Universidad de Sevilla

Grado en Física

Evaluation of PUF and QKD integration techniques as root of trust in communication systems

Trabajo de Fin de Grado

Blanca A. López Ríos

Tutores:

Macarena Cristina Martínez Rodríguez

Antonio José Acosta Jiménez

Departamento de Electrónica y Electromagnetismo

Facultad de Física

Sevilla, Junio de 2022

A mi padre, por darme alas.

Y a mi madre, por ponernos los pies en el suelo a los dos.

Resumen

La Criptografía Cuántica podría ser la próxima tecnología clave en relación a la seguridad de las comunicaciones pero, como toda nueva tecnología, presenta problemas que deben ser resueltos antes de llegar a ser una realidad en el día a día. Este trabajo discute la integración de Funciones Físicas No-Clonables (PUFs, por sus siglas en inglés) como solución a la autenticación de los extremos en un protocolo de comunicación cuántica. El uso de PUFs permitiría la autenticación de dispositivos sin necesidad de depender de terceros, además de abrir la posibilidad a la conmutación de canales de comunicación cuántica; dos características nunca vistas en la Distribución Cuántica de Claves (QKD, por sus siglas en inglés) hasta ahora. Se analiza en detalle la integración de PUFs en el protocolo BB84, ya que es la base de todos los protocolos de QKD, y se proponen dos esquemas de autenticación distintos, atendiendo a las características de los extremos de la comunicación y la distancia entre ellos. Después, estas propuestas se generalizan para el resto de protocolos de QKD. Además, se estudian distintos tipos de PUF con el objeto de encontrar la más adecuada para nuestro propósito.

Abstract

Quantum Cryptography could be the next key technology in terms of secure communication, but, as with every new technology, it presents problems that need to be solved in order to become a reality in daily life. This work discusses the integration of Physical Unclonable Functions (PUFs) as a solution for the authentication of the endpoints in quantum communication protocols. The use of PUF constructions would allow the authentication of devices without the need of relying on third parties, and support switched trustworthy quantum communication channels; two unseen features in Quantum Key Distribution (QKD) until now. We analyze in detail PUF integration within the BB84 protocol, as it is the foundation for all QKD protocols, and two proposals for an authentication scheme are made, depending on the connection characteristics of the communication endpoints and the distance between them. These proposals are then generalized for other types of QKD protocol. Moreover, different types of PUF are analyzed to conclude which ones are the most suitable for our purpose.

Contents

Chapter 1: Introduction

When cryptography is outlawed, bayl bhgynf jvyy unir cevinpl.

– John Perry Barlow

1.1 Cryptography and Public Key Distribution

The term "cryptology" comes from the Greek *kryptos* (hidden) and *logos* (word) and it refers to the science of secure information, embodying both: cryptography, the art of code-making, and cryptanalysis, the art of code-breaking.

Originally, the security of the communication depended on the secrecy of the encrypting and decrypting procedures; however, today we exchange encrypted messages for which the algorithm for encrypting and decrypting could be known by anyone without compromising the security of the communication. The scheme shown in Figure 1.1 was the first of this new type of cryptography. It relies on the fact that the emitter of the message (for now on known as Alice) and the receiver (known as Bob) have symmetric secret keys.

Symmetric key cryptography works by Alice combining the plain (non-encrypted) text with a secret key, using some encryption algorithm, to obtain the (encrypted) ciphertext

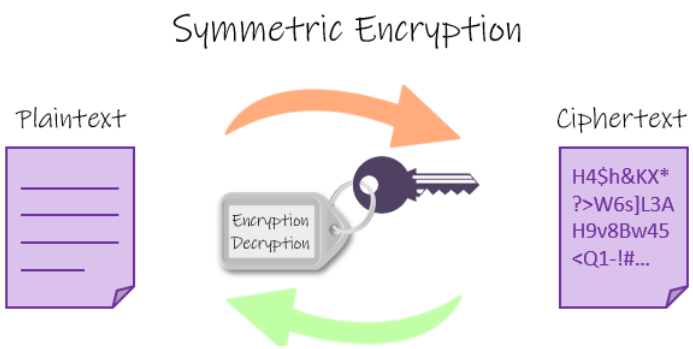


Figure 1.1: Symmetric key cryptography scheme [1].

to be sent. This encoded message is then sent to Bob, who reverses the process, recovering the plain text with the secret key using the decryption algorithm. An eavesdropper (from now on known as Eve) cannot deduce the plain message without knowing the key, even if he knows the decryption algorithm.

When using this scheme, we have to consider two difficulties it presents. First, it must not be possible for a third party to deduce the key, hence truly random numbers must be used. Second, the security in the key distribution process is absolutely a priority: the key must not be intercepted by Eve.

The symmetric key cryptography became widely replaced in the mid 70's, when public-key cryptography was developed. This new scheme uses pairs of keys: one public key and one private key. A simple explanation of this system is presented in [2], using the image shown in Figure 1.2: it is like using a padlock (the public key) and its key (the private key).

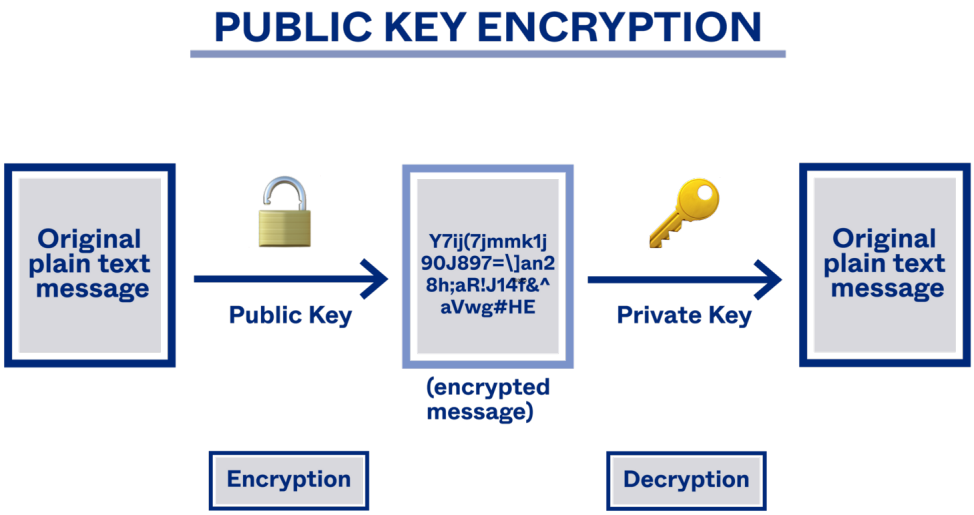


Figure 1.2: Public key cryptography scheme [3].

In a pre-communication step, Bob sends Alice an open padlock keeping with him the key. Alice makes sure that the padlock came from Bob (this is achieved by special certificates, which are emitted by trusted partners, and associate a pair of keys to a particular identity), and protects the intended message with the padlock before transmitting it. The only person who can unlock the message is then Bob.

In reality, these padlocks are one-way functions: mathematical expressions that are easy to generate, but difficult to reverse. For example, it is easy to compute the product of two prime numbers but to factorize the result is not, especially when such numbers are represented by at least 2048 bits.

Although this scheme is the most commonly used and serves well in ordinary applications, such as message encryption, digital signatures, and certificates [4], it is vulnerable to technological and mathematical progress. The development of computing systems or the discovery of an algorithm that allows the reversal of one-way functions are real threats that scientists are fully aware of.

As a paradigmatic example of this search, we have the algorithm for integer factorization proposed by Peter Shor in 1994 [5]. This algorithm, running on a quantum computer, would allow not only to reverse the one-way functions used by the most popular asymetric algorithm, the Rivest-Shamir-Adleman (RSA) algorithm [6], which works with large biprime numbers; but it would also solve the Discrete Logarithm Problem (DLP) on which others of the main asymetric cryptography schemes, such as Elliptic Curve Cryptography (ECC) [7] [8], Diffie-Hellman (DH) [9] or Digital Signature Algorithm (DSA) [10] are based. All of this in polynomial time. Therefore, suitable methods for guaranteeing security in communication are always in search and seizure.

1.2 Basic notions of Quantum Key Distribution

Quantum Key Distribution (QKD) is a quantum cryptography scheme that bases its security level on general principles of quantum physics [11]. First, the mere observation (measurement) of a quantum object perturbs it in an irreparable way, making it impossible for an eavesdropper to intercept a key represented by quantum objects without being detected. Second, the no-cloning theorem (a direct consequence of the Uncertainty Principle) states that it is not possible to duplicate an unknown state while keeping the original intact. The proof of this theorem is really easy [12], so let us discuss it, as it may help us get used to the notation we will be using in this work.

Firstly, we need to introduce some basic concepts used in QKD and quantum information technology in general. While in classical communication, information is presented in form of bits; which can hold two possible values, either of the binary digits 0 or 1, quantum information relies on quantum bits (qubits), that have quantum characteristics; being capable of simultaneously taking the value of 0 and 1.

