University of Padova

Department of Mathematics "Tullio Levi-Civita"

Master Thesis in Cybersecurity

Development of high-performance encoder for Asynchronous-Pairing QKD

Supervisor
Dr. Marco Avesani
University of Padova

Co-supervisor
Dr. Yoann Piétri
University of Padova

Master Candidate
Simone Conton

Student ID
2125863

Academic Year
2024-2025

"Quantum phenomena do not occur in a Hilbert space, they occur in a laboratory."
— A. PERES

Abstract

Quantum Key Distribution (QKD) is one of the most advanced quantum technologies, aiming to enable unconditionally secure key exchange by exploiting the physical properties of quantum states. Since the introduction of the first QKD protocol, BB84, over forty years ago, numerous schemes have been proposed. One of the most promising recent approaches is Asynchronous-Pairing QKD (AP-QKD), which combines the strong security guarantees of Measurement-Device independent (MDI) protocols with enhanced robustness to losses, all while remaining compatible with low-complexity hardware implementations. This thesis presents the experimental realization of a high-performance encoder for AP-QKD, describing its design, performance, and potential for integration in practical quantum communication systems.

Contents

Listing of figures

Listing of tables

Listing of acronyms

AP ..... Asynchronous-Pairing

BB84 ..... Bennett-Brassard 84

BS ..... Beam-Splitter

DI ..... Device-Independent

DOS ..... Denial-of-Service

EB ..... Entanglement-Based

EPR ..... Einstein-Podolsky-Rosen

ER ..... Extinction Ratio

FPGA ..... Field Programmable Gate Array

GUI ..... Graphical User Interface

HWP ..... Half Wave-Plate

MDI ..... Measurement-Device Independent

MP ..... Mode-Pairing

OTP ..... One-Time Pad

P&M ..... Prepare and Measure

PBS ..... Polarizing Beam Splitter

PDH ..... Pound-Drever-Hall

PLOB ..... Pirandola-Laurenza-Ottaviani-Banchi

PMP ..... Post-Measurement Pairing

QBER ..... Quantum Bit Error Rate

QKD ..... Quantum Key Distribution

QWP ..... Quarter Wave-Plate

RF ..... Radio Frequency

SKR ..... Secret Key Rate

SM ..... Single-Mode

SNSPD ..... Superconducting Nanowire Single Photon Detector

SPAD ..... Single Photon Avalanche Detector

SPDC ..... Spontaneous Parametric Down Conversion

TDC ..... Time-to-Digital

TF ..... Twin-Field

1

Introduction

Between seventy and eighty years ago, the world entered the Information Age. Among the events that led to such a relevant evolutionary step, many identify the invention of the transistor as the main contributor to this epochal change in the history of humankind, as it paved the way for the development of computers and all the modern technology to which we are now accustomed.
A key role was also played by the seminal idea of what is known nowadays as *the Internet*: its roots date back to 1962, when researchers first hypothesised a publicly accessible global net for communication [1].
In addition, it is impossible not to mention the groundbreaking article ''A mathematical theory of Communication'' [2], in which Claude Shannon introduced an elegant mathematical framework to describe what is known today as telecommunications. Despite having had, and still having, an enormous impact on our lives, it has often been underestimated or remained unknown to many [3].

The building blocks were set: it was just a matter of time before all the developments in different areas were merged together. In 1971, the first microprocessor was invented, and the first e-mail was sent. Since then, our society has witnessed impressive developments in communication technologies. In parallel, the need to ensure that such communications were *secure* arose. Historically speaking, there are several examples of techniques used to make communication unintelligible to anyone but the intended receiver [4]. With the evolution of communication systems, the need to maintain them secure has become a crucial concern. The methods and implementations that achieve this goal are part of what is commonly known nowadays as ''Cybersecurity''.

Going back in time to the beginning of 20^{th} century, the physical models developed up to that time could not explain phenomena such as the photoelectric effect [5] and the black-body radiation [6]. The solutions that were eventually found gave birth to the *quantum physics*. Beyond the theoretical development, which gave rise to extremely counter-intuitive implications (we will present some of them in this thesis), the principles of quantum physics form the foundation of several widely used technologies, including the already mentioned transistors and lasers, and even the Global Positioning System (GPS).

In this context, an exciting and novel field concerns quantum secure communications, which lies in the intersection of security, quantum physics, and information engineering fields.

2

Introductory material

In this chapter, we will introduce all the necessary material needed to understand the reasons why QKD systems are implemented, the underlying quantum mechanics properties on which they rely, and the goals they aim to achieve. In particular, in the first section, we will start by presenting the formal framework of secure communications, while in the second section we will provide an overview of quantum mechanics and quantum information theory. Finally, we will give an introduction to Quantum Optics and to useful tools to understand the implementation of advanced QKD protocols.

2.1 Elements of Security

Before entering into the details, let's provide a general overview of what we mean by "secure communications". In this context, the goal to be achieved is the *confidentiality*, which corresponds to the event in which the information that is being transmitted is available only to the intended receiver. The aim of a potential adversary, known as *eavesdropper*, is to learn the information that two or more legitimate users are sharing.

We can introduce two security *services*: secrecy, that intuitively regards making the communication unintelligible for the eavesdropper, and key management, which is needed to implement secrecy. In fact, secrecy can be realized by an encryption mechanism which needs to rely upon a cryptographic key to work. The QKD is a security mechanism that implements key management services and provides security by relying upon the laws of quantum mechanics.

In this section we will start by enunciating quantitative definitions of security, fol-

lowed by the introduction of key management and encryption mechanisms, finally presenting Shor's algorithm, and highlighting why it represents a severe threat in the security domain.

2.1.1 Computational and Unconditional security

In the security domain, qualitative descriptions are not sufficient: there is the need to provide quantitative evaluations. Instead of ''Is this system secure?'', the questions that need to be answered are, for example, ''*How much* secure is this system?'' or ''*Under which conditions* is this system secure?''. For this reason, we will introduce a formal framework.
Moreover, according to intuition, randomization is crucial in security. In fact, if an attacker keeps using the same strategy over and over again without succeeding, the defender will not change its behavior, as it does not need to. The converse is valid as well. It follows that, in security, determinism is not an option: probability must be considered.

Let's start by presenting the two fundamental building blocks:

Definition 2.1 (Attack)**.** *An attack is a randomized algorithm A characterized by a success event S_A and an execution time T_A (which is, in general, a random variable).*

Definition 2.2 (Security Mechanism)**.** *A security mechanism (or system, we will use both these denominations with the same meaning) is a randomized algorithm M characterized by its execution time T_M.*

From these definitions, an intuitive choice would be to define the security of a mechanism in terms of the success probability of an attack. However, this approach fails when considering the *composability*, a crucial aspect that we will explain in detail later.

We will proceed with the description of a formal structure that follows the ideas of the *Abstract Cryptography* framework introduced by Maurer and Renner [7].

Let us introduce the idea of *indistinguishability*, which is related to the capacity of distinguishing between two different systems. By considering then the ideal version of security mechanisms, we can evaluate the performances of the real mechanisms by estimating their differences with respect to their ideal counterparts (see [8] and [9]).

