*Article*

# Intercept-Resend Emulation Attacks against a Continuous-Variable Quantum Authentication Protocol with Physical Unclonable Keys

**Lukas Fladung** [1] , **Georgios M. Nikolopoulos** [1,2,*] , **Gernot Alber** [1] **and Marc Fischlin** [3]

[1]  Institut für Angewandte Physik, Technische Universität Darmstadt, D-64289 Darmstadt, Germany; lukasfladung@gmx.de (L.F.); gernot.alber@physik.tu-darmstadt.de (G.A.)
[2]  Institute of Electronic Structure and Laser, FORTH, P.O. Box 1385, GR-70013 Heraklion, Greece
[3]  Cryptoplexity, Technische Universität Darmstadt, D-64289 Darmstadt, Germany; marc.fischlin@cryptoplexity.de
[*]  Correspondence: nikolg@iesl.forth.gr

**Abstract:** Optical physical unclonable keys are currently considered to be rather promising candidates for the development of entity authentication protocols, which offer security against both classical and quantum adversaries. In this work, we investigate the robustness of a continuous-variable protocol, which relies on the scattering of coherent states of light from the key, against three different types of intercept–resend emulation attacks. The performance of the protocol is analyzed for a broad range of physical parameters, and our results are compared to existing security bounds.

## 1. Introduction

Entity authentication (or identification) is a fundamental cryptographic task, which aims at providing a verifier with assurance about the identity of another entity (a claimant) [1]. In order to offer high levels of security, modern protocols combine in the framework of a challenge–response mechanism, something that the claimant possesses together with something that the claimant knows [2]. For instance, a typical transaction through an automatic-teller machine (verifier) relies on the smart card that the user possesses, and a secret personal identification number (PIN). In each transaction, the PIN is used to verify the user to the smart card, while the latter is equipped with a chip that runs a publicly-known algorithm, and involves a numerical secret key on the card for which the verifier has a matching counterpart i.e., either shares the secret key with the verifier or holds the public key to the secret key. Verification of the smart card is performed only if the PIN is correct, and involves a number of random and independent numerical challenges, for which the chip on the card computes a response based on the implemented algorithm and the key. The user is authenticated only if the responses agree with the ones expected by the verifier. Attacks against conventional smart cards and dynamic entity-authentication protocols (EAP) are difficult but not impossible (e.g., see [3–5] and references therein). More precisely, physical invasive and non-invasive attacks, as well as software attacks (e.g., viruses), constitute a severe threat as they allow adversaries to extract the secret key from the card. The necessity for entity-authentication protocols that are robust against such types of attacks has motivated the development of physical unclonable functions (PUFs) [6–8].

In general terms, a PUF is a cryptographic primitive which converts an input challenge into an output response, by means of a random physical unclonable key (PUK). The randomness of the PUK is

introduced explicitly or implicitly during its fabrication, and it is considered to be technologically hard to clone (hence the term physical unclonable). The physical mechanism underpinning the operation of a PUF, as well as the nature of the challenge, depend on the nature of the PUK. Hence, one can have electronic, optical, magnetic, biological PUFs, etc. For a rather extensive list of PUFs and their classification, the reader may refer to Ref. [8]. Up to now, electronic and optical PUFs appear to be the most prominent classes of PUFs. An advantage of the former is that they are compatible with existing technology and hardware, but their robustness against various types of modelling attacks does not seem to be as strong as expected (see [9–12] and references therein). On the contrary, optical PUFs are not fully compatible with existing technology, but they offer many advantages relative to certain types of electronic PUFs, including high complexity, security against modeling attacks, and low cost [13].

Another advantage of optical PUFs is that they accept quantum states of light as challenges, thereby enabling the design of EAPs whose security relies on fundamental principles of quantum physics [14,15]. Typically, the operation of such an EAP relies on a set of numerical challenge–response pairs (CRPs), which is generated during the enrollment stage, and it is stored in a secure database (see Figure 1). There is also a publicly known bijective map of the set of numerical challenges onto a set of non-orthogonal quantum states of light. Whenever the holder of the PUK has to authenticate himself in a potentially unsecured verification set-up, his PUK undergoes a verification procedure, where it is interrogated by a random sequence of non-orthogonal quantum states of light. Each state corresponds to a random and independently chosen numerical challenge. The optical response of the PUK to each quantum challenge is measured and processed in order to obtain a numerical response. The user is authenticated if the recorded numerical responses do not deviate considerably from the expected numerical responses listed in the set of CRPs. The precise quantification of the deviations depends strongly on the details of the protocol, and plays a pivotal role in its security. The main point is that, even when an adversary knows the set of numerical CRPs to be used for the verification of a PUK, the impersonation of the legitimate user requires interaction of the adversary with the quantum states used for the interrogation of the PUK. This is the only way for the adversary to estimate the numerical challenges encoded on the quantum states, and to send the corresponding responses to the verifier by looking at the estimated challenges up in the set of CRPs. However, fundamental theorems of quantum physics prevent perfect discrimination between non-orthogonal quantum states. As a result, the intervention of the adversary will inevitably introduce errors that will be detected by the verifier, who can abort the authentication process.

In this context, we recently proposed a continuous-variable quantum authentication of optical PUKs, which relies on standard wavefront-shaping and homodyne–detection techniques [15]. Up to now, the protocol has been shown to offer cloning and collision resistance, while its security against an emulation attack, in which an adversary knows the challenge–response properties of the PUK and he can access the challenges during the verification, has been analyzed in Ref. [16]. The analysis of Ref. [16] is rather general and does not involve any assumptions about the type of the state-discrimination strategy adopted by the adversary. Hence, the natural question arises as to whether the security bound obtained in Ref. [16] can be attained by means of standard state-discrimination techniques, which are within reach of current or future technology. In the present work, this question is addressed for unambiguous state discrimination, minimum-error discrimination, and dual-homodyne detection.
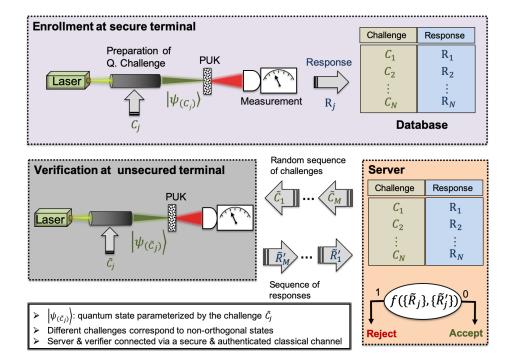
**Figure 1.** General schematic representation of the main stages and the typical operations of an entity authentication protocol (EAP) with quantum readout of a physical unclonable key (PUK). The enrollment stage is performed before the PUK is given to the user, and aims at the generation of a set of numerical challenge-response pairs (CRPs). In the verification stage, $M \gg 1$ numerical challenges are chosen at random and independently from the available set of CRPs for the particular PUK. Each numerical challenge is encoded independently in the quantum state of a laser pulse, which is scattered from the PUK. The scattered light is measured and the outcome (response) is returned to the server. The PUK is accepted or rejected based on a publicly known function, which quantifies the deviations of the recorded responses from the expected ones.

The paper is organized as follows. In Section 2, we discuss briefly the EAP, while the intercept–resend attacks under consideration are formulated in Section 3. Our main results and the robustness of the protocol are discussed in Section 4. A summary with concluding remarks is given in Section 5.

## 2. Authentication Scheme

The EAP under consideration and the related verification set-up have been discussed in detail elsewhere [15,16], but, for the sake of completeness, we will give here a brief overview, focusing mainly on the aspects of the EAP that are directly pertinent to the present work. The interested reader may refer to Refs. [15,16] for a detailed description.

