

**ROBUSTNESS BOUNDS
AND PRACTICAL LIMITATIONS
OF QUANTUM KEY DISTRIBUTION**

Vom Fachbereich Physik
der Technischen Universität Darmstadt
zur Erlangung des Grades
eines Doktors der Naturwissenschaften
(Dr. rer. nat.)

genehmigte

DISSERTATION

von

Aeysha Khaliq, M. Phil.
aus Sargodha (Pakistan)

Darmstadt 2008

D17

Referent: Prof. Dr. Barbara Drossel
Korreferent: Prof. Dr. Robert Roth
Tag der Einreichung: 31.7.2007
Tag der Mündlichen Prüfung: 25.6.2008

*To
US and Our Family*

Scientific thoughts are common heritage of mankind

Abdus Salam

Verily in the heavens and the earth, are Signs for those who believe. And in the creation of yourselves and the fact that animals are scattered (through the earth), are Signs for those of assured Faith. And in the alternation of Night and Day, and the fact that Allah sends down Sustenance from the sky, and revives therewith the earth after its death, and in the change of the winds,- are Signs for those that are wise.

Al-Quran 45:3-5

Abstract

Quantum information theory is a modern branch of theoretical physics. One of its main goals is to interpret concepts of quantum physics. This leads to a deeper understanding of quantum theory. The most common examples of practical applications of basic quantum theory are quantum computation and quantum cryptography. Quantum cryptography provides secure communication between legitimate users even in the presence of an adversary by making possible the distribution of a secret key. It then allows error correction and privacy amplification, which is elimination of adversary information, through classical communication.

In this thesis two important aspects of quantum key distribution are covered, namely robustness bounds with respect to provable entanglement for ideal protocols and practical quantum key distribution using two-way classical communication.

In part one of the thesis, ideal quantum key distribution protocols and their robustness in terms of provable entanglement are discussed. The robustness bounds are proved for most general coherent attacks. These bounds for provable entanglement are already known to be 25% for the four-state protocol and 33% for the six-state protocol. We anticipate to provide a region in which the legitimate users share entanglement. This region is large for the four-state protocol and is reduced to a smaller region for the six-state protocol because of additional constraint on it. We also investigate the information cost which the adversary has to pay in order to reach these bounds.

In part two we adopt a more practical approach. We investigate the limitation on distance of secure communication because of practical restrictions. In particular we investigate the restrictions due to the lack of single photon sources, the lossy channel and faulty detectors. These practical limitations have already been observed using one-way classical communication between legitimate users. It has been observed that it is actually the dark count rate that limit the distance up to which legitimate users can share a secret key. We have used two-way classical communication to postpone the effect of dark counts and increase the distance to considerable amount. For the purpose

we have considered an optimal attack with respect to the disturbance that an eavesdropper creates while attacking. Any other format of attacking will increase the disturbance. We show that using two-way classical communication for post processing we can increase the distance of secure communication considerably.

Zusammenfassung

Die Quanteninformationstheorie ist ein moderner Zweig der theoretischen Physik. Eines ihrer Hauptziele ist es, die Konzepte der Quantenphysik zu interpretieren. Dies führt zu einem tieferen Verständnis der Quantentheorie. Die bekanntesten Beispiele von praktischen Anwendungen der Quantentheorie sind Quantenrechnen und Quantenkryptographie. Die Quantenkryptographie erlaubt sichere Kommunikation zwischen berechtigten Nutzern auch in Gegenwart eines Angreifers durch Ermöglichung des Austausches eines sicheren Schlüssels. Sie ermöglicht ferner die Fehlerkorrektur und die *privacy amplification*, also die Reduktion der Information des Angreifers, durch klassische Kommunikation.

In dieser Arbeit werden zwei wichtige Aspekte des Quanten-Schlüsselaustausches behandelt, nämlich Robustheitsschranken in Bezug auf beweisbare Verschränkung für ideale Protokolle und praktischer Quanten-Schlüsselaustausch unter Verwendung klassischer Zweiweg-Kommunikation.

Im ersten Teil dieser Arbeit werden ideale Protokolle für den Quanten-Schlüsselaustausch und ihre Robustheit in Bezug auf beweisbare Verschränkung besprochen. Die Robustheitsschranken werden für die allgemeinstmöglichen kohärenten Angriffe bewiesen. Diese Schranken für beweisbare Sicherheit sind 25% für das Vier-Zustands-Protokoll und 33% für das Sechs-Zustands-Protokoll. Wir ermitteln einen Bereich, in dem die berechtigten Nutzer verschränkte Zustände teilen. Dieser Bereich reduziert sich wegen zusätzlicher Einschränkungen auf eine Linie für das Sechs-Zustands-Protokoll. Wir untersuchen die Informationsmenge, die der Angreifer aufgeben muß, um diese Schranken zu erreichen.

Im zweiten Teil wählen wir einen stärker praxisorientierten Zugang. Wir untersuchen die Distanz-Beschränkungen der sicheren Kommunikation unter praktischen Einschränkungen. Insbesondere untersuchen wir die Einschränkungen, die sich durch das Fehlen von Einzelphoton-Quellen, durch verlustbehaftete Kanäle und durch fehlerhafte Detektoren ergeben. Diese praktischen Beschränkungen wurden bereits für Protokolle untersucht, die klassische Einweg-Kommunikation zwischen den berechtigten Nutzern verwen-

den. Es wurde festgestellt, dass es vor allem die Dunkelzählrate ist, die die Distanz beschränkt, bis zu der die berechtigten Nutzer sich einen geheimen Schlüssel teilen können. Wir verwenden Zweiweg-Kommunikation, um die Auswirkungen der Dunkelzählrate hinauszuzögern und die Distanz wesentlich zu vergrößern. Zu diesem Zweck haben wir einen in Bezug auf die durch den Lauscher verursachte Störung optimierten Angriff betrachtet. Jede andere Art eines Angriffs würde die Störung erhöhen. Wir zeigen, dass durch Verwendung der Zweiweg-Kommunikation für die klassische Weiterverarbeitung der Bits die Distanz für sichere Kommunikation wesentlich erhöht werden kann.

Contents

1	Introduction	11
1.1	Secret-key cryptography	12
1.2	Public-key cryptography	15
1.3	Quantum cryptography	16
1.4	Thesis outline	18
2	Quantum Key Distribution (QKD) Protocols and Secure Key Rates	19
2.1	Basic quantum features vital in quantum key distribution . . .	19
2.2	Quantum key distribution protocols	22
2.2.1	Prepare and measure four- and six-state protocols . . .	22
2.2.2	Error correction and privacy amplification	25
2.2.3	Entanglement-based protocols	28
2.2.4	Equivalence between prepare and measure and the corresponding entanglement based protocols	29
2.3	Security of QKD protocols	30
2.3.1	Various attacks on ideal protocols	31
2.3.2	Security bounds based on various attacks	32
3	Bounds on Performance of QKD Protocols	39
3.1	Provable entanglement and threshold disturbances	40
3.1.1	Four-state protocol	40
3.1.2	Six-state protocol	46
3.2	The price of disentanglement	48
3.2.1	Four-state protocol	48
3.2.2	Six-state protocol	52
3.3	Entanglement and intrinsic information	54

4	Practical Quantum Key Distribution	57
4.1	Practical limitations and their fatalities in QKD	58
4.1.1	A model for imperfections	60
4.2	Limitations of one-way post processing	63
4.3	Practical QKD with two-way classical communication	66
4.3.1	An Optimal Eavesdropping strategy	66
4.3.2	Error rejection using two-way post processing	69
4.3.3	Numerical simulations and discussion	72
5	Concluding Remarks	83
A	Numerical Program for Practical QKD	87
	Bibliography	95
	Acknowledgement	100
	Curriculum Vitae	102

Chapter 1

Introduction

History ¹ of cryptography is almost as ancient as that of writing. At all times people have wished to communicate secretly without letting a third party to over hear them. Archeological revelations have shown that various cryptographic methods had been used by ancient civilizations in India, China or Mesopotamia. Ancient Egyptians used modified hieroglyph to conceal their message. Most hieroglyph used during that period were figurative. In the 5th century BC Greeks designed a scytale device based on transposition of letters. A strip of parchment or leather was rotated around a baton across which the message was written. When the end of line was reached the baton was rotated. After the parchment was removed the letters looked scrambled and only a person possessing the baton of same size could recover the message. Another important and easy cipher is the substitution cipher where each letter in a message is substituted by another letter, word or symbol. A good example is the Caesar cipher. Gaius Julius Caesar used this cipher to communicate between Roman ligeons scattered among the Roman empire. In this cipher each letter was advanced by three letters in alphabets i.e. A was replaced by D, B by E, C by F and so on. During the middle ages most ciphers were based on transposition or substitution or a combination thereof. However none of them are secure because it is possible to break them exploiting various characteristics of the language such as frequency of individual letters and their clusters.

The invention of telegraphy in 1830's started the beginning of modern electronic communication between people. From the cryptographic point of view it lacked secrecy as the message was known to the telegraph operator. In order to keep the message secret from the operator, people and companies designed various code books where significant words in the message were re-

¹Most of the information about history of cyptography is taken from [Hen02, Sin01].

placed by small nonsense words. If the code book is kept secret the telegraph becomes a cipher.

In the twentieth century the two world wars accelerated the invention of new cryptosystems. In 1917 Gilbert S. Vernam proposed a very simple secret-key substitution cipher. Though it did not become as widespread as Vernam had expected but it remains to be the only known cipher proven to be unconditionally secure and will be discussed in detail in Sec. 1.1. In 1918, Arthur Scherbius invented an ingenious electric cipher machine, called Enigma, which was patented a year later. The Enigma consisted of a set of rotating wired wheels, which performed a very sophisticated substitution cipher. After various improvements, it was adopted by the German Navy in 1926, the German Army in 1928, and the Air Force in 1935, and it was used by the Germans and Italians throughout World War II. The military Enigma had incredible 159×10^{18} possible settings (cryptographic keys). When some letter was repetitively keyed, the machine always produced a different letter and the sequence started repeating only after 16900 keyings, when the inner mechanism returned to the initial position. The immense number of potential keys led Alan Turing to construct the first electronic computer, which helped break the Enigma ciphers in the course of the War. Thus cryptography (or cryptanalysis to be more precise) was the driving force behind the development of modern computers. Today a Pentium-based computer can unscramble an Enigma-encrypted message within minutes.

1.1 Secret-key cryptography

Until 1970's most cryptographic schemes were based on *secret-key cryptosystems*, where the encrypting and decrypting ciphers were known to everybody but secrecy was ensured by a secret key known only to the legitimate users. These systems are also known as symmetric key cryptosystems as same key is used for encryption and decryption. The distribution of secret key is the main draw back of such systems.

The Vernam cipher

In 1917 Gilbert S. Vernam proposed an unbreakable secret-key cipher, the one time pad or Vernam cipher. It is a special case of substitution cipher where each alphabet of the message was replaced by a random alphabet. This string of random alphabets then forms the secret key which must be known to both sender and recipient. The principle of the cipher is that if random bits are added to the message, the bits of the resulting string are

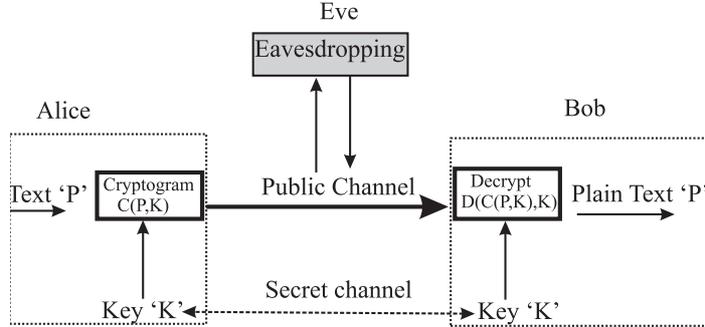


Figure 1.1: Secret key cryptosystem: In order to send plain text 'P', Alice prepares a cipher text $C(P,K)$ using secret key 'K' and plain text 'P' via a publicly known cryptogram. The cipher text is transmitted to Bob through a public channel accessible to Eve. The key 'K' is sent through secret channel to Bob. Bob decrypts the message using the secret key 'K' in a cryptogram based on knowledge of Alice's cryptogram and gets the plain text 'P'.

also random and carry no information. For a binary logic, unlike Vernam who used 26-letter alphabet, the encryption algorithm can be written as

$$C_K(M) = (c_1 = m_1 \oplus k_1, c_2 = m_2 \oplus k_2, \dots, c_n = m_n \oplus k_n), \quad (1.1)$$

where $M = (m_1, m_2, \dots, m_n)$ is the message and $K = (k_1, k_2, \dots, k_n)$ is the random key and \oplus is addition modulo 2 or exclusive OR without carry. Since addition modulo 2 is identity, therefore decryption can be done by adding the same key as

$$M = D_k(C) = (c_1 \oplus k_1, c_2 \oplus k_2, \dots, c_n \oplus k_n). \quad (1.2)$$

For the cipher to be secure, the key K must satisfy three conditions: (1) It should be as long as the message, (2) it must be purely random and (3) it must be used only once. The last condition gives the name *one-time pad* to the cipher. Claude E. Shannon in 1949 proved that under above conditions the Vernam cipher is unconditionally secure i.e. impossible to break by any computational means.

Security of Vernam cipher

A simple proof of security of Vernam cipher can be given by probability theory [Ran05]. Let M , K and C be random variables for the plain text, key

and the cipher text, respectively. Eve receives the cipher text and tries to extract the plain text from it, one finds that

$$P(M = m_i | C = c_i) = \frac{P(M = m_i \wedge C = c_i)}{P(C = c_i)} = P(M = m_i). \quad (1.3)$$

Eve has no knowledge about the key, therefore the probability that $P(K = k_i) = d^{-n}$ where d is an exponential number and n is the length of the key (and hence message). Therefore $P(C = c_i) = d^{-n}$ for Eve (by a perfect realization $M = m_i$), because the encryption function is bisection on sum of all. C is now statistically independent of M , so the second equality is justified.

Thus by intercepting the cipher text, due to the ignorance of key, Eve gets no additional information than she a priori already has. Something more formal can be deduced, that due to statistical independence of C and M , the mutual information $I(M : C) = 0$.

Despite its unconditional security, the Vernam cipher faces the problem how to securely distribute the key. This prevented it from being widely used. However, it was used for various military and diplomatic purposes, where the security outweighs the key management problem. It had been used by the infamous spies Theodore A. Hall, Klaus Fuchs, the Rosenbergs and others, who were passing atomic secrets to Moscow. Ché Guevara also encrypted his messages to Fidel Castro by means of the one-time pad. It was employed in securing the hot line between Washington and Moscow and it is said to be used for communications between nuclear submarines and for some embassy communications. However it led to the revelations of atomic spies in WWII because of the repetitive use of the key incorrectly prepared by the KGB.

Digital Encryption Standard

The most spread cryptosystem is the *Digital Encryption Standard* or DES and its variations. It was developed in 1975 by IBM and US government. It employs very simple arithmetic operations and hence can be easily implemented into hardware. The algorithm uses a 56-bit key which is then reused to encrypt the entire message, therefore it is only computationally secure. In 1997, RSA Data Security inc, published their first results to unscramble the entire message encrypted by DES. They apply brute force to search the entire space of 2^{56} possible keys to search the key on large number of computers. It took them 96 days to break it. However a DES search machine designed by Micheal Wiener in 1993 based on 1997's technology, would break DES in 3.5 hours [Wie97]. The same machine based on 2000's technology would take only 100 seconds. Cryptographers have then tried to improve the security of

DES by developing modifications to it, namely Triple DES, DESX and more. Since 2002, a new standard, the Advanced Encryption Standard (AES) has replaced the aging DES. However, with the advancement in computation it is not going to last long either.

1.2 Public-key cryptography

The advancement in electronic communications prompted the need for more secure ciphers between parties who have never met before. This resulted in the development of public-key cryptosystems, also known as asymmetric-key cryptosystem as separate key is used for encryption and decryption. Public-key cryptography was invented in 1976 by Whitfield Diffie and Martin E. Hellman. Public-key cryptography requires two keys: the public key and the private key, which form a key pair. The recipient of a message generates two keys, makes the public key public through a trusted authority and keeps his private key in a secret place to ensure its private possession. The algorithm is designed in such a way that anyone can encrypt a message using the public key, however, only the legitimate recipient can decrypt the message using his/her private key.

The security of public-key cryptography rests on various computational problems, which are believed to be intractable. The encryption and decryption algorithms utilize the so-called one-way functions. One-way functions are mathematical functions that are easy to compute in one direction, but their inversion is very difficult. It is, for example, very easy to multiply two prime numbers, but to factor the product of two large primes is already a difficult task. Other public-key cryptosystems are based, for example, on the difficulty of the discrete logarithm problem in Abelian groups on elliptic curves or other finite groups. However, it is important to point out that no one-way function has been proved to be one-way. Hence public-key cryptography cannot provide unconditional security. It is only computationally secure.

Today the most widely used public-key system is the RSA cryptosystem. RSA was invented in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman [RSA78], whose names form the acronym. RSA exploits the difficulty of factoring large numbers. The receiver picks two large primes and makes their product public. This product, called the modulus, becomes the public key. Using this key, anyone can encrypt a message. However, in order to invert the algorithm it is necessary to know the prime factors of the modulus. Although there are several ways to attack the RSA system, the most promising one still seems to be to attempt to factor the modulus.

Various public efforts have been made to attempt to develop fast factoring algorithms. A 512-bit number was factored in August 1999 by 292 computers. In 1999 Adi Shamir proposed the TWINKLE device. It is a massively parallel optoelectronic factoring device and is about three orders of magnitude faster than a conventional fast PC. It can facilitate the factoring of 512- and 768-bit keys. Today it is already recommended to move to longer key lengths and to use key sizes of 1024 bits for corporate use and 2048 bits for valuable keys.

Another threat to the security of public-key cryptosystems is the development of quantum computers. The decryption using a quantum computer would take about the same time as the encryption, thereby making public-key cryptography worthless. Shor, in 1994 has already suggested an algorithm capable of doing so [Sho94] and first experiments with small-scale quantum computers [VS⁺01] successfully pave the way to more sophisticated devices.

1.3 Quantum cryptography

All conventional classical cryptographic techniques fail to assure unconditional security. The security of conventional techniques relies on the assumption of limited advancement of mathematical algorithms and computational power in the foreseeable future, and also on limited financial resources available to a potential adversary. Computationally secure cryptosystems, no matter whether public- or secret-key, will always be threatened by breakthroughs, which are difficult to predict, and even steady progress of code-breaking allows the adversary to reach “back in time” and break earlier captured communications encrypted with weaker keys. This results in the necessity to periodically re-encrypt re-sign certain documents, which are to be of a longer lifetime, such as contracts etc., and to carefully sort information according to the used cryptosystem.

Quantum mechanics provides a way of distributing secret messages with unconditional security. It is based on known classical secret-key cryptosystems and makes use of certain quantum mechanical properties to ensure secure distribution of random and secret key. The main problem in classical secret-key cryptosystems had been the distribution of secret key. Even the only proven unconditionally secure Vernam cipher relies on random secret key which is to be distributed with each message. The security of all the classical crypto methods is undermined by the advancement of technology and computation. Quantum mechanics however provides a solution and

distributes unconditionally secure key through open channel. The security is guaranteed by basic laws of quantum mechanics. Heisenberg uncertainty principle forbids simultaneous measurement of nonorthogonal states. In the framework of classical physics it is impossible to reveal potential eavesdropping because information encoded in a state can be perfectly copied without causing any disturbance to the state. Hence all classical signals can be monitored passively. In classical communications one bit of information is encoded simultaneously on many photons, atoms or electrons. Hence it is always possible to passively listen to it by deviating a part of it or copying it. However in quantum cryptosystems one bit of information is encoded on single photon, atom or electron. In addition orthogonal states are used to encode information. Any attempt to read it causes disturbance and hence reveals eavesdropping. In addition linearity of quantum mechanics forbids perfect copying of quantum states. Hence quantum systems eliminate the side channels which cause drastic trouble in classical cryptosystems. These vital quantum properties are discussed in detail in next chapter.

It is worth noting that quantum cryptography is based on classical private key cryptosystems. Quantum cryptography solves the problem of key distribution only. Hence it has been given the name *quantum key distribution* (QKD). In general Vernam cipher (the one time pad) is used as the reliable cryptosystem since its security is unconditionally proven, provided the key is random and secret. Quantum key distribution protocols then ensure the distribution of a key which remains unknown to a potential eavesdropper. Since light travels faster with a small decoherence they are regarded as the potential carriers of information. Various properties of photons can be used to encode information such as polarization, phase, quantum correlations of Einstein-Podolsky-Rosen (EPR) pairs, wavelength or quadrature components of squeezed state of light. The only requirement on the quantum states is that they belong to mutually non-orthogonal bases of their Hilbert space, where each vector in one basis has equal length-projection onto all vectors of other basis (bases).

Quantum mechanics does not prevent all types of eavesdropping, it just detects it and reveals the presence of eavesdropper. Since only the cryptographic key is distributed this way and not the original message, no information leak occurs. When discrepancies are found, the key is simply discarded and the procedure is repeated again by users to generate another key.

1.4 Thesis outline

Thesis consists of two different parts. First in part one, we discuss ideal quantum key distribution protocols and their robustness in terms of provable entanglement. The robustness bounds are proved for most general coherent attacks. In general these bounds are already known for provable entanglement as 25% for the four-state protocol and 33% for the six-state protocol. We anticipate to provide a region in which the legitimate users share entanglement. This region is reduced to a line for six-state protocol because of additional constraint on it. We also investigate the information cost which Eve has to pay in order to reach these bounds.

In part two we adopt more practical approach. We investigate the limitation on distance of secure communication because of practical restrictions. In particular, we investigate the lack of single photon sources, the lossy channel and faulty detectors. For the purpose we consider sources as weak coherent pulses. The channels are the quantum channels where each single pulse of photon behaves as single quanta and these channels are basically optical fibres. The detectors are threshold detectors, which are click or no click detectors.

These practical limitations have already been observed using one-way classical communication between legitimate users [Lut00]. It has been observed that it is actually the dark counts that limit the distance up to which legitimate users can share a secret key [FG⁺01]. Dark counts are the clicks on detector even when there is no actual message. We have used two-way classical communication to postpone the effect of dark counts and increase the distance considerably. For the purpose we have considered an optimal attack which comprises of photon number splitting attack on all the multiphoton pulses and a joint coherent attack on the single photon pulses. This attack is optimal with respect to the disturbance that an eavesdropper creates while attacking. Any other format of attacking will increase the disturbance. We show that using two-way classical communication for post processing we can increase the distance of secure communication to a considerable quantity.

In both above mentioned parts our approach is to consider entanglement based versions of standard four- and six-state protocols.

Chapter 2

Quantum Key Distribution (QKD) Protocols and Secure Key Rates

In this chapter vital features of quantum key distribution (QKD) are explained which form the base for the work presented in chapters 3 and 4. In Sec. 2.1 vital features of quantum mechanics are discussed which form a basis for QKD protocols. Various QKD protocols are then described in detail in Sec. 2.2. This includes the description of well known BB84, six-state and decoy state protocol. Both prepare and measure and entanglement based versions of the protocols is explained and the equivalence of the two versions is then explored. In Sec. 2.3 security of QKD protocols is discussed which includes the categorization of various attacks on a protocol. Two security bounds namely Csiszar Körner and Shor-Prekill are discussed in detail which are based on individual and coherent attacks respectively. They also provide a bound on secure key rates.

2.1 Basic quantum features vital in quantum key distribution

Orthogonality plays vital role in quantum key distribution. There are three main properties of nonorthogonal states that make them ideal for key distribution protocols.

- Information gain implies perturbation: In an attempt to distinguish between two nonorthogonal states the information gain is only at the expense of causing disturbance.

Consider two non-orthogonal quantum states $|\psi\rangle$ and $|\phi\rangle$ about which Eve is trying to get information. She attaches an ancilla say in initial state $|u\rangle$ and let it unitarily interact with the unknown states $|\psi\rangle$ or $|\phi\rangle$. Assuming that this process does not cause any disturbance in the two states, the interaction is given as

$$\begin{aligned} |\psi\rangle |u\rangle &\longrightarrow |\psi\rangle |v\rangle \\ |\phi\rangle |u\rangle &\longrightarrow |\phi\rangle |v'\rangle \end{aligned}$$

Eve can determine the identity of states $|\psi\rangle$ and $|\phi\rangle$ if $|v\rangle$ and $|v'\rangle$ are different. But since inner products must be preserved under unitary interaction one gets

$$\begin{aligned} \langle\psi|\phi\rangle\langle u|u\rangle &= \langle\psi|\phi\rangle\langle v|v'\rangle \\ \langle u|u\rangle &= \langle v|v'\rangle = 1 \end{aligned}$$

which means that the states $|v\rangle$ and $|v'\rangle$ are identical and Eve cannot distinguish between the nonorthogonal states ψ and ϕ . Thus distinguishing the two states must inevitably cause disturbance in one of them.