A distinguisher D is a system that provides an input X (modeled as a random variable) to a black box that contains two systems, S_0 and S_1 (characterized by

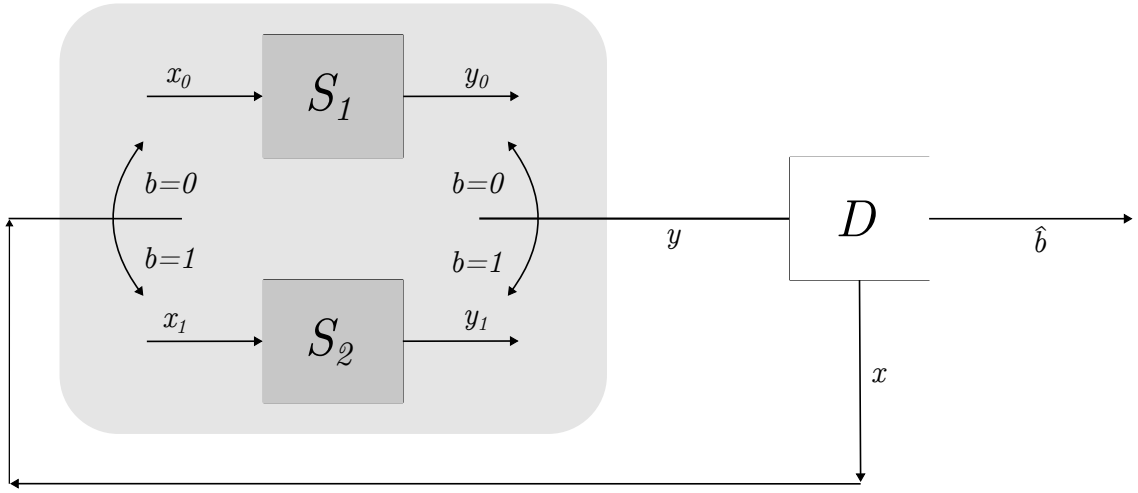

Figure 2.1: The block diagram of a system distinguisher. The grey box containing the two systems has to be considered as a black box, to which the distinguisher feeds an input and receives an output, not knowing which system has produced it.

their conditional probability mass distributions $p_{y_0|x}$ and $p_{y_1|x}$, respectively), without knowing in advance to which of the two it will be fed by the input X. Then, D observes the output Y of the black box and has to guess whether it was produced by S_0 or S_1. We can indicate with $b = 1, 2$ the decision between S_0 and S_1 at the input and $\hat{b} = 0, 1$ the guess made by D. If $b = \hat{b}$, D distinguished correctly between S_0 and S_1, *i.e.* D was able to correctly identify which of the two systems produced the output Y given the input X. We report a block diagram in figure 2.1.

We can evaluate a distinguisher using the distinguishing advantage:

Definition 2.3 (Distinguishing Advantage)**.** *The distinguishing advantage of D between the two systems S_1 and S_0 is:*

$$dist_D(S_0, S_1) = |p_{\hat{b}|b}(0|0) + p_{\hat{b}|b}(1|1) - 1| = |p_{\hat{b}|b}(0|1) + p_{\hat{b}|b}(1|0)| \tag{2.1}$$

We can notice that the distinguishing advantage can be calculated by starting either from the correct decision probability or from the error probability. Moreover, from the definition, it follows that a $\text{dist}_D(S_0, S_1) = 1$ for a perfect distinguisher, while $\text{dist}_D(S_0, S_1) = 0$ for a useless distinguisher. A distinguisher whose action corresponds to tossing a coin (*i.e.* $p_{\hat{b}|b}(0|0) = p_{\hat{b}|b}(0|1) = \frac{1}{2}$ and $p_{\hat{b}|b}(1|0) = p_{\hat{b}|b}(1|1) = \frac{1}{2}$) is useless, as well as a deterministic distinguisher (*i.e.* $p_{\hat{b}|b}(0|0) = 1$ or $p_{\hat{b}|b}(0|1) = 1$ and $p_{\hat{b}|b}(1|0) = 1$ or $p_{\hat{b}|b}(1|1) = 1$).

Starting from the distinguishing advantage, we can provide the following definition:

Definition 2.4 (ε-unconditional indistinguishability)**.** *Two systems S_0 and S_1 are ε-unconditional indistinguishable if, for any distinguisher D,*

$$dist_D(S_0, S_1) \leq \varepsilon \tag{2.2}$$

If we suppose that we need to evaluate a security mechanism in terms of distinguishing advantage, we need to find a term of comparison. For this reason we introduce the concept of *ideal mechanisms*, which are mechanisms that provide the same security services and have the same interfaces as their real counterparts. While the first condition might seem trivial, the second one has to be carefully considered when dealing with ideal counterparts of security mechanisms. Let's provide some examples: the ideal counterpart of a random number generator is a source of uniform and independent symbols, while the ideal counterpart of a cryptographic key agreement scheme is a mechanism that provides two identical copies of a random uniform string to the two legitimate users and useless information to a possible eavesdropper. The key agreement will be described and analyzed thoroughly in this thesis (the QKD is a key agreement scheme), but we want to stress the need to provide an output also for the eavesdropper: this is due to the fact that, as mentioned in the second condition, the ideal mechanism needs to take into account all the interfaces of its real counterpart and, therefore, the eavesdropper in a key agreement scheme.

We need the last step to arrive at the security definitions based on indistinguishability: intuitively, the closer a mechanism is to its ideal counterpart, the more secure it is. In fact:

Definition 2.5 (ε-unconditional security based on indistinguishability)**.** *A mechanism M is ε-unconditional secure if it is ε-unconditional indistinguishable from its ideal counterpart M^*.*

Let's now introduce one of the most crucial concepts upon which, nowadays, security relies: the computational security. From an intuitive point of view, we can think of several tasks for which security is not needed *ad infinitum*. Let us take as an example a computer that contains classified information which will be revealed in fifty years, protected by a password: if an attacker manages to find a way to derive the password, but such operation takes thousands of years, it is straightforward that this menace can be neglected. In other words, we can say that computational security guarantees unconditional security for a limited amount of time. For this reason, we provide the following definitions:

Definition 2.6 ((ε, T_0)-computational indistinguishability)**.** *Two systems S_1 and*

S_2 are (ε, T_0)-computational indistinguishable if, for any distinguisher D with complexity $T_D \leq T_0$,

$$dist_D(S_1, S_2) \leq \varepsilon \tag{2.3}$$

Definition 2.7 ((ε, T_0)-computational security)**.** *A security mechanism M is said to offer (ε, T_0)-computational security if it is (ε, T_0)-indistinguishable from its ideal counterpart M*.*

However, this formulation carries a major drawback: it does not take into account the possible evolution and improvements that the attacks might have over time. Coming back to the example we made before about the classified information stored in the computer, we must notice that the amount of operation that a computer was able to perform in a day forty years ago, now can be carried out in much less time. In other words, using this security definition might not be exhaustive, as it guarantees security just for the state-of-the-art attacks, not considering future evolutions or improvements from the adversaries.

Therefore, we allow the mechanism to depend on a security parameter $n \in \mathbb{N}$ (in our example, the length of the password). The aim is that, by increasing n, the legitimate operation remains feasible, while the adversary's operation becomes infeasible, computationally speaking. This leads to:

Definition 2.8 (Asymptotic (ε, T_0)-computational indistinguishability)**.** *Two sequences of mechanisms $S_{1,n}$ and $S_{2,n}$ are (ε, T_0)-computational indistinguishable in the asymptotic formulation if, for any polynomials $p(\cdot), q(\cdot)$ and for any sequence of distinguishers D_n with complexity $T_{D_n} \leq p(n)$, there exist n_0 such that*

$$dist_{D_n}(S_{1,n}, S_{2,n}) \leq \frac{1}{q(\cdot)} \tag{2.4}$$

for all $n > n_0$.

Definition 2.9 (Asymptotic (ε, T_0)-computational security based on indistinguishability)**.** *A sequence of mechanisms $\{M_n\}$ is (ε, T_0)-computational secure in the asymptotic formulation if it is (ε, T_0)-computationally indistinguishable in the asymptotic formulation from its ideal counterpart $\{M_n^*\}$.*

We will recall these definitions in section 2.1.3, as the vast majority of security systems nowadays rely on them.

Finally, we reach the core point: it is customary for complex security systems to be the result of the composition of simpler security systems. As an example, we

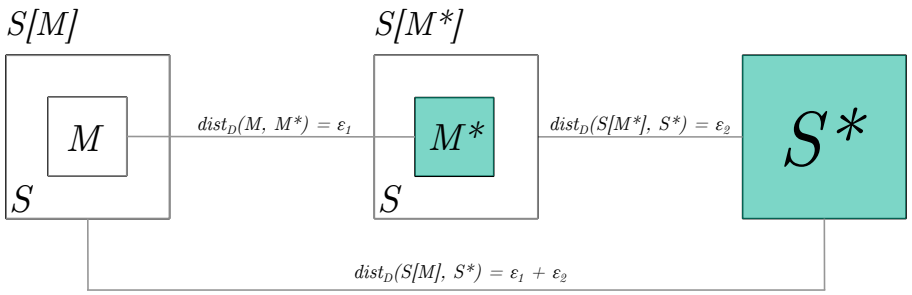

Figure 2.2: The block diagram of the composability theorem.

can take a private-key encryption mechanism, which will be formally described in section 2.1.2: it makes use of a key management mechanism that generates and distributes a cryptographic key that must remain unknown to the eavesdropper. Of course, the key management mechanism may also be decomposed into different and simpler subsystems. How can the security of the composed systems be evaluated?