As said, a qubit is the fundamental unit of quantum information, and it comes mathematically represented as a combination of the two binary states, 0 and 1. As a mental image, we can think that the values 0 and 1 act like the north and the south poles of a sphere, representing every point on the sphere by a superposition of them [13]. A scheme for this image, called the Bloch sphere, is shown in Figure 1.3. In reality, qubits are

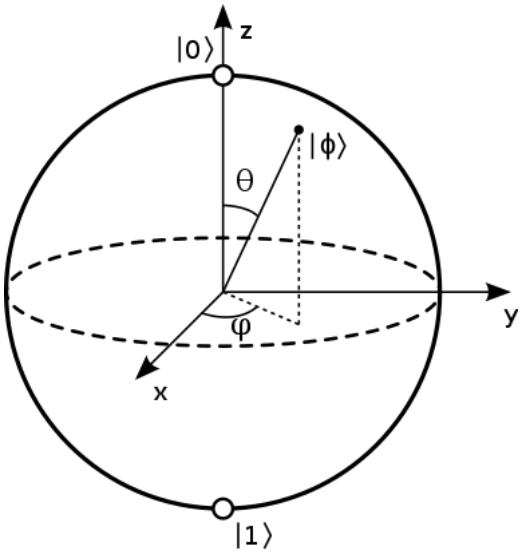


Figure 1.3: Bloch sphere [14].

quantum particles (usually photons), in a state defined by the superposition of the values 0 and 1. In summary: a qubit is like a bit that can be 0 and 1 at the same time. Moreover, as every quantum object, if this qubit is measured, the original superposition state is destroyed, and no further information can be obtained about it.

Quantum states in general are usually represented as a ket in Dirac's notation: $|\Phi\rangle$. This is the notation we will be using as well to represent qubits.

For any set of classical bits, clonning is a simple task: you read the sequence and reproduce a copy of each bit from left to right; for example, if you have the sequence 100110, the cloning procedure would yield 100110 100110, two identical copies of the original bit set. But qubits are protected from this type of cloning process since they are quantum objects. Let us begin with the proof of the no-cloning theorem using an unitary transformation U on any quantum state $|\Phi_1\rangle$ and then see if linearity validates the result or not. If this state is to be cloned, transformation results in $U(|\Phi_1\rangle\,|0\rangle) = |\Phi_1\rangle\,|\Phi_1\rangle$. Let $|\Phi_2\rangle$ be a quantum state orthogonal to state $|\Phi_1\rangle$. For operation U to clone quantum states, $U(|\Phi_1\rangle\,|0\rangle) = |\Phi_1\rangle\,|\Phi_1\rangle$ and $U(|\Phi_2\rangle\,|0\rangle) = |\Phi_2\rangle\,|\Phi_2\rangle$. Considering another state $|\Phi_3\rangle = \frac{1}{\sqrt{2}}(|\Phi_1\rangle + |\Phi_2\rangle)$. By linearity, we have:

$$U(|\Phi_3\rangle\,|0\rangle) = \frac{1}{\sqrt{2}}(U(|\Phi_1\rangle\,|0\rangle) + U(|\Phi_2\rangle\,|0\rangle)) = \frac{1}{\sqrt{2}}(|\Phi_1\rangle\,|\Phi_1\rangle + |\Phi_2\rangle\,|\Phi_2\rangle) \tag{1.1}$$

But since U is a cloning transformation, $U(|\Phi_3\rangle\,|0\rangle) = |\Phi_3\rangle\,|\Phi_3\rangle$. So, we get:

$$|\Phi_3\rangle |\Phi_3\rangle = \frac{1}{2}(|\Phi_1\rangle |\Phi_1\rangle + |\Phi_1\rangle |\Phi_2\rangle + |\Phi_2\rangle |\Phi_1\rangle + |\Phi_2\rangle |\Phi_2\rangle) \tag{1.2}$$

which is not equal to 1.1, proving the no-cloning theorem[1].

We have proved that a general quantum state cannot be cloned, thus we can be sure no qubit can be cloned by any physical method. The fact that the security of quantum communication can be guaranteed by the principles of quantum mechanics suggests the possibility of unconditional security without imposing any computational assumptions.

But not everything is as good as it seems in theory: if Alice and Bob want to establish a secret key at a distance, they need to be conected by two channels: a quantum channel, which allows them to share quantum signals; and a classical channel [11]. Although the quantum channel can be open to any possible manipulation from a third party (thanks to the reasons discussed earlier), the classical channel needs to be authenticated, meaning that Alice and Bob must certifiably identify themselves to ensure the security of the communication, and furthermore, this authentication has to be made every time Alice and Bob establish a connection. In summary, the only flaw of QKD is to know if you are sharing the key with the right person. Usually this authentication is made by the use of certificates, or by the use of a symmetric classical key scheme, where the key used has been shared beforehand. This impplies that the authentication of the the devices used by Alice and Bob relies on a third party or on human interaction [13].

1.2.1 Applications of Quantum Communication and QKD

Quantum Communication is a very recent technology and is still developing its potential. Even so, several applications are being proposed and proved in the literature. Starting from enabling secure communication between a pair of arbitrary endpoints: secure data exchanges are needed in many processes such as online banking and trading, national security, health data exchange... Other areas where Quantum Communication has been considered include Blind Quantum Computation (that is the remote use of a quantum computer without the privacy of the user being leaked to said computer), clock synchronization and longer telescope baseline [12].

[1]Note that it is still possible to "copy" the quantum state by determinating it (i.e, measuring it) and creating a new state with that information. Nevertheless, this process would destroy the original state, as the measure alters the quantum system irreparably.

1.3 Basic notions of Physical Unclonable Functions

1.3.1 What is a Physical Unclonable Function

A Physical Unclonable Function (PUF) is a device that takes advantage of inherent randomness introduced during manufacturing to give a physical entity an unique "fingerprint" [15]. PUFs are clone proof, cost efficient and resistant to various physical attacks. The output produced by a PUF (suitable to be used as a key) is internal to the device and is not assigned by an outside source (thus, the random variation is analogous to an unique fingerprint). For each PUF, an input query or "challenge" receives an instance specific output or "response", a process known as a Challenge-Response Pair (CRP). A CRP can be lodged and then later used to identify the authenticity of a PUF. Remote authentication is also possible once the CRP is recorded in a secure database only known by the trusted party (server).

Although there are many PUF constructions, we can divide them into two broad categories [16]: weak PUFs and strong PUFs. The names of the groups can be misleading, as the names are not related to the level of security provided by the PUF, instead, the two categories differ in the use the PUFs are given.

Weak PUFs have a small CRP space, that is, they can provide a small number of values[2]. As a consequence, if an attacker can physically access the PUF, they would gain the full set of CRP for any given time, and even if the PUF cannot be physically copied, the knowledge of the full set of CRPs will surely be enough to simulate the PUF behaviour (in our terms, Eve could impersonate Bob at any time). Weak PUFs are generally utilized for key reconstruction and as source of entropy for the generation of Number used Only Once (nonce)[3] and seeds.

On the other hand, strong PUFs have a very large CRP space, so large that even if an attacker can access the PUF at a given time, it would not be possible for them to record all of the CRPs. This implies that no one but the user with physical access to the PUF at the time where the challenge is received can give the correct response to be authenticated. This is why strong PUFs are usually implemented for identification and authentication processes. However, since strong PUFs generally do not have any protection that prevents an eavesdropper from challenging the PUF and getting a response, they are vulnerable against numerical modelling attacks.

[2]We are talking about low hundreds.

[3]An arbitrary number used just once in a crypthography exchange.

We can make another classification of PUFs, according to the implementation process of the PUF in an Integrated Circuit (IC): non-silicon PUFs, which require special fabrication steps, and silicon PUFs, which can be implemented by standard manufacturing processes [17].

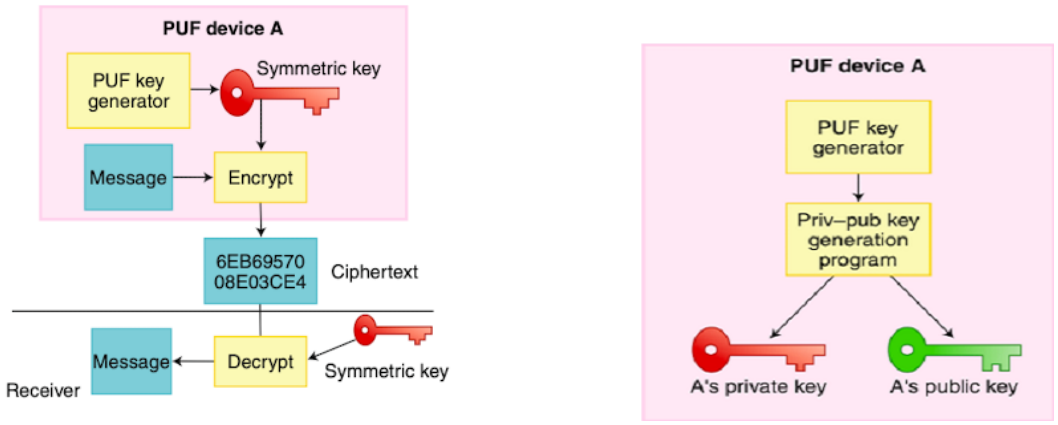
As said, non-silicon PUFs can only be implemented in ICs by adding special fabrication steps, making them costlier and more difficult to install in a device. They base their CRPs on the measurements over a special layer of deposed material that contains some kind of embedded elements. Examples of this type of PUFs are coating PUFs [18], which incorporate a layer of dielectric material containing dielectric particles of different electrical permittivity and base its CRPs in the measurement of the capacitance of said layer, and optical PUFs [19], which consist of a thin layer that contains light scattering particles that produce a speckle pattern when irradiated with a laser beam. The optical PUF will be discussed in more depth in Chapter 3.

Alternatively, we have silicon PUFs, which exploit the small variations that occur in the Complementary Metal-Oxide-Semiconductor (CMOS) manufacturing process of an IC. Depending on the parameter selected to make the PUF, we have different types of silicon PUF, being able to classify them into three subgroups [17]: leakage-current-based PUFs [20], which are based on the different leakage current consumption that different physical realizations of the same circuit have, delayed-based PUFs as arbiter PUFs [21] and Ring Oscillator (RO) PUFs [22] [23], which exploit the fact that even implementig identical layout masks, the manufacturing process inserts delays in different realizations of the same circuits, and memory-based PUFs as SRAM PUFs [24], butterfly PUFs [25] and NOR PUFs [26], which use cross-coupled circuits that count with two stable opperating points and one unstable opperating point, when the circuit is not driven by any input, the mismatches between the two ideally symmetrical parts of the cross-coupled circuit make the circuit go more often to one of the two stable states. Later in this work, we will analyze RO and butterfly PUFs in more detail.