- It is impossible to unambiguously determine two non orthogonal states: There is no quantum measurement that can reliably distinguish between the nonorthogonal states.

Suppose there is a quantum measurement \mathcal{M} which gives an outcome m whenever the state is $|\psi\rangle$. But a state $|\phi\rangle$ nonorthogonal to $|\psi\rangle$ has always a component parallel to $|\psi\rangle$ i.e. $|\phi\rangle = \alpha |\psi\rangle + \beta |\tau\rangle$ where $|\psi\rangle$ and $|\tau\rangle$ are orthogonal and $|\alpha|^2 + |\beta|^2 = 1$. Thus while making a measurement on $|\phi\rangle$ there is a non-zero probability $|\alpha|^2$ of getting an outcome m . Thus sometimes one makes an error in determining which state was prepared.

- Ideal copy of two nonorthogonal states is impossible: This is the no-cloning theorem stating that it is impossible to copy an unknown quantum state.

Suppose there is a quantum copier in an initial pure state $|c\rangle$ and it is used to create a perfect copy of two nonorthogonal states $|\psi\rangle$ and $|\phi\rangle$ by some unitary evolution \mathcal{U} then

$$\begin{aligned} |\psi\rangle |c\rangle &\longrightarrow |\psi\rangle |\psi\rangle \\ |\phi\rangle |c\rangle &\longrightarrow |\phi\rangle |\phi\rangle. \end{aligned} \tag{2.1}$$

Taking inner product of above equations gives

$$\langle \psi | \phi \rangle = (\langle \psi | \phi \rangle)^2 \quad (2.2)$$

But $x = x^2$ has only two possible solutions, $x = 1$ or $x = 0$, so either $|\psi\rangle = |\phi\rangle$ or $|\psi\rangle$ and $|\phi\rangle$ are orthogonal. Thus a cloning device can only clone states which are orthogonal to one another and therefore a general quantum cloning device is impossible.

In general, even if one allows non-unitary cloning devices, cloning of non-orthogonal states remains impossible, unless one is willing to tolerate a finite loss in fidelity. For a cloning machine with a blank copy $|b\rangle$ initially in state $|0\rangle$ producing a perfect copy of state $|\psi\rangle$, the evolution is given as

$$|\psi\rangle |b\rangle |0\rangle \longrightarrow |\psi\rangle \otimes |\psi\rangle \otimes |f_\psi\rangle \quad (2.3)$$

where $|f_\psi\rangle$ denotes the final state of copying machine. For an orthogonal state $|\tau\rangle$ the copying process is given as

$$|\tau, b, 0\rangle \longrightarrow |\tau, \tau, f_\tau\rangle.$$

However for a superimposed state $|\phi\rangle = (|\psi\rangle + |\tau\rangle)/\sqrt{2}$, the linearity of quantum mechanics implies that

$$\begin{aligned} |\phi, b, 0\rangle &= \frac{1}{\sqrt{2}}(|\psi\rangle + |\tau\rangle) \otimes |b, 0\rangle \\ &\longrightarrow \frac{1}{\sqrt{2}}(|\psi, \psi, f_\psi\rangle + |\tau, \tau, f_\tau\rangle). \end{aligned}$$

But the above obtained state is not the desired ideal copy $|\phi, \phi, f_\phi\rangle$ whatever the states $|f\rangle$ may be.

Quantum cryptography came into limelight by the introduction of Bennet-Brassard four-state protocol in 1984, the BB84 protocol, based on the idea by Wiesner in 1976. Various modified and new protocols have been introduced so far which include the six-state protocol and decoy state protocols. Both six-state and decoy state protocols have some advantages over the BB84 as the former tolerates higher error rates and the latter is able to overcome photon number splitting attack. In each protocol secret key is established after post processing. This involves (i) *error correction* or rejection to eliminate the errors in the bit string and (ii) *privacy amplification* to eliminate Eve's information about the bit string. The length of the secret key string depends on whether only Alice or Bob make an announcement (*one-way classical communication*) or both do (*two-way classical communication*). Key generation rate is hence defined as the ratio of the secret key string retained in the end to the one originally sent by Alice.

2.2 Quantum key distribution protocols

Each QKD protocol consists of three stages. In the *distribution stage*, Alice encodes her random bit-string in a random sequence of non-orthogonal signal states (e.g., polarized single photons). Such a preparation involves two mutually unbiased bases (MUBs) in the four-state protocol and three in the fully symmetric six-state protocol. A first *raw key* is established when Bob measures each received signal at random in one of the possible bases and registers his outcomes. In the *sifting stage*, Alice and Bob publicly announce the bases used in each measurement. They then reject all (ideally half) bits originated from measurements in bases different from the preparation ones. Finally, Alice and Bob post-process this *sifted key* to distill a secret key. The *post-processing stage* typically involves error-correction and privacy amplification.

2.2.1 Prepare and measure four- and six-state protocols

In the work presented in chapters 3 and 4 the conventional BB84 and six-state protocols have been analyzed. Also decoy state protocols have been considered for the key generation rates in practical QKD. It is therefore of interest to explore these protocols.

BB84 protocol

In the prepare-and-measure BB84 protocol [BB84], Alice sends a sequence of, say n qubits to Bob each of which is randomly prepared in one of the basis states $\{|0\rangle, |1\rangle\}$ or $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ which are eigenstates of two maximally conjugated physical variables, namely the two Pauli spin operators \mathcal{Z} and \mathcal{X} . The eigenstates of \mathcal{Z} , i.e. $\{|0\rangle, |1\rangle\}$, and of \mathcal{X} , i.e. $\{|\bar{0}\rangle, |\bar{1}\rangle\}$, are related by the Hadamard transformation

$$\mathcal{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad (2.4)$$

i.e. $|\bar{i}\rangle = \sum_j \mathcal{H}_{ij} |j\rangle$ ($i, j \in \{0, 1\}$). Thus $|\bar{0}\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|\bar{1}\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. In the computational basis $\{|0\rangle, |1\rangle\}$, the Pauli spin operators are represented by the matrices

$$\mathcal{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathcal{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \mathcal{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (2.5)$$

Alice's random bases choice	+	×	+	+	×	×
Alice's random bit sequence	0	0	1	0	1	1
Bob's random bases choice	×	×	×	+	×	+
Bob's bit sequence	0	0	0	0	1	0
Bases announced publicly	different	same	different	same	same	different
Sifted key	-	0	-	0	1	-

Table 2.1: BB84 protocol: Alice selects randomly from the rectilinear (+ or $\{0, 1\}$) and diagonal (\times or $\{\bar{0}, \bar{1}\}$) bases. She randomly selects the bit value 0 or 1. Bob randomly chooses the bases from the two and gets a particular bit value. Alice and Bob announce the bases and discard the bits in which bases were different. Almost 50% of the bits are discarded in this sifting process. The remaining bits form the sifted key. In general the sifted key is not totally identical owing to the presence of error rate due to noise or eavesdropping.

Bob measures the received qubits randomly in one of the two bases. The cases in which Alice and Bob used the same bases, the bit values are perfectly correlated. However in the cases in which they chose different bases the bit values are not correlated. Thus after the transmission stage there is 25% error in Bob's bit sequence. This error rate is too high to be corrected by any error correction process. However after the transmission stage, Alice and Bob apply a random permutation of their data and publicly discuss the bases chosen, discarding all the bits where they have selected different bases. In this way 50% of the bits are discarded but the key is free of the above mentioned 25% error. This shorter key after basis reconciliation is called the *sifted key*. The sifted key still contains some number of errors either due to channel noise or because of an eavesdropping attack.

Subsequently, they randomly select a number of bits from the remaining random key (sifted key) and determine their *error probability* or QBER. Pessimistically Alice and Bob attribute all error (due to channel noise or eavesdropping) to Eve. If the estimated QBER is too high the protocol is aborted. Otherwise, Alice and Bob perform error correction and privacy amplification with one- or two-way classical communication, in order to obtain a smaller number of secret and perfectly correlated random bits [BS94, BB⁺95, Mau93, GL03, Ch02].

Six-state protocol

The six-state prepare-and-measure scheme is quite similar to the BB84 (four-state) scheme [Bru98]. More precisely, Alice and Bob use at random three

bases namely, the two bases used in the BB84 plus an additional one $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ which corresponds to the \mathcal{Y} Pauli operator. In analogy to BB84, the three bases are related (up to a global phase) via the transformation

$$\mathcal{T} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}, \quad (2.6)$$

i.e. $|\bar{i}\rangle = \sum_j \mathcal{T}_{ij} |j\rangle$ and $|\bar{\bar{i}}\rangle = \sum_j \mathcal{T}_{ij}^2 |j\rangle$ with $i, j \in \{0, 1\}$. Thus $|\bar{0}\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}$ and $|\bar{1}\rangle = (|0\rangle - i|1\rangle)/\sqrt{2}$. During the sifting process 2/3rd of the bits are discarded where Alice's and Bob's bases choice differ. This is much more than 50% in BB84, hence the key generation rates are less in six-state protocol than BB84. However six-state protocol is of advantage as it can sustain higher error rates.

Decoy-state protocol

The lack of single photon pulses makes conventional BB84 and the six-state protocols vulnerable to *photon number splitting* (PNS) attack. The light source emits pulses in the form of weak coherent pulses (WCPs) with poissonian photon number distribution, $p_i = \exp(-\mu)\mu^i/i!$, where μ is the mean photon number. In PNS attack Eve gains full information of multiphoton pulses, $i \geq 2$. Such pulses are marked as tagged by Eve. The decoy state protocol has the power to counteract such attacks. In decoy state protocol, Alice randomly mixes up pulses from different laser sources which have different intensities. The essence of the decoy state protocol is this that the yield of all pulses of different intensities is same. This essentially means that the conditional probability that detector clicks when a single photon pulse hits the detector is same for all intensities, the same is true for multiphoton pulses. Hence Alice can estimate the fraction of multiphoton pulses hitting the detector and presence of Eve by comparing different yields. A decoy state protocol can be used both with two and three bases, the former being a supplement of BB84 and latter that of six-state protocol.

Consider a decoy-state protocol involving two decoy weak coherent pulses with mean photon numbers $\kappa < \nu$ fulfilling the additional requirement $\kappa \exp(-\kappa) < \nu \exp(-\nu)$, and a signal pulse with mean photon number $\mu > \kappa + \nu$. Therefore, the decoy pulses are detected with probabilities $P_{\text{exp}}^{(\kappa)}$ and $P_{\text{exp}}^{(\nu)}$ obeying the relations [Wan05, MQ⁺05]

$$\begin{aligned} P_{\text{exp}}^{(\kappa)} &= P_{\text{exp}}^{\text{dark}} e^{-\kappa} + s_1 \kappa e^{-\kappa} + s_m (1 - e^{-\kappa} - \kappa e^{-\kappa}), \\ P_{\text{exp}}^{(\nu)} &\geq P_{\text{exp}}^{\text{dark}} e^{-\nu} + s_1 \nu e^{-\nu} + s_m (1 - e^{-\kappa} - \kappa e^{-\kappa}) \frac{\nu^2 e^{-\nu}}{\kappa^2 e^{-\kappa}}. \end{aligned} \quad (2.7)$$

Thereby, s_m is the conditional probability that the detector clicks provided multiphoton pulse with mean photon number κ hits the detector, whereas s_1 is the corresponding probability for single-photon pulses. Using (2.7) one obtains

$$s_1 \geq \frac{\nu^2 e^\kappa P_{\text{exp}}^{(\kappa)} - \kappa^2 e^\nu P_{\text{exp}}^{(\nu)} - (\nu^2 - \kappa^2) P_{\text{exp}}^{\text{dark}}}{\kappa \nu (\nu - \kappa)} := \bar{s}_1. \quad (2.8)$$

The inequality in the second line of (2.7) is valid provided the inequalities $\kappa < \nu$ and $\kappa \exp(-\kappa) < \nu \exp(-\nu)$ are fulfilled. Correspondingly, the probability Δ_μ of multiphoton signal pulses can be upper-bounded as follows

$$\Delta_\mu \leq 1 - \frac{\bar{s}_1 \mu e^{-\mu}}{P_{\text{exp}}^{(\mu)}} := \tilde{\Delta}_\mu. \quad (2.9)$$

Thus Alice and Bob are able to estimate the fraction of multiphoton pulses, using the decoy state protocol. This pessimistically estimated fraction is much less than that in conventional four- and six-state protocols.

2.2.2 Error correction and privacy amplification

The distribution and measurement stage ends the quantum part of QKD protocols. As has been discussed above, the sifted key still contains errors arising from channel noise or potential eavesdropping. Alice and Bob estimate this error by first applying the random permutation. This random permutation distributes the disturbance evenly among all bits. They then sacrifice part of their data and announce the bit values for that part. The fraction of cases in which bit values differ is the bit error rate. Due to random permutation done above, Alice and Bob assume that the bit error rate in the remaining sifted key is the same. Alice and Bob then need to do *error correction* or *data reconciliation* on the remaining key so that both share the same key. In addition Eve may know part of the key without causing any disturbance. Some information about the key may also leak to Eve during error correction process. In order to eliminate Eve's information about the key Alice and Bob must do *privacy amplification*. Both *error correction* and *privacy amplification* are done on classical channel and the discussion is done publicly. Alice and Bob's aim is thus to reveal as little information as possible to the eavesdropper during error correction.

Error correction

Error correction process is the information reconciliation process which tends to make Alice and Bob's strings the same. As mentioned above very few bits

must be sent over public channel in order to leak little information to Eve. Many error correction protocols have been proposed but cascade protocol suggested by Brassard and Salvail [BS94] is the most common in use and it reveals very little information to Eve. This protocol runs in number of rounds.

Cascade protocol

In the cascade protocol Alice and Bob first perform a random but identical permutation of their bits to distribute the errors randomly. This random permutation must be different for each round. They then arrange their bits in blocks of fixed length. Alice then computes parity of each block and announces it publicly. Bob computes the parity of his corresponding block and announces 'ok' if it matches. In this case either the block contains zero errors or even number of errors. They then move on to next block. In case the parity does not match, Bob is sure there are odd number of errors in the block. Bob then does binary (bisective) search i.e. he divides the block into two halves and compares the parity of each half with Alice to locate whether error occurs in first half or second. The half in which error is present is then divided again and parity is compared. This process is repeated until the error is located which Bob corrects by flipping the bit. If the flipped bit was present in a previous block, it means that block had even number of errors and yet another error is present in that block. Bob then applies binary search to previous block and corrects the error. In order to reduce the information revealed to Eve, Alice and Bob discard last bit of each block whose parity was revealed. Before starting each round Alice and Bob randomly permute their bit strings and then perform all steps again with an increased block size.

After a large number of consecutive rounds, Alice and Bob's bit strings become errorless with high probability with Eve having partial knowledge about the string. They then need to perform privacy amplification to eliminate Eve's information.

Privacy amplification

As has been stated earlier *privacy amplification* is a classical protocol done on a public channel to eliminate Eve's information about the key. In a typical privacy amplification protocol Alice and Bob randomly permute the bits and Alice pairs up the bits. She then announces which bits she has paired up. They both then calculate the parity of their bits and keep the parity as their key sequence. Since privacy amplification is done after error correction they both have the same bit (parity) value. On the other hand if Eve knows perfectly about one bit and nothing about the other, she knows nothing

about the parity value. Even if she knows the value of both bits with 70% probability, her information about parity bit is reduced to $0.70^2 + 0.30^2 = 58\%$. This process is repeated several times with Eve's information reducing at each step. The key length reduces to half at each step. In general more complicated protocols are used which use larger blocks.

If error correction process fails to locate and correct an error, this process yields a totally uncorrelated string. Key distillation would then not be successful. Alice and Bob thus compare a part of their distilled key to check. If there is a mismatch they run the error correction process again followed by privacy amplification and get a shorter, correlated key.

More complicated and efficient privacy amplification processes are random linear hashing. Alice randomly chooses a set of linearly independent strings v_j and announces them. The secret key bits then turn out to be $s_j = v_j \cdot k$, where k is the key.

Advantage Distillation

Using one-way error correction and privacy amplification methods Alice and Bob can distill a secret key only if their mutual information is more than that between Alice and Eve or Bob and Eve. However for the case when mutual information between Alice and Bob is less than that between Alice and Eve, Alice and Bob can run a two-way advantage distillation protocol in which they gain an advantage over Eve despite the fact that their mutual information is less than Eve. This protocol has been suggested by Maurer [Mau93]. The advantage distillation protocols are less efficient than privacy amplification and are used only up to the point where one-way error correction and privacy amplification can take over.

In a typical advantage distillation protocol Alice and Bob take advantage of the authenticated channel to decide which realizations to keep whereas Eve cannot influence this process. Alice picks up several instances in which she gets the same bit value. She then announces the instances and not the bit value to Bob. Bob replies yes only if he has the same bit value for all those instances. For high error rate it is unlikely but for low error rate it is more probable that Eve makes an error than Bob. Eve can only use majority vote to decide. Thus Bob takes an advantage over Eve even if he starts with less mutual information.

There is another bit iteration protocol given by Gander and Maurer [GM94] which increases Bob's information about Alice's string more efficiently than Eve. In this two-way protocol Alice and Bob randomize their pairs and then pair up the bits. For each pair Alice announces the parity. Bob computes the parity of his pair and announces OK if the parities

match. For such cases they keep the second bit of the pair and discard the first one to compensate for the information that might have leaked to Eve by announcement of parity. For the case when parity does not match Alice and Bob discard both pairs. The retained bit string is then used for another round of parity checks.

2.2.3 Entanglement-based protocols

It has been shown that, from the point of view of an arbitrarily powerful eavesdropper, each one of BB84 and six-state prepare-and-measure schemes is equivalent to an entanglement-based QKD protocol [BBM92, LC99, SP00, Lo01, LCA05, GP01, Lo01]. These latter forms of the protocols offer advantages, in particular with respect to questions concerning their unconditional security, and work as follows: Alice prepares each of, say $2n$, entangled-qubit pairs in a particular Bell state¹, say $|\Psi^-\rangle \equiv \frac{1}{\sqrt{2}}(|0_A 1_B\rangle - |1_A 0_B\rangle)$ (where the subscripts A, B refer to Alice and Bob, respectively). This state is invariant under any unitary transformation of the form $\mathcal{U}_A \otimes \mathcal{U}_B$. Alice keeps half of each pair and submits the other half to Bob after having applied a random unitary transformation chosen either from the set $\{\mathbf{1}, \mathcal{H}\}$ (two-basis protocol) or from the set $\{\mathbf{1}, \mathcal{T}, \mathcal{T}^2\}$ (three-basis protocol). At the end of the transmission stage, Alice announces publicly the transformations she applied on the transmitted qubits and Bob reverses all of them. At this stage, in an ideal scenario Alice and Bob would share $2n$ pairs in the state $|\Psi^-\rangle^{\otimes 2n}$. Due to channel noise and the presence of a possible eavesdropper, however, at the end of the transmission stage all the $2n$ entangled-qubit pairs will be corrupted. In fact, they will be entangled among themselves as well as with Eve's probe. Thus, the next step for Alice and Bob is to estimate the number of singlets among the $2n$ shared pairs (alternatively to estimate the fraction of pairs which are in error). To this end, they apply a verification test which proceeds as follows: Firstly, Alice and Bob permute randomly all the pairs, distributing thus any influence of the channel noise and the eavesdropper equally among all the pairs [GL03, SP00]. Afterwards, they randomly select a number (say n_c) of the pairs as check pairs, they measure each one of them *separately* along a common basis and they publicly compare their outcomes. The influence of channel noise or of an eavesdropper is thus quantified by the average estimated QBER of the check pairs while, assuming that the check pairs constitute a fair sample², the estimated QBER applies also to the pairs

¹The Bell states $|\Phi^\pm\rangle \equiv (|0\rangle_A \otimes |0\rangle_B \pm |1\rangle_A \otimes |1\rangle_B)/\sqrt{2}$ and $|\Psi^\pm\rangle \equiv (|0\rangle_A \otimes |1\rangle_B \pm |1\rangle_A \otimes |0\rangle_B)/\sqrt{2}$, form an orthonormal basis in the two-qubit Hilbert space.

²In general, a logarithmic scaling of the size of the random sample with the length of Alice's and Bob's key, seems to be sufficient for security issues. See Ref. [LCA05] for a

which contribute to the final key.

After the verification test all the check pairs are dismissed and, if the QBER is too high the protocol is aborted. Otherwise, Alice and Bob apply an appropriate entanglement purification protocol (EPP) with classical one- or two-way communication [DE⁺96, BD⁺96] on the remaining $2n - n_c$ pairs, in order to distill a smaller number of almost pure entangled-qubit pairs. Finally, measuring these almost perfectly entangled-qubit pairs in a common basis, Alice and Bob obtain a secret random key, about which an adversary has negligible information.

2.2.4 Equivalence between prepare and measure and the corresponding entanglement based protocols

Entanglement based protocols seem implausible to apply using present day available technology. Alice and Bob need quantum memory to store all EPR pairs until the end of error correction and privacy amplification. They then make a measurement at the end of protocol to get a bit sequence. An additional complexity compared to prepare and measure protocols arises in preparing EPR states. However entanglement based protocols are easier to be analyzed theoretically. One can get security proofs of entanglement based protocols. An important aspect of entanglement based protocols is that, from point of view of an arbitrary Eve, they are equivalent to the corresponding prepare and measure protocols. It is because of this equivalence the security proofs of entanglement based protocols in turn mean that of prepare and measure ones. This equivalence is proved and discussed in particular in [SP00, GL03].

If the *entanglement distillation protocol* (EDP) has special properties then proving the security of prepare and measure protocol can be reduced to proving that of EDP. Shor and Preskill [SP00] considered EDP's with one-way classical communication which are equivalent to quantum-error correction codes, and furthermore, they considered the specific class of codes known as Calderbank-Shor-Steane (CSS) codes. Gottesman and Lo [GL03] have described how a similar reduction can be applied to EDP's with two-way classical communication. Like any quantum error correction code, a CSS code can correct both bit errors (pairs with $\mathcal{Z} \otimes \mathcal{Z} = -1$) and phase errors (pairs with $\mathcal{X} \otimes \mathcal{X} = -1$). But the crucial property of CSS codes is that the bit and phase error correcting procedures can be decoupled i.e. \mathcal{Z} errors can be corrected without knowing anything about the \mathcal{X} errors and vice-versa.

In the EDP protocols the key is affected by the bit error correction but

rigorous proof.

not by the phase error correction. The phase error correction is only there to expunge Eve's entanglement with Alice and Bob. What is important is not that phase error correction is actually done but rather it would have been successful if it had been done. The EDP should be such that phase error syndrome (Z-errors) measurement operators, the (X type operators) must commute with the bit error syndrome measurement operators (the Z-type operators). This way the X-type operators can be moved to the end and actually need not be applied practically. The X- type operators need a quantum computer as they involve Hadamard transform which has no classical analog. Thus the elimination of application of X-type operation eliminates the need for a quantum computer and it makes the two type of protocols equivalent. Rather than first carrying out the EDP and then measuring \mathcal{Z} for each of the k distilled pairs, Alice and Bob can instead measure \mathcal{Z} for each of n noisy pairs, and then do classical post processing of their measurement results to extract the final key. In this form, the entanglement-based protocol becomes equivalent to corresponding prepare and measure one.

2.3 Security of QKD protocols

As has been stated above there are various stages in a QKD protocol, from distribution to purification. Mainly one can divide a key generation protocol in two phases .

Phase I

Phase I consists of distribution of key bits from Alice to Bob, Eve's attacks during this distribution and sifting of key bits to estimate the disturbance or extent of noise caused by Eve or by faulty apparatus.

Phase II

Phase II consists of purifying the key bits generated in phase I. It consists of error correction or rejection to make the bit values at Alice and Bob the same followed by privacy amplification to eliminate Eve's knowledge about Alice and Bob data.

Security is based on how closely Alice and Bob can convert the data obtained in phase I to a secret key in phase II. In prepare and measure versions of QKD protocols Alice initially encodes the data and sends the encoded bits to Bob. They both then decode the data with information going one-way (one-way local operation and classical communication, LOCC) i.e. either from Alice to Bob or Bob to Alice, or two-way (two-way LOCC) i.e.

both from Alice to Bob and Bob to Alice. Security and bound on key rate is investigated from point of view of entanglement based versions of QKD protocols.