Let's consider the mechanism S that makes use of the mechanism M, let's suppose that $S[M^*]$ indicates S when it makes use of M^* (the ideal version of M) and S^* indicates the ideal version of S itself. Supposing we know the security level of $S[M^*]$ and M, we want to derive the security level of $S[M]$.

We provide (without proof) the following theorem (the relative block diagram is represented in figure 2.2):

Theorem 2.1 (Composition theorem)**.** *If M is ε_1-unconditionally secure and $S[M^*]$ is ε_2-unconditionally secure, then $S[M]$ is $(\varepsilon_1 + \varepsilon_2)$-unconditionally secure.*

This theorem might seem simple and trivial at the same time, yet it is fundamental for QKD - and security in general. Its importance lies in the fact that it guarantees assessing the security of complex security mechanisms by decomposing them into simpler ones. In particular, we want to stress that this is the direct consequence of using the security definitions based on the indistinguishability from the ideal counterparts of security mechanisms.
Finally, the result of the theorem confirms an intuitive fact: if we consider a complex security mechanism, composed of simpler security mechanisms, its security level will be proportional to the security level of the worst among the subsystems. In other words, if our aim is to design a security system, we cannot afford to relax the constraint on the security performances of one of the components, as it will be the bottleneck for the security of the entire system.

2.1.2 Encryption and Key Management Mechanisms

In this section we will present the encryption systems in a formal way, defining what *perfect secrecy* means in this domain and the necessary condition to achieve it. We will highlight the necessity of cryptographic keys in an encryption mechanism, that will lead us to the introduction of (cryptographic) key management mechanisms.

Encryption systems

As outlined at the beginning, our final goal is to obtain a secure communication between two users, Alice and Bob, by ensuring that no eavesdropper, Eve, is able to learn it.
In the model sketched in figure 2.3, we are assuming that Alice wants to share some information with Bob: this communication is threatened by the presence of Eve. In a private key encryption system, Alice composes her secret message, known as *plaintext* ($u \in \mathcal{M}$, the message space) and performs an encryption operation with a *key* ($E(u,k)$, with $k \in \mathcal{K}$, the key space). The encrypted message is called *ciphertext* ($x \in \mathcal{X}$, the cipher space) and it is transmitted over a channel. When it reaches Bob, it undergoes a *decryption* operation, $D(x,k)$, from which Bob is able to retrieve the plaintext.
It is important to notice that the information is available to Eve only during the transmission part, that is, only when the message is encrypted. Intuitively, the transformation operated by the encryption should make it impossible for Eve to derive the plaintext from the ciphertext.

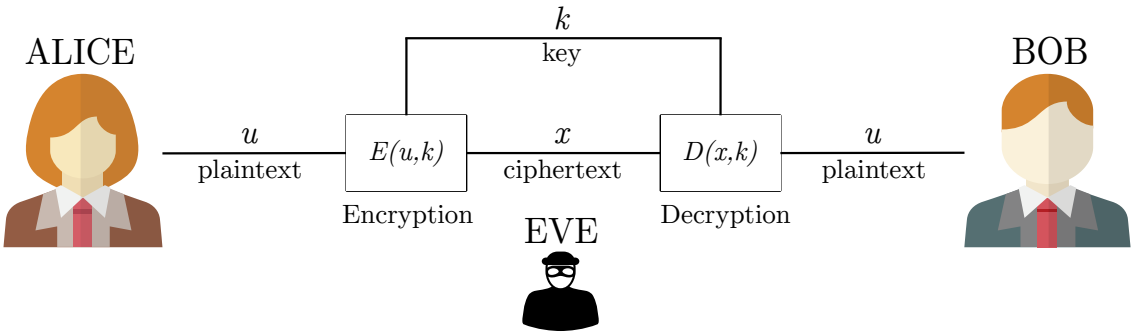

Figure 2.3: The diagram block of a general encryption scheme.

We can introduce two assumptions:

1. **Perfect reliability:** The receiver must be able to recover the secret message perfectly, therefore the decryption function must be the inverse of the encryption function, for all $k \in \mathcal{K}$:

$$D_k = E_k^{-1} \tag{2.5}$$

2. **Kerchoff's assumption:** The eavesdropper knows the system S and both the encryption and the decryption function $E(\cdot,\cdot), D(\cdot,\cdot)$.

The consequence of Kerchoff's assumption is that secrecy is based on the fact that the eavesdropper does not know the key.

What are the techniques that Eve can use to learn the plaintext that Alice is sending? The Kerchoff's assumption ensures that Eve knows the system: in particular, she might know the probability mass distribution (PMD) p_u of the plaintext. This means that she knows the probability that a specific message $u_i \in \mathcal{M}$ will be chosen by Alice and sent over the channel. Note that we are not even considering the encryption phase, but only the choice made by Alice.

Definition 2.10 (Guessing probability)**.** *The guessing probability $P_g(u)$ of Eve is defined as:*

$$P_g(u) = \max_{a \in \mathcal{M}} p_u(a) \tag{2.6}$$

Without any other information, the guessing probability represents the best strategy for Eve, since she is choosing the plaintext u with the highest probability, among all the possible messages, of being chosen by Alice.

By considering the eventuality that Eve has access to the ciphertext (it is reasonable, as she could retrieve it from the channel), we can define:

Definition 2.11 (Conditional guessing probability)**.** *The conditional guessing probability $P_g(u|x)$ of Eve is defined as:*

$$P_g(u|x) = \max_{a \in \mathcal{M}} p_{u|x}(a|b) \tag{2.7}$$

Intuitively, the conditional guessing probability cannot be lower than the guessing probability, as Eve is adding to her knowledge the information about the ciphertext, which, in the worst-case scenario for her, is meaningless. In fact:

$$P_g(u|x) = \sum_{b \in \mathcal{X}} p_x(b) \max_{a \in \mathcal{M}} p_{u|x}(a|b) \geq \max_{a \in \mathcal{M}} \sum_{b \in \mathcal{X}} p_x(b) p_{u|x}(a|b) = P_g(u) \tag{2.8}$$

Now, following the security definitions we provided, and in particular those based on the indistinguishability, we have to define the ideal world counterpart of an encryption mechanism: it is a system that takes the plaintext from Alice and delivers it to Bob, and it delivers to the eavesdropper *useless* information (*i.e.* the ciphertext that the eavesdropper gets does not bear any meaningful information about the key or the plaintext). This condition can be formally translated into:

Definition 2.12 (Perfect secrecy, Shannon [10])**.** *An encryption system is perfect if it provides* 0*-unconditional security based on the indistinguishability, i.e. the plaintext is statistically independent of the ciphertext:*

$$p_{x|u}(b|a) = p_x(b) \quad \forall a \in \mathcal{M}, b \in \mathcal{X} \tag{2.9}$$

As a consequence, perfect secrecy ensures that the conditional guessing probability is equal to the guessing probability. This means that, even in the case Eve is able to intercept the ciphertext, she will not gain any additional information from it and her best strategy will also be the weakest she can choose: a random guess.

One-Time Pad

We will now present an encryption scheme called One-Time Pad (OTP). Let us consider a finite group $(\mathbb{G}, \circ)$ and an encryption system with equal spaces $\mathcal{M} = \mathcal{X} = \mathcal{K} = \mathbb{G}$, where the key k is chosen uniformly from $\mathcal{K}$ ($k \sim \mathcal{U}(\mathbb{G})$). The encryption and decryption operations are defined as:

$$E(u, k) = u \circ k \tag{2.10}$$

$$D(x, k) = x \circ k^{-1} \tag{2.11}$$

We present the following theorem (without proof):

Theorem 2.2 (Perfect secrecy of One-Time Pad, Shannon [10])**.** *The One-Time Pad offers perfect reliability and perfect secrecy for any message distribution.*

Now different questions may arise: can this result be generalized? At which conditions? And foremost: why don't we use the One-Time Pad instead of other encryption schemes?

