard deviation over the 20 runs is represented by error bars. The SHG power was set to 30 μW. The data were acquired before the field test, and all users were connected via fiber spools with lengths slightly different from the default configuration: Alice – 26.8 km, Bob – 50.0 km, Charlie – 10.5 km, Diana – 20.6 km.

aligned. After the initial alignment, the algorithm stabilizes the QBERs at low values until the user combinations are switched again.

The available WSS has only nine outputs, so four pairs of users can be connected at most. An option to significantly extend the number of network users with WSSs is to set up a cascade of two or more WSS layers, such that the photon pair spectrum is demultiplexed to channel groups by a first WSS and is further demultiplexed into individual channels by one WSS per channel group. WSSs with up to 35 ports are commercially available [165], enabling a network with $35^2 = 1225$ users with two WSS layers. If the frequency ranges and channel widths of these WSSs are the same as for the WSS used in the field test, a bandwidth of 4.5 THz of the photon pair spectrum can be used, corresponding to 720 users.

An important advantage of using a WSS in the first layer of such a network is that it allows combining arbitrary frequency channels into a single fiber to a sub-network. The WSSs of the second layer can be placed far apart from the q-hub, realizing local centers of sub-networks, where the channel groups are then demultiplexed into individual channels. The whole sub-network could then be connected to the q-hub via a single fiber. The concept is shown in fig. 3.10.

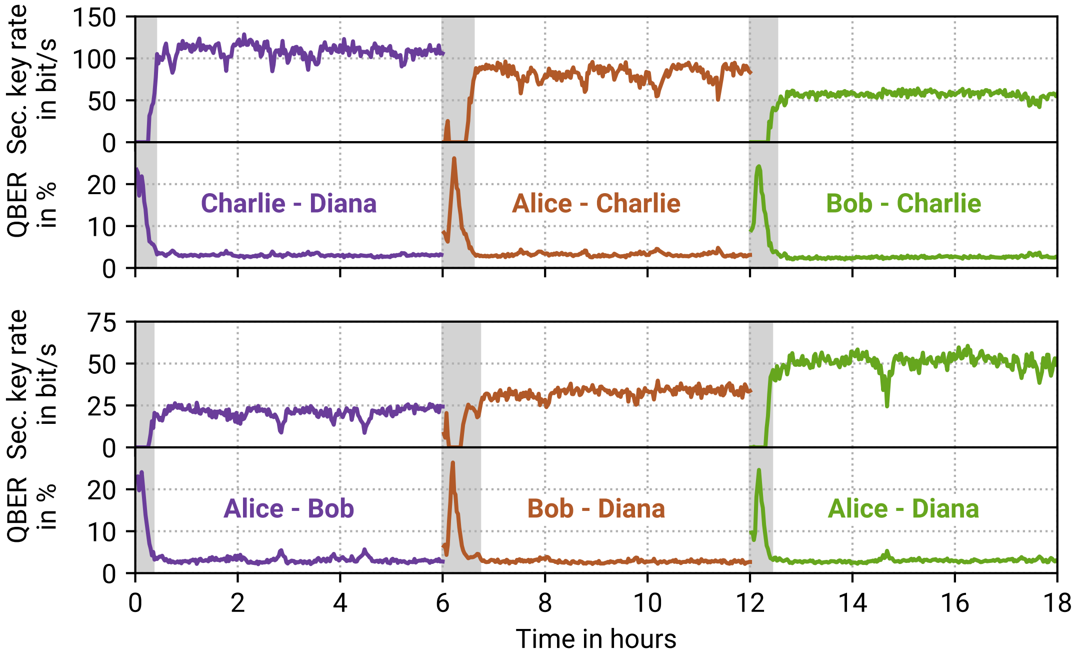


Figure 3.9: Dynamic q-hub network with automatic switching of the user combinations by reconfiguring the WSS every six hours. The gray intervals indicate the time required for the phase realignments after a channel reconfiguration.

Only a single WSS was available at the time of the field test, so a q-hub network with two WSS layers could not be realized. Therefore, the WSS and two *dense wavelength-division multiplexing* (DWDM) filters were used to demonstrate a network with cascaded demultiplexing. The demultiplexing scheme is shown in fig. 3.11. Each DWDM filter transmits light in a 200 GHz wide pass band into its first output and reflects the rest of the spectrum into its second output. The WSS is configured such that each DWDM receives two 100 GHz wide frequency channels. One channel is transmitted into the first output because it is centered in the passband, and the other is reflected in the second output. A two-hour QKD session with an average SHG power of 30 µW was set up. A secure key rate of 17(5) bit/s was measured for Alice and Bob, and 14(2) bit/s were measured for Charlie and Diana. The difference in the key rate is due to losses at Diana's fiber connector.

Fully-Connected Q-Hub Network

The approaches to realize QKD networks with the q-hub discussed so far use wavelength demultiplexing to distribute photon pairs to multiple users. Another option is to use

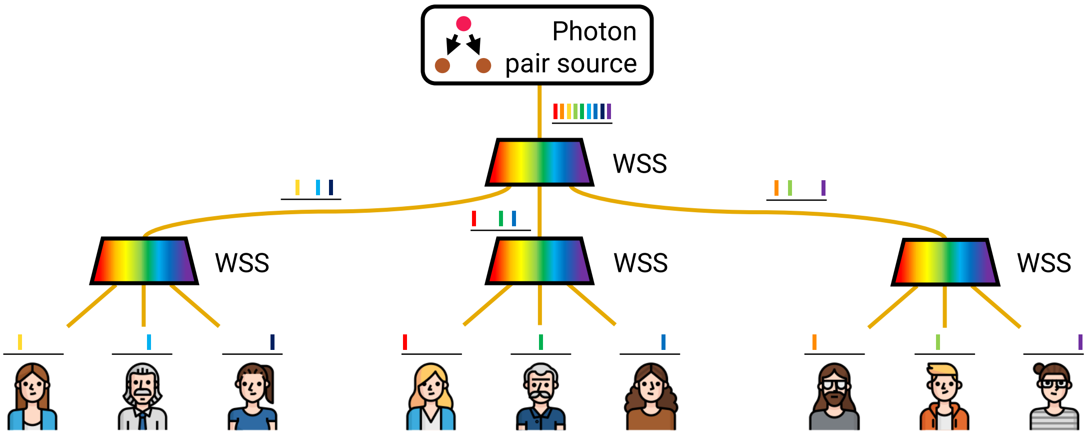


Figure 3.10: Concept of a q-hub QKD network with two WSS layers and local sub-networks. The WSS in the first layer splits the photon pair spectrum into channel groups. The WSSs in the second layer separate the channel groups into individual channels.

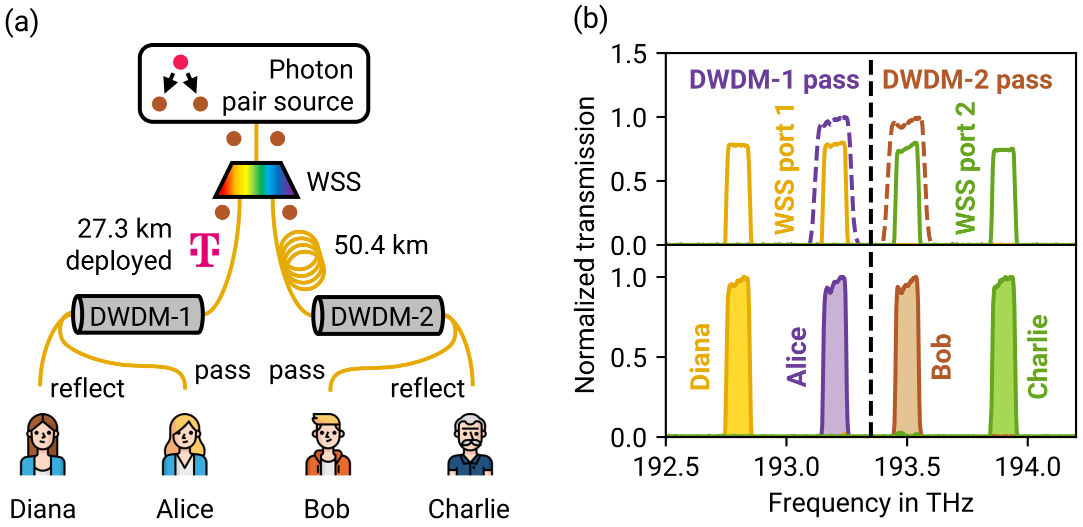


Figure 3.11: QKD experiment with two sub-networks. (a) Setup of the WDM network. The first layer is implemented using the WSS, and the second layer uses DWDM filters. The deployed fiber and the DWDM-1 are connected to port 1. A 50.4 km long spooled fiber and the DWDM-2 are connected to port 2. (b) Transmission spectra of the channels. Top: The WSS guides two 100 GHz wide channels below the center frequency (dashed line) to port 1 and two channels above the center frequency to port 2. The passbands of the DWDMs are 200 GHz wide and are centered over the inner WSS channels. Bottom: channels transmitted to the users.

time-division demultiplexing or probabilistic demultiplexing. Time-division demultiplexing can be realized, for example, by periodically switching to which users the photons are sent [112]. Random splitting of the photon pairs can be used to distribute the photons without requiring WDMs. Such a probabilistic distribution scheme has recently been used in combination with WDMs to realize a fully-connected QKD-network with 40 users [118].

One option to realize a fully-connected four-user QKD network would be to replace the WDM with a $1 \times 2N$ beam splitter. In this configuration, the whole photon pair spectrum would be used for QKD. The value of μ_p needs to be set so that the probability that more than one photon pair is produced in any channel pair is much less than one to keep the QBER low. Therefore, compared to the configuration with N separated user pairs, the overall photon pair generation rate is a factor of N lower. A disadvantage of the probabilistic splitting is that with probability $1/(2N)$ both photons are guided to the same user, such that these pairs cannot be used to generate key bits.

Fully-connected networks can also be set up by sending multiple wavelength channels to each user [26, 111, 118]. To realize such a fully-connected network with the four receivers, the WSS was configured such that each user receives three frequency channels as shown in fig. 3.12 (a). Each possible user combination is represented by a dedicated channel pair. In the fully-connected network, all users compare their detection times. When two users register counts in the same repetition cycle, they evaluate the key bit. When more than two users register counts in the same cycle, the counts are discarded.

Simultaneous QKD between all user combinations requires that the phases of all IFs are aligned according to eq. (1.2), fulfilling a set of equations simultaneously:

$$\phi_\mathrm{x} + \phi_\mathrm{y} - \phi_\mathrm{P} = 2n_\mathrm{x,y}\pi \quad \text{for} \quad (x, y) \in \{(\mathrm{A, B}), (\mathrm{A, C}), (\mathrm{A, D}), (\mathrm{B, C}), (\mathrm{B, D}), (\mathrm{C, D})\}. \tag{3.1}$$

The phase alignment is more complex than for simultaneous pairwise QKD because all IF phases are coupled via the source IF. Therefore, the phase adjustment algorithm would need to estimate the misalignment of the individual IFs from the observed QBERs in all user combinations to correct the misalignment of the individual IFs. This is challenging because the phases of different IFs can be stable, or they can drift by different amounts in the same or opposite directions. Furthermore, the number of error bits is typically low, such that the QBER is only approximately known due to the statistical uncertainty. As the QBER does not provide information about the direction of the phase misalignment, the realignment during a QKD session becomes challenging.

For a proof-of-principle demonstration of a fully-connected network, the phases are aligned before the QKD session starts, and the automatic phase realignment is turned off. The initial alignment is obtained in a three-step method developed by Lucas Bialowons [M5]:

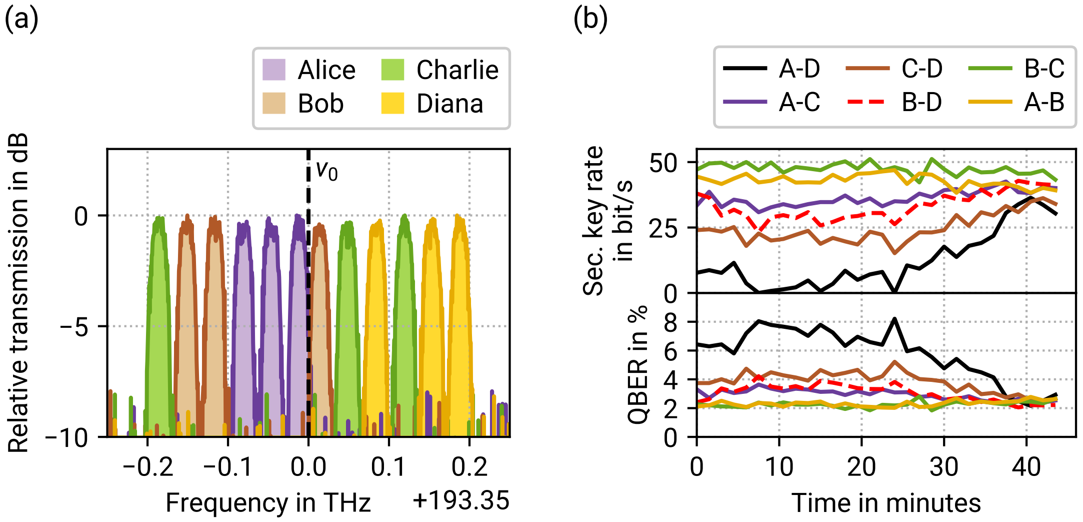


Figure 3.12: Demonstration of QKD in a fully-connected network with four users. (a) Configuration of the 25 GHz wide WSS channels. Different colors indicate the frequency channels sent to different users. Each user is connected via 5.4 km of optical fiber to the q-hub. (b) QKD results with 10 µW SHG power and twofold pulse interlacing. The IF temperatures were not actively changed after the initial phase alignment phase (not shown).

1. The QBER_p between Alice and Bob and the QBER_p between Alice and Charlie are minimized by tuning Bob's and Charlie's IFs. After this step, $\phi_\text{B} - \phi_\text{C} = 2z_\text{BC}\pi$ with $z_\text{BC} \in \mathbb{Z}$.

2. The QBER_p between Bob and Charlie is minimized by tuning the source IF. After this step, $\phi_\text{P} = 2z_\text{P}\pi$ with $z_\text{P} \in \mathbb{Z}$.

3. The QBER_p between Alice and Bob, as well as between Charlie and Diana, are minimized by tuning Alice's and Diana's IFs. After his step, $\phi_\text{A} - \phi_\text{B} = 2z_\text{AB}\pi$, $z_\text{AB} \in \mathbb{Z}$ and $\phi_\text{C} - \phi_\text{D} = 2z_\text{CD}\pi$, $z_\text{CD} \in \mathbb{Z}$.

The second step does not change the condition after the first step, and the third step does not change the condition of the phase of the pump IF from the second step. The second step leaves the condition $\phi_\text{B} - \phi_\text{C} = 2n_\text{BC}\pi$ unchanged, and together with the conditions from step three, it follows that all other conditions from eq. (3.1) are fulfilled as well.

This alignment algorithm works under the assumption that all the phases that are not actively adjusted do not change. As the optimization of the QBER for one pair of users already takes up to 40 min (cf. fig. 3.9), the phases of the interferometers would need to be stable for 120 min. Due to influences from the environment, such as ambient room temperature changes, this is a challenging requirement. To speed up the initial alignment, each of the three steps was considered completed when the QBER_p was below 5 % for two consecutive runs.

After the initial alignment, the phase alignment algorithm normally used during QKD sessions was deactivated, and keys were distributed for the next 45 min. The results are shown in fig. 3.12. The secure key rates were for five out of the six combinations above zero during the whole measurement time. For Alice and Diana, it was almost always nonzero. The initial alignment of the combination Alice-Diana with a QBER around 7 % could have been more optimal and results in a low secure key rate. However, after approximately 30 min, the curves in fig. 3.12 converge towards low QBERs and higher secure key rates for all combinations. The performance of all key exchanges involving Diana improves, especially for the combination Alice-Diana. Therefore, this trend is likely caused by a drift of Diana's phase in the direction minimizing the initial misalignment. However, this has to be considered as a lucky coincidence. A method to realign the phases during the QKD session would be necessary to achieve stable QKD for all user combinations reliably.

Operation of the Photon Pair Source with a Single Wavelength Converter

The SHG and the type-0 SPDC modules of the q-hub both contain identical type-0 wavelength converters. The cost and complexity of the q-hub could be reduced if SHG and SPDC could be achieved with only one of the converters. SHG and SPDC within the same crystal have been reported in the literature, for example, for the generation of polarization-entangled photon pairs [166–169]. To realize photon pair generation with a single wavelength converter for the q-hub, the type-0 SPDC module was modified as shown in fig. 3.13. The double pulses from the pump IF enter the converter via a circulator, and the 1550 nm light behind the converter is filtered out by the coiled fiber. A 10/90 beam splitter is installed for SHG power monitoring, and a retroreflector then sends the light back into the converter. The photon pairs are generated during the backward pass of the SHG light through the converter, leave the circulator at the third port, and pass a pump light filter consisting of a cascade of two DWDM filters and two FBGs with a suppression of about 100 dB for the 1550 nm light. These filters are required to remove laser light reflected at the input of the converter or transmitted from port 1 to port 3 of the circulator.

The QKD performance of the single-converter setup was compared to the performance of the regular setup with two converters in a 20 hour long QKD session with 50 GHz wide WSS channels for Alice and Bob. Due to the insertion losses of the pump light filter, the sifted key rate with the single-converter setup is only about 63 % of the sifted key rate obtained with the regular configuration. While the QBER_t was almost identical, the QBER_p was with 4.3 % for the single-converter setup significantly higher than for the standard setup

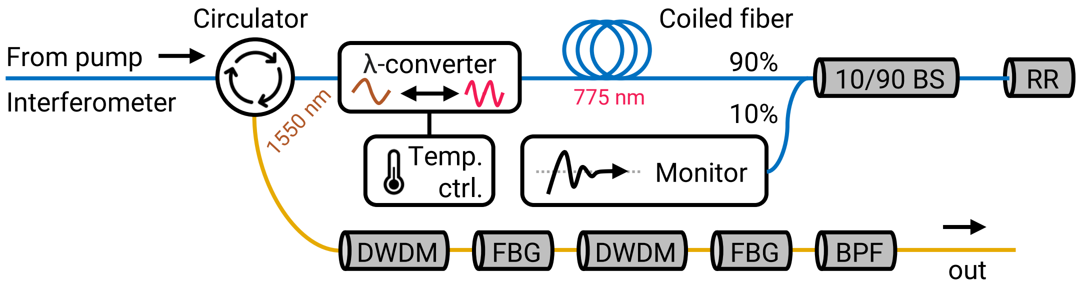


Figure 3.13: Setup of the photon pair source operated with a single wavelength converter. BS – Beam splitter, RR – Retroreflector, Temp. ctrl. – Temperature controller, FBG – Fiber Bragg grating, Monitor – Power monitoring and stabilization electronics, DWDM – DWDM-filter, BPF – C-band bandpass filter. PM fibers are shown in blue and SM fibers are shown in yellow.

with 3.0 %. The root cause for the higher QBER$_p$ is likely an increased phase instability in the pump IF. The additional circulator, the retroreflector, and the double pass through the 10/90 beam splitter introduce additional losses for the laser light and SHG light, such that a higher average power needs to be sent through the pump IF to generate a comparable μ_p. Furthermore, much larger and more frequent adjustments of the EDFA-2 pump power by the SHG power stabilization were observed. These adjustments probably result from SHG power fluctuations caused by polarization instabilities introduced by the fiber connections. The variations of the laser power passing the IF lead to variations of the power dissipated in the IF and thereby to thermal phase instabilities of the pump IF .

Two QKD experiments confirmed that the high laser power passing through the IF is the root cause of the higher QBER$_p$ in the single-converter setup. In the first experiment, the mean SHG power was reduced, and the WSS channel width was increased accordingly. In the second experiment, the same SHG power and WSS channel width were used as before, but the EDFA-2 was placed after the pump IF. In both experiments, the power passing the pump IF was significantly lower, and a lower QBER$_p$ was observed, approximately as high as the QBER$_t$. Two options exist to mitigate the problem of phase fluctuations in future experiments: The fiber connectors can be replaced by spliced connections to reduce the losses, and the order of EDFA-2 and the pump IF can be reversed to reduce the optical power in the pump IF.

Summary of Chapter 3

The successful operation of the q-hub QKD network was demonstrated in a field test at a facility of *Deutsche Telekom* in Darmstadt. The fiber link to Alice was realized by using a 27 km long fiber with an attenuation of 0.25 dB/km, which is a typical value for fibers deployed underground. This field test was the first field test of a QKD network implementing the Bennett-Brassard-Mermin 1992 (BBM92) time bin protocol with more than two users. QKD over optical fibers with a total length of 108 km between two users for more than three days was achieved. These results demonstrate the stability and reliability of the hardware, the software, and the synchronization by clock recovery.

Various operation modes, such as repetition cycle interlacing, manual and automatic switching of the user configurations, and the realization of sub-networks, were demonstrated, showcasing the versatility of the system. Quantum keys were exchanged between all possible combinations of receiver modules with similar performance, which proves the accuracy and reliability of the method to build the interferometers. Simultaneous QKD between all combinations of users in a fully-connected network was achieved for a short time with pre-aligned interferometers and without phase realignments.

The number of users that can be connected to the q-hub is limited by the wavelength-division demultiplexers and the number of receiver modules currently available. If the appropriate number of receiver modules were built, up to 78 users in 39 fixed pairs could be readily connected to the q-hub via the 50 GHz AWG. Hundreds of users could be connected in a reconfigurable network if a wavelength-division demultiplexing structure with two layers of wavelength-selective switches was used.

A selection of the field test results has been published in refs. [II, V].

4 Towards a Photonic-Chip-Based Quantum Key Hub

The size and cost of the quantum key hub could be significantly reduced by implementing it with photonic chips, also called *photonic integrated circuits* (PICs). PICs would enable the integration of the required optical functionalities in one chip or a small number of connected chips with a size of a few square millimeters. Once a chip design has been developed, multiple copies of chips with this design can be produced at a relatively low cost. Further advantages of integrated optical circuits are that they are robust and that spatial alignment of the integrated components is not required. Therefore, chip-based components could pave the way for a broader deployment of QKD systems.

Two common materials for photonic chips are silicon nitride (Si_3N_4), often in combination with silicon oxide (SiO_2), as well as indium phosphide (InP). Si_3N_4 has a comparatively high optical third-order nonlinearity and introduces relatively low losses [170], while InP enables the implementation of active components such as lasers, photodiodes, and fast modulators [171]. Photon pairs can be generated by *spontaneous four-wave mixing* (SFWM) in Si_3N_4. In SFWM, two pump photons are converted into a signal photon and an idler photon. In contrast to SPDC, for SFWM, the pump is in the same wavelength range as the generated photon pairs. Therefore, narrow filters are required to separate the pump light from the photon pairs. As the third-order nonlinearity is small, relatively high pump powers are required.

QKD with PIC-based photon sources has been demonstrated in refs. [112, 117, 118, 172]. The required pump power is lower when the pump light and the photon pairs are confined in a resonator. Therefore, SFWM is often realized in on-chip *microring resonators* (MRRs) [172–174], where the photon pairs are generated at the resonance frequencies of the MRR. QKD using the BBM92 protocol with photons generated in MRRs has been demonstrated in ref. [117]. For the q-hub, each pair of resonances symmetric around the center frequency can be used to distribute quantum keys to one pair of users.

To investigate SFWM in MRRs as an alternative to SPDC for generating photon pairs in the q-hub, a PIC with a box-shaped Si_3N_4 waveguide manufactured by *LioniX International BV* was borrowed from the research group led by Prof. Dr. Boller at the University of Twente.

In this chapter, a setup for high-frequency Pound-Drever-Hall locking is presented, enabling the stabilization of MRR resonances to the pump light. Section 4.1 presents the design of a dedicated PIC for generating photon pairs for the q-hub network. It integrates spectral filters and the photon pair generation on a single PIC. In section 4.2, the on-chip filters are tested, and photon pair generation is demonstrated.

High-Frequency Pound-Drever-Hall Locking for Microring Resonators

The borrowed PIC features multiple straight bus waveguides, each coupled to a single MRR as shown in fig. 4.1 (a). As the PIC was not packaged, a setup for coupling light from optical fibers to the chip and from the PIC into fibers by using *lensed fibers* was realized during the master's thesis of Jakob Kaltwasser [M2]. Precise alignment of the lensed fibers to the chip facets with sub-micrometer precision is realized with mechanical and piezo-based translation stages.

To generate photon pairs by cavity-enhanced SFWM on the PIC, the MRR must be tuned into resonance with the pump light by applying a current across an on-chip heating element above the MRR. Ideally, the coupling coefficient between the ring and bus waveguide matches the round trip losses in the ring, such that the ring is critically coupled, and the pump light is completely dissipated in the ring, leading to the maximal pump light intensity in the resonator. As the volume of the ring waveguide is small, the dissipated power can lead to a significant temperature change of the waveguide, changing its optical path length and thereby detuning the resonance. To achieve a stable operation for pump powers up to a few milliwatts, a resonance locking scheme based on the *Pound-Drever-Hall* (PDH) technique [178, 179] was realized during the master's thesis of Florian Vogel [M9].

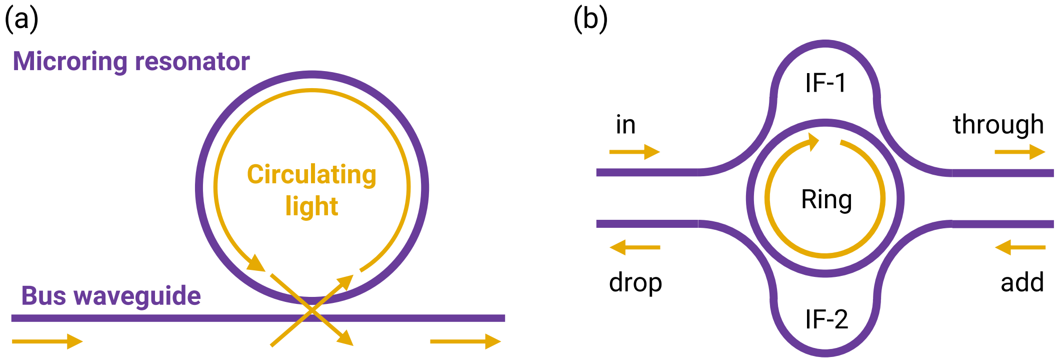


Figure 4.1: Schemes of microring resonators for photon pair generation. (a) Single ring coupled to a bus waveguide. (b) Dual imbalanced Mach-Zehnder interferometer ring (DIMITRI) [175–177].

A challenge for implementing the PDH scheme was the wide free spectral range of the MRRs of up to 180 GHz and the corresponding large resonance line widths of a few hundred megahertz. For PDH locking, phase modulation is applied to the laser light, generating sidebands outside the resonance. Due to large resonance line widths, a modulation frequency in the low gigahertz range is necessary. PDH locking is a common technique, and PDH locking of MRR at gigahertz frequencies has been reported in ref. [180]. However, no commercial solution for the locking circuit was available for such high modulation frequencies. Therefore, the locking setup for testing the PIC was built from individual components as shown in fig. 4.2. The spectrum of a CW laser[1] at 1550.5 nm is cleaned by two FBGs with 30 GHz wide reflection bands and the power is adjusted with a VOA. A phase

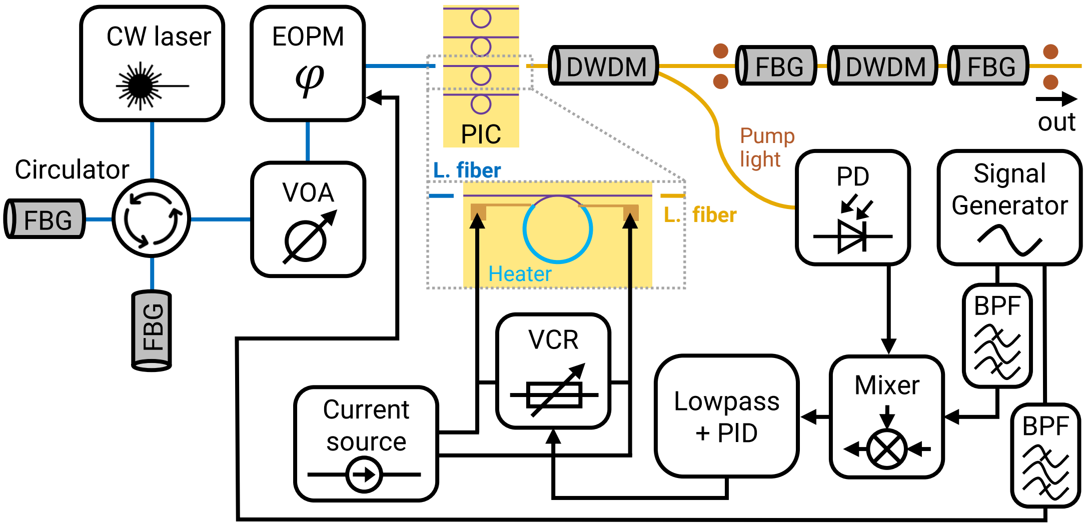


Figure 4.2: Setup for photon pair generation in microring resonators using Pound-Drever-Hall locking. The application for the unpackaged chip is shown, but the setup is also used for locking resonators on the packaged chip. FBG – Fiber Bragg grating with 30 GHz wide pass band, VOA – Variabel optical attenuator, EOPM – Electro-optic phase modulator, PIC – Photonic integrated circuit, L. fiber – Lensed fiber, DWDM – Dense wavelength-division multiplexing filter, PD – Photodiode, VCR – Voltage-controlled resistor, PID – proportional-integral-derivative controller, BPF – Bandpass filter. The zoomed inset shows one of the MRRs on the PIC to which light is coupled by a lensed fiber. The ring round trip phase is controlled by adjusting the current flowing through a heating element above the ring waveguide. Optical PM fibers are shown in blue, and SM fibers are shown in yellow. The cascade of DWDMs and FBGs is the same one used in the single-converter setup of the PPS (cf. fig. 3.13).

[1] Laser diode: QDFBLD-1550-100 from *QPhotonics*, mounted on a CLD1015 laser driver from *Thorlabs*.

modulation is applied with an EOPM driven by a bandpass-filtered sine signal generated by a signal generator[2]. A lensed fiber couples the light into the bus waveguide. Another lensed fiber collects the light transmitted through the waveguide. A 100 GHz wide DWDM filter separates the photon pairs from the remaining pump light, which is detected by an AC-coupled amplified photo diode[3] with a bandwidth of 2 GHz. The generated photon pairs are further cleaned from the remaining pump light by two FBGs and another DWDM.

The photodiode voltage is mixed in a double-balanced mixer[4] with the signal from the second output of the signal generator, which is a phase-shifted copy of the signal driving the EOPM. The mixer output is analyzed by a single-board computer[5] with analog input and output channels with a bandwidth of 60 MHz. The board is operated as a lowpass filter and digital *proportional-integral-derivative* (PID) controller by using the *pyRPL* software [181]. It provides an analog signal to an in-house-made circuit board on which a voltage-controlled resistor is implemented. A multi-channel current source[6] provides a constant current flowing through the heating element on the PIC, controlling the ring round trip phase. The heating element and the voltage-controlled resistor are connected in parallel.

When the MRR resonance shifts relative to the laser frequency, the PDH error signal changes, which the PID controller detects. The controller delivers a variable voltage to the voltage-controlled resistor, thereby changing its resistance such that the current flowing through the heating element changes, leading to a change of the ring round trip phase. The PID parameters are set up so the control loop stabilizes the ring to the laser frequency.

Using this setup, the generation of photon pairs with the borrowed PIC was demonstrated. However, coupling light to and from the PIC with lensed fibers introduces high losses and requires careful alignment, such that the optical part of this setup is not very robust and is, therefore, not optimal for the q-hub.

4.1 Design of a Photonic Integrated Circuit for the Q-Hub

To overcome the shortcomings of the borrowed PIC, a dedicated PIC was designed, integrating multiple functionalities required for the q-hub. The PIC was again manufactured by *Lionix* but with asymmetric double-stripe waveguides of the TriPleX™ platform instead of box waveguides [170, 182]. Photon pair production in a 6.5 cm long double-stripe waveguide on this platform was demonstrated in ref. [183], and the on-chip generation of

[2] Signal generator: SynthHD v2 RF from *Windfreak Technologies*.

[3] Photo diode: WL-PD2GA from *Wieserlabs*.

[4] Mixer: ZLW-11H+ from *Minicircuits*.

[5] Single-board computer: STEMlab 125-14 from *Red Pitaya*.

[6] Multi-channel current source: XPOW-40AX-CCvCV-U from *nicslab*.

time-bin entangled photon pairs in such waveguides was reported in refs. [184, 185]. For this waveguide design, *Lionix* offers PIC packaging, attaching fibers to the waveguides.

The PIC was designed to implement three important functionalities that are essential for the q-hub system: the cleaning of the pump laser light from the Raman background produced in the optical fibers, the generation of photon pairs in MRRs, and the separation of the photon pairs from remaining pump light. All functionalities can be realized with combinations of waveguides and couplers forming IFs and ring resonators that are phase-tunable by applying currents to heating elements.

An important design consideration was that the tolerances of the losses in the waveguides and the tolerances of the coupling coefficients are much higher than for standard fiber components. For an MRR to be critically coupled, the internal losses must match the coupling coefficient. Therefore, multiple MRRs were placed on the PIC with slightly different coupling coefficients to increase the probability that at least one is matched well. For redundancy, four different photon generation lines A to D with slightly different parameters are implemented on the PIC. Each line consists of a Raman filter block, a photon generation block, and a pump filter block. Each block consists of multiple resonators, as shown in fig. 4.3. A single test ring coupled to a bus waveguide without any filters is also integrated for testing purposes.

The layout was optimized to suppress scattering from pump light photons into waveguides guiding photon pairs. Furthermore, the geometric arrangement was optimized to minimize the thermal cross-talk between heating elements of different phase-sensitive elements. Thermally decoupling these elements facilitates phase alignment when operating the PIC.

Implemented Microrings Resonators for Photon Pair Generation

Two different MRR designs were implemented for photon pair generation: single-bus MRRs and dual-bus MRRs coupled to two imbalanced Mach-Zehnder IFs (cf. fig. 4.1 (b)). As there exists so far no established abbreviation for this design in the literature, it will be called *dual imbalanced Mach-Zehnder interferometer ring* (DIMITRI) in the following. Photon pair production in DIMITRIs has been demonstrated in refs. [175–177]. The IFs act as wavelength-selective couplers and improve the photon pair generation in two ways: first, the photon pairs are directly separated from the pump light because they leave the DIMITRI through a different waveguide. Second, they can be used to improve the extraction efficiency of the photons [175, 176]. For that, the OPD of the IFs is chosen such that their FSR is twice as large as that of the ring. For the DIMITRIs on the PIC, the ring FSR is chosen to be 50 GHz and the FSRs of the IFs are 100 GHz, to be in line with the ITU-T DWDM grid [74]. The group index of the waveguides is $n = 1.77$ [182], such that an MRR with an FSR of 50 GHz has a diameter of approximately 1.08 mm.

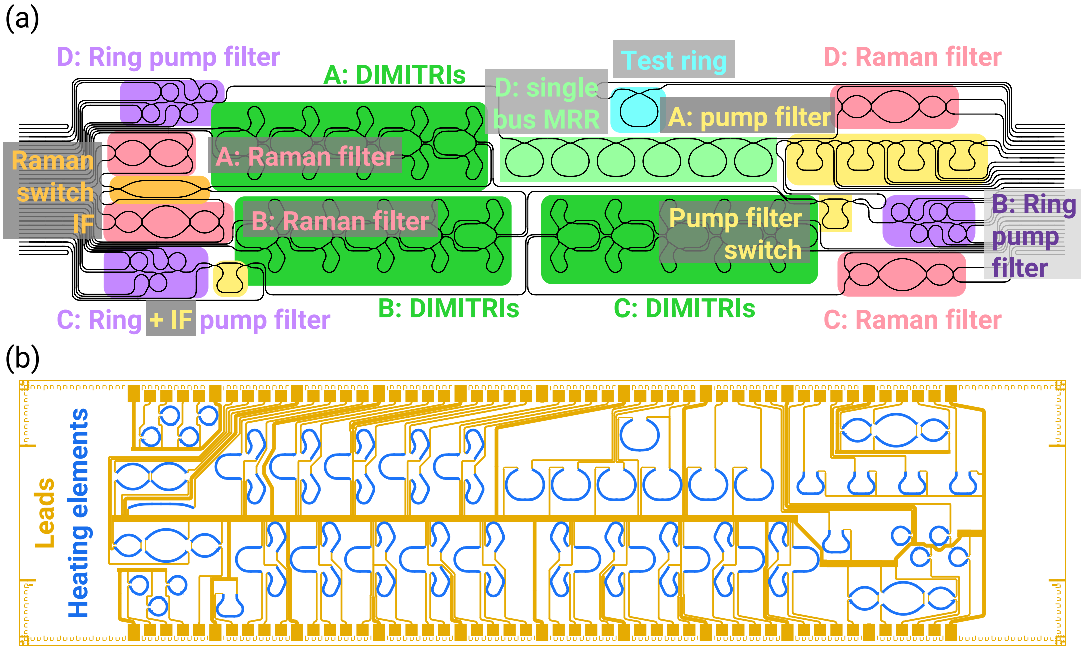


Figure 4.3: Layout of the photonic integrated circuit (PIC) with four independent photon generation lines (A to D). The dimensions are 8 mm × 32 mm. (a) Arrangements of waveguides are grouped in functional blocks (colored areas). The left and right facets each provide 32 optical ports coupled to optical fibers. Eight ports are reserved for the package alignment and cannot be used to implement functions on the PIC. (b) Arrangement of the electrical layer with leads and heating elements on top of the waveguides. The electrical current is provided via 80 contact pads in the top row and bottom row and leaves the chip via 22 larger ground pads.

The phase of IF-1 (cf. fig. 4.1 (b)) is adjusted such that coupling for the pump light from the input to the ring is maximal, and the phase of IF-2 is chosen such that the coupling of the pump light from the ring into the drop port is minimal. Photon pairs are generated in the ring at resonances with a distance of multiples of 50 GHz to the pump frequency. Photons generated with a frequency difference that is an even multiple of 50 GHz are coupled out by IF-1 into the through port, together with some pump light. Photons generated with a frequency difference to the pump frequency that is an odd multiple of 50 GHz are coupled out by IF-2 into the drop port. If IF-2 worked perfectly, no pump light would be coupled to the drop port, resulting in a pure photon pair spectrum. The maximum of the coincidence rate from photon pair generation is obtained when the coupling of IF-1 is chosen such that the ring is critically coupled and the coupling for IF-2 is chosen twice as strong [176]. The probability for a generated photon to be coupled out into the drop port is then twice as high as the probability that it is dissipated in the ring.

The waveguide propagation losses and the coupling between the bus waveguides and rings or DIMITRIs are subject to manufacturing tolerances. Therefore, multiple rings or DIMITRIs are chained up in each photon generation line to improve the chance that for at least one of the MRRs the coupling coefficients and losses match well. The coupling coefficients are designed with slight variations from MRR to MRR. Line A, B, and C each feature five DIMITRIs, and line D features six regular rings coupled to a bus waveguide. For photon pair generation, only one MRR per line is tuned in resonance with the pump light. Future PIC designs could also use simultaneous coherent photon pair generation in a series of MRRs [186].

Implemented Filters

Raman scattering in the optical fibers is one of the major sources of background noise for setups using SFWM in MRRs for photon pair generation [174, 187]. Two on-chip Raman filters were implemented to remove the Raman noise from the pump light before it enters the MRRs generating photon pairs. For lines A and B, filters consisting of two or three serially coupled rings are implemented. An optical switch implemented by a tunable IF allows to use either of the Raman filter blocks with lines A or B. In lines C and D, dedicated three-stage Raman filters are used. The ring round trip phases are tuned so that the pump light is resonant in all three rings and transmitted. The ring FSRs are chosen to be slightly different, such that the Vernier effect extends the FSR of the filter considerably. Light at resonances of the first ring is blocked by the second and third ring, light resonant in the second ring is blocked by the first and third ring, etc. The ring FSRs and coupling coefficients were designed to sufficiently suppress the Raman noise for a broad frequency range. Furthermore, by using methods from ref. [188], they were optimized so that the top of the transmission peak is flat, allowing a stable transmission of the pump light even when the rings are slightly detuned. For the optimizations, the frequency response functions of the coupled MRR filters were derived similarly as in ref. [189] by using Masons' rule [190–193] to simulate the transmission spectrum. In contrast to transfer-matrix-based methods [194, 195], which are particularly well suited for numerical investigations, Masons's rule and similar newer, more efficient methods [196, 197] enable the derivation of the analytical expression for frequency response of moderately complex linear systems such as coupled ring filters or DIMITRIs with little efforts.

Two different types of pump light filter blocks are implemented. The first type consists of four dual-bus MRRs with an FSR of 100 GHz. They are tuned in resonance with the pump light and transmit it into other waveguides, while photon pairs are off-resonant and, therefore, remain in the main bus waveguide. The second type of pump filter block consists of a series of four imbalanced Mach-Zehnder IFs with an FSR of 100 GHz. For filtering, the IF phases are adjusted to transmit the photon pairs through all IFs while the pump light is directed to other waveguides. For lines A and B, another such IF is installed so that for each line, it can be chosen if the ring filter block or the IF filter block is used to filter out the pump light. The pump filter block of line C consists of three rings and one IF, and that of line D consists of four rings.

4.2 On-Chip Photon Pair Generation

Four copies of the dedicated PIC described above were ordered from *Lionix* to increase the probability that at least some of the MRRs are almost critically coupled. Figure 4.4 shows photos of one of the packaged PICs and a microscope image where waveguides, heaters, and leads are visible. Due to limited time, only one of the PICs was tested extensively during the master's thesis of Maximilian Mengler [M8]. The PIC was placed in an enlarged version of the IF containers for optimal thermal stability, and a TCU controlled the temperature.

Photon pair generation was tested with different MRRs. Without PDH locking, the MRRs cannot be tuned stably into resonance for pump powers above about 5 mW. However, with PDH locking, the MRRs are stable even for the highest tested pump power of 15 mW.

The phases of the Raman filters and pump filters are aligned by applying constant currents to the heaters with a 40-channel current source[7] and the PDH locking setup was used to

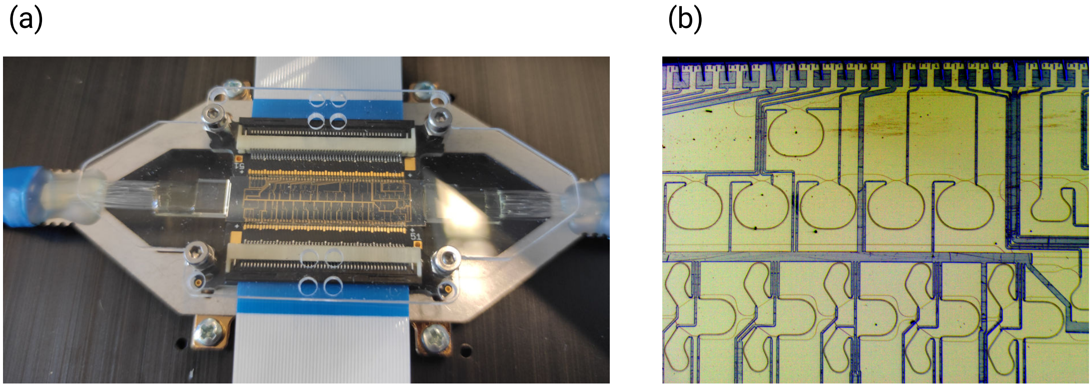


Figure 4.4: Photos of the dedicated photonic integrated circuit (PIC). (a) Packaged chip with optical fiber connections from left and right and flat band cables for the electrical connections from top and bottom. (b) Microscope image of a part of the PIC.

[7] Multi-channel current source: XPOW-40AX-CCvCV-U from *nicslab*.

stabilize the MRR generating the photon pairs. After the PIC, the cascade of DWDMs and FBGs used in the single-converter PPS experiment (cf. fig. 3.13) was connected to improve the pump light suppression. The 100 GHz AWG was used as WDM.

To demonstrate photon pair generation, the PIC was then pumped with 10 ns long laser pulses at a repetition frequency of 10 MHz and the timestamps of photons in the AWG channels with 450 GHz separation to the center frequency were acquired.

Figure 4.5 shows the crosscorrelation of the timestamps from a test of DIMITRI-2 in line A, normalized to a maximum value of 100 %. Small peaks are visible every 100 ns, indicating the correlation of photons from different pulse cycles. The peaks are triangular because the pulse shape is almost rectangular, and the crosscorrelation of two rectangle functions is a triangle. On top of the central triangle, a high 0.7 ns wide peak is visible, indicating the presence of photon pairs generated by SFWM. The *coincidence-to-accidental ratio* (CAR) can be used to roughly quantify the quality of the photon pair generation, disregarding detector imperfections such as dark counts. It is given by the ratio of coincidences measured with correlated photons from pairs divided by the accidental coincidences, meaning that it is the ratio of the height of the crosscorrelation peak at $t = 0$ to the height of the side peaks. Figure 4.5 shows that the CAR decreases for higher pump powers. For an average pump power of 0.5 mW, the CAR is around 80. The value can be compared to ref. [117], where CARs in the range of 60 to 150 were observed for the photon pairs generated by SFWM in a Si_3N_4 MRR at the same peak power. The quality of these photon pairs in ref. [117] was sufficient to demonstrate QKD, and it is therefore be expected that QKD will also be possible with the PIC designed for the q-hub.

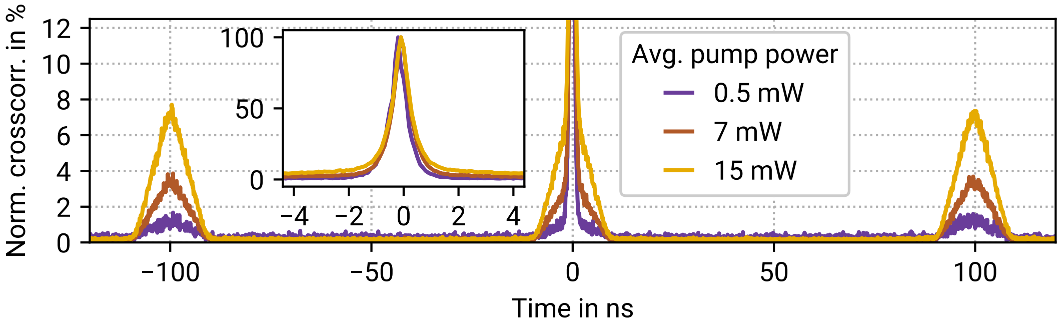


Figure 4.5: Crosscorrelation of signal and idler photons generated by DIMITRI-2 in photon generation line A with 450 GHz separation to the center frequency. The PIC was pumped with 10 ns long pulses at a repetition frequency of 10 MHz. The time resolution is 100 ps. The inset shows the central peak due to photon pairs on top of the triangular background from accidental coincidences.

However, the photon pair generation did not work as well as expected. Although photon pairs are generated, attempts to determine the conversion efficiency showed that the photon pairs are contaminated with much more noise than the photon pairs from the PPS generated by SPDC. To investigate this noise, the output spectra of the PIC were measured with the spectrograph (cf. section 2.2.2). The filter cascade of DWDMs and FBGs was installed after the chip to remove all laser light left after the on-chip pump filters. Figure 4.6 shows the spectra of line D with all MRRs detuned so that the pump light is not resonant. For some of the shown curves, the on-chip Raman filters were bypassed, or the pump light filter rings were detuned. Without Raman and pump filters, a broad Raman background is visible at both sides of the center frequency, with periodic dips due to ring resonances. The large central dip is caused by the external pump filter cascade suppressing all light in a frequency range of ±50 GHz around the center frequency.

When either the Raman filters or the pump filters are used, the Raman background is reduced but still present. The Raman filters only remove the background generated in the fibers before the PIC. If the remaining pump light is not directly removed on the chip by the pump filters, it generates further Raman photons in the fibers after the chip. The fact that a non-negligible Raman background is still present when only the Raman filters are used

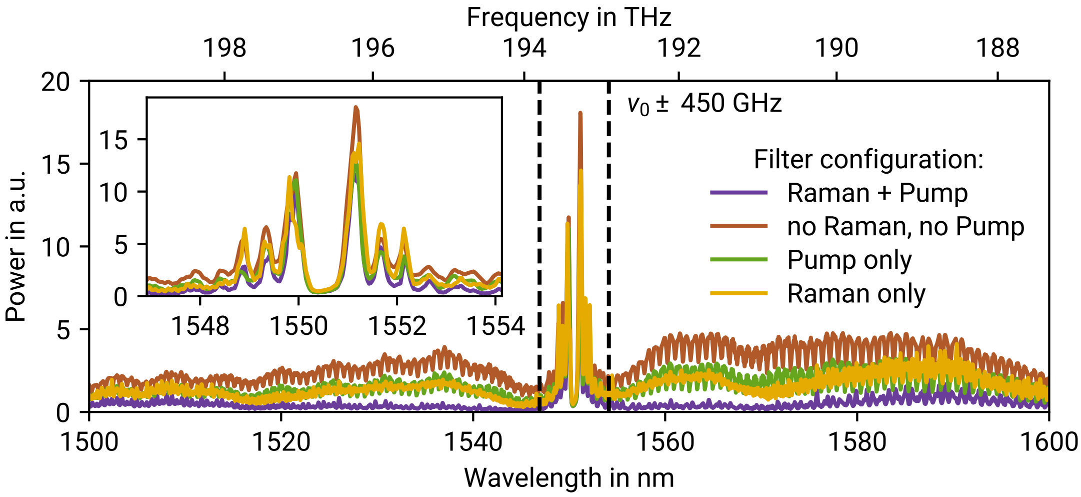


Figure 4.6: Spectra of photon generation line D with different on-chip filters, measured with the spectrograph. All microring resonators for photon generation were tuned out of resonance. The photonic integrated circuit was pumped with 10 ns long pulses at a repetition frequency of 10 MHz with an average power of 10 mW. The dashed lines show the frequency pair for which the crosscorrelation shown in fig. 4.5 was measured.

demonstrates the necessity of the on-chip pump filters. When Raman and pump filters are used, the Raman background is almost completely removed, as expected. These results show that the filters work as expected and demonstrate the advantage of on-chip spectral filters for reducing Raman noise.

In the wavelength range of ±2 nm around the center frequency, multiple high peaks with a spacing of 50 GHz are visible. They are almost independent of the filter configuration. Scans of the pump power showed that the height of these peaks scales linearly with the pump power. The rate of photon pairs generated by SFWM would scale quadratically with the pump power. Therefore, it can be concluded that the main contribution of the peaks comes from a noise process and not from photon pairs. If the noise were generated before the PIC, it would be reduced by the Raman filters, and if it were generated in the fibers after the chip, it would be reduced when the pump filters remove the pump light. Therefore, it can be concluded that the noise is generated on the PIC itself.

In principle, multiple processes can lead to such noise. Brillouin scattering in Si_3N_4 has a gain maximum at a frequency shift of approximately 11 GHz [198], which is one order of magnitude less than the frequency shift of the observed noise. Raman scattering in Si_3N_4 is typically only relevant for larger frequency shifts of several terahertz [199, 200]. Therefore, Brillouin and Raman scattering as the noise source seem unlikely. The Si_3N_4 waveguides are embedded in SiO_2, such that the background from this material should match the background from the optical fibers. The background generated in the fibers is visible in fig. 4.6, and it shows a minimum around the center frequency, such that the noise is probably also not generated in the SiO_2 of the chip. Three of the four copies of the PIC have been shown to generate the noise, and the fourth PIC has not been tested. So far, the root cause of the noise could not be identified.

The CD in the asymmetric double-stripe waveguides is relatively strong, leading to a non-constant frequency spacing of the resonances. As energy conservation only allows the generation of photon pairs at frequencies symmetric around ν_0, photon pair generation is restricted to a few resonances around the center frequency, limiting the number of users that could be connected to a q-hub with a PPS based on such a PIC. Therefore, the above-mentioned noise is particularly relevant because it affects the innermost five to six resonance pairs.

Next Steps Towards a Photonic-Chip-Based Quantum Key Hub

For future PIC designs, waveguides with lower CD would be desirable such that photon pairs for higher numbers of users can be generated. Further experiments are required to quantify the actual impact on the QKD performance. As the measured CARs are comparable to those reported in ref. [117], it is well possible that despite the noise, the quality of the photon pairs is sufficient to demonstrate QKD. Therefore, an essential next step towards a PIC-based q-hub is a test of QKD with photons generated by SFWM on the PIC.

Identifying the source of the noise and preventing its generation in future PIC generations is desirable. Future PICs for the q-hub could also directly integrate WDMs, for example, based on IF trees [201]. Furthermore, laser pulse generation at 1550 nm could be realized using InP-based PICs. As many applications benefit from combining the advantages of the different platforms, commercial suppliers offer hybrid integration of different PICs such as InP and Si_3N_4 [202]. The receivers could also use PIC-based IFs with long delays, as demonstrated in refs. [63–65, 184, 185]. Ultimately, the complete q-hub QKD system could be realized using PICs, paving the way for the cost-efficient production of a larger number of such systems for deployment in a wide range of applications.

Summary of Chapter 4

The generation of photon pairs for the q-hub by spontaneous four-wave mixing in silicon nitride *microring resonators* (MRRs) on *photonic integrated circuits* (PICs) was tested. A setup for coupling light from optical fibers to an unpackaged chip and from the chip into optical fibers was developed. The setup was used to generate photon pairs with a PIC borrowed from Prof. Dr. Boller's research group at the University of Twente. The setup was then extended to enable gigahertz-modulated Pound-Drever-Hall stabilization of the microring resonances to the pump laser frequency.

Based on the experiences with the borrowed chip, a dedicated PIC was designed. It combines MRRs for photon pair generation with spectral filters for cleaning the pump light from Raman noise and with filters separating the generated photon pairs from the pump light. Two types of MRR designs for photon pair generation are implemented: rings coupled to a bus waveguide and MRRs consisting of a ring coupled to two imbalanced interferometers. This latter design should enable better suppression of the pump light in the photon pair spectrum and higher photon pair extraction efficiencies.

Four copies of the packaged PIC were ordered, and one was tested. Using the Pound-Drever-Hall stabilization, the MRRs could be kept stably in resonance with the pump light, even for the highest tested pump power of 15 mW. Crosscorrelation measurements showed that photon pairs are generated. Unfortunately, their spectrum is contaminated with strong noise of unknown origin. From a comparison of the measured coincidence-to-accidental ratios to values reported in the literature, it is feasible that the quality of the photon pairs may nevertheless be sufficient to demonstrate QKD. Further experiments are required to identify the origin of the noise and to quantify its impact on the performance of the QKD system.

Part II

Modeling and Simulations

5 Detector Characterization and Reconstruction of Positive Operator-Valued Measures

Detector side channels can impair the security of QKD systems, and detailed knowledge about the *single-photon detectors* (SPDs) benefits the security. Furthermore, thorough detector characterizations are required for developing accurate simulation models of QKD systems. This chapter presents a detailed analysis of the SPDs used in the q-hub system.

Section 5.1 introduces the setup for the SPD characterization. An early version of the experimental setup was realized during the bachelor's thesis of Philipp Kleinpaß [B2] and it was further improved during the bachelor's thesis of Maximilian Mengler [B4].

Section 5.2 presents the measured values for dark count rates, dead times, and afterpulses, which are used for modeling the detectors in the simulations in chapters 6 and 7.

The measurement results obtained from a quantum detector can be described in terms of *positive operator-valued measures* (POVMs) characterizing the detector. In the context of detector POVMs, the time dependence of the detection process is rarely considered. An exception is a time-dependent model for POVMs of *non-photon-number-resolving* (non-PNR) detectors proposed by Gouzien et al., which includes dead time and timing jitter into the POVM model [203]. The concept of time-dependent detector tomography is introduced to narrow this gap between theory and experiment. Section 5.3 presents time-dependent and time-independent detector POVMs reconstructed from the data obtained in the characterization measurements. In addition, the detection efficiencies are calculated, showing that the detectors are slightly more efficient than specified by the manufacturer.

In section 5.4, the predictions of the timing jitter POVM model from ref. [203] are compared to measurements, showing that time-dependent detector tomography can reveal information about effects in SPDs that are not included in the POVM model from ref. [203].

The research presented in sections 5.3 and 5.4 was published in ref. [III]. These investigations were carried out in close collaboration with Robin Krebs, Thorsten Haase, and Prof. Dr. Gernot Alber from the *Theoretical Quantum Physics* research group at the

Technical University of Darmstadt. Robin Krebs developed and benchmarked an adaptive regularization method for the POVM reconstruction and worked on the test of the timing jitter model during his bachelor's thesis [B3] under the supervision of Prof. Dr. Gernot Alber and Thorsten Haase.

5.1 Setup for Detector Characterization

The setup for the detector characterization is shown schematically in fig. 5.1. Light from a CW laser[1] with a center wavelength of about 1550.52 nm is chopped into pulses by two cascaded *electro-optic amplitude modulators* (EOAMs)[2], attenuated to the single-photon level by one manual and one electronically adjustable variable optical attenuator (VOA)[3] and sent into the SPD under test. The laser and the fibers are polarization-maintaining. However, the inputs of the SPDs are multi-mode fibers that do not preserve the polarization, such that the polarization state arriving at the photodiode of the SPD is unknown.

The SPD is connected to one input channel of a *time controller* (TC), and the trigger output of the dual-channel pulse generator[4] driving the EOAMs is connected to another input. The timestamps recorded in this trigger channel provide a time reference relative to which the photon detection times are measured. The pulse generator is set up such that

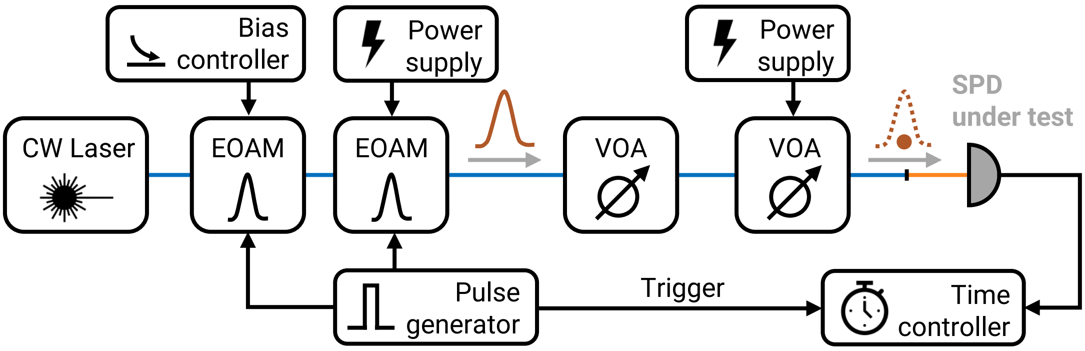


Figure 5.1: Setup for detector characterization. EOAM – Electro-optic amplitude modulator, VOA – Variable optical attenuator. PM fiber is shown in blue. The detector input is a multi-mode fiber (orange). The bias of the second EOAM and the attenuation of the second VOA are controlled by voltages provided by laboratory power supplies.

[1] Laser diode: QDFBLD-1550-100 from *QPhotonics* mounted on a CLD1015 laser driver from *Thorlabs*.
[2] Amplitude modulators: MXAN-LN-10 (low loss) and MXER-LN-10 (high extinction ratio) from *iXblue*.
[3] Electronic variable optical attenuator: V1550PA from *Thorlabs*.
[4] Pulse generator: HP 8131A from *Hewlett Packard*.

the first EOAM shapes pulses with an FWHM duration of 0.24 ns and the second modulator is opened for a window of ±5 ns around the passage time of the light pulse from the first modulator. Therefore, the first modulator determines the pulse shape, and the second modulator increases the extinction ratio between pulses outside the ±5 ns window. Thereby, photons leaking between the pulses through the first modulator are further suppressed to increase the signal-to-noise ratio. The repetition rate was set to 10 kHz such that the time between pulses is with 100 µs much longer than effects from the dead time and afterpulses. Correlations between subsequent pulses are thereby suppressed such that the detections from different pulses are independent. The first EOAM is stabilized by a bias controller (cf. section 2.1.1). The second EOAM receives a pulsed optical input with a low average optical input power such that it cannot be stabilized with a bias controller. Instead, before starting a measurement, its bias voltage is swept and readjusted to the value that minimizes the rate of photons leaking between pulses through the modulators.