2.3.1 Various attacks on ideal protocols

There are many security proofs and bounds on key rate depending on what attacks Eve can perform as well as convenience of analyzing these attacks. In principle there are three kinds of assumptions on Eve's attacks.

Individual or incoherent attacks

In individual attacks, Eve attaches an individual probe to each qubit and then measures each probe separately. For such attacks it is assumed that Eve only waits until the end of basis reconciliation part to make a measurement on her probe. Since this measurement is independent on each probe, she cannot gain more information even if she delays her measurement until the end of public discussion of error correction and privacy amplification. These are the least powerful attacks but are most convenient in analysis as in such attacks signals are not correlated and problem can be reduced to a classical one.

Collective attacks

In these attacks Eve attaches separate probe to each signal pulse as in individual attacks. She then measures all the probes collectively. Quantum estimation theory implies that collective attacks are powerful compared to individual attacks as Eve can gain more information. In analysis they are also convenient as they also do not allow correlations between signals. However in these attacks Eve waits until the very end of protocol which involves basis reconciliation, error correction and privacy amplification, to make a measurement.

Coherent or joint attacks

These are the most powerful attacks and are the worst case scenario. Here Eve attaches a single probe to all signal pulses and she has access to all signal pulses at the same time. In the end she has a single high dimensional state which she can measure by a single probe. Such attacks are difficult to analyze as Alice and Bob's signals can be correlated among themselves and with Eve's probe in any possible way. In addition like collective attacks Eve makes a measurement at the end of Basis reconciliation, error correction and privacy amplification.

2.3.2 Security bounds based on various attacks

An effort has been made to give a security bound on various protocols. The security bound comprises up to which disturbance or error rate, secret key can be distilled. These bounds are given for various attacks based on ease and complexity of their analysis. The first bound is given by Csiszár and Körner [CK78] which is based on individual attack. Later Shor and Preskill [SP00] gave a more compact bound based on coherent attacks. Both these bounds are based on one-way error correction and privacy amplification.

Csiszár-Körner Bound

The first bound on secure key generation rate was given by Csiszar and Körner [CK78] which is based on classical probability theory. It gives a lower bound on secret key generation rate. Since classical probability theory does not allow correlations between signals, this bound is valid only if Eve is restricted to individual or incoherent attacks. This bound states that secret key can be established between Alice and Bob if mutual information between Alice and Bob, $I(A, B)$ is greater than that between Eve and Alice $I(A, E)$ or Eve and Bob $I(B, E)$ i.e. if

$$I(A, B) \geq \text{Max}\{I(A, E)|I(B, E)\} \quad (2.10)$$

where $I(A, B) = H(A) - H(A|B)$. Here $H(x)$ is the Shannon entropy and is given as $H(x) = -x \log_2 x - (1 - x) \log_2 (1 - x)$. This bound is valid if Alice and Bob use one-way classical communication for data post processing which includes error correction and privacy amplification. For two-way post processing they can distill a secret key even if Alice and Bob start with less mutual information than Eve.

In order to get a lower bound on BB84 protocol one has to analyze the optimum incoherent strategy by Eve. This strategy was first reported by Fuchs *et. al* [FG⁺97], however a simple derivation was given by Cirac and Gisin [CG97] who used symmetry argument to get the same results. In this attack Eve attaches a probe in an initial state $|E\rangle$ to the qubits flying to Bob. She then lets the probe evolve into distinct probe states depending on the state of Bob's qubit with which it has interacted. The probe is then stored until the basis are announced, so that Eve can increase her chance of distinguishing the probe and hence Bob's qubit by choosing the best measurement for that particular basis. In addition Eve tries to minimize disturbance or error rate to make the qubit that Bob receives to be as close as possible to that sent by Alice. This attack is not possible using present day available technology since Eve needs quantum memory with large decoherence time to store the

ancilla (probe) as Alice and Bob can delay the announcement of bases to an infinite time. The unitary evolution in $\{0, 1\}$ basis is given as follows

$$|0_B\rangle \otimes |E\rangle \longrightarrow |0_B\rangle \otimes |E_{00}\rangle + |1_B\rangle \otimes |E_{01}\rangle \quad (2.11)$$

$$|1_B\rangle \otimes |E\rangle \longrightarrow |0_B\rangle \otimes |E_{10}\rangle + |1_B\rangle \otimes |E_{11}\rangle. \quad (2.12)$$

Similar interactions can be given for $\{\bar{0}, \bar{1}\}$ basis with Eve's states given by $E_{\bar{i}\bar{j}}$ where $i, j \in \{0, 1\}$. The first kets on right hand side of above equations, after tracing out Eve's states, form the mixed state Bob will receive and the second kets after tracing out Bob form the mixed state of Eve. The probe states E_{ij} are not normalized yet. The above two interactions can be written more neatly as

$$\begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} \otimes |E\rangle \longrightarrow \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} \otimes \begin{pmatrix} E_{00} & E_{01} \\ E_{10} & E_{11} \end{pmatrix} \quad (2.13)$$

Above probe state matrix $\mathcal{E} = \begin{pmatrix} E_{00} & E_{01} \\ E_{10} & E_{11} \end{pmatrix}$ in one basis can be transformed into the other by Hadamard transformation given as

$$\bar{\mathcal{E}} = H\mathcal{E}H^\dagger, \quad (2.14)$$

where H is the Hadamard transformation matrix given in Eq. (2.4).

Introducing the symmetry part of the argument, there are two types of symmetries to be followed by Eve:

1. Symmetry between bits: Eve doesn't know the bit value during transmission, so the bits $|0\rangle$ and $|1\rangle$ are attacked the same way by Eve. This requires that the overlaps between Eve's probes must remain invariant under the change of indices $0 \longleftrightarrow 1$ i.e. $\langle E_{01} | E_{11} \rangle = \langle E_{10} | E_{00} \rangle$
2. Symmetry between bases: The bases are announced after Eve's attack so bits in both bases are attacked the same way. Thus symmetry requires that overlaps between Eve's probe must remain invariant under the exchange of bases e.g. $\langle E_{01} | E_{11} \rangle = \langle E_{\bar{0}\bar{1}} | E_{\bar{1}\bar{1}} \rangle$

Now imposing normalization and unitarity on Eqs. (2.11) and (2.12) it requires

$$\langle E_{00} | E_{00} \rangle + \langle E_{01} | E_{01} \rangle = 1 \quad (2.15)$$

$$\langle E_{10} | E_{10} \rangle + \langle E_{11} | E_{11} \rangle = 1 \quad (2.16)$$

From symmetry argument 1 and defining new parameters F and D one gets

$$\begin{aligned}\langle E_{00}|E_{00}\rangle &= \langle E_{11}|E_{11}\rangle \equiv F \\ \langle E_{01}|E_{01}\rangle &= \langle E_{10}|E_{10}\rangle \equiv D\end{aligned}\quad (2.17)$$

where $F + D = 1$. Now for $j \in \{0, 1\}$, $\langle j|Tr_E \mathcal{U}|j\rangle \otimes |E\rangle\langle E| \otimes \langle j|\mathcal{U}^\dagger|j\rangle$, defines the probability that Bob receives the qubit undisturbed. Therefore F is the fidelity and D is the disturbance or error rate which is the probability that Bob receives the qubit disturbed.

Now from taking overlaps of Eqs. (2.11) and (2.12) and requiring unitarity i.e. the preservation of overlap before and after interaction one gets

$$\langle E_{00}|E_{10}\rangle + \langle E_{01}|E_{11}\rangle = 0. \quad (2.18)$$

Since the overlaps are real i.e. $\langle E_{00}|E_{10}\rangle = \langle E_{10}|E_{00}\rangle$ (overlaps can be made real by proper choice of phase) above equation reduces to

$$\begin{aligned}\langle E_{00}|E_{10}\rangle &= 0 \\ \langle E_{11}|E_{01}\rangle &= 0.\end{aligned}\quad (2.19)$$

Thus probe states $E_{ii} \perp E_{ji}$ and $E_{ii} \perp E_{ij}$ for $i \neq j$ and $i, j \in \{0, 1\}$, hence Eve can fully discriminate between these orthogonal states. Defining the remaining overlaps as

$$\begin{aligned}\langle E_{00}|E_{11}\rangle &= \langle E_{11}|E_{00}\rangle \equiv H \\ \langle E_{01}|E_{10}\rangle &= \langle E_{10}|E_{01}\rangle \equiv G\end{aligned}\quad (2.20)$$

Now converting Eve's probe's states into $\{\bar{0}, \bar{1}\}$ basis using Eq. (2.14) and using symmetry between the bases we get

$$F - D = H + G. \quad (2.21)$$

Eqs (2.11) and 2.12 can be now rewritten with normalized probe states \hat{E}_{ij} as

$$|0_B\rangle \otimes |E\rangle \longrightarrow \sqrt{F}|0_B\rangle \otimes |\hat{E}_{00}\rangle + \sqrt{D}|1_B\rangle \otimes |\hat{E}_{01}\rangle \quad (2.22)$$

$$|1_B\rangle \otimes |E\rangle \longrightarrow \sqrt{D}|0_B\rangle \otimes |\hat{E}_{10}\rangle + \sqrt{F}|1_B\rangle \otimes |\hat{E}_{11}\rangle. \quad (2.23)$$

We see that Bob's states are entangled with Eve's states. There is a probability F that Bob receives the same bit as Alice. In this case Eve gets away without causing any disturbance. This does not mean that Eve knows the

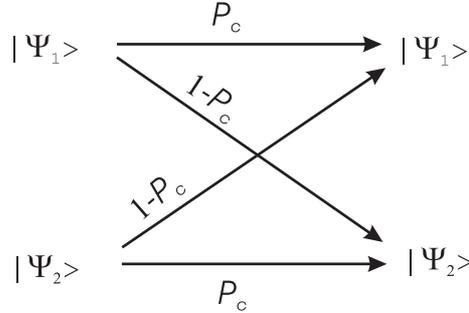


Figure 2.1: Binary symmetric channel: Figure shows a binary symmetric channel which consists of two states $|\psi_1\rangle$ and $|\psi_2\rangle$ with equal probability P_c of correct guess and probability $1 - P_c$ that state is incorrectly guessed or practically flipped from $|\psi_1\rangle$ to $|\psi_2\rangle$ and vice versa.

state correctly. She has to distinguish between four density matrices. Eve's mixed states are given as

$$\rho_i = Tr_B \mathcal{U} |i_B\rangle |E\rangle \langle E| \langle i_B| \mathcal{U}^\dagger, \tag{2.24}$$

for $i \in \{0, 1, \bar{0}, \bar{1}\}$. But since she stores her probe until the bases are announced, the problem reduces to distinguishing two density matrices in that basis. For announcement of $\{0, 1\}$ basis, Eve's density matrices are

$$\rho_0 = F |\hat{E}_{00}\rangle \langle \hat{E}_{00}| + D |\hat{E}_{01}\rangle \langle \hat{E}_{01}| \tag{2.25}$$

$$\rho_1 = F |\hat{E}_{11}\rangle \langle \hat{E}_{11}| + D |\hat{E}_{10}\rangle \langle \hat{E}_{10}|. \tag{2.26}$$

From orthogonality relations 2.19 that Eve has two orthogonal sets of states i.e. $\{\hat{E}_{00}, \hat{E}_{11}\}$ and $\{\hat{E}_{01}, \hat{E}_{10}\}$. The first set occurs with probability F and second with probability D . Since the sets are orthogonal Eve can devise a measurement to tell her probe state belongs to which set. She can thus tell whether she has caused a disturbance. Next she has to perform a measurement to discriminate between two states, generally nonorthogonal, within a set. For two states $|\psi_1\rangle$ and $|\psi_2\rangle$, the probability of guessing the state correctly is

$$P_c = \frac{1}{2} + \frac{1}{2} \sqrt{1 - |\langle \psi_1 | \psi_2 \rangle|^2}. \tag{2.27}$$

Now states in each set represent a binary symmetric channel which keeps $|\psi_i\rangle \longleftrightarrow |\psi_i\rangle$ with probability P_c and flips $|\psi_1\rangle \longleftrightarrow |\psi_2\rangle$ with probability $1 - P_c$. Such a channel is given in Figure 2.1

For such a case maximum information gain is given as

$$I = 1 - H(P_c) \quad (2.28)$$

Thus the total information gained by Eve is

$$I(B|E) = F(1 - H(P_c^F)) + D(1 - H(P_c^D)) \quad (2.29)$$

where $P_c^F = 1/2 + 1/2\sqrt{1 - |\langle \hat{E}_{00} | \hat{E}_{11} \rangle|^2}$ and $P_c^D = 1/2 + 1/2\sqrt{1 - |\langle \hat{E}_{01} | \hat{E}_{10} \rangle|^2}$ and from Eqs. (2.17) and (2.20) we have

$$\begin{aligned} \langle \hat{E}_{00} | \hat{E}_{11} \rangle &= \frac{H}{F} \\ \langle \hat{E}_{01} | \hat{E}_{10} \rangle &= \frac{G}{D} \end{aligned} \quad (2.30)$$

The information gain given in Eq. (2.29) is maximized for fixed disturbance D when $P_c^D = P_c^F$. From $F + D = 1$

$$I(B|E)_{max} = 1 - H(P_c^D) \quad (2.31)$$

and from $F + D = G + H$ it can be expressed in terms of single parameter D as

$$I(B|E)_{max} = 1 - H\left(\frac{1}{2} + \sqrt{D(1-D)}\right). \quad (2.32)$$

Eve's information gain is zero for zero disturbance, it increases with increasing disturbance until she gets full information i.e. $I(B|E) = 1$ for $D = 1/2$.

The mutual information between Alice and Bob is simply that on a binary symmetric channel with probability of flip D , hence their information gain is given as

$$I(A|B) = 1 - H(D) \quad (2.33)$$

Equating Eqs. (2.32) and (2.33) we get the threshold disturbance $D = D_0$ up to which Alice and Bob can distill a secret key using one-way error correction and privacy amplification

$$I(A|B) = I(B|E)_{max} \Leftrightarrow D = D_0 = 1 - \frac{1/\sqrt{2}}{2} \simeq 15\% \quad (2.34)$$

Since above attack is optimum therefore for any individual attack for QBER or disturbance above 15% BB84 protocol becomes insecure and either Alice and Bob have to abort the protocol or look for two-way error correction and privacy amplification.

Csiszar-Körner bound given above has some limitations. First it is valid only when Alice and Bob use one-way classical communication for error correction and privacy amplification. It has been shown that for two-way post processing like advantage distillation, Alice and Bob can distill a secret key even if they start with less mutual information than that between Eve and Alice or Bob. In fact it has been shown that two-way error correction and privacy amplification is able to distill secret key for QBER up to 30% for optimal individual coherent attacks. In addition above bound is based on classical probability theory. The classical probability theory does not allow correlations between signals so Csiszar and Körner bound is not valid for general quantum key distribution (QKD). In QKD it can only be applied if Eve is restricted to individual attacks where signals are not correlated. In principle one cannot force Eve to make a measurement. She may delay her measurement till the very end of protocol and hence remain entangled with Alice and Bob. Thus a quantum approach is needed to analyze coherent or collective attacks.

Shor-Preiskill bound

The simplest quantum approach to give a lower bound on secure key rate is used by Shor and Preskill [SP00]. Their idea is based on Lo-Chau [LC99] argument that high fidelity implies low entropy and entropy is a bound on mutual information [NC00]. Hence in order to generate a secret key one needs to generate high fidelity EPR pairs. Shor and Preskill have given an *entanglement distillation protocol* (EDP based on Calderbank-Shor-Steane code CSS code) (Calderbank and Shor [CS96] and Steane [Ste96]). These codes divide the errors into bit and phase errors, where bit errors refer to the disturbance caused by channel or noise and phase errors to Eve's correlation. Thus a channel either applies σ_x or X for bit error or a σ_z or Z operator for phase error on each signal qubit pair or an identity operator. In order to get high fidelity EPR pairs Alice and Bob need to correct these bit and phase errors.

In a CSS code, classical linear codes C_1 and C_2^\perp are used for bit and phase error correction respectively, where $C_2 \subset C_1$. the entanglement based protocol is secure if with high probability i.e. probability of success exponentially close to unity, C_1 can correct the bit errors and C_2^\perp can correct the phase errors. In the corresponding prepare and measure protocol, C_1 is used to correct bit errors and C_2 to amplify privacy. Specifically, Alice transmits the random string w through the quantum channel, randomly selects a codeword u of C_1 and announces $u + w$. Bob receives the corrupted string $u + e$, computes $u + e$, and corrects to u . The final key is the coset $u + C_2$ of C_2 in

C_1 .

If this method is used to compute the final key in the prepare and measure protocol, and if the key being distributed is very long, at what asymptotic rate can secure final key be extracted from the sifted key? The answer is the rate k/n at which high-fidelity pairs can be distilled from noisy pairs in the EDP, which depends on how noisy pairs are. The purpose of the verification test included in the protocol is to obtain a reliable estimate of the noise. In the EDP, a useful way to characterize the noise is to imagine that, after the final Hadamard transformations are applied to the pairs, all n pairs are measured in the Bell basis i.e. both $\mathcal{Z} \otimes \mathcal{Z}$ and $\mathcal{X} \otimes \mathcal{X}$ are measured. If there were no noise at all, we would find $\mathcal{Z} \otimes \mathcal{Z} = \mathcal{X} \otimes \mathcal{X} = 1$ for every pair. Denote by $n\tilde{\delta}$ the number of pairs for which we have $\mathcal{Z} \otimes \mathcal{Z} = -1$ instead; we say that $\tilde{\delta}$ is the bit error rate of the noisy pairs. Denote by $n\tilde{\delta}_p$ the number of pairs for which we have $\mathcal{X} \otimes \mathcal{X} = -1$; we say that $\tilde{\delta}_p$ is the phase error rate of the pairs.

For a given set of n pairs, the rates $\tilde{\delta}$ and $\tilde{\delta}_p$ are actually random variables, because the quantum measurement of the pairs is undeterministic. But suppose that from the verification test, we can infer that for sufficiently large n and any $\epsilon > 0$, the inequalities $\tilde{\delta} < \delta + \epsilon$ and $\tilde{\delta}_p < \delta_p + \epsilon$ are satisfied with high probability. Furthermore we may imagine that the key bits are subjected to a publicly announced random permutation (or equivalently that the CSS code is randomized), so that the bit and phase errors are randomly distributed among the qubits. It can then be shown [Ham04] that for sufficiently large n and any $\epsilon' > 0$, there exists a CSS code such that the EDP distills k high-fidelity pairs from the n noisy pairs, where

$$k/n > 1 - H_2(\delta + \epsilon + \epsilon') - H_2(\delta_p + \epsilon + \epsilon'), \quad (2.35)$$

and $H_2(\delta) = -\delta \log_2 \delta - (1 - \delta) \log_2 (1 - \delta)$ is the binary entropy function. Therefore in the prepare and measure protocol, we establish an asymptotically achievable rate of extraction of secure final key from sifted key “key generation rate”:

$$R = 1 - H_2(\delta) - H_2(\delta_p) \quad (2.36)$$

That is in the protocol $H_2(\delta)$ of the sifted key bits are asymptotically sacrificed to perform error correction and $H_2(\delta_p)$ of the sifted key bits are sacrificed to do privacy amplification.

Chapter 3

Bounds on Performance of QKD Protocols

It has been shown that legitimate users must share provable entanglement as a necessary condition for security. Thus for both four- and six-state protocols, there is some maximum (threshold) disturbance or error probability up to which quantum correlations exist between Alice and Bob. In this chapter this threshold disturbance for the above mentioned protocols is investigated. This investigation is done for most general coherent attacks. In addition, the conditions under which Eve can reach these bounds and break the security, are thoroughly studied. This analysis is done under the assumption of incoherent attacks and two-qubit coherent attacks. The analysis done in this chapter is based on ideal QKD protocols where practical limitations are not taken into consideration. This later consideration is taken into account in chapter 4.

In Sec. 3.1, the threshold disturbance up to which legitimate users share provable entanglement is calculated for both BB84 and six-state protocols. This threshold disturbance incorporates the most general coherent attack by Eve. It is then explored in Sec. 3.2 at what price in terms of information gain and probability of correct guess can Eve disentangle Alice and Bob. For the purpose incoherent attacks and two-qubit coherent attacks are considered for both BB84 and six-state. In Sec. 3.3 link between classical and quantum distillation protocols is made by showing that, at least in the context of incoherent attacks, a two-way classical protocol, the so-called advantage distillation protocol, exists which can tolerate precisely the same amount of disturbance as a quantum purification protocol.

3.1 Provable entanglement and threshold disturbances

According to a recent observation, a *necessary precondition* for secret key distillation is that the correlations established between Alice and Bob during the state distribution cannot be explained by a separable state [CLL03, AG05]. Throughout this chapter, it is considered that Alice and Bob focus on the sifted key during the post-processing (i.e., they discard immediately all the polarization data for which they have used different bases) and that they treat each pair independently. Thus, according to the aforementioned precondition, given a particular value of the estimated QBER (observable), the task of Alice and Bob is to infer whether they share provable entanglement or not. Thereby, entanglement is considered to be provable if Alice's and Bob's correlations cannot be explained by a separable state within the framework of the protocols (including post-processing) and observables under consideration.

Recently [NA05], for the same post-processing, it was estimated the threshold disturbance for provable entanglement in the context of two-basis qudit-based QKD protocols under the assumption of joint eavesdropping attacks. In particular, it was shown that for estimated disturbances below $(d-1)/2d$ (where d is the size of the information carriers), Alice and Bob can be confident that they share provable entanglement with probability exponentially close to one. For the sake of completeness, in this section, the main steps of the proof are recapitulated and adapted to the BB84 scheme. Subsequently, along the same lines, the corresponding threshold disturbance is estimated for the six-state QKD scheme. For the sake of consistency, the entanglement-based versions of the protocols are adopted. However, the estimated threshold disturbances characterize both versions of the protocols.

3.1.1 Four-state protocol

Given the unitarity and hermiticity of \mathcal{H} , the average disturbance (average error probability per qubit pair), that Alice and Bob estimate during the verification test is given by [GL03, NA05, SP00]

$$D = \frac{1}{2n_c} \sum_{b=0,1} \sum_{j_i; i=1}^{n_c} \text{Tr}_{A,B} \left\{ [\mathcal{H}_{AB}^b \mathcal{P} \mathcal{H}_{AB}^b]_{j_i} \rho_{AB} \right\}, \quad (3.1)$$

with the projector¹

¹Note that in the absence of noise and eavesdropping each pair of qubits shared between Alice and Bob is in the Bell state $|\Psi^-\rangle$. Thus, in this ideal scenario, Alice and Bob obtain

$$\mathcal{P}_{j_i} = \sum_{l=0,1} |l_A, l_B\rangle\langle l_A, l_B| = |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| \quad (3.2)$$

and $\mathcal{H}_{AB}^b \equiv \mathcal{H}_A^b \otimes \mathcal{H}_B^b$. The last equality in (3.2) indicates that the verification test is nothing more than a quality-check test of the fidelity of the $2n$ pairs with respect to the ideal state $|\Psi^-\rangle^{\otimes 2n}$ [GL03, LC99, SP00, Lo01, LCA05, GP01, Lo01]. The state ρ_{AB} in Eq. (3.1) denotes the reduced density operator of Alice and Bob for all $2n$ pairs while the index j_i indicates that the corresponding physical observable refers to the j_i -th randomly selected qubit pair. The powers of the Hadamard transformations \mathcal{H}^b , with $b \in \{0, 1\}$, reflect the fact that the errors in the sifted key originate from measurements in both complementary bases which have been selected randomly by Alice and Bob with equal probabilities.