The main parts of the verification set-up are shown in Figure 2. A coherent probe is directed to the interrogation chamber via a single-mode fiber (SMF A), and its wavefront is shaped by a phase-only spatial light modulator (SLM) thereby obtaining the quantum challenge, which is focused on the PUK. The scattered light (speckle) is collected by means of a polarizing beam-splitter and an objective. One of the speckle grains is coupled to a properly positioned single-mode fiber (SMF B), which leads to a standard homodyne detection (HD) set-up. SMF B can be translated in a controlled manner at the output plane in order to collect light from different speckle grains (different target modes). The field in the mode of the fiber is the response of the PUK to the particular challenge, and, in the HD set-up, the verifier measures at random one of the two conjugate quadratures using a strong local oscillator (LO) as reference.
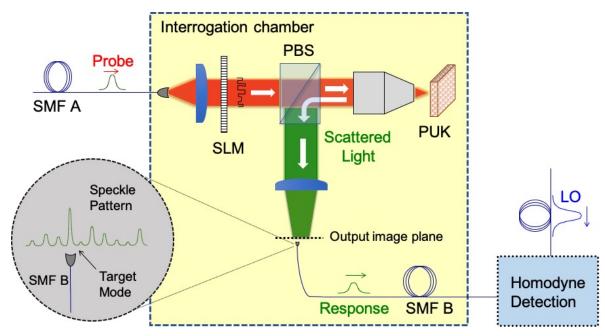
**Figure 2.** Schematic representation of the set-up for the EAP under consideration [15].

The set-up operates in the diffusive limit [15,16], and the phase-mask of the SLM is optimized so that the intensity of the scattered light in SMF B is maximized. The optimization can be performed with standard algorithms [17–19], and, for a fixed set-up, the optimal phase mask $\boldsymbol{\Phi}$ of the SLM depends strongly on the PUK $\mathcal{K}$ and the chosen target mode at the output $s$, while it is independent of the details of the probe state [20,21]. Moreover, having obtained the optimal phase pattern, one can apply a global phase shift to it, thereby determining the phase of the field at the target mode relative to the LO, without affecting the intensity [22]. Throughout this work, we assume that the probe is in a coherent state with a fixed mean number of photons $\mu_P$, which is chosen at random and independently from the symmetric set

$$\mathbb{S}_N := \left\{ |\alpha_k\rangle = |\sqrt{\mu_P}e^{i\varphi_k}\rangle \; : \; \varphi_k := \frac{2\pi k}{N}, k \in \mathbb{Z}_N \right\}, \tag{1}$$

where $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ and $N \gg 1$. We associate a randomly chosen phase shift with each possible value of $k$, which is applied on the optimal phase pattern of the SLM when the probe state $|\alpha_k\rangle$ is used. Hence, the optimal phase pattern for the probe state $|\alpha_k\rangle$ becomes $\boldsymbol{\Phi}_k := \boldsymbol{\Phi} + \omega_k$, where $\omega_k$ denotes the applied global shift, and is chosen at random and independently from a uniform distribution over finite set $\boldsymbol{\Omega}$. In the diffusive limit, the action of the entire set-up on the input probe can be represented by a linear transformation, which depends on various parameters of the set-up, including the PUK, and the (shifted) phase pattern of the SLM. The main quantity of interest is the quantum mechanical expectation value of the $\theta$-quadrature of the electric field in SMF B at the entrance of the HD set-up, which is given by [15,16]

$$\langle \hat{Q}(\theta) \rangle_k = \sqrt{2\mu_R} \cos(\chi_k - \theta), \tag{2}$$

where the mean number of photons $\mu_R$ that reach the HD set-up is smaller than $\mu_P$. Equation (2) encapsulates possible losses, and various other parameters pertaining to the set-up and the applied wavefront-shaping technique. For a fixed set-up with publicly-known parameters, $\mu_R$ can be considered fixed and known, while the phase $\chi_k$ is fully determined by the phase of the probe state $\varphi_k$, the associated random phase shift $\omega_k$, and the PUK. For $\theta = 0$ and $\pi/2$, one obtains the expectation values of the conjugate quadratures of the field $\hat{X}$ and $\hat{Y}$, respectively.

There are two distinct stages in the EAP under consideration i.e., the enrollment and the verification stages (see Figure 1). The enrollment stage takes place only once, before a PUK is given to a user, it is performed by the manufacturer, and aims at a reliable characterization of the PUK with respect to its responses to a finite set of challenges. The typical list of CRPs for the protocol under consideration is given in Table 1. We assume that the enroller has all the resources needed for the reliable estimation of the response $R_k := \{\langle \hat{X} \rangle_k, \langle \hat{Y} \rangle_k\}$ for each challenge $C_k := \{k, \mathbf{\Phi}_k\}$ [15]. After the enrollment stage, the list of CRPs is stored in a database of a server, and the PUK is given to a user.

**Table 1.** Illustration of a set of CRPs used for authentication of a PUK. The set is identified by a unique identification number (see discussion in Section 5). The angles $\theta = 0$ and $\pi/2$ refer to the quadratures $\hat{X}$ and $\hat{Y}$ of the field in SMF B at the entrance of the homodyne detection (HD) set-up, respectively (see Figure 2).

| Identification Number | | | |
|---|---|---|---|
| Challenge | | Response | |
| $k$ | Phase mask | $\theta = 0$ | $\theta = \pi/2$ |
| 0 | $\mathbf{\Phi}_0$ | $\langle \hat{X} \rangle_0$ | $\langle \hat{Y} \rangle_0$ |
| 1 | $\mathbf{\Phi}_1$ | $\langle \hat{X} \rangle_1$ | $\langle \hat{Y} \rangle_1$ |
| 2 | $\mathbf{\Phi}_2$ | $\langle \hat{X} \rangle_2$ | $\langle \hat{Y} \rangle_2$ |
| $\vdots$ | | $\vdots$ | $\vdots$ |
| $N-1$ | $\mathbf{\Phi}_{N-1}$ | $\langle \hat{X} \rangle_{N-1}$ | $\langle \hat{Y} \rangle_{N-1}$ |

The verification stage takes place each time the user wishes to authenticate himself. He has to input the PUK in a potentially unsecured verification set-up, which is connected to the database over a secure and authenticated classical channel. The server sends to the verifier a sequence of $M \gg 1$ challenges, chosen at random from the available challenges, together with a sequence of $M$ angles $(\theta_1, \theta_2, \ldots, \theta_M)$ chosen at random and independently from a uniform distribution over $\{0, \pi/2\}$. The PUK is interrogated sequentially by the $M$ challenges. In the $j$th challenge $C_{k_j} := \{k_j, \mathbf{\Phi}_{k_j}\}$, the verifier measures the $\theta_j$-quadrature of the field in SMF B. Assuming very strong LO field, the outcome of the measurement in the HD set-up follows a normal distribution $\mathcal{N}(\langle \hat{Q}(\theta_j) \rangle_{k_j}, \sigma^2)$, which is centered at the expectation value of the measured quadrature and its standard deviation $\sigma = 1/\sqrt{2\eta}$, is determined by the detection efficiency $\eta$ of the HD set-up. The outcomes from all of the $M$ measurements are returned to the server, over the classical channel. Acceptance or rejection of the PUK is decided upon the fraction of outcomes $p_{\text{in}}$ that fall within an interval (bin) of width $\Delta$, which is centered at the expectation value of the measured quadrature $\langle \hat{Q}(\theta_j) \rangle_{k_j}$. The theoretically expected probability for an outcome to fall inside the interval is given by [16]