The answers lie in the following theorem:

Theorem 2.3 (Necessary condition for perfect secrecy, Shannon [10])**.** *The necessary condition for perfect secrecy and perfect reliability is:*

$$H(k) \geq H(u) \tag{2.12}$$

where with $H(a)$ we indicate the entropy of the random variable a.

The importance of this negative result is capital. It highlights that we cannot achieve perfect secrecy unless the key has at least the same entropy as the plaintext. As a consequence[1], in a system with $\mathcal{M} = \mathcal{A}^{l_u}$ and $\mathcal{K} = \mathcal{A}^{l_k}$, perfect secrecy

[1] In particular, if $x \sim \mathcal{U}(\mathcal{N})$, then $H(x) = \log_2 |\mathcal{N}|$.

is achieved only if $l_k \geq l_u$: the key must be ''at least as long'' as the message. This limitation may be crucial in cases in which the size of information message to be encrypted is massive, resulting in the need for a key of at least the same size. Moreover, this theorem shows also the motivation for which this encryption mechanism is called ''One-Time Pad'': if we use more than once the same key to encrypt different messages, there is an increase in the entropy of the plaintext (we can think of a longer plaintext) but the entropy of the key remains the same, violating the necessary condition for perfect secrecy.

Nonetheless, the fact that the One-Time Pad ensures perfect secrecy is still a valid motivation to use it for extremely confidential message transmissions. Still, it carries a drawback: Alice and Bob need to share the same cryptographic key. This is the reason why the schemes that meet this requirement fall under the name of ''Private key'' encryption schemes.
There are private key systems that relax the constraint on the entropy of the key, but they achieve only computational security: among them, the most widely used is the AES [11]. In any case, this is the confirmation that key management mechanisms, and QKD among them, are needed.
There are other protocols, called ''Public key'' encryption schemes that achieve confidentiality without sharing a private key between the two users, but relying on a system of public and private keys: among the most famous, we mention RSA [12] and ElGamal [13] cryptosystems. These schemes are the building blocks of a large share of any encrypted communication, nowadays.

Key Management mechanisms

Following the intuition, a key exchange mechanism allows two parties, that we can call Alice and Bob, to share a cryptographic key and to avoid any possibility for an attacker to discover it. It is simple to imagine that, whenever Alice and Bob are separated by long distances, the key exchange between them is a concerning task. In fact, at first impact, one may think that the only way to securely deliver cryptographic keys between them is to rely upon a secure channel, but a channel is made secure typically by using cryptographic keys! Is this a chicken and egg problem? Actually, it is not.

Diffie-Hellman protocol

One of the most famous, elegant, and widely used solutions for this problem is known as Diffie-Hellman protocol [14]. It relies upon the discrete logarithm problem: this means that, if an adversary is capable of solving the discrete logarithm

problem, then the final key exchanged between the two legitimate users is no longer secure. From this, it follows that the Diffie-Hellman protocol can offer only computational security.

Diffie-Hellman Key Exchange
Alice and Bob agree on a group in which the logarithm problem is hard (typically, elliptic curve $(\mathcal{E}, \circ)$ or multiplicative integers mod a prime n $(\mathbb{Z}_n, \times)$ groups). If we denote the group chosen as $(\mathbb{G}, \circ)$, let $n = |\mathbb{G}|$ and $g \in \mathbb{G}$ a primitive.

Alice and Bob then sample respectively x and y such that x, y i.i.d. $\sim \mathcal{U}(\mathbb{Z}_n \backslash \{0\})$.

Subsequently, Alice computes $g^{\overset{x}{\circ}}$ and sends it to Bob, which in the meantime computed $g^{\overset{y}{\circ}}$ and sent it to Alice.

Alice receives $g^{\overset{y}{\circ}}$ and computes $k_{\mathrm{A}} = \left(g^{\overset{y}{\circ}}\right)^{x}$, while Bob computes $k_{\mathrm{B}} = \left(g^{\overset{x}{\circ}}\right)^{y}$.

It is straightforward to see that $k_{\mathrm{A}} = k_{\mathrm{B}}$, since:

$$\left(g^{\overset{y}{\circ}}\right)^{x} = g^{\overset{xy \bmod n}{\circ}} = \left(g^{\overset{x}{\circ}}\right)^{y} \tag{2.13}$$

as well as it is needed to solve the discrete logarithm problem to retrieve x, y or k from the information exchanged. Finally, the key exchanged between Alice and Bob is completely random due to the choice of x and y.

2.1.3 Security nowadays

With the introduction of the computational security definitions, we have highlighted the possibility of guaranteeing the security for a limited amount of time, that might be enough for our purposes. A trivial question might be: how can we be sure that the attacker won't be able to break our security system before?

Complexity Classes

In theoretical computer science, one of the most active research fields regards the computational complexity problems. The depth and the vastness of the research advancements in this area are considerable: for this reason, we will limit our discussion to an informal and introductory level.
The goal of this discipline is to relate the decision problems (i.e. problems which ad-

mit as a solution a binary answer) to the amount of resources needed to solve them (in particular, *time* and *memory*). A simple example of a computational problem is to indicate whether a number is prime.
It is possible to introduce the following classification for computational problems based on the amount of resources needed to find a solution (and verify whether a proposed solution is actually correct).

Definition 2.13 (P-hard problems, informal)**.** *A P-hard problem is a decision problem that can be exactly solved by an algorithm in polynomial time.*

Definition 2.14 (NP-hard problems, informal)**.** *An NP-hard problem is a decision problem for which the candidate solution can be verified by a deterministic algorithm in polynomial time.*

A remarkable example is the factorization problem, which was thought to be an NP-hard problem for a long time and will be mentioned again in this thesis. If a number is not prime, then it is possible to find at least two numbers that factorise it. While it is straightforward to verify whether the product of the factors gives the number, it is much harder to do the reverse: this is exactly the idea behind NP-hard problems. It is possible to consider also probabilistic algorithms:

Definition 2.15 (BPP-hard problems, informal)**.** *A BPP-hard problem is a decision problem that can be solved with a ''good'' success probability by a probabilistic algorithm in polynomial time.*

Definition 2.16 (BQP-hard problems, informal)**.** *A BQP-hard problem is a decision problem that can be solved with a ''good'' success probability by a quantum algorithm in polynomial time.*

We can relate the asymptotic computational security provided by a mechanism with the fact that a possible adversary, to attack it, has to solve a computational. There are several famous examples of security mechanisms that have been developed starting from a computationally difficult problem, with the precise aim of guaranteeing asymptotic computational security. Among them, RSA [12] and ElGamal [13] algorithms are used for encryption and digital signature mechanisms, and Diffie-Hellman [14] mechanism for the key-exchange.

Shor's Algorithm

In 1994, a groundbreaking article by Peter Shor [15] formalized a critical threat against several security mechanisms that relied on computational security. For example, the RSA algorithm bases its security on the problem of factorizing integers, while ElGamal and Diffie-Hellman are constructed upon the discrete logarithm

problem: both these problems were considered to be NP-hard. However, the integer factorization and the discrete logarithm problem can be reduced to a common problem: informally, we can say that the computational bottleneck is, in both cases, represented by finding the order of a number, *i.e.*, solving for r (called the *multiplicative order of a in N*) the following equation:

$$a^r \equiv 1 \bmod N \tag{2.14}$$

Shor proposed an algorithm that makes use of quantum computing tools to find the order efficiently. In other words, the problem of finding the multiplicative order of a number in a field is BQP.

The consequences of such innovation, in the world of security, are inestimable: the security mechanisms mentioned before are still used today in crucial protocols like TLS or SSH. The technological maturity in quantum computing nowadays is not enough to break the current version of such mechanisms; however, it is clear that it is no longer *if*, but rather *when* a cryptographic mechanism will be violated by Shor's algorithm. The impact of Shor's algorithm has been so crucial that in the literature it is common to differentiate between *classical cryptography*, which is vulnerable to attacks by quantum adversaries, and *post-quantum cryptography*, which exploits classical schemes that are known to be invulnerable to quantum attacks, for example the McEliece cryptosystem [16], based on the hardness of decoding linear codes.
In this framework, quantum cryptography represents an alternative that guarantees security against quantum attackers by relying on the properties of quantum mechanics.