As has been mentioned earlier, one of the crucial cornerstones for the unconditional security of the protocol is that Eve does not know in advance which pairs will be used for quality checks and which pairs will contribute to the final key. Thus she is not able to treat them differently and the check pairs constitute a classical random sample of all the pairs [GL03, LC99, SP00, Lo01]. To ensure such a homogenization, Alice and Bob permute all of their pairs randomly before the verification stage. In view of this homogenization, the eavesdropping attack (although a joint one) becomes symmetric on all the pairs [GL03, SP00] i.e., $\rho_{AB}^{(1)} = \rho_{AB}^{(2)} = \dots = \rho_{AB}^{(2n)}$. Here, the reduced density operator of Alice's and Bob's k -th pair is denoted by $\rho_{AB}^{(k)} = \text{Tr}_{AB}^{(k)}(\rho_{AB})$ and $\text{Tr}_{AB}^{(k)}$ indicates the tracing (averaging) procedure over all the qubit pairs except the k -th one. Accordingly, the average estimated disturbance (3.1) reads [NA05]

$$D = \frac{1}{2} \sum_{b=0}^1 \text{Tr}_{A,B}^{(j_1)} \left\{ [(\mathcal{H}_A^b \otimes \mathcal{H}_B^b) \mathcal{P} (\mathcal{H}_A^b \otimes \mathcal{H}_B^b)]_{j_1} \rho_{AB}^{(j_1)} \right\} \quad (3.3)$$

where $\text{Tr}_{A,B}^{(j_1)}$ denotes the tracing procedure over the j_1 -th qubit pair of Alice and Bob. So, an arbitrary eavesdropping attack which gives rise to a particular reduced single-pair state $\rho_{AB}^{(j_1)}$ is indistinguishable, from the point of view of the estimated average disturbance, from a corresponding collective (individual) attack which results in a decorrelated $2n$ -pair state of the form $\bigotimes_{j=1}^{2n} \rho_{AB}^{(j)}$.

perfectly anticorrelated measurement results whenever they perform their measurements along the same basis

Our purpose now is to estimate the threshold disturbance D_{th} such that for any estimated $D < D_{\text{th}}$ Alice and Bob can be confident that their correlations cannot have emerged from a separable state. To this end let us explore the symmetries underlying the observable under consideration i.e., the estimated average QBER. According to Eqs. (3.3) and (3.2), D is invariant under the transformations

$$\begin{aligned} (l, b) &\rightarrow (l \oplus_2 1, b), \\ (l, b) &\rightarrow (l, b \oplus_2 1), \end{aligned} \quad (3.4)$$

where \oplus_2 denotes addition modulo 2. This invariance implies that the reduced density operators $\rho_{AB}^{(j_1)}$ and

$$\tilde{\rho}_{AB}^{(j_1)} = \frac{1}{8} \sum_{g \in \mathcal{G}_1, h \in \mathcal{G}_2} U(h)U(g)\rho_{AB}^{(j_1)}U(g)^\dagger U(h)^\dagger \quad (3.5)$$

give rise to the same observed value of the QBER [NA05]. The unitary and hermitian operators appearing in Eq. (3.5) form unitary representations of two discrete Abelian groups $\mathcal{G}_1 = \{g_1, g_2, g_3, g_4\}$ and $\mathcal{G}_2 = \{h_1, h_2\}$, and are given by

$$\begin{aligned} U(g_1) &= \mathcal{X}_A \otimes \mathcal{X}_B, & U(g_2) &= \mathcal{Z}_A \otimes \mathcal{Z}_B, \\ U(g_3) &= -\mathcal{Y}_A \otimes \mathcal{Y}_B, & U(g_4) &= \mathbf{1}_A \otimes \mathbf{1}_B, \end{aligned} \quad (3.6)$$

and

$$U(h_1) = \mathcal{H}_A \otimes \mathcal{H}_B, \quad U(h_2) = \mathbf{1}_A \otimes \mathbf{1}_B. \quad (3.7)$$

Moreover, invariance of the average QBER under the symmetry transformations of Eq. (3.4) induces invariance of $\tilde{\rho}_{AB}^{(j_1)}$ under both discrete Abelian groups \mathcal{G}_1 and \mathcal{G}_2 .

The key point is now that $\rho_{AB}^{(j_1)}$ and $\tilde{\rho}_{AB}^{(j_1)}$ differ by local unitary operations and convex summation. Thus the density operator $\rho_{AB}^{(j_1)}$ is entangled if $\tilde{\rho}_{AB}^{(j_1)}$ is entangled. Our main problem of determining the values of the QBER for which Alice and Bob share provable entanglement can be reduced therefore to the estimation of the values of D for which the most general two-qubit state $\tilde{\rho}_{AB}^{(j_1)}$ (which is invariant under both Abelian discrete groups) is entangled.

The hermitian operators $U(g_1)$ and $U(g_2)$ of the group \mathcal{G}_1 constitute already a *complete set of commuting operators* in the Hilbert space of two qubits and the corresponding eigenstates are the Bell states, $|\Phi^\pm\rangle \equiv \frac{1}{\sqrt{2}}(|0_A 0_B\rangle \pm |1_A 1_B\rangle)$ and $|\Psi^\pm\rangle \equiv \frac{1}{\sqrt{2}}(|0_A 1_B\rangle \pm |1_A 0_B\rangle)$, which form an orthonormal basis

in the two-qubit Hilbert space. Thus, the most general two-qubit state which is invariant under the Abelian group \mathcal{G}_1 is given by

$$\begin{aligned} \tilde{\rho}_{AB}^{(j_1)} &= \lambda_{00} |\Phi^+\rangle\langle\Phi^+| + \lambda_{10} |\Phi^-\rangle\langle\Phi^-| \\ &+ \lambda_{01} |\Psi^+\rangle\langle\Psi^+| + \lambda_{11} |\Psi^-\rangle\langle\Psi^-|, \end{aligned} \quad (3.8)$$

with $\lambda_{\alpha\beta} \geq 0$ and

$$\sum_{\alpha, \beta \in \{0,1\}} \lambda_{\alpha\beta} = 1, \quad (3.9)$$

while additional invariance under the discrete group \mathcal{G}_2 implies that

$$\lambda_{01} = \lambda_{10}. \quad (3.10)$$

Thus, the state (3.8) with the constraint (3.10) is the most general two-qubit state invariant under the Abelian groups \mathcal{G}_1 and \mathcal{G}_2 .

For later convenience let us rewrite the state $\tilde{\rho}_{AB}^{(j_1)}$ in the computational basis, i.e.

$$\tilde{\rho}_{AB}^{(j_1)} = \frac{1}{2} \begin{pmatrix} D & 0 & 0 & G \\ 0 & F & H & 0 \\ 0 & H & F & 0 \\ G & 0 & 0 & D \end{pmatrix}, \quad (3.11)$$

with $F = 1 - D$ denoting the so-called fidelity, i.e. the total probability for Bob to receive the submitted signal undisturbed. Furthermore, the remaining parameters are given by

$$\begin{aligned} D &= \lambda_{00} + \lambda_{10}, & F &= \lambda_{01} + \lambda_{11}, \\ G &= \lambda_{00} - \lambda_{10}, & H &= \lambda_{01} - \lambda_{11}, \end{aligned} \quad (3.12)$$

with D denoting the disturbance (QBER). In general, the parameters G and H can be expressed in terms of the overlaps between different states of Eve's probe and are thus intimately connected to the eavesdropping strategy. The key point for the subsequent discussion, is that for the estimation of the threshold disturbance it is not required to know the explicit form of the "macroscopic" parameters G and H and their detailed dependencies on Eve's attack. More precisely, using Eqs. (3.12), the constraints (3.9) and (3.10) read

$$F + D = 1 \quad (3.13)$$

$$F + H = D - G \quad (3.14)$$

respectively, while non-negativity of the eigenvalues $\lambda_{\alpha\beta}$ implies

$$D \geq |G|, \quad (3.15)$$

$$F \geq |H|. \quad (3.16)$$

The possible values of the estimated disturbance for which $\tilde{\rho}_{AB}^{(j_1)}$ is entangled can be estimated by means of the fully-entangled fraction (see [NA05]) or the Peres-Horodecki criterion [Pe96, HHH96]. Using the latter, we have that $\tilde{\rho}_{AB}^{(j_1)}$ is separable *if and only if* the inequalities

$$D \geq |H|, \quad (3.17)$$

$$F \geq |G|, \quad (3.18)$$

are satisfied. As depicted in Figure 3.1, these last inequalities combined with inequalities (3.15), (3.16) and Eqs. (3.13), (3.14) imply that the symmetrized state $\tilde{\rho}_{AB}^{(j_1)}$ is entangled if and only if the estimated QBER is below 1/4 or above 3/4. Given, however, that the states $\tilde{\rho}_{AB}^{(j_1)}$ and $\rho_{AB}^{(j_1)}$ are related via local operations and convex summation, the original single-pair state $\rho_{AB}^{(j_1)}$ must also be entangled in the same regime of parameters. Moreover, the probability that the QBER has been underestimated during the verification test is exponentially small in n_c . Hence one may conclude that, whenever Alice and Bob detect an average QBER below 1/4 (or above 3/4), they can be confident that they share entanglement with probability exponentially close to one ($\sim 1 - 2^{-n_c}$), and their correlations cannot have originated from a separable state. The necessary precondition for secret-key distillation is therefore fulfilled for estimated disturbances within these intervals.

On the contrary, for $1/4 \leq D \leq 3/4$, $\tilde{\rho}_{AB}^{(j_1)}$ is separable. Of course, this does not necessarily imply that $\rho_{AB}^{(j_1)}$ is also separable. But it does indicate that in this regime of parameters, Alice's and Bob's correlations within the framework of the BB84 protocol can be explained by a separable state, namely by $\tilde{\rho}_{AB}^{(j_1)}$. So, according to [CLL03, AG05], this implies that Alice and Bob cannot extract a secret key and must abort the protocol. From now on the focus is on the regime of practical interest ($F \geq D$), where the lowest possible threshold disturbance ($D_{\text{th}} = 1/4$) is attained for $G = H = -1/4$.

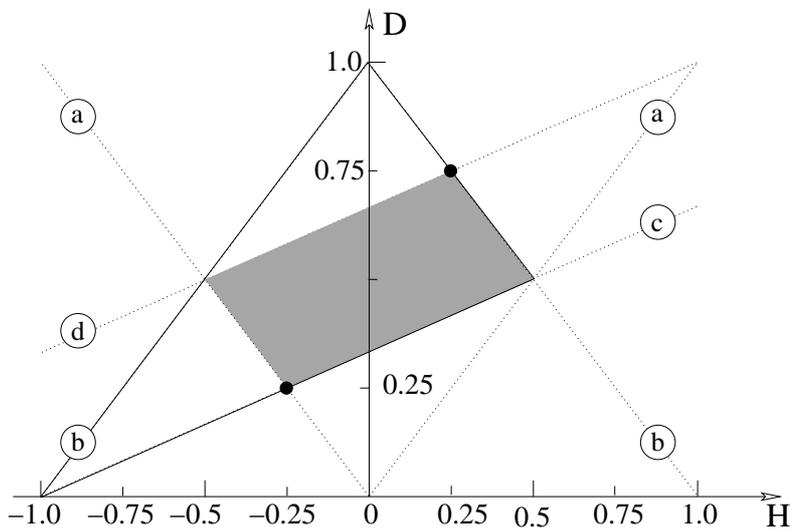


Figure 3.1: BB84 protocol: Region of the independent parameters D (QBER) and H for which the two-qubit state $\tilde{\rho}_{AB}^{(j_1)}$ is separable (shaded region). The various constraints that these parameters satisfy are indicated by straight dotted lines. Specifically, (a) Eq. (3.17); (b) Eq. (3.16); (c) Eqs. (3.15) and (3.13), (3.14); (d) Eqs. (3.18) and (3.13), (3.14). The protocol operates in the region which is defined by the solid lines.

3.1.2 Six-state protocol

The threshold disturbances for the six-state protocol can be determined in the same way. In this case, however, all three bases are used with the same probabilities and thus the average estimated disturbance (QBER) reads

$$D = \frac{1}{3} \sum_{b=0}^2 \text{Tr}_{A,B}^{(j_1)} \left\{ [(\mathcal{T}_A^b \otimes \mathcal{T}_B^b) \mathcal{P} (\mathcal{T}_A^{b\dagger} \otimes \mathcal{T}_B^{b\dagger})]_{j_1} \rho_{AB}^{(j_1)} \right\} \quad (3.19)$$

where the unitary (but not hermitian) transformation \mathcal{T} is defined in Eq. (2.6).

In analogy to the BB84 protocol, exploiting the symmetries underlying Eq. (3.19) one finds that D is invariant under the transformations

$$\begin{aligned} (l, b) &\rightarrow (l \oplus_2 1, b), \\ (l, b) &\rightarrow (l, b \oplus_3 1), \\ (l, b) &\rightarrow (l, b \oplus_3 2), \end{aligned} \quad (3.20)$$

with \oplus_3 denoting addition modulo 3. Furthermore, the invariance of D under the transformations (3.20) implies that the reduced density operators $\rho_{AB}^{(j_1)}$ and

$$\tilde{\rho}_{AB}^{(j_1)} = \frac{1}{12} \sum_{g \in \mathcal{G}_1, t \in \mathcal{G}_3} U(t) U(g) \rho_{AB}^{(j_1)} U(g)^\dagger U(t)^\dagger \quad (3.21)$$

yield the same average QBER. This latter state is invariant under the discrete Abelian groups \mathcal{G}_1 [with elements given in Eq. (3.6)] and $\mathcal{G}_3 = \{t_1, t_2, t_3\}$ with elements

$$\begin{aligned} U(t_1) &= \mathcal{T}_A \otimes \mathcal{T}_B, \\ U(t_2) &= \mathcal{T}_A^2 \otimes \mathcal{T}_B^2, \\ U(t_3) &= \mathbf{1}_A \otimes \mathbf{1}_B. \end{aligned} \quad (3.22)$$

The most general two-qubit state invariant under the Abelian groups \mathcal{G}_1 and \mathcal{G}_3 is now of the form (3.8), with

$$\lambda_{00} = \lambda_{10} = \lambda_{01}. \quad (3.23)$$

Thus, in the computational basis $\tilde{\rho}_{AB}^{(j_1)}$ is given by (3.11) with

$$\begin{aligned} D &= 2\lambda_{00}, & F &= \lambda_{11} + \lambda_{00}, \\ G &= 0, & H &= \lambda_{00} - \lambda_{11}. \end{aligned} \quad (3.24)$$

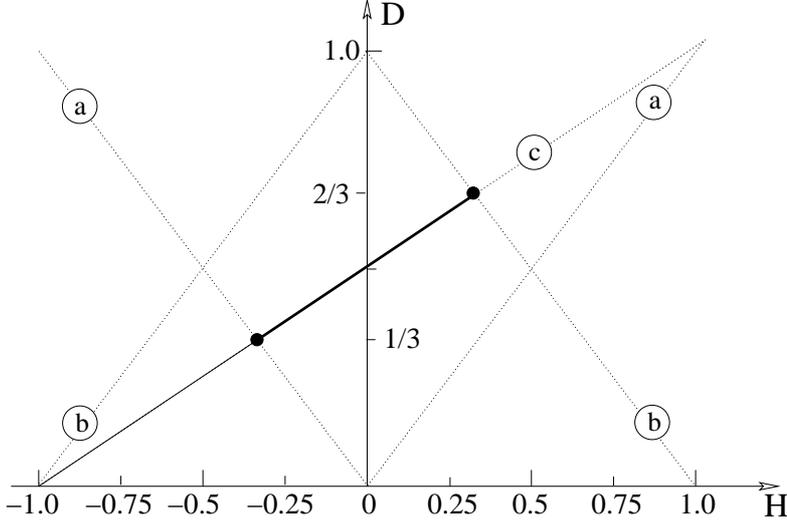


Figure 3.2: Six-state protocol: Region of the parameters D (QBER) and H for which the two-qubit state $\tilde{\rho}_{AB}^{(j_1)}$ is separable (thick solid line). The various constraints that these parameters satisfy are indicated by straight dotted lines. Specifically, (a) Eq. (3.17); (b) Eq. (3.16); (c) Eqs. (3.13) and (3.25). The protocol operates along the solid lines.

Accordingly, condition (3.14) now reads

$$F + H = D, \quad (3.25)$$

while non-negativity of the eigenvalues $\lambda_{\alpha\beta}$ implies inequality (3.16) only. Finally, applying the Peres-Horodecki criterion one finds that $\tilde{\rho}_{AB}^{(j_1)}$ is separable *if and only if* inequality (3.17) is satisfied.

As a consequence of Eqs. (3.13), (3.25) and $G = 0$, there is only one macroscopic independent parameter in our problem, say H , while combining inequalities (3.16) and (3.17) with Eqs. (3.13) and (3.25) one obtains that the reduced density operator $\tilde{\rho}_{AB}^{(j_1)}$ is separable *iff* $1/3 \leq D \leq 2/3$ (Figure 3.2). That is, no matter how powerful the eavesdropper is, Alice and Bob share always provable entanglement for estimated disturbances smaller than $1/3$. The lowest disentanglement border for the six-state scheme ($D_{\text{th}} = 1/3$) is attained for $H = -1/3$. It is also worth noting that, in contrast to BB84, in the six-state protocol there is only one disentanglement threshold since for $D > 2/3$ the protocol is not valid.

As expected, the bound for the six-state protocol is higher than the one for the BB84 protocol. In fact, as a consequence of the high symmetry of

the six-state protocol, the disentanglement area of the BB84 scheme (shaded region in Figure 3.1) shrinks to a line in Figure 3.2 (thick line). As will be seen later on, this “degeneracy” affects significantly the options of a potential eavesdropper in the framework of the six-state protocol, increasing thus the robustness of the protocol.

3.2 The price of disentanglement

In QKD issues, Eve’s attack is usually optimized by maximizing her Shannon information (or the probability of her guessing correctly Alice’s bit-string) conditioned on a fixed disturbance. Given, however, that the unconditional security of the BB84 and six-state cryptographic schemes is beyond doubt, Eve might be willing to reduce the robustness of the protocols to the lowest possible level while simultaneously maximizing any of her properties [AGS03]. Thus, what remains to be clarified now is the cost at which Eve can saturate the lowest disentanglement threshold D_{th} , in terms of her information gain and probability of correct guessing. To this end, one has to consider in detail the eavesdropping attack on the BB84 and the six-state protocols.

Such an investigation, however, is practically feasible only in the context of attacks on a few qubits. As the number of attacked qubit-pairs increases the complete treatment of the problem becomes intractable due to the large number of independent parameters involved. In this section the focus is on incoherent and two-qubit coherent attacks. The disentanglement of Alice and Bob in the framework of incoherent attacks has been extensively studied in the literature [GW99, GW00, AGS03, AMG03, Bru03]. In most of these studies, however, Eve’s attack is by default optimized to provide her with the maximal Shannon information. On the contrary, here all the flexibility is given to Eve to adjust her parameters in order to break entanglement between Alice and Bob and simultaneously maximize her properties. Finally, for the two QKD protocols under consideration, there is no related previous work on disentanglement in the context of coherent attacks.

3.2.1 Four-state protocol

Incoherent attacks

Incoherent attacks belong to the class of the so-called single-qubit or individual attacks, where Eve manipulates each transmitted qubit individually. To this end, she attaches a single probe (initially prepared in e.g. state $|0_E\rangle$)

to each transmitted qubit and lets the combined system undergo a unitary transformation of the form [FG⁺97, GR⁺02, CG97]

$$\begin{aligned} |0_B\rangle \otimes |0_E\rangle &\rightarrow \sqrt{F}|0_B\rangle \otimes |\phi_0\rangle + \sqrt{D}|1_B\rangle \otimes |\theta_0\rangle, \\ |1_B\rangle \otimes |0_E\rangle &\rightarrow \sqrt{F}|1_B\rangle \otimes |\phi_1\rangle + \sqrt{D}|0_B\rangle \otimes |\theta_1\rangle, \end{aligned} \quad (3.26)$$

with F and D being the fidelity and disturbance respectively, while $|\phi_j\rangle$ and $|\theta_j\rangle$ are normalized states of Eve's probe when Bob receives the transmitted qubit undisturbed (probability F) and disturbed (probability D), respectively. Applying unitarity and symmetry conditions on this transformation one finds that the states $|\phi_j\rangle$ are orthogonal to the states $|\theta_j\rangle$ ($j \in \{0, 1\}$), while the overlaps $\langle\phi_0|\phi_1\rangle$ and $\langle\theta_0|\theta_1\rangle$ are real-valued [FG⁺97, GR⁺02, CG97]. Thus, an incoherent attack can be described by the four parameters satisfying Eqs. (3.13), (3.14) (3.15) and (3.16) with $H = -F\langle\phi_0|\phi_1\rangle$ and $G = -D\langle\theta_0|\theta_1\rangle$. In other words, there are only two independent parameters and by fixing one of them, say D , one is able to determine any property of the attack. In Figs. 3.3, Eve's optimal information gain and probability of success in guessing the transmitted qubit correctly is given as functions of the disturbance (solid line). The optimization is performed in the usual way, i.e. for a fixed disturbance D , Eve's mutual information with Alice is maximized [FG⁺97, CG97]. It is also known that such an optimized strategy disentangles the qubits of Alice and Bob at $D^{(1)} \approx 30\%$ (vertical dotted line)[GW99], which is well above $D_{\text{th}} = 25\%$. Thus, the natural question arises is whether, under the assumption of incoherent attacks, Eve can saturate the lowest possible disentanglement border D_{th} and if yes, at which cost of information loss.

To answer this question, for a fixed disturbance D , all the possible values of G and H which are consistent with the constraints (3.13)-(3.16) and which yield a separable state of Alice and Bob are calculated numerically. In general, at any given disturbance there is more than one combination of values of G and H which fulfill all these constraints. For each of these combinations, we calculated Eve's information gain and her probability of correct guessing [FG⁺97, CG97]. The results presented as squares in Figs. 3.3, refer to those combinations of parameters which, not only disentangle the two honest parties for a particular disturbance D , but which simultaneously maximize Eve's property as well. Clearly, for disturbances close to D_{th} , the two strategies are not equivalent since they yield substantially different results. In other words, an optimal incoherent attack that maximizes Eve's information gain is certainly not the one which achieves the lowest possible robustness bound. Furthermore, our simulations show that saturation of $D_{\text{th}} = 1/4$ is feasible at the cost of $\sim 4\%$ less information gain of Eve or equivalently at the cost

of $\sim 7.44\%$ less probability of success in guessing.

Two-qubit coherent attacks

In a two-qubit coherent attack, Eve attaches one probe to two of the qubits sent by Alice. Let $|m_B\rangle$ with $m \in \{0, 1, 2, 3\}$, be the message sent from Alice to Bob in binary notation. The combined system then undergoes a unitary transformation of the form [CG97]

$$\begin{pmatrix} |0_B\rangle \\ |1_B\rangle \\ |2_B\rangle \\ |3_B\rangle \end{pmatrix} \otimes |0_E\rangle \rightarrow \mathcal{E} \otimes \begin{pmatrix} |0_B\rangle \\ |1_B\rangle \\ |2_B\rangle \\ |3_B\rangle \end{pmatrix}, \quad (3.27)$$

where \mathcal{E} is a 4×4 matrix which contains normalized states in the Hilbert space of Eve's probe

$$\mathcal{E} \equiv \begin{pmatrix} \sqrt{\alpha} |\phi_0\rangle & \sqrt{\beta} |\theta_0\rangle & \sqrt{\beta} |\omega_0\rangle & \sqrt{\gamma} |\chi_0\rangle \\ \sqrt{\beta} |\theta_1\rangle & \sqrt{\alpha} |\phi_1\rangle & \sqrt{\gamma} |\chi_1\rangle & \sqrt{\beta} |\omega_1\rangle \\ \sqrt{\beta} |\omega_2\rangle & \sqrt{\gamma} |\chi_2\rangle & \sqrt{\alpha} |\phi_2\rangle & \sqrt{\beta} |\theta_2\rangle \\ \sqrt{\gamma} |\chi_3\rangle & \sqrt{\beta} |\omega_3\rangle & \sqrt{\beta} |\theta_3\rangle & \sqrt{\alpha} |\phi_3\rangle \end{pmatrix}.$$

The states ϕ_j , θ_j , ω_j and χ_j denote Eve's probe states in cases in which Bob receives all the transmitted qubits undisturbed, one qubit disturbed or both transmitted qubits disturbed.

Applying unitarity and symmetry conditions on Eq. (3.27), the problem can be formulated in terms of the following four mutually orthogonal subspaces [CG97]

$$\begin{aligned} S_\phi &= \{\phi_0, \phi_1, \phi_2, \phi_3\}, & S_\chi &= \{\chi_0, \chi_1, \chi_2, \chi_3\}, \\ S_\theta &= \{\theta_0, \theta_1, \theta_2, \theta_3\}, & S_\omega &= \{\omega_0, \omega_1, \omega_2, \omega_3\}, \end{aligned}$$

while all the overlaps between the various states within each of these subspaces are real-valued. Thus, Eve is able to infer with certainty whether Bob has received both qubits undisturbed (S_ϕ), one qubit disturbed ($S_{\theta,\omega}$) or both qubits disturbed (S_χ). These events occur with probabilities α , 2β and γ , respectively. It can be shown that a general coherent two-qubit attack can be described in terms of five independent parameters [CG97]. The average reduced density matrix for Alice and Bob is then of the form (3.11), with $F = \alpha + \beta$, $D = \beta + \gamma$, $H = -(\alpha\langle\phi_0|\phi_1\rangle + \beta\langle\theta_0|\theta_2\rangle)$, $G = -(\gamma\langle\chi_0|\chi_1\rangle + \beta\langle\theta_0|\theta_1\rangle)$, satisfying the constraints (3.13), (3.14), (3.15) and (3.16).