5.2 Measurements of Dark Counts, Dead Times, and Afterpulses

The SPDs are free-running single-photon avalanche diodes[5], meaning that they are (non-PNR) detectors producing an electronic pulse (a *count*) whenever they detect one or multiple photons. Single-photon avalanche diodes are essentially reverse-biased p-n junctions operated in Geiger mode [204]. When an incident photon creates an electron-hole pair, the charge carriers are accelerated in the electric field across the junction. The applied voltage is so high that the charge carriers gain enough energy so that they can create further pairs of charge carriers. Thereby, an avalanche of charge carriers is started, producing a macroscopic current indicating the detection of a photon [204]. Then, the bias voltage is lowered below the breakdown voltage for some time to stop the avalanche before the bias is again increased above the breakdown voltage such that the next photon can be detected. This detection mechanism causes some effects that ideal single-photon detectors would not show. Besides the non-unity detection efficiency, the dark counts, dead times, and afterpulses are the most important effects.

Dark Count Rates

Dark counts are counts that are registered, although no photons were present. They occur when spontaneously generated charge carriers lead to avalanches [204]. To minimize this effect, the photodiodes of the ID220 SPDs are cooled down to approximately −50 °C by thermo-electric coolers. Dark counts are unwanted detection noise leading to quantum bit errors, so low dark count rates are desirable.

[5] Single-photon detectors: ID220 from *IDQuantique*.

The SPDs allow to choose between three different settings for the detection efficiencies of 10, 15, and 20 %, corresponding to different bias voltages. Furthermore, the dead times can be set between 1 and 25 µs. In general, a high detection efficiency and a short dead time are desirable to detect as many photons as possible. But the settings come with a trade-off: on the one hand, setting higher efficiencies leads to higher dark count rates and afterpulse probabilities for a given dead time. On the other hand, longer dead times reduce the dark count rate and the probability that the detector is active when the next photon arrives.

The dark count rates were measured for all eight detectors of the q-hub network at several different combinations of the dead times and efficiencies. Figure 5.2 (a) shows the dark count rate of SPD-2 as an example. At short dead times, the dark count rate is much higher than for longer dead times, especially for the highest detection efficiency of 20 %. This means that for QKD, a combination of settings needs to be chosen for which both the detection efficiency and the noise from dark counts and afterpulses are acceptable. The optimal settings used for all QKD experiments are 20 % efficiency and 10 µs dead time (cf. fig. 3.3). Figure 5.3 shows the measured dark count rates for all detectors at these settings.

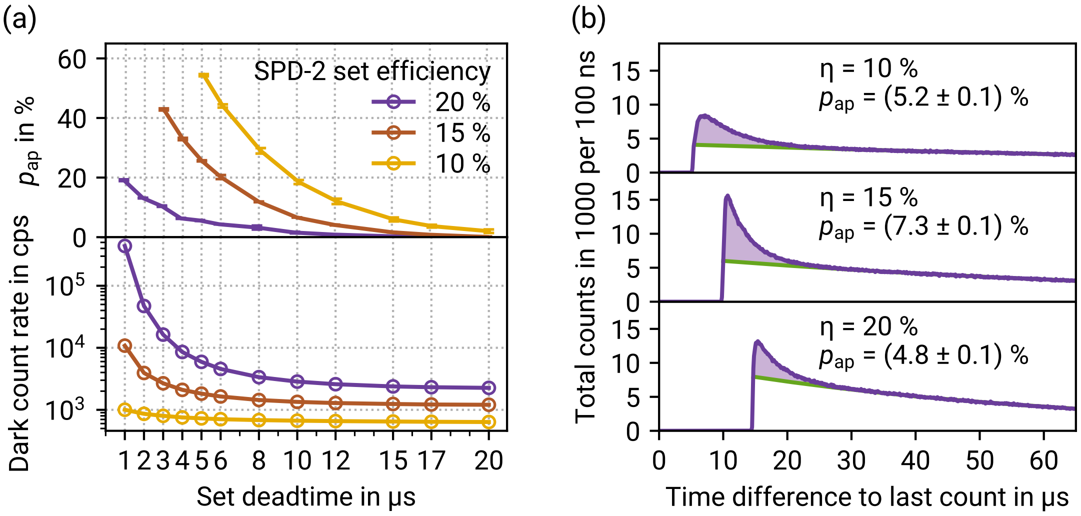


Figure 5.2: Detailed characterization of SPD-2. (a) Dark count rates and afterpulse probabilities p_{ap} for different dead times and set efficiencies. (b) Histogram of time to the next count after a count originating from a pulse for SPD-2, calculated from the POVM tomography data for the highest mean photon number $\mu = 50$ acquired over 10 min. The settings from top to bottom are 5, 10, and 15 µs dead time with set efficiencies η of 10, 15, and 20 %. The integral of the area between the exponential fit (green) and the histogram (violet) is the afterpulse probability p_{ap}.

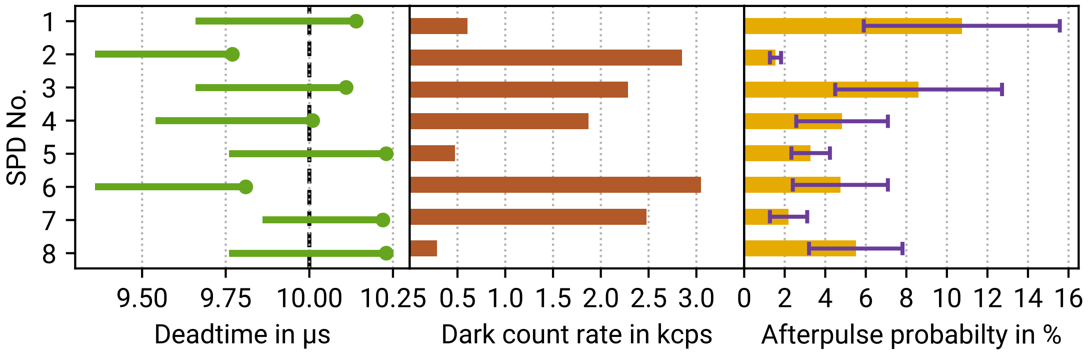


Figure 5.3: Dead times, dark count rates and afterpulse probabilities for all eight SPDs operated at 20 % set efficiency and 10 µs set dead time. The circles in the left diagram mark the rising edge of the autocorrelation, and the left end of the bar marks the shortest observed dead time.

Dead Times

After a count, the detector is automatically deactivated for a dead time τ_{dead}, during which no further counts can be registered until the detector is activated again. As photons arriving during the dead time cannot be detected, the dead time reduces the effective detection efficiency. This effect can be quantified by comparing the count rate r' of a detector with dead time to the count rate r of an identical detector without dead time. For the detector with dead time, p_{on} is the probability that the detector is active (not in the dead time) at a certain point in time. Each count contributing to rate r of the detector without dead time occurs with probability p_{on} at a time when the detector with dead time is active, meaning that $p_{\mathrm{on}} = r'/r$. The fraction of the measurement time during which the detector is deactivated is given by $r'\tau_{\mathrm{dead}}$, such that

$$p_{\mathrm{on}} = 1 - r'\tau_{\mathrm{dead}}\,. \tag{5.1}$$

By combining eq. (5.1) with $p_{\mathrm{on}} = r'/r$ from above, r can be calculated by [205]

$$r = \frac{r'}{1 - r'\tau_{\mathrm{dead}}}\,. \tag{5.2}$$

The count rate reduction due to the dead time is non-negligible at the parameters where the QKD system is operated. For example, when Alice is connected to the PPS via the deployed fiber link (cf. fig. 3.1), the count rates of her detectors are in the range of 30 kcps. The detectors are operated with a dead time of 10 µs, such that $p_{\mathrm{on}} = 0.7$.

To quantify how accurately the set dead time represents the actual dead time in practice, the detectors were illuminated with dim laser light. The dead time was extracted from the autocorrelation function of the recorded timestamps. The autocorrelation is zero for times below the dead time. It steeply increases at the dead time and approaches a constant plateau value for long times. Figure 5.3 shows the measured dead times for all SPDs. The measured dead times of all detectors match the set dead time except for SPD-2, which has a slightly shorter dead time.

Afterpulse Probabilities

Charge carriers from an avalanche can be trapped in the photodiode. Another avalanche can be triggered, although no photons are present, when these carriers are released after the dead time when the diode is biased again. Such detector counts are called afterpulses [204]. Afterpulses are another type of undesired detection noise.

To measure the afterpulse probability, the second EOAM was removed from the setup shown in fig. 5.1 to avoid the necessity of the calibration runs and to speed up the measurement. Afterpulses were measured for all eight detectors at the different set efficiencies and for different set dead times. For the three setting combinations at which data for the POVM reconstruction were acquired, the afterpulse probability can similarly be calculated from the data acquired for the POVM reconstruction.

To calculate the afterpulse probability, only those counts that are coincident with the electronic trigger pulse within a short window around the maximum of the count histogram are selected. These counts are very likely caused by photons from the light pulses. Then, the time differences between these and the following counts are calculated and collected into a histogram. As an example, the histograms of SPD-2 calculated from the data acquired for the POVM reconstruction are shown in fig. 5.2 (b). Values at time differences up to the pulse repetition time of 100 µs are due to dark counts or afterpulses. For an ideal detector with a constant dark count rate and without afterpulses and dead time, the dark counts would follow a homogeneous Poisson process with a constant rate λ. The histogram of times to the next dark count would then follow an exponential distribution $p_\lambda(t) = \lambda\,\mathrm{e}^{-\lambda t}$. For a detector with dead time, the histogram would be zero up to the dead time, where the exponential decay would start. However, in the measured histogram, an additional maximum in the count probability is visible, on top of the exponential decay, directly after the dead time. These counts are caused by afterpulses. An exponential fit for times between 40 to 100 µs is extrapolated to earlier times, showing the afterpulses (filled areas in fig. 5.2 (b)). The afterpulse probability p_{ap} is the sum of the counts in this area divided by the total number of counts in the histogram. The uncertainty of p_{ap} comes from choosing the fit range for the exponential decay. On the one hand, if the left bound of the fit range is too low, the tail of the afterpulse distribution distorts the fit, and the calculated afterpulse probability is too low. On the other hand, if the fit range starts too far apart from the afterpulses, the uncertainty in the extrapolation is high. The values and uncertainties in fig. 5.2 (b) were therefore calculated from two fits, starting from 30 and 50 µs and taking the mean. The afterpulse probabilities for all detectors are shown in fig. 5.3. The uncertainties for these values, calculated from the values acquired without the second EOAM, are larger than in fig. 5.2 (b). Without the second EOAM, the laser photons leaking through the first modulator cause a higher continuous photon flux, leading to a faster decay rate in the histogram, which increases the uncertainty of the fit.

5.3 Tomographic Reconstruction of POVMs

Two fundamentally different approaches to detailed descriptions of quantum detectors have been discussed in the literature: detailed modeling of all effects relevant to the detection process, and detector tomography. The first approach requires a thorough analysis of the relevant effects and inner workings of the detector. In contrast, the second approach makes only a few assumptions and reconstructs the measurement operator of the quantum detector from tomographic measurements with probe states [206–208].

In section 5.3.1, the POVM formalism and the concept of detector tomography for phase-insensitive detectors are briefly introduced. The time-dependent POVMs of the detectors are presented in section 5.3.2, and the detection efficiencies of the detectors are calculated. Section 5.3.3 presents the time-dependent POVMs.

5.3.1 Basic Principle of POVM Tomography for Phase-Insensitive Detectors

A quantum measurement is described by a set of measurement operators $\{\hat{M}_i\}$, with i labeling the different measurement results. When a quantum state $\hat{\rho}$ is measured, result i is obtained with probability $p_i(\hat{\rho})$. The state after a measurement yielding result i is $\hat{\rho}'_i$, given by [209]

$$\hat{\rho}'_i = \frac{\hat{M}_i \hat{\rho} \hat{M}_i^\dagger}{p_i(\hat{\rho})} \quad \text{and} \quad p_i(\hat{\rho}) = \langle \hat{\Pi}_i \rangle = \mathrm{tr}(\hat{\Pi}_i \hat{\rho}) \quad \text{with} \quad \hat{\Pi}_i = \hat{M}_i^\dagger \hat{M}_i \,. \tag{5.3}$$

When only the probabilities $p_i(\hat{\rho})$ are of interest, the explicit measurement operators M_i are not needed to describe the measurement and the operators $\hat{\Pi}_i$ are sufficient. From $p_i(\hat{\rho}) \geq 0$, it follows that the $\hat{\Pi}_i$ are Hermitian, positive semi-definite operators. The set $\{\hat{\Pi}_i\}$ is called a *positive operator-valued measure* (POVM) and the operators $\hat{\Pi}_i$ are called *POVM elements* [209]. From $\sum_i p_i(\hat{\rho}) = 1$ it follows their completeness relation

$$\sum_i \hat{\Pi}_i = \hat{\mathbb{1}} \,. \tag{5.4}$$

The SPDs used in the QKD system are single-photon avalanche diodes with no external phase reference. This means their representation in the optical phase space is rotationally symmetric around the origin, and the POVM elements are diagonal in the photon number basis [207, 208, 210]:

$$\hat{\Pi}_i = \sum_{k=0}^{\infty} \Theta_{ki} |k\rangle\langle k| \, . \tag{5.5}$$

The coefficients Θ_{ki} can be collected into the matrix $\boldsymbol{\Theta}$ for convenience.

When detection results for a tomographically complete set of input states, that is a set of states spanning the input Hilbert space of the detector, are available, the POVM itself can be reconstructed from the measurement results[6] [207, 208, 210].

Most realizations of quantum detector tomography focus on single-mode input states [208]. Examples are tomographic measurements and POVM reconstructions for avalanche photo diodes [207, 211], superconducting nanostrip detectors [212], transition edge sensors [213], time-multiplexed superconducting detectors [214], photon-number resolving detectors [215–217] and phase-sensitive detectors [218–220].

Attenuated laser light is much easier to produce in the laboratory than photon number states. From a practical point of view, it is, therefore, more convenient to perform the tomography in the (overcomplete) basis of coherent states $|\alpha\rangle$ than directly in the Fock basis [207, 208, 210]. The detection probabilities for the coherent states $|\alpha_j\rangle$ are

$$p_i(\alpha_j, \boldsymbol{\Theta}) = \sum_k C_{jk}\Theta_{ki} \quad \text{with} \quad C_{jk} = |\langle\alpha_j|k\rangle|^2 = \mathrm{e}^{-\mu_j}\frac{\mu_j^k}{k!} \quad \text{and} \quad \mu_j = |\alpha_j|^2 \, . \tag{5.6}$$

In principle, photon numbers k and mean photon numbers μ_j up to infinity need to be taken into account, but for practical numerical implementations, both values need to be truncated at some values $k_{\max}$ and $j_{\max}$. Furthermore, the probabilities $p_i(\alpha_j, \boldsymbol{\Theta})$ are not directly available from the experiment. Instead, they are approximated by the count frequency obtained by repeatedly sending light pulses into the detector. When the state $|\alpha\rangle$ is sent $N(\alpha_j)$ times, $n(\alpha_j)$ counts are observed and the probabilities $p_i(\alpha_j, \boldsymbol{\Theta})$ are approximated by the count frequency $f_i(\alpha_j) = n_i(\alpha_j)/N_i(\alpha_j)$, which are collected into the matrix $\boldsymbol{F}$. After switching into the dead time, the detector is considered active when a time longer than the set dead time plus two microseconds has passed since the last count. Equation (5.6) can then be approximated with the measured count frequencies and written in matrix notation as [207, 208]

$$\boldsymbol{F}_{j_{\max}\times i_{\max}} = \boldsymbol{C}_{j_{\max}\times(k_{\max}+1)}\boldsymbol{\Theta}_{(k_{\max}+1)\times i_{\max}} \, , \tag{5.7}$$

[6] The title of ref. [207] felicitously describes the tomography of detector POVMs as *"Measuring Measurement"*.

with $\boldsymbol{C}$ having $k_{\max} + 1$ columns for $|0\rangle$ to $|k_{\max}\rangle$. The POVM elements are obtained by solving eq. (5.7) for $\boldsymbol{\Theta}$. In general, $\boldsymbol{C}$ is not a square matrix, such that it is not invertible, and eq. (5.7) cannot be solved directly. However, solutions can be found by minimizing $\|\boldsymbol{F} - \boldsymbol{C}\boldsymbol{\Theta}\|_{\mathrm{F}}$[7] [207, 208]. To obtain meaningful results, the numerical optimization needs to be regularized [221], for example, by adding a quadratic regularization term [207, 208]

$$r \sum_{k,i} (\Theta_{k+1,i} - \Theta_{k,i})^2 \,, \tag{5.8}$$

with a *regularization coefficient* r. Regularization is required to avoid that noise in the measurements leads to irregularities in the reconstructed POVMs [207], but it biases the optimization. Therefore, r must be chosen to obtain an acceptable trade-off between well-behaved and unduly biased optimization results. One possible solution is to scan r over a range of values and to select a value for which a smooth distribution of POVM values is obtained, which is relatively insensitive to changes of r [207, 208].

For time-dependent tomography, the statistical data quality, given by the number of recorded counts per time bin, varies as a function of the time bin. This would require a manually chosen individual regularization coefficient for each time bin, which is inconvenient. A more systematic approach proposed by Robin Krebs in his bachelor's thesis is to adapt the strength of the regularization parameter to the data quality by considering the regularization term as a Bayesian prior distribution in a maximum-likelihood optimization [B3]. Based on these considerations, an adaptive expression for r was derived that decreases when $N(\alpha_j)$ grows, taking into account that higher numbers of repetitions yield more reliable statistics. This adaptive expression for r is one of the major results in ref. [III]. The importance of the regularization term and the disadvantages of static regularization terms independent of the statistical measurement uncertainty are demonstrated in a benchmarking of different regularization techniques presented in ref. [III].

Using the adaptive coefficient r, the objective function to be minimized for each time bin individually becomes

$$S(\boldsymbol{\theta}) = \|(\boldsymbol{f} - \boldsymbol{C}\boldsymbol{\theta})\|_2^2 + r \sum_k (\theta_{k+1} - \theta_k)^2 \quad \text{with} \quad r = k_{\max}^2 \max_j \left(\frac{f(\alpha_j)[1 - f(\alpha_j)]}{N(\alpha_j)} \right) . \tag{5.9}$$

The detailed derivation of the expression for r is presented in ref. [III]. For the non-PNR detectors, it is sufficient to consider only the "no-count" POVM elements

$$\hat{\Pi}_{\text{no count}} = \theta_0 |0\rangle\langle 0| \,. \tag{5.10}$$

[7] The Frobenius norm of some matrix $\boldsymbol{M}$ is given by $\|\boldsymbol{M}\|_{\mathrm{F}} = \left(\sum_{i,j} |M_{ij}|^2\right)^{1/2}$.

The element for a count is simply given by $\hat{\Pi}_{\text{count}} = \hat{\mathbb{1}} - \hat{\Pi}_{\text{no count}}$. Therefore $i = i_{\max} = 1$, such that the matrices $\boldsymbol{F}$ and $\boldsymbol{\Theta}$ from eq. (5.7) become vectors $\boldsymbol{f}$ and $\boldsymbol{\theta}$ in eq. (5.9).

5.3.2 Time-Independent POVMs

The detection efficiency of the SPDs can be deduced from the time-independent POVMs. Data to reconstruct these POVMs were acquired with the setup described in section 5.1. The total mean photon number per pulse μ was scanned from 0 to $\mu_{\max} = 50$ in steps of 2, and counts were recorded over 10 min measurement time per μ value. The values for $f(\alpha_j)$ are obtained by summing up the counts occurring in a 8 ns wide window around the pulse center and dividing the number by the number of laser pulses. Only those pulse cycles and counts are considered in which the detector is not in the dead time.

For the POVM reconstruction, a value for $k_{\max}$ must be chosen. It should be higher than $\mu_{\max}$ because a coherent state with mean photon number $\mu_{\max}$ has significant contributions from photon number states with $k > \mu_{\max}$. If $k_{\max}$ is chosen too low, the reconstructed POVM will show artifacts from the cutoff. For the implementation, the value $k_{\max} \approx \mu_{\max} + 2\sqrt{\mu_{\max}} \approx 65$, that is $\mu_{\max}$ plus two standard deviations of the Poisson distribution, was chosen, such that $C_{j_{\max}k_{\max}} \leq 1\,\%$.

To reconstruct the time-independent POVMs, eq. (5.9) was minimized numerically over $\boldsymbol{\theta}$. To facilitate the convergence of the minimization and to avoid numerical artifacts, the gradient of eq. (5.9) was implemented explicitly.

The time-independent POVMs were reconstructed for all eight SPDs at the different setting combinations. As an example, the measured no-count probabilities and the reconstructed POVM for SPD-2 are shown in fig. 5.4. For an ideal detector with efficiency η, the expected "no-count" probabilities for k incident photons and for a coherent state $|\alpha\rangle$ are given by

$$p_{\text{no count}}\big(|k\rangle\big) = \langle k|\hat{\pi}_{\text{no count}}|k\rangle = (1-\eta)^k \quad \text{and} \quad p_{\text{no count}}\big(|\alpha\rangle\big) = \langle \alpha|\hat{\pi}_{\text{no count}}|\alpha\rangle = \mathrm{e}^{-\eta\mu}. \tag{5.11}$$

The measured "no-count" probabilities match the expectation for an ideal detector. An exponential fit to the data in fig. 5.4 (a) yields the efficiency $\eta = 16.9\,\%$. However, for values above $\mu = 30$, the logarithmic plot shows that the "no-count" probability approaches a plateau of around 2.7×10^{-3}, meaning that the detector does not yield a count with this small probability even when μ is further increased. A similar effect can be observed for the reconstructed "no-count" POVMs in fig. 5.4 (b). Here, the curves for an ideal detector were calculated with the fitted efficiency $\eta = 16.9\,\%$ from fig. 5.4 (a).

Detection Efficiency

One of the most important figures characterizing an SPD is the detection efficiency η. One option to derive η from the measured data is to extract it from the exponential fit

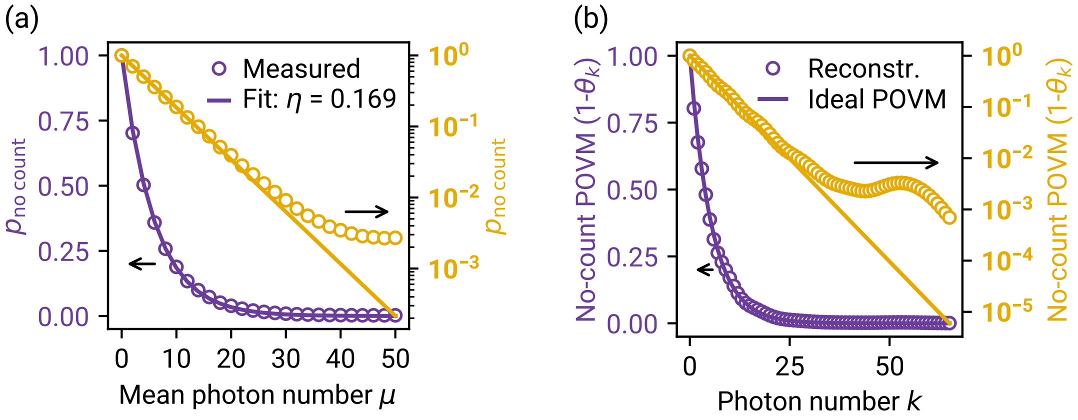


Figure 5.4: Time-independent tomography of SPD-2 for $\eta = 15\,\%$ and $\tau_{\text{dead}} = 10\,\mu\text{s}$ compared to an ideal detector (cf. eq. (5.11)). (a) Measured no-count probability for coherent wave packets with mean photon numbers μ and expectation $p_{\text{no count}}(|\alpha\rangle) = \mathrm{e}^{-\mu}$ for an ideal detector. (b) Reconstructed no-count POVMs and expectation $p_{\text{no count}}(k \text{ photons}) = (1-\eta)^k$. Both diagrams show the data in linear (left axis) and logarithmic (right axis) scale .

to $p_{\text{no count}}(|\alpha\rangle)$. Another option is to take the POVM element for one photon. Figure 5.5 shows the values obtained by using both methods for all eight[8] detectors. Additionally, the POVM values θ_1 obtained with a 100 times stronger regularization are shown. The measurement uncertainties are dominated by the accuracy to which μ is known. Systematic relative uncertainties of the values of 5 % are introduced by the photodetector used for the power calibration, and another 10 % are introduced by loss variations in the fiber-fiber connections in the setup. The variation between repeated measurements of the same detector was 8 %.

The efficiency values match the nominal set values and are generally slightly higher. Remarkably, reasonable POVMs are even obtained with the much larger regularization coefficient, and the efficiencies obtained this way are closer to the values obtained from the exponential fit for most detectors. A similar insensitivity to the regularization coefficient has been observed in ref. [207], indicating that using eq. (5.9) to calculate the adaptive regularization parameter should be understood as a rule-of-thumb and larger or smaller values may also lead to reasonable results.

[8] In ref. [III], efficiencies for only seven detectors are shown because SPD-5 was under repair when the data were measured. The data for SPD-5 were acquired after the detector returned from repair.

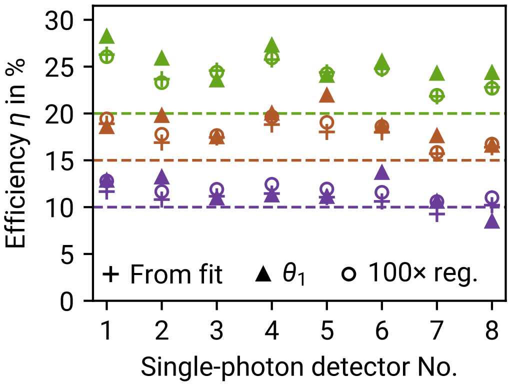


Figure 5.5: Efficiencies η of SPDs computed from an exponential fit to $p_{\text{no count}}$, from the first POVM element θ_1 using the regularization coefficient r, and from θ_1 with 100 times stronger regularization.

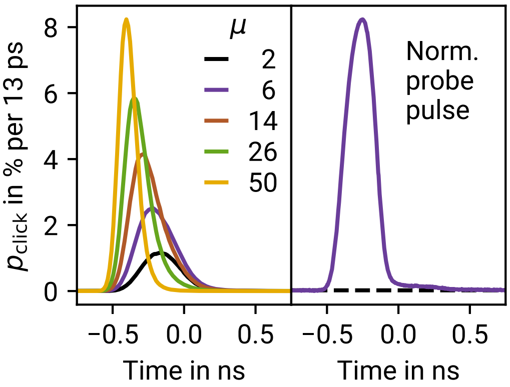


Figure 5.6: Time-dependent count probability of SPD-2 (left) in 13 ps wide time bins with $\eta = 15\,\%$ and $\tau_{\text{dead}} = 10\,\mu\text{s}$ for different values of μ and normalized probe pulse shape (right) with a FWHM of 242 ps.

5.3.3 Time-Dependent POVMs

The time resolution of the measured data allows to reconstruct the time-dependent POVMs characterizing the temporal distribution of the detector counts. The probe pulse shape and the resulting count histograms are shown in fig. 5.6 for a number of μ values. The count distribution becomes higher and narrower for increasing values of μ, and the maximum shifts to earlier times. At $\mu = 50$, the distribution is even narrower than the probe pulse. This effect is a consequence of the dead time. For pulses with high μ, a photon is with high probability detected early within the pulse, and due to the dead time, the further photons in this pulse cannot be detected. This effect is expected to become relevant for μ values above $\eta\mu \approx 1$ when a detector without dead time would often register multiple photons per pulse. The complete measured count distributions are shown in fig. 5.7 (a). The count distributions from fig. 5.6 are horizontal crosssections through this distribution.

To systematically include the time dependence into POVMs, eq. (5.5) is naturally extended to a probability density $p_{\text{count}}(t, \hat{\rho}) = \operatorname{tr}\big(\hat{\rho}\,\hat{\Pi}_{\text{count}}(t)\big)$. A time-dependent POVM can then be written as [III]

$$\hat{\pi}_{\text{count}}(t) = \mathcal{T} \sum_{k=0}^{\infty} \int_{\mathbb{R}^k} p_{\text{count},\,k}(t, \boldsymbol{\tau}_k) |\boldsymbol{\tau}_k\rangle\langle\boldsymbol{\tau}_k| \; \mathrm{d}\boldsymbol{\tau}_k \quad \text{with} \quad |\boldsymbol{\tau}_k\rangle = \bigotimes_{j=1}^{k} \hat{a}^\dagger(\tau_j)|0\rangle\,, \quad (5.12)$$

with the arrival times $\boldsymbol{\tau}_k = \{\tau_1, ..., \tau_k\}$ of k photons at the detector. Time ordering $\tau_1 < \tau_2 < \cdots < \tau_k$ is ensured by the time ordering operator $\mathcal{T}$. The probability density

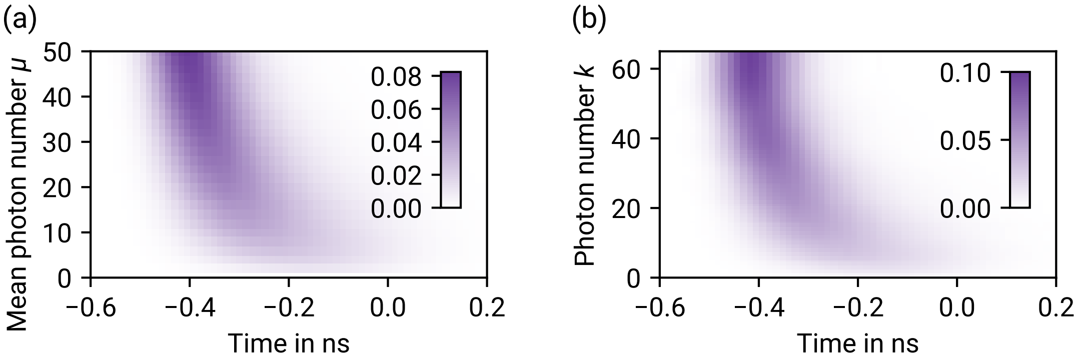


Figure 5.7: Time-dependent tomography of SPD-2 for $\eta = 15\,\%$ and τ_{dead} =10 µs. (a) Measured count probability as a function of the mean photon number μ of the probe pulse. (b) Count POVMs reconstructed by using adaptive regularization.

$p_{\text{count},\,k}(t, \boldsymbol{\tau}_k)$ describes how likely it is that a state with k photons at times $\tau_1, \ldots, \tau_k$ causes a count in the time interval $[t, t + \mathrm{d}t]$. For a time interval I, the POVM is again time-independent and given by $\hat{\Pi}_{I,\,\text{count}} = \int_I \hat{\pi}_{\text{count}}(t)\,\mathrm{d}t$ [203].

For the numerical POVM reconstruction it is convenient to split the integral in eq. (5.12) into time bins of width Δt for $i = 1, \ldots, i_{\max}$, such that the POVM consists of $i_{\max} + 1$ elements, one for a count in each time bin and one for no count in any time bin. By restricting the general time-dependent POVM from eq. (5.12) to the particular probe pulse shape shown in fig. 5.6, the time-dependent POVM can be expressed as in eq. (5.5), where a count in a specific time bin represents one detection result i. The time-dependent POVMs were then reconstructed by minimizing eq. (5.9) for each time bin individually with optimization bounds, ensuring physically reasonable results between 0 and 1. The reconstructed time-dependent POVMs are shown in fig. 5.7 (b). Similar to the count probabilities, the maximum of the distribution shifts for higher values of k to earlier times.

5.4 Test of a Timing Jitter Model

In ref. [203], Gouzien et al. proposed a POVM model for non-PNR detectors with dead time that is a special case of eq. (5.12), meaning that it assumes a specific function $p_{\text{count},\,k}(t, \boldsymbol{\tau}_k)$ in eq. (5.12). As discussed above, due to the dead time, only the first of multiple possible counts that a pulse could cause is registered. The model from ref. [203] formalizes this effect. In the following, the measured data will be used to check the validity of the model for the tested SPDs.

The model assumes that the detectors have an intrinsic timing jitter distribution $J(T)$, such that $J(t-\tau)\,\mathrm{d}t$ is the probability that a single photon arriving at τ yields a count in the interval $[t, t+\mathrm{d}t]$. Causality is ensured by $J(T<0)=0$. Further model assumptions are that the detector is deactivated directly after the first count and that it remains in the dead time for the rest of the pulse duration. The probability $p_{\mathrm{count}}(t, \boldsymbol{\tau}_k)$ in the time-dependent POVM eq. (5.12) thereby becomes [203]

$$p_{\mathrm{count}}(t, \boldsymbol{\tau}_k) = \sum_{j=1}^{k} p_1(t, \tau_j) \prod_{\substack{l=1 \\ l\neq j}}^{k} p_{1,\mathrm{not}}(t, \tau_l)\,. \tag{5.13}$$

Here, $p_1(t,\tau) = \eta J(t-\tau)$ and $p_{1,\mathrm{not}}(t,\tau) = 1-\eta \int_\tau^t J(t'-\tau)\,\mathrm{d}t'$ are the probabilities that a single photon at τ causes a count at t and that a single photon has not caused a count up to time t, respectively [203]. Equation (5.13) is the sum of the probabilities for each of the k photons to be the first photon to cause a count at t and that none of the other photons has caused a count before τ_j.

The count probability density p_{wp} for a continuous-mode probe pulse wave packet predicted by this model can be compared to the time-dependent tomographic data. The formal derivation presented in the appendix of ref. [III] yields

$$p_{\mathrm{wp}}(t) = -\frac{\partial}{\partial t} \exp\!\left(-\int_{-\infty}^{t} \lambda(t')\,\mathrm{d}t'\right) \quad \text{with} \quad \lambda(t) = \eta\left(J * |\alpha|^2\right)(t)\,. \tag{5.14}$$

This equation is the probability density of the time to the first count for an inhomogeneous Poisson process with a time-dependent count rate $\lambda(t)$. This rate is given by the time-dependent photon flux $|\alpha(t)|^2$ of the probe pulse (cf. fig. 5.6) convolved with the detector jitter distribution $J(t)$. The reason for this structure can also be understood intuitively: independent detections of photons from a coherent wave packet yield a Poisson process, which is modified by the jitter distribution. A detector without dead time could register multiple counts per pulse, but a detector with dead time registers only the first of these counts. Therefore, $p_{\mathrm{wp}}(t)$ is given by the time to the first count of the Poisson process. The detector count distribution according to the model is completely characterized by the count rate $\lambda(t)$, from which the jitter distribution can be obtained by deconvolution. To reconstruct $\lambda(t)$ the cumulative rate $\Lambda(t) = \int_{-\infty}^{t} \lambda(t')\,\mathrm{d}t'$ is defined. Integrating eq. (5.14) and using $\Lambda(t\to-\infty)=0$ yields $\int_{-\infty}^{t} p_{\mathrm{wp}}(t')\,\mathrm{d}t' = 1-\mathrm{e}^{-\Lambda(t)}$, such that $\Lambda(t) = -\ln\!\left(1-\int_{-\infty}^{t} p_{\mathrm{wp}}(t')\,\mathrm{d}t'\right)$. Differentiation yields the expression

$$\lambda(t) = \frac{\mathrm{d}\Lambda(t)}{\mathrm{d}t} = -\frac{\mathrm{d}}{\mathrm{d}t} \ln\!\left(1-\int_{-\infty}^{t} p_{\mathrm{wp}}(t')\,\mathrm{d}t'\right) = \frac{p_{\mathrm{wp}}(t)}{1-\int_{-\infty}^{t} p_{\mathrm{wp}}(t')\,\mathrm{d}t'}\,. \tag{5.15}$$

Calculating $\lambda(t)$ by eq. (5.15) only requires the measured count distribution $p_{\mathrm{wp}}(t)$ and requires neither knowledge about the detector efficiency η nor about the mean photon number μ. For the numerical deconvolution, the normalized discrete pulse shape $\boldsymbol{I}$ with $I_i = |\alpha(t_i)|^2/\mu$ and the normalized discrete count rate $\boldsymbol{\lambda} = \lambda_i = \lambda(t_i)/(\eta\mu)$ are defined. By introducing the Toeplitz matrix $\boldsymbol{T}$ constructed from $\boldsymbol{I}$, the discrete convolution becomes $\boldsymbol{\lambda} = (\boldsymbol{I} * \boldsymbol{J}) = \boldsymbol{T}\boldsymbol{J}$. To deconvolve $\boldsymbol{J}$ from $\boldsymbol{\lambda}$, $\|\boldsymbol{\lambda} - \boldsymbol{T}\boldsymbol{J}\|_2^2$ was minimized over $\boldsymbol{J}$. Writing the discrete convolution as a multiplication by a Toeplitz matrix enables the implementation of the gradient $\nabla_{J}\|\boldsymbol{\lambda} - \boldsymbol{T}\boldsymbol{J}\|_2^2 = 2\boldsymbol{T}^{\mathsf{T}}(\boldsymbol{T}\boldsymbol{J} - \boldsymbol{\lambda})$, which facilitates the convergence of the minimization. To obtain meaningful and smooth results, the optimization constraint $\boldsymbol{J}_i \geq 0$ for all i and a regularization term $\sum_i (J_{i+1} - J_i)^2$ penalizing strong variations of the first derivative, weighted by a regularization coefficient, was added. Therefore, the resulting objective function to be minimized is very similar to eq. (5.9).

Figure 5.8 shows the normalized discrete count rate $\boldsymbol{\lambda}$ and the discrete jitter distribution $\boldsymbol{J}$ obtained by deconvolution of the pulse shape for SPD-2. The count rate varies as a function of μ, shifting the maximum towards earlier times, and the same effect is visible in the deconvolved jitter distribution. The width of the jitter distribution at the base is approximately 500 ps. A very similar course was observed for the other detectors. Although the jitter rate model from ref. [203] includes the effect of the maximum shifting to earlier times due to the dead time as discussed in section 5.3.3, at least a part of the observed shift is not explained by the model. One possible reason is that the model assumes the independence of the count rate and jitter distribution of μ, which may not be the case.

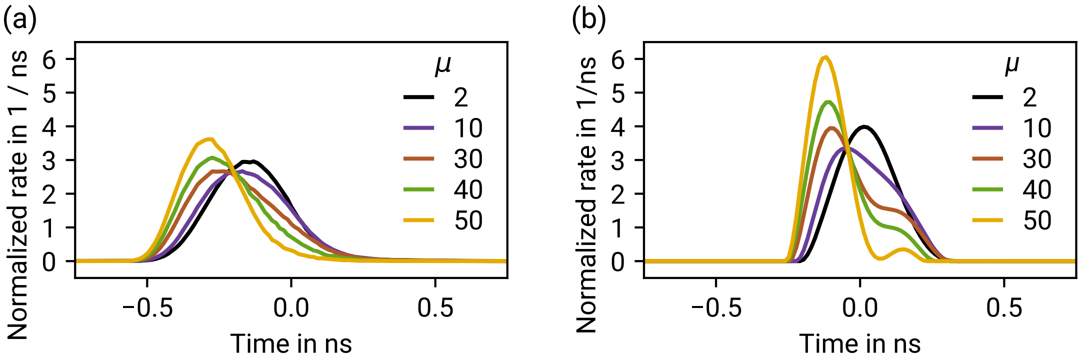


Figure 5.8: Count rates according to the jitter rate model from ref. [203] for SPD-2 operated at $\eta = 15\,\%$ set efficiency and $\tau_{\mathrm{dead}} = 10\,\mu\mathrm{s}$ dead time. (a) Normalized discrete count rate $\boldsymbol{\lambda}$ calculated from the measured data via eq. (5.15). (b) Normalized jitter distribution $J(T)$ obtained by deconvolving the probe pulse shape from $\boldsymbol{\lambda}$.

In ref. [III], a rigorous statistical analysis of the validity of the jitter rate model compared to the measured time-dependent POVM is presented. It confirms that the jitter rate model is insufficient to describe the time-dependent count distribution of the tested detectors completely.

A possible root cause for the deviation could be the violation of the assumption that photons are registered independently, which is implied by the multiplication of the probabilities in eq. (5.13). In the tested SPDs, photons trigger electron avalanches, and an electric count pulse is emitted when the avalanche current reaches a certain threshold level. The timing jitter distribution of such detectors is mainly determined by the distribution of charge carrier transit times in the absorption region and by the distribution of the avalanche build-up time in the multiplication region [222]. This means that avalanches triggered by multiple photons can add up, such that the current threshold is reached faster than for independent detections of the photons. Therefore, this effect is expected to shift the maximum of the distribution to earlier times, more than predicted by the jitter rate model.

Summary of Chapter 5

In this chapter, the single-photon detectors employed in the q-hub QKD system were thoroughly analyzed. All eight detectors were characterized by sending coherent probe pulses with a known mean photon number into the detectors and recording the times of the detector counts. The dark count rates, dead times, and afterpulse probabilities were calculated from these data. The results are used to model the detectors in the simulations presented in chapters 6 and 7. Time-independent *positive operator-valued measures* (POVMs) for the detectors were reconstructed from which the detection efficiencies were derived, and time-dependent POVMs were reconstructed from the time-dependent count distributions. For that, a new method was developed to adapt the coefficient determining the strength of the regularization to the statistical quality of the measured data.

Furthermore, the measured time-dependent count probabilities were compared to the predictions of a POVM model from the literature, taking into account the detector dead time and timing jitter. The observed deviations of the data from the model predictions are likely due to the violation of a model assumption. This example shows that measuring time-dependent detector POVMs can reveal additional information about effects in a detector that simplifying models do not consider. The results of this chapter were published in ref. [III].

6 Simulating the Photon Statistics of Multi-Mode Gaussian States by Automatic Differentiation of Generating Functions

This chapter summarizes the most important results of publication [VI], in which a new photon-number-resolved method for simulating quantum-optical setups is presented and applied to simulate the multi-user QKD network. In contrast to the simulation presented in chapter 7, this QKD simulation does not resolve the photon spectrum, significantly simplifying the implementation. The simulation method consists of three steps: modeling the setup using the *covariance formalism*, constructing a *generating function* for the photon statistics, and using *automatic differentiation* (AD) software to retrieve the photon statistics from the generating function. The method enables computing the photon number distribution, cumulative probabilities, moments, and factorial moments of the photon statistics for the relevant class of optical quantum states called *Gaussian states* (GSs). Furthermore, relevant effects in real setups, such as noise, non-unity detection efficiencies, and the simultaneous detection of multiple modes by the same detector, are easily incorporated. This versatility is the most crucial strength of the method. It comes at the price of requiring more computing resources than highly optimized algorithms for computing photon number distributions.

A simulation of the q-hub network not capable of resolving the photon statistics was implemented by Florian Niederschuh during his bachelor's thesis [B5]. Afterwards, the method to simulate the photon statistics was developed. Functionalities to simulate *photon-number-resolved* (PNR) detection were implemented by Florian Niederschuh for the demonstration of the simulation method in publication [VI]. An implementation example using the *PyTorch* framework has been published in the technical report ref. [IV].

Section 6.1 briefly reviews generating functions for probability distributions and the covariance formalism. In section 6.2, the generating functions for the photon statistics of multi-mode GSs are derived. Alternative methods to compute photon number distributions are discussed. In section 6.3, the method is applied to simulate the multi-user QKD network. The simulation results for quantum key rates and QBERs agree with measurements, showing that the simulation describes the q-hub network accurately.

6.1 Basic Mathematical Tools

This section reviews essential mathematical tools for simulating the q-hub system.

Generating functions allow to represent the probability distribution of sums of random variables efficiently. They are widely used in various disciplines, such as combinatorics, probability theory, and engineering. Their mathematical properties and applications are extensively discussed in the literature, such as refs. [223, 224]. The most relevant properties of generating functions are briefly introduced in section 6.1.1. These properties are the reason for the great flexibility of the simulation method presented in this chapter. They enable considering detection noise and the joint detection of multiple modes in the same detector in a straightforward way.

Gaussian states (GSs) are quantum states generated by Hamiltonians with a linear or quadratic dependence on the creation and annihilation operators. Many of the most common photonic quantum states are GSs, such as the vacuum state, coherent states, squeezed states, two-mode squeezed vacuum, or thermal states. Furthermore, common elements in optical setups, such as beam splitters, phase shifters, or losses, are described by transformations mapping GSs to other GSs. GSs are characterized by a *covariance matrix* and a *displacement vector*, which carry the complete information about the photon statistics of the states. The covariance formalism is therefore well suited for theoretical investigations and has been extensively discussed in the context of quantum information in various publications [100, 225–228]. The formalism is also well-suited for practical simulations of GSs in complex optical setups because the required matrix operations representing state transformations can be efficiently implemented in software. In ref. [101], the use of the formalism for simulations of quantum-optical setups with non-PNR detectors is demonstrated, and in ref. [229], the formalism is advocated as a general framework for multi-mode Gaussian quantum optics. The most relevant features of the covariance formalism are summarized in section 6.1.2.

6.1.1 Generating Functions for Probability Distributions

> *A generating function is a device somewhat similar to a bag. Instead of carrying many little objects detachedly, which could be embarrassing, we put them all in a bag, and then we have only one object to carry, the bag.*
>
> George Pólya, 1954
> in: Mathematics and Plausible Reasoning, Volume I., Chapter VI. [230]

Generating functions compactly represent an infinite sequence of numbers as the coefficients of a power series in some parameter y. For a discrete random variable N attaining non-negative integer values $n \in \mathbb{N}_0$, the probabilities $p(N = n)$ are such a sequence of numbers. They can be collected by interpreting them as the coefficients of a power series called the *probability-generating function* (PGF) [224]:

$$h(y) = \sum_{n=0}^{\infty} p(N = n) y^n = \left\langle y^N \right\rangle . \tag{6.1}$$

The probabilities can be retrieved from a given PGF by repeatedly differentiating it and evaluating it at $y = 0$ [224]:

$$p(n) = \frac{1}{n!} \frac{\mathrm{d}^n}{\mathrm{d}y^n} h(y) \bigg|_{y=0} . \tag{6.2}$$

Similarly, the mean value of the distribution can be obtained by [224]

$$\langle N \rangle = \sum_{n=0}^{\infty} p(n)\, n = \frac{\mathrm{d}\, h(y)}{\mathrm{d}y} \bigg|_{y=1} . \tag{6.3}$$

Related functions generate further quantities characterizing the probability distribution:

The cumulative probabilites $p(N \leq n)$ are generated by $h(y)/(1 - y)$ [224], which can be shown by using the geometric series (cf. eq. (A.17)):

$$\frac{h(y)}{1 - y} = \sum_{n=0}^{\infty} p(N = n) y^n \sum_{k=0}^{\infty} y^k , \tag{6.4}$$

$$p(N \leq n) = \sum_{k=0}^{n} p(k) = \frac{1}{n!} \frac{\mathrm{d}^n}{\mathrm{d}y^n} \frac{h(y)}{1 - y} \bigg|_{y=0} . \tag{6.5}$$

The moments $\mathcal{M}(k,\mu) = \left\langle (N-\mu)^k \right\rangle$ of the probability distribution are generated by the *moment-generating function* [224] related to the exponential series (cf. eq. (A.16)):

$$M(\mu, y) = \left\langle \mathrm{e}^{(N-\mu)y} \right\rangle = \sum_{n=0}^{\infty} p(n)\,\mathrm{e}^{(n-\mu)y} = \sum_{k=0}^{\infty} \frac{y^k}{k!} \left\langle (N-\mu)^k \right\rangle, \tag{6.6}$$

$$\mathcal{M}(k,\mu) = \frac{\mathrm{d}^k}{\mathrm{d}y^k} M(\mu, y)\bigg|_{y=0}. \tag{6.7}$$

The two most important types of moments are the *raw moments* $\langle N^k \rangle$ and the *central moments* $\left\langle (N - \langle N \rangle)^k \right\rangle$. An important example for the central moments is the variance $\sigma^2 = \left\langle (N - \langle N \rangle)^2 \right\rangle$. Closely related to the moment-generating function is the *characteristic function*

$$\chi(y) = M(0, \mathrm{i}y) = \left\langle \mathrm{e}^{\mathrm{i}yN} \right\rangle. \tag{6.8}$$

The falling factorial moments $n_{(k)} = \langle N_{(k)} \rangle = \langle N(N-1)\cdots(N-k+1) \rangle$ [231–233] are generated by $\left\langle (1+y)^N \right\rangle$, which can be shown by using the binomial theorem from eq. (A.18):

$$h(1+y) = \sum_{n=0}^{\infty} p(n)(1+y)^n = \sum_{n=0}^{\infty} p(n) \sum_{k=0}^{n} y^k \binom{n}{k} = \sum_{k=0}^{\infty} \frac{y^k}{k!} \langle N_{(k)} \rangle, \tag{6.9}$$

$$n_{(k)} = \frac{\mathrm{d}^k}{\mathrm{d}y^k} h(1+y)\bigg|_{y=0}. \tag{6.10}$$

The rising factorial moments $n^{(k)} = \left\langle N^{(k)} \right\rangle = \langle (N+1)\cdots(N+k) \rangle$ [234, 235] are generated by the *rising-factorial moment-generating function* $R(y)$ related to the negative binomial series (cf. eq. (A.19)):

$$R(y) = \sum_{k=0}^{\infty} \frac{y^k}{k!} \sum_{n=0}^{\infty} p(n) \frac{(n+k)!}{n!} = \sum_{n=0}^{\infty} \frac{p(n)}{(1-y)^{n+1}} = \frac{1}{1-y} \left\langle (1-y)^{-N} \right\rangle, \tag{6.11}$$

$$n^{(k)} = \frac{\mathrm{d}^k}{\mathrm{d}y^k} R(y)\bigg|_{y=0}. \tag{6.12}$$

Expressing multivariate probability distributions by multivariate generating functions is straightforward. For example, the PGF $h(y_1, y_2) = \sum_{n_1,n_2} p(n_1, n_2) y_1^{n_1} y_2^{n_2}$ generates the bivariate probability distribution $p(n_1, n_2)$.

One of the most important strengths of generating functions is the efficient way to represent the probability distribution of a sum of random variables. For two random variables N_1 and N_2 with probability distributions $p_1(N_1 = n_1)$ and $p_2(N_2 = n_2)$, the sum of the random variables follows the probability distribution

$$p(N_1 + N_2 = n) = \sum_{m=0}^{n} p_2(m) p_1(n-m)\,. \tag{6.13}$$

This probability distribution is the convolution of the individual probability distributions. Its PGF can be rewritten by using Cauchy's product formula as [223, 224]

$$h(y) = \sum_{n=0}^{\infty}\sum_{m=0}^{n} y^m p_2(m) y^{n-m} p_1(n-m) = \left(\sum_{k=0}^{\infty} y^k p_1(k)\right)\left(\sum_{l=0}^{\infty} y^l p_2(l)\right) = h_1(y)h_2(y)\,. \tag{6.14}$$

This means the PGF for a sum of random variables is the product of the PGFs of the individual random variables. Similarly, the moment and rising-factorial moment-generating functions for a sum of random variables are the products of the individual generating functions. For the cumulative probabilities and rising factorial moments of a sum of random variables, the product of the power series is multiplied by the prefactor $1/(1-y)$ only once, not for each of the individual generating functions.

6.1.2 The Covariance Formalism of Gaussian States

A photonic state with S orthogonal modes can be described by introducing S pairs of creation and annihilation operators $\hat{a}_s^\dagger$ and $\hat{a}_s$ for $s = 1 \dots S$ with commutator relations $[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{ij}$. Based on $\hat{a}_s$ and $\hat{a}_s^\dagger$, the quadrature operators

$$\hat{x}_s = \frac{1}{\sqrt{2}}\left(\hat{a}_s + \hat{a}_s^\dagger\right) \quad \text{and} \quad \hat{p}_s = \frac{1}{\mathrm{i}\sqrt{2}}\left(\hat{a}_s - \hat{a}_s^\dagger\right) \tag{6.15}$$

can be defined. It is convenient to collect the operators into vectors:

$$\hat{\boldsymbol{a}} = (\hat{a}_1, \dots, \hat{a}_S)^\mathsf{T}\,, \quad \hat{\boldsymbol{a}}^\dagger = (\hat{a}_1^\dagger, \dots, \hat{a}_S^\dagger)\,, \quad \hat{\boldsymbol{x}} = (\hat{x}_1, \dots, \hat{x}_S)^\mathsf{T}\,, \quad \hat{\boldsymbol{p}} = (\hat{p}_1, \dots, \hat{p}_S)^\mathsf{T}\,. \tag{6.16}$$

For the sake of a more compact notation, these are combined into even larger vectors[1]

$$\hat{\mathfrak{a}} = \begin{pmatrix} \hat{\boldsymbol{a}} \\ (\hat{\boldsymbol{a}}^\dagger)^\mathsf{T} \end{pmatrix} \quad \text{and} \quad \hat{\mathfrak{q}} = \begin{pmatrix} \hat{\boldsymbol{x}} \\ \hat{\boldsymbol{p}} \end{pmatrix}\,. \tag{6.17}$$

[1] In this notation, the Hermitian adjoint of a vector is obtained by transposing the outer vector and taking the Hermitian adjoint of the elements. For example, the Hermitian adjoint of $\hat{\mathfrak{a}}$ is $\hat{\mathfrak{a}}^\dagger = (\hat{\boldsymbol{a}}^\dagger, \hat{\boldsymbol{a}}^\mathsf{T}) = (\hat{a}_1^\dagger, \dots, \hat{a}_S^\dagger, \hat{a}_1, \dots, \hat{a}_S)$.

The relation between the $\hat{\mathfrak{a}}$-basis and the $\hat{\mathfrak{q}}$-basis from eq. (6.15) can thereby be written as

$$\hat{\mathfrak{q}} = \boldsymbol{\Omega}\hat{\mathfrak{a}} \quad \text{with} \quad \boldsymbol{\Omega} = \frac{1}{\sqrt{2}}\begin{pmatrix} \mathbb{1} & \mathbb{1} \\ -\mathrm{i}\mathbb{1} & \mathrm{i}\mathbb{1} \end{pmatrix}. \tag{6.18}$$

The basis-changing 2×2 blockmatrix $\boldsymbol{\Omega}$ is unitary, with $\mathbb{1}$ denoting the $S \times S$ identity.

The *characteristic function*[2] of an operator $\hat{O}$ for $\hat{x}$ and $\hat{p}$ depends on $2S$ real arguments collected into the vector $\boldsymbol{\xi}^\mathsf{T} = \left(\boldsymbol{\xi}_x^\mathsf{T}, \boldsymbol{\xi}_p^\mathsf{T}\right) = (\xi_{x_1} \ldots \xi_{x_S}, \xi_{p_1} \ldots \xi_{p_S})$:

$$\chi_{\hat{O}}(\boldsymbol{\xi}) = \mathrm{tr}\left[\hat{O} \exp\left(\mathrm{i}\boldsymbol{\xi}^\mathsf{T} \hat{\mathfrak{q}}\right)\right]. \tag{6.19}$$

The expectation values of an operator $\hat{O}$ with respect to a state $\hat{\rho}$ can be calculated by integrating the product of the characteristic functions of the state and the operator [100, 101]:

$$\langle \hat{O} \rangle = \mathrm{tr}\left(\hat{\rho}\hat{O}\right) = \frac{1}{(2\pi)^S} \int_{\mathbb{R}^{2S}} \chi_{\hat{\rho}}(\boldsymbol{\xi}) \chi_{\hat{O}}(-\boldsymbol{\xi}) \, \mathrm{d}\boldsymbol{\xi} \,. \tag{6.20}$$

Gaussian states (GSs) are states with a Gaussian characteristic function [100, 101, 226–228]

$$\chi_{\hat{\rho}}(\boldsymbol{\xi}) = \mathrm{tr}\left[\hat{\rho} \exp\left(\mathrm{i}\boldsymbol{\xi}^\mathsf{T} \hat{\mathfrak{q}}\right)\right] = \exp\left(-\frac{1}{4}\boldsymbol{\xi}^\mathsf{T} \boldsymbol{\Gamma}^{(q)} \boldsymbol{\xi} + \mathrm{i}\boldsymbol{\xi}^\mathsf{T} \boldsymbol{d}^{(q)}\right). \tag{6.21}$$

The $2S \times 2S$ matrix $\boldsymbol{\Gamma}^{(q)}$ is real and symmetric and $\boldsymbol{d}^{(q)}$ is a real vector with $2S$ components. The connection between the moment-generating function and the characteristic function (cf. eqs. (6.6) and (6.8)) can be used to obtain the first- and second-order moments of the quadrature operators from derivatives of $\chi_{\hat{\rho}}(\boldsymbol{\xi}) = \left\langle \exp\left(\mathrm{i}\boldsymbol{\xi}^\mathsf{T} \hat{\mathfrak{q}}\right)\right\rangle$:

$$\frac{1}{\mathrm{i}} \frac{\mathrm{d}}{\mathrm{d}\xi_j} \chi_{\hat{\rho}}(\boldsymbol{\xi}) \bigg|_{\boldsymbol{\xi}=0} = \langle \hat{\mathfrak{q}}_j \rangle \qquad \text{and} \qquad \frac{1}{\mathrm{i}^2} \frac{\mathrm{d}^2}{\mathrm{d}\xi_j \, \mathrm{d}\xi_k} \chi_{\hat{\rho}}(\boldsymbol{\xi}) \bigg|_{\boldsymbol{\xi}=0} = \frac{1}{2}\left\langle \hat{\mathfrak{q}}_j \hat{\mathfrak{q}}_k + \hat{\mathfrak{q}}_k \hat{\mathfrak{q}}_j \right\rangle. \tag{6.22}$$

Evaluating the derivatives for the characteristic function of a GS from eq. (6.21) shows that $\boldsymbol{\Gamma}^{(q)}$ and $\boldsymbol{d}^{(q)}$ are related to the first- and second-order moments of the quadrature operators [100, 226–228]:

$$\Gamma_{ij}^{(q)} = \langle \hat{\mathfrak{q}}_i \hat{\mathfrak{q}}_j + \hat{\mathfrak{q}}_j \hat{\mathfrak{q}}_i \rangle - 2\langle \hat{\mathfrak{q}}_i \rangle \langle \hat{\mathfrak{q}}_j \rangle \quad \text{and} \quad d_i^{(q)} = \langle \hat{\mathfrak{q}}_i \rangle \,. \tag{6.23}$$

Due to these relations, $\boldsymbol{\Gamma}^{(q)}$ and $\boldsymbol{d}^{(q)}$ are called *covariance matrix* and *displacement vector*. From eq. (6.23) it follows that the total photon number μ of the state is given by

$$\mu = \sum_s \left\langle \hat{a}_s^\dagger \hat{a}_s \right\rangle = \frac{1}{4}\,\mathrm{tr}\left(\boldsymbol{\Gamma}^{(q)} - \mathbb{1}\right) + \frac{1}{2}\boldsymbol{d}^\mathsf{T}\boldsymbol{d} \,. \tag{6.24}$$

[2] The (quantum) characteristic function of an operator shares some similarities with the (classical) characteristic function of a probability distribution from eq. (6.8).

The definition of $\boldsymbol{\Gamma}^{(q)}$ and $\boldsymbol{d}^{(q)}$ from eq. (6.23) follows refs. [100, 101, 228]. Other conventions are to arrange x and p in alternating order [225–227] or to scale $\boldsymbol{\Gamma}$ by a factor of $1/2$ [227, 236, 237]. Instead of considering $\boldsymbol{\Gamma}^{(q)}$ and $\boldsymbol{d}^{(q)}$ in the $\hat{\mathbf{q}}$-basis, they can also be represented in the complex $\hat{\mathbf{a}}$-basis [228], indicated by dropping the superscript:

$$\boldsymbol{\Gamma} = \boldsymbol{\Omega}^\dagger \boldsymbol{\Gamma}^{(q)} \boldsymbol{\Omega} \quad \text{and} \quad \boldsymbol{d} = \boldsymbol{\Omega}^\dagger \boldsymbol{d}^{(q)} . \tag{6.25}$$

In the real basis, $\boldsymbol{\Gamma}^{(q)}$ is real, symmetric and positive definite. In the complex basis, $\boldsymbol{\Gamma}$ is complex and Hermitian [228]. Working with the real- or complex-valued representation may be convenient depending on the specific application. The photon-number-resolved simulation method presented in this chapter mostly uses the real-valued representation, while the simulation in chapter 7 uses the complex-valued representation.