$$P_{\text{in}}^{(0)} = \text{erf}\left( \frac{\bar{\Delta}}{2\sqrt{2}} \right) \tag{3}$$
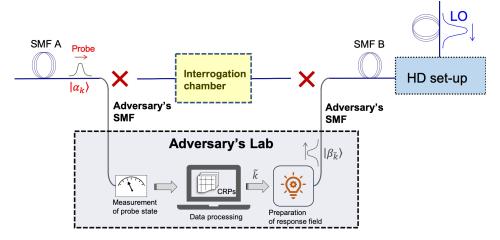
with $\bar{\Delta} = \Delta/\sigma$, which is independent of $k$ and $\theta$. For sufficiently large values of $M$, one can ensure with high confidence that for the true PUK and in the absence of cheating, the empirical probability $p_{\text{in}}$ will lie in an interval of size $2\varepsilon$ around the theoretically expected probability $P_{\text{in}}^{(0)}$ [15,16]. Hence, the PUK is accepted if $|p_{\text{in}} - P_{\text{in}}^{(0)}| < \varepsilon$, and is rejected otherwise. As we will see later on, the security parameter $\varepsilon$ plays a central role in the protocol, as it determines the regime of parameters for which an attack can be detected by the verifier.

## 3. Intercept–Resend Emulation Attacks

The emulation attacks under consideration follow closely the general theoretical framework of Ref. [16], which is summarized in Figure 3. We assume that the adversary does not have access to the preparation of the probe states, the actual PUK, the SLM, or the HD set-up. However, he has obtained

somehow a copy of all the possible CRPs to be used in the authentication of the PUK, and moreover he has obtained access to the incoming and outgoing SMFs, without being detected. Hence, if the adversary were able to estimate exactly the probe state, he would be able to impersonate successfully the holder of the PUK, by looking at the CRPs and by sending to the HD set-up the expected response state. However, quantum physics does not allow for perfect discrimination between non-orthogonal quantum states, or the measurement of non-communting quantum observables with arbitrary accuracy. As a result, it is inevitable for the adversary's intervention to introduce errors in the HD performed by the verifier.



**Figure 3.** Schematic representation of the attack under consideration [16]. The adversary has a copy of the set of the numerical CRPs, from which the challenges are chosen at random. He intercepts each one of the $M$ incoming probe states, and measures it in order to deduce the value of $k$ (see Table 1). Based on the outcome of his measurement the adversary makes an educated guess about $k$, say $\widetilde{k}$, and he looks $\widetilde{k}$ up in the set of CRPs, in order to find the corresponding expected response $R_{\widetilde{k}}$. Finally, the adversary prepares and sends to the homodyne detection (HD) set-up of the verifier a quantum state that will induce statistics consistent with $R_{\widetilde{k}}$.

Given that the probe states in the $M$ queries are chosen at random and independently from a uniform distribution over the set $\mathbb{S}_N$, from now on, we can focus on one of the queries and let $|\alpha_k\rangle$ denote the incoming probe state. The adversary's task is to obtain an estimate of the integer $k$, which determines fully the challenge and the expected response. To this end, he performs a measurement on the incoming probe state, and, based on the outcome, the adversary makes an educated guess about $k$, to be denoted by $\widetilde{k}$. For the reasons discussed above, this guess may or may not be equal to the actual $k$ used by the verifier, and thus the adversary's intervention will affect the probability with which the verifier obtains an outcome in the expected bin. More precisely, instead of Equation (3), one has [16]

$$P(\text{in}|k,\widetilde{k},\theta) = \frac{1}{2}\left\{ \text{erf}\left[\frac{2\left(\langle \hat{Q}(\theta)\rangle_k - \langle \hat{Q}(\theta)\rangle_{\widetilde{k}}\right) + \Delta}{2\sqrt{2}\sigma}\right] - \text{erf}\left[\frac{2\left(\langle \hat{Q}(\theta)\rangle_k - \langle \hat{Q}(\theta)\rangle_{\widetilde{k}}\right) - \Delta}{2\sqrt{2}\sigma}\right]\right\}, \quad (4a)$$

where $\hat{Q}_k(\theta)$ and $\hat{Q}_{\widetilde{k}}(\theta)$ denote the $\theta$-quadratures of the response field, when the adversary deduces the correct and the wrong value of $k$. Both of them are given by Equation (2) for $k$ and $\widetilde{k}$, respectively.

Given that the verifier samples from both quadratures at random and independently, after $M$ queries, the verifier will obtain an estimate of the average probability [16]

$$P_{\text{in}} = \sum_{k=0}^{N-1}\sum_{\widetilde{k}=0}^{N-1}\sum_{\theta \in \{0,\pi/2\}} P(\text{in},k,\widetilde{k},\theta) = (1 - P_{\text{err}})P_{\text{in}}^{(0)} + \frac{1}{2N}\sum_k\sum_{\widetilde{k}\neq k} P(\widetilde{k}|k)\sum_{\theta=0,\pi/2} P(\text{in}|k,\widetilde{k},\theta) \quad (4b)$$

where $P(\text{in}|k,\widetilde{k},\theta)$ is given by Equation (4a) and

$$P_{\text{err}} := \sum_k P(k,\widetilde{k} \neq k) = 1 - \frac{1}{N}\sum_k P(\widetilde{k}=k|k) \tag{5}$$

is the probability for the adversary to make an error in his estimation of $k$.

The probability $P_{\text{in}}$ takes into account all of the events irrespective of whether the adversary deduced the correct value of $k$ or not. In the second equality of Equation (4b), we have taken into account the uniform distribution of $k$ over $\mathbb{Z}_N$ and of $\theta$ over $\{0, \pi/2\}$. Moreover, we have used the fact that the state of the probe and the outcome of the adversary are independent of the quadrature to be measured by the verifier. A straightforward calculation [16] shows that $P_{\text{in}}$ is always smaller than the corresponding expression in the absence of cheating [which is given by Equation (3)], and the difference
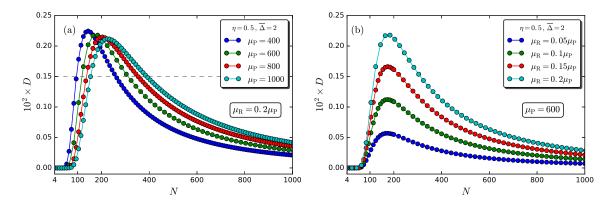
$$D := P_{\text{in}}^{(0)} - P_{\text{in}} \tag{6a}$$

basically quantifies the adversary's intervention. The adversary's intervention will be detected by the verifier when the observed deviations from $P_{\text{in}}^{(0)}$ exceed the statistical deviations i.e., when

$$D > 2\varepsilon. \tag{6b}$$

As mentioned above, the security threshold $2\varepsilon$ is determined by the sample size $M$ in the verification stage, while, in general, the exact values of $P_{\text{err}}$, $P_{\text{in}}$, and $D$, depend on the measurement applied by the adversary. However, working along the lines of Ref. [16], one readily obtains a lower bound on $P_{\text{err}}$, which in turn yields the following lower bound on $D$

$$D \geq P_{\text{err}}^{(\text{low})}\left[P_{\text{in}}^0 - P_{\text{max}}(\text{in}|\text{error})\right] := D_{\text{low}}, \tag{7}$$