Compared to an incoherent attack, a two-qubit coherent attack can improve the probability that Eve guesses correctly the whole two-bit message

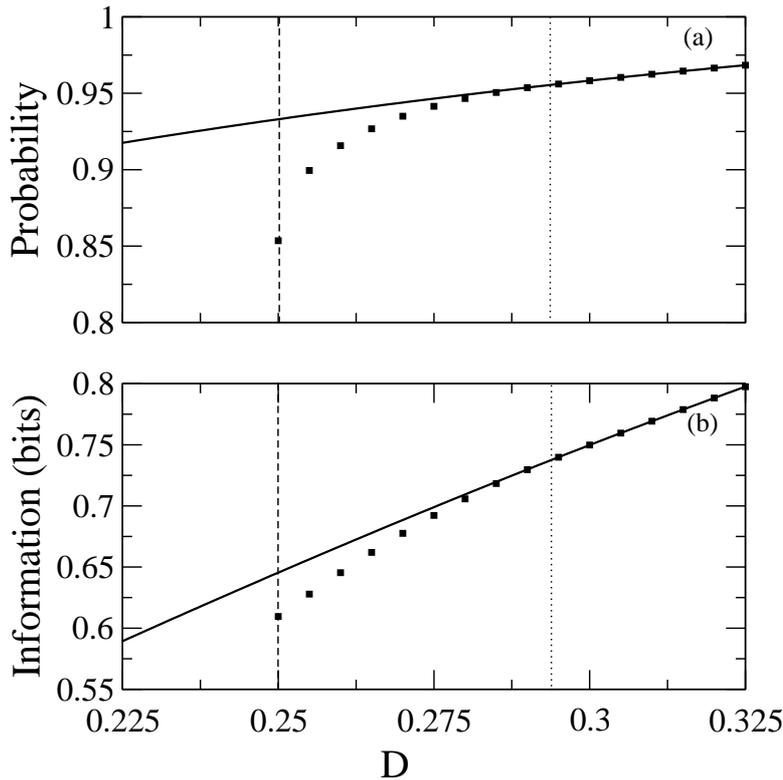


Figure 3.3: BB84 protocol — Incoherent attacks : (a) Eve’s probability of guessing correctly the transmitted message as a function of disturbance D . The solid line corresponds to an attack that maximizes Eve’s probability of success in guessing, while each square denotes the corresponding probability for an attack which in addition, disentangles Alice and Bob at the specific disturbance. (b) As in (a) but for Eve’s information gain. The vertical dotted lines correspond to the solid curves, and denote the disturbance $D^{(1)} \approx 30\%$ up to which Alice and Bob share an entangled state. The vertical dashed lines denote the lowest disentanglement threshold disturbance $D_{\text{th}} = 1/4$ which can be attained in the context of general coherent attacks and intercept-resend strategies.

sent by Alice to Bob [CG97]. Eve's optimal probability of success in guessing is plotted in Figure 3.4 (solid line), as a function of disturbance D . This curve has been obtained by maximizing Eve's probability of success in guessing conditioned on a fixed disturbance D . For such an optimal attack, it is found numerically that Alice and Bob share entanglement up to disturbances of the order of $D^{(2)} \approx 28\%$ (dotted vertical line). This is in contrast to the bound $D^{(1)} \approx 30\%$ attained in an optimal incoherent attack. Furthermore, it is also found that Eve is able to saturate the lowest possible robustness bound (dashed vertical line), at the cost of $\sim 3\%$ less probability of success in guessing. This loss of Eve's probability in guessing is substantially smaller than the corresponding loss for incoherent attacks ($\sim 7.44\%$). Thus, it could be argued that a two-qubit coherent attack which is optimized with respect to the probability of guessing only, is very close to an optimal coherent attack which also disentangles Alice and Bob at $D_{\text{th}} = 1/4$. The reason is basically that in a two-qubit coherent attack each one of the two independent macroscopic parameters G and H can be expressed in terms of two different overlaps whereas in incoherent attacks the corresponding dependencies involve a single overlap only. In a coherent attack Eve has therefore more possibilities enabling her to push the disentanglement border towards the lowest possible value, while simultaneously maximizing her probability of guessing correctly the transmitted message.

3.2.2 Six-state protocol

So far, incoherent and coherent attacks in the context of the BB84 protocol are considered where Eve's attack is determined by a set of two macroscopic parameters (G, H) . These two independent parameters give a considerable flexibility to Eve since at a given disturbance there exists a variety of physically allowed attacks. This fact is also reflected in Figure 3.1 where, for a specific disturbance, Alice and Bob can be disentangled for different values of H (and therefore of G).

In the highly symmetric six-state protocol, however, the situation is much simpler. In fact, the high symmetry of the protocol reduces significantly the options of an eavesdropper since there is only one independent macroscopic parameter in our problem, namely H . Moreover, the analysis of the attacks under consideration becomes rather straightforward [PG99]. In particular, for incoherent attacks $G = -D\langle\theta_0|\theta_1\rangle = 0$ which indicates that Eve has full information about the disturbed qubits received by Bob. However, as depicted in Figure 3.2, at a given value of D there is a unique value of H consistent with the laws of quantum mechanics. It is determined by Eqs. (3.13) and (3.25) [line (c) in Figure 3.2]. Similarly, for the two qubit

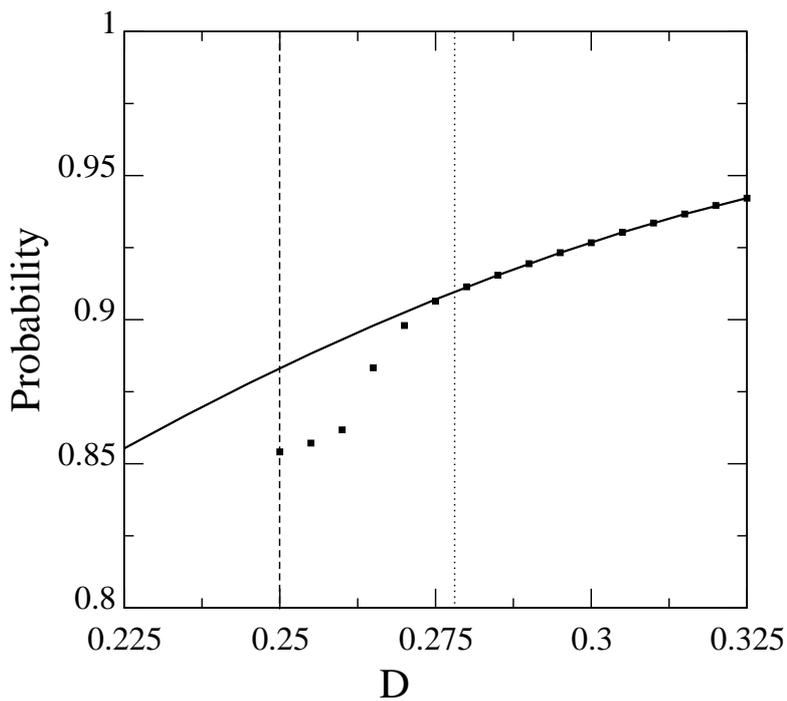


Figure 3.4: BB84 protocol — Two-qubit coherent attacks : Eve’s probability of guessing correctly a two-bit transmitted message as a function of disturbance D . The solid line corresponds to an attack that maximizes Eve’s probability of success in guessing only, while each square denotes the corresponding probability for an attack that, in addition, disentangles Alice and Bob at the specified disturbance. The vertical dotted line corresponds to the solid curve, and denotes the disturbance $D^{(2)} \approx 28\%$ up to which Alice and Bob share an entangled state. The vertical dashed line denotes the lowest possible disentanglement threshold disturbance $D_{\text{th}} = 1/4$ that can be attained in the context of general coherent attacks and intercept-resend strategies.

coherent attack one has $\langle \chi_0 | \chi_1 \rangle = \langle \theta_0 | \theta_1 \rangle = 0$ and thus $G = 0$, whereas $H = -(\alpha \langle \phi_0 | \phi_1 \rangle + \beta \langle \theta_0 | \theta_2 \rangle) = -(\alpha - \gamma) = 2D - 1$. As a result, for both incoherent and two-qubit coherent attacks, the physically allowed attack is the one that maximizes Eve's probability of guessing and simultaneously disentangles Alice and Bob at a given disturbance. It is sufficient for Eve therefore to optimize her attack with respect to her probability of correct guessing in order to disentangle Alice and Bob at the lowest possible disturbance.

3.3 Entanglement and intrinsic information

So far, the maximal disturbance up to which Alice and Bob share entanglement is discussed for both the four- and six-state protocols. Clearly, this bound indicates that in principle secret-key generation is feasible by means of a quantum purification protocol. In this section it is shown that, at least in the context of incoherent attacks, a two-way classical protocol, the so-called advantage distillation protocol, exists which can tolerate precisely the same amount of disturbance as a quantum purification protocol.

To this end, Maurer's model for classical key agreement by public discussion from common information [Mau93] is adopted. Briefly, in this classical scenario, Alice, Bob and Eve, have access to *independent* realizations of random variables X, Y and Z , respectively, jointly distributed according to P_{XYZ} . Furthermore, the two honest parties are connected by a noiseless and authentic (but otherwise insecure) channel. In the context of this model, Maurer and Wolf have shown that a useful upper bound for the secret-key rate $S(X; Y || Z)$ is the so called intrinsic information $I(X; Y \downarrow Z)$ which is defined as

$$I(X; Y \downarrow Z) = \min_{Z \rightarrow \bar{Z}} \{I(X : Y | Z)\},$$

where $I(X : Y | Z)$ is the mutual information between the variables X and Y conditioned on Eve's variable Z , while the minimization runs over all the possible maps $Z \rightarrow \bar{Z}$ [MW99].

For the current purposes, one can link this classical scenario to a quantum one. More precisely, the joint distribution P_{XYZ} can be thought of as arising from measurements performed on a quantum state $|\Psi_{ABE}\rangle$ shared between Alice, Bob and Eve. One has to, however, focus on incoherent attacks where Eve interacts individually with each qubit and performs any measurements before reconciliation. Thus, at the end of such an attack the three parties share independent realizations of the random variables X, Y and Z . Accordingly, the resulting mixed state after tracing out Eve's degrees of freedom

is of the form (3.11) where $H = -F\langle\phi_0|\phi_1\rangle$ and $G = -D\langle\theta_0|\theta_1\rangle$. It turns out [GW00] that the random variables X and Y are symmetric bits whose probability of being different is given by $\text{Prob}[X \neq Y] = D$ whereas Eve's random variable consists of two bits Z_1 and Z_2 . The first bit $Z_1 = X \oplus_2 Z$ shows whether Bob has received the transmitted qubit disturbed ($Z_1 = 1$) or undisturbed ($Z_1 = 0$). The probability that the second bit Z_2 indicates correctly the value of the bit Y is given by

$$\text{Prob}[Z_2 = Y] = \delta = \frac{1 + \sqrt{1 - \langle\phi_0|\phi_1\rangle^2}}{2}. \quad (3.28)$$

As has been shown by Gisin and Wolf [GW00], for the scenario under consideration secret key agreement is always possible *iff* the following condition holds

$$\frac{D}{1 - D} < 2\sqrt{(1 - \delta)\delta}. \quad (3.29)$$

More precisely, one can show that if the above condition is not satisfied, the intrinsic information vanishes whereas, in any other case there exists a classical protocol that can provide Alice and Bob with identical keys about which Eve has negligible information. Such a protocol, for instance is the so-called advantage distillation protocol which is described in detail elsewhere [Mau93].

In our case now, considering that Eve has adjusted the parameters in her attack to disentangle Alice and Bob at the lowest possible disturbance, Eq. (3.28) yields for the two protocols

$$\delta = \begin{cases} \frac{3+2\sqrt{2}}{6} & \text{BB84 protocol} \\ \frac{2+\sqrt{3}}{4} & \text{six-state protocol.} \end{cases}$$

Using these values of δ in Eq. (3.29) one then obtains bounds that are precisely the same with the threshold disturbances for provable entanglement derived in Section 3.2.1. In other words it is shown that, as long as Alice and Bob are entangled, a classical advantage distillation protocol is capable of providing them with a secret key, provided Eve restricts herself to individual attacks only (see also [AMG03, Bru03] for similar results).

This result is a manifestation of the link between quantum and secret correlations in both four- and six-state QKD protocols [CLL03, AG05]. For the time being, the validity of this equivalence between classical and quantum distillation protocols is restricted to individual attacks only. Investigations of tomographic QKD protocols have shown, however, that such an equivalence is invalid for coherent attacks.

Chapter 4

Practical Quantum Key Distribution

The discussion on achievable key generation rates and the bounds on performance of quantum key distribution protocols so far has assumed perfect source, quantum channel and detectors. With the present day available technology, neither of them are perfect. The source generally produces quantum signals in the form of weak coherent pulses which have a finite probability of having multiphoton pulses. An eavesdropper can take advantage of this lack of single photon pulses and she can imply more dangerous attacks. The channel connecting Alice and Bob is lossy. Eve can replace this with a perfect one and can even better her attack. The detector efficiency is less than unity and the detector has a finite probability of dark counts. These dark counts limit the distance up to which secure key can be transmitted.

In this chapter tagging attack is studied in detail. This attack has already been studied in various papers [GL⁺00, FG⁺01]. All this work has so far concentrated on one-way classical communication for post processing. It has been shown in [FG⁺01] that sudden dip in key generation rate is indeed because of dark counts. Here two-way classical communication is used to postpone disastrous effects of dark counts to a considerable distance without much loss of key rate. This attack is studied in non-trusted-device scenario.

In Sec. 4.1 practical limitations are discussed in detail. These limitations are general for all protocols. For the illustration of our results a specific model is then adopted and presented which consists of specific form of imperfections and source, detector and channel. It is then described how Eve can take advantage of these imperfections and employ tagging attack. In Sec. 4.2 the key generation rates using one-way classical communication are reviewed.

One-way classical communication is indeed limited both in key generation rate and distances. This limitation is obvious both for four- and six-state protocols. Further in Sec. 4.3, a way is devised to increase this distance and rate by using two-way classical communication for post processing. First the whole tagging attack scenario is visualized in entanglement-based picture. This allows further to visualize Alice and Bob's quantum states. The error rejection based on two-way classical communication then allows different pairing of tagged and untagged pairs. The numerical simulations for key generation rates are presented for four-state, six-state and corresponding decoy state protocols at the end of section.

4.1 Practical limitations and their fatalities in QKD

While considering practical limitations, it is pessimistically assumed that Eve has limitless power and she is restricted only by laws of physics. Alice and Bob are considered to have the present day technology only. With these limitations Eve can take advantage of Alice and Bob's faulty apparatus. There are three main factors in practical QKD: (i) Alice's source (ii) Channel connecting Alice and Bob and (iii) Bob's detector.

Optical quantum cryptography relies on the use of single photon sources. Such sources are practically difficult to realize. The present available sources use *faint laser pulses*, *entangled photon pairs*, *photon pairs by parametric down conversion* and *photon guns*. Both *faint laser pulses* and *entangled photons* generate photons which obey poissonian photon distribution. This means that both have a small probability of generating more than one photon. Even small fractions of these multiphoton pulses can have important effects on security, as will be discussed later. For weak laser pulses mean photon number must be chosen carefully. If mean photon number is too small most of the pulses are empty and detector's dark counts become effective. Mostly a mean photon number of 0.1 is used but more precisely an optimal mean photon based on transmission losses can be used. Although these states produce a key which is as secure as a single photon state but the bit rate is too low.

The problem of empty pulses is solved by the photon pairs generated by *parametric down conversion*. Here one photon is used as a trigger for the generation of other. Here a second detector triggers only when first detector has already detected a photon, hence mean photon number is 1. This way problem of empty pulses is circumvented. The photon pairs generated in

this method can be used as entangled pairs. If two photon pairs are emitted within the same time window but their basis are chosen totally independently, they produce totally uncorrelated results. These entangled pairs can be used in entanglement based cryptography or where their entanglement can be exploited. This way problem of multiphoton pulses can be avoided.

The ideal single photon device is a *photon gun*. Its a device which when a trigger is pulled, then and only then emits only one single photon. However presently available guns are far from ideal. At present there are three different methods to make a single photon gun. The first idea consists of using a two level atom. The available systems are single trapped atoms or ions but they require a lot technical effort. Single organic dye molecules are easier to handle but they have a problem of limited stability at room temperature. A good option is nitrogen-vacancy center in diamond. It is possible to excite individual nitrogen atoms with a 532-nm laser beam, which will subsequently emit a florescent beam of 700 nm. The florescence exhibits strong photon anti bunching and is stable at room temperature. However collection efficiency of such a gun is too low, currently around 0.1. In addition bandwidth of such a source is broad, currently of the order of 100 nm, which can enhance the effect of perturbations in quantum channel. The second idea is to generate photons by single electrons in a mesoscopic p-n junction. The idea is based on idea presented by Imamoglu and Yamamoto is based on Pauli exclusion principle that thermal electrons show antibunching. The experimental demonstrations have shown very low efficiency and at very low temperatures of only 50 mK. Another method of generating photons in photon guns is by photon emission in an electron-hole pairs in a semiconductor quantum dot. The frequency of the photons depends on the number of such electron hole pairs. Once a large number of such electron hole pairs are generated by optical pumping, they recombine to emit photons at different frequencies. Hence a single photon pulse is generated by spectral filtering. These dots can be integrated in solid state micro cavities but it then enhances spontaneous emission Thus photon guns are technically too complicated. In addition due to their low quantum efficiencies they practically offer no advantage over faint laser pulses with low mean photon number.

The single photons are carried to their detectors by quantum channels. The channels are called quantum because they are intended to carry information encoded in individual quantum signals. Here the term individual means that unlike classical systems where many photons carry the same information, information is encoded only once on quantum carriers.

Alice's source can have many limitations. There may be misalignment, polarization diffusion, fringe visibility and most importantly lack of single photon pulses. All optical quantum cryptography is based on single photon

Fock states. The source in general emits signal which follow poissonian distribution. Thus there is a finite probability of having more than one photon. Though Eve is not allowed to enter Alice's office but the channel connecting Alice and Bob is open to her. She can detach a photon from multiphoton while passing through the channel without disturbing the polarization of the photon. Thus she is able to do quantum non-demolition measurement. Lossy channel allows Eve to further take advantage of multiphotons. She can, in principle replace the channel with a lossless one and stop some of the single photon pulses. This way she increases the percentage of multiphotons in the final key. Since she keeps the expected click rate at Bob's detector the same, she remains undetected.

4.1.1 A model for imperfections

As stated earlier there are three main imperfections in the typical QKD implementation, the source, the channel and the detector. A model based on such imperfections has been thoroughly discussed in the literature [GR⁺02, Lut00, BL⁺00, FG⁺01].

In our case the model for source, channel and detector is taken as follows.

Source as weak attenuated laser pulse

Consider an imperfect source which with probability p_{tag} produces tagged qubits (signals). The tagged qubits are the ones from which Eve is capable of extracting the information that which random basis Alice used before their submission to Bob. Thus Eve is able to measure each one of these qubits in such a way that she can unambiguously determine its quantum state without disturbing the polarization state. This way she does not introduce any detectable errors. The remaining untagged signals are produced by Alice's source with probability $1 - p_{tag}$. These signals do not reveal full information to Eve and any intervention by Eve eventually introduces errors. Hence the overall bit error rate estimated by Alice and Bob during verification stage is due to untagged signals only. Here classical random sampling can be safely applied for the estimation of error rates and the establishment of related confidence levels during the verification test [LCA05]. Thus one can assume that the actual bit error rate in the pairs shared between Alice and Bob is the same as estimated by them in test pairs. The error rate is hence given as $\delta = (1 - p_{tag})\delta_{b,u}$, where $\delta_{b,u}$ is the probability with which an untagged qubit pair contributes to the overall bit error rate. Since there is symmetry between all the bases used in the QKD protocols under consideration, the

expected corresponding phase error probability, $\delta_{p,u}$, is the same as bit error one, i.e. $\delta_{p,u} = \delta_{b,u}$ and $\delta_{p,u} = \delta/(1 - p_{tag})$

A practically relevant special case of tagging is the signal sources currently used in various realistic set ups, which produce polarized phase randomized *weak coherent pulses* (WCPs) [GR⁺02, Lut00, BL⁺00, FG⁺01]. Both faint laser pulses and entangled photon pairs produce such pulses. The photon number distribution p_i ($i = 0, 1, \dots$) is Poissonian in this case, i.e. $p_i = \exp(-\mu)\mu^i/i!$, where μ denotes the mean photon number in the pulse. Alice encodes each of her random bit in a WCP and sends it to Bob. However, as is apparent from the distribution, in addition to single photon pulses there is a finite probability of pulses which contain more than one photon. Thus such a source deviates from ideal single photon source. The probability of having a single photon pulses is p_1 and that of multiphoton ones is $p_{tag} = 1 - p_0 - p_1$. As will be discussed later, Eve can obtain full information on all the bits encoded in multiphoton pulses by means of photon number splitting (PNS) attack. Thus for such a source multiphoton pulses are viewed as tagged and the single photon ones as untagged. Typically in WCP-based QKD protocols μ is chosen sufficiently small so that the source imitates a single photon source as closely as possible [GR⁺02]. This μ however cannot be taken too small because then dark counts of the detector become prominent. Thus μ has to be optimized for fixed distance [Lut00].

Imperfect quantum channels

In addition to imperfect signal sources, realistic set ups involve imperfect quantum channels and detectors. As a result the raw key rate P_{exp} is less than unity. P_{exp} is the probability of a single photon detection event to occur at Bob's site and sometimes referred as expected click probability. Some of the signals are lost in the lossy channel. The final click probability involves contributions both from real signals arriving at Bob's detector and from dark counts. In the adopted model, the probability for the former is given as $P_{exp}^{signal} = 1 - \exp(-\mu\eta_c\eta_{det})$, where η_c denotes the transmission efficiency of the channel and η_{det} is the detection efficiency of Bob's detector. The mean photon number in the P_{exp}^{signal} is thus reduced by factor $\eta_c\eta_{det}$. For QKD implementations at telecommunication wavelengths, η_{det} 0.1 – 0.2 and for quantum channels comprising of optical fibres

$$\eta_c = 10^{-(\alpha l + L_c)/10}. \quad (4.1)$$

Thereby, α denotes a polarization independent loss coefficient of the fibre, l is the length of the fiber, and L_c denotes the distance independent loss of the

channel.

Threshold detectors

The detectors available with present day technology are the threshold detectors. They give a click when an non-empty pulse arrives and do not click for an empty or vacuum pulse. The detectors hence cannot differentiate between single and multiphoton pulses. In addition the detector sometimes clicks even when there is no signal which results in dark counts. Though this dark count probability is very less $p_{exp}^{dark} \sim 2 \times 10^{-4} - 10^{-6}$ but it becomes effective at large distances when the actual signal probability becomes less as mentioned in Sec. (2.2.1). In this chapter two experimental setups are used, one from KTH stockholm [BG⁺99] and other called as GYS [GYS04], where author's name form the acronym. Both use avalanche photo diode (APD's), InGAs detectors for a signal with wavelength 1550nm. In KTH parameters the both the dark count probability, $p_{exp}^{dark} \sim 2 \times 10^{-4}$, and detection efficiency, $\eta_{det} \sim 0.18$, are high. GYS have used very low temperatures (-100C) which has enabled them to reduce dark counts to $p_{exp}^{dark} \sim 2 \times 10^{-6}$ but it makes detection efficiency quite low, $\eta_{det} \sim 0.045$. The effect on key generation rates can be seen in the coming sections.

Including above mentioned imperfections in source, channel and detectors, typically P_{exp} is given as [GR⁺02, Lut00, BL⁺00, FG⁺01]

$$P_{exp} = P_{exp}^{signal} + (1 - P_{exp}^{signal})P_{exp}^{dark} = 1 - e^{-\mu\eta c\eta_{det}} + e^{-\mu\eta c\eta_{det}} P_{exp}^{dark}. \quad (4.2)$$

For an ideal link involving a lossless channel and ideal detector, $P_{exp} = 1 - e^{-\mu}$.