When the interaction describing the state is given by unitary operations $\hat{U}_{1,2} = \mathrm{e}^{-\mathrm{i}\hat{H}_{1,2}}$, with $\hat{H}_1$ having a linear or $\hat{H}_2$ having a quadratic dependence on $\hat{\mathbf{a}}$ and $\hat{\mathbf{a}}^\dagger$, $\hat{H}_1$ and $\hat{H}_2$ can be written in matrix notation as [228]

$$\hat{H}_1 = \mathrm{i}\boldsymbol{h}^\mathsf{T}\hat{\mathbf{a}} \quad \text{with} \quad \boldsymbol{h} = \begin{pmatrix} -\boldsymbol{\alpha}^* \\ \boldsymbol{\alpha} \end{pmatrix} \qquad \text{and} \qquad \hat{H}_2 = \frac{1}{2}\hat{\mathbf{a}}^\dagger \boldsymbol{H} \hat{\mathbf{a}} \quad \text{with} \quad \boldsymbol{H} = \begin{pmatrix} \boldsymbol{X} & \boldsymbol{Y} \\ \boldsymbol{Y}^* & \boldsymbol{X}^* \end{pmatrix} . \tag{6.26}$$

Here, $\boldsymbol{Y} = \boldsymbol{Y}^\mathsf{T}$ and $\boldsymbol{X} = \boldsymbol{X}^\dagger$ ensure that $\boldsymbol{H}$ is Hermitian [228]. Applying $\hat{U}_{1,2}$ transforms the k-th element of $\hat{\mathbf{a}}$ according to [228]

$$\hat{U}_1^\dagger \hat{\mathrm{a}}_k \hat{U}_1 = (\hat{\mathbf{a}} + \boldsymbol{J}\boldsymbol{h})_k \quad \text{and} \quad \hat{U}_2^\dagger \hat{\mathrm{a}}_k \hat{U}_2 = (\boldsymbol{S}\hat{\mathbf{a}})_k , \quad \text{with} \tag{6.27}$$

$$\boldsymbol{S} = \mathrm{e}^{-\mathrm{i}\boldsymbol{K}\boldsymbol{H}} , \qquad \boldsymbol{J} = \begin{pmatrix} \mathbf{0} & \mathbb{1} \\ -\mathbb{1} & \mathbf{0} \end{pmatrix} , \quad \text{and} \quad \boldsymbol{K} = \begin{pmatrix} \mathbb{1} & \mathbf{0} \\ \mathbf{0} & -\mathbb{1} \end{pmatrix} . \tag{6.28}$$

Applying a unitary transformation to a state $\hat{\rho}$ such that the state after the transformation is $\hat{\rho}' = \hat{U}\hat{\rho}\hat{U}^\dagger$ changes the characteristic function to

$$\chi_{\hat{\rho}'}(\boldsymbol{\xi}) = \mathrm{tr}\Big[\hat{U}\hat{\rho}\hat{U}^\dagger \exp\big(\mathrm{i}\boldsymbol{\xi}^\mathsf{T}\hat{\mathbf{q}}\big)\Big] = \mathrm{tr}\Big[\hat{\rho} \exp\Big(\mathrm{i}\sum\nolimits_{j,k} \xi_j \Omega_{jk} \hat{U}^\dagger \hat{\mathrm{a}}_k \hat{U}\Big)\Big] . \tag{6.29}$$

Using eq. (6.27) yields the transformations for the characteristic function:

$$\hat{\rho}' = \hat{U}_1\hat{\rho}\hat{U}_1^\dagger \;\Rightarrow \chi_{\hat{\rho}'}(\boldsymbol{\xi}) = \chi(\boldsymbol{\xi})\exp(\mathrm{i}\boldsymbol{\xi}^\mathsf{T}\boldsymbol{\Omega}\boldsymbol{J}\boldsymbol{h}) , \tag{6.30}$$

$$\hat{\rho}' = \hat{U}_2\hat{\rho}\hat{U}_2^\dagger \;\Rightarrow \chi_{\hat{\rho}'}(\boldsymbol{\xi}) = \chi_{\hat{\rho}}\big((\boldsymbol{S}^{(q)})^\mathsf{T}\boldsymbol{\xi}\big) \quad \text{with} \quad \boldsymbol{S}^{(q)} = \boldsymbol{\Omega}\boldsymbol{S}\boldsymbol{\Omega}^\dagger . \tag{6.31}$$

Applying eqs. (6.30) and (6.31) to the Gaussian characteristic function shows that unitary operations are represented by simple matrix transformations of $\boldsymbol{\Gamma}$ and $\boldsymbol{d}$ [100, 226–228]:

$$\hat{\rho}' = \hat{U}_1\hat{\rho}\hat{U}_1^\dagger \quad \Rightarrow \quad \begin{matrix} \boldsymbol{\Gamma}' = \boldsymbol{\Gamma} , & \qquad \boldsymbol{d}' = \boldsymbol{d} + \boldsymbol{J}\boldsymbol{h} , \\ \boldsymbol{\Gamma}'^{(q)} = \boldsymbol{\Gamma}^{(q)} , & \qquad \boldsymbol{d}'^{(q)} = \boldsymbol{d}^{(q)} + \boldsymbol{\Omega}\boldsymbol{J}\boldsymbol{h} , \end{matrix} \tag{6.32}$$

$$\hat{\rho}' = \hat{U}_2 \hat{\rho} \hat{U}_2^\dagger \quad \Rightarrow \quad \begin{aligned} \boldsymbol{\Gamma}' &= \boldsymbol{S}\boldsymbol{\Gamma}\boldsymbol{S}^\dagger\,, & \boldsymbol{d}' &= \boldsymbol{S}\boldsymbol{d}\,, \\ \boldsymbol{\Gamma}'^{(q)} &= \boldsymbol{S}^{(q)}\boldsymbol{\Gamma}^{(q)}(\boldsymbol{S}^{(q)})^\mathsf{T}\,, & \boldsymbol{d}^{(q)} &= \boldsymbol{S}^{(q)}\boldsymbol{d}^{(q)}\,. \end{aligned} \tag{6.33}$$

The matrix $\boldsymbol{S}^{(q)}$ is symplectic with respect to $\boldsymbol{J}$, meaning that $\boldsymbol{S}^{(q)}\boldsymbol{J}(\boldsymbol{S}^{(q)})^\mathsf{T} = \boldsymbol{J}$ and $\boldsymbol{S}$ is symplectic with respect to $\boldsymbol{K}$, meaning that $\boldsymbol{S}\boldsymbol{K}\boldsymbol{S}^\dagger = \boldsymbol{K}$ [228]. An overview of applications of symplectic matrices in quantum mechanics and optics can be found in ref. [238].

When a state transformation preserves the total mean photon number of the system, it is called a *passive transformation*. For passive transformations $\boldsymbol{S}$ is unitary and $\boldsymbol{S}^{(q)}$ is orthogonal [228].

The expressions for the covariance matrices and displacement vectors of the most common GSs and the transformation matrices for the most important transformations of GSs can be found in the literature [100, 101, 225–228] and some are listed in appendix C. They constitute a versatile kit of building blocks allowing to model even complex optical setups simply and systematically: First, $\boldsymbol{\Gamma}$ and $\boldsymbol{d}$ are determined for the initial state. Then the Hamiltonians transforming the state in each step are written in the form of eq. (6.26) and the transformation matrices $\boldsymbol{S}$ are calculated from eq. (6.28) or are taken from the literature. Afterwards, eqs. (6.32) and (6.33) are used to update $\boldsymbol{\Gamma}$ and $\boldsymbol{d}$. The required matrix operations can be easily implemented with software packages such as *NumPy* [239] and *PyTorch* [29].

6.2 Generating Functions for the Photon Statistics

One of the most important results of publication [VI] is a generating function for the photon statistics of GSs in terms of $\boldsymbol{\Gamma}^{(q)}$ and $\boldsymbol{d}^{(q)}$. Variations of this generating function allow calculating the photon number distribution, cumulative probabilities, moments, and factorial moments of GSs. In section 6.2.1, the derivation of these expressions is presented, together with expressions for the matrix elements in the Fock basis and coherent state basis.

6.2.1 Derivation of Generating Functions for the Photon Statistics

Assuming independent detection of photons with efficiency η from a single-mode quantum state, the probability to detect n photons is, by analogy to Mandel's formula [240], given by [235, 241–243]:

$$p(n) = \left\langle : \frac{(\eta\hat{N})^n}{n!}\, \mathrm{e}^{-\eta\hat{N}} : \right\rangle . \tag{6.34}$$

Here, $\hat{N} = \hat{a}^\dagger\hat{a}$ is the photon number operator. The colons : : indicate the *normal order*, meaning that between the colons, the operators are sorted in such a way that all creation operators are placed left of all annihilation operators. By inserting eq. (6.34) into eq. (6.1), the PGF of the *photon number distribution* (PND) can be written as $h(y) = \langle \hat{h}(y) \rangle$, with the *generating operator* $\hat{h}(y)$. Such generating operators are common in theoretical literature about photon detection [235, 241–243]. Julian Nauth, who worked on an early version of the q-hub simulation during his master's thesis ref. [M3], showed in ref. [244] how the operator $\hat{h}(y)$ can be used to calculate the PND of biphoton states in terms of the covariance matrix.

By using eq. (6.34), the following generating operators for probabilities, moments, and factorial moments are obtained[3]:

$$h(y) = \sum_{n=0}^{\infty} y^n \left\langle : \frac{(\eta \hat{N})^n}{n!} \, \mathrm{e}^{-\eta \hat{N}} : \right\rangle = \left\langle : \mathrm{e}^{(y-1)\eta \hat{N}} : \right\rangle = \langle \hat{h}(y) \rangle \,, \tag{6.35}$$

$$M(\mu, y) = \sum_{n=0}^{\infty} \mathrm{e}^{(n-\mu)y} \left\langle : \frac{(\eta \hat{N})^n}{n!} \, \mathrm{e}^{-\eta \hat{N}} : \right\rangle = \left\langle \mathrm{e}^{-y\mu} : \exp\!\big((\mathrm{e}^y - 1) \eta \hat{N} \big) : \right\rangle = \langle \hat{M}(\mu, y) \rangle \,, \tag{6.36}$$

$$R(y) = \sum_{n=0}^{\infty} \left\langle : \frac{(\eta \hat{N})^n \, \mathrm{e}^{-\eta \hat{N}}}{n!(1-y)^{n+1}} : \right\rangle = \left\langle \frac{1}{1-y} : \exp\!\left(\frac{\eta y \hat{N}}{1-y} \right) : \right\rangle = \langle \hat{R}(y) \rangle \,. \tag{6.37}$$

The structure of $\hat{R}(y)$ is known from the generating function of the Laguerre polynomials $L_k(x)$ (cf. eq. (A.20)) and the rising factorial moments can therefore be written as $n^{(k)} = n! \, \langle : L_k(-\eta \hat{N}) : \rangle$ [245].

As discussed in section 6.1.1, the generating function of a sum of random variables is the product of the individual generating functions. Thereby, noise in the detection process can be taken into account. When the photon statistics of the noise is given by a Poissonian distribution $p_{\text{noise}} = \mathrm{e}^{-\nu} \nu^n / n!$ with noise parameter ν, its PGF is given by $h_{\text{noise}}(y) = \mathrm{e}^{(y-1)\nu}$. The generating operators, including Poissonian noise, become

$$\hat{h}(\nu, y) = \exp[\nu(y-1)] \, \hat{h}(y) \,, \tag{6.38}$$

$$\hat{M}(\nu, \mu, y) = \exp[\nu(\mathrm{e}^y - 1)] \, \hat{M}(\mu, y) \,, \quad \text{and} \tag{6.39}$$

$$\hat{R}(\nu, y) = \exp\!\left(\frac{\nu y}{1-y} \right) \hat{R}(y) \,. \tag{6.40}$$

Noise processes with different statistics can similarly be considered by multiplying the generating operators with the respective generating functions. Various kinds of detection noise can thereby easily be included in the simulation.

[3] The notation with angle brackets for classical expectations values of probability distributions should not be confused with the notation for the quantum expectation values of operators $\langle \hat{O} \rangle$. For example, the PGF of any probability distribution and, therefore, also the PGF of the PND is given by $h(y) = \langle y^N \rangle$ (cf. eq. (6.1)). However, only for the PND from eq. (6.35) it holds $h(y) = \left\langle : \mathrm{e}^{(y-1)\eta \hat{N}} : \right\rangle$.

The generating operators in eqs. (6.35) to (6.37) all involve operators of the type $\hat{g}_0[w(y)] = {:}\exp\!\big(-w(y)\,\hat{a}^\dagger\hat{a}\big){:}$ with different functions $w(y)$. The derivation of $\langle\hat{g}_0(w)\rangle$ in terms of the covariance matrix and displacement vector is the central step in deriving the generating functions for the photon statistics. For example, an expression for the PND is obtained, taking into account the detector efficiency η and noise ν. The generating operator yields a theoretical model for the POVM element $\hat{\Pi}_{N=n}$ for the detection of n photons: Combining eq. (6.2) and eq. (6.38) yields[4]

$$p(n) = \langle\hat{\Pi}_{N=n}\rangle \quad \text{with} \quad \hat{\Pi}_{N=n} = \frac{1}{n!}\frac{\mathrm{d}^n}{\mathrm{d}y^n}\,\mathrm{e}^{\nu(y-1)}\hat{g}_0[(1-y)\eta]\Big|_{y=0}. \tag{6.41}$$

By introducing two further parameters u and v, the more general operator

$$\hat{g}[u,v,w(y)] = {:}\exp\!\big(u\hat{a} + v\hat{a}^\dagger - w(y)\,\hat{a}^\dagger\hat{a}\big){:} \tag{6.42}$$

is obtained, enabling the calculation of density matrix elements [231] $\langle\alpha|\hat{\rho}|\gamma\rangle$ and $\langle n|\hat{\rho}|m\rangle$ for coherent states $|\alpha\rangle$ and $|\beta\rangle$ and photon number states $|n\rangle$ and $|m\rangle$, as shown in ref. [VI].

Derivation of the Characteristic Function of the Single-Mode Generating Operator

The next step in deriving the generating function for the photon statistics of multi-mode GSs is to derive the single-mode generating function $G(u,v,w) = \langle\hat{g}(u,v,w)\rangle$. The expectation value is given by the integral over the product of the characteristic functions of the state and the operator (cf. eq. (6.20)). As the characteristic function of a Gaussian state is directly given by $\boldsymbol{\Gamma}$ and $\boldsymbol{d}$, all that is left to do is to calculate $\chi_{\hat{g}}(\xi)$.

By using the Baker-Campbell-Haussdorf formula (cf. eq. (A.29)) and cyclic permutation of the trace, $\chi_{\hat{g}}(\boldsymbol{\xi})$ can be obtained from the trace over an operator in normal order,

$$\chi_{\hat{g}}(\xi) = \mathrm{tr}\big[\hat{g}\,\exp\!\big(\mathrm{i}(\xi_x\hat{x} + \xi_p\hat{p})\big)\big] = \exp\!\left(\frac{\xi_x^2+\xi_p^2}{4}\right)\mathrm{tr}\big[\exp\!\big(d\hat{a}^\dagger\big)\hat{g}\,\exp\!\big(c\hat{a}\big)\big], \tag{6.43}$$

with $c = (\mathrm{i}\xi_x + \xi_p)/\sqrt{2}$ and $d = (\mathrm{i}\xi_x - \xi_p)/\sqrt{2}$. Inserting the completeness relation $\mathbb{1} = \pi^{-1}\int_{\mathbb{C}}|\alpha\rangle\langle\alpha|\,\mathrm{d}^2\alpha$ [235] into the optical equivalence theorem eq. (A.30) yields

$$\mathrm{tr}\big(F(\hat{a}^\dagger,\hat{a})\big) = \frac{1}{\pi}\int_{\mathbb{C}} F(\alpha^*,\alpha)\,\mathrm{d}^2\alpha \tag{6.44}$$

[4] Note that eq. (6.41) describes a theoretical model for the POVM, assuming that photon detection is described by eq. (6.34). Whether a real detector is well described by this model could be checked by a detector tomography measurement (cf. chapter 5).

for a normally-ordered function of creation and annihilation operators $F(\hat{a}^\dagger, \hat{a})$. This allows to calculate $\mathrm{tr}\big(\mathrm{e}^{d\hat{a}^\dagger}\,\hat{g}\,\mathrm{e}^{c\hat{a}}\big) = \pi^{-1}\int_{\mathbb{C}} \mathrm{e}^{d\alpha^*}\,\mathrm{e}^{u\alpha+v\alpha^*-w|\alpha|^2}\,\mathrm{e}^{c\alpha}\,\mathrm{d}^2\alpha$ by separating the real and imaginary parts of $\alpha = a + \mathrm{i}b$ and evaluating two Gaussian integrals by using eq. (A.2):

$$\mathrm{tr}\big(\mathrm{e}^{d\hat{a}^\dagger}\,\hat{g}\,\mathrm{e}^{c\hat{a}}\big) = \frac{1}{\pi}\int_{\mathbb{R}} \mathrm{e}^{(d+v+c+u)a-wa^2}\,\mathrm{d}a \int_{\mathbb{R}} \mathrm{e}^{\mathrm{i}(c+u-d-v)b-wb^2}\,\mathrm{d}b = \frac{1}{w}\,\mathrm{e}^{(d+v)(c+u)/w}\,. \tag{6.45}$$

By collecting ξ_x and ξ_p into $\xi = (\xi_x, \xi_p)^\mathsf{T}$, this simplifies eq. (6.43) to

$$\chi_{\hat{g}}(\xi) = \frac{1}{w}\exp\!\Big(-\frac{1}{2}\frac{2-w}{2w}\xi^\mathsf{T}\xi - \mathrm{i}\xi^\mathsf{T}\zeta + \frac{uv}{w}\Big) \quad \text{with} \quad \zeta = \begin{pmatrix}\zeta_x\\ \zeta_p\end{pmatrix} = \frac{1}{w\sqrt{2}}\begin{pmatrix}-(u+v)\\ \mathrm{i}(v-u)\end{pmatrix}. \tag{6.46}$$

Derivation of the Generating Function for Multi-Mode Gaussian States

Equation (6.46) can easily be generalized to multiple modes labeled by $s = 1 \ldots S$. The characteristic functions of the individual modes are independent and can be combined to[5]

$$\chi_{\hat{g}}(\xi) = \exp\!\Big(-\frac{1}{2}\xi^\mathsf{T}\boldsymbol{A}^{\oplus 2}\xi - \mathrm{i}\xi^\mathsf{T}\zeta^{(q)} + Z\Big)\prod_{s=1}^{S}\frac{1}{w_s}\,. \tag{6.47}$$

Here, $\xi^\mathsf{T} = (\xi_x^\mathsf{T}, \xi_p^\mathsf{T})$ and $\zeta^\mathsf{T} = (\zeta_x^\mathsf{T}, \zeta_p^\mathsf{T})$ each comprise $2S$ components, $Z = \sum_s u_s v_s / w_s$, and $\boldsymbol{A} = \mathrm{diag}\big((2-w_1)/w_1, \cdots, (2-w_S)/w_S\big)/2$.

Inserting eq. (6.47) and the characteristic function for a Gaussian state from eq. (6.21) into $G(\boldsymbol{u},\boldsymbol{v},\boldsymbol{w}) = (2\pi)^{-S}\int_{\mathbb{R}^{2S}} \chi_{\hat{\rho}}(\xi)\chi_{\hat{g}}(-\xi)\,\mathrm{d}\xi$ from eq. (6.20) yields[6]

Generating function for the photon statistics and matrix elements of Gaussian states

$$G(\boldsymbol{u},\boldsymbol{v},\boldsymbol{w}) = \frac{1}{\sqrt{\det\boldsymbol{\Lambda}}}\exp\!\Big(-\frac{1}{2}\boldsymbol{z}^\mathsf{T}\boldsymbol{\Lambda}^{-1}\boldsymbol{W}\boldsymbol{z} + Z\Big) \tag{6.48}$$

Here, the following abbreviations are used: $\boldsymbol{W} = \mathrm{diag}^{\oplus 2}(\boldsymbol{w})$, $\boldsymbol{z} = \boldsymbol{d}^{(q)} + \zeta$, and

$$\boldsymbol{\Lambda} = \frac{1}{2}\boldsymbol{W}\boldsymbol{\Gamma}^{(q)} + \boldsymbol{W}\boldsymbol{A}^{\oplus 2} = \mathbb{1} + \frac{1}{2}\boldsymbol{W}\big(\boldsymbol{\Gamma}^{(q)} - \mathbb{1}\big)\,. \tag{6.49}$$

[5] Here the notation $\boldsymbol{A}^{\oplus 2} = \boldsymbol{A}\oplus\boldsymbol{A} = \left(\begin{smallmatrix}\boldsymbol{A} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{A}\end{smallmatrix}\right)$ is used.

[6] The integral $G(\boldsymbol{u},\boldsymbol{v},\boldsymbol{w}) = \Big((2\pi)^S\prod_{s=1}^{S} w_s\Big)^{-1}\int_{\mathbb{R}^{2S}} \exp\Big[-\frac{1}{2}\xi^\mathsf{T}\Big(\frac{1}{2}\boldsymbol{\Gamma}^{(q)} + \boldsymbol{A}^{\oplus 2}\Big)\xi + \mathrm{i}\xi^\mathsf{T}\boldsymbol{z}^{(q)} + Z\Big]\,\mathrm{d}\xi$ is solved by using eq. (A.3) and $\prod_s w_s = \sqrt{\det(\boldsymbol{W})}$ is then absorbed into $\det\big(\boldsymbol{\Gamma}^{(q)}/2 + \boldsymbol{A}^{\oplus 2}\big)\det(\boldsymbol{W}) = \det(\boldsymbol{\Lambda})$.

Expressions for Probabilities and Moments

The probabilities and moments of the multivariate photon statistics are retrieved from eq. (6.48) by repeated differentiation. For that, eqs. (6.38) to (6.40) are generalized by introducing D differentiation parameters $y_1, \dots, y_D$ for detectors $d = 1, \dots, D$, each detecting M_d modes with additional Poissonian noise ν_d. The total number of modes is $S = \sum_d M_d$ and the modes are indexed by s enumerating $m_d = 1_d, \dots, M_d$ for all D detectors in the order $1_1, 2_1, \dots, M_1, 1_2, \dots M_2, \dots\dots M_D$. At this point, it is convenient to use a multi-index notation: For tuples $\boldsymbol{x}$ and $\boldsymbol{k}$, the abbreviation $\prod_i x_i^{k_i} = \boldsymbol{x}^{\boldsymbol{k}}$ is used, such that $\boldsymbol{w}^{-\mathbf{1}} = \prod_s w_s^{-1}$. The factorials and derivatives are compactly noted as $\boldsymbol{n}! = \prod_d (n_d!)$ and $\boldsymbol{\partial}_{\boldsymbol{y}}^{\boldsymbol{n}} = \prod_d \partial^{n_d} / \partial(y_d)^{n_d}$. Using these abbreviations, the final expressions for the multivariate probabilities and moments yield

Generating-function-based expressions for the photon statistics of Gaussian states

$$p(\boldsymbol{n}, \boldsymbol{\nu}, \boldsymbol{\eta}) = \langle \hat{\Pi}_{\boldsymbol{N}=\boldsymbol{n}} \rangle = \frac{1}{\boldsymbol{n}!} \boldsymbol{\partial}_{\boldsymbol{y}}^{\boldsymbol{n}} \exp\left(\sum_{d=1}^{D} (y_d - 1)\nu_d \right) G_0(\boldsymbol{w}) \bigg|_{\boldsymbol{y}=\mathbf{0}} \quad \text{with } w_s = \eta_{m_d}(1 - y_d)\,, \tag{6.50}$$

$$p(\boldsymbol{N} \leq \boldsymbol{n}, \boldsymbol{\nu}, \boldsymbol{\eta}) = \langle \hat{\Pi}_{\boldsymbol{N}\leq\boldsymbol{n}} \rangle = \frac{1}{\boldsymbol{n}!} \boldsymbol{\partial}_{\boldsymbol{y}}^{\boldsymbol{n}} (\mathbf{1} - \boldsymbol{y})^{-\mathbf{1}} \exp\left(\sum_{d=1}^{D} (y_d - 1)\nu_d \right) G_0(\boldsymbol{w}) \bigg|_{\boldsymbol{y}=\mathbf{0}} \quad \text{with } w_s = \eta_{m_d}(1 - y_d)\,, \tag{6.51}$$

$$\mathcal{M}(\boldsymbol{\mu}, \boldsymbol{k}, \boldsymbol{\nu}, \boldsymbol{\eta}) = \langle (\hat{\boldsymbol{N}} - \boldsymbol{\mu})^{\boldsymbol{k}} \rangle = \boldsymbol{\partial}_{\boldsymbol{y}}^{\boldsymbol{k}} \exp\left(\sum_{d=1}^{D} (\mathrm{e}^{y_d} - 1)\nu_d - \mu_d y_d \right) G_0(\boldsymbol{w}) \bigg|_{\boldsymbol{y}=\mathbf{0}} \quad \text{with } w_s = \eta_{m_d}(1 - \mathrm{e}^{y_d})\,, \tag{6.52}$$

$$n_{(\boldsymbol{k})}(\boldsymbol{\nu}, \boldsymbol{\eta}) = \left\langle \prod\nolimits_d \hat{N}_{d(k_d)} \right\rangle = \boldsymbol{\partial}_{\boldsymbol{y}}^{\boldsymbol{k}} \exp\left(\sum_{d=1}^{D} y_d \nu_d \right) G_0(\boldsymbol{w}) \bigg|_{\boldsymbol{y}=\mathbf{0}} \quad \text{with } w_s = -\eta_{m_d} y_d\,, \quad \text{and} \tag{6.53}$$

$$n^{(\boldsymbol{k})}(\boldsymbol{\nu}, \boldsymbol{\eta}) = \left\langle \prod\nolimits_d \hat{N}_d^{(k_d)} \right\rangle = \boldsymbol{\partial}_{\boldsymbol{y}}^{\boldsymbol{k}} (\mathbf{1} - \boldsymbol{y})^{-\mathbf{1}} \exp\left(\sum_{d=1}^{D} \frac{\nu_d y_d}{1 - y_d} \right) G_0(\boldsymbol{w}) \bigg|_{\boldsymbol{y}=\mathbf{0}} \quad \text{with } w_s = \frac{\eta_{m_d} y_d}{y_d - 1}\,. \tag{6.54}$$

These equations connect the covariance formalism and the photon statistics. Therefore, they are the central element of the proposed simulation method and one of the major results of publication [VI]. They allow calculating the PND, cumulative probabilities, moments, and factorial moments of the photon statistics by evaluating repeated derivatives of the generating function $G_0(\boldsymbol{w}) = G(\boldsymbol{0}, \boldsymbol{0}, \boldsymbol{w})$. Noise processes with different statistics could be considered by multiplication with the corresponding generating functions.

Similarly, multivariate extensions for matrix elements in the photon number basis and coherent state basis are obtained as demonstrated in ref. [VI]. For multi-mode Fock states $|\boldsymbol{n}\rangle$ and $|\boldsymbol{m}\rangle$ and multi-mode coherent states $|\boldsymbol{\alpha}\rangle$ and $|\boldsymbol{\beta}\rangle$ the expressions are [VI]

$$\langle\boldsymbol{\alpha}|\hat{\rho}|\boldsymbol{\beta}\rangle = \mathrm{e}^{-(|\boldsymbol{\alpha}|^2+|\boldsymbol{\beta}|^2)/2} G(\boldsymbol{\alpha}^*, \boldsymbol{\beta}, \boldsymbol{1}) \quad \text{and} \tag{6.55}$$

$$\langle\boldsymbol{n}|\hat{\rho}|\boldsymbol{m}\rangle = \frac{(-\boldsymbol{1})^{\boldsymbol{l}}}{\sqrt{\boldsymbol{n}!\boldsymbol{m}!}} \partial_{\boldsymbol{w}}^{\boldsymbol{l}}\, \partial_{\boldsymbol{u}}^{\boldsymbol{\Delta n}}\, \partial_{\boldsymbol{v}}^{\boldsymbol{\Delta m}}\, G(\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w})\Big|_{\substack{\boldsymbol{u}=\boldsymbol{0}\\ \boldsymbol{v}=\boldsymbol{0}\\ \boldsymbol{w}=\boldsymbol{1}}} . \tag{6.56}$$

Here, $\boldsymbol{l}$ is given by $l_s = \min(n_s, m_s)$ and the abbreviations $\boldsymbol{\Delta n} = \boldsymbol{n} - \boldsymbol{l}$ and $\boldsymbol{\Delta m} = \boldsymbol{m} - \boldsymbol{l}$ are used. By setting $\boldsymbol{l} = \boldsymbol{0}$ in eq. (6.56), an equation derived in ref. [246] is obtained. The advantage of eq. (6.56) over this expression is that for each mode, only $\max(n_s, m_s)$ instead of $n_s + m_s$ derivatives are required. This facilitates the numerical evaluation of the derivatives, especially when $|n_s - m_s|$ is relatively small.

The POVM elements from eqs. (6.48) and (6.51) enable easy modeling of more complex detections. Examples are the probability to detect n_A photons in detector A and n_B photons in detector B given by $\langle\hat{\Pi}_{N_A=n_A}\hat{\Pi}_{N_B=n_B}\rangle$, the probability for n_1 or n_2 photons in the same detector given by $\langle\hat{\Pi}_{N=n_1 \text{ or } N=n_2}\rangle = \langle\hat{\Pi}_{N=n_1} + \hat{\Pi}_{N=n_2}\rangle$ for $n_1 \neq n_2$ and the probabilities to detect any photon number except for n or for more than n photons given by $\langle\hat{\Pi}_{N\neq n}\rangle = \langle\hat{\mathbb{1}} - \hat{\Pi}_{N=n}\rangle$ and $\langle\hat{\Pi}_{N>n}\rangle = \langle\hat{\mathbb{1}} - \hat{\Pi}_{N\leq n}\rangle$. Such operators were used for example in refs. [101, 229] to obtain the count probabilities of non-PNR detectors from the vacuum probability by calculating $\langle\hat{\Pi}_{N>0}\rangle = \langle\hat{\mathbb{1}} - \hat{\Pi}_{N=0}\rangle$. Similar operators will be used in section 6.3 to model the non-PNR detectors in the QKD system. The POVM operators from eqs. (6.48) and (6.51) enable setting up such combined detection operators for PNR detection as well. This is best illustrated with an example: The probability to not detect n_A photons in detector A and to detect more than n_B photons in detector B is given by

$$\Big\langle(\hat{\mathbb{1}} - \hat{\Pi}_{N_A=n_A})(\hat{\mathbb{1}} - \hat{\Pi}_{N_B\leq n_B})\Big\rangle = 1 - \langle\hat{\Pi}_{N_A=n_A}\rangle - \langle\hat{\Pi}_{N_B\leq n_B}\rangle + \langle\hat{\Pi}_{N_A=n_A}\hat{\Pi}_{N_B\leq n_B}\rangle \tag{6.57}$$

$$= 1 - \frac{1}{n_A!}\frac{\partial^{n_A}}{\partial {y_A}^{n_A}} G_A\Big|_{y_A=0} - \frac{1}{n_B!}\frac{\partial^{n_B}}{\partial {y_B}^{n_B}}\frac{G_B}{1-y_B}\Big|_{y_B=0} + \frac{1}{n_A!n_B!}\frac{\partial^{n_A+n_B}}{\partial {y_A}^{n_A}\,\partial {y_B}^{n_B}}\frac{G_{AB}}{1-y_B}\Big|_{\substack{y_A=0\\ y_B=0}} . \tag{6.58}$$

Here, G_A, G_B, and G_{AB} are the functions $G(\mathbf{0},\mathbf{0},\boldsymbol{w})$ with $\boldsymbol{w}$ as in eqs. (6.48) and (6.51), where only the rows and columns entering detector A, B or both detectors are kept in $\boldsymbol{d}$, $\boldsymbol{W}$ and $\boldsymbol{\Lambda}$.

Extension of the Simulation Method to Non-Gaussian States

The expressions presented above allow calculating the matrix elements and the photon statistics only for GSs. However, the method can be extended to further classes of non-Gaussian states obtained from GSs by PNR detection [247]. Furthermore, states called photon-added and photon-subtracted GSs [234],

$$\hat{\rho}_{+\boldsymbol{k}} = \frac{\hat{\boldsymbol{a}}^{\dagger\boldsymbol{k}}\hat{\rho}\hat{\boldsymbol{a}}^{\boldsymbol{k}}}{\operatorname{tr}\left(\hat{\boldsymbol{a}}^{\dagger\boldsymbol{k}}\hat{\rho}\hat{\boldsymbol{a}}^{\boldsymbol{k}}\right)} \quad \text{and} \quad \hat{\rho}_{-\boldsymbol{k}} = \frac{\hat{\boldsymbol{a}}^{\boldsymbol{k}}\hat{\rho}\hat{\boldsymbol{a}}^{\dagger\boldsymbol{k}}}{\operatorname{tr}\left(\hat{\boldsymbol{a}}^{\boldsymbol{k}}\hat{\rho}\hat{\boldsymbol{a}}^{\dagger\boldsymbol{k}}\right)}, \tag{6.59}$$

can be simulated. The addition or subtraction of photons can have non-trivial effects on the photon statistics. For example, photon subtraction from a thermal state *increases* the mean photon number of the state [234, 248]. The expressions for matrix elements of multi-mode photon-added and multi-mode photon-subtracted GSs are derived in ref. [VI]. The resulting expressions are [VI]

$$\operatorname{tr}\left(\hat{\rho}_{-\boldsymbol{k}}\hat{g}_0(\boldsymbol{w})\right) = \frac{(-\mathbf{1})^{\boldsymbol{k}}}{\boldsymbol{m}_{(\boldsymbol{k})}}\partial_{\boldsymbol{w}}^{\boldsymbol{k}}\, G_0(\boldsymbol{w}) \quad \text{and} \tag{6.60}$$

$$\operatorname{tr}\left(\hat{\rho}_{+\boldsymbol{k}}\hat{g}_0(\boldsymbol{w})\right) = \frac{1}{\boldsymbol{m}^{(\boldsymbol{k})}}\partial_{\boldsymbol{r}}^{\boldsymbol{k}}\, G_0(\boldsymbol{w}')\prod_s \frac{1}{1-r_s(1-w_s)}\bigg|_{\boldsymbol{r}=\mathbf{0}}. \tag{6.61}$$

Here, G_0 is the generating function of the underlying GS. The elements of $\boldsymbol{w}'$ are given by $w_s' = 1-[(1-w_s)^{-1}-r_s]^{-1}$ and the coefficients are given by the factorial moments $\boldsymbol{m}^{(\boldsymbol{k})} = \boldsymbol{n}^{(\boldsymbol{k})}(\boldsymbol{\nu}=\mathbf{0},\boldsymbol{\eta}=\mathbf{1})$ and $\boldsymbol{m}_{(\boldsymbol{k})} = \boldsymbol{n}_{(\boldsymbol{k})}(\boldsymbol{\nu}=\mathbf{0},\boldsymbol{\eta}=\mathbf{1})$. The photon statistics of the photon-added and photon-subtracted GSs are obtained by replacing $G_0(\boldsymbol{w}) = \operatorname{tr}[\hat{\rho}\hat{g}_0(\boldsymbol{w})]$ in eqs. (6.50) to (6.54) by the expressions from eqs. (6.60) and (6.61). Thereby, all the quantities characterizing the photon statistics of multi-mode photon-added and multi-mode photon-subtracted GSs can also be obtained by repeated differentiation.

6.2.2 Implementation and Discussion of the Simulation Method

To compute the photon statistics from the generating functions, the multivariate higher-order derivatives can be evaluated, for example, by using *automatic differentiation* (AD) [249, 250]. The mathematical operations required to compute the function are automatically tracked by the AD software down to the level of elementary operations such as addition, multiplication, or the evaluation of $\sin(x)$. To evaluate the derivative, the AD software applies the well-known differentiation rules for these operations and combines them via the chain rule to the derivative of the function. For example, instead of approximating $\sin(x)$ numerically, the AD software uses the fact that the derivative of $\sin(x)$ is given by $\cos(x)$ and evaluates $\cos(x)$ in the derivative computation. In contrast to finite-difference approximations, the accuracy of AD is therefore only limited by the working precision. In machine learning, AD is used for training artificial neural networks [251], and therefore popular machine learning libraries such as *TensorFlow* [252] and *PyTorch* [29, 253] provide AD functionalities. As machine learning is gaining more and more attention, these software libraries are consistently extended.

To differentiate the generating functions in ref. [VI], *PyTorch 1.11.0* was used in a very basic configuration. The option for acceleration by using the graphics processing unit (GPU) was not chosen, and the only changed setting was the numerical precision, which was increased from the default value of float32 to float64. *PyTorch* is an up-to-date software framework with several advantages for differentiating the generating functions. Using *PyTorch*, implementing eqs. (6.50) to (6.54) in software to compute the photon statistics requires relatively little effort. *PyTorch* provides many functions for linear algebra, for example, to compute inverse matrices, determinants, or products of matrices and vectors, such that the multivariate higher-order derivatives can be implemented with only six lines of Python code, as demonstrated in ref. [IV].

Generating functions for the photon statistics are treated in textbooks such as refs. [233, 235, 245] and were applied for numerical calculations of the PND produced by multiple two-mode squeezers [254, 255]. Nevertheless, AD of generating functions has rarely been applied for practical numerical simulations. One possible reason may be that evaluating the higher-order derivatives requires resource-intensive computations. While AD of the generating functions is a very convenient method to compute the photon statistics, other methods perform better. The computational resources required to evaluate the expressions increase with the order of the derivatives and the size of $\boldsymbol{\Gamma}$ and $\boldsymbol{d}$. Tests showed that the computing time increases approximately by a factor of three for each additional photon number [VI]. For example, the computation of $p(n = 11)$ for a single-mode state on a regular desktop computer already took several minutes and required multiple Gigabytes of memory. The computation of $p(n_1 = 0, n_2 = 6)$ for a 1024×1024 covariance matrix representing 256 two-mode squeezers took less than 13 seconds [VI]. These numbers show that the computations require many numerical computations at higher photon numbers. To investigate if the results are still numerically accurate, values obtained from analytical formulas for simple Gaussian states were compared to the values obtained by AD in ref. [VI]. The comparison showed that the precision of the results from AD is very high even when the higher-order derivatives require a large number of numerical operations [VI].

Discussion of Alternative Methods to Compute the Photon Statistics

Besides AD, other options to evaluate the derivatives of the generating functions exist. One option is to use finite-difference approximations [229]. However, this method can quickly accumulate numerical inaccuracies. Another method uses the fact that generating functions are convergent power series. For example, probabilities can be retrieved from a PGF by approximating Cauchy's integral formula on a circle γ in the complex plane around the origin [256]:

$$h(y) = \sum_{n=0}^{\infty} p(n)\, y^n \quad \Rightarrow \quad p(n) = \frac{1}{2\pi \mathrm{i}} \oint_\gamma \frac{h(z)}{z^{n+1}}\, \mathrm{d}z\,. \tag{6.62}$$

The integral is then approximated numerically [257]. This method used the fact that the probabilities are non-negative and sum up to $\sum_{n=0}^{\infty} p(n) = 1$, such that the PGF converges at least for y on the complex unit disk. The method has also been extended to multivariate PGFs and moment-generating functions [258–260] and is discussed in detail in ref. [261].

Another approach to calculate the PND from $\boldsymbol{\Gamma}$ and $\boldsymbol{d}$ yields the formula [236, 237]

$$p(\boldsymbol{n}) = \frac{1}{\boldsymbol{n}!\sqrt{\det \boldsymbol{\Lambda}_1}} \exp\!\left(-\frac{1}{2}\boldsymbol{d}^\dagger \boldsymbol{\Lambda}_1^{-1} \boldsymbol{d}\right) \prod_i \left(\frac{\partial^2}{\partial \alpha_i\, \partial \alpha_i^*}\right)^{n_i} \exp\!\left(\frac{1}{2}\boldsymbol{\alpha}^\mathrm{T} \boldsymbol{A} \boldsymbol{\alpha} + \boldsymbol{d}^\dagger \boldsymbol{\Lambda}_1^{-1} \boldsymbol{\alpha}\right), \tag{6.63}$$

with $\boldsymbol{A} = \begin{pmatrix} \boldsymbol{0} & \mathbb{1}_S \\ \mathbb{1}_S & \boldsymbol{0} \end{pmatrix} (\mathbb{1}_{2S} - \boldsymbol{\Lambda}_1^{-1})$ and $\boldsymbol{\alpha}^\mathrm{T} = (\alpha_1, \ldots, \alpha_S, \alpha_1^*, \ldots, \alpha_S^*)$. Here, $\boldsymbol{\Lambda}_1 = (\boldsymbol{\Gamma} + \mathbb{1})/2$ is the matrix $\boldsymbol{\Lambda}$ from eq. (6.49) with $\boldsymbol{W}$ set to $\mathbb{1}$. For a practical evaluation, eq. (6.63) has some disadvantages compared to the formula for the PGF from eq. (6.50). It requires the evaluation of twice as many derivatives as the PND, and the detection efficiency is not directly incorporated. Most importantly, it is not a regular generating function because it requires two derivatives per photon number. Therefore, it is not directly possible to use this expression to model the joint detection of multiple modes in one detector or to model noise by multiplying it with the noise PGF. The exponential function to be differentiated in eq. (6.63) generates the multivariate Hermite polynomials, and the PND can therefore be expressed in terms of these polynomials [262–264]. However, the resulting expressions are seldom used for practical computations because evaluating them for higher photon numbers is complicated [265–267].

The task of finding the PND of a GS or the count distribution of non-PNR detectors is known as *Gaussian boson sampling* (GBS). The computational complexity of GBS has been theoretically investigated in the context of quantum computing [236, 237, 268–274] and GBS experiments have been realized experimentally to pursue the demonstration of the computational advantage of quantum computers over classical computers [275–277]. In

GBS research, often, a different method to compute the PND is considered. The expressions involve the *Hafnian* and *loop Hafnian* function for PNR detectors and the *Torontonian* and *loop Torontonian* function for non-PNR detectors [236, 271, 273, 278, 279]. For example, for GSs with $\boldsymbol{d} = \boldsymbol{0}$, the PND is obtained from the Hafnian function $\mathrm{haf}(\boldsymbol{A}_S)$[7] as

$$p(\boldsymbol{n}) = \frac{\mathrm{haf}(\boldsymbol{A}_S)}{\boldsymbol{n}!\sqrt{\det \boldsymbol{\Lambda}_1}}\,, \tag{6.65}$$

where $\boldsymbol{A}$ and $\boldsymbol{\Lambda}_1$ are the same matrices as in eq. (6.63) and $\boldsymbol{A}_S$ is derived from $\boldsymbol{A}$ by repeating rows and columns, depending on the number of photons to be detected in a particular mode [236, 237, 271]. The fact that the PNDs $p(\boldsymbol{n})$ of GSs without displacement can be calculated from eqs. (6.50) and (6.65) shows that $\mathrm{haf}(\boldsymbol{A}_S)$ and the generating function for the PND are related, and the relation is called the *Hafnian master theorem* [281].

Evaluating Hafnian-type functions with state-of-the-art algorithms scales with $\mathcal{O}(N^3 2^{N/2})$ for N detected photons [273], and even faster methods have recently been developed [274]. This means the runtime scales exponentially with the number of photons, similar as it was observed for differentiating the PGF with *PyTorch*. However, the scaling factor per additional photon of the specialized algorithms for evaluating Hafnians is lower than with the general-purpose tool *PyTorch*. Algorithms to evaluate Hafnians and for other GBS-related computations are available from the software library *The Walrus* [282]. After ref. [VI] was released, a method to compute the moments of the PND via the Hafnian approach was presented in ref. [283], and the computation speed is compared to the generating function approach from ref. [VI], showing a significant advantage of the Hafnian method.

An expression for the PND of GSs with $\boldsymbol{d} = \boldsymbol{0}$ that is similar to the PGF from eq. (6.50) was derived in ref. [229]:

$$p(\boldsymbol{n}) = \frac{(-\boldsymbol{1})^{\boldsymbol{n}}}{\boldsymbol{n}!}\partial_{\boldsymbol{y}}^{\boldsymbol{n}} \det\!\left(\mathbb{1} + \frac{1}{2}\,\mathrm{diag}^{\oplus 2}(\boldsymbol{w})(\boldsymbol{\Gamma} - \mathbb{1})\,\mathrm{diag}^{\oplus 2}(\boldsymbol{w})\right)^{-1/2}\Bigg|_{\boldsymbol{y}=\boldsymbol{1}} \quad \text{with} \quad w_s = \sqrt{y_j}\,. \tag{6.66}$$

For the derivation of this formula, each PNR detector was formally replaced by a multiport beamsplitter with non-PNR detectors at the outputs, and the number of counts in the non-PNR detectors was considered. The derivation used the formula for the calculation of the count probability of non-PNR detectors and is led by the intuition that by taking

[7] The Hafnian of a $2n \times 2n$ matrix $\boldsymbol{B}$ is given by [273, 278, 280]

$$\mathrm{haf}(\boldsymbol{B}) = \sum_{M \in \mathrm{PMP}(2n)} \prod_{(i,j)\in M} B_{ij}\,, \tag{6.64}$$

where $\mathrm{PMP}(2n)$ is the set of *perfect matchings*, that is the set of partitions of $\{1, 2, \ldots, 2n\}$ into subsets of size 2. For example, $\mathrm{PMP}(4) = \{(1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}$ and $\mathrm{haf}(\boldsymbol{B}_{4\times 4}) = B_{1,2}B_{3,4} + B_{1,3}B_{2,4} + B_{1,4}B_{2,3}$.

the limit of a beam splitter with infinitely many outputs, the probability that multiple photons end up in the same non-PNR detector vanishes. In contrast to eq. (6.50), noise, detection efficiencies, and states with $\boldsymbol{d} \neq \mathbf{0}$ are not covered by eq. (6.66). The authors of ref. [229] pointed out that an advantage of eq. (6.66) over the Hafnian formulas is that the size of the covariance scales only linearly with the number of frequency modes, but the number of required derivatives is not changed. In contrast, the Hafnian method does not distinguish between spatial and frequency modes. To model the joint detection of multiple frequencies, Hafnians for all different detection patterns over these modes must be calculated and combined [229]. The expressions of the photon statistics from eqs. (6.50) to (6.54) share this advantage with eq. (6.66). In chapter 7, this advantage is taken to the limit to formulate expressions for the photon statistics in terms of a continuum of frequency modes.

6.3 QKD Simulation without Frequency Resolution

The relatively simple matrix operations of the covariance formalism allow modeling even of complex quantum-optical setups with moderate efforts. To demonstrate the method, the q-hub QKD system was simulated, including all relevant imperfections of the setup [VI]. The only aspect not included is the spectrum of the photon pairs because considering it requires some additional efforts. Therefore, a separate, frequency-resolved simulation of the QKD system is presented in chapter 7.

6.3.1 Simulation Model of the QKD Setup

The setup of the simulated QKD system is shown in fig. 6.1 (a). The key exchanges of different user pairs are independent, such that only two users of the QKD system are considered in the model. The simulation includes various kinds of imperfections: The detectors are modeled as non-PNR detectors with efficiencies $\eta < 1$, and the dead times, dark counts, and afterpulses are taken into account. The mean photon pair numbers generated by the first and the second half of the pump pulse are not precisely the same because the splitting ratios of the beam splitters in the pump IF are not exactly 50 %, and because the losses in the IF arms are different. Due to the frequency-dependent losses in the WDM, the transmission probability for a photon pair is not the product of the transmission probabilities of the individual photons. The transmission links introduce significant losses. For the receiver IFs, splitting ratios deviating from 50 % and unbalanced losses in the IF arms are also considered. Furthermore, the interference at the beam splitters is not perfect due to polarization misalignment of the Faraday mirrors, leading to imperfect interference

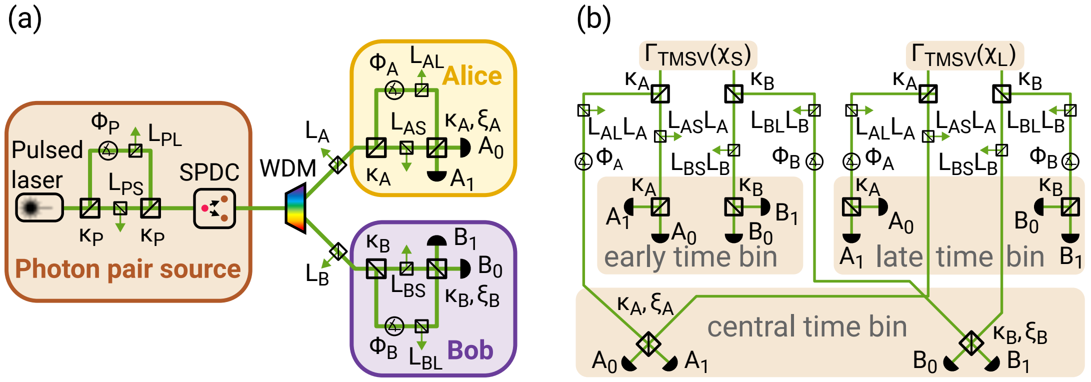


Figure 6.1: Simulated setup of the QKD system. (a) Schematic setup of the PPS and the receivers. Mach-Zehnder IFs are shown for clarity, but Michelson IFs are used in practice. Losses are modeled by introducing beam splitters coupling out a fraction of the light. L – Losses, ϕ – Interferometer phases, κ – Beam splitter coupling coefficients, ξ – Mode mismatch parameters, $A_0 \ldots$ B_1 – Detectors. (b) Unfolded setup for the simulation. The time bins are represented by separate modes and by introducing individual detectors for each time bin. The state after SPDC is given by two TMSV states for the two halves of the pump pulse. The squeezing parameters χ_S and χ_L are determined by the phase, losses, and beam splitter ratios of the IF in the source. The mode mismatch model from ref. [101] shown in fig. 6.2 is used to consider imperfect interference at the beam splitters.

in the central time bin. The mode mismatch is considered by using a model from ref. [101] shown in fig. 6.2.

To represent the different time bins, the setup is unfolded as shown in fig. 6.1 (b). Each physical detector is split up into three virtual detectors for the three time bins. The phases and the imperfect interference affect only the central time bin. For the early and late time bin, the phase is irrelevant and therefore omitted, and the mode mismatch of the beam splitters is not considered.

Modeling the setup in the covariance formalism is straightforward, although the setup is complex. Only four building blocks are necessary: the covariance matrix of TMSV and the transformations of the covariance matrix representing losses, phase shifters, and beam splitters. The transformations are listed in appendix C. The covariance matrix of the final state contains 20 modes: Two times four modes represent detection in the early and late time bins in the four detectors, and three times four modes are required for the central time bin due to the mode mismatch. The joint detection of three modes per detector is a practical example where the ability of the generating-function-based simulation method to describe the joint detection of multiple modes efficiently is helpful.

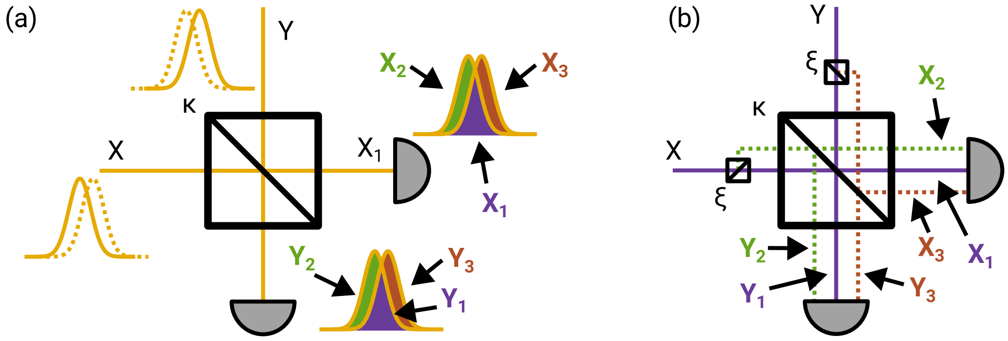


Figure 6.2: Scheme of the mode mismatch model proposed by Takeoka et al. in ref. [101]. (a) The beam splitter with coupling coefficient κ is modeled by decomposing the input modes X and Y into an interfering part (violet) and two non-interfering parts (green and brown). (b) The decomposition is modeled by introducing two additional mismatch beam splitters with coupling ratios ξ splitting off the non-interfering mismatch modes. Each detector receives two mismatch modes and the interfering part of the main mode.

Values for the propagation losses in the fibers, insertion losses of the fiber-optical components, and interference visibilities of the IFs were measured. Depending on the user combination to be simulated, the parameters for the specific receivers were then used in the simulation. The values for the mode mismatch parameters were calculated from the interference visibilities [M5]. The detection efficiencies, dark count rates, and afterpulse probabilities were obtained from the detector characterization presented in section 5.2.

Modeling the Non-PNR Detection in Three Time Bins

In the QKD experiment, non-PNR detectors are used, which can discern only vacuum and non-vacuum. For detectors without dead time, the measurement operators are given by the complement of the projection to vacuum (cf. eq. (5.10)) as $\hat{\Pi}_{\text{count}} = \hat{\mathbb{1}} - \hat{\Pi}_{\text{N=0}}$. Using eqs. (6.48) and (6.50) and taking into account that $\boldsymbol{d} = \boldsymbol{0}$ for the TMSV states in the simulation, the expectation value of a detection operator for the modes M becomes

$$p(\text{count in modes } M) = \langle \hat{\mathbb{1}} - \hat{\Pi}_{N_M=0} \rangle = 1 - \frac{\mathrm{e}^{-\nu}}{\sqrt{\det \boldsymbol{\Lambda}_M^{(q)}}} \,. \tag{6.67}$$

Here, $\boldsymbol{\Lambda}_M^{(q)}$ only contains the rows and columns of $\boldsymbol{\Lambda}^{(q)}$ representing the modes entering this particular detector, and the differentiation parameter is set to $y = 0$.

The noise parameter ν depends on the afterpulse probability and dark count rate. It can be derived by considering the detection in any of the three time bins for a detector without dead time. For a time bin of width ΔT, the noise parameter is given by $\nu_{\text{time bin}} = r_{\text{noise}}\Delta T$ with the noise rate r_{noise}. The noise rate is given by[8]

$$r_{\text{noise}} = \underbrace{r_{\text{dark}}}_{\substack{\text{Dark count}\\ \text{rate}}} + \underbrace{(\alpha - 1)\,\overbrace{f_{\text{rep}}\,\mu_M}^{\text{Photon rate}}}_{\substack{\text{Afterpulse rate}\\ \text{from photons}}} \,, \tag{6.68}$$

with the afterpulse factor $\alpha = 1 + p_{\text{ap}}/(1 - p_{\text{ap}})$ depending on the afterpulse probability p_{ap} (cf. eq. (B.7)). The mean photon number per repetition cycle in the modes M entering the detector is given by $\mu_M = \operatorname{tr}(\boldsymbol{\Gamma}_M^{(q)} - \mathbb{1})/4$ (cf. eq. (6.24)), and $\boldsymbol{\Gamma}_M^{(q)}$ is the final covariance to which the transformation representing detection losses was already applied by using eq. (C.8).

The noise rate in eq. (6.68) describes counts uncorrelated to the photon arrival time distribution, but afterpulses are correlated to the preceding clicks. However, the dead time and the afterpulse distribution extend over time scales in the order of magnitude of 10 µs (cf. fig. 5.2 (b)), which is about three orders of magnitude longer than the repetition cycle time of 10 ns. Therefore, at the time scale of one pulse repetition, the afterpulses can be assumed to contribute to the uncorrelated background.

For the derivation of key rates and QBERs, count operators such as in eq. (6.67) can be combined, as demonstrated in eq. (6.58). In the experiment, the detector POVMs have four exclusive detection results: a count in the early (E), central (C), or late (L) time bin or no count (no). Furthermore, due to the dead time, the detectors are only sensitive to incoming photons with a certain probability p_{on} (cf. eq. (5.1)). Therefore, the POVM elements are given by

$$\begin{aligned} \hat{\Pi}_{\mathrm{E}} &= p_{\text{on}}\hat{\mathbb{1}}_{\mathrm{C,L}}\big(\hat{\mathbb{1}}_{\mathrm{E}} - \hat{\Pi}_{N_E=0}\big)\,, & \hat{\Pi}_{\mathrm{L}} &= p_{\text{on}}\hat{\Pi}_{N_{\mathrm{E,C}}=0}\big(\hat{\mathbb{1}}_{\mathrm{L}} - \hat{\Pi}_{N_{\mathrm{L}}=0}\big)\,,\\ \hat{\Pi}_{\mathrm{C}} &= p_{\text{on}}\hat{\mathbb{1}}_{\mathrm{L}}\hat{\Pi}_{N_{\mathrm{E}}=0}\big(\hat{\mathbb{1}}_{\mathrm{C}} - \hat{\Pi}_{N_{\mathrm{C}}=0}\big)\,, \quad \text{and} & \hat{\Pi}_{\text{no}} &= p_{\text{off}}\hat{\mathbb{1}} + p_{\text{on}}\hat{\Pi}_{N=0}\,, \end{aligned} \tag{6.69}$$

with $p_{\text{off}} = 1 - p_{\text{on}}$ and the completeness relation $\hat{\mathbb{1}} = \hat{\Pi}_{\mathrm{E}} + \hat{\Pi}_{\mathrm{C}} + \hat{\Pi}_{\mathrm{L}} + \hat{\Pi}_{\text{no}}$ (cf. eq. (5.4)). Here, the abbreviation $N_{\mathrm{E,C,L}} = N$ indicates all time bins together. Due to the dead time, a count in the early or central time bin deactivates the detector for the subsequent time bins, which is represented by the operators $\hat{\Pi}_{N_{\mathrm{E}}=0}$ in $\hat{\Pi}_{\mathrm{C}}$ and $\hat{\Pi}_{N_{\mathrm{E,C}}=0}$ in $\hat{\Pi}_{\mathrm{L}}$. For the security of the key exchange, it is recommended that participants obtaining counts in both detectors in the same repetition randomly assign one of the values [40, 284], but this functionality

[8] In ref. [VI], a slightly different approach is used to calculate r_{noise}. In eq. (6.68), r_{dark} is the measured dark count rate, which includes the afterpulses of noise counts. In ref. [VII], the dark count rate is defined without these afterpulses, leading to a different expression for the noise rate yielding the same result.

is currently neither implemented in the data evaluation nor in the simulation. Instead, only those repetitions are used for key generation where one of Alice's and one of Bob's detectors yield counts, but none of the others.

The probability for a joint detection between detectors A_0 in time bin i and B_0 in time bin j with $i, j \in \{E, C, L\}$, and no count in the other detectors, for example, is given by

$$p_{A_{0,i},B_{0,j}} = \langle \hat{\Pi}_{A_{0,i}} \hat{\Pi}_{B_{0,j}} \hat{\Pi}_{A_{1,\mathrm{no}}} \hat{\Pi}_{B_{1,\mathrm{no}}} \rangle \,. \tag{6.70}$$

Equation (6.70) assumes that the probabilities p_{on} for different detectors are independent, such that the probability for multiple detectors to be active is the product of their individual probabilities p_{on}. This assumption is approximately correct when the coincidence rate is much lower than the individual count rates. If a significant fraction of the counts occurs in coincidence, the detectors are often simultaneously deactivated and activated, and the probabilities for them to be active at a given time are not independent anymore. For the QKD system, the individual count rates are orders of magnitude higher than the coincidence rates due to transmission losses and detection efficiencies, such that the independence of the probabilities p_{on} is approximately fulfilled.