where $P_{\text{max}}(\text{in}|\text{error}) := \max_{k,\widetilde{k}}\left\{P(\text{in}|k,\widetilde{k})\right\}_{\widetilde{k}\neq k}$. This bound is expected to hold irrespective of the adversary's measurement, and its dependence on various parameters of the protocol has been discussed in detail elsewhere [16]. In particular, it has been shown that, for any given combination of parameters $\{\varepsilon, \Delta, \mu_P, \mu_R\}$, the secure operation region for the protocol becomes wider for increasing $\eta$. Typical HD set-ups have $\eta > 0.5$, and $\eta = 0.5$ can be considered as the worst-case scenario for the security of the protocol. The size of the bin width $\Delta$ relative to the detection efficiency is a free parameter that can be chosen at will, in order to optimize the performance of the protocol. For any given combination of $\{\varepsilon, \eta, \mu_P, \mu_R\}$, it has been shown that the optimal value is $\Delta \simeq 2\sigma$. Hence, although our simulations have been extended to various combinations of $\eta$ and $\Delta$, throughout the present work, we focus on numerical results for $\eta = 0.5$ and $\Delta = 2\sigma$. To facilitate the analysis of our results for the three different attacks, in Figure 4, we plot the lower bound $D_{\text{low}}$ as a function of $N$, for different values $\mu_P$ and $\mu_R$. As explained in Ref. [16], the depicted asymmetric bell-shape stems from the fact that $D_{\text{low}}$ is a product of two functions of $N$ with opposite monotonicity (see Equation (7)). More precisely, $P_{\text{err}}^{(\text{low})}$ increases with increasing $N$ approaching a non-zero value determined by the classical limit, while $P_{\text{in}}^{(0)} - P_{\text{max}}(\text{in}|\text{error})$ decreases with increasing $N$, approaching zero for large values of $N$. A crucial parameter for the security of the protocol is the mean number of photons that reach the HD set-up. The larger $\mu_R$ is for a fixed $N$, the easier the verifier can discriminate between $\langle\hat{Q}_k(\theta)\rangle$ and $\langle\hat{Q}_{\widetilde{k}\neq k}(\theta)\rangle$. In general, $\mu_R$ can be increased in two different ways: (i) increasing $\mu_P$ for fixed losses in the set-up; (ii) improving the set-up, thereby reducing the losses. Figure 4a,b refers to these two cases, and in both of them we see that, for a given $\varepsilon$, the secure region gets wider with increasing $\mu_R$, which is in agreement with the aforementioned role of $\mu_R$ in the discrimination of different responses.

**Figure 4.** The lower bound $D_{\text{low}}$, as a function of the number of different probe states $N$, for various values of $\mu_P$ but fixed ratio $\mu_R/\mu_P$ (**a**); and various values of $\mu_R$ for fixed $\mu_P$ (**b**). The vertical dashed line mark the security threshold $2\varepsilon = 15 \times 10^{-4}$, and the protocol is secure against any intercept–resend attack for $D_{\text{low}} > 2\varepsilon$.

### 3.1. Dual Homodyne–Detection Attack

In a dual homodyne–detection attack (DHA), for each probe, the adversary performs a joint measurement of the non-commuting observables $\{\hat{X}_k, \hat{Y}_k\}$, by means of an eight-port interferometric set-up [23,24], thereby obtaining a bivariate random variable $(x, y)$, which follows the two-dimensional normal distribution

$$P_k^{(\text{DH})}(x, y) = \frac{1}{2\pi} \exp\left( -\frac{\left[x - \langle \hat{X}_A \rangle_k\right]^2 + \left[y - \langle \hat{Y}_A \rangle_k\right]^2}{2} \right), \tag{8a}$$

where $\langle \hat{X}_A \rangle_k$ and $\langle \hat{Y}_A \rangle_k$ refer to the expectation values of the quadratures of the electric field in SMF A, when the field is in state $|\alpha_k\rangle$. Assuming negligible losses in SMF A and in the set-up of the adversary, we have

$$\langle \hat{X}_A \rangle_k = \langle \alpha_k | \hat{X}_A | \alpha_k \rangle = \sqrt{2\mu_P} \cos(\varphi_k), \quad \langle \hat{Y}_A \rangle_k = \langle \alpha_k | \hat{Y}_A | \alpha_k \rangle = \sqrt{2\mu_P} \sin(\varphi_k). \tag{8b}$$
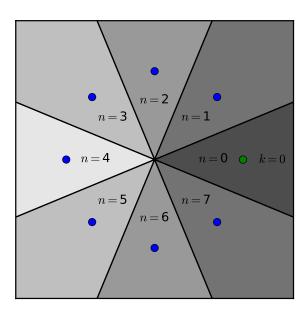
Moreover, in Equation (8a), we have assumed perfect detection efficiency for the adversary ($\sigma_{\text{DH}} = 1$), which is the worst-case scenario for the security of the protocol. Hence, when the efficiency in the HD set-up of the verifier is $\eta \geq 0.5$, we have $\sigma \leq \sigma_{\text{DH}}$. This suggests that, for either of the quadratures, the adversary samples from a distribution, which is at least as broad as the distribution sampled by the verifier.

To proceed further, we have to define a strategy for the adversary to make an educated guess for the probe stare $|\alpha_k\rangle$, given the random outcome of the dual-homodyne detection $(x, y)$. Recall here that the adversary has obtained a copy of the list of the CRPs for the particular PUK, which allows him to discretize the phase space as shown in Figure 5 . The $k$-th sector corresponds to the probe state $|\alpha_k\rangle$. It is centered at $\{\langle \hat{X}_A \rangle_k, \langle \hat{Y}_A \rangle_k\}$, and its angular extension is from $\varphi_k - \pi/N$ to $\varphi_k + \pi/N$, while its radius $\rho$ extends from 0 to $\pm\infty$. Thus, when the random outcome $(x, y)$ falls in the $\widetilde{k}$-th sector, the adversary concludes that the probe state was $|\alpha_{\widetilde{k}}\rangle$, and thus the response expected by the verifier is $R_{\widetilde{k}}$. Working in polar coordinates, the probability for the random outcome $(x, y)$ to fall within the $\widetilde{k}$-th sector given that the probe state was $|\alpha_k\rangle$ is given by the integral

$$P^{(\text{DH})}(\widetilde{k}|k) = \frac{1}{2\pi} \int_{\varphi_{\widetilde{k}} - \frac{\pi}{N}}^{\varphi_{\widetilde{k}} + \frac{\pi}{N}} d\gamma \int_0^\infty \rho \exp\left[ -\frac{\rho^2 + 2\mu_P - \sqrt{8\mu_P}\rho\cos(\gamma - \varphi_k)}{2} \right] d\rho, \tag{9}$$

where we have set $x = \rho \cos(\gamma)$, $y = \rho \sin(\gamma)$, and used Equations (8a) and (8b). Setting $\gamma' = \gamma - \varphi_k$, one can readily confirm that this probability depends only on the difference $n := (\tilde{k} - k) \mod N$. Therefore, the probability for the adversary to deduce the wrong probe state is given by

$$P_{\text{err}}^{(\text{DH})} = 1 - \sum_{k=0}^{N-1} p(k) P^{\text{DH}}(\tilde{k} = k | k) = 1 - P^{\text{DH}}(\tilde{k} = k | k). \tag{10}$$



**Figure 5.** Discretization of the phase space for $n = 8$. The segment for the actual probe state $k = 0$ (green) and all other possible probe states (blue) are shown. The coloring displays the probabilities $P^{\text{DH}}(\tilde{k} | k = 0)$ for $\tilde{k} = 0, 1, \ldots, n - 1$ (dark: high probability).