The overall bit-error rate in the sifted key has also two contributions and is modeled by [GR⁺02, Lut00, BL⁺00, FG⁺01]

$$\delta = \delta_{opt} + \delta_{det} = \frac{\delta_0 P_{exp}^{signal} + \frac{1}{2} P_{exp}^{dark}}{P_{exp}}. \quad (4.3)$$

The first contribution is a measure of optical quality of the whole setup. In particular, the constant δ_0 accounts for possible alignment errors, polarization diffusion or fringe visibility. The second contribution δ_{det} , originates from dark counts at Bob's detectors. A factor of 1/2 indicates that in half such cases Bob's random measurement result would be differing from Alice. Hence, an error will be generated in half of the cases only. In the most pessimistic scenario usually adopted in security proofs, all the error rate δ is attributed to Eve. This pessimistic approach is the so called non-trusted device scenario.

Finally, any imperfections, losses, and noise significantly affect the fraction of tagged qubits arriving at Bob's site. In general, the new (effective) tagging probability Δ , can be expressed in terms of the parameters characterizing the channel, the source and the detectors. An upper bound on Δ , for example, may be obtained by the following consideration, in the case of a photon source emitting phase-averaged WCPs [Lut00, BL⁺00]. An eavesdropper, Eve, with unlimited power may not only obtain perfect information about all the classical bits originating from multiphoton pulses but she may also increase the fraction of these multiphoton pulses as much as possible without affecting Bob's expected click-rate probability. For this purpose she can replace the lossy quantum channel by a perfect one (i.e., $\eta_c = 1$) so that all multiphoton pulses are transmitted perfectly. In order to keep P_{exp} constant she has to block an appropriate number of single-photon pulses. Thus, the maximum probability of tagged pulses arriving at Bob's detector, which Eve can have perfect knowledge about, is given by [Lut00, BL⁺00]

$$\Delta \approx \frac{1 - (1 + \mu) \exp(-\mu)}{P_{\text{exp}}}, \quad (4.4)$$

while the corresponding probability for single-photon pulses is given by $(1 - \Delta)$, so that they sum up to unity.

4.2 Limitations of one-way post processing

Knowing the experimental setup it is now of interest to see the achievable rates and distances using one-way classical communication. As stated in Sec. 2.3.2, Gottesman, Lo, Lütkenhaus and Preskill (GLLP) have derived security of BB84 protocol in realistic scenario of tagging attack using one-way classical communication [GL⁺00]. The tagging attack is referred to as a weak basis dependent attack, that is where Eve already knows the basis of some of the signals, that is the tagged ones. They have shown that tagging does not make the key insecure, rather it only effects the key generation rates and distance up to which key is secure. For one-way CSS based post-processing the asymptotic rate is given as

$$R_{\text{CSS}} = \frac{P_{\text{exp}}}{\beta} [1 - \Delta - H(\delta) - (1 - \Delta) H(\delta_{\text{p,u}})]. \quad (4.5)$$

Here $H(x) := -x \log_2 x - (1 - x) \log_2(1 - x)$ is the binary shannon entropy. For the analysis of the key generation rates, GLLP have considered the most pessimistic scenario. It is called the *non trusted device scenario*. In this

scenario all errors including dark counts are attributed to Eve. Eve is in fact allowed to take advantage of dark counts as well. In addition she increases the percentage of tagged pulses in the ones reaching Bob by replacing the lossy channel by a perfect one. Thus the estimated bit error rate δ in equation (4.5) is coming only from untagged pulses and is given as $\delta = (1 - \Delta)\delta_{b,u}$. The phase error correction also includes all the errors in equation (4.3) and is given as

$$\delta_{p,u} = \delta/(1 - \Delta) \quad (4.6)$$

The expected click rate or the raw key rate P_{exp} is given by equation (4.2). The factor $1/\beta$ accounts for the fraction of raw bits thrown away during sifting process. Clearly for the four-state protocol $\beta = 2$ (two basis) and for six-state protocol (three basis) $\beta = 3$. In addition through out this work the correlations between bit flip and phase flip errors have not been considered. Such a consideration can increase the rate of six-state protocol but considering worst case scenario of no correlation, one can stick to the rate given by equation (4.5) for both protocols.

Using the analysis of GLLP, the typical key generation rate as a function of distance (i.e. the length l of the fiber) for BB84 and six-state protocol is given in Figure 4.1. The rate is given on logarithmic scale which shows a linear decrease before a cut off at about 25km is reached. This cut off is due to the presence of dark counts. The contribution to the error rate by actual signal pulses decreases as the length of fiber increases. As a result at a certain distance (25 km in this case), dark counts become the main contributor to error rate. Almost all the key is hence lost during error correction and privacy amplification. This point is clear by the dotted line which shows the key rate for four-state protocol in the absence of dark counts. It may be noted that both four- and six-state show the cut off at the same distance. However it can be increased for six-state protocol if correlations between bit and phase errors are taken into account.

The maximally tolerable error rates limit the distance up to which a secure key can be generated. Since Eve has full information about tagged pulses, its the error rate on untagged pulses which limits this distance. It has been shown in Chapter 3 that provable entanglement is necessary criteria for extraction of secure key. Thus if Alice and Bob can ensure the presence of such correlations in the untagged part of the key, they can ensure security. This is possible only if the corresponding error rate $\delta/(1 - \Delta)$ does not exceed $1/4$ for the four-state and $1/3$ for the six-state protocol i.e.

$$\frac{\delta}{1 - \Delta} < \frac{\beta - 1}{2\beta}, \quad \text{for } \beta \in \{2, 3\}. \quad (4.7)$$

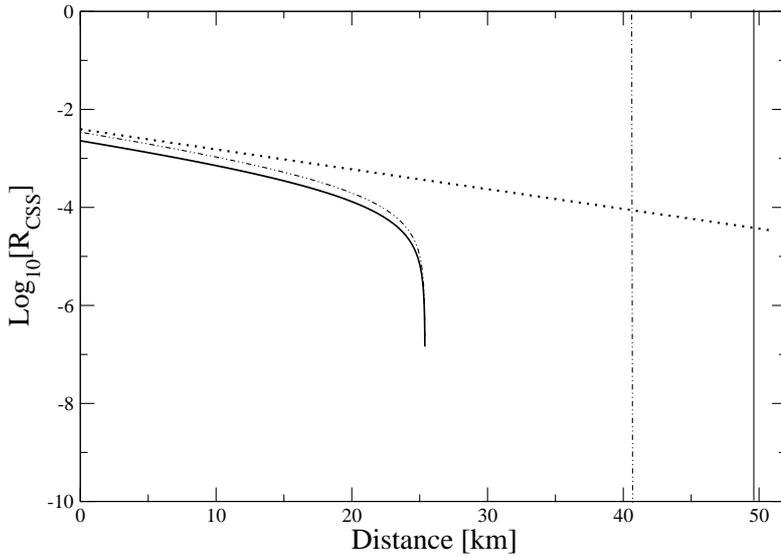


Figure 4.1: Achievable secret-key rates as given by equation (4.5), for non-ideal implementations of the four-state (full curve) and the six-state (dot-dashed curve) QKD protocols: Error correction and privacy amplification are performed by means of asymmetric CSS codes which involve one-way classical communication only. The vertical lines indicate the maximum allowed distances for secret-key generation as determined by equation (4.7) for the four-state (solid line at ~ 42 km) and the six-state protocol (dot-dashed line at ~ 50 km). Also shown is the secret-key rate of the four-state protocol in the absence of dark counts (dotted curve). All relevant parameters are chosen as in the experiment of Ref. [BG⁺99] i.e., $\alpha = 0.2\text{dB/km}$, $L_c = 1\text{dB}$, $\delta_0 = 1\%$, $P_{\text{exp}}^{\text{dark}} = 2 \times 10^{-4}$, and $\eta_{\text{det}} = 0.18$. The mean photon number μ is optimized at each distance so that the key generation rate is maximum

This is the generalized form of the necessary condition given in Chapter 3, in the absence of tagging. Indeed the intercept-resend attack by Eve can always break entanglement between Alice and Bob at an error rate $\delta \geq (1 - \Delta)(\beta - 1)/2\beta$.

Since both δ and Δ depend on length of the fiber, equation (4.7) limits the distance up to which secure key can be distilled. These distances are given by solid vertical lines for four-state and dotted vertical line for six-state protocol. Indeed the distance actually reached by one-way post processing is much less than this achievable distance. There is a gap of around 15 km for four-state protocol and that of 25 km for six-state protocol, between achieved and allowed distances. In the following sections it is shown how this gap can be decreased by using two-way post processing.

4.3 Practical QKD with two-way classical communication

Knowing the limited distance achieved by one-way post processing, an attempt is made to increase this distance. It has been found in Ref. [KNA06] that the upper bound on achievable distances can be reached if two-way post processing is used prior to the one-way. Two-way post processing involves error rejection by applying bilateral XOR gate on qubit pairs. This process reduces the error rates and positive rate is then achieved by applying CSS based post processing which is considered above. In order to see the effect of two-way post processing, a quantum approach is used in which the entanglement-based version of the four- and the six-state protocols are to be considered. This requires the derivation of reduced quantum state of Alice and Bob just before the post processing. For the purpose it is important to consider the effect of Eve's attack on Alice and Bob's system. In the non trusted device scenario all dark counts and channel losses will be given to Eve.

4.3.1 An Optimal Eavesdropping strategy

Tagging attack has already been discussed at the end of Sec. 4.1.1 where tagged qubits arrive at Bob's detector with probability Δ . Let N be the total number of qubits shared between Alice and Bob then for a fairly large sample (i.e. large value of N) it is expected that $N_u \approx (1 - \Delta)N$ pairs are untagged and $N_t \approx \Delta N$ are tagged pairs.

In an optimal attack by Eve, in this work no correlations between tagged and untagged signals are considered. As stated earlier Eve's aim is to max-

imize her information about Alice's and Bob's qubit pairs. She attains all information about tagged ones, then she attacks the remaining untagged ones separately. Each tagged qubit pair is also dealt separately. Nevertheless it seems an optimal strategy by Eve as she doesn't introduce any errors on the tagged ones and on untagged ones she applies any joint coherent attack. The coherent attack however introduces bit flip errors. Any attempt to jointly attack the tagged and untagged ones will increase the errors introduced by Eve. Keeping this in view the reduced state of Alice and Bob can be derived separately for tagged and untagged bits.

Attack on tagged qubits

Attack on tagged qubits can be divided into two parts. First Eve applies quantum non-demolition (QND) measurement to measure the photon number in each pulse. This way she is able to separate the multiphoton (tagged) pulses from the single photon (untagged) ones. This attack does not disturb the polarization of the photon. On multiphoton pulses she then attaches a probe to split one photon from each pulse without disturbing polarization. Such an attack can be described by Jaynes-Cummings Hamiltonian, where first Eve let a three level atom interact with the pulse coming from Bob. With known 'n' and fixed interaction time the atom exists in the one of the two polarization excited modes and an n photon pulse is left with one photon less. Eve then couples this atom to a field of her own which is in vacuum mode and adjusting the interaction time, her atom is left in ground state and field in polarization mode of Alice and Bob. In this way she is able to detach a photon and remains maximally entangled to Alice and Bob [Lut00].

Now in order to determine the reduced state of Alice and Bob for all tagged pairs, $\rho_t^{(N_t)}$, it is to be kept in mind that Eve attacks each pair separately. Hence the reduced state is left as a product state i.e. $\rho_t^{(N_t)} \approx \sigma^{\otimes N_t}$. It is thus sufficient to consider one of these qubit pairs. In entanglement based version after the distribution stage Alice announces which rotation I or H she has applied. Bob as well as Eve undo the rotation. The combined state of Alice, Bob and Eve in view of above mentioned photon splitting attack is given as

$$\begin{aligned} |\chi\rangle_{ABE} &= \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |0\rangle_B \otimes |\tilde{0}\rangle_E + |1\rangle_A \otimes |1\rangle_B \otimes |\tilde{1}\rangle_E) \\ &\equiv \frac{1}{\sqrt{2}} (|\Phi^+\rangle \otimes |0\rangle_E + |\Phi^-\rangle \otimes |1\rangle_E). \end{aligned} \quad (4.8)$$

Thereby, Eve's pure ancilla states $|0\rangle_E = (|\tilde{0}\rangle_E + |\tilde{1}\rangle_E) / \sqrt{2}$ and $|1\rangle_E = (|\tilde{0}\rangle_E - |\tilde{1}\rangle_E) / \sqrt{2}$ are orthogonal. The Bell state $|\Phi^-\rangle = (|0\rangle_A \otimes |0\rangle_B -$

$|1\rangle_A \otimes |1\rangle_B / \sqrt{2}$ characterizes the phase errors introduced by Eve's ideal attack. The equal amplitudes of magnitude $1/\sqrt{2}$ reflect the fact that Eve does not perturb Alice's and Bob's measurement statistics by her attack. Correspondingly, the reduced quantum state of Alice and Bob resulting from such an ideal attack is a random mixture of the ideal Bell state $|\Phi^+\rangle$ and the corresponding phase-flipped Bell state $|\Phi^-\rangle$, i.e.,

$$\sigma = \frac{1}{2}(|\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-|). \quad (4.9)$$

The separability of above state reflects the fact that Eve has a perfect copy of Bob's qubit and thus secret-key distillation is impossible [NKA06, CLL03, AG05].

Attack on untagged qubits

As discussed earlier, Eve is able to do any coherent attack on the untagged signals. In general the state obtained is a very complex state where the qubit pairs are not only entangled among themselves but also with Eve. Such a complex state is very difficult to analyze. However Alice and Bob apply a random permutation on all qubit pairs just after reception of qubits by Bob. If an entanglement purification protocol is applied in such a way that it commutes with Bell measurement then it has been proved in [GL03] that any coherent attack can be reduced to a Pauli attack and an uncorrelated Pauli attack gives the same fidelity as a correlated one. Since the final fidelity is the focus of interest, it is enough to consider the Pauli attack on a single qubit pair. A pauli attack applies operator \mathcal{X} with probability q_x , \mathcal{Z} with probability q_z and \mathcal{Y} with probability q_y . The state which results from an uncorrelated Pauli attack is the tensor product of individual qubit pair state i.e. $\rho_u^{(N_u)} = \tau^{\otimes N_u}$ and is a Bell diagonal state given as

$$\begin{aligned} \tau &= q_I |\Phi^+\rangle\langle\Phi^+| + q_z |\Phi^-\rangle\langle\Phi^-| \\ &+ q_x |\Psi^+\rangle\langle\Psi^+| + q_y |\Psi^-\rangle\langle\Psi^-|. \end{aligned} \quad (4.10)$$

The above state is rotation invariant under $\{\mathcal{I}, \mathcal{H}\}$ which puts an additional constraint on τ that $q_x = q_z$ for four-state protocol. For six-state protocol the state is invariant under $\{\mathcal{I}, \mathcal{T}, \mathcal{T}^2\}$ which puts an additional constraint that $q_x = q_y = q_z$.

Alice and Bob's point of view

It is assumed that Alice and Bob are not having Eve's technology. They only have threshold detectors which cannot distinguish between a single and

a multiphoton pulse. Thus they are unable to site the exact location of tagged and untagged pulses. As a result all qubit pairs appear identical to them. They just know that fraction Δ are tagged and $1 - \Delta$ are untagged. Formally speaking, Alice and Bob share N qubit-pairs in the quantum state

$$\rho_{\text{tot}}^{(N)} = \frac{1}{\Pi} \sum_{\Pi} \Pi (\sigma^{\otimes N_t} \otimes \tau^{\otimes N_u}) \Pi^\dagger, \quad (4.11)$$

where N_t and N_u are the number of tagged and untagged pairs respectively. The summation runs over all possible permutations and expresses Alice's and Bob's ignorance about the precise location of the tagged pairs within the block of N pairs. In the limit of large N , $N_u \approx (1 - \Delta)N$ and $N_t \approx \Delta N$, thus for Alice and Bob all pairs are in identical state ρ given as

$$\rho_{\text{tot}}^{(N)} \approx \rho^{\otimes N}, \quad (4.12)$$

where

$$\rho = \Delta\sigma + (1 - \Delta)\tau. \quad (4.13)$$

Now in order to estimate the bit error rate, Alice and Bob randomly sample their pairs and measure them along a common Z-basis. They then announce their result and determine in which cases the results differ. The overall bit error probability determined this way is given as

$$\delta = (1 - \Delta)\delta_{\text{b,u}} = (1 - \Delta)(q_x + q_y) \quad (4.14)$$

Here $\delta_{\text{b,u}}$ is the error probability for a single untagged pair and is determined by state τ .

4.3.2 Error rejection using two-way post processing

Having got the states for both tagged and untagged qubit pairs, one can apply the error rejection process to enhance the distance. For the purpose the two-way post processing is used. This two-way post processing is based on B-steps of Gottesman-Lo type [GL03, Ch02]. In the preceding work all the qubit pairs are taken to be identical. In the present scenario the pairs are no longer attacked the same way. Therefore one has to take into account the influence of B-steps on tagged and untagged pairs. The tagging probability changes with each B-step.

In a B-step Alice and Bob first pair up their EPR pairs i.e. they form tetrad of their qubit pairs. Within each tetrad they then apply a bilateral exclusive-OR operation (BXOR) operation. This operation is given as local

unitary operation $\text{XOR}_{a \rightarrow b} : |x\rangle_a \otimes |y\rangle_b \mapsto |x\rangle_a \otimes |x \oplus y\rangle_b$, on their halves. Thereby, \oplus denotes addition modulo 2 while a and b denote the control and target qubit, respectively. Accordingly, for the two qubit-pairs constituting the random tetrad it gives the following map in the Bell basis

$$\text{BXOR}_{a \rightarrow b} : |\Psi_{i,j}^{(a)}\rangle \otimes |\Psi_{x,y}^{(b)}\rangle \mapsto |\Psi_{i,j \oplus y}^{(a)}\rangle \otimes |\Psi_{i \oplus x,y}^{(b)}\rangle, \quad (4.15)$$

where $i, j, x, y \in \{0, 1\}$ and the Bell states are denoted by $|\Psi_{0,0}\rangle \equiv |\Phi^+\rangle$, $|\Psi_{0,1}\rangle \equiv |\Phi^-\rangle$, $|\Psi_{1,0}\rangle \equiv |\Psi^+\rangle$, and $|\Psi_{1,1}\rangle \equiv |\Psi^-\rangle$. Subsequently, Alice and Bob measure their target qubits (b) in the Z-basis and compare their outcomes. The target pair is always discarded while the control qubit-pair is kept if and only if their outcomes agree i.e., if and only if $i = x$. In general, this procedure is repeated many times (many rounds of B-step).

Alice and Bob now apply the above mentioned operation on their pairs. There are four different combinations in which qubit pairs can be paired up. A tagged control pair can pair up with tagged target pair as well as with untagged target pair. Vice versa an untagged control pair may pair up with both tagged and untagged target pairs, yielding different states. We will see that whenever an untagged pair is paired with a tagged one, the resulting state is a tagged pair as described below

Untagged target pairing up with Untagged control pair

For such a pairing both target and control pairs are in state given by equation (4.10). The probability for such pairing is $(1 - \Delta)^2$ as is evident from equation (4.13). The control pair is kept only if Alice and Bob's measurements agree. The BXOR operation maps the control pair to a renormalized Bell diagonal state given as [GL03]

$$\begin{aligned} q'_I &= \frac{(q_I + q_z)^2 + (q_I - q_z)^2}{2Q_{u,s}}, \\ q'_z &= \frac{(q_I + q_z)^2 - (q_I - q_z)^2}{2Q_{u,s}}, \\ q'_x &= \frac{(q_x + q_y)^2 + (q_x - q_y)^2}{2Q_{u,s}}, \\ q'_y &= \frac{(q_x + q_y)^2 - (q_x - q_y)^2}{2Q_{u,s}}, \end{aligned} \quad (4.16)$$

where $Q_{u,s} = (q_I + q_z)^2 + (q_x + q_y)^2$ is the probability with which the control qubit-pair is kept. Moreover, conservation of probability requires the relation $q_I + q_z + q_x + q_y = q'_I + q'_z + q'_x + q'_y = 1$.

Tagged target pairing up with tagged control pair

In view of equations (4.12-4.13) such a pairing takes place with probability Δ^2 . The two pairs are in the same Bell-diagonal state given by equation (4.9), and thus the map (4.16) applies also in this case. Setting $q_x = q_y = 0$ and $q_I = q_z = 1/2$, one has that the control pair always survives and is again tagged i.e., its state is given by (4.9).

Tagged target pairing up with untagged control pair

Such a pairing occurs with probability $\Delta(1 - \Delta)$. Using the map (4.15) and the form of the states τ and σ given by equations (4.10) and (4.9) respectively, one immediately obtains that for the case under consideration the control pair survives with probability $Q_{t,s} = (q_I + q_z)$ and is left in a quantum state of the form (4.9). Knowing that one of the purifications of such a state is equation (4.8), and giving all the purification to Eve [NC00], one may conclude that the state of the surviving control pair refers to the tagged state of equation (4.8). In other words, the initially untagged control pair becomes tagged when paired with a tagged target pair. This is equivalent to the XOR operation of an unknown classical bit S with a totally known classical bit M . Since the target bit $T = S \oplus M$ is announced publically, S becomes perfectly known to Eve.

Untagged target pairing up with tagged control pairs

This is equivalent to previous case.

Thus an untagged pair when pairs up with tagged ones gets tagged. The only case in which it results in an untagged pair is the one in which both target and control pairs are untagged. The fraction of tagged pairs goes on increasing with each B-step.

The survival probability for a qubit pair in the mixed quantum state of equation (4.13) with σ and τ given by equations (4.9) and (4.10) respectively, is given as

$$P'_s = (1 - \Delta)^2 Q_{u,s} + 2\Delta(1 - \Delta)Q_{t,s} + \Delta^2. \quad (4.17)$$

Moreover, its new quantum state is given by

$$\rho' = \Delta'\sigma + (1 - \Delta')\tau', \quad (4.18)$$

with the renormalized tagging probability

$$\Delta' = \frac{[\Delta^2 + 2\Delta(1 - \Delta)(q_I + q_z)]}{P'_s}, \quad (4.19)$$

and with the untagged renormalized quantum state

$$\begin{aligned}\tau' &= q'_I |\Phi^+\rangle\langle\Phi^+| + q'_z |\Phi^-\rangle\langle\Phi^-| \\ &+ q'_x |\Psi^+\rangle\langle\Psi^+| + q'_y |\Psi^-\rangle\langle\Psi^-|\end{aligned}\quad (4.20)$$

where the new probabilities (q'_I, q'_z, q'_y, q'_x) are determined by equations (4.16). Correspondingly, the bit-error probability of this new quantum state is given by

$$\delta' = (1 - \Delta')\delta'_{b,u} = (1 - \Delta')(q'_x + q'_y). \quad (4.21)$$

As a result of the B-step, however, the probabilities of bit and phase errors for an untagged qubit are not equal anymore. In particular, one has

$$\delta'_{p,u} = (q'_z + q'_I). \quad (4.22)$$

Consider now that immediately after one such B-step Alice and Bob switch to a one-way CSS-like EPP to distill a secret key. The overall asymptotically achievable secret-key generation rate is given by the corresponding modification of equation (4.5) i.e.,

$$R_{\text{BCSS}} = \frac{P_{\text{exp}} P'_s}{2\beta} (1 - \Delta' - H(\delta') - (1 - \Delta')H(\delta'_{p,u})), \quad (4.23)$$

where Δ' , δ' and $\delta'_{p,u}$ are given by equations (4.17-4.22). The additional factor of $1/2$ accounts for the target qubit-pairs which are always thrown away during the B-step. With the help of the recursion relations 4.16 and 4.19 asymptotically achievable secret-key generation rates can also be determined for cases in which B-steps are applied iteratively before the final use of the one-way CSS-like EPP. In that case, however, the factor of $1/2$ should be replaced by $1/2^n$, for n B-steps. The rate R_{BCSS} is therefore a generalization of the GLLP rate R_{CSS} to a post-processing where the one-way CSS-like EPP is initialized by a number of B-steps. Indeed, the rate 4.23 directly reduces to the rate 4.5 in the absence of B-steps i.e., by setting $(q'_I, q'_z, q'_y, q'_x) = (q_I, q_z, q_y, q_x)$, $P'_s = 1$, $\Delta' = \Delta$, and dropping the factor $1/2$.

4.3.3 Numerical simulations and discussion

In order to examine the effect of two-way post processing on key generation rates numerical simulations are performed. As stated above an eavesdropper is assumed to have unlimited technological powers. She can replace the lossy channel by a lossless one. In addition all the errors including dark counts are attributed to Eve. She can take advantage of these errors by adjusting them to her benefit.