Each detection operator in eq. (6.70) consists of two terms (cf. eq. (6.67)), such that expanding eq. (6.70) yields 16 terms. The expression can be simplified by approximating

$$\hat{\Pi}_{\mathrm{no}} = \hat{\Pi}_{N=0} + p_{\mathrm{off}}(\hat{\mathbb{1}} - \hat{\Pi}_{N=0}) \approx \hat{\Pi}_{N=0} \,. \tag{6.71}$$

This approximation is justified when $p_{\mathrm{off}} \ll 1$ and $\hat{\Pi}_{N=0} \approx \hat{\mathbb{1}}$, which is the case when the count probability itself is low. By using eq. (6.71), the number of terms from eq. (6.70) is reduced from 16 to four. The count probability for a joint detection between $A_{0,E}$ and $B_{0,L}$, for example, becomes

$$\begin{aligned} p_{\mathrm{count}(A_{0,E},B_{0,L})} &\approx p_{A_{0,\mathrm{on}}}\, p_{B_{0,\mathrm{on}}} \exp(-\nu_{B_{0,\mathrm{E,C}}} - \nu_{A_1} - \nu_{B_1}) \\ &\times \left(\frac{1}{\sqrt{\det \boldsymbol{\Lambda}^{(q)}_{B_{0,\mathrm{E,C}}A_1B_1}}} - \frac{\exp(-\nu_{A_{0,\mathrm{E}}})}{\sqrt{\det \boldsymbol{\Lambda}^{(q)}_{A_{0,\mathrm{E}}B_{0,\mathrm{E,C}}A_1B_1}}} - \frac{\exp(-\nu_{B_{0,\mathrm{L}}})}{\sqrt{\det \boldsymbol{\Lambda}^{(q)}_{B_0A_1B_1}}} + \frac{\exp(-\nu_{A_{0,\mathrm{E}}} - \nu_{B_{0,\mathrm{L}}})}{\sqrt{\det \boldsymbol{\Lambda}^{(q)}_{A_{0,\mathrm{E}}B_0A_1B_1}}} \right) . \end{aligned} \tag{6.72}$$

Equation (6.72) and the corresponding probabilities for other combinations of detectors and time bins are implemented in the simulation.

Corrections of the Photon Statistics

To obtain correct results from the simulation, the photon statistics of the PPS must be represented correctly. For a single TMSV state, the photon pair statistics follow a Bose-Einstein distribution (cf. eq. (1.21)), whereas the photon pair distribution produced by infinitely many independent two-mode squeezers is a Poissonian distribution (cf. eq. (7.5)) [254]. The importance of the photon statistics becomes evident when the probabilities for producing one and two photon pairs are compared. For low values of μ_p, the quantum key rate is mainly determined by the pulses containing one photon pair. The ratio of the probability to obtain one photon pair given a Bose-Einstein distribution divided by the probability for one photon pair from a Poisson distribution is approximately 0.95 at $\mu_\mathrm{p} = 0.05$ where the QKD system is operated, such that the raw key rate is approximately the same. However, the probability of obtaining two photon pairs determines the contribution of multi-photon-pair effects to the QBER. The ratio between the probabilities for two pairs is approximately 1.8, meaning that this QBER contribution differs significantly for the two statistics. The photon pair distribution of the state produced by the PPS is between these two extreme cases. The exact pair statistics depend on the joint spectral amplitude of the photon pairs and will be considered in more detail in section 7.1. The Schmidt number can be used to quantify the number of effectively contributing two-mode squeezers. As shown in section 7.1, the Schmidt number for the photon pairs used in the q-hub system is about 60. This number is only a rough estimation. However, the pair statistics are almost Poissonian at such high Schmidt numbers. To accurately represent the probabilities for the emission of one and two photon pairs, it is a sufficiently good approximation to assume 60 equally strong two-mode squeezers. For a direct implementation, 60 pairs of TMSV states would have to be set up, and the dimension of all matrices in the covariance matrix formalism would be scaled by this factor, resulting in much higher computing times. However, the covariance matrix would be block-diagonal as the same beam splitters, phase shifts, and losses are applied to all squeezers. Therefore, the evaluation is simplified by computing only one of these blocks and applying the rule for block determinants when the determinants for the detection probabilities are calculated (cf. eqs. (6.67) and (6.72)), meaning that the determinant of the block is raised to the power of 60.

Another correction of the photon statistics needs to be introduced to take into account the frequency-dependent insertion loss of the WDM. In section 2.2.1, it was discussed that the average transmission probability for a photon pair through the WDM is not the product of the average transmission probabilities for the individual photons. However, using the covariance formalism without frequency resolution implies that the transmission probability for a photon pair is automatically the product of the transmission probabilities for the individual photons. Therefore, the spectral correlation factor $c_{\Delta I}$ from eq. (2.6) can not be taken into account directly. To obtain at least approximately correct correlations, the values for μ_p, η_s, and η_i can be transformed to new values μ'_p, η'_s, and η'_i. As the photon pair statistics in the experiment is almost Poissonian, Poissonian statistics are assumed to simplify the derivation, such that the probability for the production of one photon pair is $\mu_\mathrm{p}\,\mathrm{e}^{-\mu_\mathrm{p}}$. To derive the transformation, the probabilities for the detection of a signal, an idler, and both photons from a pair are required to be equal for the original and transformed values of μ_p, η_s, and η_i. The transformed values are obtained by solving the following equations for the generation and transmission probabilities:

$$\begin{array}{rrcll} & \textbf{Transformed} & & \textbf{Original} & \\ \textbf{Signal} & \mu'_\mathrm{p}\,\mathrm{e}^{-\mu'_\mathrm{p}}\eta'_\mathrm{s} & = & \mu_\mathrm{p}\,\mathrm{e}^{-\mu_\mathrm{p}}\eta_\mathrm{s}\,, & (6.73) \\ \textbf{Idler} & \mu'_\mathrm{p}\,\mathrm{e}^{-\mu'_\mathrm{p}}\eta'_\mathrm{i} & = & \mu_\mathrm{p}\,\mathrm{e}^{-\mu_\mathrm{p}}\eta_\mathrm{i}\,, & (6.74) \\ \textbf{Pair} & \mu'_\mathrm{p}\,\mathrm{e}^{-\mu'_\mathrm{p}}\eta'_\mathrm{s}\eta'_\mathrm{i} & = & \mu_\mathrm{p}\,\mathrm{e}^{-\mu_\mathrm{p}}\eta_\mathrm{s}\eta_\mathrm{i}c_{\Delta I}\,. & (6.75) \end{array}$$

For the transformed quantities, the pair transmission probability is simply the product of the signal and idler transmissions. In contrast, for the original quantities, it includes the spectral correlation factor $c_{\Delta I}$. The equations lead to the conditions

$$\eta'_\mathrm{s} = c_{\Delta I}\eta_\mathrm{s}\,, \qquad \eta'_\mathrm{i} = c_{\Delta I}\eta_\mathrm{i}\,, \quad \text{and} \quad \mu'_\mathrm{p}\,\mathrm{e}^{-\mu'_\mathrm{p}} = \frac{\mu_\mathrm{p}\,\mathrm{e}^{-\mu_\mathrm{p}}}{c_{\Delta I}}\,. \tag{6.76}$$

Using the transformed parameters η'_s, η'_i, and μ'_p in the simulation, therefore, yields at least in the leading order, for the generation of one photon pair, the correct relation between the individual transmission probabilities and the pair transmission probabilities. When $\mu_\mathrm{p} \ll 1$, such that $\mu'_\mathrm{p} \approx \mu_\mathrm{p}/c_{\Delta I}$, the probabilities for the transmission of higher numbers of photons or photons pairs are at least approximately correct. For example, the probability for the generation and transmission of two pairs is given by

$$\frac{\mu'^2_\mathrm{p}}{2}\,\mathrm{e}^{-\mu'_\mathrm{p}}\eta'^2_\mathrm{s}\eta'^2_\mathrm{i} = \frac{\mu'^2_\mathrm{p}}{2}\,\mathrm{e}^{-\mu_\mathrm{p}}c^3_{\Delta I}\eta^2_\mathrm{s}\eta^2_\mathrm{i} \approx \frac{\mu^2_\mathrm{p}}{2}\,\mathrm{e}^{-\mu_\mathrm{p}}c^2_{\Delta I}\eta^2_\mathrm{s}\eta^2_\mathrm{i}\,, \tag{6.77}$$

which is approximately the probability of observing two photon pairs when the initial parameters and $c_{\Delta I}$ are used. The same approximation works for the probability for the production of higher numbers of photon pairs, using $\mu'^n_\mathrm{p} \approx \mu^n_\mathrm{p}/c^n_{\Delta I}$.

6.3.2 Simulation Results

Simulation of Quantum Key Rates and QBERs

The sifted key rates and QBERs are obtained by simulating the joint detection probabilities for the different combinations of detectors and time bins and multiplying them with the source repetition rate. In the experiment, the QBER_p is not entirely stable due to temperature fluctuations in the IFs, and this effect is not considered in the simulation.

Therefore, only the QBER$_t$ is compared to the experimental values. Figure 6.3 shows the simulation results along with values measured for different combinations of QKD users that were presented in fig. 7 of publication [II][9]. The simulated key rates and the QBERs match the measurements. The key rate decreases with increasing transmission distances due to the insertion losses of the fiber links. The variations in the QBER$_t$ are mainly caused by the variation in the dark count rates and afterpulse probabilities. The simulated sifted key rate and the QBER$_t$ are slightly lower than the measured values. A possible reason for the difference is that μ_p is underestimated.

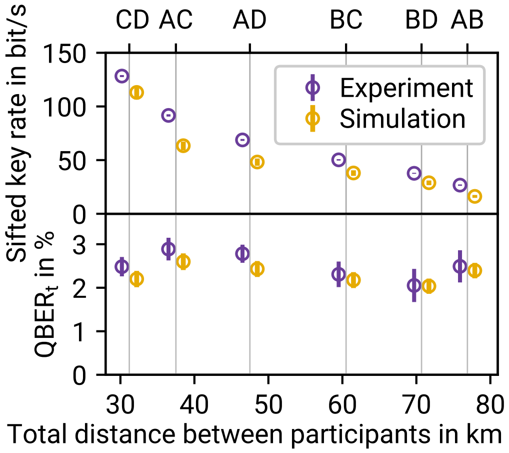


Figure 6.3: Simulated and measured sifted key rates and QBERs in the time basis for different transmission distances in the QKD network. The combination of users Alice (A), Bob (B), Charlie (C), and Diana (D) is indicated at the top. The error bars for the measured data indicate the standard deviation. For the simulation, the uncertainty is given by a variation of μ_p of ±10 %.

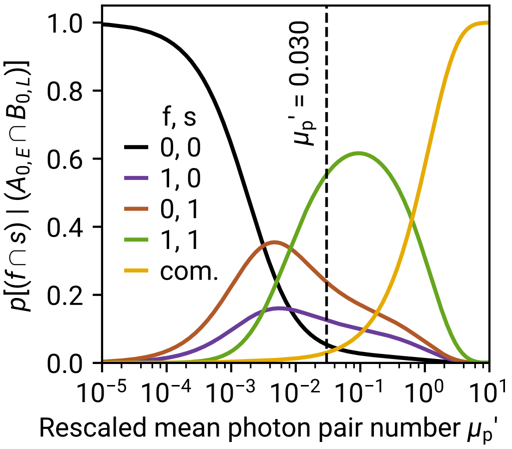


Figure 6.4: Probability that f and s photon pairs were produced by the first and second pump pulse, given a detection in $A_{0,\mathrm{E}}$ and $B_{0,\mathrm{L}}$. One minus the sum is the complementary probability "com.", comprising $f \geq 2$ or $s \geq 2$. The QKD system is operated at $\mu_p = 0.053$ corresponding to $\mu_p' = 0.030$ with probabilities (from "com." over $f, s = 0, 0$ to $f, s = 1, 1$) of 5, 13, 24, and 55 %.

[9] The simulation results presented in fig. 6 and fig. 7 of publication [VI] are slightly different from the results shown in figs. 6.3 and 6.4. Here, an improved value for the crystal efficiency according to ref. [VIII] is used to calculate μ, a Schmidt number of 60 instead of 100 is assumed, and the calculation of the noise parameter was revised. Furthermore, in ref. [VI], only the key rate was rescaled by $c_{\Delta I}$ to correct for the correlation introduced by the frequency-dependent losses in the WDM instead of rescaling μ, η_s, and η_i.

Analysis of the Contribution of Two-Pair Emissions to Bit Errors in the Time Basis

On the one hand, quantum bit errors in the time basis are observed in some repetitions where multiple photon pairs are generated. On the other hand, not all errors in the time basis are caused by multiple-photon-pair production. The ability of the simulation to calculate detection probabilities for individual photon numbers allows to analyze the contribution of multi-photon-pair emission to the quantum bit error rate. Specifically, it allows to answer the following question: Given that a time basis error is observed, what is the probability that a certain number of photon pairs was produced in this repetition?

To simplify the analysis, only time basis errors consisting of the count combination $A_{0,\mathrm{E}}$, $B_{0,\mathrm{L}}$ are considered. The probability that f photon pairs were produced by the first half-pulse and s pairs were produced by the second half-pulse, given that a time basis error $A_{0,\mathrm{E}}$, $B_{0,\mathrm{L}}$ is observed, can be calculated by using Bayes' theorem eq. (A.28):

$$p[(f \cap s) \,|\, (A_{0,\mathrm{E}} \cap B_{0,\mathrm{L}})] = \frac{p[(A_{0,\mathrm{E}} \cap B_{0,\mathrm{L}}) \,|\, (f \cap s)]}{p(A_{0,\mathrm{E}} \cap B_{0,\mathrm{L}})} p(f \cap s)\,. \tag{6.78}$$

Here, $p(f \cap s)$ is the probability that f photon pairs were produced by the first half-pulse and s pairs were produced by the second half-pulse. The emission probabilities of the two halves are independent of each other, such that $p(f \cap s) = p(f)p(s)$. The values for $p(f)$ and $p(s)$ are obtained by simulating the probability of finding f or s photons directly after the SPDC, respectively. The probability $p(A_{0,\mathrm{E}} \cap B_{0,\mathrm{L}})$, is simulated as before. Neglecting the effect that due to the dead time a detection in an earlier time bin of the same repetition prevents detections in the later time bins, $p[(A_{0,\mathrm{E}} \cap B_{0,\mathrm{L}})|(f \cap s)] = p(A_{0,\mathrm{E}}|f)p(B_{0,\mathrm{L}}|s)$ can be factorized into the independent probabilities $p(A_{0,\mathrm{E}}|f)$ and $p(B_{0,\mathrm{L}}|f)$. They can be derived by tracing the path of a photon through the setup and calculating the total transmissions $T_{A_{0,\mathrm{E}}}$ and $T_{B_{0,\mathrm{L}}}$ from the SPDC to the detectors:

$$p(A_{0,\mathrm{E}} \,|\, 1) = \left(1 - \mathrm{e}^{-\nu_{A_{0,\mathrm{E}}}}(1 - T_{A_{0,\mathrm{E}}})\right) p_{\mathrm{on},A_{0,\mathrm{E}}}\,, \tag{6.79}$$

$$p(B_{0,\mathrm{L}} \,|\, 1) = \left(1 - \mathrm{e}^{-\nu_{B_{0,\mathrm{L}}}}(1 - T_{B_{0,\mathrm{L}}})\right) p_{\mathrm{on},B_{0,\mathrm{L}}}\,. \tag{6.80}$$

Similarly, the probabilities $p(A_{0,\mathrm{E}} \,|\, 0)$ and $p(B_{0,\mathrm{L}} \,|\, 0)$ are nonzero due to noise counts and are obtained by setting $T_{A_{0,\mathrm{E}}} = T_{B_{0,\mathrm{L}}} = 0$ in eqs. (6.79) and (6.80).

Figure 6.4 shows $p[(f \cap s) \,|\, (A_{0,\mathrm{E}} \cap B_{0,\mathrm{L}})]$ for different combinations of f and s as a function of μ. For $\mu < 10^{-3}$, the largest contribution to count combinations $A_{0,\mathrm{E}}$, $B_{0,\mathrm{L}}$ is due to noise counts, for which $f = s = 0$. The combinations $f = 1, s = 0$ and $f = 0, s = 1$ are due to one noise count and one photon. They are at least partially relevant in the range of $10^{-4} < \mu < 1$. The two curves are different because the fiber link lengths and dark count rates for Alice and Bob are different. For $\mu > 0.1$, effects from two or more photon pairs produced by the first or second half of the pump pulse become relevant. In the experiment, the QKD system is operated at $\mu = 0.053$, where 55 % of the time basis errors occur when one photon pair is produced by each half of the two pump pulses. It can be concluded that multi-photon-pair effects are one of the most relevant sources of quantum bit errors.

Summary of Chapter 6

A new method to simulate the photon number distribution, moments, and factorial moments of multi-mode Gaussian states by automatic differentiation of generating functions was presented and published in ref. [VI]. The simulation method consists of two steps: First, the setup is modeled using the covariance formalism. Then, the covariance matrix and displacement vector of the final state are inserted into the generating functions, from which the photon statistics are obtained by automatic differentiation.

The method requires more computational resources than highly optimized algorithms for computing the photon number distribution based on the evaluation of Hafnian-type functions. Therefore, it is best suited for simulations where low photon numbers or moments of the photon statistics are of interest. The strength of the simulation lies in its flexibility, allowing to easily include imperfections such as noise and the detection of multiple modes in the same detector.

A simulation of the multi-user QKD system was implemented. Automatic differentiation is implemented by using the *pyTorch* framework. The application of *pyTorch* for this task is demonstrated in the technical report ref. [IV]. The simulated quantum key rates and *quantum bit error rates* (QBERs) are in agreement with measured values. The photon-number-resolved simulation was used to analyze the contribution of multi-photon-pair emission to the QBER in the time basis. The results showed that multi-photon-pair emission is the dominant source of quantum bit errors in the time basis.

7 Frequency-Resolved Simulation of the Q-Hub QKD System

The simulation results in section 6.3.2 showed that multi-photon-pair emission is the dominant source of quantum bit errors in the time basis. However, the simulation presented in section 6.3 does not consider the spectra of the photons. When the photon spectra are broad and the fiber transmission links are long, the *chromatic dispersion* (CD) in the fiber links can lead to the leakage of photons into adjacent time bins, which increases the QBER and decreases the achievable secure key rates.

In this chapter, a simulation of the q-hub system including all effects from the previous simulation and the effects from chromatic dispersion is presented. To combine the frequency resolution and the ability to simulate effects from the photon statistics, the covariance formalism of Gaussian states described in section 6.1.2 needs to be extended to represent the photon spectra. In the covariance formalism, separate modes are represented by columns and rows of the covariance matrix. Therefore, the strong frequency entanglement of the photons in the q-hub QKD system poses a challenge for the numerical simulation. Simulation methods resorting to a fine discretization of the frequency space require more computational resources for photon pairs with stronger frequency entanglement. The photon pairs used in the q-hub system are so strongly entangled that a direct discretization of the frequency space would require resource-intensive computations in the simulation. For even stronger entanglement, realizing simulations on a desktop computer using this approach would become impractical.

Early efforts to simulate the q-hub QKD system were undertaken in collaboration with Julian Nauth during his master's thesis [M3] under the supervision of Alexander Sauer and Prof. Dr. Gernot Alber from the *Theoretical Quantum Physics* research group. Nauth later extended these methods and published them in ref. [244].

Furthermore, mathematical methods to efficiently simulate the q-hub system or other quantum-optical setups with strongly entangled biphoton states were developed during the master's thesis of Philipp Kleinpaß [M7]. The methods and results presented in this chapter are based on these results and will be submitted for publication as ref. [VII].

In section 7.1, the Schmidt decomposition is reviewed as a tool relating the joint spectral amplitude to the photon statistics of the SPDC state.

In section 7.2, the covariance formalism is extended to Gaussian states with a continuum of modes in the frequency domain. The matrix operations modeling state transformations in the covariance formalism become integral operators in the continuous limit. The practically relevant consequences for the calculations are discussed.

The continuous-mode extension of the covariance formalism facilitates the transformation to the time domain. Furthermore, it is well compatible with the formulation of the photon statistics in terms of generating functions presented in chapter 6 because the number of derivatives in these expressions is independent of the number of modes per detector. This is an essential advantage of the generating-function-based method compared to the Hafnian-based approach of computing the photon statistics. Computing the Hafnian function requires that discrete matrix rows and columns represent each mode individually. An extension of Hafnian-based method to a continuum of modes is yet to be developed.

Section 7.3 describes the frequency-resolved modeling of the q-hub system in detail. Operations affecting discrete degrees of freedom are separated from the continuous representation of time and frequency, enabling simplifications of the expressions.

Section 7.4 presents approximations facilitating the computation of detection probabilities for strongly entangled biphoton states. The approximations are given in terms of expansions yielding the Poissonian photon statistics of a maximally entangled state when truncated after the leading order. The expressions allow to improve the accuracy of the approximations systematically by evaluating the expansions to higher orders.

In section 7.5, simulation results for the QKD performance are presented and compared to measurements, showing excellent agreement. Furthermore, the impact of CD on the $\mathrm{QBER}_{\mathrm{t}}$ is analyzed for photon pairs from type-II SPDC.

7.1 Schmidt Decomposition of the Joint Spectral Amplitude

To describe the quantum state generated by broadband SPDC, the unitary operator

$$\hat{U}_{\mathrm{SPDC}} = \exp\left(\frac{\chi}{2}\iint \tilde{\psi}(\omega_{\mathrm{s}},\omega_{\mathrm{i}})\hat{a}_{\mathrm{s}}^{\dagger}(\omega_{\mathrm{s}})\hat{a}_{\mathrm{i}}^{\dagger}(\omega_{\mathrm{i}})\,\mathrm{d}\omega_{\mathrm{s}}\,\mathrm{d}\omega_{\mathrm{i}} - \mathrm{H.c.}\right), \tag{7.1}$$

with the *joint spectral amplitude* (JSA) $\tilde{\psi}(\omega_{\mathrm{s}},\omega_{\mathrm{i}})$, is applied to vacuum (cf. eq. (1.25)). For the calculations in sections 2.3.1 and 2.3.2, only the first-order expansion of the state from eq. (1.28) comprising at most one photon pair was used, neglecting effects from multi-photon-pair emission. The approximation that at most one photon pair is generated is common in the literature and used, for example, in refs. [119, 285–289]. Sometimes, approximations taking the production of up to two photon pairs are used [290, 291]. For the two-photon interference in time-bin entanglement experiments, the influence of the two-pair component was analyzed in ref. [102]. In this chapter, the complete photon statistics are considered.

Due to the non-negligible width of the pump pulse spectrum, the production of photon pairs at different frequencies is not independent. Therefore, the photon statistics depend on the shape of the JSA. It is convenient to decouple the different contributions, so that the SPDC state is given by a tensor product of M independent *two-mode squeezed vacuum* (TMSV) states [254, 292] with different amplitudes $\chi\sigma_k/2$:

$$|\psi_{\mathrm{SPDC}}\rangle = \bigotimes_{k=0}^{M-1} \exp\Big(\frac{\chi\sigma_k}{2}\hat{A}_k^\dagger\hat{B}_k^\dagger\Big)|0\rangle\,. \tag{7.2}$$

The wave packet creation operators are defined[1] similar as in eq. (1.22) [254, 286, 292]:

$$\hat{A}_k^\dagger = \int \tilde{u}_k(\omega_{\mathrm{s}})\hat{a}_{\mathrm{s}}^\dagger(\omega_{\mathrm{s}})\,\mathrm{d}\omega_{\mathrm{s}} \quad \text{and} \quad \hat{B}_k^\dagger = \int \tilde{v}_k^*(\omega_{\mathrm{i}})\hat{a}_{\mathrm{i}}^\dagger(\omega_{\mathrm{i}})\,\mathrm{d}\omega_{\mathrm{i}}\,. \tag{7.3}$$

Here, $\{\tilde{u}_k(\omega_{\mathrm{s}})\}$ and $\{\tilde{v}_k(\omega_{\mathrm{i}})\}$ are sets of orthonormal basis functions, fulfilling

$$\int \tilde{u}_i(\omega_{\mathrm{s}})\tilde{u}_j^*(\omega_{\mathrm{s}})\,\mathrm{d}\omega_{\mathrm{s}} = \delta_{ij} \quad \text{and} \quad \int \tilde{v}_i(\omega_{\mathrm{i}})\tilde{v}_j^*(\omega_{\mathrm{i}})\,\mathrm{d}\omega_{\mathrm{i}} = \delta_{ij}\,, \tag{7.4}$$

such that the wave packet operators commute with $[\hat{A}_i,\hat{A}_j^\dagger] = [\hat{B}_i,\hat{B}_j^\dagger] = \delta_{ij}$. The k-th two-mode squeezer generates photon pairs with signal and idler wave packet shapes given by u_k and v_k^*, respectively. The photon statistics of the complete state are given by the joint statistics of all these two-mode squeezers and depend on the distribution of the parameters σ_k [254, 255]. While the photon pair statistics of one two-mode squeezer resembles the photon statistics of a thermal state, in the limit of infinitely many equally strong squeezers, the photon pair distribution becomes a Poissonian distribution [254]. The PND in the limit of infinitely many equally strong squeezers can be derived by considering the PGFs. The PGF of the thermal distribution is $\langle y^N\rangle = [(1 - y\tanh^2 r)\cosh^2 r]^{-1}$ (cf. eq. (1.21)). When the total mean photon pair number μ_{p} is equally distributed over M squeezers, the squeezing amplitude of each squeezer becomes $r_M = [\mathrm{arsinh}(\mu_{\mathrm{p}}/M)]^{1/2}$. The PGF for M such squeezers is the product of all M of these generating functions. Taking the

[1] It is convenient to use the complex conjugate function $\tilde{v}_k^*(\omega')$ instead of $\tilde{v}_k(\omega')$ in eq. (7.3) to later facilitate the notation using integral operators.

limit $M \to \infty$, expanding the coefficient of y up to the linear order in μ_p and using $\mathrm{e}^x = \lim_{M\to\infty}(1 + x/M)^M$ yields

$$\lim_{M\to\infty}\left[\left(1 - y\tanh^2 r_M\right)\cosh^2 r_M\right]^{-M} = \lim_{M\to\infty}\left(1 + (1-y)\mu_\mathrm{p}/M\right)^{-M} = \mathrm{e}^{(y-1)\mu_\mathrm{p}}\,, \quad (7.5)$$

which is the PGF of the Poisson distribution [254].

Depending on the exact shape of the JSA, the photon statistics is in between the two limiting cases of thermal statistics and the Poissonian statistics. It can be calculated numerically by differentiating the probability-generating function when the distribution of the σ_k is known [254]. To find the σ_k as well as the basis functions, the JSA is expressed as a weighted sum of products of functions $\tilde{u}_k(\omega_\mathrm{s})$ and $\tilde{v}_k^*(\omega_\mathrm{i})$, which is called a *Schmidt decomposition* [254, 286, 292–295]:

$$\tilde{\psi}(\omega_\mathrm{s}, \omega_\mathrm{i}) = \sum_k \sigma_k \tilde{u}_k(\omega_\mathrm{s})\tilde{v}_k^*(\omega_\mathrm{i})\,. \quad (7.6)$$

By convention, the real non-negative *Schmidt coefficients* $\sigma_k \geq 0$ are sorted in decreasing order $\sigma_0 \geq \sigma_1 \geq \ldots$. The functions $\tilde{u}_k(\omega_\mathrm{s})$ and $\tilde{v}_k^*(\omega_\mathrm{i})$ and the wave packets with the respective shapes are called *left Schmidt modes* and *right Schmidt modes*. From the normalization $\iint |\tilde{\psi}(\omega_\mathrm{s}, \omega_\mathrm{i})|^2 \,\mathrm{d}\omega_\mathrm{s}\,\mathrm{d}\omega_\mathrm{i} = 1$ if follows $\sum_k \sigma_k^2 = 1$. The crucial difference between the Schmidt decomposition and a regular expansion of $\tilde{\psi}(\omega_\mathrm{s}, \omega_\mathrm{i})$ in a two-dimensional orthonormal basis is that the summation runs only over a single index. The Schmidt decomposition can be considered as the continuous analog of the *singular value decomposition* (SVD)[2] of matrices [255].

The Schmidt decomposition is useful to quantify the frequency entanglement of the signal and idler photons by the *Schmidt number* [254, 255]

$$K = \frac{1}{\sum_k \sigma_k^4}\,. \quad (7.7)$$

The Schmidt number can be regarded as an effective number of contributing Schmidt modes. The more Schmidt modes contribute, the larger the Schmidt number and the

[2] Every rectangular complex matrix $\boldsymbol{M}$ can be decomposed into a product of two unitary matrices $\boldsymbol{U}$ and $\boldsymbol{V}$ and a diagonal matrix $\boldsymbol{\Sigma}$ as $\boldsymbol{M} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^\dagger$, which is called a *singular value decomposition* [296]. The columns $\boldsymbol{u}_i$ of $\boldsymbol{U}$ are called *left-singular vectors* and the columns $\boldsymbol{v}_j$ of $\boldsymbol{V}$ are called *right-singular vectors*. The elements $\sigma_k \geq 0$ of $\boldsymbol{\Sigma}$ are uniquely determined and called *singular values*. The SVD can thereby be expressed as $\boldsymbol{M} = \sum_k \sigma_k \boldsymbol{u}_k \boldsymbol{v}_k^\dagger$. Each summand is a matrix of the same shape as $\boldsymbol{M}$, which is the outer product of a left-singular and a right-singular vector, weighted by the singular value. One way to compute the SVD is to diagonalize $\boldsymbol{M}\boldsymbol{M}^\dagger = \boldsymbol{U}\boldsymbol{\Sigma}^2\boldsymbol{U}^\dagger$ and $\boldsymbol{M}^\dagger\boldsymbol{M} = \boldsymbol{V}\boldsymbol{\Sigma}^2\boldsymbol{V}^\dagger$ [296]: The eigenvectors are the columns of $\boldsymbol{U}$ and $\boldsymbol{V}$ respectively, and the eigenvalues are the squared singular values.

stronger the frequency entanglement between the photons. If, for example, all Schmidt coefficients are zero except for $\sigma_0 = 1$, then $K = 1$ and the state

$$|\psi\rangle = \iint \tilde{\psi}(\omega_\mathrm{s}, \omega_\mathrm{i})|\omega_\mathrm{s}, \omega_\mathrm{i}\rangle \,\mathrm{d}\omega_\mathrm{s}\,\mathrm{d}\omega_\mathrm{i} = \int \tilde{u}_0(\omega_\mathrm{s})\hat{a}_\mathrm{s}^\dagger(\omega_\mathrm{s})|0\rangle \,\mathrm{d}\omega_\mathrm{s} \otimes \int \tilde{v}_0^*(\omega_\mathrm{i})\hat{a}_\mathrm{i}^\dagger(\omega_\mathrm{i})|0\rangle \,\mathrm{d}\omega_\mathrm{i} \tag{7.8}$$

is separable and not frequency-entangled at all.

Analytical Schmidt Decomposition of a Two-Dimensional Gaussian Rotated by 45°

For a two-dimensional Gaussian JSA, the Schmidt decomposition can be calculated analytically [255, 297]. For the strongly entangled SPDC states used in the q-hub system, the JSA is a narrow antidiagonal stripe (cf. fig. 2.16) and can be roughly approximated as a Gaussian rotated by 45° with respect to the signal-idler coordinate system. For such a Gaussian with standard deviation s_- in ω_--direction and $s_+ < s_-$ in ω_+-direction, the expressions from refs. [255, 297] can be simplified, yielding the Schmidt decomposition

$$\tilde{u}_k(\omega_\mathrm{s}) = \frac{1}{\sqrt{g}}\,\phi_k\!\left(\frac{\omega_\mathrm{s}}{g}\right), \quad \tilde{v}_k^*(\omega_\mathrm{i}) = \frac{[\mathrm{sgn}(1-r)]^k}{\sqrt{g}}\,\phi_k\!\left(\frac{\omega_\mathrm{i}}{g}\right) \quad \text{and} \quad \sigma_k = \frac{2\sqrt{r}}{1+r}\left|\frac{1-r}{1+r}\right|^k, \tag{7.9}$$

with the normalized Hermite functions $\phi_k(x) = (2^k k!\sqrt{\pi})^{-1/2}\,\mathrm{e}^{-x^2/2}H_k(x)$ comprising the Hermite polynomial $H_k(x)$ as well as the aspect ratio $r = s_-/s_+$ and the geometric mean $g = \sqrt{s_+ s_-}$ of the standard deviations. The Schmidt number of the 2D-Gaussian becomes

$$K = \frac{1}{2}\left(r + \frac{1}{r}\right). \tag{7.10}$$

As an example, the Schmidt decomposition for a Gaussian with an aspect ratio of $r = 8$ is shown in fig. 7.1 (a). The JSA and first three Schmidt modes in both directions are shown in the top row, along with the distribution of the first Schmidt coefficients. Infinitely many Schmidt components contribute, and the Schmidt coefficients decrease exponentially (cf. eq. (7.9)). The Schmidt number according to eq. (7.10) is $K = 4.0625$. Although the Schmidt number is close to four, the approximation by the leading four components shown in fig. 7.1 (b) only roughly resembles the JSA. More components are needed to obtain a better approximation. Although the JSA is typically not a 2D Gaussian, these results can provide an intuition of how the Schmidt decomposition of a JSA with a high aspect ratio between the ω_- and ω_+ directions would approximately look like. The aspect ratio r can be estimated from the width of the pump pulse spectrum and of the phase matching function, and an order-of-magnitude estimation of the Schmidt number becomes

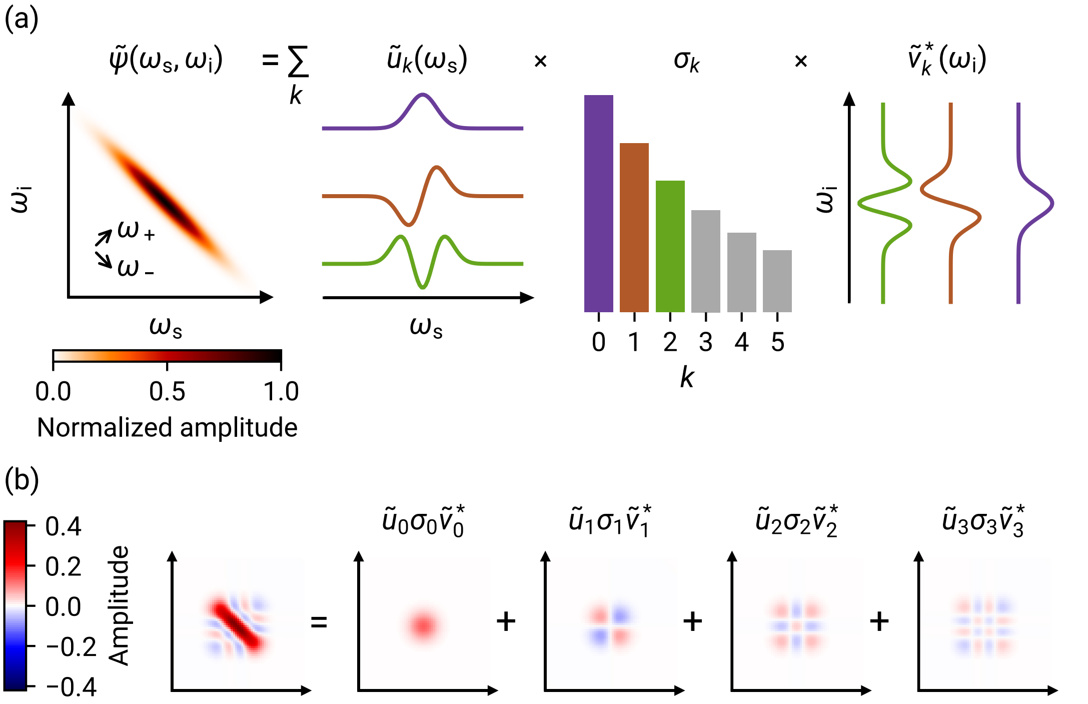


Figure 7.1: Schmidt decomposition of a 45° rotated Gaussian with aspect ratio $r = s_-/s_+ = 8$, resulting in a Schmidt number of $K = 4.0625$. (a) The JSA $\tilde{\psi}(\omega_s, \omega_i)$ (left) is the sum of products of Schmidt modes, weighted with the Schmidt coefficients. The first three Schmidt modes and coefficients according to eq. (7.9) are shown. (b) Approximation of the JSA as the sum of the first four contributions of the Schmidt decomposition. Each term is factorized in the signal-idler coordinate system. Infinitely many terms are required to represent the JSA exactly.

possible by using eq. (7.10). For the JSA from fig. 2.16, the aspect ratio of the FWHMs is approximately 120, and by using eq. (7.10), it can be estimated that at least 60 Schmidt modes are required to obtain a fair approximation. However, fig. 7.1 (b) showed that a good approximation may require more components.

Numerical Computation of the Schmidt Decomposition

For JSAs other than the 2D Gaussian, finding an analytical Schmidt decomposition is non-trivial [255]. Especially when the JSA is obtained from measurements, the Schmidt decomposition needs to be computed numerically. One possible approach is to expand $\tilde{\psi}(\omega_\mathrm{s}, \omega_\mathrm{i})$ in two sets of orthonormal functions $\{\tilde{o}_i^{(1)}(\omega_\mathrm{s})\}$ and $\{\tilde{o}_j^{(2)}(\omega_\mathrm{i})\}$ as [294]

$$\tilde{\psi}(\omega_\mathrm{s}, \omega_\mathrm{i}) = \sum_{i,j} E_{ij}\, \tilde{o}_i^{(1)}(\omega_\mathrm{s})\, \tilde{o}_j^{(2)}(\omega_\mathrm{i})\,, \tag{7.11}$$

with expansion coefficients $E_{ij} = \iint \tilde{\psi}(\omega_\mathrm{s}, \omega_\mathrm{i})\, \tilde{o}_i^{*(1)}(\omega_\mathrm{s})\, \tilde{o}_j^{*(2)}(\omega_\mathrm{i})\, \mathrm{d}\omega_\mathrm{s}\, \mathrm{d}\omega_\mathrm{i}$. Then, the coefficient matrix $\boldsymbol{E}$ is numerically decomposed into its SVD representation $\boldsymbol{E} = \boldsymbol{U\Sigma V}^\dagger$ and inserting the component-wise expression $E_{ij} = \sum_k \sigma_k U_{ik} V_{jk}^*$ into eq. (7.11) yields the Schmidt decomposition [255, 294]

$$\begin{aligned}
\tilde{\psi}(\omega_\mathrm{s}, \omega_\mathrm{i}) &= \sum_k \sigma_k \underbrace{\Big(\sum\nolimits_i U_{ik}\, \tilde{o}_i^{(1)}(\omega_\mathrm{s}) \Big)}_{=\tilde{u}_k(\omega_\mathrm{s})} \underbrace{\Big(\sum\nolimits_j V_{jk}^*\, \tilde{o}_j^{(2)}(\omega_\mathrm{i}) \Big)}_{=\tilde{v}_k^*(\omega_\mathrm{i})} \\
&= \underbrace{\left(\tilde{u}_0(\omega_\mathrm{s}), \tilde{u}_1(\omega_\mathrm{s}), \dots\right)}_{=\tilde{\boldsymbol{u}}^\mathsf{T}(\omega_\mathrm{s})} \underbrace{\begin{pmatrix} \sigma_0 & 0 & 0 \\ 0 & \sigma_1 & 0 \\ 0 & 0 & \ddots \end{pmatrix}}_{=\boldsymbol{\Sigma}} \underbrace{\begin{pmatrix} \tilde{v}_0^*(\omega_\mathrm{i}) \\ \tilde{v}_1^*(\omega_\mathrm{i}) \\ \vdots \end{pmatrix}}_{=\tilde{\boldsymbol{v}}^*(\omega_\mathrm{i})} \\
&= \tilde{\boldsymbol{u}}^\mathsf{T}(\omega_\mathrm{s}) \boldsymbol{\Sigma} \tilde{\boldsymbol{v}}^*(\omega_\mathrm{i})\,.
\end{aligned} \tag{7.12}$$

For JSAs with a high Schmidt number, the direct numerical implementation of the orthogonal basis expansion can be numerically challenging. In the example of the 2D Gaussian function, the Schmidt modes are the Hermite functions (cf. eq. (7.9)). The Hermite functions are also suitable as basis functions for the expansion [294], but they exhibit an increasing number of oscillations with increasing order. The numerical evaluation of the integral of the JSA with such oscillatory functions required to obtain the expansion coefficients E_{ij} can lead to convergence issues [255].

Another approach to calculating the Schmidt decomposition completely avoids the evaluation of integrals. For the computation, the JSA is discretized on a frequency grid with a resolution fine enough to resolve all relevant details, the discrete values are collected into a matrix $\tilde{\boldsymbol{\Psi}}$, and the SVD $\tilde{\boldsymbol{\Psi}} = \boldsymbol{U\Sigma V}^\dagger$ is computed directly [255]. The columns of $\boldsymbol{U}$ and the rows of $\boldsymbol{V}^\dagger$ are discrete approximations of the Schmidt modes, and the Schmidt coefficients are the singular values in $\boldsymbol{\Sigma}$. When the JSA is very narrow, it attains non-negligible values only on a narrow diagonal stripe in ω_--direction and $\tilde{\boldsymbol{\Psi}}$ can be represented by a sparse matrix which attains non-negligible values only on a few counter-diagonals. Solvers such as the *PROPACK* sparse SVD solver [298] can efficiently compute SVDs of sparse matrices by avoiding the operation with zero entries [255].

However, even computing the sparse matrix SVD may become infeasible in the limit of very strong entanglement. But in this limit, the photon statistics approaches Poissonian statistics, and the actual distribution of the Schmidt coefficients obtained from the SVD becomes less relevant. Therefore, an expansion for the limit of high entanglement yielding Poissonian photon statistics plus small corrections will be presented in section 7.4 to simplify the numerical evaluation of the detection probabilities.

7.2 Derivation of the Continuous-Mode Covariance for SPDC Photons

The first step for the simulation of the QKD system is to derive the covariance matrix of the biphoton state produced by SPDC. One option to take into account the spectral degree of freedom is to replace the elements of the vectors $\hat{\boldsymbol{a}} = (\hat{a}_1, \dots, \hat{a}_S)^\mathsf{T}$ and $\hat{\boldsymbol{a}}^\dagger = (\hat{a}_1^\dagger, \dots, \hat{a}_S^\dagger)$ from eq. (6.16) by a vector of creation and annihilation operators for N different frequency modes [229]:

$$\begin{aligned} \hat{\boldsymbol{a}} &= (\hat{a}_{1,\omega_1}, \hat{a}_{1,\omega_2}, \dots, \hat{a}_{1,\omega_N}, \hat{a}_{2,\omega_1}, \hat{a}_{2,\omega_2}, \dots\dots \hat{a}_{S,\omega_N})^\mathsf{T} \quad \text{and} \\ \hat{\boldsymbol{a}}^\dagger &= (\hat{a}^\dagger_{1,\omega_1}, \hat{a}^\dagger_{1,\omega_2}, \dots, \hat{a}^\dagger_{1,\omega_N}, \hat{a}^\dagger_{2,\omega_1}, \hat{a}^\dagger_{2,\omega_2}, \dots\dots \hat{a}^\dagger_{S,\omega_N})\,. \end{aligned} \tag{7.13}$$

The $2S \times 2S$ covariance matrix for S spatial degrees of freedom would thereby become a $2SN \times 2SN$ matrix, which may be quite large. For example, in the QKD system, 4 detectors each receive 3 modes representing the mode mismatch at the beam splitter by the mode mismatch model from ref. [101] (cf. fig. 6.2). Assuming that at least 20 discretization points over the narrow stripe of the JSA are required and taking the aspect ratio of the JSA of approximately 120 into account, the number of required discrete frequency modes can be roughly estimated to be 2400. This means that the covariance matrix would be a square matrix of dimension 57600, and storing the whole matrix in float64 precision would require 26.5 GB of memory. Less memory is required when the data are stored in a sparse matrix format, but, nevertheless, handling such large arrays with a desktop computer is rather inconvenient. For even stronger frequency entanglement, or when a finer resolution is used, the covariance matrices become even larger and the computations become impractical.

Continuous-Mode Limit of the Covariance Formalism

Therefore, instead of discretizing the JSA in the frequency domain, it is more convenient to derive the expressions for the detection probabilities for continuous spectra. For that, the covariance formalism needs to be extended to a continuum of modes for frequencies and times. This continuous formulation also facilitates the conversion of the JSA to the time domain by the *inverse Fourier transformation* (IFT). The IFT attains a particularly simple form when the complex representation of the covariance is used. Therefore, the complex variant of the covariance, $\boldsymbol{\Gamma}$, (cf. eq. (6.25)) will be used in this chapter.

Much less literature is available about continuous-mode GSs than about discrete-mode GSs. Therefore, its practical application will be discussed in detail. A formal discussion of some mathematical properties of continuous-mode GSs can be found in ref. [299].

From a practical point of view, it is often sufficient to think of operations with continuous-mode GSs as if they were described with the discrete operators from eq. (7.13) and to replace summations representing matrix multiplications by integrals[3]. When $\tilde{\psi}(\omega_{\mathrm{s}}, \omega_{\mathrm{i}})$ is discretized on a fine frequency grid, it becomes the matrix $\tilde{\boldsymbol{\Psi}}$. The continuous analog of the product of $\tilde{\boldsymbol{\Psi}}$ with some other matrix $\tilde{\boldsymbol{M}}$ is the application of a *Hilbert-Schmidt integral operator* $\tilde{\Psi}$ on the Hilbert space L^2 of square-integrable functions to another such operator $\tilde{M}$. The integral operators are represented by the kernel functions $\tilde{\psi}(\omega, \omega')$[4] and $\tilde{m}(\omega, \omega')$:

Analogy of integral operators as continuous limit of matrix multiplications

$$\underbrace{(\tilde{\boldsymbol{\Psi}}\tilde{\boldsymbol{M}})_{nm} = \sum_l \tilde{\Psi}_{nl}\tilde{M}_{lm}}_{\text{Discrete: matrix multiplication}} \quad \Leftrightarrow \quad \underbrace{(\tilde{\Psi}\tilde{M})(\omega, \omega') = \int \tilde{\psi}(\omega, w)\tilde{m}(w, \omega')\,\mathrm{d}w}_{\text{Continuous: integral operators}}\,. \tag{7.14}$$

The kernel of the transposed operator $\tilde{\Psi}^{\mathsf{T}}$ is $\tilde{\psi}(\omega', \omega)$, obtained by swapping the arguments, and the kernel of $\tilde{\Psi}^{\dagger}$ is $\tilde{\psi}^{*}(\omega', \omega)$, respectively. Products of block matrices containing integral operator blocks are evaluated as regular matrix operations on the level of the block structure and as integral operators for the individual blocks.

To derive the covariance of the SPDC state $\hat{U}_{\mathrm{SPDC}}|0\rangle$, the unitary operator $\hat{U}_{\mathrm{SPDC}} = \mathrm{e}^{-\mathrm{i}\hat{H}_{\mathrm{SPDC}}}$, with $\hat{H}_{\mathrm{SPDC}} = \hat{\mathbf{a}}^{\dagger}\boldsymbol{H}_{\mathrm{SPDC}}\hat{\mathbf{a}}/2$ and $\hat{\mathbf{a}}^{\dagger} = \left(\hat{\mathbf{a}}^{\dagger}, \hat{\mathbf{a}}^{\mathsf{T}}\right)$ (cf. eq. (6.26)), is compared to $\hat{U}_{\mathrm{SPDC}} = \exp\!\left(\chi \iint \tilde{\psi}(\omega, \omega')\hat{a}_{\mathrm{s}}^{\dagger}(\omega)\hat{a}_{\mathrm{i}}^{\dagger}(\omega')\,\mathrm{d}\omega\,\mathrm{d}\omega'/2 - \mathrm{H.c.}\right)$ from eq. (7.1).

[3] A notable exception to this rule is the SVD. The Schmidt decomposition as its continuous analog still contains a discrete summation over the singular values.

[4] For the integral kernels, the signal and frequency ω_{s} and ω_{i} will not always be the first and second arguments, respectively. Therefore, the notation ω and ω' for the first and second argument is used.

The matrices $\boldsymbol{H}_{\mathrm{SPDC}}$ for parallel ($\parallel$) polarized photons from type-0 SPDC and for orthogonal ($\perp$) polarized photons from type-II SPDC are given by

$$\tilde{\boldsymbol{H}}_\parallel = \mathrm{i}\chi \begin{array}{ccc} \hat{a}(\omega') & \hat{a}^\dagger(\omega') & \\ 0 & \tilde{\Psi}_\parallel & \hat{a}^\dagger(\omega) \\ -\tilde{\Psi}^*_\parallel & 0 & \hat{a}(\omega) \end{array} \quad \text{and} \tag{7.15}$$

$$\tilde{\boldsymbol{H}}_\perp = \frac{\mathrm{i}\chi}{2} \begin{array}{ccccc} \hat{a}_s(\omega') & \hat{a}_i(\omega') & \hat{a}_s^\dagger(\omega') & \hat{a}_i^\dagger(\omega') & \\ 0 & 0 & 0 & \tilde{\Psi}_\perp & \hat{a}_s^\dagger(\omega) \\ 0 & 0 & \tilde{\Psi}_\perp^{\mathsf{T}} & 0 & \hat{a}_i^\dagger(\omega) \\ 0 & -\tilde{\Psi}_\perp^* & 0 & 0 & \hat{a}_s(\omega) \\ -\tilde{\Psi}_\perp^\dagger & 0 & 0 & 0 & \hat{a}_i(\omega) \end{array} . \tag{7.16}$$

The JSA blocks in $\tilde{\boldsymbol{H}}$ are linear integral operators with kernel functions $\tilde{\psi}$ and the kernels of the vectors containing the creation and annihilation operators in the continuous picture are $\hat{\mathbf{a}}_\perp^\dagger(\omega) = \big(\hat{a}_{\mathrm{s}}^\dagger(\omega), \hat{a}_{\mathrm{i}}^\dagger(\omega), \hat{a}_{\mathrm{s}}(\omega), \hat{a}_{\mathrm{i}}(\omega)\big)$ and $\hat{\mathbf{a}}_\parallel^\dagger(\omega) = \big(\hat{a}^\dagger(\omega), \hat{a}(\omega)\big)$. The annotations in eqs. (7.15) and (7.16) show which JSA operators are combined with which creation and annihilation operators. For example, for parallel polarized photons, $\hat{H}_{\mathrm{SPDC}}$ is given by

$$\begin{aligned} \hat{H}_{\mathrm{SPDC}} = \frac{\hat{\mathbf{a}}^\dagger \boldsymbol{H}_{\mathrm{SPDC}} \hat{\mathbf{a}}}{2} &= \frac{\mathrm{i}\chi}{2} \iint \big(\hat{a}^\dagger(\omega), \hat{a}(\omega)\big) \begin{pmatrix} 0 & \tilde{\psi}(\omega,\omega') \\ -\tilde{\psi}^*(\omega,\omega') & 0 \end{pmatrix} \begin{pmatrix} \hat{a}(\omega') \\ \hat{a}^\dagger(\omega') \end{pmatrix} \mathrm{d}\omega\,\mathrm{d}\omega' \\ &= \frac{\mathrm{i}\chi}{2} \iint \tilde{\psi}(\omega,\omega') \hat{a}^\dagger(\omega) \hat{a}^\dagger(\omega')\,\mathrm{d}\omega\,\mathrm{d}\omega' + \mathrm{H.c.}\,. \end{aligned} \tag{7.17}$$

For parallel polarized photons, signals and idlers cannot be distinguished by their polarization as it is the case for type-II photons. Therefore, $\tilde{\boldsymbol{H}}_\parallel$ consists only of two nonzero blocks instead of four, and the JSA operator is symmetric, meaning that $\tilde{\Psi}_\parallel = \tilde{\Psi}_\parallel^{\mathsf{T}}$.

Covariance of the SPDC State

The initial state before the SPDC is vacuum, represented by the covariance $\tilde{\boldsymbol{\Gamma}} = \mathbb{1}$. The covariance after SPDC according to eq. (6.28) is given by $\tilde{\boldsymbol{\Gamma}} = \tilde{\boldsymbol{S}} \mathbb{1} \tilde{\boldsymbol{S}}^\dagger = \mathrm{e}^{-2\mathrm{i}\boldsymbol{K}\tilde{\boldsymbol{H}}}$, resulting in

$$\tilde{\boldsymbol{\Gamma}}_\perp = \exp\left[\chi \begin{pmatrix} 0 & 0 & 0 & \tilde{\Psi}_\perp \\ 0 & 0 & \tilde{\Psi}_\perp^{\mathsf{T}} & 0 \\ 0 & \tilde{\Psi}_\perp^* & 0 & 0 \\ \tilde{\Psi}_\perp^\dagger & 0 & 0 & 0 \end{pmatrix}\right] \quad \text{and} \quad \tilde{\boldsymbol{\Gamma}}_\parallel = \exp\left[2\chi \begin{pmatrix} 0 & \tilde{\Psi}_\parallel \\ \tilde{\Psi}_\parallel^\dagger & 0 \end{pmatrix}\right]. \tag{7.18}$$

The block-antidiagonal structure of the matrix allows to separate the power series expansion of the exponential into two contributions: Odd powers of $\tilde{\boldsymbol{H}}$ are block-antidiagonal and even powers are block-diagonal, leading for example for $\tilde{\boldsymbol{\Gamma}}_{\parallel}$ to

$$\tilde{\boldsymbol{\Gamma}}_{\parallel} = \sum_{n=0}^{\infty} \frac{(2\chi)^{2n}}{(2n)!} \begin{pmatrix} (\tilde{\Psi}\tilde{\Psi}^{\dagger})^{n} & 0 \\ 0 & (\tilde{\Psi}^{\dagger}\tilde{\Psi})^{n} \end{pmatrix} + \sum_{n=0}^{\infty} \frac{(2\chi)^{2n+1}}{(2n+1)!} \begin{pmatrix} 0 & (\tilde{\Psi}\tilde{\Psi}^{\dagger})^{n}\tilde{\Psi} \\ (\tilde{\Psi}^{\dagger}\tilde{\Psi})^{n}\tilde{\Psi}^{\dagger} & 0 \end{pmatrix} . \tag{7.19}$$

To evaluate the series, the integral operator $\tilde{\Psi}$ is represented by its Schmidt decomposition[5]:

$$\tilde{\Psi} = \sum_{k} \sigma_k |\tilde{u}_k\rangle\langle\tilde{v}_k| = \underbrace{(|\tilde{u}_0\rangle, |\tilde{u}_1\rangle, \dots)}_{=\tilde{\mathfrak{u}}} \underbrace{\begin{pmatrix} \sigma_0 & 0 & 0 \\ 0 & \sigma_1 & 0 \\ 0 & 0 & \ddots \end{pmatrix}}_{=\boldsymbol{\Sigma}} \underbrace{\begin{pmatrix} \langle\tilde{v}_0| \\ \langle\tilde{v}_1| \\ \vdots \end{pmatrix}}_{=\tilde{\mathfrak{v}}^{\dagger}} = \tilde{\mathfrak{u}}\boldsymbol{\Sigma}\tilde{\mathfrak{v}}^{\dagger} . \tag{7.20}$$

This allows to express the products of the JSA operators compactly by $\tilde{\Psi}\tilde{\Psi}^{\dagger} = \tilde{\mathfrak{u}}\Sigma^{2}\tilde{\mathfrak{u}}^{\dagger}$ and $\tilde{\Psi}^{\dagger}\tilde{\Psi} = \tilde{\mathfrak{v}}\Sigma^{2}\tilde{\mathfrak{v}}^{\dagger}$, such that the series expansion of the covariance matrices become

$$\tilde{\boldsymbol{\Gamma}}_{\perp} = \begin{pmatrix} \tilde{\mathfrak{u}}\cosh(\chi\Sigma)\tilde{\mathfrak{u}}^{\dagger} & 0 & 0 & \tilde{\mathfrak{u}}\sinh(\chi\Sigma)\tilde{\mathfrak{v}}^{\dagger} \\ 0 & \tilde{\mathfrak{v}}^{*}\cosh(\chi\Sigma)\tilde{\mathfrak{v}}^{\mathsf{T}} & \tilde{\mathfrak{v}}^{*}\sinh(\chi\Sigma)\tilde{\mathfrak{u}}^{\mathsf{T}} & 0 \\ 0 & \tilde{\mathfrak{u}}^{*}\sinh(\chi\Sigma)\tilde{\mathfrak{v}}^{\mathsf{T}} & \tilde{\mathfrak{u}}^{*}\cosh(\chi\Sigma)\tilde{\mathfrak{u}}^{\mathsf{T}} & 0 \\ \tilde{\mathfrak{v}}\sinh(\chi\Sigma)\tilde{\mathfrak{u}}^{\dagger} & 0 & 0 & \tilde{\mathfrak{v}}\cosh(\chi\Sigma)\tilde{\mathfrak{v}}^{\dagger} \end{pmatrix} \quad \text{and} \tag{7.21}$$

$$\tilde{\boldsymbol{\Gamma}}_{\parallel} = \begin{pmatrix} \tilde{\mathfrak{u}}\cosh(2\chi\Sigma)\tilde{\mathfrak{u}}^{\dagger} & \tilde{\mathfrak{u}}\sinh(2\chi\Sigma)\tilde{\mathfrak{v}}^{\dagger} \\ \tilde{\mathfrak{v}}\sinh(2\chi\Sigma)\tilde{\mathfrak{u}}^{\dagger} & \tilde{\mathfrak{v}}\cosh(2\chi\Sigma)\tilde{\mathfrak{v}}^{\dagger} \end{pmatrix} . \tag{7.22}$$

7.3 State Transformations by the QKD Setup

The setup consists of single-mode fibers and waveguides, so the simulation does not consider spatial modes. Polarization effects are irrelevant for the QKD protocol, and the elongation of the wave packets due to polarization-mode dispersion in the fiber links is negligible (cf. section 1.3.1). Therefore, the polarization is not modeled.

Separation of Parallel Polarized Photons by Wavelength Demultiplexing

A *wavelength-division demultiplexer* (WDM) separates the parallel polarized photons, and the frequency channels are chosen not to overlap, which can be used to distinguish the photons similar as in the case of the type-II SPDC. The wavelength separation into non-overlapping

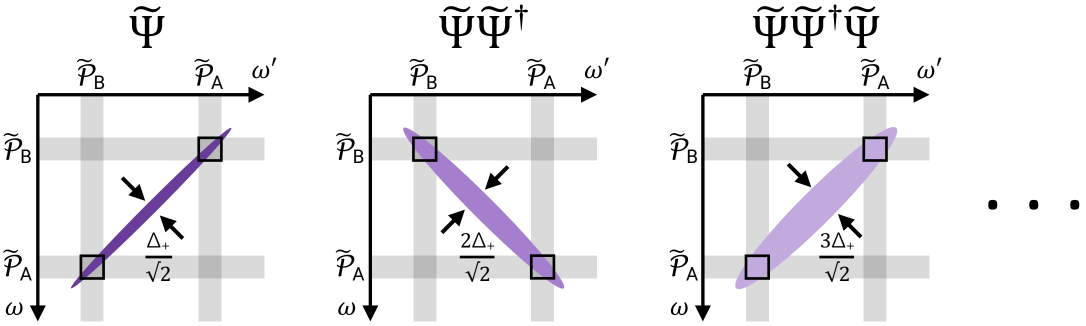
[5] The Dirac notation $|\tilde{u}_k\rangle$ and $\langle\tilde{v}_k|$ is here used with the usual meaning for square-integrable functions. For example the inner product is given by $\langle\tilde{u}_j|\tilde{u}_k\rangle = \int \tilde{u}_j^{*}(\omega)\tilde{u}_k(\omega)\,\mathrm{d}\omega$.

frequency channels is modeled by applying projection matrices $\tilde{\boldsymbol{P}}_{\mathrm{AB}} = (\tilde{\mathcal{P}}_{\mathrm{A}} \oplus \tilde{\mathcal{P}}_{\mathrm{B}})^{\oplus 2}$, transforming the covariance to $\tilde{\boldsymbol{\Gamma}}_{\|} \to \tilde{\boldsymbol{P}}_{\mathrm{AB}} \tilde{\boldsymbol{\Gamma}}_{\|} \tilde{\boldsymbol{P}}_{\mathrm{AB}}$. The projection operators $\tilde{\mathcal{P}}_{\mathrm{A}}$ and $\tilde{\mathcal{P}}_{\mathrm{B}}$ select the frequencies sent to Alice and Bob, respectively. Their kernels are given by $\tilde{P}(\omega, \omega') = \delta(\omega - \omega') \,\mathrm{rect}_{\Delta I}(\omega - \omega_c)$, selecting frequencies in an interval of width ΔI around the center frequencies ω_c of the channels.