As we have said, strong PUFs are usually implemented for identification and authentication processes. Therefore, we will focus on them, as our goal is to set a PUF-based ID to overcome the QKD flaw: being sure you are sharing the key with the right person.

1.3.2 Using a PUF as authenticator

Currently, the PUF-derived key is usually presented in a symmetric manner, the first type of scheme we discussed in Section 1.1. The verifier who enrols the PUF key and the PUF



(a) Symmetric scheme. (b) Asymmetric scheme.

Figure 1.4: PUF key scheme for device authentication [27].

device (prover) restores the same key (in essence: if Alice wants to verify that it is Bob who is receiving the message, she must know his PUF beforehand) [27]. This scheme is shown in Figure 1.4a, where the PUF device counts with a key generator, which is used to derive an actual key suitable for symmetric cryptographic algorithms. Using a PUF-based symmetric scheme authentication would not be any better than using a shared-key authentication scheme, not adding any extra security layer.

On the other hand, PUFs can also offer us an asymmetric scheme: a PUF device with its key generator, derives a key that meets the constraints imposed by an asymmetric cryptographic algorithm and can be used directly as a private key. Then, a corresponding public key is generated, building upon the private key and being broadcasted on a public-key server [27]. This scheme is shown in Figure 1.4b.

Another possibility of creating a public and private key pair is to use the PUF to produce a stream of random bits which, combined with another random number source (or sources), is used to seed a public-private key pair generation process [28].

The advantage of this asymmetric key setting is that the private and public key pair is bound to the PUF device. Any party can now conveniently authenticate this PUF device by sending a nonce and accepting the PUF authenticity if the private key signature (that is, the nonce signed) is correctly verified by using the public key. Secure device-to-device communication is naturally enabled, and only the intended PUF device can apply the private key to open/decrypt the message encoded by its public key [27]. This application can be seen in Figure 1.5.

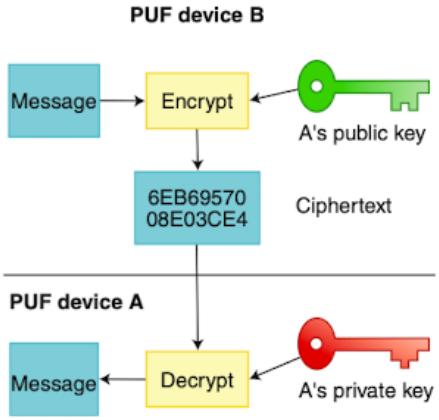


Figure 1.5: PUF asymmetric key scheme application for device authentication [27].

1.4 Goals and motivations

Threatened by the increase of computational power and the evolution of cryptanalysis techniques, cryptography has to implement new technologies and schemes in order to ensure security against new strong attacks. QKD provides a scheme for secure key sharing relying on Quantum Mechanics Principles. Although the information is physically secure in this scheme, the endpoints need to be sure they are sharing this information with the right peer, i.e. they need mutual authentication in order to ensure totally secure communication.

Nowadays, this authentication presents two problems: first, it is traditionally done by the use of special certificates, relying its security on an external third party with human intervention [13]; second, the authentication schemes do not allow the use of switched QKD channels: every time a new connection between two endpoints is established, the human-mediated process has to be repeated [11].

This work analyzes a possible solution for these authentication issues, using special PUF constructions, addressing both: the need of an external trusted third party and the limitations for switched QKD channels.

The structure is as follows: in Chapter 2, the BB84 protocol is explained in depth, as it lays the foundations for all the other QKD protocols. Next, in Chapter 3, the integration of a PUF-based authentication into the BB84 protocol is analyzed; firstly, discussing the theoretical authentication scheme (Section 3.1), and secondly, evaluating which type of PUF is the most appropriate for it (Section 3.2). In Chapter 4, other QKD protocols are taken into account, exploring the integration of a PUF-based authentication scheme

within them. Finally, Chapter 5 gathers the conclusions of this dissertation.

Chapter 2: The BB84 protocol

When you change the way you look at things, the things you look at change.

– Wayne Dyer

The BB84 protocol is a discrete variable coding named after its inventors, Charles Bennet and Gilles Brassard, and the year of its first publication (1984) [29]. This protocol was the first quantum cryptography protocol and laid the foundation for following proposals.

2.1 Protocol definition

The protocol is as follows:

1. Alice prepares a random set of qubits selected from one of the next four states:

$$\text{Base 1} \leftrightarrow \left\{ \begin{array}{l} |\Phi_0\rangle = |0\rangle \\ |\Phi_1\rangle = |1\rangle \end{array} \right\} \tag{2.1}$$

$$\text{Base 2} \leftrightarrow \left\{ \begin{array}{l} |\Phi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |\Phi_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array} \right\} \tag{2.2}$$

   and send them to Bob via a quantum channel. Note that each pair of states forms a base of a two-dimension quantum space; therefore, the conditions $\langle\Phi_0|\Phi_1\rangle = 0$ and $\langle\Phi_+|\Phi_-\rangle = 0$ corresponding to scalar products between states have to be satisfied. At the same time, states in the different bases defined are not orthogonal and have maximum overlapping[1]. This means that there is no measurement procedure capable of determining with 100% certainty the specific state in which Alice prepared the qubit.

[1]Overlap is the meassure of the diferrence between two quantum states, i.e $|\langle\Phi_a|\Phi_b\rangle|$.

2. Bob receives the qubits and randomly chooses one of the two possible bases to measure, performs the measurement, and records the results.

3. Bob uses a public channel to announce to Alice the position and the base used to measure each bit (without indicating the result of this measure). This sequence is called the raw key.

4. Alice and Bob keep the bits for which the base employed in the enconding and the decoding processes coincide and discard the rest[2]. This generates what is called the sifted key, which has the length of around half of the bits originally sent (due to Bob having 50% chance to choose the right base).

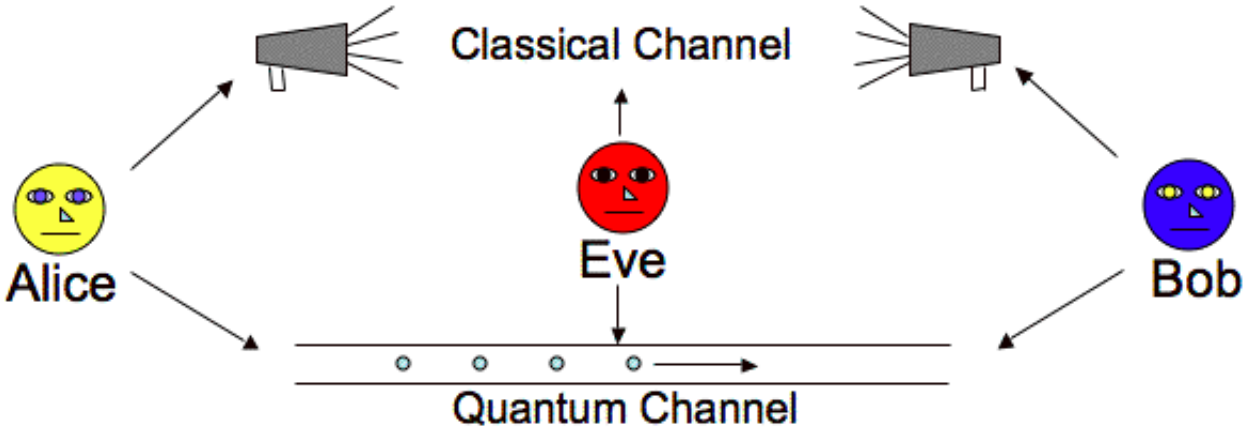


Figure 2.1: A basic sketch of Quantum Key Distribution [30].

There is no mechanism to prevent the interception of the qubits sent in the first step by an unwanted eavesdropper (Eve). So it is thought possible for Eve to know part of the key. Anyway, the QKD system allows Alice and Bob to detect the presence of an intruder.

Note that, as Bob, Eve has to choose one of the bases described in Step 1 to perform the measurement and determine the incoming state. Therefore, she has a 50% chance of employing the incorrect base, resulting in a disagreement between what Bob detects and what Alice had sent. Using this fact, Alice and Bob have a really simple way to detect Eve: they just have to perform an error detection check by sharing a subset of the bits. If the error rate is high, they discard the key and start over. If the error rate is

[2]If Bob measures a qubit in the original base it was sent, they can be sure both have the same value for that specific bit.

small, Alice and Bob can carry out other processes known as error correction and privacy amplification over the rest of the bits in the key that have not been made public.

While a quantum error correcting protocol is necessary to preserve quantum states against noise and other unwanted interactions that may occur during the communication process [31], privacy amplification is a general cryptography technique for distilling highly secret shared information from a larger body of shared information that is only partially secret [32], i.e. privacy amplification is used to counteract the knowledge Eve may have acquired by spying the communication.

The unconditional security of the BB84 protocol has been proved with different methods [33] [34].

2.2 Practical implementation

Let us now discuss the most relevant methods for the implementation of the BB84 protocol [35].

2.2.1 Polarization encoded systems

In this scheme Alice has four laser diodes which emit photon pulses polarized at $-\frac{\pi}{4}$, 0, $\frac{\pi}{4}$ and $\frac{\pi}{2}$ rad. For a given bit, only one diode is triggered. After a set of attenuating filters, just a photon is sent for each bit, encoding the information in its polarization.