After the measurement, the adversary prepares and sends to the verifier a coherent state $|\beta_{\tilde{k}}\rangle$, which is consistent with his educated guess about the probe state, and will induce the expected statistics at the HD set-up of the verifier. The average probability $P_{\text{in}}^{(\text{DH})}$ for the state $|\beta_{\tilde{k}}\rangle$ to result in an outcome within the expected bin is given by Equation (4b), after substituting $P(\tilde{k}|k)$ by $P^{(\text{DH})}(\tilde{k}|k)$, which is given by Equation (9). Hence, the adversary's intervention will introduce errors in the estimate to be obtained by the verifier, which are quantified by the difference

$$D^{(\text{DH})} := P_{\text{in}}^{(0)} - P_{\text{in}}^{(\text{DH})} = P_{\text{err}}^{(\text{DH})} \left\{ P_{\text{in}}^{(0)} - \frac{1}{P_{\text{err}}^{(\text{DH})}} \left[ \frac{1}{2N} \sum_k \sum_{\tilde{k} \neq k} P^{(\text{DH})}(\tilde{k}|k) \sum_{\theta = 0, \pi/2} P(\text{in}|k, \tilde{k}, \theta) \right] \right\}. \tag{11}$$

The term inside the brackets is the joint probability for the adversary to deduce the wrong value for $k$, and the outcome of the HD of the verifier to fall within the expected bin.

### 3.2. Unambiguous State-Discrimination Attack

Assume now that the adversary applies an ideal unambiguous discrimination (UD) measurement to each probe, in order to deduce which of the $N$ possible coherent states is used by the verifier [25–28]. The adversary will either obtain a conclusive result, or an inconclusive result. In the former case, he learns the actual state of the probe with certainty, whereas, in the latter, he learns nothing about the incoming state, which is destroyed by the measurement, and additional measurement on it will not provide any useful information. Given that the adversary has the list of CRPs, a conclusive result implies that the adversary knows precisely the response expected by the verifier, whereas, in the case of an inconclusive result, all of the possible responses are equally probable.

The minimum probability for an inconclusive result is [25]

$$P_{\text{inc}} = 1 - N \cdot \min_{r \in \mathbb{Z}_N} \left( \frac{1}{N} \sum_{j=0}^{N-1} e^{-i2\pi jr/N} \cdot e^{|\alpha|^2 (e^{i2\pi j/N} - 1)} \right), \tag{12}$$

which is independent of the value of $k$ i.e., independent of the probe state. In the case of a conclusive outcome, the adversary will prepare and send a coherent state, which will induce the expected statistics at the HD set-up of the verifier. Hence, the probability for the verifier to get a result inside the bin, given that the adversary obtained a conclusive outcome, is equal to $P_{\text{in}}^{(0)}$ (see Equation (3)). On the contrary, in the case of an inconclusive result, the adversary has no information on the probe state or on the response expected by the verifier. Given that the verifier expects a response state for each probe, the adversary has to send a state to the HD set-up of the verifier. Hence, we assume that, in the case of an inconclusive outcome, the adversary has to choose at random one of the $N$ equally probable responses, and send a coherent state $|\beta_{\widetilde{k}}\rangle$ that will induce the corresponding statistics at the HD set-up of the verifier. This choice is independent of the probe state, and thus the conditional probability for the random choice to yield $\widetilde{k}$, given an inconclusive result on the input state $|\alpha_k\rangle$ is given by

$$P^{(\text{UD})}(\widetilde{k}|\text{inc}, k) = P^{(\text{UD})}(\widetilde{k}) = \frac{1}{N}. \tag{13}$$

Using this equation, the overall error probability reads

$$P_{\text{err}}^{(\text{UD})} = P_{\text{inc}} \frac{N-1}{N}. \tag{14}$$

Using the fact that a conclusive outcome always yields the correct value of $k$, while the occurrence of a conclusive or inconclusive result is independent of $k$, one readily obtains

$$P^{(\text{UD})}(\widetilde{k} \neq k|k) = \frac{P_{\text{inc}}}{N}. \tag{15}$$

The average probability for the verifier to get an outcome inside the expected bin after an unambiguous-state-discrimination attack (UDA) is given by Equations (4a) and (4b), after replacing $P(\widetilde{k}|k)$ by Equation (15) and $P_{\text{err}}$ by $P_{\text{err}}^{(\text{UD})}$. Accordingly, the deviations that will be observed by the verifier are quantified by the difference

$$D^{(\text{UD})} = P_{\text{err}}^{(\text{UD})} \left\{ P_{\text{in}}^{(0)} - \frac{1}{P_{\text{err}}^{(\text{UD})}} \left[ \frac{1}{2N} \sum_k \sum_{\widetilde{k} \neq k} P^{(\text{UD})}(\widetilde{k}|k) \sum_{\theta=0,\pi/2} P(\text{in}|k, \widetilde{k}, \theta) \right] \right\}, \tag{16}$$

where $P(\text{in}|k, \widetilde{k}, \theta)$ is given by Equation (4a).

### 3.3. Minimum-Error State Discrimination Attack

The third attack we consider relies on a minimum-error state-discrimination measurement [29,30]. Each of the possible outcomes $\widetilde{k} \in \{0, 1, \dots N - 1\}$ is characterized by a corresponding probability operator measure element $\widehat{\Pi}_{\widetilde{k}}$, also referred to as a positive operator-valued measure. The probability for the adversary to obtain outcome $\widetilde{k}$, given that the probe state $|\alpha_k\rangle$ was used, is

$$P^{(\text{SR})}(\widetilde{k}|k) = \text{Tr}\left( \hat{\rho}_k \widehat{\Pi}_{\widetilde{k}} \right), \tag{17}$$

where $\hat{\rho}_k := |\alpha_k\rangle \langle \alpha_k|$. When the adversary obtains the outcome $\widetilde{k}$, he concludes that the probe was also in state $|\alpha_{\widetilde{k}}\rangle$, and thus the response expected by the verifier is $R_{\widetilde{k}} = \{\langle \hat{X}_{\widetilde{k}} \rangle, \langle \hat{Y}_{\widetilde{k}} \rangle\}$.

Given that the authentication scheme works with the symmetric set of states $\mathbb{S}_N$, the optimal measurement that minimizes the error probability is the square-root measurement [29,30], where the operator $\widehat{\Pi}_k$ is given by

$$\widehat{\Pi}_k := \frac{1}{N} \hat{\rho}^{-\frac{1}{2}} \hat{\rho}_k \hat{\rho}^{-\frac{1}{2}}, \tag{18}$$

with $\hat{\rho} := \sum_k \hat{\rho}_k / N$. The average probability for the adversary to deduce the wrong probe state is given by

$$P_{\text{err}}^{(\text{SR})} = \frac{1}{N} \sum_{k=0}^{N-1} \sum_{\widetilde{k} \neq k} P^{(\text{SR})}(\widetilde{k}|k) = 1 - \frac{1}{N} \sum_{k=0}^{N-1} \text{Tr}\left(\hat{\rho}_k \widehat{\Pi}_k\right). \tag{19}$$

As in the previous attacks, given the outcome $\widetilde{k}$, the adversary prepares and sends to the verifier a coherent state that will induce statistics compatible with the response $R_{\widetilde{k}}$. The probability $P_{\text{in}}^{(\text{SR})}$ for the verifier to obtain an outcome within the expected bin is given by Equations (4a) and (4b), after replacing $P(\widetilde{k}|k)$ by $P^{(\text{SR})}(\widetilde{k}|k)$, which is given by Equations (17) and (18). Hence, the adversary's intervention will introduce errors in the estimate to be obtained by the verifier, which are quantified by the difference $D^{(\text{SR})} := P_{\text{in}}^{(0)} - P_{\text{in}}^{(\text{SR})}$. Using Equation (4b) we have for the square-root-measurement attack (SRA)
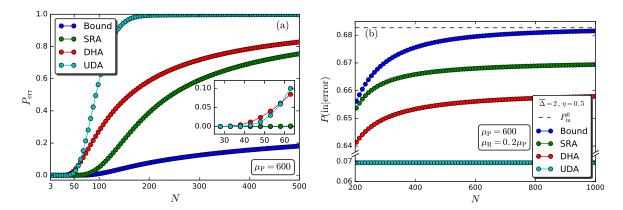
$$D^{(\text{SR})} = P_{\text{err}}^{(\text{SR})} \left\{ P_{\text{in}}^{(0)} - \frac{1}{P_{\text{err}}^{(\text{SR})}} \left[ \frac{1}{2N} \sum_k \sum_{\widetilde{k} \neq k} P^{(\text{SR})}(\widetilde{k}|k) \sum_{\theta=0,\pi/2} P(\text{in}|k,\widetilde{k},\theta) \right] \right\}. \tag{20}$$