2.2 Quantum Mechanics & Quantum Information

To understand the principles upon which Quantum Key Distribution protocols are designed, it is necessary to have a basic knowledge of some elements of quantum mechanics and quantum information theory. In the following, we will provide an introduction to the general framework of quantum mechanics, we will enunciate three properties that are crucial for QKD, and finally we will highlight how it is possible to use light to encode quantum, presenting some elements of quantum optics..

2.2.1 State, Measurement, Collapse

Quantum states

A quantum state can be described by a complex vector in a Hilbert space[2]. We will adopt the *Dirac notation*, according to which we call the vector $|\psi\rangle \in \mathcal{H}$ a *ket*. Its Hermitian conjugate $\langle\psi| = (|\psi\rangle)^\dagger$ is called *bra*.

The use of a Hilbert space guarantees the existence of a *scalar product* $\langle\phi|\psi\rangle \in \mathbb{C}$ that satisfies the following properties:

- **Non-commutativity**: $\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^*$, where we indicate the complex conjugate of $a \in \mathbb{C}$ as a^*.
- **Linearity:** $\langle\phi| (\alpha |\psi_1\rangle + \beta |\psi_2\rangle) = \alpha\langle\phi|\psi_1\rangle + \beta\langle\phi|\psi_2\rangle$.

Since $\langle\psi|\psi\rangle = 0$ if and only if $|\psi\rangle$ is the null vector, the norm satisfies $\|\psi\|^2 = \langle\psi|\psi\rangle \geq 0$. A quantum state can be represented only by a normalized vector, *i.e.* $\langle\psi|\psi\rangle = 1$.

The fact that a quantum state $|\psi\rangle$ is defined within a Hilbert space $\mathcal{H}_d$ of dimension d ensures that, given an orthonormal basis $\{e_i\}_{0\leq i\leq d-1}$, it is possible to express $|\psi\rangle$ as a linear combination of the basis elements:

$$|\psi\rangle = \sum_{i=0}^{d-1} \langle e_i|\psi\rangle |e_i\rangle = \sum_{i=0}^{d-1} c_i |e_i\rangle \tag{2.15}$$

In the case of a Hilbert space $\mathcal{H}_2$ of dimension $d = 2$, the quantum states are called also "qubits" (from quantum bits) and a basis of the Hilbert space is the *computational basis* $\{|0\rangle, |1\rangle\}$, where

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{2.16}$$

$$|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.17}$$

Classically speaking, the bit can assume a binary value *i.e.* either 0 or 1. In quantum mechanics, the fact that a quantum state can be expressed as a linear combination of other quantum states determines the *superposition principle* (that is considered to be the first postulate of quantum mechanics), according to which

[2]Historically, other notations have been proposed: see, for example, the wavefunction notation introduced by Schrödinger.

a quantum system, described by a quantum state, can find itself in more than one state simultaneously. This condition is called also *quantum superposition*. Let's consider the state $|\psi\rangle$ defined as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.18}$$

The system described by $|\psi\rangle$ is in the state $|0\rangle$ and in the state $|1\rangle$ at the same time.

Up to now we have described the *pure states*, *i.e.* the states that bear maximal information about the quantum system they are describing. If we now consider the ensemble of states $\{|\psi\rangle_1, \{|\psi\rangle_2, ..., |\psi\rangle_K\}$ and the set of probabilities $\{p_1, p_2, ..., p_K\}$ (that satisfy $\sum_{k=1}^{K} p_k = 1$), we can define the *density operator* $\hat{\rho}$ as:

$$\hat{\rho} = \sum_{k=1}^{K} p_k\,|\psi_k\rangle\langle\psi_k| \tag{2.19}$$

where $|\psi_k\rangle\langle\psi_k|$ is the outer product (the result is a matrix). The density operator (also called the density matrix) is Hermitian, non-negative, and it has a unit trace[3].

The formalism of density matrices (introduced by Von Neumann [17]) is used to describe *mixed* (*i.e.* non-pure) *states*, that are states that do not contain all the available information about a quantum system. In other words, the system finds itself in the state $|\psi_1\rangle$ with probability p_1, in the state $|\psi_2\rangle$ with probability p_2 and so on. This is extremely different with respect to the quantum superposition mentioned before, which is a peculiarity of quantum mechanics and it requires the simultaneity, which is not the case described by mixed states.
As a remark, we want to underline that the density matrices and the Dirac notations can coexist, as the density matrix of a pure state $|\psi\rangle$ is simply

$$\hat{\rho}_{|\psi\rangle} = |\psi\rangle\langle\psi| \tag{2.20}$$

This is intuitive when we consider the fact that pure states bear maximal information, therefore the probability that the system they are describing will be in exactly that state is 1, which, substituted in equation 2.19, gives equation 2.20.

We conclude this presentation of quantum states by introducing the *Bloch sphere* (shown in figure 2.4), a three-dimensional sphere with unit radius that contains all the possible qubits. Since a pure quantum bidimensional state can be expressed in

[3]The trace of a matrix $\hat{A}$ is defined as $\mathrm{Tr}[\hat{A}] = \sum_i \langle e_i|\,\hat{A}\,|e_i\rangle$. It is independent of the basis chosen.

terms of the equatorial φ and azimuthal θ angles as:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{2.21}$$

it is possible to map them into a sphere. All the pure states are located on the surface of the sphere, while the mixed states are inside the sphere. The completely mixed state is located in the origin and it is the normalized identity $\hat{\rho}^{\text{mixed}} = \frac{\mathbf{1}}{2}$.

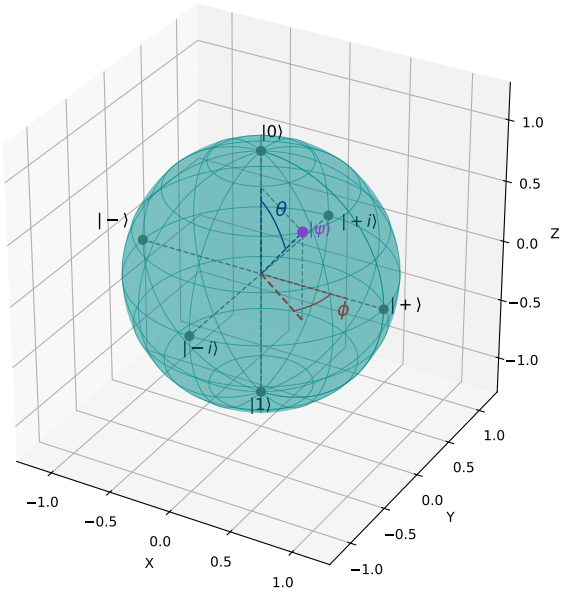

Figure 2.4: The Bloch sphere. The six intersections of the axis are named according the convention $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and $|\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i\,|1\rangle)$. A pure state $|\psi\rangle$ is also represented and the azimuthal and equatorial angles are highlighted.

Measurement

Given a quantum system, we can understand in which state it is by performing a *masurement*. Every measurable physical quantity, called *observable*, is described by a Hermitian operator $\hat{\mathrm{A}} = \hat{\mathrm{A}}^{\dagger}$ acting on $\mathcal{H}$. The outcomes of the measurement are the eigenvalues of the operator, that are non-negative since the operator is Hermitian.

If the spectrum of an observable is discrete and non-degenerate, we can express it

as a linear combination of *projectors* $\hat{\Pi}_i$:

$$\hat{\mathrm{A}} = \sum_i \lambda_i \hat{\Pi}_i \tag{2.22}$$

where λ_i are the eigenvalues of $\hat{\mathrm{A}}$. A projector is an operator defined as $\hat{\Pi} = |\psi\rangle\langle\psi|$.

According to the fact that we already know the possible outcomes of a measurement (the eigenvalues), it is interesting to derive the associated probabilities of observing such outcomes. The *Born Rule* states that:

Theorem 2.4 (Born Rule [18])**.** *Let $\hat{\rho}$ be the density matrix representing a quantum system, and let $\hat{\mathrm{A}}$ be an observable with a spectral decomposition:*

$$\hat{A} = \sum_j \lambda_j \hat{\Pi}_j \tag{2.23}$$

where λ_j are the eigenvalues of $\hat{\mathrm{A}}$ and $\hat{\Pi}_j$ are the corresponding orthogonal projectors.