Figure 7.2 schematically shows the selected frequency channels for a narrow JSA. The direction of the stripe is antidiagonal for odd iterations of JSAs and diagonal for even iterations of JSAs. When the width of the stripe is Δ_+ in ω_+ direction, $\tilde{\psi}(\omega, \omega')$ is only non-negligible for $|\omega_{\mathrm{s}} + \omega_{\mathrm{i}} - 2\omega_0| < \Delta_+/2$. The kernel containing n products of $\tilde{\psi}$,

$$\tilde{\psi}^{(n)}(\omega_1, \omega_{n+1}) = \int_{\mathbb{R}^{n-1}} \tilde{\psi}(\omega_1, \omega_2) \tilde{\psi}^*(\omega_3, \omega_2) \tilde{\psi}(\omega_3, \omega_4) \ldots \,\mathrm{d}\omega_2 \ldots \mathrm{d}\omega_n \,, \tag{7.23}$$

is only nonzero if the arguments of all JSAs are within the narrow stripes, requiring $|\omega_j + \omega_{j+1} - 2\omega_0| < \Delta_+/2$ for $j = 1 \ldots n+1$. For a JSA with a stripe of width Δ_+ in ω_+-direction, the width of the stripe of a term with n iterations of $\tilde{\Psi}$ is therefore bounded by $n\,\Delta_+$. When Δ_+ is much smaller than the separation of the frequency channels, apply-



$\tilde{\Psi}$
$\tilde{\Psi}\tilde{\Psi}^\dagger$
$\tilde{\Psi}\tilde{\Psi}^\dagger\tilde{\Psi}$
$\tilde{\mathcal{P}}_{\mathrm{B}}$
$\tilde{\mathcal{P}}_{\mathrm{A}}$
ω'
ω
$\frac{\Delta_+}{\sqrt{2}}$
$\frac{2\Delta_+}{\sqrt{2}}$
$\frac{3\Delta_+}{\sqrt{2}}$
...

Figure 7.2: Schematic visualization of the iterated integral operators $\tilde{\Psi}$. The JSA $\tilde{\psi}(\omega, \omega')$ attains non-negligible values only on a narrow anti-diagonal stripe of width Δ_+ in ω_+-direction, appearing as width $\Delta_+/\sqrt{2}$ in the signal-idler coordinate system. The terms with an odd number of JSAs, such as $\tilde{\Psi}$ or $\tilde{\Psi}\tilde{\Psi}^\dagger\tilde{\Psi}$, attain non-negligible values only on narrow anti-diagonal stripes and terms with an even number of JSAs are non-negligible only on diagonal stripes. The width of the stripe for n iterated JSAs is $n\,\Delta_+/\sqrt{2}$. By applying the projector $\tilde{\mathcal{P}}_{\mathrm{A}} \oplus \tilde{\mathcal{P}}_{\mathrm{B}}$, the frequency channels A and B (light gray) are selected. Applying the projector from both sides selects four squares (dark gray). When Δ_+ is much smaller than the channel separation, non-negligible values (in black squares) are obtained only for the projections of AB and BA channel combinations for odd iterations as well as for AA and BB projections for even iterations. The other projections yield zero (cf. eq. (7.24)).

ing $\tilde{\boldsymbol{P}}_{\mathrm{AB}}$ to the leading orders of the series expansion in eq. (7.19) will yield nonzero values only for the AB and BA channel combinations for terms with odd iterations. Analogously, nonzero values for the AA and BB combinations are only obtained for terms with even orders of JSAs. The other combinations of the projection operators select frequency intervals that are outside of the band, yielding zero:

$$\begin{aligned} 0 &\approx \tilde{\mathcal{P}}_{\mathrm{A}}(\tilde{\Psi}^{\dagger}\tilde{\Psi})^{n}\tilde{\mathcal{P}}_{\mathrm{B}} = \tilde{\mathcal{P}}_{\mathrm{B}}(\tilde{\Psi}^{\dagger}\tilde{\Psi})^{n}\tilde{\mathcal{P}}_{\mathrm{A}} = \tilde{\mathcal{P}}_{\mathrm{A}}(\tilde{\Psi}\tilde{\Psi}^{\dagger})^{n}\tilde{\mathcal{P}}_{\mathrm{B}} = \tilde{\mathcal{P}}_{\mathrm{B}}(\tilde{\Psi}\tilde{\Psi}^{\dagger})^{n}\tilde{\mathcal{P}}_{\mathrm{A}}\,, \\ 0 &\approx \tilde{\mathcal{P}}_{\mathrm{A}}(\tilde{\Psi}^{\dagger}\tilde{\Psi})^{n}\tilde{\Psi}^{\dagger}\tilde{\mathcal{P}}_{\mathrm{A}} = \tilde{\mathcal{P}}_{\mathrm{B}}(\tilde{\Psi}^{\dagger}\tilde{\Psi})^{n}\tilde{\Psi}^{\dagger}\tilde{\mathcal{P}}_{\mathrm{B}} = \tilde{\mathcal{P}}_{\mathrm{A}}(\tilde{\Psi}\tilde{\Psi}^{\dagger})^{n}\tilde{\Psi}\tilde{\mathcal{P}}_{\mathrm{A}} = \tilde{\mathcal{P}}_{\mathrm{B}}(\tilde{\Psi}\tilde{\Psi}^{\dagger})^{n}\tilde{\Psi}\tilde{\mathcal{P}}_{\mathrm{B}}\,. \end{aligned} \tag{7.24}$$

By using the symmetry $\tilde{\Psi} = \tilde{\Psi}^{\mathsf{T}}$ for type-0 photons and defining the operators

$$\tilde{\mathfrak{u}}_{\mathrm{A}} = (\tilde{\mathcal{P}}_{\mathrm{A}} \oplus 0)\tilde{\mathfrak{u}}\,, \quad \tilde{\mathfrak{u}}_{\mathrm{B}} = (0 \oplus \tilde{\mathcal{P}}_{\mathrm{B}})\tilde{\mathfrak{u}}\,, \quad \tilde{\mathfrak{v}}_{\mathrm{A}} = (\tilde{\mathcal{P}}_{\mathrm{A}} \oplus 0)\tilde{\mathfrak{v}}\,, \quad \text{and} \quad \tilde{\mathfrak{v}}_{\mathrm{B}} = (0 \oplus \tilde{\mathcal{P}}_{\mathrm{B}})\tilde{\mathfrak{v}}\,, \tag{7.25}$$

the covariance matrix for parallel photons after the projection to the frequency channels attains a similar structure as $\tilde{\boldsymbol{\Gamma}}_{\perp}$ in eq. (7.21):

$$\tilde{\boldsymbol{\Gamma}}_{\parallel} \approx \begin{pmatrix} \tilde{\mathfrak{u}}_{\mathrm{A}}\cosh(2\chi\,\boldsymbol{\Sigma})\tilde{\mathfrak{u}}_{\mathrm{A}}^{\dagger} & 0 & 0 & \tilde{\mathfrak{u}}_{\mathrm{A}}\sinh(2\chi\,\boldsymbol{\Sigma})\tilde{\mathfrak{v}}_{\mathrm{B}}^{\dagger} \\ 0 & \tilde{\mathfrak{v}}_{\mathrm{B}}^{*}\cosh(2\chi\,\boldsymbol{\Sigma})\tilde{\mathfrak{v}}_{\mathrm{B}}^{\mathsf{T}} & \tilde{\mathfrak{v}}_{\mathrm{B}}^{*}\sinh(2\chi\,\boldsymbol{\Sigma})\tilde{\mathfrak{u}}_{\mathrm{A}}^{\mathsf{T}} & 0 \\ 0 & \tilde{\mathfrak{u}}_{\mathrm{A}}^{*}\sinh(2\chi\,\boldsymbol{\Sigma})\tilde{\mathfrak{v}}_{\mathrm{B}}^{\mathsf{T}} & \tilde{\mathfrak{u}}_{\mathrm{A}}^{*}\cosh(2\chi\,\boldsymbol{\Sigma})\tilde{\mathfrak{u}}_{\mathrm{A}}^{\mathsf{T}} & 0 \\ \tilde{\mathfrak{v}}_{\mathrm{B}}\sinh(2\chi\,\boldsymbol{\Sigma})\tilde{\mathfrak{u}}_{\mathrm{A}}^{\dagger} & 0 & 0 & \tilde{\mathfrak{v}}_{\mathrm{B}}\cosh(2\chi\,\boldsymbol{\Sigma})\tilde{\mathfrak{v}}_{\mathrm{B}}^{\dagger} \end{pmatrix}. \tag{7.26}$$

The projections in eq. (7.24) are only zero for low orders for which the stripe has not reached a width covering the other two projection intervals (cf. fig. 7.2). The approximation in eq. (7.26) is therefore only valid when such a width is reached only for high, negligible expansion orders of the cosh and sinh functions.

Reordering of the Covariance

The detection probabilities finally calculated in the simulation are given by expressions involving determinants such as $\det\big(\mathbb{1} + \boldsymbol{W}(\boldsymbol{\Gamma}^{(q)} - \mathbb{1})/2\big)$ (cf. eq. (6.48)). Here, $\boldsymbol{\Gamma}^{(q)}$ is the covariance represented in time domain. The diagonal matrix $\boldsymbol{W} = \operatorname{diag}^{\oplus 2}(\boldsymbol{w})$ with $w_s = \eta_{m_d}(1 - y_d)$ contains the differentiation parameters y_d. Applying the transformation $\boldsymbol{\Omega}$ from eq. (6.18) to switch between the real and complex representation of the covariance does not change the determinant because $\boldsymbol{\Omega}$ is unitary. Therefore, the determinant can also be computed directly from the complex covariance $\boldsymbol{\Gamma}$ by

$$\det(\mathbb{1} + \boldsymbol{W}\boldsymbol{Z}) \quad \text{with} \tag{7.27}$$

$$\boldsymbol{Z} = \frac{1}{2}(\boldsymbol{\Gamma} - \mathbb{1})\,. \tag{7.28}$$

However, the usual notion of a matrix determinant breaks down in the continuous mode limit. The determinant is nevertheless well-defined because $\boldsymbol{Z}$ is a *trace class operator*[6] [300, 301]. The trace of a trace class operator $T : [a,b] \rightarrow [a,b]$ with Kernel function $t(x,y)$ is given by the direct continuous analog of the matrix trace:

$$\mathrm{tr}(T) = \int_a^b t(x,x)\,\mathrm{d}x\,. \tag{7.29}$$

The trace of $\boldsymbol{Z}$ is related to the total mean photon number of the state (cf. eq. (6.24)) by

$$\mu = \frac{1}{2}\,\mathrm{tr}(\boldsymbol{Z})\,. \tag{7.30}$$

The expressions in the time domain and in the frequency domain can be simplified by rearranging the order of the creation and annihilation operators:

$$\hat{\mathbf{a}}^\dagger = \left(\hat{a}_\mathrm{s}^\dagger, \hat{a}_\mathrm{i}^\dagger, \hat{a}_\mathrm{s}, \hat{a}_\mathrm{i}\right) \quad \rightarrow \quad \hat{\mathbf{a}}^\dagger = \left(\hat{a}_\mathrm{s}^\dagger, \hat{a}_\mathrm{i}, \hat{a}_\mathrm{s}, \hat{a}_\mathrm{i}^\dagger\right). \tag{7.31}$$

The reordering is a unitary transformation[7] and therefore it does not change the determinant. Knowing that the final expression for the detection probabilities in the time domain depend on $\det(\mathbb{1} + \boldsymbol{W}\boldsymbol{Z})$ and that $\boldsymbol{Z}$ and $\tilde{\boldsymbol{Z}}$ are related by the Fourier transformation and projections, the reordering can already be applied in the frequency domain:

$$\det\!\left(\mathbb{1} + \boldsymbol{W}\tilde{\boldsymbol{Z}}\right) = \det\!\left[\mathbb{1} + \boldsymbol{W}\begin{pmatrix} \tilde{\boldsymbol{\Theta}} & \mathbf{0} \\ \mathbf{0} & \tilde{\boldsymbol{\Theta}}^* \end{pmatrix}\right] = \left|\det\!\left(\mathbb{1} + \mathrm{diag}(\boldsymbol{w})\tilde{\boldsymbol{\Theta}}\right)\right|^2. \tag{7.32}$$

The matrix of operators $\tilde{\boldsymbol{\Theta}}$ is obtained by swapping the second and the last rows and columns of $\tilde{\boldsymbol{\Gamma}}_\perp$ and $\tilde{\boldsymbol{\Gamma}}_\parallel$ from eqs. (7.21) and (7.26):

$$\tilde{\boldsymbol{\Theta}} = \frac{1}{2}\begin{array}{c} \begin{array}{cc} \hat{a}_\mathrm{A}(\omega') & \hat{a}_\mathrm{B}^\dagger(\omega') \end{array} \\ \begin{pmatrix} \tilde{\mathfrak{u}}[\cosh(\boldsymbol{X}) - \mathbb{1}]\tilde{\mathfrak{u}}^\dagger & \tilde{\mathfrak{u}}\sinh(\boldsymbol{X})\tilde{\mathfrak{v}}^\dagger \\ \tilde{\mathfrak{v}}\sinh(\boldsymbol{X})\tilde{\mathfrak{u}}^\dagger & \tilde{\mathfrak{v}}[\cosh(\boldsymbol{X}) - \mathbb{1}]\tilde{\mathfrak{v}}^\dagger \end{pmatrix} \end{array} \begin{array}{c} \\ \hat{a}_\mathrm{A}^\dagger(\omega) \\ \hat{a}_\mathrm{B}(\omega) \end{array} \tag{7.33}$$

For parallel photons $\tilde{\mathfrak{u}}$ and $\tilde{\mathfrak{v}}$ are $\tilde{\mathfrak{u}}_\mathrm{A}$ and $\tilde{\mathfrak{v}}_\mathrm{B}$ given by eq. (7.25), but the index is dropped in the following to simplify the notation. When $\chi\sigma_0 \ll 1$, such that the cosh function can be

[6] A compact linear operator T is a trace class operator if the sum over its singular values, that is the sum of the square roots of the eigenvalues of $T^\dagger T$, is finite [300, 301]. The values of w_s in $\boldsymbol{W}$ are between 0 and 1 (cf. eqs. (6.50) to (6.54)), meaning that $\mathrm{tr}(\boldsymbol{W}\boldsymbol{Z}) \leq \mathrm{tr}(\boldsymbol{Z})$. Therefore, $\boldsymbol{W}\boldsymbol{Z}$ is a trace-class operator as well.

[7] The transformation matrix for the reordering is given by $\boldsymbol{U} = \left(\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{smallmatrix}\right)$.

expanded to the second order, from eqs. (7.21), (7.22) and (7.30) it follows $\chi \approx 2\sqrt{\mu_\mathrm{p}}$ for orthogonal photons and $\chi \approx \sqrt{2\mu_\mathrm{p}}$ for parallel photons. The diagonal matrix $\boldsymbol{X}$ contains the singular values and is given by

$$\boldsymbol{X} = \begin{cases} \chi\,\boldsymbol{\Sigma}_\perp \approx 2\sqrt{\mu_\mathrm{p}}\boldsymbol{\Sigma}_\perp & \text{for orthogonally polarized photons and} \\ 2\chi\,\boldsymbol{\Sigma}_\parallel \approx 2\sqrt{2\mu_\mathrm{p}}\boldsymbol{\Sigma}_\parallel & \text{for parallel polarized photons.} \end{cases} \tag{7.34}$$

Equation (7.33) represents the state after SPDC and demultiplexing and will be further transformed to model the setup.

Modeling the Interferometer in the Photon Pair Source

The IF in the PPS splits the SHG pulses into two separate pulses with a delay determined by the OPD of the IF. The SPDC process is pumped with a coherent double pulse given by $\tilde{\alpha}_{\mathrm{s+l}}(\omega_\mathrm{s}+\omega_\mathrm{i}) = \tilde{\alpha}(\omega_\mathrm{s}+\omega_\mathrm{i})\big(c_\mathrm{s}\,\mathrm{e}^{\mathrm{i}L_{\mathrm{P,s}}[2k_0-(\omega_\mathrm{s}+\omega_\mathrm{i}-2\omega_0)/v_\mathrm{g}]} + c_\mathrm{l}\,\mathrm{e}^{\mathrm{i}L_{\mathrm{P,l}}[2k_0-(\omega_\mathrm{s}+\omega_\mathrm{i}-2\omega_0)/v_\mathrm{g}]}\big)$. The coefficients c_s and c_l are determined by the beam splitter coupling and transmission coefficients of the short and long arm of the pump IF. For simplicity, it is assumed that c_s and c_l are real, as their constant complex phases could always be absorbed into the $\mathrm{e}^{\mathrm{i}2Lk_0}$ terms. Furthermore, they are normalized to $|c_\mathrm{s}|^2 + |c_\mathrm{l}|^2 = 1$ to keep the JSA normalized, and the amplitude is absorbed into χ. For ideal 50/50 beam splitters and identical transmission losses in both IF arms, $c_\mathrm{s} = c_\mathrm{l} = 1/\sqrt{2}$.

The JSA of the SPDC state generated by the double pulses is given by

$$\tilde{\psi}_{\mathrm{s+l}}(\omega_\mathrm{s},\omega_\mathrm{i}) = \tilde{\psi}(\omega_\mathrm{s},\omega_\mathrm{i})\big(c_\mathrm{s}\,\mathrm{e}^{\mathrm{i}L_{\mathrm{P,s}}[2k_0-(\omega_\mathrm{s}+\omega_\mathrm{i}-2\omega_0)/v_\mathrm{g}]} + c_\mathrm{l}\,\mathrm{e}^{\mathrm{i}L_{\mathrm{P,l}}[2k_0-(\omega_\mathrm{s}+\omega_\mathrm{i}-2\omega_0)/v_\mathrm{g}]}\big)\,. \tag{7.35}$$

By introducing integral operators $\tilde{\mathcal{R}}_{\mathrm{P},\gamma}$ for the phase rotation with kernel functions

$$\tilde{R}_{\mathrm{P},\gamma}(\omega,\omega') = \mathrm{e}^{\mathrm{i}L_{\mathrm{P},\gamma}(k_0-\omega_0/v_\mathrm{g})}\,\mathrm{e}^{\mathrm{i}\omega L_{\mathrm{P},\gamma}/v_\mathrm{g}}\,\delta(\omega-\omega') \quad \text{and} \quad \gamma \in \{\mathrm{s},\mathrm{l}\}\,, \tag{7.36}$$

the Schmidt decomposition of $\tilde{\Psi}_{\mathrm{s+l}}$ can be expressed in terms of $\tilde{\Psi} = \tilde{\mathfrak{u}}\boldsymbol{\Sigma}\tilde{\mathfrak{v}}$:

$$\tilde{\Psi}_{\mathrm{s+l}} = c_\mathrm{s}\tilde{\mathfrak{u}}_\mathrm{s}\boldsymbol{\Sigma}\tilde{\mathfrak{v}}_\mathrm{s}^\dagger + c_\mathrm{l}\tilde{\mathfrak{u}}_\mathrm{l}\boldsymbol{\Sigma}\tilde{\mathfrak{v}}_\mathrm{l}^\dagger \quad \text{with} \quad \tilde{\mathfrak{u}}_\gamma = \tilde{\mathcal{R}}_{\mathrm{P},\gamma}\tilde{\mathfrak{u}}\,, \quad \tilde{\mathfrak{v}}_\gamma = \tilde{\mathcal{R}}_{\mathrm{P},\gamma}^\dagger\tilde{\mathfrak{v}}\,. \tag{7.37}$$

When in eq. (7.18) $\tilde{\boldsymbol{\Gamma}}$ is calculated with $\tilde{\Psi}_{\mathrm{s+l}}$ instead of $\tilde{\Psi}$, the products $\tilde{\Psi}_{\mathrm{s+l}}^\dagger\tilde{\Psi}_{\mathrm{s+l}}$ and $\tilde{\Psi}_{\mathrm{s+l}}\tilde{\Psi}_{\mathrm{s+l}}^\dagger$ yield terms containing the products $\tilde{\mathfrak{u}}_\mathrm{s}^\dagger\tilde{\mathfrak{u}}_\mathrm{l}$ and $\tilde{\mathfrak{v}}_\mathrm{s}\tilde{\mathfrak{v}}_\mathrm{l}^\dagger$ and vice versa, such that for example

$$\tilde{\Psi}_{\mathrm{s+l}}^\dagger\tilde{\Psi}_{\mathrm{s+l}} = c_\mathrm{s}^2\tilde{\mathfrak{v}}_\mathrm{s}^\dagger\boldsymbol{\Sigma}^2\tilde{\mathfrak{v}}_\mathrm{s}^\dagger + c_\mathrm{l}^2\tilde{\mathfrak{v}}_\mathrm{l}\boldsymbol{\Sigma}^2\tilde{\mathfrak{v}}_\mathrm{l}^\dagger + c_\mathrm{s}c_\mathrm{l}\tilde{\mathfrak{v}}_\mathrm{s}\boldsymbol{\Sigma}\underbrace{\tilde{\mathfrak{u}}_\mathrm{s}^\dagger\tilde{\mathfrak{u}}_\mathrm{l}}_{=0}\boldsymbol{\Sigma}\tilde{\mathfrak{v}}_\mathrm{l}^\dagger + c_\mathrm{s}c_\mathrm{l}\tilde{\mathfrak{v}}_\mathrm{l}\boldsymbol{\Sigma}\underbrace{\tilde{\mathfrak{u}}_\mathrm{l}^\dagger\tilde{\mathfrak{u}}_\mathrm{s}}_{=0}\boldsymbol{\Sigma}\tilde{\mathfrak{v}}_\mathrm{s}^\dagger\,. \tag{7.38}$$

The last two terms vanish, which can be seen by evaluating, for example, $(\tilde{\mathfrak{u}}_\mathrm{s}^\dagger \tilde{\mathfrak{u}}_\mathrm{l})_{ij}$ in the time domain. Using the Parseval-Plancherel identity eq. (A.8) and identifying the result as the autocorrelation of $u_i(t)$ yields, with $\Delta L_\mathrm{P} = L_{\mathrm{P},l} - L_{\mathrm{P},s}$,

$$(\tilde{\mathfrak{u}}_\mathrm{s}^\dagger \tilde{\mathfrak{u}}_\mathrm{l})_{ij} = \int \mathrm{e}^{\mathrm{i}\Delta L_\mathrm{P}(k_0+\omega-\omega_0)/v_\mathrm{g}} \tilde{u}_i^*(\omega)\tilde{u}_j(\omega)\,\mathrm{d}\omega = \mathrm{e}^{\mathrm{i}\Delta L_\mathrm{P}(k_0-\omega_0)/v_\mathrm{g}}(u_i \star u_i)\left(-\frac{\Delta L_\mathrm{P}}{v_\mathrm{g}}\right)\delta_{ij}\,. \tag{7.39}$$

As the two halves of the pump pulse are well separated in the time domain so that they do not overlap, the autocorrelation of the basis functions at a delay $\Delta L_\mathrm{P}/v_\mathrm{g}$ of the IF is zero.

Therefore, by defining $\boldsymbol{X}_\gamma = c_\gamma \boldsymbol{X}$, the SPDC state is represented by

$$\tilde{\boldsymbol{\Theta}}_\mathrm{s+l} = \frac{1}{2} \sum_{\gamma\in\{\mathrm{s,l}\}} \begin{pmatrix} \tilde{\mathfrak{u}}_\gamma[\cosh(\boldsymbol{X}_\gamma) - \mathbb{1}]\tilde{\mathfrak{u}}_\gamma^\dagger & \tilde{\mathfrak{u}}_\gamma \sinh(\boldsymbol{X}_\gamma)\tilde{\mathfrak{v}}_\gamma^\dagger \\ \tilde{\mathfrak{v}}_\gamma \sinh(\boldsymbol{X}_\gamma)\tilde{\mathfrak{u}}_\gamma^\dagger & \tilde{\mathfrak{v}}_\gamma[\cosh(\boldsymbol{X}_\gamma) - \mathbb{1}]\tilde{\mathfrak{v}}_\gamma^\dagger \end{pmatrix}. \tag{7.40}$$

Propagation in the Fiber Links and Transformation to the Time Domain

The rest of the setup is modeled with the same transformations as shown in fig. 6.1 (a). Frequency-dependent transmissions and phase rotations due to propagation and chromatic dispersion in the fiber links are modeled by introducing the operators $\tilde{\boldsymbol{T}}_\mathrm{fib}$ and $\tilde{\boldsymbol{R}}_\mathrm{fib}$[8]:

$$\tilde{\boldsymbol{T}}_\mathrm{fib} = \begin{pmatrix} \tau_\mathrm{fib}^{(\mathrm{A})}(\omega) & 0 \\ 0 & \tau_\mathrm{fib}^{(\mathrm{B})}(\omega) \end{pmatrix} \quad \text{and} \quad \tilde{\boldsymbol{R}}_\mathrm{fib} = \begin{pmatrix} \mathrm{e}^{\mathrm{i}\phi_\mathrm{fib}^{(\mathrm{A})}(\omega)} & 0 \\ 0 & \mathrm{e}^{-\mathrm{i}\phi_\mathrm{fib}^{(\mathrm{B})}(\omega)} \end{pmatrix}. \tag{7.41}$$

Here, $\phi_\mathrm{fib}^{(\mathrm{A/B})}(\omega) = k(\omega)L_\mathrm{fib}^{(\mathrm{A/B})}$ represents the propagation in the fiber links of lengths $L_\mathrm{fib}^{(\mathrm{A/B})}$ with the quadratic phase in $k(\omega)$ describing the acquired chirp due to chromatic dispersion and $\tau_\mathrm{fib}(\omega)$ is the real-valued frequency-dependent transmission function. For the implementation, the dependence of the transmission loss over the frequency intervals of the photons is neglected because around the center wavelength of 1550 nm, the attenuation shows a flat minimum (cf. fig. 1.5). Therefore, $\tau_\mathrm{fib}(\omega)$ only comprises the transmission function of the WDM channels (cf. fig. 2.15).

[8] The notation with a function of a single argument such as $t(\omega)$ as matrix element is here used to represent the integral operator with kernel $K(\omega,\omega') = t(\omega)\delta(\omega-\omega')$. Applying it to some function $f(\omega)$ yields $\int t(\omega)\delta(\omega-\omega')f(\omega')\,\mathrm{d}\omega = t(\omega)f(\omega)$. The negative sign in the exponent for the phase rotation in the lower right block is due to the reordering of matrix elements in eq. (7.31). In the covariance formalism, losses in general are modeled by applying a transmission matrix $\boldsymbol{T}$ according to eq. (C.8) to $\boldsymbol{\Gamma}$ as $\boldsymbol{\Gamma}' = \boldsymbol{T}\boldsymbol{\Gamma}\boldsymbol{T} + (1-\boldsymbol{T}^2)\mathbb{1}$. For $\boldsymbol{Z} = (\boldsymbol{\Gamma} - \mathbb{1})/2$ this simplifies to the transformation $\boldsymbol{Z}' = \boldsymbol{T}\boldsymbol{Z}\boldsymbol{T}$ and analogously for $\boldsymbol{\Theta}$, so that $\tilde{\boldsymbol{T}}_\mathrm{fib}$ is directly applied to $\tilde{\boldsymbol{\Theta}}_\mathrm{s+l}$.

At this point it is convenient to transform $\tilde{\boldsymbol{\Theta}}$ to the time domain by applying the unitary IFT operator $\mathcal{F}^{-1}$ with $(\mathcal{F}^{-1}\tilde{f})(t) = (2\pi)^{-1/2}\int \mathrm{e}^{-\mathrm{i}\omega t}\tilde{f}(\omega)\,\mathrm{d}\omega$. Collecting the IFT operators into $\boldsymbol{F}^{-1} = \mathcal{F}^{-1} \oplus \left(\mathcal{F}^{-1}\right)^*$ yields $\boldsymbol{\Theta}_{\mathrm{fib}}$ in the time domain:

$$\boldsymbol{\Theta}_{\mathrm{fib}} = \boldsymbol{F}^{-1}\tilde{\boldsymbol{R}}_{\mathrm{fib}}\tilde{\boldsymbol{T}}_{\mathrm{fib}}\tilde{\boldsymbol{\Theta}}_{\mathrm{s+l}}\tilde{\boldsymbol{T}}^{\dagger}_{\mathrm{fib}}\tilde{\boldsymbol{R}}^{\dagger}_{\mathrm{fib}}\left(\boldsymbol{F}^{-1}\right)^{\dagger}. \tag{7.42}$$

Introducing $\exp\left(\mathrm{i}\phi_0^{(\gamma)}\right) = \exp\left(\mathrm{i}L_{\mathrm{P},\gamma}(k_0 - \omega_0/v_{\mathrm{g}})\right)$, $T_{\mathrm{P},\gamma} = L_{\mathrm{P},\gamma}/v_{\mathrm{g}}$ and

$$\boldsymbol{u}^{\mathsf{T}}_{\gamma,\mathrm{A}}(t) = \exp\left(\mathrm{i}\phi_0^{(\gamma)}\right)\mathcal{F}_{\omega}^{-1}\left(\mathrm{e}^{\mathrm{i}\phi^{(\mathrm{A})}_{\mathrm{fib}}(\omega)}\tau^{(\mathrm{A})}_{\mathrm{fib}}(\omega)\tilde{\boldsymbol{u}}^{\mathsf{T}}_{\gamma}(\omega)\right)(t - T_{\mathrm{P},\gamma}) \quad \text{and} \tag{7.43}$$

$$\boldsymbol{v}^{\mathsf{T}}_{\gamma,\mathrm{B}}(t) = \exp\left(-\mathrm{i}\phi_0^{(\gamma)}\right)\left(\mathcal{F}_{\omega}^{-1}\right)^*\left(\mathrm{e}^{-\mathrm{i}\phi^{(\mathrm{B})}_{\mathrm{fib}}(\omega)}\tau^{(\mathrm{B})}_{\mathrm{fib}}(\omega)\tilde{\boldsymbol{v}}^{\mathsf{T}}_{\gamma}(\omega)\right)(t - T_{\mathrm{P},\gamma}), \tag{7.44}$$

with $\tilde{\boldsymbol{u}}^{\mathsf{T}}(\omega)$ and $\tilde{\boldsymbol{v}}^{\mathsf{T}}(\omega)$ defined in eq. (7.12), yields the matrix of kernels

$$\boldsymbol{\Theta}_{\mathrm{fib}}(t,t') = \frac{1}{2}\sum_{\gamma\in\{\mathrm{s,l}\}}\begin{pmatrix} \boldsymbol{u}^{\mathsf{T}}_{\gamma,\mathrm{A}}(t)[\cosh(\boldsymbol{X}_{\gamma}) - \mathbb{1}]\boldsymbol{u}^{*}_{\gamma,\mathrm{A}}(t') & \boldsymbol{u}^{\mathsf{T}}_{\gamma,\mathrm{A}}(t)\sinh(\boldsymbol{X}_{\gamma})\boldsymbol{v}^{*}_{\gamma,\mathrm{B}}(t') \\ \boldsymbol{v}^{\mathsf{T}}_{\gamma,\mathrm{B}}(t)\sinh(\boldsymbol{X}_{\gamma})\boldsymbol{u}^{*}_{\gamma,\mathrm{A}}(t') & \boldsymbol{v}^{\mathsf{T}}_{\gamma,\mathrm{B}}(t)[\cosh(\boldsymbol{X}_{\gamma}) - \mathbb{1}]\boldsymbol{v}^{*}_{\gamma,\mathrm{B}}(t') \end{pmatrix}. \tag{7.45}$$

Receiver Interferometers

The receiver modules are modeled by applying a sequence of transformations to the state consisting of a combination of transformations for beam splitters, losses, and phase shifts:

1. The beam splitters of the interferometers couple the light with coupling coefficients $\kappa^2_{\mathrm{A/B}}$ to the short arms and with $1-\kappa^2_{\mathrm{A/B}}$ to the long arms. The transformation matrix for the first pass through the beam splitter is $\tilde{\boldsymbol{B}}^{(\mathrm{I})}$.

2. Losses and phase shifts due to propagation in the interferometer arms are described by the transmission matrix $\tilde{\boldsymbol{T}}_{\mathrm{IF}}$ and phase rotation matrix $\tilde{\boldsymbol{R}}_{\mathrm{IF}}$ defined analogously to $\tilde{\boldsymbol{T}}_{\mathrm{fib}}$ and $\tilde{\boldsymbol{R}}_{\mathrm{fib}}$ in eq. (7.41).

3. Imperfect interference modeled by the mode mismatch model from ref. [101] is represented by the beam splitter transformation $\tilde{\boldsymbol{B}}^{(\mathrm{II})}_{\mathrm{MM}}$ for the second pass through the IF's beam splitter. The transformation $\tilde{\boldsymbol{B}}^{(\mathrm{II})}_{\mathrm{MM}}$ is constructed from elementary beam splitter transformations as shown in fig. 6.2.

4. Losses from the detector efficiencies are represented by $\tilde{\boldsymbol{T}}_{\mathrm{det}}$.

The photons are detected in the three time bins E, C, or L. Projections onto the corresponding time intervals $i \in I_{\mathrm{E}}, I_{\mathrm{C}}, I_{\mathrm{L}}$ for detectors $d \in \{0,1\}$ are represented by applying time-domain projection operators $\mathcal{P}_{u,i_d}$. For each user $u \in \{\mathrm{A},\mathrm{B}\}$, the projections for all time bins and both detectors are collected into $\boldsymbol{P}_u$ and the projections of Alice and Bob are summarized into $\boldsymbol{P} = \boldsymbol{P}_\mathrm{A} \oplus \boldsymbol{P}_\mathrm{B}$.

The final operator $\boldsymbol{\Theta}_\mathrm{f}$ after applying all transformations in the receivers is given by

$$\boldsymbol{\Theta}_\mathrm{f} = \boldsymbol{P}\boldsymbol{S}_\mathrm{recv}\begin{pmatrix}\boldsymbol{\Theta}_\mathrm{fib} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{0}_{10\times 10}\end{pmatrix}\boldsymbol{S}_\mathrm{recv}^\dagger\boldsymbol{P} \quad \text{with} \quad \boldsymbol{S}_\mathrm{recv} = \boldsymbol{F}^{-1}\tilde{\boldsymbol{T}}_\mathrm{det}\tilde{\boldsymbol{B}}^{(\mathrm{II})}_\mathrm{MM}\tilde{\boldsymbol{R}}_\mathrm{IF}\tilde{\boldsymbol{T}}_\mathrm{IF}\tilde{\boldsymbol{B}}^{(\mathrm{I})}\left(\boldsymbol{F}^{-1}\right)^\dagger . \tag{7.46}$$

The matrix $\boldsymbol{\Theta}_\mathrm{f}$ consists of 12×12 operator blocks for the four detectors, each receiving three spatial mode groups due to the mode mismatch. The matrix $\boldsymbol{\Theta}_\mathrm{fib}$ consists only of 2×2 blocks. Therefore, the matrix size is extended by inserting zero blocks representing the additional modes in the vacuum state before they are coupled to the modes of $\boldsymbol{\Theta}_\mathrm{fib}$ by beam splitters.

Size Reduction of the Block Matrix Structure

Similar to eq. (7.41), each of the transformation matrices in $\boldsymbol{S}_\mathrm{recv}$ is block-diagonal because the transformations for the different spatial mode groups are independent. In eq. (7.46), only the first two columns of $\boldsymbol{S}_\mathrm{recv}$ are relevant because they are multiplied with $\boldsymbol{\Theta}_\mathrm{fib}$ and the other ten columns are multiplied with zeros. Equation (7.46) can therefore also be written as

$$\boldsymbol{\Theta}_\mathrm{f} = \begin{pmatrix}\boldsymbol{P}_\mathrm{A}\boldsymbol{s}_\mathrm{A} & 0\\ 0 & \boldsymbol{P}_\mathrm{B}\boldsymbol{s}_\mathrm{B}^*\end{pmatrix}\boldsymbol{\Theta}_\mathrm{fib}\begin{pmatrix}\boldsymbol{s}_\mathrm{A}^\dagger\boldsymbol{P}_\mathrm{A} & 0\\ 0 & \boldsymbol{s}_\mathrm{B}^\mathsf{T}\boldsymbol{P}_\mathrm{B}\end{pmatrix} , \tag{7.47}$$

with vectors of operators $\boldsymbol{s}_\mathrm{A}$ and $\boldsymbol{s}_\mathrm{B}$ given by $\boldsymbol{s} = \mathcal{F}^{-1}\tilde{\boldsymbol{s}}\mathcal{F}$ and $\tilde{\boldsymbol{s}}$ given by

$$\tilde{\boldsymbol{s}} = \begin{pmatrix}\big(\eta_0\xi\big(\mathrm{e}^{\mathrm{i}\phi_\mathrm{s}}\kappa^2\tau_\mathrm{s} + \mathrm{e}^{\mathrm{i}\phi_\mathrm{l}}r^2\tau_\mathrm{l}\big)\big)(\omega)\\ \big(\eta_1\kappa r\xi\big(\mathrm{e}^{\mathrm{i}\phi_\mathrm{s}}\tau_\mathrm{s} - \mathrm{e}^{\mathrm{i}\phi_\mathrm{l}}\tau_\mathrm{l}\big)\big)(\omega)\\ \big(\mathrm{e}^{\mathrm{i}\phi_\mathrm{s}}\tau_\mathrm{s}\eta_0\kappa^2\sqrt{1-\xi^2}\big)(\omega)\\ \big(\mathrm{e}^{\mathrm{i}\phi_\mathrm{s}}\tau_\mathrm{s}\eta_1\kappa r\sqrt{1-\xi^2}\big)(\omega)\\ \big(\mathrm{e}^{\mathrm{i}\phi_\mathrm{l}}\tau_\mathrm{l}\eta_0 r^2\sqrt{1-\xi^2}\big)(\omega)\\ \big(-\mathrm{e}^{\mathrm{i}\phi_\mathrm{l}}\tau_\mathrm{l}\eta_1\kappa r\sqrt{1-\xi^2}\big)(\omega)\end{pmatrix}\begin{array}{l} X_1\\ Y_1\\ X_2\\ Y_2\\ X_3\\ Y_3\end{array} . \tag{7.48}$$

The entries depend on the parameters of the components in Alice's and Bob's IFs, and in general, $\tilde{\boldsymbol{s}}_\mathrm{A}$ and $\tilde{\boldsymbol{s}}_\mathrm{B}$ are different. The labels X_1 to Y_3 enumerate the modes of the mode mismatch model from ref. [101] as shown in fig. 6.2. The first two entries of $\tilde{\boldsymbol{s}}$ represent the interfering modes, and the last four represent the non-interfering modes. The vector $\tilde{\boldsymbol{s}}_\mathrm{A}$ is given by the first column of a 6×6 matrix obtained by successive application of the transformations in one receiver IF, that is of the beam splitter transformation with the coupling coefficient κ and $r = \sqrt{1-\kappa^2}$, phase shifts ϕ and transmissions τ for both IF arms, the mode mismatch transformation with the mismatch parameter ξ for the interference at the beam splitter consisting of five individual beam splitter transformations (cf. fig. 6.2), and the transmissions η representing the detector efficiencies.

Direct handling of the 12×12 operator block matrix $\boldsymbol{\Theta}_\mathrm{f}$ from eq. (7.46) is rather inconvenient. Fortunately, the size of the matrix for which the determinant is computed can be reduced to 2×2 blocks by applying Sylvester's determinant theorem[9], such that the determinant can be written as

$$\det(\mathbb{1}_{12\times 12} + \boldsymbol{W}_\mathrm{AB}\boldsymbol{\Theta}_\mathrm{f}) = \det(\mathbb{1}_{2\times 2} + \boldsymbol{\Xi})\,, \tag{7.49}$$

with the diagonal matrix $\boldsymbol{W}_\mathrm{AB} = \boldsymbol{W}_\mathrm{A} \oplus \boldsymbol{W}_\mathrm{B}$ containing the differentiation parameters, and

$$\boldsymbol{\Xi} = \begin{pmatrix} \tilde{\boldsymbol{s}}_\mathrm{A}^\dagger \boldsymbol{W}_\mathrm{A} \boldsymbol{P}_\mathrm{A} \tilde{\boldsymbol{s}}_\mathrm{A} & 0 \\ 0 & \tilde{\boldsymbol{s}}_\mathrm{B}^\mathrm{T} \boldsymbol{W}_\mathrm{B} \boldsymbol{P}_\mathrm{B} \tilde{\boldsymbol{s}}_\mathrm{B}^* \end{pmatrix} \boldsymbol{\Theta}_\mathrm{fib}\,. \tag{7.50}$$

The parameters η, κ, r, and τ are, in general, slowly varying frequency-dependent functions. However, over the narrow frequency range of a DWDM channel, they are assumed to be frequency-independent to simplify the calculation. Furthermore, it is assumed that the CD in the IFs is negligible, such that the phase acquired along an IF arm of length L is given by $\phi(\omega) = k_0 L + (\omega - \omega_0)L/v_\mathrm{g}$. Thereby, the kernel of the phase rotation operator in the time domain becomes $\big(\mathcal{F}^{-1}\,\mathrm{e}^{\mathrm{i}\phi(\omega)}\mathcal{F}\big)(t,t') = \mathrm{e}^{\mathrm{i}(k_0 L - \omega_0 L/v_\mathrm{g})}\delta(L/v_\mathrm{g} + t' - t)$. The expression $\boldsymbol{s}_u^\dagger \boldsymbol{W}_u \boldsymbol{P}_u \boldsymbol{s}_u$ for a single user $u \in \{\mathrm{A}, \mathrm{B}\}$ is essentially an inner product of $\boldsymbol{s}_u^\dagger$ and $\boldsymbol{s}_u$, weighted with the entries of $\boldsymbol{W}_u \boldsymbol{P}_u$:

$$(\boldsymbol{s}_u^\dagger \boldsymbol{W}_u \boldsymbol{P}_u \boldsymbol{s}_u)(t,t') = \sum_{\substack{\alpha,\beta \in \{\mathrm{s},\mathrm{l}\} \\ d \in \{0,1\},\, i_d}} C_{\alpha,\beta}^{(d,u)} \delta\Big(T_\beta^{(u)} - T_\alpha^{(u)} + t' - t\Big) w_{\Delta i_d}^{(u,d)}\, \mathrm{rect}_{\Delta i_d}^{(d,u)}\Big(T_\beta^{(u)} + t'\Big)\,. \tag{7.51}$$

Here, $T_\alpha^{(u)} = L_\alpha^{(u)}/v_\mathrm{g}$ and $T_\beta^{(u)} = L_\beta^{(u)}/v_\mathrm{g}$. The variables α and β enumerate the short and long IF paths s and l and the detectors are labeled by $d \in \{0,1\}$. The coefficients are given by $C_{\alpha,\beta}^{(d,u)} = c_{\alpha,\beta}^{(d,u)} \exp\big(\mathrm{i}(k_0 - \omega_0/v_\mathrm{g})(L_\alpha^{(u)} - L_\beta^{(u)})\big)$ with $c_{\alpha,\beta}^{(d,u)}$ given by table 7.1. The rectangle function represents the time-domain projection onto an interval of width Δi_d centered around its argument. The widths Δi_d can differ for different users and detectors. The summation over i_d takes into account that the projection for a detector can consist of multiple time intervals.

[9] Sylvester's determinant theorem states that $\det(\mathbb{1}_m + \boldsymbol{AB}) = \det(\mathbb{1}_n + \boldsymbol{BA})$ for matrices $\boldsymbol{A}_{m\times n}$ and $\boldsymbol{B}_{n\times m}$ [302]. This relation is also valid for trace class operators [300].

Table 7.1: Table of coefficients $c_{\alpha,\beta}^{(d,u)}$ of the kernels of $\varXi$ for the path combinations $\alpha, \beta \in \{\mathrm{s}, \mathrm{l}\}$ and detectors $d \in \{0, 1\}$. In general, the coefficients are different for different users u.

$c_{\alpha,\beta}^{(d,u)}$	s, s	s, l	l, s	l, l
Detector 0	$(\eta_0 \tau_\mathrm{s} \kappa^2)^2$	$(\eta_0 \xi \kappa r)^2 \tau_\mathrm{s} \tau_\mathrm{l}$	$(\eta_0 \xi \kappa r)^2 \tau_\mathrm{s} \tau_\mathrm{l}$	$(\eta_0 \tau_\mathrm{l} r^2)^2$
Detector 1	$(\eta_1 \tau_\mathrm{s} \kappa r)^2$	$-(\eta_1 \xi \kappa r)^2 \tau_\mathrm{s} \tau_\mathrm{l}$	$-(\eta_1 \xi \kappa r)^2 \tau_\mathrm{s} \tau_\mathrm{l}$	$(\eta_1 \tau_\mathrm{l} \kappa r)^2$

The kernels of $\varXi$ are obtained from eq. (7.50) with $t_{\alpha,\beta}^{(u)} = t + T_\alpha^{(u)} - T_\beta^{(u)}$:

$$\varXi(t, t') = \frac{1}{2} \sum_{\substack{\gamma,\alpha,\beta \in \{\mathrm{s},\mathrm{l}\} \\ d \in \{0,1\},\, i_d}} \begin{pmatrix} C_{\alpha,\beta}^{(d,\mathrm{A})} w_{i_d}^{(d,\mathrm{A})} \operatorname{rect}_{\Delta i_d}^{(d,\mathrm{A})}\Big(T_\alpha^{(\mathrm{A})} + t\Big) & 0 \\ 0 & C_{\alpha,\beta}^{*(d,\mathrm{B})} w_{i_d}^{(d,\mathrm{B})} \operatorname{rect}_{\Delta i_d}^{(d,\mathrm{B})}\Big(T_\alpha^{(\mathrm{B})} + t\Big) \end{pmatrix}$$
$$\times \begin{pmatrix} \boldsymbol{u}_{\gamma,\mathrm{A}}^{\mathsf{T}}\Big(t_{\alpha,\beta}^{(\mathrm{A})}\Big)[\cosh(\boldsymbol{X}_\gamma) - \mathbb{1}]\boldsymbol{u}_{\gamma,\mathrm{A}}^{*}(t') & \boldsymbol{u}_{\gamma,\mathrm{A}}^{\mathsf{T}}\Big(t_{\alpha,\beta}^{(\mathrm{A})}\Big) \sinh(\boldsymbol{X}_\gamma) \boldsymbol{v}_{\gamma,\mathrm{B}}^{*}(t') \\ \boldsymbol{v}_{\gamma,\mathrm{B}}^{\mathsf{T}}\Big(t_{\alpha,\beta}^{(\mathrm{B})}\Big) \sinh(\boldsymbol{X}_\gamma) \boldsymbol{u}_{\gamma,\mathrm{A}}^{*}(t') & \boldsymbol{v}_{\gamma,\mathrm{B}}^{\mathsf{T}}\Big(t_{\alpha,\beta}^{(\mathrm{B})}\Big)[\cosh(\boldsymbol{X}_\gamma) - \mathbb{1}]\boldsymbol{v}_{\gamma,\mathrm{B}}^{*}(t') \end{pmatrix}. \tag{7.52}$$

7.4 Approximations for the Computation of Detection Probabilities

When the aspect ratio of the JSA is large because the photons are strongly entangled, a direct discretization of the biphoton wave function requires many points to represent it accurately. Therefore, the computation of the cosh and sinh functions via the SVD and the computation of the determinants become computationally expensive in the limit of strong entanglement. This section presents approximations facilitating the evaluation for strongly entangled biphoton states.

Truncation of the Schmidt Decomposition

The evaluation of the cosh and sinh terms in $\varXi$ requires the Schmidt decomposition of the JSA. The example of the two-dimensional Gaussian JSA showed that the Schmidt decomposition might be a sum of infinitely many terms. It must be truncated after a finite number of terms for numerical computations.

The *Hilbert-Schmidt norm* of $\tilde{\Psi}$ is $\|\tilde{\Psi}\|_{\mathrm{HS}} = \Big(\iint |\tilde{\psi}(\omega, \omega')|^2 \,\mathrm{d}\omega \,\mathrm{d}\omega'\Big)^{1/2}$. The approximation $\tilde{\psi}_N(\omega, \omega') = \sum_{k=0}^{N-1} \sigma_k \tilde{u}_k(\omega) \tilde{v}_k^*(\omega')$ using the largest N Schmidt values is the best possible approximation expressing $\tilde{\psi}$ as a sum of N products of one-dimensional functions $\tilde{u}(\omega)$ and $\tilde{v}(\omega')$ meaning that it minimizes the error in the Hilbert-Schmidt norm $E_{\mathrm{HS}}(N) = \|\tilde{\Psi} - \tilde{\Psi}_N\|_{\mathrm{HS}}$ [293]:

$$E^2_{\mathrm{HS}}(N) = \iint \left|\tilde{\psi}(\omega,\omega') - \tilde{\psi}_N(\omega,\omega')\right|^2 \mathrm{d}\omega\,\mathrm{d}\omega' = \sum_{k=N}^{M-1} \sigma_k^2 = \|\tilde{\Psi}\|^2_{\mathrm{HS}} - \|\tilde{\Psi}_N\|^2_{\mathrm{HS}} \,. \quad (7.53)$$

Therefore, for practical computations, always the components with the largest Schmidt coefficients should be kept. For the normalized JSA, $\|\tilde{\Psi}\|_{\mathrm{HS}} = \sqrt{\sum_k \sigma_k^2} = 1$ such that the error introduced by the truncation is given by

$$E_{\mathrm{HS}}(N) = \left(1 - \sum_{k=0}^{N-1} \sigma_k^2\right)^{1/2} . \quad (7.54)$$

The stronger the entanglement, the more Schmidt modes are required, such that the truncation of the Schmidt components works particularly well for photon pairs that are not too strongly entangled.

Truncation of the Sinh and Cosh Series

When the entanglement is strong, many Schmidt components are required to obtain a sufficiently good approximation of the JSA. In this case, a different approximation can be used. When the total mean photon pair number is low and distributed over many Schmidt modes, the cosh and sinh functions can be approximated by their series expansions truncated after the N-th power,

$$\cosh_N(x) = \sum_{\substack{n=0 \\ n \text{ even}}}^{N} \frac{x^n}{n!} \quad \text{and} \quad \sinh_N(x) = \sum_{\substack{n=0 \\ n \text{ odd}}}^{N} \frac{x^n}{n!} \,. \quad (7.55)$$

The first few terms of the series can be efficiently computed by discretizing the JSA on a fine grid and performing sparse matrix multiplications.

The trace of $\boldsymbol{Z}$ is related to the total mean photon number by eq. (7.30) via $2\mu = \mathrm{tr}(\boldsymbol{Z})$ and it is therefore directly related to the truncation error of the cosh series. By using the mediant inequality[10], the relative error in the total mean photon number μ due to the truncation of the cosh series in eq. (7.40) can be estimated as

$$E_\mu(N) = \frac{\sum_k \cosh(c_\gamma x_k) - \cosh_N(c_\gamma x_k)}{\sum_k[\cosh(c_\gamma x_k) - 1]} \leq \max_\gamma\left(\frac{\cosh(c_\gamma x_0) - \cosh_N(c_\gamma x_0)}{\cosh(c_\gamma x_0) - 1}\right). \tag{7.57}$$

For parallel polarized photons, $x_0 = 2\chi\sigma_{\|,0}$ and for orthogonal polarized photons $x_0 = \chi\sigma_{\perp,0}$ (cf. eq. (7.34)). The coefficient c_γ is close to $1/\sqrt{2}$, corresponding to two half-pulses with equal amplitude. The advantage of using the mediant inequality is that the estimation only requires the computation of the first Schmidt coefficient, which can be obtained efficiently by discretizing the JSA and performing an SVD truncated to the first component.

Expansion of the Determinant

The computation of the detection probabilities for vacuum requires the evaluation of $\sqrt{\det(\mathbb{1} + \boldsymbol{W}\boldsymbol{Z}_\mathrm{f})}$ for the trace-class operator $\boldsymbol{Z}_\mathrm{f} = (\boldsymbol{\Gamma}_\mathrm{f} - \mathbb{1})/2$ and the final covariance $\boldsymbol{\Gamma}_\mathrm{f}$ after all transformations. This type of operator determinant is called a *Fredholm determinant*. Methods for the numerical evaluation of Fredholm determinants are discussed in ref. [304]. The recommended method for smooth kernels is the Nytröm method, approximating the operator determinant by the determinant of a matrix of values obtained by two-dimensional numerical quadrature approximations of the kernel [304]. However, many integration points would be required to approximate JSA with high aspect ratios. One of the simplest quadrature rules would be to replace integrations with Riemann sums, corresponding to the evaluation of the kernel on a rectangular grid and the subsequent computation of the determinant of the resulting discrete matrix.

Another option to evaluate the determinant is to expand it according to the *Plemelj-Smithies formula* for trace class operators [300]:

$$\det(\mathbb{1} + \boldsymbol{W}\boldsymbol{Z}_\mathrm{f}) = \exp\{\mathrm{tr}[\ln(\mathbb{1} + \boldsymbol{W}\boldsymbol{Z}_\mathrm{f})]\} = \exp\left(-\sum_{n=1}^{\infty}\frac{(-1)^n}{n}\,\mathrm{tr}\big((\boldsymbol{W}\boldsymbol{Z}_\mathrm{f})^n\big)\right). \tag{7.58}$$

The expression becomes apparent by recalling that the determinant is the product of the eigenvalues and that the trace is the sum of the eigenvalues. The series converges when

[10] The mediant or "baseball" inequality [303] states that for R ratios $r_i = a_i/b_i$ for non-negative values a_i and positive values b_i with $r_1 \leq r_2 \leq \cdots \leq r_R$ it holds

$$r_1 \leq \frac{a_1 + a_2 + \cdots + a_R}{b_1 + b_2 + \cdots + b_R} \leq r_R\,. \tag{7.56}$$

the absolute values of all eigenvalues of $\boldsymbol{W}\boldsymbol{Z}_\mathrm{f}$ are less than one. From eq. (7.30) it is known that $\mathrm{tr}(\boldsymbol{Z}_\mathrm{f}) = 2\mu$. The total mean photon number per channel pair for the QKD system is $\mu \approx 0.1$. After the SPDC and after all transformations, projections, and losses, the final mean photon number μ is much lower, such that it can be expected that the series in eq. (7.58) converges rapidly. In ref. [VII], a bound for the error from truncating the series expansion is derived.

Publication [VII] also shows that for the parameters of the type-II QKD system, the errors introduced by truncating the cosh and sinh series or the determinant expansion after $N = 2$ are negligible compared to the uncertainties in the measured parameters of the setup. For type-0 SPDC, the aspect ratio of the relevant part of the JSA covering the WDM channels is lower. Therefore, the full SVD is computed because truncating the Schmidt decomposition would introduce additional errors, and the cosh and sinh series are evaluated up to $N = 5$ (cf. appendix D).

The Limit of Poissonian Photon Statistics

Using the complex-valued variant of the covariance formalism and provided that the *Neumann series* [305] $(\mathbb{1} + \boldsymbol{W}\boldsymbol{Z})^{-1} = \mathbb{1} + \sum_{n=1}^{\infty}(-\boldsymbol{W}\boldsymbol{Z})^n$ and the series in eq. (7.58) converge, the generating function for the photon statistics from eq. (6.48) can be written as

$$\begin{aligned} G_0(\boldsymbol{w}) &= \Big[\det(\mathbb{1} + \boldsymbol{W}\boldsymbol{Z})\,\exp\!\Big(\boldsymbol{d}^\dagger(\mathbb{1} + \boldsymbol{W}\boldsymbol{Z})^{-1}\boldsymbol{W}\boldsymbol{d}\Big)\Big]^{-1/2} \\ &= \exp\!\left[-\frac{1}{2}\left(\boldsymbol{d}^\dagger\boldsymbol{W}\boldsymbol{d} + \sum_{n=1}^{\infty}(-1)^n\left(\boldsymbol{d}^\dagger(\boldsymbol{W}\boldsymbol{Z})^n\boldsymbol{W}\boldsymbol{d} - \frac{1}{n}\,\mathrm{tr}\Big((\boldsymbol{W}\boldsymbol{Z})^n\Big)\right)\right)\right]. \end{aligned} \tag{7.59}$$

Truncating the expression after the first contributing orders in $\boldsymbol{d}$ and $\boldsymbol{Z}$ and using eq. (6.24) relates the vacuum detection probability for $\eta = 1$ to the total mean photon number μ:

$$p_\mathrm{vac} = \exp\!\left(-\frac{1}{2}\big(\boldsymbol{d}^\dagger\boldsymbol{d} + \mathrm{tr}(\boldsymbol{Z})\big)\right) = \exp(-\mu)\,. \tag{7.60}$$

This expression is the vacuum detection probability expected for a Poissonian photon number distribution. For QKD simulation with type-II SPDC, $\boldsymbol{d} = \boldsymbol{0}$. Truncating the determinant expansion to $N = 2$ yields for $\boldsymbol{Z}_\mathrm{f}$[11]

$$G_0(\boldsymbol{w}) \approx \exp\!\left[-\frac{1}{2}\left(\mathrm{tr}(\boldsymbol{W}\boldsymbol{Z}_\mathrm{f}) - \frac{1}{2}\,\mathrm{tr}\Big((\boldsymbol{W}\boldsymbol{Z}_\mathrm{f})^2\Big)\right)\right] \tag{7.61}$$

$$\approx \exp\!\left[-\,\mathrm{tr}(\boldsymbol{\Xi}) + \frac{1}{2}\,\mathrm{tr}\Big((\boldsymbol{\Xi}_{(\diagup)})^2\Big)\right]. \tag{7.62}$$

[11] Here it is used that the reordering transformation in eq. (7.31) is unitary and therefore does not change the eigenvalues. Therefore, $\boldsymbol{\Theta}_\mathrm{fib}$ and $\boldsymbol{\Theta}_\mathrm{f}$ are Hermitian and have real eigenvalues. Using eqs. (7.32) and (7.50) and cyclic permutation of the trace yields $\mathrm{tr}\big((\boldsymbol{W}\boldsymbol{Z}_\mathrm{f})^n\big) = 2\,\mathrm{tr}(\boldsymbol{\Xi}^n)$.

Here, $\mathit{\Xi}$ is split up into the block-diagonal part $\mathit{\Xi}_{(\diagdown)}$ and the block-antidiagonal part $\mathit{\Xi}_{(\diagup)}$ by $\mathit{\Xi} = \mathit{\Xi}_{(\diagdown)} + \mathit{\Xi}_{(\diagup)}$, such that $\mathrm{tr}(\mathit{\Xi}^2) = \mathrm{tr}[(\mathit{\Xi}_{(\diagdown)})^2] + \mathrm{tr}[(\mathit{\Xi}_{(\diagup)})^2]$. From eqs. (7.61) to (7.62), the term $\mathrm{tr}[(\mathit{\Xi}_{(\diagdown)})^2]$ describing correlations among detection events of each individual user is neglected because it is of fourth order in $\mathit{\Psi}$, such that the coefficient is small compared to the second-order contributions.