Initial values for error rates q 's

In order to start numerical simulations the initial values for the error rates given in 4.16 are required. At the start of the EPP protocol the bit error rate is obtained by combining Eqs. 4.3 and 4.14 and is given as

$$\delta = (1 - \Delta)(q_x + q_y) = \frac{\delta_0 P_{\text{exp}}^{\text{signal}} + \frac{1}{2} P_{\text{exp}}^{\text{dark}}}{P_{\text{exp}}} \quad (4.24)$$

where P_{exp} , $P_{\text{exp}}^{\text{signal}}$ and Δ are given before. In order to enter the map 4.16 for B steps, one needs to know the quantities q_x , q_y, q_z and q_{I} explicitly. This can be obtained by taking into account various other constraints. The state 4.10 being a physical state must be normalized. The normalization condition reads

$$q_{\text{I}} = 1 - q_x - q_y - q_z. \quad (4.25)$$

In addition there is symmetry between all the bases used in the QKD protocols. In four-state protocol, the state must remain invariant under the transformation $\{\mathcal{I}, \mathcal{H}\}$ Hence one other constraint reads

$$q_x = q_z \quad (4.26)$$

Six-state protocol requires the invariance under $\{\mathcal{I}, \mathcal{T}, \mathcal{T}^2\}$ which requires

$$q_x = q_y = q_z \quad (4.27)$$

Thus for the six-state protocol the initial values of q_x , q_y, q_z and q_{I} are given explicitly as

$$\begin{aligned} q_x &= q_y = q_z = \frac{\delta_0 P_{\text{exp}}^{\text{signal}} + \frac{1}{2} P_{\text{exp}}^{\text{dark}}}{2(1 - \Delta)P_{\text{exp}}} \\ q_{\text{I}} &= 1 - \frac{3(\delta_0 P_{\text{exp}}^{\text{signal}} + \frac{1}{2} P_{\text{exp}}^{\text{dark}})}{2(1 - \Delta)P_{\text{exp}}}. \end{aligned} \quad (4.28)$$

On the contrary such a unique choice is not possible for four-state protocol. There is one open parameter $0 \leq q_y \leq 1$. However it is known that the map 4.16 gives least value of secret key rate and largest value of phase error rate for $q_y = 0$ [GL03]. Hence $q_y = 0$ gives the worst possible scenario for map 4.16 for four-state protocol. Thus for four-state protocol initial values can be chosen as

$$\begin{aligned} q_y &= 0, \\ q_x &= q_z = \frac{\delta_0 P_{\text{exp}}^{\text{signal}} + \frac{1}{2} P_{\text{exp}}^{\text{dark}}}{(1 - \Delta)P_{\text{exp}}}, \\ q_{\text{I}} &= 1 - \frac{2(\delta_0 P_{\text{exp}}^{\text{signal}} + \frac{1}{2} P_{\text{exp}}^{\text{dark}})}{(1 - \Delta)P_{\text{exp}}}. \end{aligned} \quad (4.29)$$

With these initial values one can perform the numerical simulations to see the effect of B steps followed by one-way CSS codes on key generation rates. It is to be noted that in both four- and six-state protocols, all the error rates are distance dependent. As the distance increases, the losses increase and Eve gains more power and knowledge about the key. She is able to take full advantage of all losses, noise and inefficient detectors.

Experimental parameters

Since the aim of this work is to explore the effect of B-steps on dark counts, it is of interest to consider two sets of parameters. As described above in KTH parameters [BG⁺99] the probability of dark counts is relatively high, i.e. of the order of 10^{-4} and detector inefficiency is low, of the order of 0.18.

The theme of the entanglement distillation protocol is to apply one-way CSS like post processing until it works. Once the cutoff is reached then B-steps are applied until the error rates are low enough that again one-way post processing can be applied. For shorter distances one-way post processing alone is enough. The distance between Alice and Bob is represented by the length of optical fibre connecting Alice and Bob. At shorter distance the secret key rate is determined by equations (4.3), (4.5) and (4.6). However as the distance increases B-steps must be applied and then the corresponding key generation rate is given by equation (4.23) combined with equations (4.17-4.22). The initial condition for error rates for B-steps are given by equation (4.29) for four-state protocol and by equation (4.28) for six-state protocol. In both the cases the mean photon number is optimized at each distance to get maximum possible secret-key rate.

The influence of different number of B-steps is depicted in Figure 4.2 for four-state protocol and in Figure 4.3 for six-state protocol. For $n = 0$, i.e. no B-step and one-way post processing alone, the significant rate is achieved only up to 25 km for both protocols. This distance increases significantly with one application of B-step. Just one application of B-step increases this distance to 30 km for four-state protocol and to 34 km in the six-state protocol. In addition at each application of B-step there is a sudden increase in key generation rate. This is because the B-step decreases the bit-error rate significantly and this makes the effect of dark counts less significant. This effect of dark counts however becomes dominant again as the distance increases. This results in a new dip in key generation rate. An application of second B-step then increases the key generation rate again. However for increasing number of B-steps, this effect becomes less dominant as the phase error probability of the untagged pairs increases after each B-step and dark counts become more effective in phase error part. It can also be noticed that

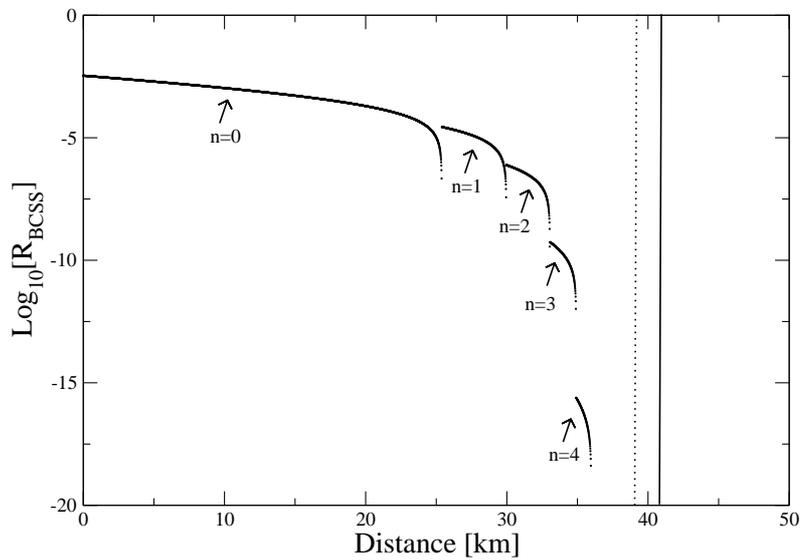


Figure 4.2: Four-state protocol: The secret key generation rates resulting from multiple application of B-steps followed by one-way CSS based post processing. Here n indicates the number of B-steps required prior to one-way post processing. The solid vertical line indicates the maximum allowed distance according to inequality 4.7 and the dotted line is the asymptotically achievable distance by inequality (4.31). The parameters are the same as for Figure 4.1

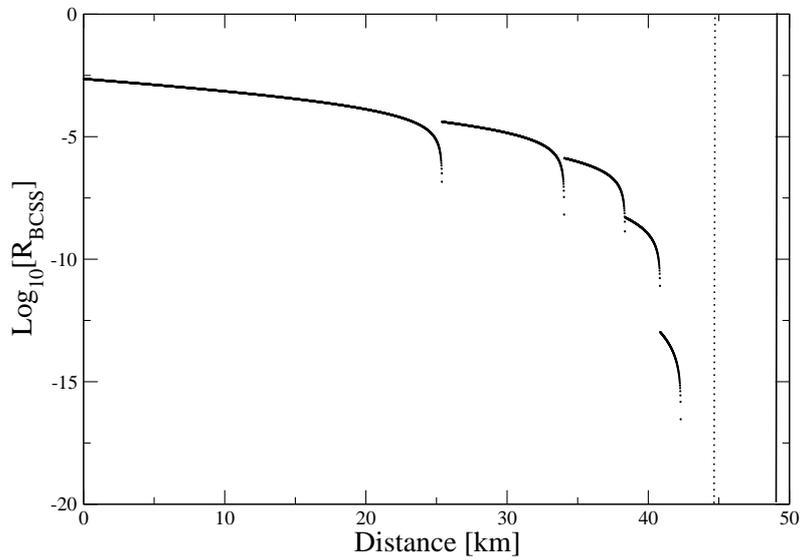


Figure 4.3: Six-state protocol: The parameters are the same as for four-state protocol in Figure 4.2. n denotes the number of B-steps applied

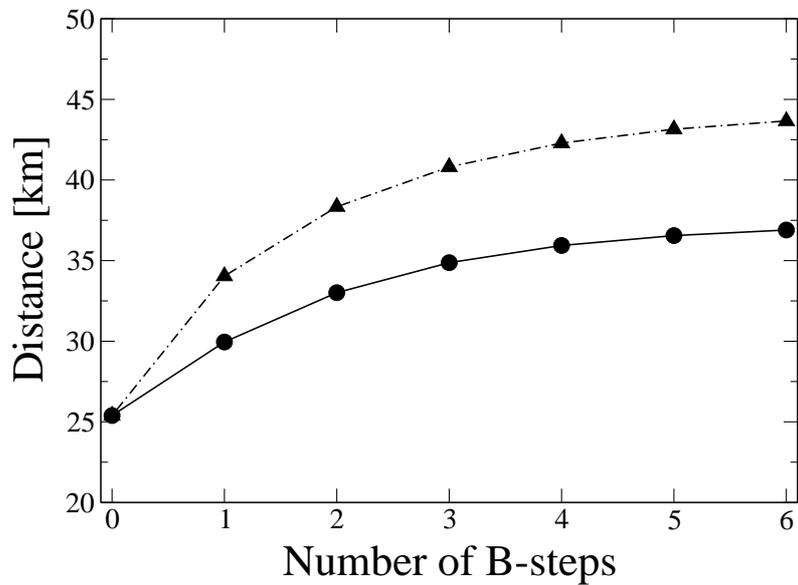


Figure 4.4: Maximum achievable distance for different numbers of B-steps for the four-state (lower curve) and the six-state protocol (upper curve).

in six-state protocol each application of B-step results in larger distance with lesser decrease in secret-key rate as compared to four-state protocol. This is because six-state protocol can sustain higher error rates.

The maximum possible distance reached with each B-step is depicted in Figure 4.4. The maximum distance tends to saturate for around 37km for four-state protocol and 44km for six-state protocol after six B-steps. This effect indicates that there is a limit to which B-steps together with one-way CSS can work. The maximum possible reachable distances are given by equation (4.7) after which Alice and Bob are no more sharing an entangled state. However there is another limit on achievable distance up to which B-step can work. This limit is provided by [RA06]. Since tagged pairs are already known it is enough to concentrate on purification of untagged pairs alone. If two-way post processing consists of just B-steps followed by CSS code then it has been shown [RA06] that the inequality

$$\left(q_1 - \frac{1}{4}\right)^2 + \left(q_z - \frac{1}{4}\right)^2 > \frac{1}{8}, \quad (4.30)$$

is the necessary condition for the purification of Bell diagonal state of the form 4.10. Therefore from equations (4.24-4.27), inequality (4.30) yields

$$\Delta < \begin{cases} 1 - 5\delta & \text{four-state protocol} \\ \frac{1}{2}(2 - 5\delta - \sqrt{5}\delta) & \text{six-state protocol.} \end{cases} \quad (4.31)$$

These borders are depicted by dotted vertical lines in Figures 4.2 and 4.3

In Figure 4.5 the possible values of tagging probability Δ and error probability δ are plotted. Both Δ and δ are the quantities which Alice and Bob can measure in the beginning and they can decide whether they should apply the suggested entanglement purification protocol or not. These plots are consistent with inequalities (4.7) and (4.31). According to the necessary condition (4.7) secret-key distillation is not possible in the black region. However there is a small grey region which is not accessible by B-steps followed by one-way CSS, although in principle allowed by 4.7. Thus having initial values of Δ and δ in white region Alice and Bob can confidently start the B-steps followed by one-way CSS like post processing.

It is clear from Figures 4.2, 4.3 and 4.4 that the maximum allowed threshold distances are already reached after a few B-steps. It is therefore enough to apply a few B-steps without much loss in secret-key rates. These secret-key rates however fall steeply for higher number of B-steps.

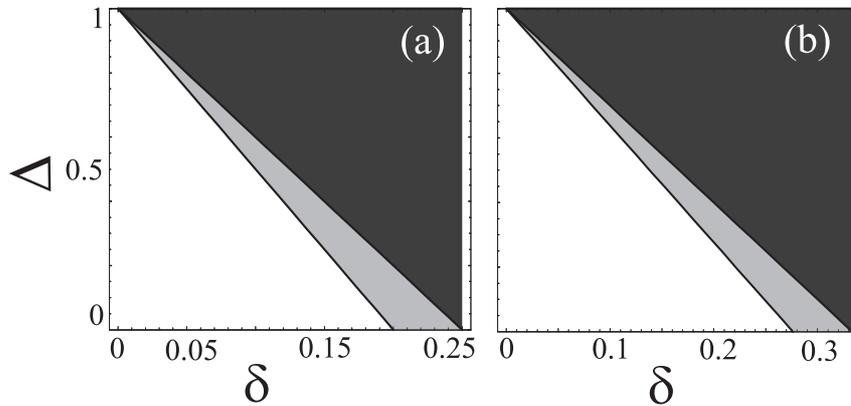


Figure 4.5: Regions bounded by equations (4.7) (white+grey) and (4.31) (white) for the four-state (a) and the six-state (b) QKD protocols. Secret key distillation is not possible by any means in the black region. The grey region is not accessible to B-steps and CSS-like EPP.

Effect of B-steps on decoy state protocol

It is now of interest to explore the influence of B-steps on decoy state protocols. Decoy state protocols are developed to suppress imperfections arising from multiphoton pulses. Alice and Bob can get a lower bound on the yield of single photon pulses by comparing the total yield of decoy pulses before starting the experiment. Decoy state protocol has been explained in Sec. (2.2.1), we briefly explain it again for the sake of completeness.

The yields of single and multiphoton pulses of both decoy and signal pulses is the same. Consider a decoy state protocol involving two decoy weak coherent pulses with mean photon numbers κ and ν and signal pulse with mean photon number μ . The values of kappa and mu are fixed so that these pulses fulfill the requirements $\kappa < \nu$ and $\kappa \exp(-\kappa) < \nu \exp(-\nu)$ and $\mu > \kappa + \nu$. Let s_1 be the probability that the detector clicks provided a single photon pulse hits it and s_m be the click probability of detector when multiphoton pulse hits it. Clearly these probabilities or yields are the same for all decoy and signal pulses. The probabilities $P_{\text{exp}}^{(\kappa)}$ and $P_{\text{exp}}^{(\nu)}$ of the decoy pulses to be detected at the detector obey the relation [Wan05, MQ+05]

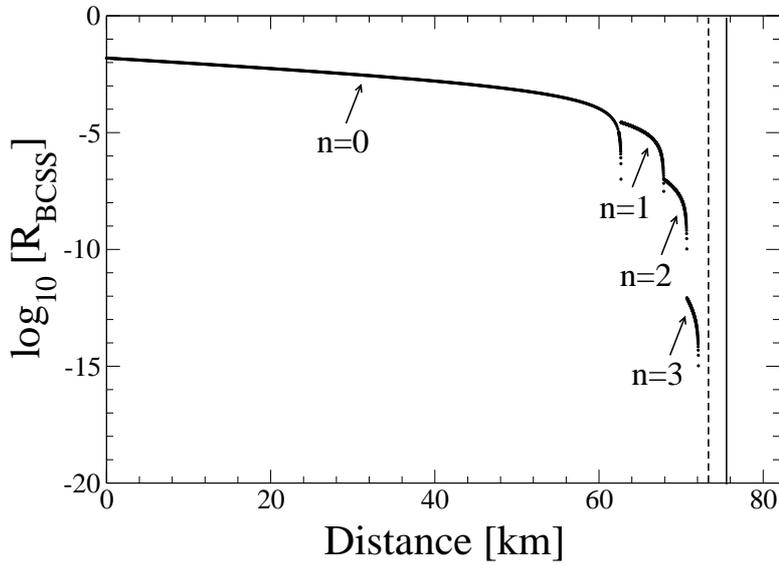


Figure 4.6: Four-state protocol with decoy pulses: The parameters are the same as in Figure 4.2, while $\mu = 0.55$, $\kappa = 0.10$, and $\nu = 0.27$.

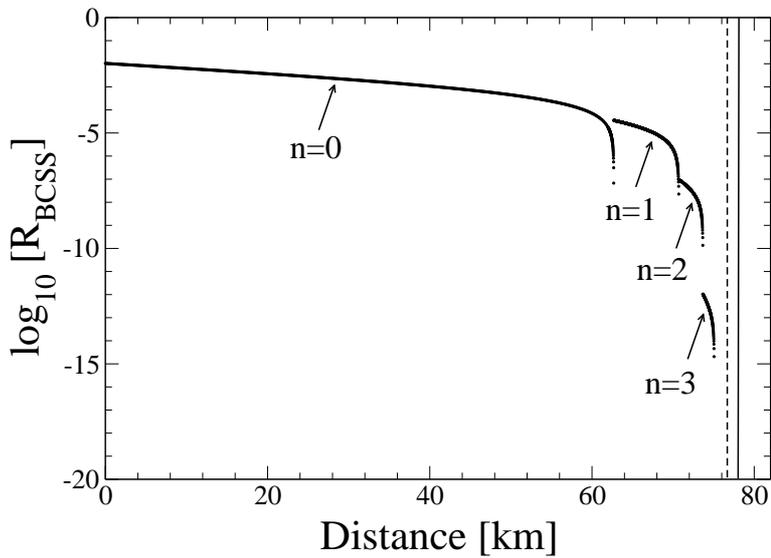


Figure 4.7: Six-state protocol with decoy pulses: The parameters are the same as in Figure 4.6.

$$\begin{aligned}
P_{\text{exp}}^{(\kappa)} &= P_{\text{exp}}^{\text{dark}} e^{-\kappa} + s_1 \kappa e^{-\kappa} + s_m (1 - e^{-\kappa} - \kappa e^{-\kappa}), \\
P_{\text{exp}}^{(\nu)} &\geq P_{\text{exp}}^{\text{dark}} e^{-\nu} + s_1 \nu e^{-\nu} + s_m (1 - e^{-\kappa} - \kappa e^{-\kappa}) \frac{\nu^2 e^{-\nu}}{\kappa^2 e^{-\kappa}}.
\end{aligned} \tag{4.32}$$

Thereby $P_{\text{exp}}^{\text{dark}}$ is the probability of dark counts and can be exactly determined if Alice sends a decoy vacuum pulse in between. Using above relations one obtains

$$s_1 \geq \frac{\nu^2 e^{\kappa} P_{\text{exp}}^{(\kappa)} - \kappa^2 e^{\nu} P_{\text{exp}}^{(\nu)} - (\nu^2 - \kappa^2) P_{\text{exp}}^{\text{dark}}}{\kappa \nu (\nu - \kappa)} := \bar{s}_1. \tag{4.33}$$

Since the signal single photon pulse has the same probability of being detected at the detector, the probability Δ_μ of multiphoton signal pulse can be upper bounded as follows

$$\Delta_\mu \leq 1 - \frac{\bar{s}_1 \mu e^{-\mu}}{P_{\text{exp}}^\mu} := \tilde{\Delta}_\mu \tag{4.34}$$

In particular, a lower bound on the resulting secret-key generation rate is obtained from equations (4.16), (4.17), (4.19), (4.21), and (4.23). Thereby, the recursive relations have to be solved by setting $\Delta = \tilde{\Delta}_\mu$ in the initial conditions (4.28) and (4.29) for the six- and the four-state protocol, respectively. These initial conditions take into account that the phase-error probability can be bounded from above by $\delta/(1 - \tilde{\Delta}_\mu)$. The resulting lower bound on the secret-key generation rate and its dependence on the length of the optical fibre used for the transmission of photons are depicted in figures 4.6 and 4.7 for the four- and the six-state protocol, respectively. Following ref. [Wan05], μ , κ and ν are chosen to be equal to 0.55, 0.10 and 0.27, respectively. Typically, multiple application of B-steps increase the distance over which a secret key can be exchanged significantly. The maximum distances and their dependence on the number of applied B-steps is shown in Figure 4.8 for both protocols with decoy pulses. The asymptotically achievable maximum distances of the order of 80 km are reached already after a few B-steps. Moreover, it is worth noting that the net increase in distance of about 15 km (after 2 or 3 B-steps) is the same as that for the conventional four- and six-state protocols.

Experimental parameters with low dark count rate

The main aim of this work had been to see the postponement of dark count effects. It is therefore of interest to explore the case where dark counts are

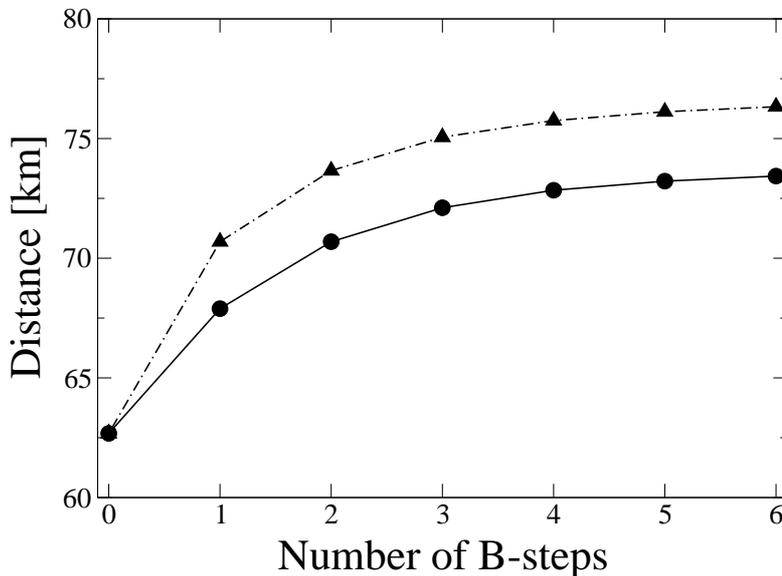


Figure 4.8: Maximum achievable distances for different numbers of B-steps for the four-state (lower curve) and the six-state (upper curve) protocols with decoy pulses.

already too low. Following the experimental set up by the ref. [GYS04], the dark counts are 10^{-2} times lower than the previous parameters. As stated earlier such low dark counts occur by lowering the temperature which results in very low detection efficiency, of the order of $\eta_{\text{det}} = 0.045$. The resulting key generation rates are shown in Figure 4.9. It is clear that low dark counts already enhance the distance without any B-steps to a considerable value. The low detection efficiency does not affect this enhancement much. The achieved distance by one-way classical communication alone is already too close to the maximum achievable distance. Thus the percentage increase in distance is not much compared to one-way post processing.

In conclusion the use of two-way classical communication which mainly consists of inclusion of CNOT operation (the B-steps) has increased the distance considerably for both four- and six-state protocols. As mentioned above the main aim of B-steps is to postpone the effect of dark counts which had been the main hindrance in protocols based on one-way post processing.

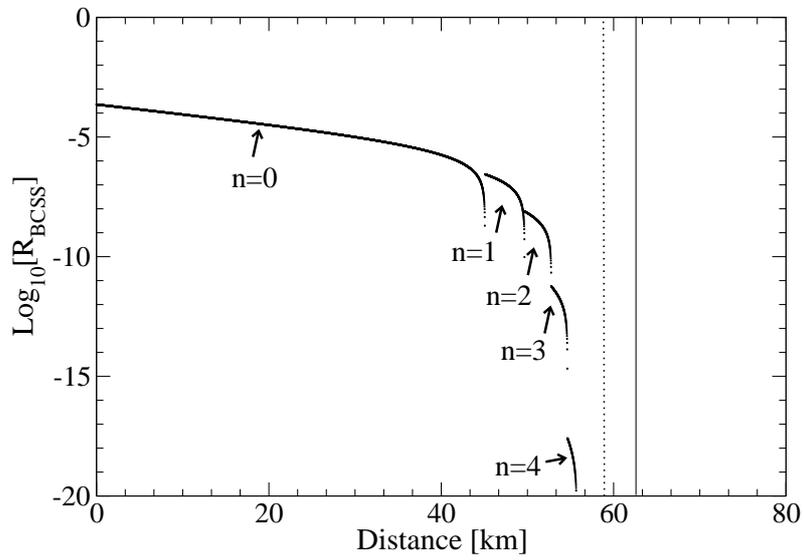


Figure 4.9: Secret key generation rates for four-state protocol. $P_{\text{exp}}^{\text{dark}} = 2 \times 10^{-6}$ and $\eta_{\text{det}} = 0.045$. The rest of the parameters are same as in Figure 4.2

Chapter 5

Concluding Remarks

The thesis successfully compiles the major results on robustness bounds on performance of ideal quantum key distribution protocols and use of two-way classical communication to enhance the distance up to which secret key can be distributed for the corresponding protocols with major practical limitations. For both purposes the entanglement-based versions reducible to corresponding prepare and measure protocols are used.