Then the probability of obtaining the measurement outcome λ_j is:

$$P(\lambda_j) = \mathrm{Tr}\left[\hat{\Pi}_j \hat{\rho}\right] \tag{2.24}$$

It is easy to observe that, starting from equation 2.24, it is possible to arrive, for a pure state $|\phi\rangle$, at the form:

$$P(\lambda_j) = |\langle\psi_i|\phi\rangle|^2 \tag{2.25}$$

where the projector Π_j associated with the eigenvalue λ_j is $\Pi_j = |\psi_j\rangle\langle\psi_j|$.

The Born rule allows us to highlight the intrinsic randomness of quantum mechanics. Let's suppose we have the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and the two projectors $\hat{\Pi}_1 = |0\rangle\langle 0|$ and $\hat{\Pi}_2 = |1\rangle\langle 1|$. According to equation 2.25:

$$P_{|0\rangle} = |\langle 0|\psi\rangle\,|^2 = \left|\frac{1}{\sqrt{2}}(\langle 0|0\rangle + \langle 0|1\rangle)\right|^2 = \frac{1}{2} \tag{2.26}$$

$$P_{|1\rangle} = |\langle 1|\psi\rangle\,|^2 = \left|\frac{1}{\sqrt{2}}(\langle 1|0\rangle + \langle 1|1\rangle)\right|^2 = \frac{1}{2} \tag{2.27}$$

From a classical point of view, this result is completely counter-intuitive. It means that if we have a system that is in a certain state and we measure the probability that this system is in another, different state, we obtain a non-null result.

Collapse

A well-known postulate of quantum mechanics, that goes under the name of *collapse of the wavefunction*, states that, after having measured a quantum system with an observable and having obtained as an outcome an eigenvalue of the observable, the system collapses into the eigenstate associated with that eigenvalue. Let's suppose to have the mixed state $\hat{\rho}$ and the observable $\hat{\mathrm{A}} = \sum_i \lambda_i \hat{\Pi}_i$, if the outcome of the measurement is λ_j (associated to the projector $\hat{\Pi}_j$) then the state $\hat{\rho}$ collapses into $\hat{\rho}'$ according to:

$$\hat{\rho}' = \frac{\hat{\Pi}_j \hat{\rho} \hat{\Pi}_j}{\mathrm{Tr}[\hat{\rho}\hat{\Pi}_j]} \tag{2.28}$$

while for pure states it easy to derive:

$$|\psi'\rangle = \frac{\hat{\Pi}_j |\psi\rangle}{\sqrt{\langle\psi| \hat{\Pi}_j |\psi\rangle}} \tag{2.29}$$

2.2.2 Entanglement, Uncertainty Principle, No-Cloning

We continue this section dedicated to Quantum Mechanics and Quantum Information by presenting three properties, peculiar to the quantum world, that will be crucial in the field of Quantum Key Distribution.

Entanglement

To describe entanglement, it is fundamental to introduce *joint* quantum systems. From the mathematical point of view, let's suppose to have a Hilbert space $\mathcal{H}^A_{d_A}$ of dimension d_A and a Hilbert space $\mathcal{H}^B_{d_B}$ of dimension d_B. We define the joint state $\mathcal{H}^{AB}_{d_{AB}}$ as the tensor product between $\mathcal{H}^A_{d_A}$ and $\mathcal{H}^B_{d_B}$:

$$\mathcal{H}^{AB}_{d_{AB}} = \mathcal{H}^A_{d_A} \otimes \mathcal{H}^B_{d_B} \tag{2.30}$$

Moreover, if $\{|a_i\rangle_A\}_{0\leq i\leq d_A-1}$ constitutes a basis for $\mathcal{H}^A_{d_A}$ and $\{|b_i\rangle_B\}_{0\leq i\leq d_B-1}$ constitutes a basis for $\mathcal{H}^B_{d_B}$, one basis of the joint space is the tensor product $\{|a\rangle_A \otimes |b\rangle_B\}$ between the two bases of the single spaces. The dimension d_{AB} of $\mathcal{H}^{AB}_{d_{AB}}$ is the product $d_A \cdot d_B$ between the dimensions of the two bases. Therefore, a generic vector $|\psi\rangle_{AB} \in \mathcal{H}^{AB}_{d_{AB}}$ can be expressed as:

$$|\psi\rangle_{AB} = \sum_{a,b} \psi_{ab} |a\rangle_A \otimes |b\rangle_B \tag{2.31}$$

We will express the tensor product $|a\rangle_A \otimes |b\rangle_B$ also as $|a\rangle_A |b\rangle_B$ or, in a more compact form, as $|ab\rangle_{AB}$.

A state $|\psi\rangle_{AB}$ of the joint Hilbert space $\mathcal{H}^{AB}_{d_{AB}}$ is called *separable* if it is possible to represent it as the tensor product between two states $|\phi_1\rangle_A$ and $|\phi_2\rangle_B$ belonging to the two Hilbert spaces composing the joint system. In formulas:

$$|\psi\rangle_{AB} = |\phi_1\rangle_A \otimes |\phi_2\rangle_B \tag{2.32}$$

When this condition is not met, the state is called *entangled*.These definitions can be generalized for joint spaces defined as the tensor product of more than two subspaces.

In the case $d_A = d_B = 2$, and therefore $d_{AB} = 4$, the Bell states, defined as:

$$\left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B\right) \tag{2.33}$$

$$\left|\Phi^-\right\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B\right) \tag{2.34}$$

$$\left|\Psi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B\right) \tag{2.35}$$

$$\left|\Psi^-\right\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B\right) \tag{2.36}$$

constitute a basis for the joint Hilbert space and they are known as the *maximally entangled* states. The motivation lies in the fundamental feature of entanglement: the correlation.

Before providing an explanation to the last sentence, we have to define the behaviour of the scalar product in the joint space. If $|\phi\rangle_{AB} = |a_1\rangle_A |b_1\rangle_B$ and $|\psi\rangle_{AB} = |a_2\rangle_A |b_2\rangle_B$, then:

$$\langle\phi|\psi\rangle_{AB} = \langle a_1|a_2\rangle_A \langle b_1|b_2\rangle_B \tag{2.37}$$

Let's consider the situation in which a Bell state, say $|\Phi^+\rangle$ has been created and the two states composing the pair have been sent to two different locations, A and B. Moreover, let's suppose that in the location A it has been done a measurement of the state in the computational basis, and the outcome of the measurement is $|0\rangle_A$. Given this information, what is the state $|\phi\rangle_B$ in B? We can derive it as:

$$|\phi\rangle_B = {}_A\left\langle 0\middle|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}} \left({}_A\langle 0|0\rangle_A \otimes |0\rangle_B + {}_A\langle 0|1\rangle_A \otimes |1\rangle_B\right) = \frac{1}{\sqrt{2}} |0\rangle_B \tag{2.38}$$

Therefore, apart from the normalization factor, we have *perfect correlation* between the outcome of the measurements, no matter what the distance that separates the two states is. As a side note, in case the state was $|\Psi^-\rangle$ we would have had *perfect anticorrelation*.

For our purposes, this presentation of entanglement is enough. We want to mention the fact that it is a delicate argument that was responsible for one of the most known paradox concerning quantum physics, the EPR (Einstein, Podolsky, Rosen) paradox [19]. Moreover, pairs of entangled states can be created in a laboratory by using photons through a process known as Spontaneous Parametric Down Conversion (SPDC), in which the properties of non-linear crystals allow the generation of entanglement (see for more details [20], [21], [22]).