For simulating QKD with photons from type-II SPDC, truncating the sinh and cosh series after $N = 2$ yields the following approximations for the kernels in $\mathit{\Xi}$ (cf. eq. (7.52)):

$$\boldsymbol{u}^{\mathsf{T}}_{\gamma,\mathrm{A}}\Big(t^{(\mathrm{A})}_{\alpha,\beta}\Big)[\cosh_2(\boldsymbol{X}_\gamma) - \mathbb{1}]\boldsymbol{u}^{*}_{\gamma,\mathrm{A}}(t') = \frac{\chi^2 c_\gamma^2}{2} \int \psi^{(\gamma)}_{\mathrm{fib}}\Big(t^{(\mathrm{A})}_{\alpha,\beta} - T_{\mathrm{P},\gamma}, u\Big)\psi^{*(\gamma)}_{\mathrm{fib}}(t' - T_{\mathrm{P},\gamma}, u)\,\mathrm{d}u\,, \tag{7.63}$$

$$\boldsymbol{v}^{\mathsf{T}}_{\gamma,\mathrm{B}}\Big(t^{(\mathrm{B})}_{\alpha,\beta}\Big)[\cosh_2(\boldsymbol{X}_\gamma) - \mathbb{1}]\boldsymbol{v}^{*}_{\gamma,\mathrm{B}}(t') = \frac{\chi^2 c_\gamma^2}{2} \int \psi^{*(\gamma)}_{\mathrm{fib}}\Big(u, t^{(\mathrm{B})}_{\alpha,\beta} - T_{\mathrm{P},\gamma}\Big)\psi^{(\gamma)}_{\mathrm{fib}}(u, t' - T_{\mathrm{P},\gamma})\,\mathrm{d}u\,, \tag{7.64}$$

$$\boldsymbol{u}^{\mathsf{T}}_{\gamma,\mathrm{A}}\Big(t^{(\mathrm{A})}_{\alpha,\beta}\Big)\sinh_2(\boldsymbol{X}_\gamma)\boldsymbol{v}^{*}_{\gamma,\mathrm{B}}(t') = \chi c_\gamma \psi^{(\gamma)}_{\mathrm{fib}}\Big(t^{(\mathrm{A})}_{\alpha,\beta} - T_{\mathrm{P},\gamma}, t' - T_{\mathrm{P},\gamma}\Big)\,, \tag{7.65}$$

$$\boldsymbol{v}^{\mathsf{T}}_{\gamma,\mathrm{B}}\Big(t^{(\mathrm{B})}_{\alpha,\beta}\Big)\sinh_2(\boldsymbol{X}_\gamma)\boldsymbol{u}^{*}_{\gamma,\mathrm{A}}(t') = \chi c_\gamma \psi^{*(\gamma)}_{\mathrm{fib}}\Big(t' - T_{\mathrm{P},\gamma}, t^{(\mathrm{B})}_{\alpha,\beta} - T_{\mathrm{P},\gamma}\Big)\,. \tag{7.66}$$

Here, $\psi^{(\gamma)}_{\mathrm{fib}}(t, t')$ is the kernel of $\mathrm{e}^{2\mathrm{i}\phi_0^{(\gamma)}}\mathcal{F}^{-1}\,\mathrm{e}^{\mathrm{i}\phi^{(\mathrm{A})}_{\mathrm{fib}}}\tau^{(\mathrm{A})}_{\mathrm{fib}}\tilde{\mathit{\Psi}}\,\mathrm{e}^{\mathrm{i}\phi^{(\mathrm{B})}_{\mathrm{fib}}}\tau^{(\mathrm{B})}_{\mathrm{fib}}\mathcal{F}^{*}$, describing the biphoton wave packet after the propagation through the fiber links, with $\phi_0^{(\gamma)} = (k_0 - \omega_0/v_{\mathrm{g}})L_{\mathrm{P},\gamma}$:

$$\psi^{(\gamma)}_{\mathrm{fib}}(t, t') = \mathrm{e}^{2\mathrm{i}\phi_0^{(\gamma)}}\mathcal{F}^{-1}_{\omega,\omega'}\Big\{\exp\Big[\mathrm{i}\Big(\phi^{(\mathrm{A})}_{\mathrm{fib}}(\omega) + \phi^{(\mathrm{B})}_{\mathrm{fib}}(\omega')\Big)\Big]\tau^{(\mathrm{A})}_{\mathrm{fib}}(\omega)\,\tau^{(\mathrm{B})}_{\mathrm{fib}}(\omega')\,\tilde{\psi}(\omega, \omega')\Big\}(t, t')\,. \tag{7.67}$$

Evaluating the traces of the terms in eq. (7.62) by using eq. (7.29) and the approximations eqs. (7.63) to (7.66) yields

$$\begin{aligned}\mathrm{tr}(\Xi) = \sum_{\substack{\gamma,\alpha,\beta\\ d,\, i_d}} \frac{\chi^2 c_\gamma^2}{4}\Bigg(& C_{\alpha,\beta}^{(d,\mathrm{A})} w_{i_d}^{(d,\mathrm{A})} \int_{I_{d,\mathrm{A}}} \mathrm{d}t \int \mathrm{d}u\, \psi_{\mathrm{fib}}^{(\gamma)}\Big(t - T_{\beta,\gamma}^{(\mathrm{A})}, u\Big)\, \psi_{\mathrm{fib}}^{*(\gamma)}\Big(t - T_{\alpha,\gamma}^{(\mathrm{A})}, u\Big),\\ & + C_{\alpha,\beta}^{*(d,\mathrm{B})} w_{i_d}^{(d,\mathrm{B})} \int_{I_{d,\mathrm{B}}} \mathrm{d}t \int \mathrm{d}u\, \psi_{\mathrm{fib}}^{*(\gamma)}\Big(u, t - T_{\beta,\gamma}^{(\mathrm{B})}\Big)\, \psi_{\mathrm{fib}}^{(\gamma)}\Big(u, t - T_{\alpha,\gamma}^{(\mathrm{B})}\Big)\Bigg), \end{aligned} \tag{7.68}$$

$$\begin{aligned}\mathrm{tr}\Big[\big(\Xi_{(\diagup)}\big)^2\Big] = \frac{1}{2} \sum_{\substack{\gamma,\gamma',\alpha,\alpha'\\ \beta,\beta',d,d'\\ i_d, i_{d'}}} \Bigg(& \chi^2 c_\gamma^2 C_{\alpha,\beta}^{(d,\mathrm{A})} C_{\alpha',\beta'}^{*(d',\mathrm{B})} w_{i_d}^{(d,\mathrm{A})} w_{i_d}^{(d,\mathrm{B})}\\ & \times \iint_{\substack{I_{d,\mathrm{A}}\\ I_{d',\mathrm{B}}}} \psi_{\mathrm{fib}}^{(\gamma)}\Big(t_\mathrm{A} - T_{\beta,\gamma}^{(\mathrm{A})}, t_\mathrm{B} - T_{\alpha',\gamma}^{(\mathrm{B})}\Big)\, \psi_{\mathrm{fib}}^{*(\gamma')}\Big(t_\mathrm{A} - T_{\alpha,\gamma'}^{(\mathrm{A})}, t_\mathrm{B} - T_{\beta',\gamma'}^{(\mathrm{B})}\Big)\, \mathrm{d}t_\mathrm{B}\, \mathrm{d}t_\mathrm{A}\Bigg). \end{aligned} \tag{7.69}$$

with the abbreviations $T_{\alpha,\gamma}^{(u)} = T_\alpha^{(u)} + T_{\mathrm{P},\gamma}$ and $T_{\beta,\gamma}^{(u)} = T_\beta^{(u)} + T_{\mathrm{P},\gamma}$ as well as $u \in \{\mathrm{A}, \mathrm{B}\}$.

The terms in eq. (7.62) as well as eqs. (7.68) and (7.69) are the final expressions implemented in the frequency-resolved type-II QKD simulation. A more intuitive understanding of the terms can be developed by considering as an example the detection in the early time bins of detectors A_0 and B_0. All terms in the sum that are associated with this combination of detectors and time bins vanish. When the leakage of photons out of the time bins due to CD is negligible, the generating function for the detection can be written as

$$G_0 = \exp\Big[-\mu_\mathrm{P}\Big(w_\mathrm{E}^{(0,\mathrm{A})} p_\mathrm{E}'(\mathrm{A}_0) + w_\mathrm{E}^{(0,\mathrm{B})} p_\mathrm{E}'(\mathrm{B}_0) - w_\mathrm{E}^{(0,\mathrm{A})} w_\mathrm{E}^{(0,\mathrm{B})} p_\mathrm{E}'(\mathrm{A}_0 \cap \mathrm{B}_0)\Big)\Big] \quad \text{with} \tag{7.70}$$

$$p_\mathrm{E}'(\mathrm{A}_0) = C_{\mathrm{s,s}}^{(0,\mathrm{A})} \int_{E_{0,\mathrm{A}}} \mathrm{d}t \int \mathrm{d}u \left|\psi_{\mathrm{fib}}^{(\mathrm{s})}\Big(t - T_{\mathrm{s,s}}^{(\mathrm{A})}, u\Big)\right|^2, \tag{7.71}$$

$$p_\mathrm{E}'(\mathrm{B}_0) = C_{\mathrm{s,s}}^{(0,\mathrm{B})} \int_{E_{0,\mathrm{B}}} \mathrm{d}t \int \mathrm{d}u \left|\psi_{\mathrm{fib}}^{(\mathrm{s})}\Big(u, t - T_{\mathrm{s,s}}^{(\mathrm{B})}\Big)\right|^2, \quad \text{and} \tag{7.72}$$

$$p_\mathrm{E}'(\mathrm{A}_0 \cap \mathrm{B}_0) = C_{s,s}^{(0,\mathrm{A})} C_{s,s}^{(0,\mathrm{B})} \int_{E_{0,\mathrm{A}}} \mathrm{d}t_\mathrm{A} \int_{E_{0,\mathrm{B}}} \mathrm{d}t_\mathrm{B} \left|\psi_{\mathrm{fib}}^{(\mathrm{s})}\Big(t_\mathrm{A} - T_{\mathrm{s,s}}^{(\mathrm{A})}, t_\mathrm{B} - T_{\mathrm{s,s}}^{(\mathrm{B})}\Big)\right|^2. \tag{7.73}$$

The generating function in eq. (7.70) is the PGF of the general bivariate Poisson distribution [306, 307]. The probabilities $p_\mathrm{E}'(\mathrm{A}_0)$ and $p_\mathrm{E}'(\mathrm{B}_0)$ denote the probability that a photon created by the SPDC process is transmitted to and registered by Alice's or Bob's detector labeled with "0" in the early time bin, respectively. The mean photon number is given by $\mu = \mathrm{tr}[\cosh(X_\gamma)] \approx c_\gamma^2/2$, such that $c_\gamma^2/4$ is approximately the mean photon pair number μ_P. The coefficients $C_{s,s}^{(0,\mathrm{A})}$ and $C_{s,s}^{(0,\mathrm{B})}$ are the transmissions probabilites through the interferometers given by $(\eta_0 \tau_s \kappa^2)^2$ (cf. table 7.1). The time offsets $T_{\mathrm{s,s}}^{(\mathrm{A})}$ and $T_{\mathrm{s,s}}^{(\mathrm{B})}$ are identical when the delays of all IFs are the same. The integrals in $p'_\mathrm{E}(\mathrm{A}_0)$ and $p'_\mathrm{E}(\mathrm{B}_0)$ are the marginal distributions of the biphoton probability density observed by Alice and Bob and the integral in $p'_\mathrm{E}(\mathrm{A}_0 \cap \mathrm{B}_0)$ is the probability for a joint detection of the photons by Alice and Bob. Here, the efficiencies η of the detectors are already absorbed into the probabilities p', such that the differentiation parameters are given by $w_\mathrm{E}^{(0,\mathrm{A/B})} = 1 - y_{\mathrm{A/B}}$. The probability-generating functions of the marginal distributions are $G_\mathrm{A}(y_\mathrm{A})$ and $G_\mathrm{B}(y_\mathrm{B})$. Using

$$G_\mathrm{A}(y_\mathrm{A}) = \sum_{n_\mathrm{A}} y_\mathrm{A}^{n_\mathrm{A}} \sum_{n_\mathrm{B}} p(n_\mathrm{A}, n_\mathrm{B}) = \sum_{n_\mathrm{A}, n_\mathrm{b}} y_\mathrm{A}^{n_\mathrm{A}} y_\mathrm{B}^{n_\mathrm{B}} p(n_\mathrm{A}, n_\mathrm{B})\big|_{y_\mathrm{B}=1} = G_0(y_\mathrm{A}, y_\mathrm{B} = 1)\,, \tag{7.74}$$

and similarly $G_\mathrm{B}(y_\mathrm{B}) = G_0(y_\mathrm{A} = 1, y_\mathrm{B})$, shows that the marginal distributions are given by the Poisson distributions

$$p_\mathrm{A}(n_\mathrm{A}) = \frac{1}{n_\mathrm{A}!}\frac{\partial^n}{\partial {y_\mathrm{A}}^n}\,\mathrm{e}^{-\mu_\mathrm{P}(1-y_\mathrm{A})p'_\mathrm{E}(\mathrm{A}_0)} \quad \text{and} \quad p_\mathrm{B}(n_\mathrm{B}) = \frac{1}{n_\mathrm{B}!}\frac{\partial^n}{\partial {y_\mathrm{B}}^n}\,\mathrm{e}^{-\mu_\mathrm{P}(1-y_\mathrm{B})p'_\mathrm{E}(\mathrm{B}_0)}\,. \tag{7.75}$$

Importantly, the bivariante Poisson distribution also yields the correct correlations. For example, for an ideal setup without losses, $p'_\mathrm{E}(\mathrm{A}_0) = p'_\mathrm{E}(\mathrm{B}_0) = p'_\mathrm{E}(\mathrm{A}_0 \cap \mathrm{B}_0) = 1$, and differentiating eq. (7.70) yields

$$p(n_\mathrm{A}, n_\mathrm{B}) = \frac{1}{n_\mathrm{A}! n_\mathrm{B}!}\frac{\partial^{n_\mathrm{A}+n_\mathrm{B}}}{\partial {y_\mathrm{A}}^{n_\mathrm{A}}\,\partial {y_\mathrm{B}}^{n_\mathrm{B}}}\,\mathrm{e}^{\mu_\mathrm{P}(y_\mathrm{A} y_\mathrm{B} - 1)}\Bigg|_{\substack{y_A=0\\ y_B=0}} = \frac{\mu_\mathrm{P}^{n_\mathrm{A}}}{n_\mathrm{A}!}\,\mathrm{e}^{-\mu_\mathrm{P}}\,\delta_{n_\mathrm{A}, n_\mathrm{B}}\,. \tag{7.76}$$

In this case, as expected for a setup without losses, the photon pairs are perfectly correlated so that Alice and Bob observe the same photon numbers following a Poissonian distribution.

The stronger the entanglement, the faster the series expansions of the cosh and sinh functions and of the determiant converge. The observation that the generating functions in eqs. (7.59) and (7.70) yield Poissonian photon statistics when the expansion is truncated after the leading terms well matches the fact that for infinitely many equally strong squeezers, the photon statistics becomes Poissonian (cf. eq. (7.5)). For strongly entangled states, the leading terms of the series expansion yield the Poissonian photon statistics expected for the maximally entangled state, and higher expansion orders of the cosh and sinh functions and determinant from eqs. (7.55) and (7.58) yield minor corrections to these statistics.

Evaluating eqs. (7.71) to (7.73), or eq. (7.62) for other combinations of detectors and time bins, requires computing of the marginal distributions of the temporal biphoton probability density and the joint detection probability. These are the same functions that need to be computed when the assumption is made that at most one photon pair is generated (cf. eqs. (1.30) and (1.31)), as it was done for example to investigate the effects of misaligned IFs on $\mathrm{QBER_p}$ and of the CD on $\mathrm{QBER_t}$ in section 2.3. The advantage of eq. (7.62) compared to these equations is that it yields not only the term for precisely one photon pair but a Poissonian statistics with components from multiple generated pairs, which approximates the true photon statistics well when the entanglement is strong.

7.5 Simulation Results

To check that the simulation accurately describes the performance of the QKD system, key rates and QBERs were simulated and measured for different values of the mean photon pair number per pulse μ_p for different repetition frequencies and transmission distances.

The synchronization of the TCs and the source was realized electronically, such that the uncertainty from the clock recovery does not broaden the arrival time distributions of the photons, although this effect is small (cf. fig. 2.30 (d))[12]. The measured data were evaluated using the dead time postselection for all detectors (cf. section 3.1).

For the simulation, the relevant parameters of all optical components in the setup were determined by measurements or from the component data sheets (cf. section 6.3). To take into account the dead time, the computed detection probabilities are multiplied by the probability p_on that the detector is active (cf. eq. (5.1)). The detection, including dark counts, afterpulses, and the blocking of detections in later time bins due to the dead time, is modeled as described in section 6.3.1. The methods for simulating QKD with photon pairs from type-II and type-0 SPDC are different and separated into two simulations. Appendix D discusses the most relevant details of the implementations.

Effects of Phase Misalignment and Chromatic Dispersion on the QBER

The two-photon interference in the central peak is critical for the security of the QKD protocol. To demonstrate the characteristic cosine-shaped dependence of the $\mathrm{QBER_p}$ on the IF phases (cf. eq. (1.2)) experimentally, a QKD experiment with Alice and Bob in default configuration was set up, and the $\mathrm{QBER_p}$ was recorded while scanning the temperature of Bob's IF. The measured data are compared to the simulation results in fig. 7.3. The

[12] Some of the measurements were acquired at a repetition frequency of 100 MHz instead of the 110 MHz usually used in chapter 3. The clock generator was defective at the time of the measurement and the synchronization had to be realized by using the electronic outputs of the TCs, which provide pulses with repetition frequencies up to 100 MHz only.

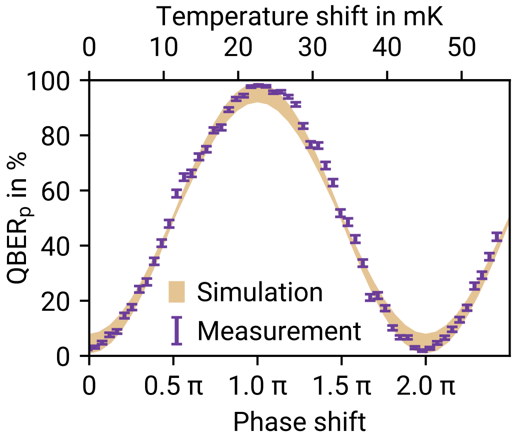


Figure 7.3: Comparison of the measured and simulated QBER$_p$ for a QKD session with Alice and Bob in the default configuration. The phase was tuned by adjusting the temperature of Bob's IF. The phase tuning coefficient $\partial \phi / \partial T$ was determined from a cosine fit.

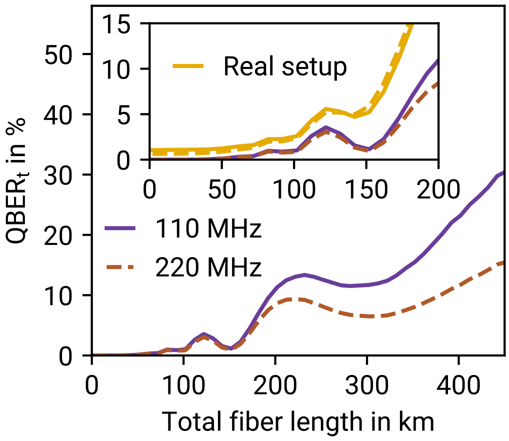


Figure 7.4: Simulated QBER$_t$ as a function of the total fiber length between Alice and Bob for QKD with type-II photons for an ideal setup without losses, afterpulses and dark counts and in comparison in the inset for the parameters of the real setup.

simulation was run with two different data sets for the parameters characterizing the optical components: The worst-case scenario uses the lowest estimates for the transmissions through the components and the highest estimates for the mode mismatches, dead times, and afterpulse probabilities, and the best-case scenario uses the corresponding best-case estimates for these values. The error band indicates the range of values between both scenarios. The IF temperature was translated to the IF phase by fitting a cosine function to the experimental data. Within the measurement accuracy, the simulation results well match the measured correlation.

One of the most relevant advantages of the frequency-resolved simulation compared to the simulation in section 6.3 is its ability to consider the elongation of the biphoton wave packets due to CD. In fig. 2.26, it was already shown that the elongation is more critical for the type-II photons than for the type-0 photons demultiplexed into 100 GHz wide DWDM channels. To investigate the relevance of the elongation, the QBER$_t$ between Alice and Bob observed at the pulse repetition frequencies of 110 and 220 MHz was simulated as a function of the total transmission distance, assuming that the fibers from the q-hub to Alice and Bob have the same lengths. To isolate the effect of the CD on the QBER$_p$, the simulations were run for an ideal setup without losses, afterpulses, and dark counts and, for comparison, with the realistic parameters. The results are shown in fig. 7.4. The QBER$_t$

increases with increasing fiber length as expected, because more photons leak into adjacent time bins for longer fibers. However, the curve is not monotonous. Local maxima appear for lengths at which side lobes of the photon spectrum (cf. fig. 2.22) overlap with neighboring time bins. The effect is well visible for the simulation of the ideal setup. For the real setup, other noise contributions blur the effect and lead to higher values of $\mathrm{QBER_t}$.

For fiber lengths longer than approximately 200 km, the $\mathrm{QBER_t}$ with twofold pulse interlacing at a repetition rate of 220 MHz is significantly lower than the $\mathrm{QBER_t}$ at 110 MHz. This result may appear counterintuitive at first because, for twofold interlacing, the time bins are packed more densely, and one could expect that, therefore, effects from photons leaking into adjacent time bins would already become relevant for shorter fiber lengths. However, a detailed analysis shows that because Alice's and Bob's fibers are equally long, the frequency anticorrelation of the photons leads in both cases to photon leakage into time bin combinations that do not lead to quantum bit errors in the time basis. Furthermore, for twofold pulse interlacing, photons from time bin combinations that would usually be discarded during postselection can leak into early-early and late-late time bin combinations of adjacent repetition cycles, thereby leading to additional bit values. Therefore, for the same fiber length, the $\mathrm{QBER_t}$ with twofold pulse interlacing is lower than without interlacing. The effect is discussed in detail in ref. [VII]. Comparing the curves for the ideal and real setup, it can be concluded that QKD with photon pairs from type-II SPDC is limited to total fiber lengths of about 150 km between two users because for longer fibers, the $\mathrm{QBER_t}$ becomes too high due to CD. In comparison, if an AWG with 50 or 100 GHz wide channels is used for demultiplexing type-0 photons, the spectrum is narrower such that for the practically relevant transmission distances up to 90 km between the source and the users, no photon leakage into adjacent time bins is observed (cf. fig. 2.26 (b)).

Sifted Key Rates and QBERs in the Time Basis

An advantage of using the covariance formalism for the simulations is that it takes into account effects from the generation of multiple photon pairs per pump pulse. The key rates and QBERs were measured and simulated to investigate the effects for different mean photon numbers per pulse μ_p. The results are shown in fig. 7.5. Instead of the total QBER, only the $\mathrm{QBER_t}$ is compared because the $\mathrm{QBER_p}$ was not entirely stable for all measurements. Depending on the fiber lengths and SPDC types, the sifted key rates show maxima for different fiber lengths. For small values of μ_p, the sifted key rate increases with μ_p because the probability for a pump pulse to generate a photon pair grows. For high values of μ_p, the count rate becomes so high that p_on decreases significantly due to the dead time, and the sifted key rate decreases with increasing μ_p. For shorter distances, the losses are lower, and the count rates are higher, such that the maximum of the sifted key rates is reached for lower values of μ_p than the longer distances. Comparing the two

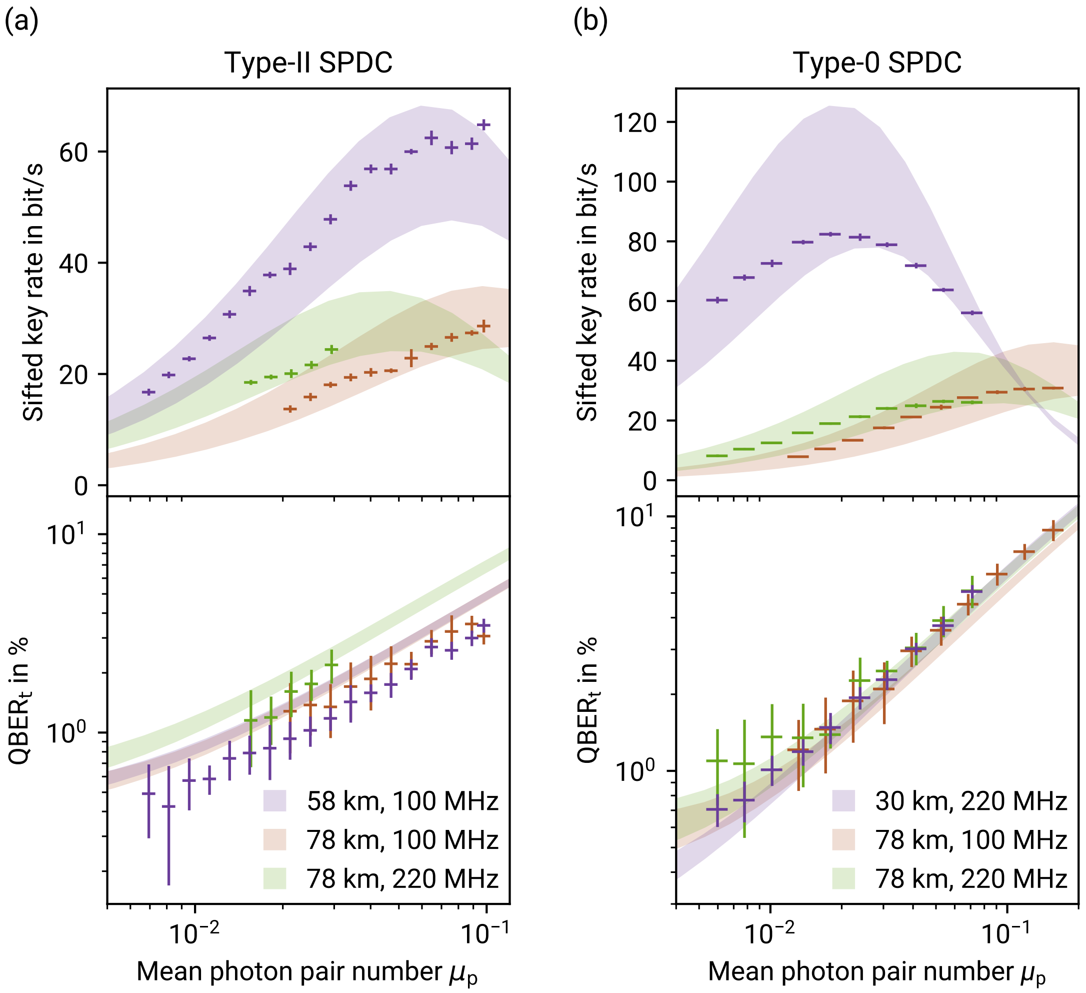


Figure 7.5: Comparison of the measured QKD performance and results from the frequency-resolved simulations. The markers show the measured data, and the bands mark the range of values between the best-case and worst-case estimates from the simulation. The vertical error bars for the measured data are obtained from the statistical uncertainty of the key rates and QBERs. The horizontal error bars are obtained from the uncertainty of μ_p, which is mainly determined by the uncertainty of the SPDC conversion efficiency. (a) For the type-II measurements, Alice is connected via the 26.8 km long deployed fiber, and Bob is connected via a 30.8 or 50.4 km long spooled fiber. (b) For the type-0 measurements, the distance between Charlie and Diana is 30 km, and the distance between Alice and Bob is 78 km. Alice is connected via the deployed fiber.

measurements at the longer distance of 78 km, the maximum is reached earlier for the measurement with the higher repetition rate due to the same effect.

The measured and simulated key rates well match for QKD with type-0 and type-II photons pairs. The QBERs also agree, but the QBERs in the type-II simulation are slightly higher than the measured QBERs, especially for the distance of 58 km. A possible reason is a value of μ_p in the experiment that is slightly lower than the value assumed in the simulation, leading to an overestimation of the quantum bit errors due to multi-photon-pair emission. However, overall, it can be concluded that the simulation and the measured data closely match. The simulation correctly represents the dependence of the key rates and QBERs on the transmission distance, repetition frequency, and mean photon pair number per pulse μ_p, including the maximum in the sifted key rate due to the detector saturation.

Summary of Chapter 7

Frequency-resolved simulations of the q-hub QKD system with photon pairs generated by type-II and type-0 *spontaneous parametric down-conversion* (SPDC) were presented. For that, the covariance formalism of Gaussian states was extended to a continuum of frequency modes. In the continuous-mode limit, the matrices describing the quantum state and its transformations become integral operators. The continuous-mode formulation is compatible with the method of simulating the photon statistics of Gaussian states using generating functions presented in chapter 6. This is an essential advantage of the generating-function-based method to computing the photon statistics compared to the Hafnian-based method, for which extensions to a continuum of modes are yet to be developed.

Approximations of the covariance and detection probabilities for strongly entangled states were derived, simplifying the computations. The biphoton states used in the q-hub QKD system are so strongly entangled that it is sufficient to expand the expression for the detection probabilities to the first contributing order, yielding Poissonian photon statistics. Several methods are used to reduce the computational resources required for the simulation, such as the application of Sylvester's determinant theorem or the evaluation of the biphoton amplitude after the transmission trough fibers with chromatic dispersion in a diagonal coordinate system based on Andrianov's method.

The simulated key rates and quantum bit errror rates match the measurements, demonstrating that the simulation considers all relevant effects. In the future, the simulation can be used to predict the influence of changes in the setup, enabling systematic optimizations of the QKD performance. The methods developed for the simulation will also be useful for simulating other quantum-optical setups using strongly entangled biphoton states. They will be published in ref. [VII] together with the simulation results for the q-hub system.

Summary

The main goals of the research presented in this thesis were to develop a robust multi-user QKD network, to demonstrate its flexibility, scalability, and reliability in a field test, and to develop detailed models of this system, enabling the analysis of relevant setup imperfections.

In the first part of this thesis, the implementation and characterization of an entanglement-based star-shaped QKD network for four users with a central *quantum key hub* (q-hub) was presented.

In chapter 2, the q-hub system was described in detail. In contrast to other entanglement-based QKD networks reported in the literature, the q-hub network uses the BBM92 time-bin QKD protocol. The protocol requires that the optical path differences of the interferometers in the receivers and the photon pair source are matched with an accuracy of a few micrometers. A method to build such interferometers quickly and reliably was developed, and a patent for the method is pending. The receivers are synchronized by clock recovery from the photon arrival times with a precision better than 100 ps, and a patent is also pending for the clock recovery method.

The field test of the q-hub QKD network at a facility of *Deutsche Telekom* presented in chapter 3 was the first field test of a multi-user QKD network using the BBM92 time-bin protocol. Key transmissions between the users were demonstrated for more than three days over optical fiber lengths of up to 108 km between the users. A length of 27 km this fiber link was deployed underground. The flexibility of the network was demonstrated with various experiments. Examples are the interlacing of pulse repetitions to increase the key rate, dynamic switching of the users combinations with a wavelength-selective switch, and the operation of a fully-connected QKD network. Three different wavelength demultiplexers were tested. It was shown that using the arrayed-waveguide grating with 50 GHz channel widths, up to 78 users can be readily connected to the network. By cascaded demultiplexing with multiple wavelength-selective switches, networks with hundreds of users are feasible.

In chapter 4, photon pair generation by spontaneous four-wave mixing in silicon nitride microring resonators on photonic chips, also called *photonic integrated circuits* (PICs), was demonstrated as a first step towards even more compact and robust photon pair sources for the q-hub. A setup for coupling light to the waveguides was developed for the first tests with a borrowed PIC, and a dedicated PIC was designed to generate photon pairs. It combines filters for cleaning the pump light from Raman noise, microring resonators for photon pair generation, and filters separating the remaining pump light from the photon pairs on a single chip. Pound-Drever-Hall locking of the microring resonators to the laser frequency was implemented, allowing to keep the microring resonators in resonance with the pump light even for the highest tested pump powers. Photon pair generation was demonstrated, showing that a large amount of noise photons is generated on the chip. Further investigations are required to identify and eliminate the root cause of this noise. Nevertheless, comparing values for the coincidence-to-accidental ratio reported in the literature showed that the quality of the photon pairs may be sufficient to demonstrate QKD.

In the second part of the thesis, an entire framework for characterizing the q-hub network was developed. It comprises a method for time-resolved tomography of the single photon detectors, a new method to simulate the photon statistics of multi-mode Gaussian states, and a frequency-resolved numerical simulation model of the q-hub system considering all relevant imperfections of the setup.

In chapter 5, the detectors of the q-hub system were characterized by sending laser pulses attenuated to the single-photon level into the detectors and recording the time-dependent count probabilities. The dark count rates, dead times, and afterpulse probabilities were calculated from these data. Time-independent *positive operator-valued measures* (POVMs) were reconstructed, allowing to calculate the detection efficiencies. For the reconstruction of time-dependent POVMs, a new method was introduced to adjust the strength of the regularization to the statistical data quality. The measured count distributions were compared to the predictions of a POVM model from the literature. The deviation of the measured data from the model predictions demonstrates that measuring time-dependent detector POVMs can reveal additional information about the detectors.

In chapter 6, a general new method was presented to simulate the photon statistics of Gaussian states by automatically differentiating generating functions. It uses the covariance formalism to model quantum-optical setups systematically by applying simple matrix operations to the covariance matrices and displacement vectors describing Gaussian states. The photon number distribution, its moments, and factorial moments are evaluated by automatically differentiating the corresponding generating functions. This method is flexible, so various kinds of imperfections of optical setups can be considered. Simulation results for key rates and quantum bit error rates in the q-hub QKD system match the measurements. It was shown that the generation of multiple photon pairs per pump pulse is one of the most relevant sources of quantum bit errors.

In chapter 7, a frequency-resolved simulation of the q-hub QKD system was presented. For the modeling, the covariance formalism of Gaussian states was extended to a continuum of frequency modes, and approximations for strongly entangled biphoton states were developed to reduce the required computational resources. The simulation results match the measured data, indicating that the simulation accurately describes all relevant effects. The simulation enables future optimizations of the q-hub system. The developed methods will also facilitate frequency-resolved simulations of other quantum-optical setups using strongly entangled photon pairs.

Compared to multi-user QKD networks based on polarization entanglement, the key transmission in the q-hub network is independent of polarization changes in the fiber links, which can occur due to mechanical stress or temperature changes. Therefore, the q-hub is particularly well suited to implement QKD networks in metropolitan areas where many users are located within a radius of about 50 km and where the polarization in the fiber links is not stable because aerial fibers or fibers deployed underground are exposed to vibrations and the weather. Q-hub networks could be applied to set up quantum-secure networks for the healthcare or financial sectors or government or law enforcement organizations. The presented theoretical frameworks for the detector analysis and the photon-number-resolved and frequency-resolved simulation methods will enable systematic numerical modeling of such QKD networks, reducing the time and development costs and enabling systematic optimizations of the QKD performance.

Outlook

Further technical improvements could make the presented QKD system even more compact, robust, and cost-effective, paving the way toward large-scale implementations of q-hub networks.

Possible Improvements of the Receivers

The current interferometer (IF) housing containers are relatively heavy because a sizeable thermal mass smooths out fast temperature fluctuations due to the ambient air. Furthermore, the control loop thermistors are placed close to thermoelectric coolers (TECs) to avoid temperature oscillations due to resonances of the control circuit. Therefore, the temperature control reacts relatively slowly to temperature setpoint changes. After applying a setpoint temperature step of 2 kelvin, it takes 15 to 30 min for the container to stabilize at the new temperature with millikelvin precison [28] and it takes up to 40 min to align the phases after switching the user combinations (cf. fig. 3.9). For real-world applications, waiting for such a long time before keys can be exchanged is impractical. To speed up the alignment, the thermal mass of the containers could be reduced, requiring better insulation at the same time to maintain the temperature stability.

For all experiments presented in this thesis, the container temperatures were always set above room temperature to avoid switching between cooling and heating, prolonging the TEC lifetime. When the ability to cool the container is not required, the TECs could be replaced by cartridge heaters, which, in contrast to the TECs, do not require contact with a thermal bath on the other side. This would allow to improve the thermal decoupling of the container from the environment by insulating the bottom of the housing container. However, due to the better insulation, it is no longer possible to quickly remove heat from the container when necessary to keep the phase of the interferometer stable.

Furthermore, a more sophisticated control loop algorithm could replace the currently used controller. Temperature readings from multiple points within the containers and from the outside could be combined to predict the temperature changes in the container based on the temperature changes of the environment, allowing to compensate them accordingly. In general, the fibers of the IF arms cannot be placed close together due to their different lengths, such that a variation of the temperature distribution within the container affects the IF phase even when the average container temperature is kept constant. The temperature distribution could be homogenized by installing multiple independently controllable heaters or TECs. For fine-grained control, the ability to cool some parts of the container and simultaneously heat other parts is desirable, requiring TECs instead of cartridge heaters.

The demonstration in section 3.2 showed that QKD with the q-hub also works for fully-connected networks. For the demonstration, the phase realignment was turned off. A major next step towards stable QKD in a fully connected network would be the implementation of a phase alignment algorithm capable of realigning the phases during the QKD session.

The costs per receiver would be the main cost driver for large-scale q-hub networks. The single-photon detectors (SPDs) are the most expensive part of the receivers, such that reducing their number would reduce the costs per receiver module. Therefore, another possible improvement of the receivers would be reducing the number of detectors from two to one, which can be realized using SPDs with spatial multi-mode input. The single-mode output fibers of the IFs can be extended and combined with a fiber combiner into one multi-mode fiber to which the SPD is connected. By adjusting the fiber lengths, the delay can be chosen such that the peaks of the arrival time histograms from the two IF outputs are interlaced, similar to twofold pulse interlacing. This modification of the setup has been implemented and will be published in ref. [IX].

To improve the security of the q-hub system, countermeasures against well-known attacks on the receivers could be implemented. For example, the attack in ref. [53] used detector blinding with strong light pulses to compromise a similar QKD system. Various countermeasures against detector blinding have been proposed, such as monitoring the optical input power of the receiver with a second detector or monitoring the current at the photo diode [308].

The maximum key rates achievable with the q-hub network are mainly limited by the detection efficiency, dead time, and timing jitter of the single-photon detectors. Efficiencies of 20 % and dead times of 10 µs were chosen for the field test. Superconducting nanowire single-photon detectors with efficiencies greater than 70 %, dead times around 40 ns and timing jitter below 30 ps are commercially available [309]. If such detectors were used in the q-hub network, the key rate would be increased by a factor of 12 solely due to the higher detection efficiency. Furthermore, the much lower timing jitter would allow for a reduction of the time bin width. Pulse generators and amplitude modulators with bandwidths of tens of gigahertz are commercially available. Assuming that the width of the time bins can be reduced to 95 ps, 32-fold pump pulse interlacing could be used to increase the repetition rate to approximately 3.5 GHz. However, dispersion compensation would be required to avoid photon leakage into adjacent time bins. Therefore, by using superconducting nanowire single-photon detectors, the key rate could be increased by roughly two orders of magnitude overall, such that key rates in the range of kilobits per second over dozens of kilometers of optical fiber would become feasible. However, superconducting-nanowire single-photon detectors are much more cost-intensive than the single-photon avalanche diodes currently used in the q-hub system.

Interferometers with Phase Shifters and Alternative QKD Protocols

An option to speed up the alignment of future generations of the IFs is to integrate phase shifters. Piezo-based fiber stretchers could be used to control the IF phases directly, as demonstrated in refs. [116, 133, 162]. Directly stretching the fiber of one of the IF arms would enable much quicker phase alignments than changing the temperature without introducing additional insertion losses. Alternatively, lithium-niobate-based electro-optic phase modulators (EOPMs) with gigahertz switching bandwidths are available, but they introduce losses of about 2 dB, which would lead to a significant reduction of the key rate. The base plates in the IF containers are already prepared for installing such modulators (cf. fig. 2.27) and a second IF per receiver. IFs with EOPMs were planned during the master's thesis of Lucas Bialowons [M5]. The EOPMs and further components were purchased, but the IFs could not be realized due to limited time. With IFs comprising EOPMs, different QKD protocols could be realized, such as phase-coding protocol with a continuous-wave (CW) photon pair source (PPS) [31] or quantum secret sharing between three users [310]. An advantage of using a CW entanglement protocol is that the PPS becomes much simpler because a pulse generation stage is not required. EOPMs in the receivers, on the contrary, complicate the setup. However, phase coding with a continuous PPS can also be realized by setting up two IFs per user for two different phase bases [31]. For that, a 50/50 beam splitter randomly directs arriving photons to one of the IFs, realizing a passive basis choice. The phases of both IFs are shifted by $\pi/2$ to realize the different bases. The protocol has been implemented in ref. [311] and can readily be realized with the PPS and IFs of the q-hub QKD system.

Postprocessing Software

In the previous chapters, it was demonstrated that the hardware of the q-hub system, the software for data acquisition and setup operation, and the synchronization by clock recovery are fully functional. For the field test, the q-hub and the four receiver modules were set up in the same room. The timestamps of all four users were evaluated on the same computer that operated the photon source. Postprocessing software for the keys and remote communication over an authenticated classical channel must be implemented to operate the receivers at different locations. Early implementation efforts for the QKD systems in Darmstadt date back to the masters's theses of Tobias Diehl and Micha Ober and to the Ph.D. of Sabine Euler [312]. The results were published in the technical report ref. [313], and Oleg Nikiforov made the software publicly available as a *GitLab* project [314]. Later, parts of the software were analyzed for cache side channels in joint efforts with the research group of Prof. Dr. Heiko Mantel from the *Computer Science* department of the *Technical University of Darmstadt*. Side channels in parts of the software were found and removed [56]. A fully functional postprocessing software stack for the q-hub QKD system is currently under development. Once the software for key postprocessing and remote control is completed, the receivers and the source can be separated to demonstrate QKD between remote locations.

Possible Improvements of the Photon Pair Source

The current implementation of the PPS has proven to be robust and flexible, but further improvements are possible. A relatively simple improvement would be the replacement of the 10/90 beam splitter for monitoring the second-harmonic pump power. The currently installed beam splitter shows relatively large variations of the splitting ratio of 10 % of the value, which is the most significant source of the uncertainty for the measurements of the source performance, such as the crystal conversion efficiency. For QKD, a time-dependent variation of the splitting ratio leads to variations of the mean photon pair number μ_p during the QKD session. The beam splitter could be replaced by a more stable one to improve the overall stability of the system.

As discussed in section 2.1.2, the number of users could be slightly increased by shifting the q-hub center wavelength from 1550.5 nm to the center of the operating range of the WSS at 1547.9 nm. The fiber Bragg gratings used in EDFA-2 are not reflective at this wavelength, so EDFA-2 cannot be used without replacing the FBGs. However, one EDFA is sufficient to generate the required pulse powers for type-0 SPDC. The width of the bandpass filter used in EDFA-1 is 6.5 nm. Therefore, using EDFA-1 instead of EDFA-2, the center wavelength could be tuned to the center wavelength of the WSS. The temperature of the wavelength converters can be easily adjusted with the temperature controllers to achieve phase matching at this wavelength.

Some of the most expensive parts of the PPS are the type-0 wavelength converters. It was demonstrated that the PPS can also be operated with a single converter in a bidirectional configuration. The setup could be changed permanently to this configuration. The second converter could then be used to set up another type-0 PPS. A fully functional pulsed laser system is available from Nikiforov's QKD system for two users. Multiple wavelength demultiplexers are also already in use, such that a second q-hub system is easily completed. Thereby, a QKD network with two q-hubs key hubs could be built.

Another option to simplify the PPS would be to directly generate laser pulses at a wavelength of 775 nm and to set up the IF in the PPS for this wavelength, such that second-harmonic generation is not required. Laser diodes at 775 nm are commercially available, but the lithium niobate-based amplitude modulators for 775 nm are typically limited to much lower input powers than at 1550 nm. However, due to the high efficiency of the wavelength converters, only moderate powers are required. The q-hub was typically operated at an average pump power of 60 µW at 775 nm, corresponding to a pulse peak power of 660 µW. If laser pulses with this power could be generated by using a 775 nm laser diode and an amplitude modulator, the converter could be used for the photon pair generation, and neither second-harmonic generation nor fiber amplifiers would be required anymore. However, the pump interferometer would need to be set up with different fiber components for 775 nm. The calculation of the required OPD accuracy in section 2.3.1 showed that for the pump interferometer, path length deviations of up to 2 mm are acceptable. Achieving this tolerance is feasible even when the pump interferometer is not built from the same components as the receiver interferometers.

Yet another option is to abandon the pump interferometer completely and to produce the double pulses directly. However, the method requires that the jitter of the pulses is sufficiently low. A fixed phase relation of the two halves of the pump is required. It can be achieved by choosing a stable pump laser with a coherence length much longer than the separation and duration of the two halves of the pump pulses. Tests by Oleg Nikiforov showed that generating electronic double pulses with the pulse generator *HP8131A* and applying them to a single amplitude modulator results in high QBERs, probably because the timing jitter is too large. However, the method has been demonstrated successfully in refs. [63–65] by producing a pulse train of equidistant pulses with a first amplitude modulator and extinguishing every third pulse with a second amplitude modulator.

If QKD protocols with a continuous PPS, such as the phase coding protocol with active or passive basis choice, were implemented, no pulse generation would be required. The PPS setup could be simplified to a stable laser diode at 775 nm and a wavelength converter with pump light filters.

Possible Extensions and Improvements of the QKD Simulations

For the photon-number-resolved simulation, a further research topic could be a systematic comparison of the computation speed for the photon statistics between the Hafnian-based approach and the generating-function-based approach presented in this thesis. The theoretical complexity of the generating function-based approach could be analyzed, and the speed of different software frameworks for automatic differentiation, such as *Tensorflow* [252] or *JAX* [315, 316] for computing the higher-order derivatives could be compared.

The computation speed of the generating-function-based approach could possibly be improved by using different algorithms for the computation of the derivatives of the determinant. The standard method for computing the determinant implemented in *PyTorch* is based on the *LU* decomposition, with an operation count scaling with the matrix dimension n approximately as $2n^3/3$ [296]. The real covariance $\boldsymbol{\Gamma}^{(q)}$ is symmetric and positive definite [228] and so is the matrix $\boldsymbol{\Lambda}$ (cf. eq. (6.49)). Therefore, the determinant could also be computed from the Cholesky decomposition $\boldsymbol{\Lambda} = \boldsymbol{L}\boldsymbol{L}^\dagger$ by $\sqrt{\det(\boldsymbol{\Lambda})} = \prod_i L_{ii}$. Computing the Cholesky decomposition requires only roughly half as many operations as computing the *LU* decomposition [296]. As the required computation time for the photon number distribution scales roughly exponentially with the number of derivatives, even a relatively moderate speedup, such as a factor of two per derivative, could lead to a significant speedup for higher photon numbers. Another way to improve the computation speed for the higher-order derivatives could be to use so-called *Taylor-mode differentiation* instead of the direct approach of the nested application of the first-order differentiation rules [249, 316]. For linear algebra functions such as the Cholesky decomposition, the relevant expressions are known and have been implemented in the *AlgoPy* software [317, 318]. In *JAX*, the implementation of Taylor-mode differentiation is pursued [316], but it is not yet implemented for the matrix decompositions. Yet another option proposed in ref. [229] is to compute derivatives of the determinant by using Jacobi's formula $\partial \det(\boldsymbol{M})/\partial y = \det(\boldsymbol{M})\, \mathrm{tr}[\boldsymbol{M}^{-1}\partial \boldsymbol{M}/\partial y]$ [319].

The frequency-resolved QKD simulation could be extended to include the photon polarization. Thereby, QKD systems using polarization encoding could be modeled. Furthermore, other types of PPSs with different joint spectral amplitudes could be simulated, such as PPSs based on spontaneous four-wave mixing in microring resonators. Parameter scans could be performed to analyze the impact of different imperfections on the QKD performance, allowing systematic improvements of the system.

Appendix

A Formulary

In the following, some useful mathematical relations used throughout this thesis are listed for reference.

Complex Exponential Integrals

Dirac delta distribution

$$\delta(t) = \frac{1}{2\pi}\int \mathrm{e}^{\mathrm{i}\omega t}\,\mathrm{d}\omega \tag{A.1}$$

Complex Gaussian integral [320]

$$\int \exp\!\left(-ax^2 + bx\right) = \sqrt{\frac{\pi}{a}}\exp\!\left(\frac{b^2}{4a}\right) \tag{A.2}$$

Multivariate Gaussian integral [321]

$$\int_{\mathbb{R}^N} \mathrm{e}^{-\boldsymbol{x}^\mathsf{T}\boldsymbol{A}\boldsymbol{x}/2+\mathrm{i}\boldsymbol{b}^\mathsf{T}\boldsymbol{x}}\,\mathrm{d}\boldsymbol{x} = \sqrt{\frac{(2\pi)^N}{\det\boldsymbol{A}}}\,\mathrm{e}^{-\boldsymbol{b}^\mathsf{T}\boldsymbol{A}^{-1}\boldsymbol{b}/2} \tag{A.3}$$

The integral in eq. (A.2) converges for $a, b \in \mathbb{C}$ when $\operatorname{Re}(a) > 0$ as well as for $\operatorname{Re}(a) = 0$ when $\operatorname{Re}(b) = 0$ and $\operatorname{Im}(b) \neq 0$. Here, $\sqrt{a}$ is the principal square root of a. Equation (A.3) holds for complex vectors $\boldsymbol{b}$ and real, symmetric, positive definite matrices $\boldsymbol{A}$.

Different conventions for the Fourier transform exist in the literature. In this thesis, the following definitions are used:

Fourier transform

$$\tilde{f}(\omega) = \mathcal{F}_t\big(f(t)\big)(\omega) = \frac{1}{\sqrt{2\pi}}\int f(t)\,\mathrm{e}^{\mathrm{i}\omega t}\,\mathrm{d}t \tag{A.4}$$

Inverse Fourier transform

$$f(t) = \mathcal{F}_\omega^{-1}\big(\tilde{f}(\omega)\big)(t) = \frac{1}{\sqrt{2\pi}}\int \tilde{f}(\omega)\,\mathrm{e}^{-\mathrm{i}\omega t}\,\mathrm{d}\omega \tag{A.5}$$

Some useful relations involving the Fourier transform are listed below:

Shift in time or frequency

$$\mathcal{F}_t\big(f(t-t_0)\,\mathrm{e}^{-\mathrm{i}\omega_0 t}\big)(\omega) = \mathrm{e}^{\mathrm{i}(\omega-\omega_0)t_0}\tilde{f}(\omega-\omega_0) \tag{A.6}$$

Complex conjugation

$$\mathcal{F}_t\big(f^*(t)\big)(\omega) = \big(\tilde{f}(-\omega)\big)^* \tag{A.7}$$

Parseval-Plancherel identity

$$\int f(t)h^*(t)\,\mathrm{d}t = \int \tilde{f}(\omega)\big(\tilde{h}(\omega)\big)^*\,\mathrm{d}\omega \tag{A.8}$$

Convolution

$$(f * h)(t) = \int f(\tau)h(t-\tau)\,\mathrm{d}\tau \tag{A.9}$$

Cross-correlation

$$(f \star h)(t) = \int f^*(\tau)h(\tau+t)\,\mathrm{d}\tau \tag{A.10}$$

Convolution theorem

$$\mathcal{F}_t[(g * h)(t)](\omega) = \sqrt{2\pi}\tilde{g}(\omega)\tilde{h}(\omega) \tag{A.11}$$

Normalized autocorrelation

$$g_f^{(1)}(t) = \frac{(f \star f)(t)}{\int |f(\tau)|^2\,\mathrm{d}\tau} \tag{A.12}$$

Normalized spectral density

$$s_f(\omega) = \frac{|\tilde{f}(\omega)|^2}{\int |\tilde{f}(\omega)|^2\,\mathrm{d}\omega} \tag{A.13}$$

Wiener-Khinchine theorem

$$g_f^{(1)}(t) = \int s_f(\omega)\,\mathrm{e}^{-\mathrm{i}\omega t}\,\mathrm{d}\omega \tag{A.14}$$

Coherence time [235]

$$\tau_{\text{coh.}} = \int |g_f^{(1)}(t)|^2\,\mathrm{d}t = 2\pi \int s_f^2(\omega)\,\mathrm{d}\omega \tag{A.15}$$

Series and Special Functions

Exponential series

$$\exp(y) = \sum_{k=0}^{\infty} \frac{y^k}{k!} \tag{A.16}$$

Geometric series

$$\frac{1}{1-y} = \sum_{k=0}^{\infty} y^k \quad \text{for} \quad |y| < 1 \tag{A.17}$$

Binomial theorem

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \tag{A.18}$$

Negative binomial series [223]

$$\frac{1}{(1-y)^{n+1}} = \sum_{k=0}^{\infty} \frac{(k+n)!}{k!n!} y^k \quad \text{for} \quad |y| < 1 \tag{A.19}$$

Generating function of the Laguerre polynomials [245]

$$\sum_{n=0}^{\infty} y^n L_n(x) = \frac{1}{1-y} \exp\left(\frac{-xy}{1-y}\right) \tag{A.20}$$

Rectangle function

$$\mathrm{rect}_\tau(x) = \begin{cases} 0 & \text{if } |x| > |\tau|/2 \\ 0.5 & \text{if } |x| = |\tau|/2 \\ 1 & \text{if } |x| < |\tau|/2 \end{cases} \tag{A.21}$$

Sine cardinal [98]

$$\mathrm{sinc}(x) = \begin{cases} \sin(x)/x & \text{if } x \neq 0 \\ 1 & \text{if } x = 0 \end{cases} \tag{A.22}$$

Fourier transform of a rectangle

$$\mathcal{F}_t[\mathrm{rect}_\tau(t)](\omega) = \frac{\tau}{\sqrt{2\pi}}\,\mathrm{sinc}\left(\frac{\omega\tau}{2}\right) \tag{A.23}$$

Probability Rules

For events A and B with probabilities $p(A)$ and $p(B)$, the following probability rules hold:

Addition rule

$$p(A \cup B) = p(A) + p(B) - p(A \cap B) \tag{A.24}$$

Multiplication rule

$$p(A \cap B) = p(A\,|\,B)\,p(B) = p(B\,|\,A)\,p(A) \tag{A.25}$$

Conditional probability

$$p(A\,|\,B) = \frac{p(A \cap B)}{p(B)} \tag{A.26}$$

Law of total probability

$$p(A) = \sum_i p(A \cap B_i) \tag{A.27}$$

Bayes' theorem

$$p(A\,|\,B) = \frac{p(B\,|\,A)\,p(A)}{p(B)} \tag{A.28}$$

Here, $p(A\,|\,B)$ is the conditional probability that A occurs, given that B occurs.

Quantum Mechanics

The Baker-Campbell-Hausdorff formula states that for two operators $\hat{O}_1$ and $\hat{O}_2$ with commutator $[\hat{O}_1, \hat{O}_2]$ and $[\hat{O}_1, [\hat{O}_1, \hat{O}_2]] = [\hat{O}_2, [\hat{O}_1, \hat{O}_2]] = 0$, it holds [235, 322]

$$\exp\left(\hat{O}_1 + \hat{O}_2\right) = \exp\left(\hat{O}_1\right)\exp\left(\hat{O}_2\right)\exp\left(-\left[\hat{O}_1, \hat{O}_2\right]/2\right). \tag{A.29}$$

The optical equivalence theorem states that the expectation value of a normally-ordered function of creation and annihilation operators $F(\hat{a}^\dagger, \hat{a})$ is given by [233, 235, 322]

$$\mathrm{tr}\left(\hat{\rho}F(\hat{a}^\dagger, \hat{a})\right) = \int_{\mathbb{C}} P(\alpha)F(\alpha^*, \alpha)\,\mathrm{d}^2\alpha\,. \tag{A.30}$$

Here, $P(\alpha)$ is the Glauber–Sudarshan P-function given by $\hat{\rho} = \int_{\mathbb{C}} P(\alpha)|\alpha\rangle\langle\alpha|\,\mathrm{d}^2\alpha$.

B Model for Calculating the Generated Photon Pair Rate

To calculate the crystal efficiency from eq. (2.3), the average SHG pump power as well as the signal and idler timestamps are recorded, and the generated photon pair rate R_{pair} needs to be calculated. For that, a model was developed, including various imperfections of the setup, such as the detector dead times, dark counts, afterpulses, and frequency-dependent transmission losses.

A simulation based on artificially generated timestamps shows that all these effects must be included in the calculation to obtain correct values. The core functionalities of this simulation were implemented during the master's thesis of Maximilian Mengler [M8].

B.1 Calculation of the Generated Photon Pair Rate

To calculate R_{pair} from the signal and idler count rates r_{s} and r_{i} and from the coincidence count rate R, a model from ref. [323] is extended to include effects from dead times, afterpulses and frequency-dependent losses. The following definitions are used:

$\zeta_{\text{s/i}}$	Average spectral transmission efficiency (cf. eq. (2.4))
$t_{\text{s/i}}$	Transmission efficiency independent of the spectrum
$\eta_{\text{s/i}}$	Detection efficiency
$\alpha_{\text{s/i}}$	Afterpulse factor
$d_{\text{s/i}}$	Dark count rate
ζ_{pair}	Average spectral joint transmission efficiency (cf. eq. (2.5))
γ	Beam splitting factor
τ	Duration of the coincidence window

The coincidence window size τ is set in the data evaluation software, and the dark count rates $d_{\text{s/i}}$ are known from separate measurements. The model assumes that all counts are due to dark counts, photons, or afterpulses. Other noise sources, such as a photon background scaling with the pump power, are not included. The count rates r_s and r_i as well as the coincidence count rate R are given by:

$$r_{\mathrm{s/i}} = \zeta_{\mathrm{s/i}}\eta_{\mathrm{s/i}}t_{\mathrm{s/i}}\alpha_{\mathrm{s/i}}R_{\mathrm{pair}} + d_{\mathrm{s/i}} \quad \text{Rate of signal / idler photons} \tag{B.1}$$

$$R = C + U \quad \text{Rate of coincidences} \tag{B.2}$$

$$C = \gamma\zeta_{\mathrm{pair}}t_\mathrm{s}t_\mathrm{i}\eta_\mathrm{s}\eta_\mathrm{i}R_{\mathrm{pair}} \quad \text{Rate of coincidences from photon pairs} \tag{B.3}$$

$$U = (r_\mathrm{s} - C)(r_\mathrm{i} - C)\tau \quad \text{Rate of accidental coincidences} \tag{B.4}$$

Accidental coincidences are coincidences not caused by SPDC photons from the same pair. The uncorrelated rate $r_\mathrm{s} - C$ describes all signal detections except those where a pair was produced and both photons were detected. The probability for such an uncorrelated detection to be detected in coincidence with an uncorrelated idler detection is $\tau(r_\mathrm{i} - C)$.

Inserting eq. (B.4) into eq. (B.2) and solving for C yields

$$C = \frac{1}{2\tau}\Big((r_\mathrm{s} + r_\mathrm{i})\tau - 1 + \sqrt{[1 - (r_\mathrm{s} + r_\mathrm{i})\tau]^2 - 4\tau(\tau r_\mathrm{s} r_\mathrm{i} - R)}\Big). \tag{B.5}$$

Thereby, C can be directly calculated from the measured rates r_s, r_i, and R.

Inserting eq. (B.3) into eq. (B.4) and using eq. (B.1) yields

$$R_{\mathrm{pair}} = \gamma\frac{\zeta_{\mathrm{pair}}}{\zeta_\mathrm{s}\zeta_\mathrm{i}}\frac{(r_\mathrm{s} - d_\mathrm{s})(r_\mathrm{i} - d_\mathrm{i})}{\alpha_\mathrm{s}\alpha_\mathrm{i}C} \quad \text{and} \quad t_{\mathrm{s/i}} = \frac{r_{\mathrm{s/i}} - d_{\mathrm{s/i}}}{\zeta_{\mathrm{s/i}}\eta_{\mathrm{s/i}}\alpha_{\mathrm{s/i}}R_{\mathrm{pair}}}. \tag{B.6}$$

Equation (B.6) allows to calculate the pair rate R_{pair} and the transmission values $t_{\mathrm{s/i}}$ from the measured rates when $\zeta_{\mathrm{s/i}}$, $\eta_{\mathrm{s/i}}$, and $\alpha_{\mathrm{s/i}}$ are known. For example, the $t_{\mathrm{s/i}}$ contain the unknown efficiency for coupling photons from the SPDC crystal waveguide into the fibers.