## 4. Numerical Results and Discussion

We have performed extensive simulations on the aforementioned three different types of intercept–resend attacks, and, in this section, we discuss our main findings on the security of the proposed protocol. As discussed in Section 3, the protocol is secure when the difference of probabilities (6a) exceeds the security threshold $2\varepsilon$, attained by sampling. Hence, for a given value of $\varepsilon$, the main quantity of interest for the security of the protocol is the difference of probabilities $D$, which, for the three different attacks, is given in Equations (11), (16), and (20). A lower bound on $D$ has been obtained in Ref. [16], through the Holevo bound and Fano's inequality, and it is given in Equation (7). In all of the cases, we see that $D$ is of the form $D = P_{\text{err}}[P_{\text{in}}^{(0)} - P(\text{in}|\text{error})]$, where $P_{\text{err}}$ is the error probability in each case, $P_{\text{in}}^{(0)}$ is the probability for the verifier to obtain an outcome inside the bin in the absence of any attack (see Equation (3)), and $P(\text{in}|\text{error})$ is the corresponding probability in the presence of the attack, and given that the adversary has made an error in deducing the right probe state.

Both $P_{\text{err}}$ and $P(\text{in}|\text{error})$ depend on the attack under consideration. Hence, it is instructive to look at them separately, in comparison with the corresponding quantities determining the lower bound in Equation (7), before we discuss the dependence of $D$ on the various parameters of the protocol. In Figure 6a, we plot the probability for the adversary to deduce the wrong probe state, as a function of the number of different probe states $N$ used in the protocol, and for a fixed mean number of photons in the probe. The error probabilities for the three attacks are given by Equations (10), (14), and (19), while, for the sake of comparison, we also show the lower bound on the error probability $P_{\text{err}}^{(\text{low})}$ (blue curve). In all of the cases, we find a monotonic increase of the error probability with $N$. For $N < 50$, the error probabilities for all of the three attacks are very close to the lower bound, and they start deviating from it as we increase $N$. The deviation is slower in the case of the square-root-measurement attack (green curve), which is practically indistinguishable from the lower bound (blue curve) up to $N \simeq 60$, and it remains close to it for values of $N$ up to about 100. The error probability for the unambiguous-state-discrimination attack exhibits the fastest increase, and $P_{\text{err}}^{(\text{UD})} \simeq 1$ for $N \simeq 100$

(gray curve). The dual-homodyne–detection attack stands between the other two attacks. The same behavior has been found for other values of $\mu_P$, and the main difference is that the error probability increases slower with $N$, for increasing values of $\mu_P$.
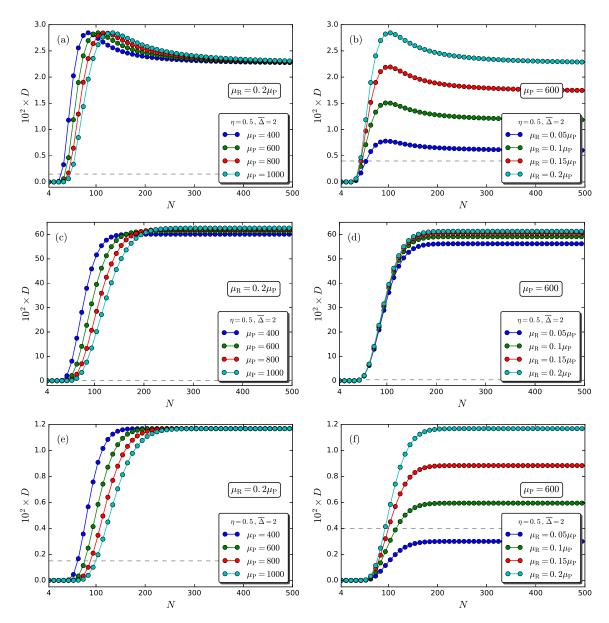


**Figure 6.** (**a**) Probability for the adversary to deduce the wrong probe state in the case of dual-homodyne–detection attack (red curve, DHA), square-root-measurement attack (green curve, SRA) and unambiguous-state-discrimination attack (gray curve, UDA), as a function of the number of different probe states $N$. The lower bound is also shown (blue curve); (**b**) conditional probability $P(\text{in}|\text{error})$ for the verifier to obtain a result inside the expected bin given that the adversary inferred the wrong probe state, as function of $N$ and for different attacks. The maximum value $P_{\max}(\text{in}|\text{error})$ is also shown (blue curve), and all of the probabilities are compared to the probability $P_{\text{in}}^0$ in the absence of an attack (dashed vertical line).

Let us turn now to the other quantity of interest, namely the conditional probability $P(\text{in}|\text{error})$ relative to $P_{\text{in}}^{(0)}$. As depicted in Figure 6b, for either of the three attacks under consideration $P(\text{in}|\text{error})$ increases with $N$, approaching an asymptotic value that is below $P_{\text{in}}^{(0)}$ as well as below the asymptotic value of $P_{\text{err}}$ for the same attack (compare to Figure 6a). This is in contrast to the behavior of $P_{\max}(\text{in}|\text{error})$ (blue curve), which approaches $P_{\text{in}}^{(0)}$ (dashed vertical line) as we increase $N$.

Based on these findings, we expect the lower bound $D_{\text{low}}$ to approach zero as we increase $N$ (which is in accordance with Figure 4), whereas, for all three of the attacks, $D$ is expected to approach a non-zero value as we increase $N$. Indeed, as shown in Figure 7, this is confirmed by our simulations. As a result, for a given security threshold $\varepsilon$ and fixed losses (i.e., fixed ratio $\mu_R/\mu_P$), there is a very broad regime of values for $N$ and $\mu_P$ where $D$ exceeds $2\varepsilon$ and the protocol is secure against all of the three attacks. The secure regime is considerably broader than the one predicted by the lower bound (compare to Figure 4). The strongest attack seems to be the square-root-measurement attack. Consider, for instance, the case of $2\varepsilon = 15 \times 10^{-4}$. We have $D^{(SR)} > 2\varepsilon$ for $N > 100$ (see Figure 7e), whereas, for the other two attacks, we find $D^{(DH)} > 2\varepsilon$ for $N > 45$ (see Figure 7a), $D^{(UD)} > 2\varepsilon$ for $N > 60$ (see Figure 7c). By contrast to the lower bound $D_{\text{low}}$ (see Figure 4a), where there is an upper bound on the values of $N$ for which the condition $D_{\text{low}} > 2\varepsilon$ is satisfied, we do not find any such bound for either of the three attacks we have considered in this work. Moreover, for all three of the attacks, we find that the rise of $D$ with $N$ gets slower as we increase $\mu_P$, which is in agreement with the analogous behavior obtained for the error probability.