Non-commuting observables and Uncertainty Principle

Given two operators $\hat{\mathrm{A}}$ and $\hat{\mathrm{B}}$ we define their *commutator* as:

$$[\hat{\mathrm{A}}, \hat{\mathrm{B}}] = \hat{\mathrm{A}}\hat{\mathrm{B}} - \hat{\mathrm{B}}\hat{\mathrm{A}} \tag{2.39}$$

If $[\hat{\mathrm{A}}, \hat{\mathrm{B}}] = 0$, we say that $\hat{\mathrm{A}}$ and $\hat{\mathrm{B}}$ *commute*. We present (without proof) the following theorem:

Theorem 2.5. *Two observables $\hat{A} \in \mathcal{H}_{AB}$ and $\hat{B} \in \mathcal{H}_{AB}$ commute if and only if one can construct an orthonormal basis of $\mathcal{H}_{AB}$ with eigenvectors common to $\hat{A}$ and $\hat{B}$.*

The consequence of this theorem is that two commuting observables can be *simultaneously* measured. In fact, given two commuting (they are also called ''compatible'') observables, their order of application is irrelevant: measuring one observable before the other one does not cause any loss of information. As a consequence, it is possible to measure them at the same time. All the observables of classical mechanics are compatible: we can measure the position and the velocity of a car at the exact same time, as well as measuring the position will not cause a loss of information in the case we want to measure the velocity afterwards. In quantum mechanics this is not always true.

Let $\langle\hat{\mathrm{A}}\rangle$ be the expected value of the operator $\hat{\mathrm{A}}$. In quantum mechanics, the *uncertainty* $(\Delta\hat{\mathrm{A}})_\psi$ of the operator $\hat{\mathrm{A}}$ acting on the state $|\psi\rangle$ is defined as:

$$(\Delta\hat{\mathrm{A}})_\psi = \sqrt{\langle\hat{\mathrm{A}}^2\rangle_\psi - \langle\hat{\mathrm{A}}\rangle_\psi^2} \tag{2.40}$$

We are now ready to present the following fundamental theorem:

Theorem 2.6 (Uncertainty Principle, Robertson [23]). *If $\hat{A}_\psi$ and $\hat{B}_\psi$ are two observables and $|\psi\rangle$ is a pure quantum state, then the following inequality is satisfied:*

$$(\Delta\hat{A})_\psi(\Delta\hat{B})_\psi \geq \frac{1}{2}\left|\langle[\hat{A},\hat{B}]\rangle_\psi\right| \tag{2.41}$$

This theorem is a generalization of the famous Heisenberg's Uncertainty Principle, in which Heisenberg derived the uncertainty relation of the position and momentum quantum operators [24].
The relevance of this theorem is capital: it states that, in quantum mechanics, some quantities cannot be measured simultaneously *and* precisely. This result is expected if we recall the collapse of the wavefunction: let's suppose we have a quantum state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and the following projectors:

$$\hat{\Pi}_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \tag{2.42}$$

$$\hat{\Pi}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \tag{2.43}$$

It is easy to verify that $[\hat{\Pi}_1, \hat{\Pi}_2] \neq 0$. If we measure $|\psi\rangle$ with $\hat{\Pi}_1$ and then with $\hat{\Pi}_2$, $|\psi\rangle$ will collapse in $|\psi'\rangle = |0\rangle$. If the order of measurement is reversed, $|\psi\rangle$ will collapse in $|\psi'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

No-Cloning Theorem

So far, we have presented several aspects of quantum mechanics that differentiate all the phenomena happening in quantum systems from the classical world, the one we are used to. In the following, we will introduce another of these peculiar aspects. In classical information theory, it is always possible to make a copy of a state that bears some information. Let's suppose to have a bit stored in a memory: we can perfectly (*i.e.* without losing information about it) copy it in another storage device. Surprisingly, this cannot happen in the quantum world. In other words, it is not possible to perfectly copy an arbitrarily unknown quantum state. This result goes under the name of "No-Cloning Theorem" and it was shown by Wootters and Zurek in 1982 [25].

To prove the No-Cloning Theorem, let's suppose to have an ideal quantum copy machine, that is a device whose input is the joint state $|\psi\rangle_A |0\rangle_C |x\rangle_x$, where $|\psi\rangle$ is the state for which we want a copy, $|0\rangle_C$ is the state on which the copying machine

will copy the content of $|\psi\rangle$ and $|x\rangle_x$ is a generic state representing other possible inputs. The output, intuitively, is $|\psi\rangle_A |\psi\rangle_C |x\rangle_x$. Let's try to use the copying machine with $|\psi\rangle = |0\rangle$ and $|\psi\rangle = |1\rangle$:

$$|0\rangle_A |0\rangle_C |x\rangle_x \xrightarrow{COPY} |0\rangle_A |0\rangle_C |x\rangle_x \tag{2.44}$$

$$|1\rangle_A |0\rangle_C |x\rangle_x \xrightarrow{COPY} |1\rangle_A |1\rangle_C |x\rangle_x \tag{2.45}$$

We observe that the copying operation is a linear operation. Exploiting this, let's try to copy $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$:

$$|\psi\rangle_A |0\rangle_C |x\rangle_x \xrightarrow{COPY} \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_C |x\rangle_x + |1\rangle_A |1\rangle_C |x\rangle_x) \neq |\psi\rangle_A |\psi\rangle_C |x\rangle_x \tag{2.46}$$

With a simple proof we showed the impossibility of building a quantum copying machine. Relaxing the constraints, it can be shown that it is possible to design a copying machine that is capable of obtaining ''blurred'' (*i.e.* non-perfect) copies of quantum states (see [26]).

2.3 Fundamentals of Quantum Optics

2.3.1 Polarization encoding and Jones calculus

In the following, we will present how it is possible to use light, and in particular photons, to encode quantum states.

Starting from the general equation of the quantum electric field of an electromagnetic wave travelling in vacuum[4]:

$$\hat{\mathbf{E}}(\mathbf{r}, t) = i \sum_{\mathbf{k},s} \sqrt{\frac{\hbar\omega_{\mathbf{k}}}{2\varepsilon_0 V}} \left[ ]\hat{a}_{\mathbf{k},s} e^{i(\mathbf{k}\cdot\mathbf{r} - \omega_{\mathbf{k}} t)} - \hat{a}^\dagger_{\mathbf{k},s} e^{-i(\mathbf{k}\cdot\mathbf{r} - \omega_{\mathbf{k}} t)} \right] \boldsymbol{\varepsilon}_{\mathbf{k},s} \tag{2.47}$$

we observe its dependence on the polarization vector $\boldsymbol{\varepsilon}_{\mathbf{k},s}$ that lies in a plane orthogonal to the propagation axis. If we assume, as a convention, that the horizontal and vertical directions are aligned with the X and Y axes, respectively, a linearly polarized single photon state in the horizontal and vertical direction will

[4]The electromagnetic field can be quantized by treating each mode as a quantum harmonic oscillator. In this formalism, first introduced by Dirac, the field is described in terms of annihilation and creation operators, $\hat{a}$ and $\hat{a}^\dagger$, which destroy or create photons in the various polarization states. As a result, the classical electric field $\mathbf{E}(\mathbf{r}, t)$ is replaced by the field operator $\hat{\mathbf{E}}(\mathbf{r}, t)$, expressed as a linear combination of these operators. A detailed derivation can be found in standard references such as [27].

be indicated, respectively, by:

$$|H\rangle \equiv |0\rangle \tag{2.48}$$

$$|V\rangle \equiv |1\rangle \tag{2.49}$$

Following this analogy, we can define the photons linearly polarized with an angle of $\pm 45°$ with respect to the horizontal direction (called diagonally and antidiagonally polarized) as:

$$|D\rangle \coloneqq \frac{1}{\sqrt{2}}(|H\rangle + |V)\rangle \tag{2.50}$$

$$|A\rangle \coloneqq \frac{1}{\sqrt{2}}(|H\rangle - |V)\rangle \tag{2.51}$$

Analogously, the right and left circularly polarized photons are defined, respectively, as:

$$|R\rangle \coloneqq \frac{1}{\sqrt{2}}(|H\rangle + i\,|V)\rangle \tag{2.52}$$

$$|L\rangle \coloneqq \frac{1}{\sqrt{2}}(|H\rangle - i\,|V)\rangle \tag{2.53}$$

Since the two states composing the pair are orthonormal, each pair constitutes a basis for the bidimensional Hilbert space. In particular, we define the $\mathbb{Z}$ basis as $\mathbb{Z} = \{|H\rangle, |V\rangle\}$, the $\mathbb{X}$ basis as $\mathbb{X} = \{|D\rangle, |A\rangle\}$, and the $\mathbb{Y}$ basis as $\mathbb{Y} = \{|R\rangle, |L\rangle\}$.