These photons travel by optic fiber to Bob's location, where they are extracted and put through a set of waveplates designed to restore the initial polarization states, which may have suffered a little transformation due to the fiber path. Then, they reach a Beam-Splitter (BS), responsible of implementing the random base choice and finish their route travelling through a polarizing BS (for base 1 photons are analyzed in a vertical-horizontal filter and for base 2 they go through a diagonal filter) endend in two photon-countig detectors.

As an example, let us take the values of Figure 2.2 (this is: bit=0 if the polarization is $\frac{\pi}{2}$ or $\frac{\pi}{4}$ rad, and bit=1 if the polarization is 0 or $-\frac{\pi}{4}$ rad). Imagine that a 0 rad polarized photon prepared by Alice reaches the symmetric BS and it is randomly transmitted to "base 1", it will surely be counted as "1", thus the used filter does not change its state. On the other hand, when it reaches the symmetric BS, it has 50% chance to be transmitted to "base 2", where the used filter will transform the original state, producing an uncertain result.

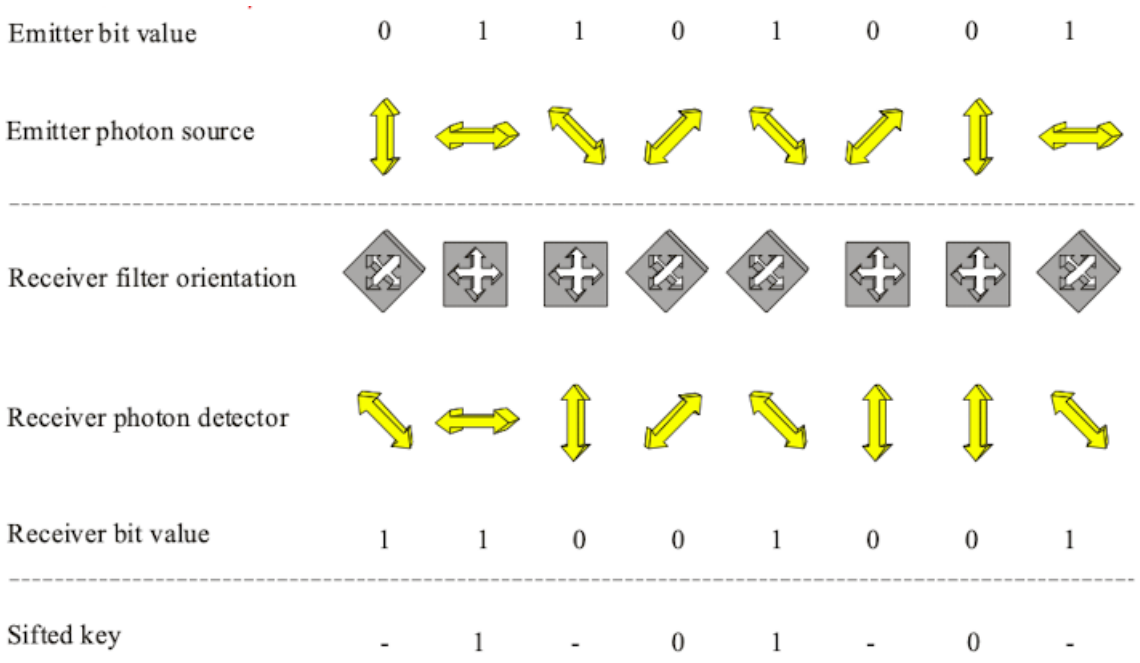


Figure 2.2: Polarization encoding scheme [2].

2.2.2 Phase encoded systems

This scheme is based on the properties of interferometers, and the coding is implemented by changing the relative optical path lengths or phase between the internal arms of an interferometer. In these systems, Alice and Bob share an interferometer, each of them controlling a phase modulator in their respective half. The probability of counting a photon sent by Alice as 1 or 0 varies due to an interference phenomenon related to the phase difference $\Delta\varphi = \varphi_A - \varphi_B$ (in an identical manner to the classical interference pattern). For example, imagine that the device is built to give a 0 if $\Delta\varphi = 0$ rad and return a 1 if $\Delta\varphi = \pi$ rad. Halfway values will not be deterministic: if $\Delta\varphi = \pm\frac{\pi}{2}$ rad the photon is equally likely to be counted as 0 or as 1. As in every other QKD design, if any measurement is applied over the system (even if it is "just" to locate the photon, i.e. know in which arm of the interferometer it is) the information is lost.

The main flaw of using this strategy is the complexity of keeping the path difference stable when the distance between Alice and Bob is larger than a few meters.

2.2.3 Frequency encoded systems

In these systems, Alice has a source that emits short pulses of monochromatic light with a frequency ω_0. The beam goes through an Electro-Optical Modulator (EOM) that mod-

ulates its phase with a radio frequency $\Omega << \omega_0$ and a small modulation depth. This process generates two sidebands at frequencies $\omega_0 \pm \Omega$. The EOM is driven by a radiofrequency local oscillator whose phase, φ_A, can be changed between four values: 0, π and $\frac{\pi}{2}$, $\frac{3\pi}{2}$, which implement the pair of conjugated bases. Before being sent, the signal is attenuated to ensure that it contains only one photon per bit.

When the photon arrives at Bob's location, it experiences a second modulation by another EOM, which has its own local oscillator with the same frequency Ω and a phase φ_B that can be varied among two values: 0 and $\frac{\pi}{2}$ which represent the choice between bases that Bob has to make to measure the qubits. The sidebands at frequencies $\omega_0 \pm \Omega$ are mutually coherent and thus interfere.

These designs are controlled by the phase of the radiofrequency oscillators, which is six orders of magnitude smaller than the optical frequency and thus easier to stabilize and synchronize.

2.3 Conclusions

The BB84 protocol is the most widely known QKD protocol, as it was the first of its kind and laid the groundwork for the following proposals. We have analyzed the protocol steps, that can be divided in a first part where qubits are involved (Step 1 and Step 2) and a second part where classical information needs to be exchanged (Step 3 and Step 4). An error detecting check, quantum error correction and privacy amplification are then performed.

This protocol can be implemented in several ways, being the use of polarization encoded systems the most used. The security of this protocol has been proved in the literature, as long as the channels used in the processes are authenticated.

Chapter 3: Integration of PUFs into the BB84 protocol

Some things don't mix. Some things don't mix at all, but sometimes in life you have to take the risk.

– Pat Conroy

As we have seen in the previous chapters, the main flaw (and we could daresay the only) in QKD is the authentication of the endpoints of the communication channels. Even more, we could limit the authentication to the classical channel: the one where Alice and Bob share the security sensitive information. Through the quantum channel they exchange qubits, but these qubits do not represent a threat if they are shared with someone else. The qubits are not a key by themselves since Alice and Bob have to go through the steps described in the previous chapter to create an actual key[1].

Integrating PUFs at the endpoints of the classical channel (that is, in the devices used by Alice and Bob) and using them to authenticate the points mentioned in an appropriate step of the communication protocol can be a solution to the dilemma presented in the previous paragraph.

With the aim of ensuring secure communication by QKD, let us first analyze in which step of the BB84 protocol the authentication by PUFs can be included, and second discuss the type of PUF that better suits our purpose.

[1]Also, as discussed in section 1.2, the qubits are "protected" from eavesdroppers by Quantum Mechanics principles.

3.1 Adding an authentication step in the BB84 protocol

At first this analysis might seem easy or even trivial: just add the authencation step wherever, it does not matter as long as the aunthentication is made. But altering a protocol "in the right way" is never a minor discussion, since changing the protocol in an inappropriate manner can lead to big problems like a huge reduction in the speed in the communication and added difficulties in the use of the protocol in real life with the available infrastructures.

An obvious answer to the question "where do we authenticate the endpoints of our communication?" is: before the communication even starts. And that is a good answer. Easy, fast, and secure? In some schemes, the infrastructure used for the quantum channel and the classical channel can be shared. For example, in the practical implementation schemes we have discussed in Chapter 2, the quantum channel was a path of optical fiber that (in general) can also be used as a public channel to exchange the classical information using transmission techniques such as Dense Wave Division Multiplexing (DWDM) [36]. But this is not always the case, and sometimes the channels for the qubits and the classical bits are physically separated. On the other hand, performing the authentication in this early stage can open the door for Eve to wait for the authentication to end, and then, irrupt in the middle of the channel keeping the information sent by Alice and avoiding Bob from communicating Alice that something is wrong with the communication. Eve could get the key if we do not authenticate again at least once more before starting the classical communication.

Another option is to add the authentication step in the middle of the protocol: the qubits are protected from Eve by quantum mechanics, so we can restrict the use of the PUFs in both endpoints to a step prior to the classical communication. The problem of Alice sending the qubits to Eve instead of Bob does not exist: Bob only has to tell Alice that he has not received anything, and she will resend the qubits. Eve does not get any information from the fact that the qubits are sent to her because, to make the key, she will have to authenticate herself on the classical channel.

Both solutions presents its own problem to be addressed: in the first one, we would need a second authentication process before starting the classical communication, meanwhile, in the second option, Alice may have to prepare a new set of qubits and resend them.

The process of preparing and sending qubits takes some time, depending on how far away Alice and Bob are and which enconding system is being used. Using the data shown in Table 3.1, we can perform a simple operation and calculate how much time sending a 2048 bit sifted key consumes. This time increases from 2 ms to 2 min when Alice and Bob are separated by a few hundred kilometers.

	Encoding system				
	Polarization		**Phase**		**Frequency**
Distance	1 km	200 km	20.06 km	100.8 km	50 km
Sifted-key rate	4 Mbit/s	30 bit/s	1.02 Mbit/s	10.1 bit/s	19.2 bit/s
	[37]	[38]	[39]		[40]

Table 3.1: Sifted key rates performed by different encoding systems, depending on the distance.