Keeping the mean number of photons $\mu_P$ in the probe constant, and increasing the losses in the set-up (i.e., decreasing the mean number of photons that reach the HD set-up relative to $\mu_P$), we find that lower security thresholds have to be attained by the verifier, so that to ensure the security of the protocol against both the dual-homodyne–detection and the square-root-measurement attacks. For example, we see that the protocol is not secure against the square-root-measurement attack when $2\varepsilon = 4 \times 10^{-4}$ and $\mu_P = 600$, with $\mu_R = 0.05\mu_P$, but it is secure against the dual-homodyne–detection attack if $N > 50$ (see Figure 7b,f, respectively). Moreover, for the particular chosen value of $2\varepsilon$, we find

that the protocol becomes secure against both of these attacks if $\mu_R = 0.1\mu_P$ and $N > 110$. Security against the two attacks when the losses in the set-up are such that $\mu_R = 0.05\mu_P$ requires $N \geq 110$ and sufficiently large sample size $M$ so that $2\varepsilon \lesssim 3 \times 10^{-4}$. By contrast, we find small changes in the variation of $D^{(\mathrm{UD})}$ with $N$, which suggests that the unambiguous-state-discrimination attack is weaker than the other two.



**Figure 7.** Difference of probabilities $D = P_{\mathrm{in}}^0 - P_{\mathrm{in}}$ as a function of the total number of different probe states $N$, for the dual-homodyne–detection attack (**a**,**b**); the unambiguous-state-discrimination attack (**c**,**d**); and the square-root-measurement attack (**e**,**f**). The horizontal dashed lines mark the security threshold $2\varepsilon = 15 \times 10^{-4}$ (l.h.s) and $2\varepsilon = 4 \times 10^{-4}$ (r.h.s). The protocol is secure against a specific type of intercept–resend attack when the corresponding value of $D$ exceeds $2\varepsilon$.

## 5. Concluding Remarks

In this work, we have analyzed the seurity of the verification stage in the EAP of Ref. [15] against three specific intercept–resend emulation attacks. Our results suggest that the protocol is secure against all of the attacks simultaneosuly for a broad range of values for the relevant parameters of the protocol. Moreover, the performance of all of these attacks has been compared to the lower security bound

obtained in Ref. [16], by means of the Fano's inequality and the Holevo bound. None of the attacks considered here saturates the expected lower bound. Hence, the existence as well as the details of the attack that will saturate the lower security bound remain a subject of future work. One may wonder whether the displaced-photon counting [31] can achieve this goal. We believe that this is not the case for a number of reasons. Firstly, the probability for the adversary to deduce the wrong state is expected to be higher for the displaced-photon counting than for the square-root measurement discussed here. This is because our protocol relies on a set of symmetric states, and it is well-known that the square-root measurement minimizes the probability of error in this case [29,30]. Higher error probability means that it is easier for the verifier to detect the adversary's intervention. Secondly, the displaced-photon counting has been shown to outperform the dual-homodyne measurement in phase estimation, only for phases in a narrow region around $\varphi = 0$ [31]. Outside this region, the dual-homodyne measurement outperforms by the same amount the displaced-photon counting. In our protocol, the random phase of a probe state lies in the interval $[0, 2\pi)$, and all of the possible values are equally probable. As a result, on average, the performance of the displaced-photon counting is expected to be very close to the performance of the dual-homodyne detection discussed here.

As far as experimental realizations of the present attacks are concerned, the dual-homodyne–detection attack can be implemented with current technology [32]. On the contrary, to the best of our knowledge, the experimental realization of the unambiguous-state-discrimination attack and of the square-root measurement attack for arbitrary number of symmetric coherent states is not known. A rather simple linear-optics implementation of unambiguous state-discrimination has been proposed in Ref. [33], which is far from optimal for large values of $N$.

The present work focuses on the verification of a PUK, assuming that the user has already been verified successfully to the PUK (see Section 1). Analogous to conventional smart cards, the verification of the user to the PUK can be achieved through a PIN which is known to the legitimate owner of the PUK. This is necessary for any EAP, in order to prevent impersonation in case the PUK is stolen. When the PUK is given to a legitimate user, it is accompanied by the PIN, which has been generated during the enrollment stage, and it is not shown in Figure 1. One way to combine an optical PUK with a PIN is to exploit the techniques of Refs. [6,34]. For example, one can assume that the PUK is illuminated by classical light, whose wavefront has been modified by a random SLM phase mask $\boldsymbol{\Psi}$ [The pattern $\boldsymbol{\Psi}$ should not be confused with the optimal phase masks $\boldsymbol{\Phi}$ (and $\boldsymbol{\Phi}_k$), which are used for the verification of the PUK as discussed in the previous sections of the present work. The former is a totally random phase mask, whereas the latter are optimized with respect to a particular target mode at the output.]. The response of the PUK to classical light with random wavefront $\boldsymbol{\Psi}$ is a random speckle, which can be processed with standard algorithms to result in a numerical random binary string, say $w = w_{\text{id}}||w_{\text{pin}}$ [34]. We may assume, that the last $n$ bits of $w$, denoted by $w_{\text{pin}}$, define the $n$-bit PIN, whereas the first part $w_{\text{id}}$ serves as an identification number for the list of CRPs to be used for the authentication of the particular PUK (see Table 1). In this way, the list of CRPs, the PUK, and the PIN are linked through a random phase mask, which is known only to the verifier, as well as to the authority that issues and distributes the PUKs.

Analogous to conventional smart cards, at the beginning of the verification stage, the user types in his PIN and inserts his PUK to the verifier's set-up. The verifier imprints the pattern $\boldsymbol{\Psi}$ on the wavefront of the incoming light by means of his SLM, and the speckle of the scattered light is processed to yield the classical string $w$. If the last $n$ bits of $w$ agree with the PIN of the user, the verifier proceeds to the verification of the PUK; otherwise, the authentication is aborted immediately. For the verification stage, the verifier sends to the server the key $w_{\text{id}}$ over a secure and authenticated classical channel, and the server returns a sequence of $M$ challenges chosen at random and independently from the list of CRPs with identification number equal to $w_{\text{id}}$. The verification stage proceeds as discussed in Section 2, as well as in Refs. [15,16]. If an adversary has stolen the PUK, he cannot impersonate the legitimate owner without knowledge of the PIN, while the probability for an adversary to guess correctly the $n-$bit PIN is negligible. Moreover, the random string $w$ is essentially the output of

a physical one-way function with input $\mathbf{\Psi}$, while the probability for the $j$th bit of $w$ to be 0 or 1 is expected to be approximately equal to 0.5 [6,34]. As a result, it is hard for an adversary to infer the random pattern $\mathbf{\Psi}$, or the PIN from $w_{\mathrm{id}}$. It is worth emphasizing that one can incorporate both of the validation of the PIN and the verification of the PUK in the set-up of Figure 2, after a few amendments. More precisely, by adding a half-wave plate and an additional PBS at the output, one can select to image the speckle onto a camera (for the PIN validation), or onto the optical plane where SMF B is positioned (for the PUK verification) [20,21]. Hence, the set-up can operate in two different modes. Note also that, in the "PIN-validation" mode, an intense probe has to be used in order to obtain a clear speckle, whereas, in the "PUK-verification" mode, the set-up has to operate with parameters that are dictated by the present as well as previous security analyses. Finally, we cannot exclude alternative ways to link an optical PUK to a PIN e.g., through the control of laser parameters (such as the angle of incidence and the wavelength) [6], and/or the control of the target mode at the output [35].