For robustness bounds it has been shown that legitimate users share provable entanglement only for disturbance $D < 25\%$ and $D > 75\%$ for the four-state and for $D < 33\%$ for the six-state protocol. This limitations restricts the entanglement sharing region in a plot of combination of amplitudes of Bell diagonal states. For the four-state protocol the disentanglement or separable state region is bounded by four lines whereas for the six-state protocol it is reduced to a line due to the additional constraint coming from the presence of third basis. It is then shown how an adversary Eve can reach these bounds. In general analysis of eavesdropping attacks, it is the Shannon information of Eve which is maximized. In our case we analyze how much sacrifice Eve has to make on her probability of correct guessing and/or information gain. This analysis is done for incoherent attacks and two-qubit coherent attack for the four-state protocol. It turns out that for incoherent attack the saturation of the threshold disturbance $D = 25\%$ is possible by Eve at the cost of 4% less information gain by Eve or equivalently at the cost of 7.44% less correct probability of guessing. For two-qubit coherent attack this threshold disturbance bound is achievable at the cost of 3% less correct probability of guessing which is substantially lower than the incoherent attack. Moreover for maximizing both information gain and probability of correct guessing, the legitimate users get disentangled at $D = 30\%$ for an incoherent attack and at $D = 28\%$ for two-qubit coherent attack. For the six-state protocol the physically allowed attack is the one which maximizes Eve's probability

of correct guessing and simultaneously disentangles the legitimate users for both incoherent and two-qubit coherent attacks.

In the analysis of practical quantum key distribution the practical limitations considered are presence of multiphoton pulses which exhibit poissonian behavior. The lossy quantum channel is taken to be optical fibre having exponential loss. The detectors are the threshold detectors which are the click or no-click detectors with some probability of producing a click even in the absence of actual signal. This later clicking is called dark count. In this scenario two-way classical communication is introduced which involves the addition of B-steps or CNOTs when one way classical communication fails. The B-step reduces the error rates to a value where one-way post processing can take over. So the key-generation rates are given by the same GLLP bound just including the fraction of pairs discarded in each case. Due to the presence of multiphoton pulses all pairs are not identically treated as in the preceding works but Eve tags the multiphoton pairs and the single photon ones remain untagged. During B-step any pair pairing up with tag pairs becomes totally known to Eve. Inclusion of this important aspect further increases the number of bits known to Eve. Then the privacy amplification process needs to be done only on single photon pulses. We have shown that inclusion of B-steps enhances the distance of secure communication to about 80% for four-state and to 100% for six-state protocol. The important observation during above analysis was that actually inclusion of a B-step enables to, some extent, overcome only the dark counts. The key rate suddenly falls again when the dark counts again become effective. Thus B-steps postpone the effect of dark counts to some distance. The analysis is done for four- and six-state and the corresponding decoy-state protocols. Since decoy state protocols are already designed to overcome the effect of dark counts, the increase in distance is not as pronounced as for the four- and six-state protocols. It is worth noting that the effect of dark counts can never be suppressed, they can only be postponed.

In a recent development [MS07] in the field of practical quantum key distribution, the same technique of using B-steps is implemented to show quantum key distribution using passive decoy state selection. Though their source and detectors are different than proposed by us but the results definitely show that indeed B-steps are an efficient mean of enhancing distances up to which secret key can be distributed between legitimate users. They have used standard parametric down conversion to produce photon sources which exhibit both poissonian and thermal statistics in extremal cases. The detection process involves time multiplexed detection (TMD) since it is cost effective and easy to handle experimentally. The legitimate users need to discard all slots in the postprocessing stage where the TMD result was zero

and use the inverted probability distribution in the rate calculations. Since this type of filtering is applied in the postprocessing phase, it does not modify the actual signal transmission and no physical blocking is required.

Appendix A

Numerical Program for Practical QKD Using Two-way Classical Communication

The fortran program is given which is used in numerical simulations for practical QKD.

program: Two-way practical QKD with KTH parameters

```
implicit none
integer i,imax,B,distmax,Bstep
real dist,ddist,log2,Rate_opt,golden
real ax,bx,cx,tol,etadet,etac,alpha,Lc,P0,mu,Pdark,nu
common/bla/B
common/xs/etac,etadet,alpha,Lc,P0,Pdark
common/stp/Bstep
external RCSS,RBCSS
Character data4
```

Choosing protocol: B=2 BB84, B=3 Six-state

B=2

Initial Values:

```
ddist=1d0/100d0
distmax=44
imax=distmax/ddist
```

Constant parameters:

```
etadet=0.18d0
alpha=0.2d0
Lc=1d0
P0=0.01d0
Pdark=2d0*1d-4
Bstep=0
do 30 dist=0d0,distmax,ddist
do 30 i=0,imax,1
dist=i*ddist
etac=10^(-(alpha.dist+Lc)/10d0)
```

For golden initial values:

```
ax=0d0.etadet.etac
bx=1d0.etadet.etac
cx= 2d0.etadet.etac
tol=1d-5

if(Bstep.eq.0) then
Rate_opt = golden(ax,bx,cx,RCSS,tol,mu)
else
Rate_opt = golden(ax,bx,cx,RBCSS,tol,nu)
endif

if(Rate_opt.lt.0) then
open(14,file=data4,access='append')
write(14,*) dist,log(-Rate_opt)/log(10d0)
close(14)
else
Bstep=Bstep+1
endif

30 continue

stop

end
```

NUMERICAL_RECIPES ROUTINE FOR MINIMIZATION:

```

FUNCTION golden(ax,bx,cx,f,tol,xmin)
REAL golden,ax,bx,cx,tol,xmin,f,R,C
EXTERNAL f
PARAMETER (R=.61803399,C=1.-R)
REAL f1,f2,x0,x1,x2,x3

x0=ax
x3=cx

if(abs(cx-bx).gt.abs(bx-ax))then
  x1=bx
  x2=bx+C*(cx-bx)
else
  x2=bx
  x1=bx-C*(bx-ax)
endif

f1=f(x1)
f2=f(x2)

1  if(abs(x3-x0).gt.tol*(abs(x1)+abs(x2)))then
    if(f2.lt.f1)then
      x0=x1
      x1=x2
      x2=R.x1+C.x3
      f1=f2
      f2=f(x2)
    else
      x3=x2
      x2=x1
      x1=R.x2+C.x0
      f2=f1
      f1=f(x1)
    endif
    goto 1
  endif

if(f1.lt.f2)then

```

```

        golden=f1
        xmin=x1
    else
        golden=f2
        xmin=x2
    endif

    return

    END

```

FUNCTION RCSS:

```

    Real Function RCSS(mu)
    implicit none
    integer B
    Real etac,alpha,Lc,etadet
    Real mu,Pexp,Delta,Pdark,PexpSignal
    Real pz,px,py,p,P0
    Real H,x,y
    Common/bla/B
    Common/xs/etac,etadet,alpha,Lc,P0,Pdark

```

Basic Formulas:

```

    PexpSignal=1d0-exp(-(mu*etac*etadet))
    Pexp=PexpSignal+Pdark-PexpSignal*Pdark
    Delta=(1d0-(1d0+mu).exp(-mu))/Pexp

```

Error probability:

```

    p=(P0.PexpSignal+(Pdark/2d0))/Pexp

    If (B.eq.2) then
        py=0d0                ! BB84
        px=p
        pz=p
    else
        py=p/2d0              ! Six-state
        px=p/2d0
        pz=p/2d0
    endif

```

```

endif

x=px+py
y=((pz+py)-(Pdark/2d0)/Pexp)/(1d0-Delta)
RCCS=-Pexp.(1d0-Delta-H(x)-(1d0-Delta).H(y))/B

return

end

```

RBCSS:

```

Real Function RBCSS(mu)
implicit none
integer B,j,Bstep
Real8 etac,alpha,Lc,etadet
Real mu,Pexp,Delta,Pdark,PexpSignal
Real px,py,pz,pi,p,P0,px1,pi1,py1,pz1
Real H, x,y
Real Ps,Qus,Qts
common/xs/etac,etadet,alpha,Lc,P0,Pdark
Common/stp/Bstep
Common/bla

```

Basic Formulas:

```

PexpSignal=1d0-exp(-(mu.etac.etadet))

Pexp=PexpSignal+Pdark-PexpSignal.Pdark

Delta=(1d0-(1d0+mu).exp(-mu))/Pexp

```

Error probability:

```

p=(P0.PexpSignal+(Pdark/2d0))/Pexp

If (B.eq.2) then
  py=0d0 ! BB84
  px=p/(1-Delta)
  pz=p/(1-Delta)

```

```

        pi=1d0-px-py-pz
    else
        py=p/2d0/(1-Delta)      ! Six-state
        px=p/2d0/(1-Delta)
        pz=p/2d0/(1-Delta)
        pi=1d0-px-py-pz
    endif

do 33 j=1,Bstep,1

Qus = (pi+pz).(pi+pz)+(px+py).(px+py);
Qts = (pi+pz);
Ps = (1-Delta).(1-Delta).Qus+2.Delta.(1-Delta).Qts+Delta.Delta;
Delta = (Delta*Delta+2*Delta*(1-Delta)*(pi+pz))/Ps;
pz1 = 2.0.pi.pz/Qus;
px1 = (px.px+py.py)/Qus;
py1 = 2.px.py/Qus;
pi1 = 1d0-px1-py1-pz1;
pi = pi1
px = px1;
py = py1;
pz = pz1;

33 continue

x = (1-Delta)*(px+py);
y = pz+py-(Pdark/2d0)/Pexp;
RBCSS=-Pexp.Ps.(1d0-Delta-H(x)-(1d0-Delta).H(y))/(2d0^Bstep)/B

return

end

```

Entropy:

```

Real Function H(x)
implicit none
Real x,logbase

H=-x.logbase(x)-(1d0-x).logbase(1d0-x)

```

```
return
```

```
end
```

CHANGE OF LOG TO THE BASE e TO 2:

```
Real Function logbase(x)
```

```
implicit none
```

```
Real x
```

```
if(x.lt.1d-100) then
```

```
    logbase=0d0
```

```
else
```

```
    logbase=log(x)/log(2d0)
```

```
endif
```

```
return
```

```
end
```


Bibliography

- [AG05] A. ACÍN, N. GISIN
Phys. Rev. Lett. **94**, 020501 (2005).
- [AGS03] A. ACÍN, N. GISIN AND V. SCARANI
Quant. Info. Comp. **3**, 563 (2003)
- [AMG03] A. ACÍN, L. MASANES AND N. GISIN
Phys. Rev. Lett. **91**, 167901 (2003).
- [BB84] C.H. BENNETT, G. BRASSARD
in *Proceedings IEEE International Conference on Computers, Systems and Signal Processing, Bangalore* (New York:IEEE, New York, 1984), p. 175.
- [BB⁺95] C.H. BENNETT, G. BRASSARD, C. CREPEAU AND U.M. MAURER
IEEE Trans. Inf. Theory **41**, 1915 (1995).
- [BBM92] C.H. BENNETT, G. BRASSARD AND N.D. MERMIN Phys. Rev. Lett. **68**, 557 (1992).
- [BB⁺96] C.H. BENNETT, G. BRASSARD, S. POPESCU, B. SCHUMACHER, J.A. SMOLIN, W.K. WOOTERS
Phys. Rev. Lett. **76**, 722 (1996).
- [BD⁺96] C.H. BENNETT, D.P. DIVINCENZO, J.A. SMOLIN, W.K. WOOTERS
Phys. Rev. A **54**, 3824 (1996).
- [BG⁺99] M. BOURENNANE, F. GIBSON, A. KARLSSON, A. HENING, P. JONSON, D. LJUNGGREN, E. SUNDBERG
Optics Express **4**, 383 (1999).

- [BL⁺00] G. BRASSARD, N. LÜTKENHAUS, T. MOR, B.C. SANDERS
Phys. Rev. Lett. **85**, 1330 (2000).
- [Bru98] D. BRUSS
Phys. Rev. Lett. **81**, 3018 (1998).
- [Bru03] D. BRUSS *et. al.*
Phys. Rev. Lett. **91**, 097901 (2003).
- [BS94] G. BRASSARD AND L. SALVAIL
in *Advances in Cryptology — EUROCRYPT '93 Proceedings, Lecture Notes in Computer Science*, edited by T. Helleseeth (Springer Verlag, New York) **765**, p. 410, (1994).
- [Ch02] H.F. CHAU
Phys. Rev. A **66**, 060302 (2002).
- [CK78] I. CSISZÁR AND J. KÖRNER
IEEE Trans. Inf. Theory **IT-24**, 339 (1978).
- [CLL03] M. CURTY, M. LEWENSTEIN, N. LÜTKENHAUS
Phys. Rev. Lett. **92**, 217903 (2003).
- [CG97] I. CIRAC AND N. GISIN
Phys. Lett. A **229**, 1 (1997).
- [Coc97] W.G. COCHRAN
Sampling Techniques (John Wiley & Sons, New York, 1997).
- [CS96] A.R. CALDERBANK AND P.W. SHOR
Phys. Rev. A **54**, 1098 (1996).
- [DE⁺96] D. DEUTSCH, A. EKERT, R. JOZSA, C. MACCHIAVELLO, S. POPESCU, A. SANPERA
Phys. Rev. Lett. **77**, 2818 (1996).
- [FG⁺97] C.A. FUCHS, N. GISIN, R.B. GRIFFITHS, C.S. NIU AND A. PERES
Phys. Rev. A **56**, 1163 (1997).
- [FG⁺01] S. FELIX, N. GISIN, A. STEFANOV AND H. ZBINDEN
J. Mod. Opt. **48**, 2009 (2001).
- [GL03] D. GOTTESMAN AND H.K. LO
IEEE Trans. Inf. Theory **49**, 457 (2003).

- [GL⁺00] D. GOTTESMAN, H.-K. LO, N. LÜTKENHAUS AND J. PRESKILL
Quantum Inf. Comput. **4**, 325 (2004).
- [GM94] M.J. GANDER AND U.M. MAURER
On the secret-key rate of binary random variables, In proceedings of
IEEE international symposium on information theory, 351 (1994).
- [GP01] D. GOTTESMAN AND J. PRESKILL
Phys. Rev. A **63**, 022309 (2001).
- [GR⁺02] N. GISIN, G. RIBORDY, W. TITTEL AND H. ZBINDEN
Rev. Mod. Phys. **74**, 145 (2002).
- [GW99] N. GISIN AND S. WOLF
Phys. Rev. Lett. **83**, 4200 (1999).
- [GW00] N. GISIN AND S. WOLF
in *Proceedings CRYPTO 2000 Lecture Notes in Computer Science*,
(Springer Verlag, Heidelberg), **1880**, 482.
- [GYS04] C. GOBBY, Z.L. YUAN AND A. J. SHIELDS
Appl. Phys. Lett. **84** 3762 (2004).
- [Ham04] M. HAMADA
J. Phys. A **37** 8303 (2004).
- [Hen02] M. HENDRYCH
Experimental Quantum Cryptography Doctoral Thesis Olomouc
(2002).
- [HHH96] M. HORODECKI, P. HORODECKI AND R. HORODECKI
Phys. Lett. A **223**, 1 (1996).
- [ILM01] H. INAMORI, N. LÜTKENHAUS AND D. MAYERS
e-print arXiv:quant-ph/0107017.
- [KNA06] A. KHALIQUE, G.M. NIKOLOPOULOS AND GERNOT ALBER
Eur. Phys. J. D **40**, 453 (2006).
- [KP02] M. KOASHI AND J. PRESKILL
Phys. Rev. Lett. **90**, 057902 (2002).
- [Lo01] H.K. LO
Quant. Info. Comput. **2**, 81 (2001).

- [Lo01] H.K. LO
J. Phys. A. **34**, 6957 (2001).
- [Lut00] N. LÜTKENHAUS
Phys. Rev. A. **61**, 052304 (2000).
- [LC99] H.K. LO AND H.F. CHAU
Science **283**, 2050 (1999).
- [LCA05] H.K. LO, H.F. CHAU AND M. ARDEHALI
J. Cryptology **18**, 133 (2005); see also quant-ph/0011056.
- [LJ02] N. LÜTKENHAUS AND M. JAHMA
New J. Phys. **4**, 44 (2002).
- [Mau93] U. MAURER
IEEE transactions on information theory,**39**, 733 (1993).
- [May01] D. MAYERS
Journal of ACM **48**, 351 (2001).
- [MW99] U. MAURER AND S. WOLF
IEEE Trans. Inf. Theory **45**, 499 (1999).
- [MS07] W. MAUERER AND C. SILBERHORNE
Phys. Rev. A **75**, 050305 (2007).
- [MQ⁺05] X. MA, B. QI, Y. ZHAO AND H.-K. LO
Phys. Rev. A **72**, 012326 (2005).
- [NA05] G.M. NIKOLOPOULOS AND G. ALBER
Phys. Rev. A **72**, 032320 (2005).
- [NKA06] G.M. NIKOLOPOULOS, A. KHALIQUE AND G. ALBER
Eur. Phys. J. D **37**, 441 (2006).
- [NC00] M.A. NIELSEN AND I.L. CHUANG
Quantum computation and Quantum Information (Cambridge University Press, cambridge, 2000).
- [Pe96] A. PERES
Phys. Rev. Lett. **77**, 1413 (1996).
- [PG99] H. BECHMANN-PASQUINUCCI AND N. Gisin
Phys. Rev. A **59**, 4238 (1999).

- [Ran05] K. RANADE
Quantenkryptographie und Verschränkung Diplom Thesis, Darmstadt (2005).
- [RA06] K. RANADE AND G. ALBER
J. Phys. A **39**, 1701 (2006).
- [RSA78] R.L. RIVEST, A. SHAMIR, AND L.M. ADLEMAN
Communications of the ACM **21**, 120 (1978).
- [Sin01] S. SINGH
The Code Book. How to make It, Break It, Hack It, Crack It (Dela-corte Press, New York, 2001).
- [Sha49] C.E. SHANNON
Bell Syst. Tech. J **28**, 656 (1949).
- [Ste96] A.M. STEANE
Proc. Roy. Soc. Lond. A **452**, 2551 (1996).
- [Sho94] P.W. SHOR
in Proc. 35th Annual Symposium on Foundations of Comp. Science, IEEE, Bellingham, P.124 (1994).
- [SP00] P.W. SHOR AND J. PRESKILL
Phys. Rev. Lett. **85**, 441 (2000).
- [Tho02] S.K. THOMPSON
Sampling (John Wiley & Sons, New York, 2002).
- [VS⁺01] L.M.K. VANDERSYPEN, M. STEFFEN, G. BREYTA, C.S. YAN-NONI, M.H. SHERWOOD AND I.L. CHUANG
Nature **414**, 883 (2001).
- [Wan05] X.B. WANG
Phys. Rev. A **72**, 012322 (2005).
- [Wie97] MICHAEL WIENER
An Update, RSA Laboratories Cryptobytes **3**, 6 (1997).

Acknowledgement

The research leading to this thesis has been carried out in Theoretische Quantenphysik group at Technische Universität Darmstadt under the supervision of Prof. Gernot Alber. I am grateful to Prof. Alber for providing me the opportunity to work in a learning and inspiring environment in his group.

I am indeed very much grateful to Prof. Norbert Lütkenhaus for all the discussions and guidance on my work. The inspiring discussions with him kept me motivated for my work. I thank Prof. Barbara Drossel for refereeing and to Prof. Robert Roth for co-refereeing my thesis. Special thanks to Prof. Thomas Walther and Prof. Friedemann Kaiser for all their help and support.

I also thank all the previous and present members of Theoretische Quantenphysik group at TU Darmstadt for the unique atmosphere throughout the years. Particular thanks to Georgios Nikolopoulos for being available for all scientific and moral support. Without him it would not have been possible for me to finish this work. Thanks are also due to Kedar Ranade for all the scientific discussions and help. I would also like to express my warmest thanks to Oliver Kern, Oliver Zobay and Joseph Renes for being there for all academic and non-academic support.

I deeply acknowledge the understanding, help and care of my friends Pallavi Thiagarajan, Achim Gädke and Florian Greil throughout my PhD work.

I am obliged to Deutscher Akademischer Austauschdienst (DAAD) for partially supporting my PhD work and my stay in Germany.

I am indeed indebted to my family specially my parents, my sister Uzma Khaliq and my friend Naureen Ghafoor for their love and support throughout my PhD work and in all the difficult times.

Curriculum Vitae

AEYSHA KHALIQUE

Institut für Angewandte Physik aykhalique@yahoo.com

Technische Universität Darmstadt

Hochschulstr. 4a

D-64289 Darmstadt, Germany

FIELDS OF INTERESTS

Research Interests: Quantum optics and quantum information; especially quantum cryptography and key distribution and foundations of quantum mechanics.

Other Interests: Quantum chaos, computational physics.

EDUCATION

MPhil Physics, Quaid-e-Azam University Islamabad May 2001.

Thesis: *Quantum non-demolition state measurement using atomic scattering*

Supervisor: Prof. Dr. Suhail Zubairy

Advisor: Asst. Prof. Farhan Saif

MSc, Physics, Quaid-e-Azam University Islamabad Pakistan 1998.

BSc, Physics/Mathematics/Statistics, F.G Girls College, Rawalpindi Pakistan 1995.

FSc, Pre-Medical/Mathematics, F.G Girls College, Rawalpindi Pakistan 1992.

School, Fazaia Inter College, Chaklala Pakistan 1990.

RESEARCH EXPERIENCE

Oct. 2003–July 2007	PhD student Group of G. Alber, Technische Universität Darmstadt, Germany In quantum cryptography
June 2001–June 2003	Research associate at Quaid-e-Azam University Group of Asst. Prof. Farhan Saif, Islamabad, Pakistan In quantum chaos and information theory
Feb. 2000– June 2001	MPhil research fellow at Quaid-e-Azam University Group of Prof. Dr. Suhail Zubairy, Islamabad, Pakistan In quantum optics

TEACHING EXPERIENCE

April 2005–July 2005	Teaching Assistant for Basic Quantum Mechanics lecture course for Bachelor students at Technische Universität Darmstadt, Germany
Dec. 2001–Feb. 2002	Lecturer for Basic Physics course to Software Engineers at NIIT, National University of Science and Technology
Sep. 2001–Dec. 2001	Lecturer for Basic Physics course to Bachelors of Computer Sciences at ICBCS campus of Indiana Pollis College
Jan. 2001–June 2001	Lecturer for Basic Physics course to Software Engineers at MCS, National University of Science and Technology Rawalpindi Pakistan
March 1998–June 1999	Teacher for Physics and Mathematics to O Levels at Khaldunia High School Islamabad Pakistan
Aug. 1995–Jan. 1996	Teacher for Physics, Mathematics and Biology to 9th/10th and Urdu to 3rd Grade at The State School Chaklala Pakistan

PUBLICATIONS

4. A. Khalique, G. M. Nikolopoulos and G. Alber,
*Postponement of dark-count effects in practical quantum key-
distribution by two-way post processing*,
Eur. Phys. J. D. **40**, 453 (2006)

3. G. M. Nikolopoulos, A. Khalique and G. Alber,
Provable entanglement and information cost for qubit-based quantum key distribution protocols
Eur. Phys. J. D **37**, 441 (2006)
2. A. Khalique and F. Saif,
Engineering entanglement in external degrees of freedom of atoms via atomic scattering in Bragg regime
Phys. Lett. A. 314, **37** (2003)
1. A. Khalique and F. Saif, *Quantum non-demolition state measurement via atomic scattering in Bragg regime*
J. Phys. Soc. Jpn. **71**, 2587 (2002)

CONFERENCES ATTENDED

International conferences on quantum information:
Trieste 2004, München 2004, Vienna 2005, Darmstadt 2005, Frankfurt 2006,
Cochem 2007.

AWARDS

DAAD fellowship for doctoral programme in TU Darmstadt, 2003–2005.

PROFESSIONAL ACTIVITIES

Member of Deutsche Physikalische Gesellschaft.

PERSONAL DETAILS

Born 10 March 1974 in Sargodha, Pakistan. Pakistani Citizen.
Language abilities: English, German, Urdu (national), Saraiki (native)

Hiermit erkläre ich an Eides Statt, dass ich die vorliegende Disseration selbständig verfasst und nur die angegebenen Hilfsmittel verwendet habe. Ich habe bisher keinen Versuch unternommen, an einer anderen Hochschule das Promotionsverfahren einzuleiten.

Darmstadt, im Juni 2008