A PUF authentication can be considered instantaneous compared to the time frame illustrated in Table 3.1, regardless of how far away the channel endpoints are.

It is fair to say that Alice will not mistake Bob for Eve *always*, and option two presents another advantage over doing two authentications: the channels may not share physical infrastructure. Although we have focused on optical fiber to discuss the practical implementation of the protocol and this medium can be used for both quantum and classical information, not every scheme works in this terms, and the quantum and the classical channels can be independent and uncorrelated. This implies that the protocol we would use to authenticate one channel can differ from the one we would use to authenticate the other, delaying inevitably (and for sure in every new connection between two endpoints) the communication process.

For all the reasons discussed above and because no solution is perfect, we will need to choose one or the other depending on the specific situation, after an analysis of the available infrastructures, distances, encoding systems, environments, etc.

In the next section, we will analyze the PUFs that best suit our goal of giving a PUF-based ID to the devices at our two endpoints.

3.2 Choosing the best authenticating PUF

As we have discussed, many factors must be considered when choosing a PUF to attach to Alice and Bob devices. Measurements of some of these factors reported in the literature can be found in Table 3.2.

PUF Type	PUF Quality factor		
	Sensitivity to enviroment		Implementation Difficulty
	Temperature	Voltage	
Coating [18]	Very high	-	High
Optical [19]	Very high	-	Very high
Leakage Current (180 nm) [20]	Very high	Very high	Medium
Arbiter (180 nm) [21]	4.82% (20 - 70ºC)	3.74% (2% ΔV)	Low
RO (90 nm) [24]	0% (20 - 65ºC)	3.15% (20% ΔV)	Very low
SRAM (90 nm) [41]	12% (-20 - 80ºC)	-	Very low
Butterfly (65 nm) [25]	2.3% (-20 - 80ºC)	-	Very low
NOR (130 nm) [26]	3.91% (0 - 70ºC)	5.47% (20% ΔV)	Low

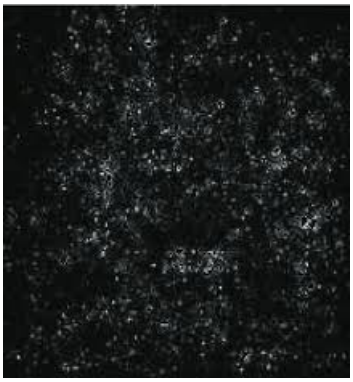
Table 3.2: Measurements of sensitivity to environment and implementation difficulty for different types of PUFs [17].

In Table 3.2 we consider how changes in temperature and voltage affect a specific PUF construction, and how difficult it is to implement said PUF construction on an IC. Based on these measurements, we can conclude that silicon PUFs are easier to implement and less sensitive to environmental changes. However, we will consider implementing a non-silicon PUF, the optical PUF, because it is reprogramable. This advantage will be discussed in depth later. We will also consider the implementation of a RO and a butterfly PUF, thus they are the silicon PUFs with the best reported results in the literature[2].

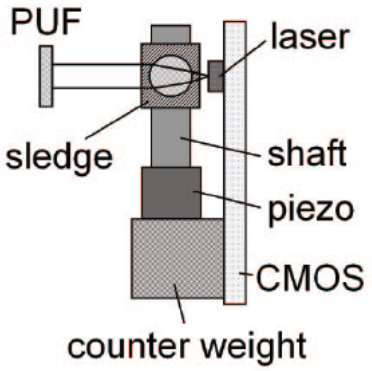
3.2.1 First candidate: Optical PUF

An optical PUF [19] consists of a thin layer that contains light-scattering particles that produce a speckle pattern like the one presented in Figure 3.1a when hit by a laser beam. Note that in order to obtain a digital binary output, we need to process the original response of the PUF by adding additional structures as shown in Figure 3.1b.

[2]Note that for more information about the other types we will not consider, and their measurements, a reference for each one is shown in Table 3.2 next to the name of the PUF type.



(a) Speckle pattern [42].



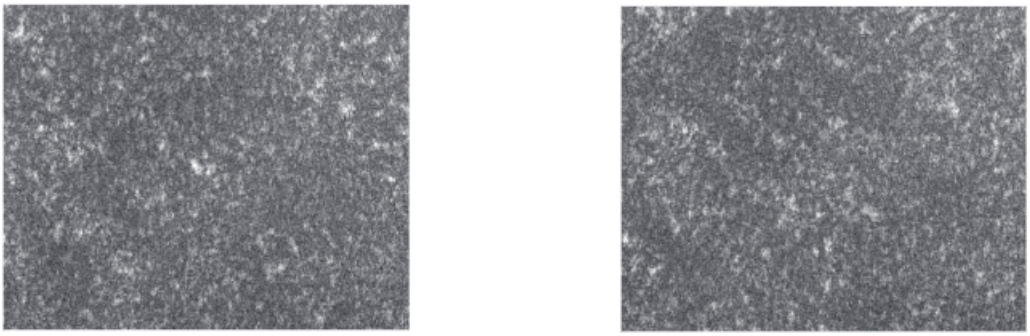
(b) Structure scheme [19].

Figure 3.1: Optical PUF.

This type of PUFs is very difficult to clone in any physical way, due to the sensitivity of the scattering phenomena to very small variations in the locations of the scattering particles. It also presents a huge advantage over other types of PUFs: optical PUFs are reconfigurable.

As we have said, irradiating the PUF with a laser beam gives us a speckle pattern. But if we use an enough energetic laser, we will be able to perturb the particle positions, achieving a new unique and unclonable pattern; see Figure 3.2 for an example.

This attribute is very useful to solve possible future problems such as key leakages: if somehow an unwanted party manages to get the PUF information and becomes capable of modelling it, we can simply "shake" the particles to get a new ID for the communication



(a) Before.

(b) After.

Figure 3.2: An optical PUF speckle pattern before and after irradiation with an energetic laser beam [19].

device. This is not possible in many other types of PUF because they usually rely on an IC characteristic and the only solution to obtain a new PUF is to change said IC for a new one.

While the possibility of having virtually infinite PUFs with just one device is really appealing, it is important to note that optical PUFs are really sensitive to environmental factors: temperature, humidity, movement, and ageing can seriously damage the device, which is also difficult and expensive to integrate in an already built device compared to other types of PUF; as shown in Table 3.2.

3.2.2 Second candidate: Ring Oscillator PUF

An oscillator is a circuit that converts a DC signal into an alternating signal with a specific frequency. A RO is a type of oscillator formed by an odd number of inverter gates. A specific frequency can be achieved by changing the number of inverter gates.

A RO PUF [22] exploits the random but static variations between the frequencies of two allegedly identical ROs. For each comparison of a pair of ROs, we get a bit of information; that is, a PUF formed by n identic ROs could produce $\frac{n!}{2!(n-2)!}$ response bits. But to use these responses as a PUF-based ID we need these bits to be uncorrelated. Otherwise, Eve could deduce the entire ID code by knowing some of the bits.

It has been proven that the frequency of a RO on a chip is influenced by its location on the chip [24]. Ideally, we could eliminate this correlation effect by analyzing the distribution of the RO frequencies, but this process can be costly and certainly time-consuming. As an intermediate solution, to counteract the correlation between bits, the ROs are placed as close as possible and compared only with adjacent ROs. A pessimistic estimate assuming maximum correlation leaves us with (n-1) independent bits for a PUF of n-ROs.

To use a PUF as an ID, we need it to be reliable. That is, we need it to respond the same way for a given challenge without changing when things like temperature and supply voltage fluctuate. As shown in Table 3.2, RO PUFs deal really well with this type of environmental variation, contrary to what we had with optical PUFs. However, it is true that alterations in the voltage supply deteriorate the uniqueness of the PUF [22]. Uniqueness measures how accurately the PUF can identify the device where it is implemented; therefore, if we lose uniqueness, we lose the ability to distinguish two different emitters or receivers.

RO PUFs are really easy to install because we can build them in ordinary Field

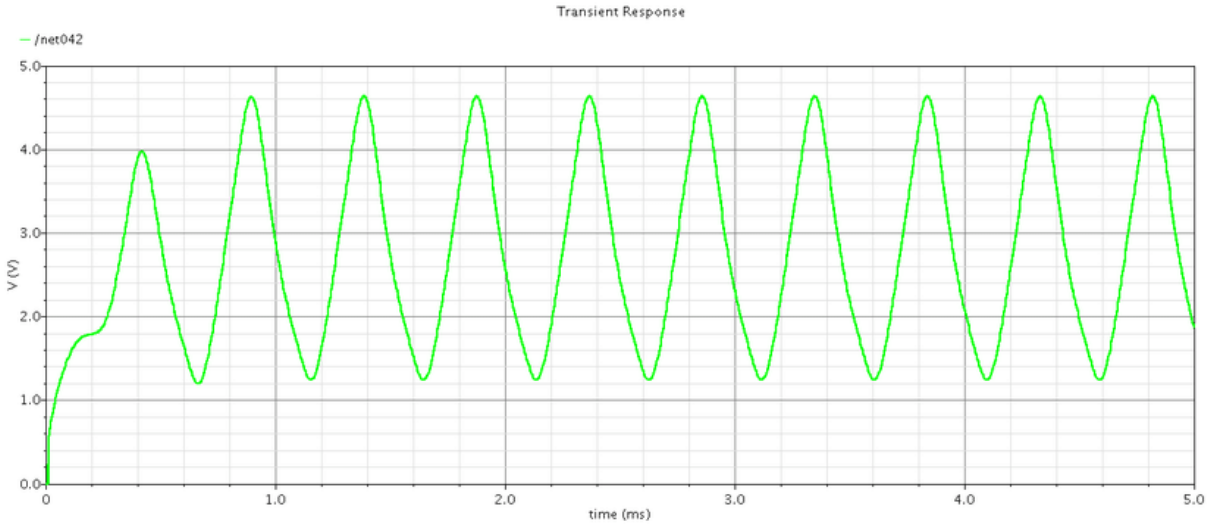


Figure 3.3: 5-stage RO output [44].