Probabilistic Splitting of Parallel Polarized Photon Pairs

When the photon pairs are split by a WDM or polarization beam splitter, the beam splitting factor is set to $\gamma = 1$. The separation can also be achieved probabilistically for parallel polarized photons by inserting a 50/50 beam splitter instead of a WDM. The probability of observing a count in one of the detectors from the signal or the idler photon or both photons is given by the probability addition rule (cf. eq. (A.24)) $p(s \cup i) = p(s) + p(i) - p(s \cap i)$. Assuming $\eta_\mathrm{s}\zeta_\mathrm{s}t_\mathrm{s} = \eta_\mathrm{i}\zeta_\mathrm{i}t_\mathrm{i} = \eta\zeta t$ yields $p(s) = p(i) = \eta\zeta t/2$ and the term $p(s \cap i) = \eta^2\zeta_{\mathrm{pair}}t^2/4$, which can be neglected when the transmission probabilities including all losses and detector efficiencies in the experiment are low. Therefore, inserting the 50/50 splitter leaves the rates r_s and r_i almost unchanged. In contrast, the coincidence rate is reduced by a factor of two because, with 50 % probability, both photons are directed to the same detector. The beam splitting factor is therefore set to $\gamma = 1/2$.

When the detector exhibits no dead time and no afterpulses, r_{s}, r_{i}, and R are directly given by the measured count rates and the rate of coincidences. Two options exist to include effects from afterpulses and dark counts: A statistical treatment or data postselection. Both are discussed in the following.

Statistical Treatment of Afterpulses and Dark Counts

Afterpulses increase the count rates of the detectors by introducing uncorrelated counts. The afterpulse rate is given by $r_{\mathrm{ap}} = (r_{\mathrm{g}} + r_{\mathrm{ap}})p_{\mathrm{ap}}$, with the afterpulse probability p_{ap} and the rate of genuine counts r_{g} which are not afterpulses. The term $r_{\mathrm{ap}}p_{\mathrm{ap}}$ on the right-hand side takes into account that an afterpulse can generate another afterpulse with probability p_{ap}. Solving for $r_{\mathrm{ap}}/r_{\mathrm{g}}$ shows that the average number of counts produced by one genuine count is given by the afterpulse factor

$$\alpha = 1 + \frac{r_{\mathrm{ap}}}{r_{\mathrm{g}}} = \frac{1}{1 - p_{\mathrm{ap}}} \,. \tag{B.7}$$

Dark counts are not multiplied by α because the measured dark count rate already includes the afterpulses of genuine dark counts.

The detector dead time can be treated statistically as described in section 5.2. The rates that a detector would have measured without dead time are calculated from the measured rates r_{m} and R_{m} by using eq. (5.2):

$$r_{\mathrm{s/i}} = \frac{r_{\mathrm{m,s/i}}}{1 - \tau r_{\mathrm{m,s/i}}} \,, \tag{B.8}$$

$$R = \frac{R_{\mathrm{m}}}{(1 - \tau_{\mathrm{s}} r_{\mathrm{m,s}})(1 - \tau_{\mathrm{i}} r_{\mathrm{m,i}})} \,. \tag{B.9}$$

Equation (B.6) is then applied to these corrected rates.

Removing Afterpulses and Dead Time by Data Postselection

In the statistical treatment of afterpulses and dead time, it is assumed that the detection events are described by two independent processes, such that in eq. (B.9), the two factors $1 - \tau r_{\mathrm{m,s/i}}$ can be multiplied. This assumption is only approximately fulfilled because coincident detections lead to a simultaneous deactivation of the detectors and a simultaneous reactivation. Furthermore, in fig. 5.2 (b), it can be seen that the detection efficiency is not instantly restored after the dead time. The afterpulses are assumed to contribute as uncorrelated noise, but due to the time-dependent afterpulse distribution, the coincidence probability between afterpulses is increased. These effects can distort the results of the efficiency calculation.

As an alternative, data postselection can be used to entirely remove the effects introduced by the dead time and afterpulses. For that, only the counts with a sufficiently long time difference to the preceding count are selected. The detector is considered *ready* for the subsequent detection when a time of τ_{sel} has passed since the last count. Counts registered when the detectors are not ready are discarded. To find a suitable value for τ_{sel}, the afterpulse histograms in fig. 5.2 (b) are examined. It shows that effects from afterpulses and from the dead time are limited to some tens of microseconds after a count. Based on these histograms, $\tau_{\mathrm{sel}} = 40\,\mu\mathrm{s}$ is chosen. The principle of the data postselection for the individual detector and coincidence count rates are shown in fig. B.1. The postselected count and coincidence rates are used for the crystal conversion efficiency calculation, eliminating the effects of the dead times and afterpulses. The count rate under the condition that a detector is ready is the number of accepted counts divided by the sum of all time intervals in which the detector was ready, which is given by the sum of the green time intervals in fig. B.1. Coincidence counts are only selected when both detectors are ready.

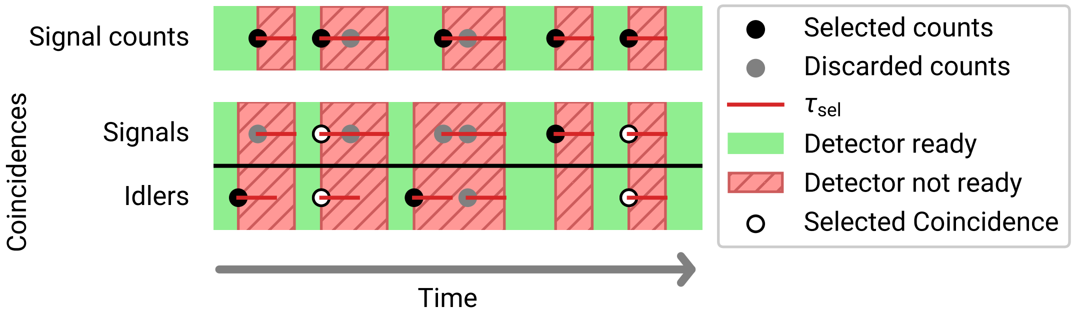


Figure B.1: Data postselection for the crystal efficiency calculation. The upper diagram shows the selection of counts and the time intervals when the detector is ready for exemplary signal counts. A coincidence is only selected if both detectors are ready, as shown in the lower diagram. When both detectors are ready, and a signal and an idler are registered with a time difference $\Delta t \leq \tau/2$, the counts are considered coincident.

B.2 Model Verification with Simulated Timestamps

To verify the crystal efficiency calculation model and to quantify the influence of different corrections, artificial timestamps were generated with parameters close to the experimental values:

- The pair rate R_{pair} is calculated via eq. (2.3). Emission times for photon pairs following a Poissonian process with rate R_{pair} are sampled.

- The transmission probabilities to pass the 7 nm wide bandpass filter, given by ζ_{s}, ζ_{i}, and ζ_{pair}, are considered. A random fraction of $p(s) = \zeta_{\mathrm{s}}$ of the pair times are kept. These are the signal photons passing the frequency-dependent losses of the filter. A random fraction $p(i\,|\,s) = p(i \cap s)/p(s) = \zeta_{\mathrm{pair}}/\zeta_{\mathrm{s}}$ of signal times is selected. These are the idler counts that are detected in coincidence with signal counts. A random fraction $p(i\,|\,\bar{s}) = p(i \cap \bar{s})/p(\bar{s})$ of those pair times that are not signal times ($\bar{s}$) is selected, these are the idler counts that are not paired with a signal count. Applying the law of total probability from eq. (A.27) yields $p(i \cap \bar{s}) = \zeta_{\mathrm{i}} - \zeta_{\mathrm{pair}}$, such that $p(i\,|\,\bar{s}) = (\zeta_{\mathrm{i}} - \zeta_{\mathrm{pair}})/(1 - \zeta_{\mathrm{s}})$. Finally, the paired and unpaired idler times are combined into the total list of idler counts.

- Half of the signals and half of the idlers are randomly selected to be sent into the first detector to model probabilistic photon pair splitting with a 50/50 beam splitter. The photons that were not selected are those reflected by the beam splitter. They are sent into the second detector.

- The frequency-independent losses are applied by selecting random fractions $\eta_{\mathrm{s/i}} t_{\mathrm{s/i}}$ from the signals and idlers.

- Dark counts are modeled by a Poisson process with a rate corresponding to the measured dark count rate divided by the afterpulse factor, taking into account that the measured dark count rates already include afterpulses. The dark count timestamps are merged with the photon timestamps.

- All counts are shifted by small random time offsets following a Gaussian distribution modeling the timing jitter of the detectors and acquisition electronics.

- Afterpulses with a random time distribution roughly following the shape of the measured afterpulse distribution are introduced according to the afterpulse probability. The afterpulses are introduced together with the dead time effect. Timestamps are rejected when they follow within the dead time after a count or afterpulse. An afterpulse leads with probability p_{ap} to another afterpulse.

The conversion efficiency calculation model was applied to the simulated timestamps. Figure B.2 compares the nominal values used for the simulation to the values obtained from the postselection model and to the statistical model considering different effects. When deadtimes, afterpulses and the spectral correlation factor $c_{\Delta I} = \zeta_{\text{pair}}/(\zeta_{\text{s}}\zeta_{\text{i}})$ (cf. eq. (2.6)) of the bandpass filter are not taken into account, the reconstruction underestimates the crystal efficiency by more than a factor of 1.5 and overestimates the transmission probabilities for signals and idlers. Considering the dead time leaves the estimated value for ϵ almost unchanged and leads to higher estimates for the transmission probabilities $\eta_{\text{s}}t_{\text{s}}$ and $\eta_{\text{i}}t_{\text{i}}$. Taking into account the afterpulses leads to an even lower estimate for the conversion efficiency ϵ and to even higher estimates for the transmission probabilities. Considering additionally $c_{\Delta I}$ improves the estimates to values close to the set values. This shows that the effects from the dead times, afterpulses, and the spectral correlation factor must all be considered to obtain correct estimates. The best estimates are obtained from the model that includes $c_{\Delta I}$ and removes effects from dead times and afterpulses by data postselection. The statistical uncertainties of this model, shown by error bars, are slightly larger than for the other models because the postselection reduces the number of timestamps from which the values are estimated.

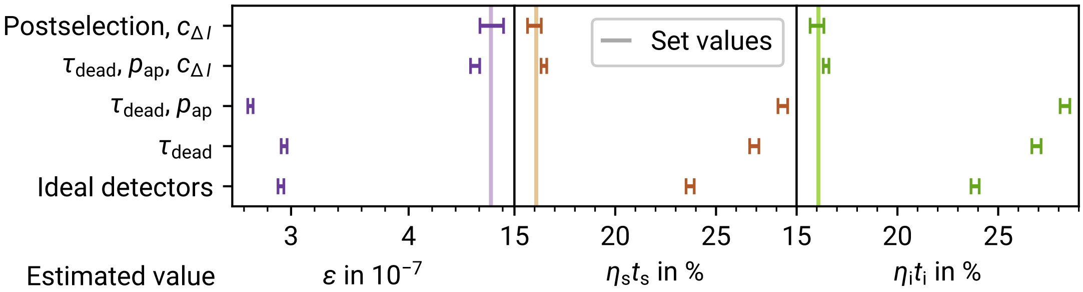


Figure B.2: Verification of the crystal conversion efficiency calculation model. The measured efficiency over the 0.7 nm wide frequency interval ΔI of the bandpass filter is $\epsilon = 4.7 \times 10^{-7}$ and the measured transmissions $\eta_{\text{s/i}}t_{\text{s/i}}$ are 16.1 %. Using these values, timestamps were simulated, and five reconstruction models including different effects were applied to estimate ϵ and $\eta_{\text{s/i}}t_{\text{s/i}}$ from these data. The results are compared to the set values (vertical lines) of the timestamps simulation. The labels "τ_{dead}", "p_{ap}" and "$c_{\Delta I}$" indicate whether the dead times, afterpulses, or the spectral correlation factor are taken into account. The model "Ideal detectors" does not take into any of the effects. The "Postselection" model eliminates effects from afterpulses and dead times by data postselection. The error bars indicate the statistical uncertainties originating from the finite number of counts and coincidences for the simulated measurement time of 120 s.

C Examples for Common Gaussian States and Transformations

Representation of some of the most important Gaussian states and transformations are listed below.

- The vacuum state $|0\rangle$ is represented by $\boldsymbol{\Gamma} = \mathbb{1}$ and $\boldsymbol{d} = 0$ [101].
- The coherent state is represented by $\boldsymbol{\Gamma} = \mathbb{1}$ and $\boldsymbol{d}^{(q)} = \sqrt{2}\begin{pmatrix}\mathrm{Re}(\alpha)\\ \mathrm{Im}(\alpha)\end{pmatrix}$ [101].
- The single-mode displaced squeezed thermal state $\hat{\rho} = D(\alpha)S(\chi)\hat{\rho}_{\mathrm{th}}(\mu_{\mathrm{th}})S^{\dagger}(\chi)D^{\dagger}(\alpha)$ is represented by $\boldsymbol{d}^{(q)} = \sqrt{2}\big(\mathrm{Re}(\alpha), \mathrm{Im}(\alpha)\big)^{\mathsf{T}}$ and [225, 227]

$$\boldsymbol{\Gamma}^{(q)} = (1 + 2\mu_{\mathrm{th}})\left[\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\cosh(2r) + \begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}\sinh(2r)\right]. \tag{C.1}$$

Here, $D(\alpha) = \exp(\alpha\hat{a}^{\dagger} - \alpha^{*}\hat{a})$ and $S(\chi) = \exp[(\chi\hat{a}^{\dagger 2} - \chi^{*}\hat{a}^{2})/2]$ are the displacement and squeezing operators with squeezing parameter $\chi = r\,\mathrm{e}^{\mathrm{i}\theta}$, and

$$\hat{\rho}_{\mathrm{th}}(\mu_{\mathrm{th}}) = \sum_{k=0}^{\infty}\frac{{\mu_{\mathrm{th}}}^{k}}{(1+\mu_{\mathrm{th}})^{k+1}}|k\rangle\langle k| \tag{C.2}$$

is a thermal state with mean photon number μ_{th} [227].

- The TMSV state $|\psi\rangle_{\mathrm{TMSV}} = \exp\big(r\,\mathrm{e}^{\mathrm{i}\theta}\hat{a}_{\mathrm{s}}^{\dagger}\hat{a}_{\mathrm{i}}^{\dagger} - r\,\mathrm{e}^{-\mathrm{i}\theta}\hat{a}_{\mathrm{s}}\hat{a}_{\mathrm{i}}\big)|0\rangle$ from eq. (1.20) is represented by $\boldsymbol{d}^{(q)} = 0$ and

$$\boldsymbol{\Gamma}^{(q)} = \begin{pmatrix}\cosh(2r) & \cos(\theta)\sinh(2r) & 0 & \sin(\theta)\sinh(2r)\\ \cos(\theta)\sinh(2r) & \cosh(2r) & \sin(\theta)\sinh(2r) & 0\\ 0 & \sin(\theta)\sinh(2r) & \cosh(2r) & -\cos(\theta)\sinh(2r)\\ \sin(\theta)\sinh(2r) & 0 & -\cos(\theta)\sinh(2r) & \cosh(2r)\end{pmatrix}. \tag{C.3}$$

- The transformation for the phase rotation of a single mode is represented by [101]

$$\boldsymbol{S}^{(q)} = \begin{pmatrix} \cos(\phi) & \sin(\phi) \\ -\sin(\phi) & \cos(\phi) \end{pmatrix} . \tag{C.4}$$

- The transformation for a beam splitter coupling two modes, with a field transmission of κ and $\kappa^2 + r^2 = 1$, $\kappa, r \in \mathbb{R}$, is represented by [101]

$$\boldsymbol{S}^{(q)} = \begin{pmatrix} \kappa & r & 0 & 0 \\ -r & \kappa & 0 & 0 \\ 0 & 0 & \kappa & r \\ 0 & 0 & -r & \kappa \end{pmatrix} = \begin{pmatrix} \kappa & r \\ -r & \kappa \end{pmatrix}^{\oplus 2} . \tag{C.5}$$

- If a beam splitter is introduced into one of the modes of a state, an additional mode containing vacuum needs to be introduced for the second beam splitter input before the beam splitter transformation can be applied. This is performed by inserting two new columns and rows into $\boldsymbol{\Gamma}^{(q)}$ for the x and p components with 1 on the diagonal.

- Sometimes, only a subset $M = \{m_1, m_2, \dots\}$ of all modes is of interest, and the other modes are removed by a partial trace. For that, the unwanted modes are deleted from $\boldsymbol{\Gamma}$ and $\boldsymbol{d}$. Formally this is achieved by applying the projection matrix $\boldsymbol{P}_M$ to $\boldsymbol{\Gamma}$:

$$\boldsymbol{\Gamma}' = \boldsymbol{P}_M \boldsymbol{\Gamma} \boldsymbol{P}_M \,, \quad \text{and} \quad \boldsymbol{d}' = \boldsymbol{P}_M \boldsymbol{d} \,. \tag{C.6}$$

  The projection matrix is described by a vector $\boldsymbol{p}$ of diagonal elements:

$$\boldsymbol{P}_M = \mathrm{diag}(\boldsymbol{p})^{\oplus 2} \quad \text{with} \quad p_s = \begin{cases} 1 & \text{if } s \in M \,, \\ 0 & \text{otherwise.} \end{cases} \tag{C.7}$$

- Combining the last three operations, losses can be modeled by introducing an auxiliary mode containing vacuum, coupling it to the mode experiencing losses with a beam splitter with transmission τ^2 and $\tau > 0$, and tracing out the auxiliary mode. The combined loss transformation for a single-mode reads [101]

$$\boldsymbol{\Gamma}' = \tau^2 \boldsymbol{\Gamma} + (1 - \tau^2)\mathbb{1} \,, \;\; \boldsymbol{d}' = \tau \boldsymbol{d} \,. \tag{C.8}$$

D Details on the Implementation of the Frequency Resolved Simulation

Two different simulations were set up as the QKD system can be operated with type-0 or type-II SPDC. Although the simulations are conceptually very similar, some details of the implementations are different.

D.1 Details of the Type-II Simulation

Series Expansions

The spectrum of the photons from type-II SPDC shows side lobes, and the QBER increases when the CD elongates the wave packet so much that photons leak into adjacent time bins (cf. fig. 2.26 (a)). Therefore, the frequency range of the JSA for the type-II simulation must be chosen large enough to cover the side lobes. The type-II simulation, therefore, uses the approximations of the cosh and sinh functions to order $N = 2$ from eqs. (7.63) to (7.66). It evaluates the expansion of the determinant to the second order by using the expressions for $\mathrm{tr}(\mathit{\Xi})$ and $\mathrm{tr}\big[\big(\mathit{\Xi}_{(\diagup)}\big)^2\big]$ from eqs. (7.68) and (7.69).

Inverse Fourier Transformation

As the signal and idler frequencies are close to the minimum of the frequency-dependent attenuation coefficient in the SMFs around 1550 nm (cf. fig. 1.5), the transmission losses in the fiber are assumed to be frequency-independent, meaning that the transmission factors $\tau_{\mathrm{fib,\,A/B}}$ are independent of the frequency. For the propagation phases $\phi_{\mathrm{fib}}(\omega) = k(\omega)L$, the approximation of $k(\omega)$ up to the $\mathcal{O}\big((\omega - \omega_0)^2\big)$ term from eq. (1.11) is used. The phase terms from the propagation through the fiber links that are constant or linear in ω_{s} and ω_{i} are omitted because they only represent the absolute phase and overall arrival time of the wave packets, which are of no further relevance. The shape of the biphoton wave packet after the transmission through the fiber links is obtained by evaluating the two-dimensional IFT in the diagonal $\omega_\pm$ coordinate system:

$$\begin{aligned}\psi_{\mathrm{fib}}(t_{\mathrm{s}}, t_{\mathrm{i}}) &= \frac{1}{2\pi} \iint \tilde{\psi}(\omega_{\mathrm{s}}, \omega_{\mathrm{i}})\, \mathrm{e}^{-\mathrm{i}\omega_{\mathrm{s}} t_{\mathrm{s}} - \mathrm{i}\omega_{\mathrm{i}} t_{\mathrm{i}}}\, \mathrm{e}^{\mathrm{i}\beta[L_{\mathrm{s}}(\omega_{\mathrm{s}}-\omega_0)^2 + L_{\mathrm{i}}(\omega_{\mathrm{i}}-\omega_0)^2]/2}\, \mathrm{d}\omega_{\mathrm{s}}\, \mathrm{d}\omega_{\mathrm{i}} \\ &= \frac{\mathrm{e}^{-\mathrm{i}\omega_0 t_+}}{2} \overbrace{\mathcal{F}^{-1}_{\omega_-}\Big[\tilde{\Phi}(\omega_-)\, \mathrm{e}^{\mathrm{i}\omega_-^2 \beta L_+/8} \underbrace{\mathcal{F}^{-1}_{\omega'}\Big[\tilde{A}(\omega')\, \mathrm{e}^{\mathrm{i}\omega'^2 \beta L_+/8}\Big]\Big(\frac{t_+}{2} - \omega_- \frac{\beta L_-}{4}\Big)}_{\text{Inner IFT computed by using standard IFFT}}\Big]\Big(\frac{t_-}{2}\Big)}^{\text{Outer IFT computed by using Andrianov's method}} .\end{aligned} \tag{D.1}$$

Here, the abbreviations $\omega' = \omega_+ - 2\omega_0$ and $L_\pm = L_{\mathrm{s}} \pm L_{\mathrm{i}}$ have been introduced, and $\tilde{A}(\omega') = \tilde{\alpha}(\omega' - 2\omega_0)$ is the envelope of the pump pulse spectrum as before. The initial JSA $\tilde{\psi}(\omega_{\mathrm{s}}, \omega_{\mathrm{i}})$ is represented by points on a rectangular grid in the diagonal coordinate system. The phase oscillations introduced by the quadratic phase term $\mathrm{e}^{\mathrm{i}\omega'^2 \beta L_+/8}$ in the inner IFT are sufficiently slow in the narrow spectral range of $\tilde{A}(\omega')$ such that the IFT can be evaluated by directly applying the IFFT. In the outer IFT, the factor $\mathrm{e}^{\mathrm{i}\omega_-^2 \beta L_+/8}$ can introduce considerable phase oscillations when the transmission links are long. In these cases, which include the transmission distances used in the field test, Andrianov's method [91] (cf. eq. (1.16)) is used to compute the IFT efficiently.

Evaluation of Wave Packet Overlaps

The evaluation of the vacuum detection probabilities requires the evaluation of overlap integrals (cf. eqs. (7.68) and (7.69)) of the type

$$\int_{I_{\mathrm{A}}} \int_{I_{\mathrm{B}}} \Psi_{\mathrm{fib}}(t_{\mathrm{A}}, t_{\mathrm{B}}) \Psi^*_{\mathrm{fib}}(t_{\mathrm{A}} - t', t_{\mathrm{B}} - t'')\, \mathrm{d}t_{\mathrm{B}}\, \mathrm{d}t_{\mathrm{A}} \tag{D.2}$$

and the summation of multiple of such terms. Depending on the arguments t' and t'' and the elongation of the wave packets due to CD, some or most of these integrals do not have a significant overlap. The summation in eq. (7.69), for example, runs over $2^8 \times 3^2 = 2304$ terms. To reduce the computation time, the shifts in the arguments are compared to the extent of the grids. Integrals for which the discretization grids do not overlap are set directly to zero. This is the case when the elongation of the wave packet due to CD is not large enough to lead to a leakage of photons into adjacent time bins. For combinations with non-zero overlap, ψ_{fib} and ψ^*_{fib} are interpolated to a joint diagonal grid. The integral is then approximated by summing up the products of the values on the grid points in the rectangle spanned by the detection intervals I_{A} and I_{B}.

Besides the elongation of the wave packet envelope, CD leads to a quadratic time dependence of the phase of the wave packet. When Andrianov's method is used to compute the IFT, the quadratic phase becomes directly apparent outside the FTs. Therefore, under the overlap integral eq. (D.2) a phase factor

$$\exp\left(-\frac{\mathrm{i}t_-^2}{2\beta L_+}\right)\exp\left(\frac{\mathrm{i}(t_- - t' + t'')^2}{2\beta L_+}\right) = \exp\left(\frac{\mathrm{i}(t' - t'')^2}{2\beta L_+}\right)\underbrace{\exp\left(-\mathrm{i}t_-\frac{t' + t''}{\beta L_+}\right)}_{\text{Oscillating term}} \tag{D.3}$$

appears, oscillating in t_--direction. When the oscillation period $\beta L_+/(t' + t'')$ is much larger than the resolution of the discrete approximation of the integral, the sum can be evaluated as usual. However, when sufficiently many oscillations are present within a single discrete step Δt_-, the oscillations cancel the integral approximately to zero. Therefore, if $\Delta t_- \geq 100\beta L_+/(t' + t'')$, the integral value is set to zero. Otherwise, the discretization is refined such that $\beta L_+/(t' + t'') \geq 12\Delta t_-$ and the integral is evaluated.

Errors in the Time Basis from Adjacent Repetition Cycles

Compared to the frequency-independent simulation, the most relevant advantage of the frequency-resolved simulation is the ability to model *chromatic dispersion* (CD). As discussed in section 2.3.1, CD elongates the photon wave packets in time. When the wave packets become too long, photons leak into adjacent time bins. Within one repetition cycle, this leakage is automatically represented by sums over the different path combinations and time bins in Ξ. Additionally, photons from adjacent pulse repetition cycles can leak into the time bins, as shown in fig. D.1. As the simulation computes the detection probabilities only for one repetition cycle, such inter-cycle leakage effects are not automatically included. In principle, extending the simulation to cover multiple pulse repetitions would be possible by extending the pump pulse shape to multiple repetition cycles. However, this approach would significantly increase the required computational resources. Instead, inter-cycle leakage is modeled by adjusting the vacuum detection probabilities from the single-cycle simulation.

All pulse repetitions are equal, so considering the N-th repetition cycle is sufficient. When the dispersion effects are not too strong, it is sufficient to consider the leakage from directly adjacent time bins only, as shown in fig. D.1. In general, the probability that photons leak from time bin i in cycle $N - z$ with $z \in \mathbb{Z}$ into time bin j in cycle N is the same probability that photons from time bin i in cycle N leak into time bin j in cycle $N + z$. Furthermore, the detection of photons in different repetition cycles is independent, except for the dead

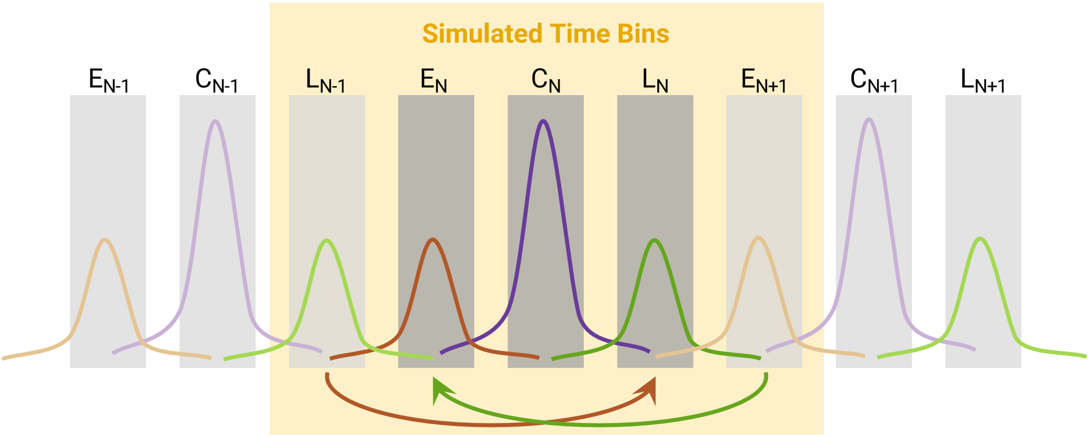


Figure D.1: Model of photon leakage into adjacent time bins due to chromatic dispersion for the N-th repetition cycle with time bins E (early), C (central), and L (late). For simplicity, it is assumed that photons do not leak into time bins beyond the directly adjacent time bins, such that it is sufficient to simulate the additional time bins L_{N-1} to L_{E+1}. The probability that photons from L_{N-1} leak into E_N is the same as the probability that photons from L_N leak into E_{N+1}. Therefore, the vacuum detection probability for E_N is multiplied by the vacuum probability for E_{N+1} (green arrow). Similarly, the vacuum probability obtained for L_N is multiplied by the vacuum probability for L_{N-1} (brown arrow).

time effect. The probability that some detector measures vacuum in a set of time bins $\{i\}$, including the leakage, is therefore given by

$$p'_{\text{vac}}(\{i\}) = p_{\text{vac}}(\{i\}) \prod_{\substack{z\in\mathbb{Z}\\ z\neq 0}} p_{\text{vac, no noise}}\left(\{i\} + \frac{z}{f_{\text{rep}}}\right). \tag{D.4}$$

The vacuum probability $p_{\text{vac}}(\{i\})$ for the N-th pulse cycle alone is obtained directly from the determinant describing the detection probability. The probabilities $p_{\text{vac, nonoise}}(\{\bar{i}\} + z/f_{\text{rep}})$ take into account that vacuum is only measured when additionally no photons from any other repetition cycle have leaked into $\{i\}$ in cycle N, which is the same probability as the probability that no photon has leaked from cycle N into the time bins $\{i\}$ of any other repetition. These probabilities only consider photon counts and are therefore calculated for zero noise. The probabilities for coincident counts are modified similarly, as described in ref. [VII].

D.2 Details of the Type-0 Simulation

Singular Value Decomposition of the JSA

The type-0 SPDC spectrum is much broader than the type-II spectrum and almost constant over the width of the WDM channels used for QKD. Due to the large aspect ratio between the ω_- and ω_+ directions of the overall type-0 JSA, a direct computation of the Schmidt decomposition of the full JSA would require a considerable amount of computational resources. However, the frequency range on which the decomposition needs to be computed can be reduced to a domain including the frequency channel and a relatively small neighborhood. For iterations of the JSA operator such as $(\tilde{\Psi}^\dagger \tilde{\Psi})^n \tilde{\Psi}$ it was discussed that the narrow antidiagonal stripe of width Δ_+ (in the diagonal coordinate system) on which the JSA attains non-negligible values broadens at most by Δ_+ for each JSA factor in such a product (cf. fig. 7.2 and eq. (7.23)). A slice through the stripe in the direction of ω_A or ω_B also has a width of Δ_+ (in the rectilinear coordinate system). A value of the JSA at some point (ω_1, ω_2) can therefore not spread to points that are further apart from (ω_1, ω_2) than Δ_+ in the products $\tilde{\Psi}^\dagger \tilde{\Psi}$ or $\tilde{\Psi}\tilde{\Psi}^\dagger$. More generally, the value of a product involving N JSA operators at some point (ω_1, ω_2) on the stripe is therefore not affected by points of the JSA that are further apart from (ω_1, ω_2) than $N\Delta_+$ in the direction of ω_A or ω_B. When the cosh and sinh series expansions are truncated after order N, it is therefore sufficient to compute the iterated JSA kernels on a square given by the channel width $\pm N\Delta_+$ in each direction.

For the type-0 simulation, the series are truncated at $N = 5$, and the domain on which the JSA is evaluated is therefore chosen to the channel width $\pm 5\Delta_+$ in each direction. On this domain, the Schmidt decomposition is approximated by the SVD of the discretized JSA, and the approximations $\cosh_{N=5}$ and $\sinh_{N=5}$ are computed from the singular values.

Inverse Fourier Transformation and Evaluation of the Determinant

To obtain the shape of the biphoton wave packet in the time domain, the left and right singular vectors are multiplied by $\tau_{\mathrm{fib,A}}(\omega)\exp(\mathrm{i}\phi_{\mathrm{fib}}^{(\mathrm{A})}(\omega))$ and $\tau_{\mathrm{fib,B}}(\omega)\exp(\mathrm{i}\phi_{\mathrm{fib}}^{(\mathrm{B})}(\omega))$ representing the frequency-dependent losses in the WDM and the phases acquired in the fiber links. Similar to the type-II simulation, only the phase terms with a quadratic ω-dependence are considered. The shape of the wave packet in the time domain is obtained by taking the IFFT of the singular vectors, meaning that eqs. (7.43) and (7.44) are computed numerically. Thereby, the biphoton wave packet is represented by points in the rectilinear coordinate system. From a practical point of view, it is convenient to evaluate the IFFT for discrete frequency vectors centered at the channel center frequencies. This corresponds to shifting the argument of the Fourier transform, which, by the FT shift theorem, corresponds to multiplying the result with phase terms with linear ω dependence. These phase terms do not change the determinant of Ξ and can be discarded, meaning that the IFFTs can be centered at the channel center frequencies.

Photon leakage into adjacent time bins due to CD can be considered with the same method as for the type-II simulation. However, photon leakage is currently not implemented in the type-0 simulation because the effect is for the relevant transmissions distances negligible due to the narrower channel spectra (cf. fig. 2.26 (b)).

The sum in eq. (7.52) requires the addition of multiple matrices with relative time shifts, which is implemented by interpolating the transformed singular vectors to a common grid. The determinant of the resulting matrix is then computed numerically. This numerical computation benefits considerably from the reordering of the matrix in eq. (7.32) and from the application of eq. (7.49), reducing the matrix size from 24×24 to 2×2 blocks of the same size. The number of operations to calculate the determinant via *LU* decomposition scales with the third power of the matrix dimension [296], such that the speedup for computing the determinant over all modes can be roughly estimated to a factor of $12^3 = 1728$.

Acknowledgements

First, I want to thank Prof. Dr. Thomas Walther for supervising my thesis, for his support, and for the freedom to work on all the exciting research sub-topics presented in this thesis. I also want to thank Prof. Dr. Gerhard Birkl for studying my work and being the second referee of this thesis.

My special thanks go to my project partners Oleg Nikiforov, Maximilian Tippmann, Jakob Kaltwasser, and Maximilian Mengler.

Many thanks also go to all of the students who worked on this project: Daniel Hofmann, Lucas Bialowons, Florian Vogel, Till Dolejsky, Philipp Kleinpaß, Florian Niederschuh, Tim Röpke, and Christian Schaub.

I thank Robin Krebs, Thorsten Haase, Alexander Sauer, Julian Nauth, and Prof. Dr. Gernot Alber from the *Theoretical Quantum Physics* research group for the great collaborations on the detector tomography and an early version of the frequency-resolved simulation.

I also thank Karen Böhling and Dr. Mathias Sinther for their support in organizational matters in the *Laser and Quantum Optics* research group and Dr. Thorsten Führer for the IT support. I thank the other Ph.D. candidates and students from the research group for their support. Furthermore, I thank the *CROSSING* research center for enabling the interdisciplinary exchange and the opportunity to participate in various transferable skills training courses.

I thank Prof. Dr. K. J. Boller for lending the unpackaged photonic chip to me. I also want to thank Felix Wissel, Matthias Gunkel, Paul Wagner, Udo Backer, and the rest of the team of the *Deutsche Telekom Network Innovation Center* in Darmstadt for lending me optical test equipment and fiber spools and for their support during the field test.

Last but not least, I thank my family and friends for their support and motivation while working on the research for this thesis.

The work presented in this doctoral thesis is a part of the research project *P4 – Quantum Key Hubs* of the collaborative research center *CROSSING* funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under grant No. SFB 1119–236615297.

Since the author is not a native speaker, the online English grammar tool *grammarly* was used to check grammar and spelling.

Associated Publications

Publications in Journals, Manuscripts, and Reports

[I] S. Euler, E. Fitzke, O. Nikiforov, D. Hofmann, T. Dolejsky, and Th. Walther. Spectral characterization of SPDC-based single-photon sources for quantum key distribution. The European Physical Journal Special Topics **230** (2021), 1073–1080 (cit. on pp. xvii, 46, 49, 74).

[II] E. Fitzke, L. Bialowons, T. Dolejsky, M. Tippmann, O. Nikiforov, Th. Walther, F. Wissel, and M. Gunkel. Scalable Network for Simultaneous Pairwise Quantum Key Distribution via Entanglement-Based Time-Bin Coding. PRX Quantum **3** (2022), 020341 (cit. on pp. xvii, xviii, 26, 28, 58, 73–75, 81, 93, 149).

[III] E. Fitzke, R. Krebs, T. Haase, M. Mengler, G. Alber, and Th. Walther. Time-dependent POVM reconstruction for single-photon avalanche photo diodes using adaptive regularization. New Journal of Physics **24** (2022), 023025 (cit. on pp. xvii, xviii, 109, 117, 119, 120, 122, 124).

[IV] E. Fitzke, F. Niederschuh, and Th. Walther. Simulating the Photon Statistics of Gaussian States Employing Automatic Differentiation from PyTorch. Technical Report. DOI: 10.26083/tuprints-00023061. Technische Universität Darmstadt, 2022 (cit. on pp. xvii, xix, 125, 139, 151).

[V] T. Dolejsky, E. Fitzke, L. Bialowons, M. Tippmann, O. Nikiforov, and Th. Walther. Flexible reconfigurable entanglement-based quantum key distribution network. The European Physical Journal Special Topics (2023) (cit. on pp. xvii, xviii, 75, 93).

[VI] E. Fitzke, F. Niederschuh, and Th. Walther. Simulating the photon statistics of multimode Gaussian states by automatic differentiation of generating functions. APL Photonics **8** (2023), 026106 (cit. on pp. xvii, xix, 125, 132, 134, 137–139, 141, 142, 145, 149, 151).

[VII] P. Kleinpass, E. Fitzke, and Th. Walther. Approximating Highly Entangled Biphoton States for QKD Simulations. Manuscript to be submitted (2023) (cit. on pp. xvii, xix, 145, 153, 175, 181, 183, 212).

[VIII] M. Tippmann, E. Fitzke, O. Nikiforov, P. Kleinpass, T. Dolejsky, M. Mengler, and Th. Walther. A flexible modular all-fiber based photon pair source for quantum key distribution in a network. Submitted Manuscript (2023) (cit. on pp. xvii, xviii, 26, 42, 46, 74, 149).

[IX] J. Kaltwasser, J. Seip, E. Fitzke, M. Tippmann, and T. Walther. Reducing the number of single-photon detectors in quantum-key-distribution networks by time multiplexing. Phys. Rev. A **109** (2024), 012618 (cit. on pp. xvii, 190).

Contributions at International Conferences

E. Fitzke, T. Dolejsky, M. Tippmann, L. Bialowons, O. Nikiforov, F. Wissel, M. Gunkel, and Th. Walther. An Entanglement-Based QKD System for Scalable Robust Multi-User Networks. Conference on Lasers and Electro-Optics (CLEO), San Jose - California - United States 2022 (Highlighted Talk).

E. Fitzke, M. Tippmann, and Th. Walther. A scalable quantum key distribution network based on time-bin entanglement. Frontiers of Quantum and Mesoscopic Thermodynamics (FQMT), Prag - Czech Republic 2022 (Talk).

M. Tippmann, E. Fitzke, L. Bialowons, T. Dolejsky, O. Nikiforov, and Th. Walther. A reconfigurable scalable network for entanglement-based multi-user QKD. International Conference on Quantum Communication, Measurement and Computing (QCMC). Lisbon - Portugal 2022 (Poster).

L. Bialowons, E. Fitzke, M. Tippmann, O. Nikiforov, and Th. Walther. A Scalable Multi-User QKD Hub for Entanglement-Based Phase-Time Coding. Quantum Information and Measurement VI (QIM), Washington, DC - United States 2021 (Online, Talk).

O. Nikiforov, E. Fitzke, D. Hofmann, K. Roth, and Th. Walther. Test of a Time-bin Entanglement-based QKD System in a Commercial Optical Link. QCALL ESR Conference, Mondello - Italy 2019 (Poster).

E. Fitzke, D. Hofmann, T. Dolejsky, O. Nikiforov, J. Nauth, and Th. Walther. Spectral Characterization of Photon Pairs for Quantum Key Distribution. QCALL ESR Conference, Mondello - Italy 2019 (Poster).

Contributions at National Conferences

F. Niederschuh, E. Fitzke, and Th. Walther. Photon-number resolved model for multimode quantum optical setups based on Gaussian states. DPG spring meeting. QI 6.5. Hannover - Germany 2023 (Poster).

A. Klute, M. Tippmann, L. Bialowons, E. Fitzke, and Th. Walther. Design of a 4-party active base choice phase-coding quantum key distribution multi-user hub. DPG spring meeting. QI 6.16. Hannover - Germany 2023 (Poster).

F. VOGEL, E. FITZKE, J. KALTWASSER, and TH. WALTHER. Photon pair generation using spontaneous four-wave mixing (SFWM) in microring resonators on a photonic silicon chip. DPG spring meeting. Q 60.2. Erlangen - Germany 2022 (Poster).

M. TIPPMANN, E. FITZKE, L. BIALOWONS, O. NIKIFOROV, and TH. WALTHER. A scalable four user quantum key hub for phase-time coding quantum key distribution. DPG spring meeting. Q 60.3. Erlangen - Germany 2022 (Poster).

M. MENGLER, E. FITZKE, R. KREBS, T. HAASE, G.ALBER, and TH. WALTHER. Time-dependent single photon detector tomography. DPG spring meeting. Q 60.4. Erlangen - Germany 2022 (Poster).

P. KLEINPASS, E. FITZKE, and TH. WALTHER. Simulation of fiber-based quantum key distribution (QKD) with highly entangled states including multi-photon pair effects. DPG spring meeting. Q 60.5. Erlangen - Germany 2022 (Poster).

T. DOLEJSKY, E. FITZKE, M. TIPPMANN, L. BIALOWONS, O. NIKIFOROV, and TH. WALTHER. Quantum Key Distribution based on time-bin entanglement in a scalable star-shaped network. DPG spring meeting. Q 60.6. Erlangen - Germany 2022 (Poster).

J. NAUTH, E. FITZKE, A. SAUER. G. ALBER, and TH. WALTHER. Simulation of generation and transmission of photons from SPDC for quantum key distribution with phase-time coding. DPG fall meeting. FM 31.6. Freiburg - Germany 2019 (Talk).

M. TIPPMANN, O. NIKIFOROV, E. FITZKE, and TH. WALTHER. Fiber-based source for QKD around 1550 nm. DPG fall meeting. FM 86.4. Freiburg - Germany 2019 (Poster).

D. HOFMANN, E. FITZKE, O. NIKIFOROV, and TH. WALTHER. Spectral characterization of an entangled photon pair source for QKD. DPG spring meeting. Q 41.32. Rostock - Germany 2019 (Poster).

K. ROTH, S. SCHÜRL, E. FITZKE, O. NIKIFOROV, and TH. WALTHER. An FPGA based time-acquisition system for QKD. DPG spring meeting. Q 41.27. Rostock - Germany 2019 (Poster).

M. TIPPMANN, O. NIKIFOROV, E. FITZKE, and TH. WALTHER. All-fiber source for time-bin entangled photon pairs at 1550 nm. DPG spring meeting. Q 41.26. Rostock - Germany 2019 (Poster).

Associated Master’s and Bachelor’s Theses

The following theses of bachelor and master students are associated with the work presented in this doctoral thesis.

Master’s Theses

[M1] D. Hofmann. Charakterisierung einer Photonenpaarquelle zum Quantenschlüsselaustausch in einem Telekommunikationsnetzwerk. Master’s thesis, supervised by Prof. Dr. Thomas Walther and Erik Fitzke (2019) (cit. on pp. xvii, 25, 43, 48, 50).

[M2] J. Kaltwasser. Photonen-Paar-Erzeugung für ein ein Mehrparteien- Quantenschlüsselsystem mit SFWM in Mikroring-Resonatoren. Master’s thesis, supervised by Prof. Dr. Thomas Walther and Erik Fitzke (2020) (cit. on pp. xvii, 96).

[M3] J. Nauth. Modeling and Simulation of Photon Generation, Transmission and Detection for QKD with Phase-Time Coding. Master’s thesis, supervised by Prof. Dr. Gernot Alber and Alexander Sauer (2020) (cit. on pp. xvii, 133, 153).

[M4] M. Tippmann. Development of a pulsed all-fiber SPDC photon pair source. Master’s thesis, supervised by Prof. Dr. Thomas Walther and Oleg Nikiforov (2020) (cit. on pp. xvii, 25, 34).

[M5] L. Bialowons. Completion of a 4-Party Time-bin Entanglement QKD System. Master’s thesis, supervised by Prof. Dr. Thomas Walther and Erik Fitzke (2021) (cit. on pp. xvii, 43, 61, 65, 66, 75, 81, 89, 144, 191).

[M6] T. Dolejsky. Towards a Distributed Quantum Key Distribution Network. Master’s thesis, supervised by Prof. Dr. Thomas Walther and Erik Fitzke (2022) (cit. on pp. xvii, 75).

[M7] P. Kleinpass. Description and Simulation of Entanglement-Based Phase-Time Quantum Key Distribution. Master’s thesis, supervised by Prof. Dr. Thomas Walther and Erik Fitzke (2022) (cit. on pp. xvii, 153).

[M8] M. MENGLER. Characterization of a Photonic Chip for Photon Pair Generation by Spontaneous Four-Wave-Mixing. Master's thesis, supervised by Prof. Dr. Thomas Walther and Erik Fitzke (2022) (cit. on pp. xvii, 43, 102, 201).

[M9] F. VOGEL. Stabilisierung von Mikroringresonatoren zur Photonenpaarproduktion mit SFWM mittels PDH-Locking. Master's thesis, supervised by Prof. Dr. Thomas Walther and Erik Fitzke (2022) (cit. on pp. xvii, 96).

Bachelor's Theses

[B1] T. DOLEJSKY. Hong-Ou-Mandel-Experiment mit SPDC Photonen für das Quantenhub-Projekt. Bachelor's thesis, supervised by Prof. Dr. Thomas Walther and Erik Fitzke (2019) (cit. on p. xvii).

[B2] P. KLEINPASS. Time-resolved tomography measurements of a single-photon avalanche diode. Bachelor's thesis, supervised by Prof. Dr. Thomas Walther and Erik Fitzke (2020) (cit. on pp. xvii, 63, 109).

[B3] R. KREBS. Time Resolved Quantum Detector Tomography. Bachelor's thesis, supervised by Prof. Dr. Gernot Alber and Thorsten Haase (2020) (cit. on pp. xvii, 110, 117).

[B4] M. MENGLER. Charakterisierung der Effizienz und des Jitters von Einzelphotonendetektoren mittels POVMs. Bachelor's thesis, supervised by Prof. Dr. Thomas Walther and Erik Fitzke (2020) (cit. on pp. xvii, 109).

[B5] F. NIEDERSCHUH. Simulation der Interferenz beim Phase-Time-Coding basierend auf gaussschen Zuständen. Bachelor's thesis, supervised by Prof. Dr. Thomas Walther and Erik Fitzke (2020) (cit. on pp. xvii, 125).

[B6] T. RÖPKE. Programming a DAC card for the use in quantum key distribution with phase modulators. Bachelor's thesis, supervised by Prof. Dr. Thomas Walther and Erik Fitzke (2020) (cit. on p. xvii).

[B7] C. SCHAUB. Optimierung der Taktrückgewinnung aus einzelnen Photonendetektionen für ein Quantenschlüsselsystem. Bachelor's thesis, supervised by Prof. Dr. Thomas Walther and Erik Fitzke (2022) (cit. on pp. xvii, 69).

List of Tables

List of Figures

Bibliography

[1] R. A. Grimes. Cryptography Apocalypse - Preparing for the Day When Quantum Computing Breaks Today's Crypto. DOI: 10.1007/s00287-020-01239-6. John Wiley & Sons 2019 (cit. on p. xv).

[2] National Security Agency. Quantum Computing and Post-Quantum Cryptography. General Information. Last accessed Sep. 26 2023, https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF. 2021 (cit. on pp. xv, 4).

[3] Agence nationale de la sécurité des systèmes d'information (ANSSI). ANSSI views on the Post-Quantum Cryptography transition. Position Paper. Last accessed Sep. 26 2023, https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/. 2021 (cit. on pp. xv, 4).

[4] National Cyber Security Center. Preparing for Quantum-Safe Cryptography. White Paper. Last accessed Sep. 26 2023, https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography. 2020 (cit. on pp. xv, 4).

[5] Federal Office for Information Security (BSI). Quantum-safe cryptography - fundamentals, current developments and recommendations. Last accessed Sep. 26 2023, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html (2022) (cit. on pp. xv, 3, 4, 8).

[6] The White House. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. Last accessed Sep. 26 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (2022) (cit. on p. xv).

[7] C. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In: International Conference on Computers, Systems & Signal Processing - Bangalore, India 1984 (cit. on pp. xvi, 4, 5).

[8] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science **560** (2014), 7–11 (cit. on pp. xvi, 4, 5).

[9] ID Quantique. Providing the ultimate, long-term data protection in a post-quantum world. Last accessed Sep. 26 2023, https://www.idquantique.com/quantum-safe-security/products/#quantum_key_distribution (2023) (cit. on p. xvi).

[10] MagiQ. MagiQ QPN - Ultimate Cryptography Solution for Network Security. Last accessed Sep. 26 2023, https://www.magiqtech.com/solutions/network-security/ (2023) (cit. on p. xvi).

[11] Quantum Optics Jena. Quantum Key Distribution Systems. Last accessed Sep. 26 2023, https://qo-jena.com/products-overview/ (2023) (cit. on p. xvi).

[12] Quantum Telecommunications Italy. Quantum Key Distribution in Software Defined Networks - Bringing QKD in real world telecommunications. Last accessed Sep. 26 2023, https://www.qticompany.com/wp-content/uploads/2023/08/flyer-A5_SDN_v2.pdf (2023) (cit. on p. xvi).

[13] Quantum Telecommunications Italy. Free Space Quantum Key Distribution. Last accessed Sep. 26 2023, https://www.qtlabs.at/products-and-services/free-space-qkd/ (2023) (cit. on p. xvi).

[14] KEEQuant. Quantum Key Distribution - Products. Last accessed Sep. 26 2023, https://www.keequant.com/products/ (2023) (cit. on p. xvi).

[15] QuantumCTek. Quantum Products. Last accessed Sep. 26 2023, http://www.quantum-info.com/English/product/ (2023) (cit. on p. xvi).

[16] Toshiba. Quantum Key Distribution - The new age of secure communication, powered by quantum physics. Last accessed Sep. 26 2023, https://www.global.toshiba/ww/products-solutions/security-ict/qkd/products.html (2023) (cit. on p. xvi).

[17] W. Li *et al.* High-rate quantum key distribution exceeding 110 Mb s^{-1}. Nature Photonics **17** (2023), 416–421 (cit. on p. xvi).

[18] S. Wang *et al.* Twin-field quantum key distribution over 830-km fibre. Nature Photonics **16** (2022), 154–161 (cit. on p. xvi).

[19] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields. 600-km repeater-like quantum communications with dual-band stabilization. Nature Photonics **15** (2021), 530–535 (cit. on p. xvi).

[20] Y. LIU *et al.* Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber Distance. Phys. Rev. Lett. **130** (2023), 210801 (cit. on p. xvi).

[21] J. YIN *et al.* Satellite-based entanglement distribution over 1200 kilometers. Science **356** (2017), 1140–1144 (cit. on p. xvi).

[22] S.-K. LIAO *et al.* Satellite-Relayed Intercontinental Quantum Network. Phys. Rev. Lett. **120** (2018), 030501 (cit. on p. xvi).

[23] Y.-A. CHEN *et al.* An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature **589** (2021), 214–219 (cit. on p. xvi).

[24] X. ZHONG, W. WANG, R. MANDIL, H.-K. LO, and L. QIAN. Simple Multiuser Twin-Field Quantum Key Distribution Network. Phys. Rev. Applied **17** (2022), 014025 (cit. on p. xvi).

[25] Y.-L. TANG *et al.* Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network. Phys. Rev. X **6** (2016), 011024 (cit. on p. xvi).

[26] S. K. JOSHI *et al.* A trusted node-free eight-user metropolitan quantum communication network. Science Advances **6** (2020), eaba0959 (cit. on pp. xvi, 27, 89).

[27] M. ALSHOWKAN *et al.* Reconfigurable Quantum Local Area Network Over Deployed Fiber. PRX Quantum **2** (2021), 040304 (cit. on pp. xvi, 27).

[28] O. NIKIFOROV. Field Test of a Quantum Key Distribution System. Doctoral Thesis. Institute for Applied Physics: Technical University of Darmstadt, 2022 (cit. on pp. xvii, 12, 25, 28, 29, 40, 63, 65, 66, 76, 81, 84, 189).

[29] A. PASZKE *et al.* PyTorch: An Imperative Style, High-Performance Deep Learning Library. In: Advances in Neural Information Processing Systems 32. Ed. by H. WALLACH, H. LAROCHELLE, A. BEYGELZIMER, F. D'ALCHÉ-BUC, E. FOX, and R. GARNETT. Last accessed Sep. 26 2023, http://papers.neurips.cc/paper/9015-pytorch-an-imperative-style-high-performance-deep-learning-library.pdf. Curran Associates, Inc. 2019, 8024–8035 (cit. on pp. xix, 132, 139).

[30] M. DWORKIN, E. BARKER, J. NECHVATAL, J. FOTI, L. BASSHAM, E. ROBACK, and J. DRAY. Advanced Encryption Standard (AES). DOI: 10.6028/NIST.FIPS.197 (2001) (cit. on p. 3).

[31] N. GISIN, G. RIBORDY, W. TITTEL, and H. ZBINDEN. Quantum cryptography. Rev. Mod. Phys. **74** (2002), 145–195 (cit. on pp. 3–5, 9, 11, 191).

[32] J. BUCHMANN. Einführung in die Kryptographie. 6th ed. DOI: 10.1007/978-3-642-39775-2. Springer 2016 (cit. on p. 3).

[33] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science. DOI: 10.1109/SFCS.1994.365700. 1994, 124–134 (cit. on p. 3).

[34] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing **26** (1997), 1484–1509 (cit. on p. 3).

[35] National Institute of Standards and Technology (NIST). NIST IR 8413-upd1 – Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. DOI: 10.6028/NIST.IR.8413-upd1 (2022) (cit. on p. 4).

[36] W. Beullens. Breaking Rainbow Takes a Weekend on a Laptop. In: Advances in Cryptology – CRYPTO 2022. Ed. by Y. Dodis and T. Shrimpton. DOI: 10.1007/978-3-031-15979-4_16. Springer Nature Switzerland 2022, 464–479 (cit. on p. 4).

[37] W. Castryck and T. Decru. An Efficient Key Recovery Attack on SIDH. In: Advances in Cryptology – EUROCRYPT 2023. Ed. by C. Hazay and M. Stam. DOI: 10.1007/978-3-031-30589-4_15. Springer Nature Switzerland 2023, 423–447 (cit. on p. 4).

[38] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Du ek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. Rev. Mod. Phys. **81** (2009), 1301–1350 (cit. on pp. 4, 5, 8).

[39] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs. Attacks on practical quantum key distribution systems (and how to prevent them). Contemporary Physics **57** (2016), 366–387 (cit. on pp. 4, 8).

[40] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan. Secure quantum key distribution with realistic devices. Rev. Mod. Phys. **92** (2020), 025002 (cit. on pp. 4–8, 145).

[41] G. Brassard and L. Salvail. Secret-Key Reconciliation by Public Discussion. In: Advances in Cryptology — EUROCRYPT '93. Ed. by T. Helleseth. DOI: 10.1007/3-540-48285-7_35. Springer Berlin Heidelberg 1994, 410–423 (cit. on p. 6).

[42] J. Martínez Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin. Demystifying the Information Reconciliation Protocol Cascade. Quantum Information and Computation **15** (2014), 0453–0477 (cit. on p. 6).

[43] R. Gallager. Low-density parity-check codes. IRE Transactions on Information Theory **8** (1962), 21–28 (cit. on p. 6).

[44] A. Nakassis and A. Mink. LDPC error correction in the context of quantum key distribution. In: Quantum Information and Computation X. Ed. by E. Donkor, A. R. Pirich, and H. E. Brandt. Vol. 8400. DOI: 10.1117/12.919117. International Society for Optics and Photonics. SPIE 2012, 840009 (cit. on p. 6).

[45] S. H. Gupta and B. Virmani. LDPC for Wi-Fi and WiMAX technologies. In: 2009 International Conference on Emerging Trends in Electronic and Photonic Devices & Systems. DOI: 10.1109/ELECTRO.2009.5441120. 2009, 262–265 (cit. on p. 6).

[46] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover Hashing Against Quantum Side Information. IEEE Transactions on Information Theory **57** (2011), 5524–5535 (cit. on p. 6).

[47] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. Phys. Rev. A **72** (2005), 012332 (cit. on pp. 6, 8).

[48] R. Renner. Security of Quantum Key Distribution. International Journal of Quantum Information **06** (2008), 1–127 (cit. on p. 6).

[49] C. Portmann and R. Renner. Security in quantum cryptography. Rev. Mod. Phys. **94** (2022), 025008 (cit. on p. 6).

[50] P. W. Shor and J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. Phys. Rev. Lett. **85** (2000), 441–444 (cit. on p. 7).

[51] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros. Efficient reconciliation protocol for discrete-variable quantum key distribution. 2009 IEEE International Symposium on Information Theory (2009), 1879–1883 (cit. on p. 7).

[52] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photonics **4** (2010), 686–689 (cit. on p. 8).

[53] J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.-Å. Larsson. Hacking the Bell test using classical light in energy-time entanglement-based quantum key distribution. Science Advances **1** (2015), e1500793 (cit. on pp. 8, 9, 190).

[54] H.-K. Lo, M. Curty, and B. Qi. Measurement-Device-Independent Quantum Key Distribution. Phys. Rev. Lett. **108** (2012), 130503 (cit. on p. 8).

[55] W. Zhang *et al.* A device-independent quantum key distribution system for distant users. Nature **607** (2022), 687–691 (cit. on p. 8).

[56] A. Weber, O. Nikiforov, A. Sauer, J. Schickel, G. Alber, H. Mantel, and T. Walther. Cache-Side-Channel Quantification and Mitigation for Quantum Cryptography. In: Computer Security – ESORICS 2021. Ed. by E. Bertino, H. Shulman, and M. Waidner. DOI: 10.1007/978-3-030-88428-4_12. Springer International Publishing 2021, 235–256 (cit. on pp. 8, 192).

[57] J. Barrett, R. Colbeck, and A. Kent. Memory Attacks on Device-Independent Quantum Cryptography. Phys. Rev. Lett. **110** (2013), 010503 (cit. on p. 8).

[58] M. Curty and H.-K. Lo. Foiling covert channels and malicious classical post-processing units in quantum key distribution. npj Quantum Information **5** (2019), 14 (cit. on p. 8).

[59] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theorem. Phys. Rev. Lett. **68** (1992), 557–559 (cit. on p. 9).

[60] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication. Phys. Rev. Lett. **82** (1999), 2594–2597 (cit. on pp. 9, 11, 54).

[61] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Quantum Cryptography Using Entangled Photons in Energy-Time Bell States. Phys. Rev. Lett. **84** (2000), 4737–4740 (cit. on pp. 9, 11, 54, 62).

[62] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin. Distribution of Time-Bin Entangled Qubits over 50 km of Optical Fiber. Phys. Rev. Lett. **93** (2004), 180502 (cit. on pp. 9, 11, 62, 63).

[63] T. Honjo *et al.* Long-distance entanglement-based quantum key distribution over optical fiber. Opt. Express **16** (2008), 19118–19126 (cit. on pp. 9, 106, 193).

[64] H. Takesue, K.-i. Harada, K. Tamaki, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, and S.-i. Itabashi. Long-distance entanglement-based quantum key distribution experiment using practical detectors. Opt. Express **18** (2010), 16777–16787 (cit. on pp. 9, 106, 193).

[65] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, and H. Takesue. Entanglement distribution over 300 km of fiber. Opt. Express **21** (2013), 23241–23249 (cit. on pp. 9, 106, 193).