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| PUK | Physical unclonable key |
| EAP | Entity authentication protocol |
| HD | Homodyne detection |
| LO | Local oscillator |
| SMF | Single mode fiber |
| SLM | Spatial light modulator |
| CRP | Challenge response pair |
| DHA | Dual-homodyne–detection attack |
| UDA | Unambiguous-state-discrimination attack |
| SRA | Square-root-measurement attack |

## References

1. Menezes, A.; van Oorschot, P.; Vanstone, S. *Handbook of Applied Cryptography*; CRC Press: Boca Raton, FL, USA, 1996.
2. Martin, K.M. *Everyday Cryptography: Fundamental Principles and Applications*; Oxford University Press: Oxford, UK, 2012.
3. Herder, C.; Yu, M.D.; Koushanfar, F.; Devadas, S. Physical Unclonable Functions and Applications: A Tutorial. *Proc. IEEE* **2014**, *102*, 1126–1141. [CrossRef]
4. Rührmair, U.; Holcomb, D.E. PUFs at a Glance. In Proceedings of the Conference on Design, Automation and Test in Europe (DATE'14), Dresden, Germany, 24–28 March 2014.
5. Daihyun, L.; Lee, J.W.; Gassend, B.; Suh, G.E.; van Dijk, M.; Devadas, S. Extracting secret keys from integrated circuits. *IEEE Trans. Very Large Scale Integr. Syst.* **2005**, *13*, 1200–1205. [CrossRef]
6. Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. Physical one-way functions. *Science* **2002**, *297*, 2026–2030. [CrossRef] [PubMed]
7. Maes, R. *Physically Unclonable Functions: Constructions, Properties and Applications*; Springer: New York, NY, USA, 2013.

8. McGrath, T.; Bagci, I.E.; Wang, Z.M.; Roedig, U.; Young, R.J. A PUF taxonomy. *Appl. Phys. Rev.* **2019**, *6*, 011303. [CrossRef]

9. Santikellur, P.; Bhattacharyay, A.; Chakraborty, R.S. Deep Learning Based Model Building Attacks on Arbiter PUF Compositions. Cryptology ePrint Archive, Report 2019/566. 2019. Available online: https://eprint.iacr.org/2019/566 (accessed on 24 October 2019).

10. Khalafalla, M.; Gebotys, C. PUFs Deep Attacks: Enhanced modeling attacks using deep learning techniques to break the security of double arbiter PUFs. In Proceedings of the 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), Florence, Italy, 25–29 March 2019; pp. 204–209.

11. Ganji, F.; Forte, D.; Seifert, J.P. PUFmeter a Property Testing Tool for Assessing the Robustness of Physically Unclonable Functions to Machine Learning Attacks. *IEEE Access* **2019**, *7*, 122513–122521. [CrossRef]

12. Delvaux, J. Machine-Learning Attacks on PolyPUFs, OB-PUFs, RPUFs, LHS-PUFs, and PUF–FSMs. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2043–2058. [CrossRef]

13. Rührmair, U.; Hilgers, C.; Urban, S.; Weiershäuser, A.; Dinter, E.; Forster, B.; Jirauschek, C. Optical PUFs Reloaded. Cryptology ePrint Archive, Report 2013/215. 2013. Available online: https://eprint.iacr.org/2013/215 (accessed on 24 October 2019).

14. Goorden, S.A.; Horstmann, M.; Mosk, A.P.; Škorić, B.; Pinkse, P.W.H. Quantum-secure authentication of a physical unclonable key. *Optica* **2014**, *1*, 421–424. [CrossRef]

15. Nikolopoulos, G.M.; Diamanti, E. Continuous-variable quantum authentication of physical unclonable keys. *Sci. Rep.* **2017**, *7*, 46047. [CrossRef]

16. Nikolopoulos, G.M. Continuous-variable quantum authentication of physical unclonable keys: Security against an emulation attack. *Phys. Rev. A* **2018**, *97*, 012324. [CrossRef]

17. Vellekoop, I.M. Feedback-based wavefront shaping. *Opt. Express* **2015**, *23*, 12189–12206. [CrossRef]

18. Mosk, A.P.; Lagendijk, A.; Lerosey, G.; Fink, M. Controlling waves in space and time for imaging and focusing in complex media. *Nat. Photonics* **2012**, *6*, 283. [CrossRef]

19. Poppoff, S.K.; Lerosey, G.; Fink, M.; Boccara, A.C.; Gigan, S. Controlling light through optical disordered media: transmission matrix approach. *New J. Phys.* **2011**, *13*, 123021. [CrossRef]

20. Defienne, H.; Barbieri, M.; Chalopin, B.; Chatel, B.; Walmsley, I.; Smith, B.; Gigan, S. Nonclassical light manipulation in a multiple-scattering medium. *Opt. Lett.* **2014**, *39*, 6090–6093. [CrossRef] [PubMed]

21. Huisman, T.J.; Huisman, S.R.; Mosk, A.P.; Pinkse, P.W. Controlling single-photon Fock-state propagation through opaque scattering media. *Appl. Phys. B* **2014**, *116*, 603–607. [CrossRef]

22. Huisman, S.R.; Huisman, T.J.; Wolterink, T.A.W.; Mosk, A.P.; Pinkse, P.W.H. Programmable multiport optical circuits in opaque scattering materials. *Opt. Express* **2015**, *23*, 3102–3116. [CrossRef]

23. Leonhardt, U.; Böhmer, B.; Paul, H. Uncertainty relations for realistic joint measurements of position and momentum in quantum optics. *Opt. Commun.* **1995**, *119*, 296–300. [CrossRef]

24. Schleich, W.P. *Quantum Optics in Phase Space*; John Wiley & Sons: Hoboken, NJ, USA, 2011.

25. Chefles, A.; Barnett, S.M. Optimum unambiguous discrimination between linearly independent symmetric states. *Phys. Lett. A* **1998**, *250*, 223–229. [CrossRef]

26. Ivanovic, I.D. How to differentiate between non-orthogonal states. *Phys. Lett. A* **1987**, *123*, 257–259. [CrossRef]

27. Peres, A. How to differentiate between non-orthogonal states. *Phys. Lett. A* **1988**, *128*, 19. [CrossRef]

28. Dieks, D. Overlap and distinguishability of quantum states. *Phys. Lett. A* **1988**, *126*, 303–306. [CrossRef]

29. Barnett, S.M.; Croke, S. Quantum state discrimination. *Adv. Opt. Photonics* **2009**, *1*, 238–278. [CrossRef]

30. Weir, G. Optimal Discrimination of Quantum States. Ph.D. Thesis, University of Glasgow, Glasgow, UK, 2018.

31. Izumi, S.; Takeoka, M.; Wakui, K.; Fujiwara, M.; Ema, K.; Sasaki, M. Optical phase estimation via the coherent state and displaced-photon counting. *Phys. Rev. A* **2016**, *94*, 033842. [CrossRef]

32. Croal, C.; Peuntinger, C.; Heim, B.; Khan, I.; Marquardt, C.; Leuchs, G.; Wallden, P.; Andersson, E.; Korolkova, N. Free-Space Quantum Signatures Using Heterodyne Measurements. *Phys. Rev. Lett.* **2016**, *117*, 100503.10.1103/PhysRevLett.117.100503. [CrossRef] [PubMed]

33. Van Enk, S. Unambiguous state discrimination of coherent states with linear optics: Application to quantum cryptography. *Phys. Rev. A* **2002**, *66*, 042313. [CrossRef]

34. Horstmayer, R.; Judkewitz, B.; Vellekoop, I.M.; Assawaworrarit, S.; Yan, C. Physical key-protected one-time pad. *Sci. Rep.* **2013**, *3*, 3543. [CrossRef]

35. Nikolopoulos, G.M. Optical scheme for cryptographic commitments with physical unclonable keys. *Opt. Express* **2019**, *27*, 29367–29379. [CrossRef]