Programmable Gate Arrays (FPGAs) and require a very small area. A 5-stage RO PUF (which provides us with 4 independent bits) needs almost a full Configurable Logic Block (CLB), so, to get a 2048 bit key, we would need 512 CLBs, which is totally affordable in a typical FPGA [43].

RO PUFs do present a little disadvantage over other types of PUF: we need some time to obtain the desired response, as the frequencies of the ROs must be stabilized. The output of a 5-stage RO can be seen in Figure 3.3. As shown, the RO needs almost 1 ms to stabilize.

3.2.3 Third candidate: Butterfly PUF

A butterfly PUF [25] is a cross-coupled circuit that behaves as shown in Figure 3.4: it can be brought to an unstable state before allowing it to settle to one of two possible stable states.

To achieve this performance, we can use two latches[3] that bring opposite values when excited with high voltage (this is, for high voltage, Latch 1 gives a 1 and Lacth 2 gives a 0); as a result, when applying this voltage we bring the complete circuit to an unstable point, as both latches have opposite signals on their outputs. When the applied voltage is reduced, the butterfly PUF cell goes to one of the two possible stable states,

[3]A latch is a circuit which retains whatever output state results from a momentary input signal until reset by another signal.

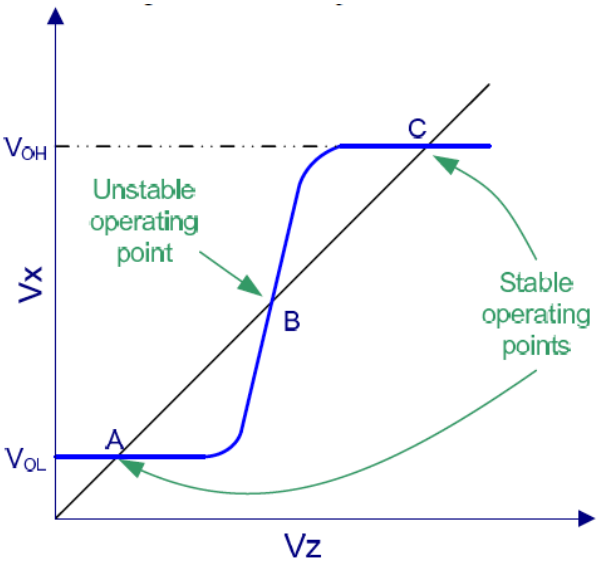


Figure 3.4: Example of cross-coupled circuit behaviour [25].

0 or 1, depending on the differences in the delays of the connecting wires, which are designed as symmetric as possible and similar to every other butterfly PUF cell that may be installed in the device, ensuring that the variation of the responses is based on the intrinsic characteristics of the IC.

A circuit diagram of a butterfly PUF cell is shown in Figure 3.5.

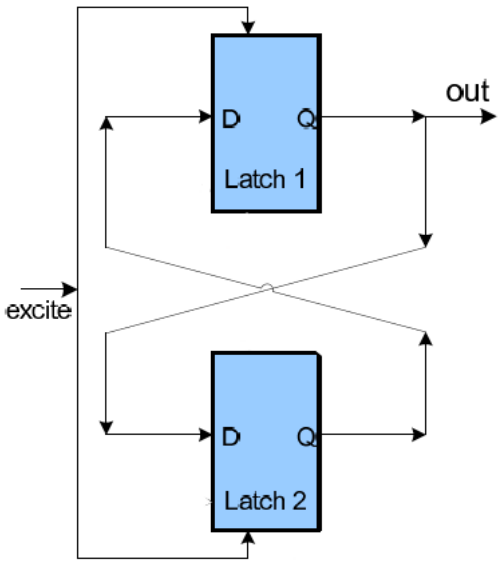


Figure 3.5: Butterfly PUF cell scheme based on a cross-coupled circuit of two latches [25].

This type of PUF can be easily implemented in any FPGA, making it a really cheap and simple way to add an authentication PUF-based device to our communication end-

point. Another advantage of a butterfly PUF is that its responses are directly binary; meanwhile, other PUFs (as we saw when discussing the optical one) need further processing to achieve a digital output. Also, butterfly PUF responses are obtained almost instantaneously, in contrast to other types, such as the RO PUF.

3.3 Conclusions

We have discussed first the correct position of an authentication step inside the BB84 protocol, concluding that depending on how far away our endpoints are, and by which infrastructure are they connected, it is more appropriate to use a scheme with two authentications or a scheme with only one right before starting the classical communication.

If Alice and Bob are separated more than a few tens of kilometers and their quantum and classical channels share the same physical infrastructure, it would be better for the communication process to rely on two authentications: one before starting the protocol and the other in the middle, before classical communication starts.

If Alice and Bob are closer than a few tens of kilometers, it would be better in terms of time consumption and easiness to do just one authentication in the middle of the protocol, after sending the qubits and right before Alice and Bob start sharing classical information. Even if the channels share its infrastructure. This is due to the fact that we have discussed earlier: Alice will not always mistake Bob at the beginning of the communication, saving an authentication round.

If we have any other circumstances, for example, if they are separated more than a few tens of kilometers but the two communication channels do not share their infrastructure, other things like the encoding system or the authentication protocols available for each channel must be taken into account. In general, it will be easier to use the two-authentication scheme, as the authentication protocols are usually faster than the sifted key rates presented in Table 3.1 for different BB84 encoding systems.

Second, we discussed which type of PUF was better for integrating it as an ID for the devices located at our endpoints (i.e. Alice and Bob devices), analyzing different parameters such as environmental sensitivity and implementation difficulty. After a first filter, we limit our candidates to three: optical, RO and butterfly PUFs.

In most applications, the butterfly PUF would be our final choice, as it presents an easy, cheap, and reliable source of achieving a PUF-based ID for a device. On the other hand, we have seen that optical PUFs, as reconfigurable PUFs, give us the chance of renewing our ID (if, for example, an attacker becomes capable of modelling its responses)

without having to modify the device. Although optical PUFs are definitely more expensive and sensitive than butterfly PUFs, the fact that they are reconfigurable may be a decisive attribute when the aim is to protect a device at an endpoint exchanging highly sensitive information, as changing the physical structure of the PUF might be complex if it has to be done several times in a short period of time.

Chapter 4: Integration of PUFs into other QKD protocols

Something that looks like a protocol but does not accomplish a task is not a protocol - it's a waste of time.

– Bruce Schneier

We have focused on analyzing the BB84 protocol, as it was the first protocol proposed for QKD and it is the foundational reference for most today's practical implementations. However, tens of QKD protocols have been proposed since the publication of Bennet and Brassard in 1984.

We can divide QKD protocols into two categories [45]: prepare-and-mesure-based protocols and entanglement-based protocols.

4.1 Prepare-and-measure-based protocols

As the name suggests, in this first type of protocol, the emitter "prepares" the information in the form of qubits and sends them to the receiver, relying on Heisenberg's Uncertainty Principle to protect the information against eavesdroppers. BB84 belongs to the prepare-and-measure category.

Some other protocols of this type are the B92 protocol [46], which is a simplification of the BB84 which only uses two encoding states, the SSP protocol [47], which can be seen as a version of the BB84 with an additional base of the quantum space, the SARG04 protocol [48] and the S13 protocol [49].

The analysis we have made for the BB84 protocol can be applied to any of these prepare-and-measure protocols due to the similarities that all of them share.

In recent years, a different kind of prepare-and-measure protocol has been proposed. An optical field admits two interpretations: a system of single photons or a wave that

travels in space with observable phase and amplitude. While all the protocols presented above work with the first interpretation, this new type of protocol, known as Continuous-Variable (CV) protocols, uses the wave interpretation. Altough in both cases we have to deal with the problems of noise and loss in transmission, the second interpretation comes with an advantage: detecting and measuring the phase and the amplitude of an optical wave is more efficient in operational conditions, suitable for its widespread application.

Basically, CV protocols use the quadrature modulations and measurements of phase and amplitude from a bright laser to encrypt the information [50]. Depending on the protocol, the preparation and measurement processes will differ, and as we saw in the BB84 this will surely affect the secure key rates provided by the protocols. Publications on CV protocols have reported faster secure key rates [51] than discrete-variable protocols, predicting a record of 3 Mbit/s at a distance of 30 km. Although it is a huge improvement over the values presented in Table 3.1 for the different practical implementations of the BB84 protocol, it can be seen [51] that the secure key rate in CV protocols drops drastically when distances are greater than 100 km. Therefore, a two-authentication scheme would still be more efficient when Alice and Bob are separated by more than some tens of kilometers.

4.2 Entanglement-based protocols

Two particles are said to be entangled if the state of the system both form cannot be written as a product as a state-vector for each particle [52]. Imagine a system of two particles, each of spin $\frac{1}{2}$, in a state that can be written as:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|+\rangle_1 |-\rangle_2 \pm |-\rangle_1 |+\rangle_2) \tag{4.1}$$

Here $|+\rangle$ and $|-\rangle$ impplies positive and negative projection of the spin on the z-axis respectively, and the subscript indicates the particle to which the ket belongs. Imagine now that these two particles (each described as 4.1) are separated, and that we measure one of them. The state collapse due to the measurement would fix not only the projection value of the measured particle, but also the projection value of the other one. For example, if we measure particle 1 and it gives a positive projection of the spin as a result, we can be sure that measuring particle 2 would have a negative projection outcome. Entanglement-based QKD bases its protocols on this phenomenon.