[66] E. Waks, A. Zeevi, and Y. Yamamoto. Security of quantum key distribution with entangled photons against individual attacks. Phys. Rev. A **65** (2002), 052310 (cit. on p. 9).

[67] K. Tamaki, M. Koashi, and N. Imoto. Unconditionally Secure Key Distribution Based on Two Nonorthogonal States. Phys. Rev. Lett. **90** (2003), 167904 (cit. on p. 9).

[68] J. D. Franson. Bell inequality for position and time. Phys. Rev. Lett. **62** (1989), 2205–2208 (cit. on p. 11).

[69] R. Engelbrecht. Nichtlineare Faseroptik - Grundlagen und Anwendungsbeispiele. DOI: 10.1007/978-3-642-40968-4. Springer Vieweg 2015 (cit. on pp. 11–13, 15, 16).

[70] International Telecommunication Union - Telecommunication Standardization Sector. ITU-T G.652 - Characteristics of a single-mode optical fibre and cable. Recommendation. Last accessed Sep. 26 2023, https://www.itu.int/rec/T-REC-G.652-201611-I/en. 2016 (cit. on pp. 11, 13, 76).

[71] Corning Inc. Corning SMF-28 Optical Fiber. Product Information PI1036. 2002 (cit. on p. 12).

[72] Corning Inc. Corning SMF-28 Ultra Optical Fiber. Product Information PI1424. Last accessed Sep. 26 2023, https://www.corning.com/media/worldwide/coc/documents/Fiber/PI1424_11-16.pdf. 2021 (cit. on p. 12).

[73] Corning Inc. AN 103 - Single Fiber Fusion Splicing. Application Note. Last accessed Sep. 26 2023, https://www.corning.com/media/worldwide/coc/documents/Fiber/application-notes/AN103.pdf. 2020 (cit. on pp. 12, 13).

[74] International Telecommunication Union - Telecommunication Standardization Sector. ITU-T G.694.1 - Spectral grids for WDM applications: DWDM frequency grid. Recommendation. Last accessed Sep. 26 2023, https://www.itu.int/rec/T-REC-G.694.1/en. 2020 (cit. on pp. 13, 29, 32, 99).

[75] J. P. Gordon and H. Kogelnik. PMD fundamentals: Polarization mode dispersion in optical fibers. Proceedings of the National Academy of Sciences **97** (2000), 4541–4550 (cit. on p. 13).

[76] R. Wagner. Phenomenological approach to polarisation dispersion in long single-mode fibres. Electronics Letters **22** (1986), 1029–1030(1) (cit. on p. 13).

[77] A. Vannucci and A. Bononi. Statistical characterization of the Jones matrix of long fibers affected by polarization mode dispersion (PMD). Journal of Lightwave Technology **20** (2002), 811–821 (cit. on p. 13).

[78] L. E. Nelson and R. M. Jopson. Introduction to polarization mode dispersion in optical systems. Journal of Optical and Fiber Communications Reports **1** (2004), 312–344 (cit. on p. 13).

[79] S. Wengerowsky *et al.* Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre. npj Quantum Information **6** (2020), 5 (cit. on pp. 13, 14).

[80] S. P. Neumann, A. Buchner, L. Bulla, M. Bohmann, and R. Ursin. Continuous entanglement distribution over a transnational 248 km fiber link. Nature Communications **13** (2022), 6134 (cit. on pp. 13, 14).

[81] Y. Shi, S. Moe Thar, H. S. Poh, J. A. Grieve, C. Kurtsiefer, and A. Ling. Stable polarization entanglement based quantum key distribution over a deployed metropolitan fiber. Applied Physics Letters **117** (2020), 124002 (cit. on p. 13).

[82] S. Wengerowsky *et al.* Entanglement distribution over a 96-km-long submarine optical fiber. Proceedings of the National Academy of Sciences **116** (2019), 6684–6688 (cit. on p. 14).

[83] K. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima. Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days. Opt. Express **21** (2013), 31395–31401 (cit. on p. 14).

[84] Y.-Y. Ding, H. Chen, S. Wang, D.-Y. He, Z.-Q. Yin, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han. Polarization variations in installed fibers and their influence on quantum key distribution systems. Opt. Express **25** (2017), 27923–27936 (cit. on p. 14).

[85] J. Chen, G. Wu, Y. Li, E. Wu, and H. Zeng. Active polarization stabilization in optical fibers suitable for quantum key distribution. Opt. Express **15** (2007), 17928–17936 (cit. on p. 14).

[86] G. B. Xavier, G. V. de Faria, T. F. da Silva, G. P. Temporão, and J. P. von der Weid. Active polarization control for quantum communication in long-distance optical fibers with shared telecom traffic. Microwave and Optical Technology Letters **53** (2011), 2661–2665 (cit. on p. 14).

[87] D.-D. Li *et al.* Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback. Opt. Express **26** (2018), 22793–22800 (cit. on p. 14).

[88] F. Mitschke. Fiber Optics - Physics and Technology. 2nd ed. DOI: 10.1007/978-3-662-52764-1. Springer Nature 2016 (cit. on p. 16).

[89] S. J. Orfanidis. Electromagnetic Waves and Antennas. Online Book. Last accessed Sep. 26 2023, https://www.ece.rutgers.edu/~orfanidi/ewa/. 2016 (cit. on p. 17).

[90] H. Xia, C. Wang, S. Blais, and J. Yao. Ultrafast and Precise Interrogation of Fiber Bragg Grating Sensor Based on Wavelength-to-Time Mapping Incorporating Higher Order Dispersion. J. Lightwave Technol. **28** (2010), 254–261 (cit. on pp. 17, 18).

[91] A. Andrianov, A. Szabo, A. Sergeev, A. Kim, V. Chvykov, and M. Kalashnikov. Computationally efficient method for Fourier transform of highly chirped pulses for laser and parametric amplifier modeling. Opt. Express **24** (2016), 25974–25982 (cit. on pp. 17, 18, 210).

[92] V. Torres-Company, D. E. Leaird, and A. M. Weiner. Dispersion requirements in coherent frequency-to-time mapping. Opt. Express **19** (2011), 24718–24729 (cit. on p. 18).

[93] M. A. Muriel, J. Azaña, and A. Carballar. Real-time Fourier transformer based on fiber gratings. Opt. Lett. **24** (1999), 1–3 (cit. on p. 18).

[94] Y. Dai, J. Li, Z. Zhang, F. Yin, W. Li, and K. Xu. Real-time frequency-to-time mapping based on spectrally-discrete chromatic dispersion. Opt. Express **25** (2017), 16660–16671 (cit. on p. 18).

[95] A. Khodadad Kashi, L. Sader, R. Haldar, B. Wetzel, and M. Kues. Frequency-to-Time Mapping Technique for Direct Spectral Characterization of Biphoton States From Pulsed Spontaneous Parametric Processes. Frontiers in Photonics **3** (2022) (cit. on pp. 18, 51).

[96] L. Gruner-Nielsen, M. Wandel, P. Kristensen, C. Jorgensen, L. Jorgensen, B. Edvold, B. Palsdottir, and D. Jakobsen. Dispersion-compensating fibers. Journal of Lightwave Technology **23** (2005), 3566–3579 (cit. on p. 18).

[97] C. Shannon. Communication in the Presence of Noise. Proceedings of the IRE **37** (1949), 10–21 (cit. on p. 18).

[98] Z.-Y. J. Ou. Multi-Photon Quantum Interference. 1st ed. DOI: 10.1007/978-0-387-25554-5. Springer Science & Business Media 2007 (cit. on pp. 19, 21–23, 47, 48, 199).

[99] C. Gerry and P. Knight. Introductory Quantum Optics. DOI: 10.1017/CBO9780511791239. Cambridge University Press 2004 (cit. on p. 20).

[100] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi. Quantum information with Gaussian states. Physics Reports **448** (2007), 1–111 (cit. on pp. 20, 126, 130–132).

[101] M. Takeoka, R.-B. Jin, and M. Sasaki. Full analysis of multi-photon pair effects in spontaneous parametric down conversion based photonic quantum information processing. New Journal of Physics **17** (2015), 043030 (cit. on pp. 20, 126, 130–132, 137, 143, 144, 160, 169, 170, 207, 208).

[102] V. Scarani, H. de Riedmatten, I. Marcikic, H. Zbinden, and N. Gisin. Four-photon correction in two-photon Bell experiments. The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics **32** (2005), 129–138 (cit. on pp. 20, 155).

[103] R. Loudon. The Quantum Theory of Light. 3rd ed. Oxford University Press 2000 (cit. on p. 21).

[104] B. Brecht, D. V. Reddy, C. Silberhorn, and M. G. Raymer. Photon Temporal Modes: A Complete Framework for Quantum Information Science. Phys. Rev. X **5** (2015), 041017 (cit. on p. 21).

[105] N. Quesada and J. E. Sipe. Effects of time ordering in quantum nonlinear optics. Phys. Rev. A **90** (2014), 063840 (cit. on p. 21).

[106] S. Helmfrid and G. Arvidsson. Influence of randomly varying domain lengths and nonuniform effective index on second-harmonic generation in quasi-phase-matching waveguides. J. Opt. Soc. Am. B **8** (1991), 797–804 (cit. on pp. 23, 52).

[107] D. Chang, C. Langrock, Y.-W. Lin, C. R. Phillips, C. V. Bennett, and M. M. Fejer. Complex-transfer-function analysis of optical-frequency converters. Opt. Lett. **39** (2014), 5106–5109 (cit. on pp. 23, 52).

[108] M. Santandrea, M. Stefszky, and C. Silberhorn. General framework for the analysis of imperfections in nonlinear systems. Opt. Lett. **44** (2019), 5398–5401 (cit. on pp. 23, 52).

[109] J. W. Goodman. Statistical Optics. Wiley 1985 (cit. on p. 23).

[110] W. Grice, R. Bennink, D. Earl, P. Evans, T. Humble, R. Pooser, J. Schaake, and B. Williams. Multi-client quantum key distribution using wavelength division multiplexing. In: Quantum Communications and Quantum Imaging IX. Ed. by R. E. Meyers, Y. Shih, and K. S. Deacon. Vol. 8163. DOI: 10.1117/12.893788. International Society for Optics and Photonics. SPIE 2011, 89–95 (cit. on p. 27).

[111] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin. An entanglement-based wavelength-multiplexed quantum communication network. Nature **564** (2018), 225–228 (cit. on pp. 27, 89).

[112] W.-T. Fang, Y.-H. Li, Z.-Y. Zhou, L.-X. Xu, G.-C. Guo, and B.-S. Shi. On-chip generation of time-and wavelength-division multiplexed multiple time-bin entanglement. Opt. Express **26** (2018), 12912–12921 (cit. on pp. 27, 54, 89, 95).

[113] I. Herbauts, B. Blauensteiner, A. Poppe, T. Jennewein, and H. Hübel. Demonstration of active routing of entanglement in a multi-user network. Opt. Express **21** (2013), 29013–29024 (cit. on p. 27).

[114] E. Y. Zhu, C. Corbari, A. Gladyshev, P. G. Kazansky, H.-K. Lo, and L. Qian. Toward a reconfigurable quantum network enabled by a broadband entangled source. J. Opt. Soc. Am. B **36** (2019), B1–B6 (cit. on p. 27).

[115] N. B. Lingaraju, H.-H. Lu, S. Seshadri, D. E. Leaird, A. M. Weiner, and J. M. Lukens. Adaptive bandwidth management for entanglement distribution in quantum networks. Optica **8** (2021), 329–332 (cit. on p. 27).

[116] J.-H. Kim, J.-W. Chae, Y.-C. Jeong, and Y.-H. Kim. Quantum communication with time-bin entanglement over a wavelength-multiplexed fiber network. APL Photonics **7** (2022). 016106 (cit. on pp. 28, 191).

[117] W. Wen, Z. Chen, L. Lu, W. Yan, W. Xue, P. Zhang, Y. Lu, S. Zhu, and X.-s. Ma. Realizing an Entanglement-Based Multiuser Quantum Network with Integrated Photonics. Phys. Rev. Appl. **18** (2022), 024059 (cit. on pp. 28, 54, 95, 103, 105).

[118] X. Liu *et al.* 40-user fully connected entanglement-based quantum key distribution network without trusted node. PhotoniX **3** (2022), 2 (cit. on pp. 28, 89, 95).

[119] C. Lee *et al.* Entanglement-based quantum communication secured by nonlocal dispersion cancellation. Phys. Rev. A **90** (2014), 062331 (cit. on pp. 28, 154).

[120] X. Liu *et al.* An entanglement-based quantum network based on symmetric dispersive optics quantum key distribution. APL Photonics **5** (2020). 076104 (cit. on p. 28).

[121] J. Liu, Z. Lin, D. Liu, X. Feng, F. Liu, K. Cui, Y. Huang, and W. Zhang. High-dimensional quantum key distribution using energy-time entanglement over 242 km partially deployed fiber. Quantum Sci. Technol. (2023). in press (cit. on p. 28).

[122] S. Gilbert, W. Swann, and C. Wang. Hydrogen cyanide $H^{13}C^{14}N$ absorption reference for 1530 nm to 1565 nm wavelength calibration - SRM 2519a. Special Publication (NIST SP). DOI: 10.6028/NIST.SP.260-137. 2005 (cit. on p. 32).

[123] M. Fiorentino, S. M. Spillane, R. G. Beausoleil, T. D. Roberts, P. Battle, and M. W. Munro. Spontaneous parametric down-conversion in periodically poled KTP waveguides and bulk crystals. Opt. Express **15** (2007), 7479–7488 (cit. on p. 42).

[124] O. Gayer, Z. Sacks, E. Galun, and A. Arie. Temperature and wavelength dependent refractive index equations for MgO-doped congruent and stoichiometric $LiNbO_3$. Applied Physics B **91** (2008), 343–348 (cit. on pp. 47, 48).

[125] M. Avenhaus, A. Eckstein, P. J. Mosley, and C. Silberhorn. Fiber-assisted single-photon spectrograph. Opt. Lett. **34** (2009), 2873–2875 (cit. on p. 51).

[126] A. O. C. Davis, P. M. Saulnier, M. Karpiski, and B. J. Smith. Pulsed single-photon spectrometer by frequency-to-time mapping using chirped fiber Bragg gratings. Opt. Express **25** (2017), 12804–12811 (cit. on p. 51).

[127] A. C. Gray, S. A. Berry, L. G. Carpenter, J. C. Gates, P. G. R. Smith, and C. B. E. Gawith. Investigation of PPLN Waveguide Uniformity via Second Harmonic Generation Spectra. IEEE Photonics Technology Letters **32** (2020), 63–66 (cit. on pp. 52, 53).

[128] A. Thomas. Photon pair sources in periodically poled Ti:LiNbO$_3$ waveguides. Last accessed Sep. 26 2023, https://nbn-resolving.org/urn:nbn:de:hbz:466:2-8517. PhD thesis. 2011 (cit. on p. 52).

[129] M. Martinelli. A universal compensator for polarization changes induced by birefringence on a retracing beam. Optics Communications **72** (1989), 341–344 (cit. on p. 54).

[130] V. Secondi, F. Sciarrino, and F. De Martini. Quantum spin-flipping by the Faraday mirror. Phys. Rev. A **70** (2004), 040301 (cit. on p. 54).

[131] R. Bhandari. A useful generalization of the Martinelli effect. Optics Communications **88** (1992), 1–5 (cit. on p. 54).

[132] M. Martinelli, P. Martelli, and A. Fasiello. A universal compensator for polarization changes induced by non-reciprocal circular birefringence on a retracing beam. Optics Communications **366** (2016), 119–121 (cit. on p. 54).

[133] A. Boaron *et al.* Secure Quantum Key Distribution over 421 km of Optical Fiber. Phys. Rev. Lett. **121** (2018), 190502 (cit. on pp. 54, 62, 191).

[134] R. Slavík, G. Marra, E. N. Fokoua, N. Baddela, N. V. Wheeler, M. Petrovich, F. Poletti, and D. J. Richardson. Ultralow thermal sensitivity of phase and propagation delay in hollow core optical fibres. Scientific Reports **5** (2015), 15447 (cit. on p. 62).

[135] M. Bousonville, M. Czwalinna, M. Felber, T. Ladwig, H. Schlarb, S. Schulz, C. Sydlo, P. Kownacki, and S. Jablonski. New Phase Stable Optical Fiber. In: Proceedings of Beam Instrumentation Workshop. Last accessed Sep. 26 2023, https://accelconf.web.cern.ch/BIW2012/papers/mopg033.pdf. 2012 (cit. on p. 62).

[136] A. H. Hartog, A. J. Conduit, and D. N. Payne. Variation of pulse delay with stress and temperature in jacketed and unjacketed optical fibres. Optical and Quantum Electronics **11** (1979), 265–273 (cit. on p. 62).

[137] M. Elezov, M. Scherbatenko, D. Sych, and G. Goltsman. Active and passive phase stabilization for the all-fiber Michelson interferometer. Journal of Physics: Conference Series **1124** (2018), 051014 (cit. on p. 62).

[138] P. Toliver, J. M. Dailey, A. Agarwal, and N. A. Peters. Continuously active interferometer stabilization and control for time-bin entanglement distribution. Opt. Express **23** (2015), 4135–4143 (cit. on pp. 62, 63).

[139] J. Smoot. arcTEC Structure - Improved Performance and Life Span in Peltier Modules. CUI Devices - Online Product Information. Last accessed Sep. 26 2023, https://www.cuidevices.com/blog/arctec-structure-improved-performance-and-longer-life-in-peltier-modules. 2010 (cit. on p. 65).

[140] D. Mills. Internet time synchronization: the network time protocol. IEEE Transactions on Communications **39** (1991), 1482–1493 (cit. on p. 68).

[141] J. C. Bienfang *et al.* Quantum key distribution with 1.25 Gbps clock synchronization. Opt. Express **12** (2004), 2011–2016 (cit. on p. 68).

[142] A. Tanaka *et al.* Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization. Opt. Express **16** (2008), 11354–11360 (cit. on p. 68).

[143] J. Williams, M. Suchara, T. Zhong, H. Qiao, R. Kettimuthu, and R. Fukumori. Implementation of quantum key distribution and quantum clock synchronization via time bin encoding. In: Quantum Computing, Communication, and Simulation. Ed. by P. R. Hemmer and A. L. Migdall. Vol. 11699. DOI: 10.1117/12.2581862. International Society for Optics and Photonics. SPIE 2021, 16–25 (cit. on p. 68).

[144] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier. Provably secure and high-rate quantum key distribution with time-bin qudits. Science Advances **3** (2017), e1701491 (cit. on p. 68).

[145] N. Walenta *et al.* A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. New Journal of Physics **16** (2014), 013047 (cit. on p. 68).

[146] R. Ursin *et al.* Entanglement-based quantum communication over 144 km. Nature Physics **3** (2007), 481–486 (cit. on p. 68).

[147] T. Scheidl *et al.* Feasibility of 300 km quantum key distribution with entangled states. New Journal of Physics **11** (2009), 085002 (cit. on p. 68).

[148] S. Ecker, B. Liu, J. Handsteiner, M. Fink, D. Rauch, F. Steinlechner, T. Scheidl, A. Zeilinger, and R. Ursin. Strategies for achieving high key rates in satellite-based QKD. npj Quantum Information **7** (2021), 5 (cit. on p. 68).

[149] M. Lipinski, T. Wlostowski, J. Serrano, and P. Alvarez. White rabbit: a PTP application for robust sub-nanosecond synchronization. In: 2011 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication. DOI: 10.1109/ISPCS.2011.6070148. 2011, 25–30 (cit. on p. 68).

[150] M. Lipinski, E. van der Bij, J. Serrano, T. Wlostowski, G. Daniluk, A. Wujek, M. Rizzi, and D. Lampridis. White Rabbit Applications and Enhancements. In: 2018 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS). DOI: 10.1109/ISPCS.2018.8543072. 2018, 1–7 (cit. on p. 68).

[151] K. Sulimany, R. Dudkiewicz, S. Korenblit, H. S. Eisenberg, Y. Bromberg, and M. Ben-Or. Fast and Simple One-Way High-Dimensional Quantum Key Distribution. In: Frontiers in Optics + Laser Science 2021. DOI: 10.1364/FIO.2021.FW1E.3. Optica Publishing Group 2021, FW1E.3 (cit. on p. 68).

[152] M. Alshowkan, P. G. Evans, B. P. Williams, N. S. V. Rao, C. E. Marvinney, Y.-Y. Pai, B. J. Lawrie, N. A. Peters, and J. M. Lukens. Advanced architectures for high-performance quantum networking. J. Opt. Commun. Netw. **14** (2022), 493–499 (cit. on p. 68).

[153] C. Clivati *et al.* Coherent phase transfer for real-world twin-field quantum key distribution. Nature Communications **13** (2022), 157 (cit. on p. 68).

[154] A. Valencia, G. Scarcelli, and Y. Shih. Distant clock synchronization using entangled photon pairs. Applied Physics Letters **85** (2004), 2655–2657 (cit. on p. 68).

[155] C. Ho, A. Lamas-Linares, and C. Kurtsiefer. Clock synchronization by remote detection of correlated photon pairs. New Journal of Physics **11** (2009), 045011 (cit. on pp. 68, 73).

[156] C. Spiess, S. Töpfer, S. Sharma, A. Kr i , M. Cabrejo-Ponce, U. Chandrashekara, N. L. Döll, D. Rieländer, and F. Steinlechner. Clock Synchronization with Correlated Photons. Phys. Rev. Appl. **19** (2023), 054082 (cit. on pp. 68, 73).

[157] C.-Z. Wang, Y. Li, W.-Q. Cai, W.-Y. Liu, S.-K. Liao, and C.-Z. Peng. Synchronization using quantum photons for satellite-to-ground quantum key distribution. Opt. Express **29** (2021), 29595–29603 (cit. on p. 68).

[158] L. Calderaro, A. Stanco, C. Agnesi, M. Avesani, D. Dequal, P. Villoresi, and G. Vallone. Fast and Simple Qubit-Based Synchronization for Quantum Key Distribution. Phys. Rev. Applied **13** (2020), 054041 (cit. on p. 68).

[159] C. Agnesi, M. Avesani, L. Calderaro, A. Stanco, G. Foletto, M. Zahidy, A. Scriminich, F. Vedovato, G. Vallone, and P. Villoresi. Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder. Optica **7** (2020), 284–290 (cit. on p. 68).

[160] W. Riley and D. Howe. Handbook of Frequency Stability Analysis. Special Publication (NIST SP). Last accessed Sep. 26 2023, https://www.nist.gov/publications/handbook-frequency-stability-analysis. 2008 (cit. on p. 70).

[161] International Telecommunication Union - Telecommunication Standardization Sector. ITU-T G.810 - Definitions and terminology for synchronization networks. Recommendation. Last accessed Sep. 26 2023, https://www.itu.int/rec/T-REC-G.810/en. 1996 (cit. on p. 70).

[162] Y. Pelet, G. Sauder, M. Cohen, L. Labonté, O. Alibart, A. Martin, and S. Tanzilli. Operational entanglement-based quantum key distribution over 50 km of field-deployed optical fibers. Phys. Rev. Appl. **20** (2023), 044006 (cit. on pp. 73, 191).

[163] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter. Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. New Journal of Physics **13** (2011), 073024 (cit. on p. 79).

[164] Hubert+Suhner Polatis. Polatis 576 - 576x576 Port Software-defined Optical Circuit Switch. Product Information. Last accessed Sep. 26 2023, https://www.polatis.com/polatis576.asp. 2023 (cit. on p. 85).

[165] Lumentum. TrueFlex Twin 1x35 Wavelength Selective Switch (Twin 1x35 WSS). Online (Jul. 14 2023): https://www.lumentum.com/en/products/trueflex-twin-1x35-wavelength-selective-switch (2023) (cit. on p. 86).

[166] Y.-K. Jiang and A. Tomita. The generation of polarization-entangled photon pairs using periodically poled lithium niobate waveguides in a fibre loop. Journal of Physics B: Atomic, Molecular and Optical Physics **40** (2007), 437 (cit. on p. 91).

[167] S. Arahira, N. Namekata, T. Kishimoto, H. Yaegashi, and S. Inoue. Generation of polarization entangled photon pairs at telecommunication wavelength using cascaded $\chi^{(2)}$ processes in a periodically poled $LiNbO_3$ ridge waveguide. Opt. Express **19** (2011), 16032–16043 (cit. on p. 91).

[168] F. Steinlechner, S. Ramelow, M. Jofre, M. Gilaberte, T. Jennewein, J. P. Torres, M. W. Mitchell, and V. Pruneri. Phase-stable source of polarization-entangled photons in a linear double-pass configuration. Opt. Express **21** (2013), 11943–11951 (cit. on p. 91).

[169] M. CABREJO-PONCE, C. SPIESS, A. L. M. MUNIZ, P. ANCSIN, and F. STEINLECHNER. GHz-pulsed source of entangled photons for reconfigurable quantum networks. Quantum Science and Technology **7** (2022), 045022 (cit. on p. 91).

[170] K. WÖRHOFF, R. G. HEIDEMAN, A. LEINSE, and M. HOEKMAN. TriPleX: a versatile dielectric photonic platform. Advanced Optical Technologies **4** (2015), 189–207 (cit. on pp. 95, 98).

[171] J. KLAMKIN, H. ZHAO, B. SONG, Y. LIU, B. ISAAC, S. PINNA, F. SANG, and L. COLDREN. Indium Phosphide Photonic Integrated Circuits: Technology and Applications. In: 2018 IEEE BiCMOS and Compound Semiconductor Integrated Circuits and Technology Symposium (BCICTS). DOI: 10.1109/BCICTS.2018.8550947. 2018, 8–13 (cit. on p. 95).

[172] F. SAMARA, N. MARING, A. MARTIN, A. S. RAJA, T. J. KIPPENBERG, H. ZBINDEN, and R. THEW. Entanglement swapping between independent and asynchronous integrated photon-pair sources. Quantum Science and Technology **6** (2021), 045024 (cit. on p. 95).

[173] C. REIMER *et al.* Integrated frequency comb source of heralded single photons. Opt. Express **22** (2014), 6535–6546 (cit. on p. 95).

[174] F. SAMARA, A. MARTIN, C. AUTEBERT, M. KARPOV, T. J. KIPPENBERG, H. ZBINDEN, and R. THEW. High-rate photon pairs and sequential Time-Bin entanglement with Si_3N_4 microring resonators. Opt. Express **27** (2019), 19309–19318 (cit. on pp. 95, 101).

[175] C. C. TISON, J. A. STEIDLE, M. L. FANTO, Z. WANG, N. A. MOGENT, A. RIZZO, S. F. PREBLE, and P. M. ALSING. Path to increasing the coincidence efficiency of integrated resonant photon sources. Opt. Express **25** (2017), 33088–33096 (cit. on pp. 96, 99).

[176] C. WU *et al.* Bright photon-pair source based on a silicon dual-Mach-Zehnder microring. Science China Physics, Mechanics & Astronomy **63** (2019), 220362 (cit. on pp. 96, 99, 100).

[177] P. ZHU, Y. LIU, C. WU, S. XUE, X. YU, Q. ZHENG, Y. WANG, X. QIANG, J. WU, and P. XU. Near 100% spectral-purity photons from reconfigurable micro-rings. Chinese Physics B **29** (2020), 114201 (cit. on pp. 96, 99).

[178] R. W. P. DREVER, J. L. HALL, F. V. KOWALSKI, J. HOUGH, G. M. FORD, A. J. MUNLEY, and H. WARD. Laser phase and frequency stabilization using an optical resonator. Applied Physics B **31** (1983), 97–105 (cit. on p. 96).

[179] E. D. Black. An introduction to Pound-Drever-Hall laser frequency stabilization. American Journal of Physics **69** (2001), 79–87 (cit. on p. 96).

[180] J. P. Chambers. High Frequency Pound-Drever-Hall Ring Resonator Optical Sensing. Master's thesis, supervised by Dr. Christi K. Madsen, Texas A & M University, Last accessed Sep. 26 2023, https://core.ac.uk/download/pdf/147131794.pdf (2007) (cit. on p. 97).

[181] L. Neuhaus, R. Metzdorff, S. Chua, T. Jacqmin, T. Briant, A. Heidmann, P.-F. Cohadon, and S. Deléglise. PyRPL (Python Red Pitaya Lockbox) An open-source software package for FPGA-controlled quantum optics experiments. In: 2017 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC). DOI: 10.1109/CLEOE-EQEC.2017.8087380. 2017, 1–1 (cit. on p. 98).

[182] C. G. H. Roeloffzen *et al.* Low-Loss Si_3N_4 TriPleX Optical Waveguides: Technology and Applications Overview. IEEE Journal of Selected Topics in Quantum Electronics **24** (2018), 1–21 (cit. on pp. 98, 99).

[183] X. Zhang, Y. Zhang, C. Xiong, and B. J. Eggleton. Correlated photon pair generation in low-loss double-stripe silicon nitride waveguides. Journal of Optics **18** (2016), 074016 (cit. on p. 98).

[184] C. Xiong *et al.* Compact and reconfigurable silicon nitride time-bin entanglement circuit. Optica **2** (2015), 724–727 (cit. on pp. 99, 106).

[185] X. Zhang, B. A. Bell, A. Mahendra, C. Xiong, P. H. W. Leong, and B. J. Eggleton. Integrated silicon nitride time-bin entanglement circuits. Opt. Lett. **43** (2018), 3469–3472 (cit. on pp. 99, 106).

[186] L. G. Helt, J. E. Sipe, and M. Liscidini. Super spontaneous four-wave mixing in single-channel side-coupled integrated spaced sequence of resonator structures. Opt. Lett. **37** (2012), 4431–4433 (cit. on p. 101).

[187] S. Bahrani, M. Razavi, and J. Salehi. Wavelength Assignment in Hybrid Quantum-Classical Networks. Scientific Reports **8** (2018) (cit. on p. 101).

[188] J. Yang, Q. Zhou, F. Zhao, X. Jiang, B. Howley, M. Wang, and R. T. Chen. Characteristics of optical bandpass filters employing series-cascaded double-ring resonators. Optics Communications **228** (2003), 91–98 (cit. on p. 101).

[189] C. Chaichuay, P. P. Yupapin, and P. Saeung. The serially coupled multiple ring resonator filters and Vernier effect. Optica Applicata **39** (2009). Last accessed Sep. 26 2023, https://opticaapplicata.pwr.edu.pl/article.php?id=2009100175, 175–194 (cit. on p. 101).

[190] S. J. Mason. Feedback Theory-Some Properties of Signal Flow Graphs. Proceedings of the IRE **41** (1953), 1144–1156 (cit. on p. 101).

[191] S. J. Mason. Feedback Theory-Further Properties of Signal Flow Graphs. Proceedings of the IRE **44** (1956), 920–926 (cit. on p. 101).

[192] C. A. Desoer. The Optimum Formula for the Gain of a Flow Graph or a Simple Derivation of Coates' Formula. Proceedings of the IRE **48** (1960), 883–889 (cit. on p. 101).

[193] D. Younger. A simple derivation of Mason's gain formula. Proceedings of the IEEE **51** (1963), 1043–1044 (cit. on p. 101).

[194] R. Orta, P. Savi, R. Tascone, and D. Trinchero. Synthesis of multiple-ring-resonator filters for optical systems. IEEE Photonics Technology Letters **7** (1995), 1447–1449 (cit. on p. 101).

[195] J. K. S. Poon, J. Scheuer, S. Mookherjea, G. T. Paloczi, Y. Huang, and A. Yariv. Matrix analysis of microring coupled-resonator optical waveguides. Opt. Express **12** (2004), 90–103 (cit. on p. 101).

[196] S. L. Jeng, B. H. Lue, and W. H. Chieng. Transfer matrix method for deriving transfer functions of LTI systems. In: Sixth International Conference on Electronics and Information Engineering. Ed. by Q. Zhang. Vol. 9794. DOI: 10.1117/12.2203247. International Society for Optics and Photonics. SPIE 2015, 979439 (cit. on p. 101).

[197] S.-L. Jeng, R. Roy, and W.-H. Chieng. A Matrix Approach for Analyzing Signal Flow Graph. Information **11** (2020) (cit. on p. 101).

[198] S. Gundavarapu *et al.* Sub-hertz fundamental linewidth photonic integrated Brillouin laser. Nature Photonics **13** (2019), 60–67 (cit. on p. 105).

[199] A. Dhakal, P. Wuytens, A. Raza, N. Le Thomas, and R. Baets. Silicon Nitride Background in Nanophotonic Waveguide Enhanced Raman Spectroscopy. Materials **10** (2017) (cit. on p. 105).

[200] W. Lee, P. Muñoz-Galindo, I. Hegeman, Y.-S. Yong, M. Dijkstra, S. M. García-Blanco, and H. L. Offerhaus. Study on multiple waveguide platforms for waveguide integrated Raman spectroscopy. OSA Continuum **3** (2020), 1322–1333 (cit. on p. 105).

[201] M. S. Hai, A. Leinse, T. Veenstra, and O. Liboiron-Ladouceur. A Thermally Tunable 1×4 Channel Wavelength Demultiplexer Designed on a Low-Loss Si_3N_4 Waveguide Platform. Photonics **2** (2015), 1065–1080 (cit. on p. 106).

[202] Lionix International. Photonic Integrated Circuit Packaging and Assembly. Product Information. Last accessed Sep. 26 2023, https://www.lionix-international.com/photonics/pic-technology/assembly-and-packaging-service/. 2023 (cit. on p. 106).

[203] É. Gouzien, B. Fedrici, A. Zavatta, S. Tanzilli, and V. D'Auria. Quantum description of timing jitter for single-photon ON-OFF detectors. Phys. Rev. A **98** (2018), 013833 (cit. on pp. 109, 121–123).

[204] F. Zappa, S. Tisa, A. Tosi, and S. Cova. Principles and features of single-photon avalanche diode arrays. Sensors and Actuators A: Physical **140** (2007), 103–112 (cit. on pp. 111, 114).

[205] A. Patil. Dead time and count loss determination for radiation detection systems in high count rate applications. Last accessed Sep. 26 2023, https://scholarsmine.mst.edu/doctoral_dissertations/2148/. PhD thesis. Missouri University of Science and Technology, 2010 (cit. on p. 113).

[206] A. Luis and L. L. Sánchez-Soto. Complete Characterization of Arbitrary Quantum Measurement Processes. Phys. Rev. Lett. **83** (1999), 3573–3576 (cit. on p. 115).

[207] A. Feito, J. S. Lundeen, H. Coldenstrodt-Ronge, J. Eisert, M. B. Plenio, and I. A. Walmsley. Measuring measurement: theory and practice. New J. Phys. **11** (2009), 093038 (cit. on pp. 115–117, 119).

[208] J. S. Lundeen, A. Feito, H. Coldenstrodt-Ronge, K. L. Pregnell, C. Silberhorn, T. C. Ralph, J. Eisert, M. B. Plenio, and I. A. Walmsley. Tomography of quantum detectors. Nature Physics **5** (2009), 27–30 (cit. on pp. 115–117).

[209] M. A. Nielsen and I. L. Chuang. Quantum Computation and Quantum Information. DOI: 10.1017/CBO9780511976667. Cambridge University Press 2010 (cit. on p. 115).

[210] H. B. Coldenstrodt-Ronge, J. S. Lundeen, K. L. Pregnell, A. Feito, B. J. Smith, W. Mauerer, C. Silberhorn, J. Eisert, M. B. Plenio, and I. A. Walmsley. A proposed testbed for detector tomography. Journal of Modern Optics **56** (2009), 432–441 (cit. on p. 116).

[211] V. D'Auria, N. Lee, T. Amri, C. Fabre, and J. Laurat. Quantum decoherence of single-photon counters. Physical Review Letters **107** (2011), 050504 (cit. on p. 116).

[212] M. K. Akhlaghi, A. H. Majedi, and J. S. Lundeen. Nonlinearity in single photon detection: modeling and quantum tomography. Optics Express **19** (2011), 21305 (cit. on p. 116).

[213] G. Brida, L. Ciavarella, I. P. Degiovanni, M. Genovese, L. Lolli, M. G. Mingolla, F. Piacentini, M. Rajteri, E. Taralli, and M. G. Paris. Quantum characterization of superconducting photon counters. New J. Phys. **14** (2012), 085001 (cit. on p. 116).

[214] C. M. Natarajan, L. Zhang, H. Coldenstrodt-Ronge, G. Donati, S. N. Dorenbos, V. Zwiller, I. A. Walmsley, and R. H. Hadfield. Quantum detector tomography of a time-multiplexed superconducting nanowire single-photon detector at telecom wavelengths. Opt. Express **21** (2013), 893–902 (cit. on p. 116).

[215] J. J. Renema, G. Frucci, Z. Zhou, F. Mattioli, A. Gaggero, R. Leoni, M. J. A. de Dood, A. Fiore, and M. P. van Exter. Modified detector tomography technique applied to a superconducting multiphoton nanodetector. Optics Express **20** (2012), 2806 (cit. on p. 116).

[216] J. J. Renema *et al.* Experimental test of theories of the detection mechanism in a nanowire superconducting single photon detector. Physical Review Letters **112** (2014), 117604 (cit. on p. 116).

[217] M. Endo, T. Sonoyama, M. Matsuyama, F. Okamoto, S. Miki, M. Yabuno, F. China, H. Terai, and A. Furusawa. Quantum detector tomography of a superconducting nanostrip photon-number-resolving detector. Opt. Express **29** (2021), 11728–11738 (cit. on p. 116).

[218] L. Zhang, H. B. Coldenstrodt-Ronge, A. Datta, G. Puentes, J. S. Lundeen, X.-M. Jin, B. J. Smith, M. B. Plenio, and I. A. Walmsley. Mapping coherence in measurement via full quantum tomography of a hybrid optical detector. Nature Photonics **6** (2012), 364–368 (cit. on p. 116).

[219] S. Grandi, A. Zavatta, M. Bellini, and M. G. A. Paris. Experimental quantum tomography of a homodyne detector. New J. Phys. **19** (2017), 053015 (cit. on p. 116).

[220] L. Zhang, A. Datta, H. B. Coldenstrodt-Ronge, X.-M. Jin, J. Eisert, M. B. Plenio, and I. A. Walmsley. Recursive quantum detector tomography. New J. Phys. **14** (2012), 115005 (cit. on p. 116).

[221] M. Pereyra. Maximum-a-Posteriori Estimation with Bayesian Confidence Regions. SIAM Journal on Imaging Sciences **10** (2017), 285–302 (cit. on p. 117).

[222] E. Amri, G. Boso, B. Korzh, and H. Zbinden. Temporal jitter in free-running InGaAs/InP single-photon avalanche detectors. Opt. Lett. **41** (2016), 5728–5731 (cit. on p. 124).

[223] H. S. Wilf. Generatingfunctionology. 2nd ed. DOI: 10.1016/C2009-0-02369-1. Elsevier 1994 (cit. on pp. 126, 129, 198).

[224] R. Chattamvelli and R. Shanmugam. Generating Functions in Engineering and the Applied Sciences. DOI: 10.1007/978-3-031-79410-0. Morgan & Claypool Publishers 2019 (cit. on pp. 126–129).

[225] A. Ferraro, S. Olivares, and M. Paris. Gaussian States in Quantum Information. Napoli Series on physics and Astrophysics. Bibliopolis 2005 (cit. on pp. 126, 131, 132, 207).

[226] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd. Gaussian quantum information. Rev. Mod. Phys. **84** (2012), 621–669 (cit. on pp. 126, 130–132).

[227] S. Olivares. Quantum optics in the phase space. The European Physical Journal Special Topics **203** (2012), 3–24 (cit. on pp. 126, 130–132, 207).

[228] G. Adesso, S. Ragy, and A. R. Lee. Continuous Variable Quantum Information: Gaussian States and Beyond. Open Systems & Information Dynamics **21** (2014), 1440001 (cit. on pp. 126, 130–132, 194).

[229] O. F. Thomas, W. McCutcheon, and D. P. S. McCutcheon. A general framework for multimode Gaussian quantum optics and photo-detection: Application to Hong-Ou-Mandel interference with filtered heralded single photon sources. APL Photonics **6** (2021), 040801 (cit. on pp. 126, 137, 140–142, 160, 194).

[230] G. Pólya. Mathematics and Plausible Reasoning, Volume 1: Induction and Analogy in Mathematics. Chapter VI: A More General Statement. DOI: 10.2307/j.ctv14164db.10. Princeton University Press 1954 (cit. on p. 127).

[231] G. Adam. Density Matrix Elements and Moments for Generalized Gaussian State Fields. Journal of Modern Optics **42** (1995), 1311–1328 (cit. on pp. 128, 134).

[232] S. M. Barnett, L. S. Phillips, and D. T. Pegg. Imperfect photodetection as projection onto mixed states. Optics Communications **158** (1998), 45–49 (cit. on p. 128).

[233] S. Barnett and P. M. Radmore. Methods in Theoretical Quantum Optics. Oxford Series in Optical and Imaging Sciences. Oxford University Press 2002 (cit. on pp. 128, 139, 199).

[234] S. M. Barnett, G. Ferenczi, C. R. Gilson, and F. C. Speirits. Statistics of photon-subtracted and photon-added states. Phys. Rev. A **98** (2018), 013809 (cit. on pp. 128, 138).

[235] L. Mandel and E. Wolf. Optical Coherence and Quantum Optics. DOI: 10.1017/CBO9781139644105. Cambridge University Press 1995 (cit. on pp. 128, 132–134, 139, 198, 199).

[236] C. S. Hamilton, R. Kruse, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex. Gaussian Boson Sampling. Phys. Rev. Lett. **119** (2017), 170501 (cit. on pp. 131, 140, 141).

[237] R. Kruse, C. S. Hamilton, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex. Detailed study of Gaussian boson sampling. Phys. Rev. A **100** (2019), 032326 (cit. on pp. 131, 140, 141).

[238] Arvind, B. Dutta, N. Mukunda, and R. Simon. The real symplectic groups in quantum mechanics and optics. Pramana **45** (1995), 471–497 (cit. on p. 132).

[239] C. R. Harris *et al.* Array programming with NumPy. Nature **585** (2020), 357–362 (cit. on p. 132).

[240] L. Mandel. V - Fluctuations of Light Beams. In: ed. by E. Wolf. Vol. 2. Progress in Optics. DOI: 10.1016/S0079-6638(08)70560-2. Elsevier 1963, 181–248 (cit. on p. 132).

[241] P. L. Kelley and W. H. Kleiner. Theory of Electromagnetic Field Measurement and Photoelectron Counting. Phys. Rev. **136** (1964), A316–A334 (cit. on pp. 132, 133).

[242] M. Lax and M. Zwanziger. Exact Photocount Statistics: Lasers near Threshold. Phys. Rev. A **7** (1973), 750–771 (cit. on pp. 132, 133).

[243] D. Walls and G. J. Milburn. Quantum Optics. 2nd ed. DOI: 10.1007/978-3-540-28574-8. Springer 2008 (cit. on pp. 132, 133).

[244] J. K. Nauth. Full time-dependent counting statistics of highly entangled biphoton states. Phys. Rev. A **106** (2022), 053716 (cit. on pp. 133, 153).

[245] J. Perina. Quantum Statistics of Linear and Nonlinear Optical Phenomena. 2nd ed. DOI: 10.1007/978-94-011-2400-3. Springer Science & Business Media 1991 (cit. on pp. 133, 139, 198).

[246] N. Quesada, L. G. Helt, J. Izaac, J. M. Arrazola, R. Shahrokhshahi, C. R. Myers, and K. K. Sabapathy. Simulating realistic non-Gaussian state preparation. Phys. Rev. A **100** (2019), 022341 (cit. on p. 137).

[247] D. Su, C. R. Myers, and K. K. Sabapathy. Conversion of Gaussian states to non-Gaussian states using photon-number-resolving detectors. Phys. Rev. A **100** (2019), 052301 (cit. on p. 138).

[248] Y. I. Bogdanov, K. G. Katamadze, G. V. Avosopiants, L. V. Belinsky, N. A. Bogdanova, A. A. Kalinkin, and S. P. Kulik. Multiphoton subtracted thermal states: Description, preparation, and reconstruction. Phys. Rev. A **96** (2017), 063803 (cit. on p. 138).

[249] A. Griewank and A. Walther. Evaluating Derivatives. Second. DOI: 10.1137/1.9780898717761. Society for Industrial and Applied Mathematics 2008 (cit. on pp. 138, 194).

[250] U. Naumann. The Art of Differentiating Computer Programs - An Introduction to Algorithmic Differentiation. DOI: 10.1137/1.9781611972078. SIAM 2012 (cit. on p. 138).

[251] A. G. Baydin, B. A. Pearlmutter, A. A. Radul, and J. M. Siskind. Automatic Differentiation in Machine Learning: a Survey. Journal of Machine Learning Research **18** (2018), 1–43 (cit. on p. 139).

[252] Martín Abadi *et al.* TensorFlow: Large-Scale Machine Learning on Heterogeneous Systems. Last accessed Sep. 26 2023, https://www.usenix.org/system/files/conference/osdi16/osdi16-abadi.pdf (2015) (cit. on pp. 139, 193).

[253] A. Paszke, S. Gross, S. Chintala, G. Chanan, E. Yang, Z. DeVito, Z. Lin, A. Desmaison, L. Antiga, and A. Lerer. Automatic differentiation in PyTorch. In: Neural Information Processing Systems (NIPS-W). Last accessed Sep. 26 2023, https://openreview.net/forum?id=BJJsrmfCZ. 2017 (cit. on p. 139).

[254] W. Mauerer, M. Avenhaus, W. Helwig, and C. Silberhorn. How colors influence numbers: Photon statistics of parametric down-conversion. Phys. Rev. A **80** (2009), 053815 (cit. on pp. 139, 147, 155, 156).

[255] W. Mauerer. On Colours, Keys, and Correlations: Multimode Parametric Down-conversion in the Photon Number Basis. Last accessed Sep. 26 2023, https://nbn-resolving.org/urn:nbn:de:bvb:29-opus-14638. Doctoral Thesis. Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), 2009 (cit. on pp. 139, 155–159).

[256] A. Bourchtein and L. Bourchtein. Complex Analysis. DOI: 10.1007/978-981-15-9219-5. Springer Singapore 2021 (cit. on p. 140).

[257] J. Abate and W. Whitt. Numerical inversion of probability generating functions. Operations Research Letters **12** (1992), 245–251 (cit. on p. 140).

[258] G. L. Choudhury, D. M. Lucantoni, and W. Whitt. Multidimensional Transform Inversion with Applications to the Transient M/G/1 Queue. The Annals of Applied Probability **4** (1994), 719–740 (cit. on p. 140).

[259] G. L. Choudhury and W. Whitt. Computing distributions and moments in polling models by numerical transform inversion. Performance Evaluation **25** (1996), 267–292 (cit. on p. 140).

[260] G. L. Choudhury and D. M. Lucantoni. Numerical Computation of the Moments of a Probability Distribution from its Transform. Operations Research **44** (1996), 368–381 (cit. on p. 140).

[261] J. Abate and W. Whitt. The Fourier-series method for inverting transforms of probability distributions. Queueing Systems **10** (1992), 5–87 (cit. on p. 140).

[262] V. V. Dodonov, O. V. Man'ko, and V. I. Man'ko. Multidimensional Hermite polynomials and photon distribution for polymode mixed light. Phys. Rev. A **50** (1994), 813–817 (cit. on p. 140).

[263] P. Kok and S. L. Braunstein. Multi-dimensional Hermite polynomials in quantum optics. Journal of Physics A: Mathematical and General **34** (2001), 6185–6195 (cit. on p. 140).

[264] J. Huh. Multimode Bogoliubov transformation and Husimi's Q-function. Journal of Physics: Conference Series **1612** (2020), 012015 (cit. on p. 140).

[265] S. Berkowitz and F. J. Garner. The Calculation of Multidimensional Hermite Polynomials and Gram-Charlier Coefficients. Mathematics of Computation **24** (1970), 537–545 (cit. on p. 140).

[266] G. Cariolaro and G. Pierobon. Fock expansion of multimode pure Gaussian states. Journal of Mathematical Physics **56** (2015), 122109 (cit. on p. 140).

[267] D. S. Phillips, M. Walschaers, J. J. Renema, I. A. Walmsley, N. Treps, and J. Sperling. Benchmarking of Gaussian boson sampling using two-point correlators. Phys. Rev. A **99** (2019), 023836 (cit. on p. 140).

[268] S. Aaronson and A. Arkhipov. The Computational Complexity of Linear Optics. In: Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing. STOC '11. DOI: 10.1145/1993636.1993682. Association for Computing Machinery 2011, 333–342 (cit. on p. 140).

[269] A. P. Lund, A. Laing, S. Rahimi-Keshari, T. Rudolph, J. L. O'Brien, and T. C. Ralph. Boson Sampling from a Gaussian State. Phys. Rev. Lett. **113** (2014), 100502 (cit. on p. 140).

[270] S. Rahimi-Keshari, A. P. Lund, and T. C. Ralph. What Can Quantum Optics Say about Computational Complexity Theory? Phys. Rev. Lett. **114** (2015), 060501 (cit. on p. 140).

[271] N. QUESADA, J. M. ARRAZOLA, and N. KILLORAN. Gaussian boson sampling using threshold detectors. Phys. Rev. A **98** (2018), 062322 (cit. on pp. 140, 141).

[272] N. QUESADA, R. S. CHADWICK, B. A. BELL, J. M. ARRAZOLA, T. VINCENT, H. QI, and R. GARCÍA–PATRÓN. Quadratic Speed-Up for Simulating Gaussian Boson Sampling. PRX Quantum **3** (2022), 010306 (cit. on p. 140).

[273] A. BJÖRKLUND, B. GUPT, and N. QUESADA. A Faster Hafnian Formula for Complex Matrices and Its Benchmarking on a Supercomputer. ACM J. Exp. Algorithmics **24** (2019) (cit. on pp. 140, 141).

[274] J. F. F. BULMER *et al.* The boundary for quantum advantage in Gaussian boson sampling. Science Advances **8** (2022), eabl9236 (cit. on pp. 140, 141).

[275] D. J. BROD, E. F. GALVÃO, A. CRESPI, R. OSELLAME, N. SPAGNOLO, and F. SCIARRINO. Photonic implementation of boson sampling: a review. Advanced Photonics **1** (2019), 1–14 (cit. on p. 140).

[276] H.-S. ZHONG *et al.* Quantum computational advantage using photons. Science **370** (2020), 1460–1463 (cit. on p. 140).

[277] H.-S. ZHONG *et al.* Phase-Programmable Gaussian Boson Sampling Using Stimulated Squeezed Light. Phys. Rev. Lett. **127** (2021), 180502 (cit. on p. 140).

[278] N. QUESADA. Franck-Condon factors by counting perfect matchings of graphs with loops. The Journal of Chemical Physics **150** (2019), 164113 (cit. on p. 141).

[279] J. F. F. BULMER, S. PAESANI, R. S. CHADWICK, and N. QUESADA. Threshold detection statistics of bosonic states. Phys. Rev. A **106** (2022), 043712 (cit. on p. 141).

[280] E. R. CAIANIELLO. On quantum field theory — I: explicit solution of Dyson's equation in electrodynamics without use of feynman graphs. Il Nuovo Cimento (1943-1954) **10** (1953), 1634–1652 (cit. on p. 141).

[281] V. V. KOCHAROVSKY, V. V. KOCHAROVSKY, and S. V. TARASOV. The Hafnian Master Theorem. Linear Algebra and its Applications **651** (2022), 144–161 (cit. on p. 141).

[282] B. GUPT, J. IZAAC, and N. QUESADA. The Walrus: a library for the calculation of hafnians, Hermite polynomials and Gaussian boson sampling. Journal of Open Source Software **4** (2019), 1705 (cit. on p. 141).

[283] Y. CARDIN and N. QUESADA. Photon-number moments and cumulants of Gaussian states. Preprint, Last accessed Dec. 23 2023): https://arxiv.org/pdf/2212.06067.pdf (2022) (cit. on p. 141).

[284] N. LÜTKENHAUS. Security against individual attacks for realistic quantum key distribution. Phys. Rev. A **61** (2000), 052304 (cit. on p. 145).

[285] W. P. Grice and I. A. Walmsley. Spectral information and distinguishability in type-II down-conversion with a broadband pump. Phys. Rev. A **56** (1997), 1627–1634 (cit. on p. 154).

[286] C. K. Law, I. A. Walmsley, and J. H. Eberly. Continuous Frequency Entanglement: Effective Finite Hilbert Space and Entropy Control. Phys. Rev. Lett. **84** (2000), 5304–5307 (cit. on pp. 154–156).

[287] T. E. Keller and M. H. Rubin. Theory of two-photon entanglement for spontaneous parametric down-conversion driven by a narrow pump pulse. Phys. Rev. A **56** (1997), 1534–1541 (cit. on p. 154).

[288] Y. M. Mikhailova, P. A. Volkov, and M. V. Fedorov. Biphoton wave packets in parametric down-conversion: Spectral and temporal structure and degree of entanglement. Phys. Rev. A **78** (2008), 062327 (cit. on p. 154).

[289] K. E. Dorfman, S. Asban, B. Gu, and S. Mukamel. Hong-Ou-Mandel interferometry and spectroscopy using entangled photons. Communications Physics **4** (2021), 49 (cit. on p. 154).

[290] Z. Y. Ou, J.-K. Rhee, and L. J. Wang. Photon bunching and multiphoton interference in parametric down-conversion. Phys. Rev. A **60** (1999), 593–604 (cit. on p. 155).

[291] C. Müller, A. Ahlrichs, and O. Benson. General and complete description of temporal photon correlations in cavity-enhanced spontaneous parametric down-conversion. Phys. Rev. A **102** (2020), 053504 (cit. on p. 155).

[292] S. Parker, S. Bose, and M. B. Plenio. Entanglement quantification and purification in continuous-variable systems. Phys. Rev. A **61** (2000), 032305 (cit. on pp. 155, 156).

[293] E. Schmidt. Zur Theorie der linearen und nichtlinearen Integralgleichungen. Mathematische Annalen **63** (1907), 433–476 (cit. on pp. 156, 173).

[294] L. Lamata and J. León. Dealing with entanglement of continuous variables: Schmidt decomposition with discrete sets of orthogonal functions. Journal of Optics B: Quantum and Semiclassical Optics **7** (2005), 224 (cit. on pp. 156, 159).

[295] A. Y. Bogdanov, Y. I. Bogdanov, and K. A. Valiev. Schmidt modes and entanglement in continuous-variable quantum systems. Russian Microelectronics **35** (2006), 7–20 (cit. on p. 156).

[296] L. N. Trefethen and D. Bau III. Numerical Linear Algebra. DOI: 10.1137/1.9780898719574. SIAM 1997 (cit. on pp. 156, 194, 214).

[297] D. B. Horoshko, L. La Volpe, F. Arzani, N. Treps, C. Fabre, and M. I. Kolobov. Bloch-Messiah reduction for twin beams of light. Phys. Rev. A **100** (2019), 013837 (cit. on p. 157).

[298] R. M. Larsen. PROPACK homepage. Last accessed Sep. 26 2023, http://sun.stanford.edu/~rmunk/PROPACK/ (2012) (cit. on p. 159).

[299] B. V. Rajarama Bhat, T. C. John, and R. Srinivasan. Infinite mode quantum Gaussian states. Reviews in Mathematical Physics **31** (2019), 1950030 (cit. on p. 161).

[300] I. Gohberg, S. Goldberg, and N. Krupnik. Traces and Determinants of Linear Operators. DOI: 10.1007/978-3-0348-8401-3. Springer Basel AG, Birkenhäuser Verlag 2000 (cit. on pp. 166, 171, 174).

[301] J. B. Conway. A Course in Operator Theory. DOI: 10.1090/gsm/021. American Mathematical Soc. 2000 (cit. on p. 166).

[302] C. Pozrikidis. An Introduction to Grids, Graphs, and Networks. Oxford University Press 2014 (cit. on p. 171).

[303] J. M. Steele. The Cauchy-Schwarz Master Class: An Introduction to the Art of Mathematical Inequalities. DOI: 10.1017/CBO9780511817106. Cambridge University Press 2004 (cit. on p. 174).

[304] F. Bornemann. On the numerical evaluation of Fredholm determinants. Mathematics of Computation **79** (2010), 871–915 (cit. on p. 174).

[305] D. Werner. Funktionalanalysis. 8th ed. DOI: 10.1007/978-3-662-55407-4. Springer Spektrum 2018 (cit. on p. 175).

[306] S. Loukas and C. D. Kemp. The Index of Dispersion Test for the Bivariate Poisson Distribution. Biometrics **42** (1986), 941–948 (cit. on p. 177).

[307] K. Kawamura. The structure of bivariate poisson distribution. Kodai Mathematical Seminar Reports **25** (1973), 246–256 (cit. on p. 177).

[308] P. Acheva, K. Zaitsev, V. Zavodilenko, A. Losev, A. Huang, and V. Makarov. Automated verification of countermeasure against detector-control attack in quantum key distribution. EPJ Quantum Technology **10** (2023), 22 (cit. on p. 190).

[309] ID Quantique SA. ID281 Superconducting nanowire series. Product Brochure. 2023 (cit. on p. 190).

[310] W. Tittel, H. Zbinden, and N. Gisin. Experimental demonstration of quantum secret sharing. Phys. Rev. A **63** (2001), 042301 (cit. on p. 191).

[311] G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden. Long-distance entanglement-based quantum key distribution. Phys. Rev. A **63** (2000), 012309 (cit. on p. 191).

[312] S. Euler. Erzeugung und Charakterisierung von Einzelphotonen aus PDC in PPKTP für Anwendungen in der Quanteninformation. Last accessed Sep. 26 2023, https://nbn-resolving.org/urn:nbn:de:tuda-tuprints-71838. PhD thesis. Darmstadt, 2017 (cit. on p. 192).

[313] P. M. Notz, O. Nikiforov, and T. Walther. Software bundle for data post-processing in a quantum key distribution experiment. Technical Report. DOI: 10.25534/tuprints-00014042. Technische Universität Darmstadt, 2020 (cit. on p. 192).

[314] Oleg Nikiforov. qkd-tools. GitLab project. Last accessed Sep. 26 2023, https://git.rwth-aachen.de/oleg.nikiforov/qkd-tools. 2021 (cit. on p. 192).

[315] R. Frostig, M. Johnson, and C. Leary. Compiling machine learning programs via high-level tracing. Systems for Machine LearningConference, https://mlsys.org/Conferences/doc/2018/146.pdf (2018) (cit. on p. 193).

[316] J. Bettencourt, M. J. Johnson, and D. Duvenaud. Taylor-Mode Automatic Differentiation for Higher-Order Derivatives in JAX. In: Program Transformations for ML Workshop at NeurIPS 2019. Last accessed Sep. 26 2023, https://openreview.net/forum?id=SkxEF3FNPH. 2019 (cit. on pp. 193, 194).

[317] S. Walter. Structured higher-order algorithmic differentiation in the forward and reverse mode with application in optimum experimental design. DOI: 10.18452/16514. PhD thesis. Humboldt-Universität zu Berlin, Mathematisch-Naturwissenschaftliche Fakultät II, 2012 (cit. on p. 194).

[318] S. F. Walter and L. Lehmann. Algorithmic differentiation in Python with AlgoPy. Journal of Computational Science **4** (2013), 334–344 (cit. on p. 194).

[319] J. Magnus and H. Neudecker. Matrix Differential Calculus with Applications in Statistics and Econometrics. 3rd ed. DOI: 10.1002/9781119541219. John Wiley & Sons Ltd 2019 (cit. on p. 194).

[320] A. Zee. Quantum Field Theory in a Nutshell. 2nd ed. Princeton University Press 2010 (cit. on p. 197).

[321] H. T. C. Stoof, D. B. M. Dickerscheid, and K. Gubbels. Ultracold Quantum Fields. DOI: 10.1007/978-1-4020-8763-9. Springer Science & Business Media 2009 (cit. on p. 197).

[322] W. P. Schleich. Quantum Optics in Phase Space. 1st ed. DOI: 10.1002/3527602976. Wiley 2001 (cit. on p. 199).

[323] M. M. Hayat, S. N. Torres, and L. M. Pedrotti. Theory of photon coincidence statistics in photon-correlated beams. Optics Communications **169** (1999), 275–287 (cit. on p. 201).