The first entanglement-based protocol was proposed by Artur Ekert in 1991 [53],

followed by Bennett, Brassard and Mermin in 1992 [54], and the DPS (2003) and the COW (2004) protocols [55] [56].

In these schemes, one member of an entangled pair is sent to Alice, the other one is sent to Bob, and measures are made at both endpoints.

For this kind of protocol, a record for a secure key rate of 1 Gbit/s has been reported using Superconducting Nanowire Single-Photon Detectors (SNSPDs) over a distance of 1 m [57]. Another research [58] has reported a secure key rate of 300 bit/s over an atmospheric free-space link with a distance of 143 km between the Canary Islands of La Palma y Tenerife. Some promising technologies such as quantum repeaters could help to improve these rates, but nowadays they are all theoretical and definitely difficult to implement.

This discussion has led us to the same conclusion we had with the prepare-and-measure protocols: until we have the technology to ensure faster QKD secure key rates over distances greater than a few tens of kilometers, it is better to rely on two classical authentication processes whenever a connection is established.

4.3 Conclusions

After analyzing all the differents types of QKD protocol, we have come to the same conclusion we had for the BB84 protocol: only in cases where the endpoints of the communication are closer than a few tens of kilometers, using the scheme with just one authentication before the classical information exchange would be more appropiate. Nowadays, the technology available does not allow high enough secure key rates for greater distances, hence relying on a scheme with two PUF-based authentication ensure more speed in the general communication process than having to re-do a process involving quantum information (i.e having to resend the qubits).

Our PUF choices have not changed, as in every proposed protocol, Alice and Bob's devices do not differ in their classical physical abilities, matching the data shown in Table 3.2. Therefore butterfly PUFs would be our choice for ordinary endpoints, while optical PUFs would be more appropiate for more sensitive endpoints.

Chapter 5: Conclusions

Alea iacta est.

– Julio César

QKD is one of the key paths in the evolution of cryptography. But it still has a long way to go before it can be implemented in today's infrastructures. In this work, we have tried to take a small step to make QKD a daily reality, using accessible technologies to add a needed authentication process inside QKD protocols.

Firstly, we analyzed the most relevant QKD protocol, the BB84 protocol, proposing two different authentication schemes depending on the characteristics of the endpoints we are trying to connect. The first scheme, proposed for distances less than a few tens of kilometers, counts with one authentication step before the classical communication within the protocol starts. We proposed a second scheme for distances larger than a few tens of kilometers, and discussed the advantages of authenticating twice inside the BB84 protocol, once before the start of the protocol and once before starting the classical communication, as the authentication processes are much faster than processes that involve sending quantum information between distant points.

Secondly, we discussed the best PUF construction to use as the authentication device at the QKD protocol endpoints. We reduce our options to two final candidates, the optical PUF and the butterfly PUF, arguing that the optical PUF would be more appropriate for endpoints that require special security needs, while the butterfly PUF (easier to install and preserve) would be our final proposal for an authenticator PUF in regular communication exchanges.

After analyzing and giving an answer for the BB84 protocol, we looked at other types of QKD protocols, relying on the secure key rates reported in the literature to argue the convenience of the two possible authentication schemes proposed for the BB84 protocol. As long as technologies such as quantum repeaters are out of hand, we found that secure key rates drop drastically when distances of more than a few tens of kilometers

are involved, leaving us with the same result we had with the BB84 protocol: it is more effective to authenticate twice using our elected PUF than having to repeat a process where quantum information is involved.

Although we have found some articles proposing or theorizing about a PUF-based authentication in QKD [59] [60] [61] [62], we have not found an extensive analysis of the integration of this kind of authentication in QKD protocols as the one we have done in this work. All these recent papers suggest that this is a promising area, where practical experiences must be made to support our proposal.

Glossary

BS Beam-Splitter.

CLB Configurable Logic Block.
CMOS Complementary Metal-Oxide-Semiconductor.
CRP Challenge-Response Pair.
CV Continuous-Variable.

DH Diffie-Hellman.
DLP Discrete Logarithm Problem.
DSA Digital Signature Algorithm.
DWDM Dense Wave Division Multiplexing.

ECC Elliptic Curve Cryptography.
EOM Electro-Optical Modulator.

FPGA Field Programable Gate Array.

IC Integrated Circuit.

nonce Number used Only Once.

PUF Physical Unclonable Function.

QKD Quantum Key Distribution.
qubit Quantum Bit.

RO Ring Oscillator.
RSA Rivest-Shamir-Adleman.

SNSPD Superconducting Nanowire Single-Photon Detector.

Bibliography

[1] 101computing.net. Symmetric vs. asymmetric encryption — 101 computing. URL `https://www.101computing.net/symmetric-vs-asymmetric-encryption/`. Last visited: June 2022.

[2] ID Quantique S.A. Understanding Quantum Cryptography. *IDQ, Quantum-Safe Security Resources*, 2020. URL `https://www.quantumcommshub.net/wp-content/uploads/2020/09/Understanding-Quantum-Cryptography_White-Paper.pdf`. Last visited: June 2022.

[3] PNGAll.com. Encryption PNG Picture — PNG All. URL `https://www.pngall.com/encryption-png/download/95933`. Last visited: June 2022.

[4] P. Kumaraswamy, C. V. Guru Rao, V. Janaki, and B. Bhaskar. Applications of Public Key Cryptography and functioning process. *International Journal of Innovative Technology and Exploring Engineering*, 8, 2019. doi: 10.35940/ijitee.F1100.0486S419.

[5] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th Annual IEEE Symposium on Foundations of Computer Science*, pages 124–134. IEEE Computer Society, 1994. doi: 10.1109/SFCS.1994.365700.

[6] R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 2:120–126, 1978. doi: 10.1145/359340.359342.

[7] N. Torii and K. Yokoyama. Elliptic Curve Cryptosystem. *Fujitsu Scientific and Technical Journal*, 48:203–209, 2000. doi: 10.1090/s0025-5718-1987-0866109-5.

[8] V. Miller. Use of Elliptic Curves in Cryptography. In *Advances in Cryptology - CRYPTO '85 Proceedings*, pages 417–426. Springer Berlin Heidelberg, 1986. doi: 10.1007/3-540-39799-X_31.

[9] W. Diffie and M. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976. doi: 10.1109/TIT.1976.1055638.

[10] National Institute of Standards and Technology. Federal Information Processing Standards Publication: Digital Signature Standard (DSS). 1994. doi: 10.6028/NIST.FIPS.186.

[11] V. Martin, J. P. Brito, C. Escribano, M. Menchetti, C. White, A. Lord, F. Wissel, M. Gunkel, P. Gavignet, N. Genay, O. Le Moult, C. Abellán, A. Manzalini, A. Pastor-Perales, V. López, and D. López. Quantum Technologies in the Telecommunications Industry. *EPJ Quantum Technol.*, 2021. doi: 10.1140/epjqt/s40507-021-00108-9.

[12] A. Singh, K. Dev, H. Siljak, H. D. Joshi, and M. Magarini. Quantum Internet-Applications, Functionalities, Enabling Technologies, Challenges, and Research Directions. *IEEE Communications Surveys and Tutorials*, 23:2218–2247, 2021. doi: 10.1109/comst.2021.3109944.

[13] S. Ehlen, H. Hagemeier, T. Hemmert, S. Kousidis, M. Lochter, S. Reinhardt, and T. Wunderer. Quantum-safe cryptography. Fundamentals, current developments and recommendations. Federal Office for Information Security (BSI), 2021. URL `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html`. Last visited: June 2022.

[14] favpng.com. Quantum Computing Bloch Sphere Qubit. URL `https://urlzs.com/CBq1w`. Last visited: June 2022.

[15] R. Maes. *Physical Unclonable Fuctions. Constructions, Properties and Applications.* Springer Berlin Heidelberg, 1st edition, 2013. doi: 10.1007/978-3-642-41395-7.

[16] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young. A PUF taxonomy. *Applied Physics Reviews*, 6, 2019. doi: 10.1063/1.5079407.

[17] S. Eiroa, I. Baturone, A. J. Acosta, and J. Dávila. Using physical unclonable functions for hardware authentication: A survey. In *Proceedings XXV Conference on Design of Circuits and Integrated Systems*, 2010. URL `https://digital.csic.es/handle/10261/96029?locale=en`. Last visited: June 2022.

[18] P. Tuyls, G. J. Schrijen, B. Škorić, J. van Geloven, N. Verhaegh, and R. Wolters. *Read-Proof Hardware from Protective Coatings.* Springer Berlin Heidelberg, 2006. doi: 10.1007/11894063_29.

[19] K. Kursawe, A. R. Sadeghi, D. Schellekens, B. Skoric, and P. Tuyls. *Reconfigurable Physical Unclonable Functions - Enabling technology for tamper-resistant storage.* IEEE, 2009. doi: 10.1109/HST.2009.5225058.

[20] Y. Alkabani, F. Koushanfar, N. Kiyavash, and M. Potkonjak. *Trusted Integrated Circuits: A Nondestructive Hidden Characteristics Extraction Approach*, volume 5284. Springer Berlin Heidelberg, 2008. doi: 10.1007/978-3-540-88961-8_8.

[21] G. E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. In *DAC '07: Proceedings of the 44th Annual Design Automation Conference*, pages 9–14. Association for Computing Machinery, 2007. doi: 10.1145/1278480.

[22] S. Eiroa and I. Baturone. An analysis of ring oscillator PUF behavior on FPGAs. In *2011 International Conference on Field-Programmable Technology*, pages 1–4. IEEE, 2011. doi: 10.1109/FPT.2011.6132673.

[23] M. C. Martínez-Rodríguez, E. Camacho-Ruiz, P. Brox, and S. Sánchez-Solano. A Configurable RO-PUF for Securing Embedded Systems Implemented on Programmable Devices. *Electronics*, 10(16), 2021. doi: 10.3390/electronics10161957.

[24] A. Maiti and P. Schaumont. Improving the quality of a Physical Unclonable Function using configurable Ring Oscillators. In *2009 International Conference on Field Programmable Logic and Applications*, pages 703–707. IEEE, 2009. doi: 10.1109/FPL.2009.5272361.

[25] S. S Kumar, J. Guajardo, R. Maes, G.-J Schrijen, and P. Tuyls. Extended abstract: The butterfly PUF protecting IP on every FPGA. In *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, pages 67–70. IEEE, 2008. doi: 10.1109/HST.2008.4559053.

[26] Y. Su, J. Holleman, and B. P. Otis. A Digital 1.6 pJ/bit Chip Identification Circuit Using Process Variations. *IEEE Journal of Solid-State Circuits*, 43:69–77, 2008. doi: 10.1109/JSSC.2007.910961.

[27] Y. Gao, S. F. Al-Sarawi, and D. Abbott. Physical Unclonable Functions. *Nature Electronics*, 3:81–91, 2020. doi: 10.1038/s41928-020-0372-5.

[28] B. Cambou, M. Gowanlock, B. Yildiz, D. Ghanaimiandoab, K. Lee, S. Nelson, C. Philabaum, A. Stenberg, and J. Wright. Post Quantum Cryptographic Keys Generated with Physical Unclonable Functions. *Applied Sciences*, 11(6), 2021. doi: 10.3390/app11062801.

[29] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014. doi: 10.1016/j.tcs.2014.05.025. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[30] M. Haitjema. A Survey of the Prominent Quantum Key Distribution Protocols. Washington University in St. Louis, 2007. URL `https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/`. Last visited: June 2022.

[31] E. Knill and R. Laflamme. Theory of quantum error-correcting codes. *Physical Review A - Atomic, Molecular, and Optical Physics*, 55:900–911, 1997. doi: 10.1103/PhysRevA.55.900.

[32] A. M. Abbas, S. El-Kassas, and A. Goneid. Privacy Amplification in Quantum Cryptography BB84 using Combined Univarsal - Truly Random Hashing Implementing security typed applications. *IJINS*, 3:98–115, 2014. URL `http://ijins.iaescore.com/index.php/IJINS/article/view/20288`. Last visited: June 2022.

[33] P. W. Shor and J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.*, 85:441–444, 2000. doi: 10.1103/PhysRevLett.85.441.

[34] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Physical Review Letters*, 95, 2005. doi: 10.1103/PhysRevLett.95.080501.

[35] A. Ruiz-Alba, D. Calvo, V. García-Muñoz, A. Martínez, W. Amaya, J.G. Rozo, J. Mora, and J. Campmany. Practical Quantum Key Distribution based on the BB84 protocol. *Waves Magazine*, 1(3):4–14, 2011. URL `http://hdl.handle.net/10251/53967`. Last visited: June 2022.

[36] J. Vinod and M. Srinivas. 6 - Emerging Trends in Packet Optical Convergence. In *Network Convergence*, pages 525–552. Morgan Kaufmann, 2014. doi: 10.1016/B978-0-12-397877-6.00006-0.

[37] X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, J. Bienfang, D. Su, R. F. Boisvert, C. Clark, and C. Williams. Quantum key distribution system operating at sifted-key rate over 4 Mbit/s. In Eric J. Donkor, Andrew R. Pirich, and Howard E. Brandt, editors, *Quantum Information and Computation IV*, volume 6244, pages 182–189. International Society for Optics and Photonics, SPIE, 2006. doi: 10.1117/12.664455.

[38] Y. Liu, T. Y. Chen, J. Wang, W. Q. Cai, X. Wan, L. K. Chen, J. H. Wang, S. B. Liu, H. Liang, L. Yang, C. Z. Peng, K. Chen, Z. B. Chen, and J. W. Pan. Decoy-state quantum key distribution with polarized photons over 200 km. *Optics Express*, 18: 8587–8594, 2010. doi: 10.1364/OE.18.008587.

[39] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields. Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate. *Optics Express*, 16: 18790–18797, 2008. doi: 10.1364/OE.16.018790.

[40] J. Cussey, F. Patois, N. Pelloquin, and J. M. Merolla. High Frequency Spectral Domain QKD Architecture with Dispersion Management for WDM Network. In *OFC/NFOEC 2008 - 2008 Conference on Optical Fiber Communication/National Fiber Optic Engineers Conference*, pages 1–3. IEEE, 2008. doi: 10.1109/OFC.2008.4528717.

[41] J. Guajardo, S. S Kumar, G. J. Schrijen, and P. Tuyls. Physical Unclonable Functions and Public-Key Crypto for FPGA IP protection. In *2007 International Conference on Field Programmable Logic and Applications*. IEEE, 2007. doi: 10.1109/FPL.2007.4380646.

[42] U. Rührmair, C. Hilgers, S. Urban, A. Weiershäuser, E. Dinter, B. Forster, and C. Jirauschek. Optical PUFs Reloaded. Cryptology ePrint Archive, paper 2013/215. URL `https://eprint.iacr.org/2013/215.pdf`. Last visited: June 2022.

[43] V. Betz and J. Rose. VPR: A new packing, placement and routing tool for FPGA research. In W. Luk, P. Y. K. Cheung, and M. Glesner, editors, *Field-Programmable Logic and Applications*, pages 213–222. Springer Berlin Heidelberg, 1997. doi: 10.1007/3-540-63465-7_226.

[44] M. F Ali. *Manufacturing and Modeling of an Organic Thin Film Transistor*. PhD thesis, Military Technical College (Egypt), 2016.

[45] A. I. Nurhadi and N. R. Syambas. Quantum Key Distribution (QKD) Protocols: A Survey. In *Proceeding of 2018 4th International Conference on Wireless and Telematics, ICWT 2018*, pages 1–5. Institute of Electrical and Electronics Engineers Inc., 2018. doi: 10.1109/ICWT.2018.8527822.

[46] C. H Bennett. Quantum Cryptography Using Any Two Nonorthogonal States. *Physical Review Letters*, 68:3121–3124, 1992. doi: 10.1103/PhysRevLett.68.3121.

[47] H. Bechmann-Pasquinucci and N. Gisin. Incoherent and Coherent Eavesdropping in the 6-state Protocol of Quantum Cryptography. *Physical Review Letters*, 59:4238–4248, 199. doi: 10.1103/PhysRevA.59.4238.

[48] V. Scarani, A. Acín, G. Ribordy, and N. Gisin. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Physical Review Letters*, 92, 2004. doi: 10.1103/PhysRevLett.92.057901.

[49] E. H. Serna. Quantum Key Distribution From A Random Seed. arXiv, 2013. doi: 10.48550/arXiv.1311.1582.

[50] O. Thearle. *Protocols and Resources for New Generation Continuous Variable Quantum Key Distribution*. PhD thesis, Australian National University (Australia), 2017. URL `https://anuquantumoptics.org/pdf/theses/2017thearle.pdf`. Last visited: June 2022.

[51] X. Tang, R. Kumar, S. Ren, A. Wonfor, R. V. Penty, and I. H. White. Performance of continuous variable quantum key distribution system at different detector bandwidth. *Optics Communications*, 471, 2020. doi: 10.1016/j.optcom.2020.126034.

[52] A. Whitaker. *The new quantum age: from Bell's theorem to quantum computation and teleportation*. Oxford University Press, reprint edition, 2016. ISBN 9780198754763.

[53] A. K Ekert. Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*, 67:661–663, 1991. doi: 10.1103/physrevlett.67.661.

[54] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theorem. *Physical Review Letters*, 68:557–559, 1992. doi: 10.1103/PhysRevLett.68.557.

[55] K. Inoue, E. Waks, and Y. Yamamoto. Differential-phase-shift Quantum Key Distribution using coherent light. *Physical Review A - Atomic, Molecular, and Optical Physics*, 68, 2003. doi: 10.1103/PhysRevA.68.022317.

[56] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani. Towards practical and fast Quantum Cryptography. arXiv, 2004. doi: 10.48550/arXiv.quant-ph/0411022.

[57] S. P. Neumann, M. Selimovic, M. Bohmann, and R. Ursin. Experimental entanglement generation for Quantum Key Distribution beyond 1 Gbit/s. arXiv, 2021. doi: 10.48550/arXiv.2107.07756.

[58] S. Ecker, B. Liu, J. Handsteiner, M. Fink, D. Rauch, F. Steinlechner, T. Scheidl, A. Zeilinger, and R. Ursin. Strategies for achieving high key rates in satellite-based QKD. *npj Quantum Information*, 7, 2021. doi: 10.1038/s41534-020-00335-5.

[59] R. Uppu, T. A. W. Wolterink, S. A. Goorden, B. Skoric, A. P. Mosk, and P. W. H. Pinkse. Secure communication with coded wavefronts. In *2017 Conference on Lasers and Electro-Optics Europe and European Quantum Electronics Conference (CLEO/Europe-EQEC)*. OSA - The Optical Society, 2017. doi: 10.1109/cleoe-eqec.2017.8087422.

[60] G. Gianfelici, H. Kampermann, and D. Bruß. Theoretical framework for Physical Unclonable Functions, including quantum readout. *Physical Review A*, 101:042337, 2020. doi: 10.1103/PhysRevA.101.042337.

[61] A. Lord. Where Does QKD Fit in a Post-quantum Secure World? In *Quantum West*, volume 11714. SPIE, 2021. doi: 10.1117/12.2593555.

[62] G. M. Nikolopoulos. Remote quantum-safe authentication of entities with Physical Unclonable Functions. *Photonics*, 8(7), 2021. doi: 10.3390/photonics8070289.