It is straightforward that, in order to encode a classical bit, it is sufficient to choose a basis and assign the 0 value to one polarization and the 1 value to the other one: this is exactly the principle of using polarization to encode information.

Practically speaking, we will now show how it is possible to change the polarization of the light. According to a formalism known as *Jones calculus*, a quantum state described by the vector $|\psi\rangle = \alpha\,|H\rangle + \beta\,|V\rangle$ is transformed by a polarization device into

$$|\psi'\rangle \coloneqq \alpha'\,|V\rangle + \beta'\,|H\rangle = S^J\,|\psi\rangle \tag{2.54}$$

where we used the scattering matrix S^J to describe the transformation.

Intuitively, a ''polarization device'' is a tool used to manipulate the polarization of the light that enters it. A well-known example is given by the waveplates, that are devices made of birefringent material (with a different refractive index for the two orthogonal axes, such that the fast axis is characterized by n_{fast} and the slow

axis by n_{slow}, that respect $n_{\text{fast}} < n_{\text{slow}}$). We define the retardance induced by the waveplate as $\Gamma \coloneqq \frac{2\pi}{\lambda} d\delta_n$[5].
The scattering matrix of a waveplate is:

$$S \equiv \begin{pmatrix} e^{-i\frac{\Gamma}{2}} & 0 \\ 0 & e^{+i\frac{\Gamma}{2}} \end{pmatrix} \tag{2.55}$$

By tuning it to $\Gamma = \pi$ we obtain the so-called Half Wave-Plate (HWP), while with $\Gamma = \frac{\pi}{2}$ we have the Quarter Wave-Plate (QWP). It is possible to show that, by combining a HWP and a QWP, it is possible to obtain the six polarization states that we introduced before.

2.3.2 Quantum states of light

The quantization of the electric field (introduced in section 2.3.1) in terms of the creation and annihilation operators led to the definition of different types of quantum states: among them, we will present the Fock states and the coherent states.

Let's reduce ourselves, for simplicity, to the case of a single mode electric field. We define the *number operator* $\hat{n}$ as the product between the creation and the annihilation operator:

$$\hat{n} \coloneqq \hat{a}^\dagger \hat{a} \tag{2.56}$$

The eigenstates of the number operator are called *Fock states*. Of course, they must respect the relation:

$$\hat{n} \left|n\right\rangle = n \left|n\right\rangle \tag{2.57}$$

The action of $\hat{a}^\dagger$ and $\hat{a}$ on a Fock state $\left|n\right\rangle$ is defined respectively as

$$\hat{a}^\dagger \left|n\right\rangle = \sqrt{n+1} \left|n+1\right\rangle, \ \hat{a} \left|n\right\rangle = \sqrt{n} \left|n-1\right\rangle \tag{2.58}$$

From this it follows that a Fock state $\left|n\right\rangle$ can be expressed as:

$$\left|n\right\rangle = \frac{\hat{a}^\dagger}{\sqrt{n!}} \left|0\right\rangle \tag{2.59}$$

This is an explanation of why $\hat{a}$ and $\hat{a}^\dagger$ are called creation and annihilation operator. A system that contains *exactly* n quantum states of light (*i.e.* n photons) is described by the Fock state $\left|n\right\rangle$.
Since they are complete and orthonormal, they constitute a basis for the Fock space

[5] In this formula, λ is the wavelength of the light impinging the device, d is the thickness of the waveplate and $\delta_n = n_{\text{slow}} - n_{\text{fast}}$.

$\mathcal{F}$, defined as the infinite direct sum $\bigoplus$ of increasing n-photon Hilbert spaces $\mathcal{H}_n$:

$$\mathcal{F} = \bigoplus_{n=0}^{\infty} \mathcal{H}_1^n \tag{2.60}$$

The behavior of Fock states is said to be non-classical: for example, they have non-positive Wigner functions (a quasi-probabilistic representation in the ''phase space''). However, they are extremely useful in many areas, for example, when dealing with single-photon effects.

If now we consider the annihilation operator $\hat{a}$, we define *coherent states* its eigenstates, that are the states $|\alpha\rangle$ that satisfy:

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle \tag{2.61}$$

Since the Fock states constitute a basis for the Fock space, it is easy to show that coherent states can be expressed as a linear combination of Fock states. In particular:

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle \tag{2.62}$$

A coherent states can be written as a *displaced vacuum state*:

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle \tag{2.63}$$

by exploiting the displacement operator $\hat{D} \coloneqq e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}$.

On the contrary with respect to Fock states, there are several examples in which coherent states behave similarly to classical states (for example, they have a non-negative Wigner function). Moreover, for our purposes, we can consider the light emitted by a laser made of coherent states.

2.3.3 Beam-splitter

A beam-splitter (BS) is an optical component whose purpose is, as its name suggests, to split a light beam. A BS can be realized both for fiber and free-space setups, and one of its most relevant characteristics is the splitting ratio, *i.e.* the percentage of light that exits from each of its two outputs. In this thesis, we will deal with BS composed of two inputs and two outputs.
From the formal point of view, they are described by a matrix, called *scattering*

matrix, defined as:

$$\mathcal{S}_{BS} = \begin{bmatrix} \sqrt{T}e^{i\phi_{11}} & \sqrt{R}e^{i\phi_{12}} \\ \sqrt{R}e^{i\phi_{21}} & \sqrt{T}e^{i\phi_{22}} \end{bmatrix} \tag{2.64}$$

in which R and T must satisfy

$$R + T = 1 \tag{2.65}$$

due to the conservation of energy and the phases must respect

$$\phi_{11} + \phi_{22} = \pi + \phi_{12} + \phi_{21} \tag{2.66}$$

The last equation allows a certain freedom while choosing the phases, resulting in different conventions. The most used ones are $\phi_{11} = \phi_{22} = 0, \phi_{12} = \frac{\pi}{2}, \phi_{21} = -\frac{3}{2}\pi$ to which it is associated the scattering matrix

$$\mathcal{S}_{BS} = \begin{bmatrix} \sqrt{T} & i\sqrt{R} \\ i\sqrt{R} & \sqrt{T} \end{bmatrix} \tag{2.67}$$

and $\phi_{11} = \phi_{22} = \phi_{21} = 0, \phi_{12} = -\pi$ which leads to

$$\mathcal{S}_{BS} = \begin{bmatrix} \sqrt{T} & -\sqrt{R} \\ \sqrt{R} & \sqrt{T} \end{bmatrix} \tag{2.68}$$

It is easy to prove that a BS behaves differently depending on which type of states enter it. Considering a balanced BS ($T = R = 0.5$), if there is a single photon state (*i.e.* the Fock state $|1\rangle$) impinging it, the joint state of the output $|\Psi\rangle$ is the entangled state ($|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$), while if at the two inputs two identical single photon states enter simultaneously, a famous phenomenon, known as Hong-Ou-Mandel effect [28] happens.

3

Quantum Key Distribution

The aim of Quantum Key Distribution (QKD) is to provide an unconditionally secure way of delivering cryptographic keys between two users by relying on the laws of quantum physics. In this chapter, we will present the seminal QKD protocol, named BB84 after the surnames of the researchers that proposed it. We will provide an extended overview of its theoretical execution and of the security properties that it satisfies, finally concluding with the properties and the challenges that characterize real-world implementations.

3.1 BB84

The first QKD protocol was presented in 1984 by Bennett and Brassard in a groundbreaking article [29]. We will now present the most basic version of BB84, that served as a fundamental reference for both the practical implementations (see section 3.3) and for evolved schemes (see chapter 4), and that nonetheless shows all its crucial features.

3.1.1 Setup and execution

The two legitimate parties, usually called *Alice* and *Bob*, are connected by two public channels. The first, the quantum channel, is used to exchange quantum states, *i.e.* photons, between them. The second channel is a classical channel that must be authenticated and we consider it to be errorless. We want to stress that both channels are public; therefore, a possible eavesdropper, *Eve*, is potentially able to read the quantum and classical communications. Moreover, we must also consider

the possibility that she forges or modifies messages in the quantum channel (and not in the classical one, since it is authenticated). The setup is shown in figure 3.1.

In a BB84 exchange, Alice chooses two *mutually unbiased* bases to encode her quantum states, which typically are $\mathbb{Z} = \{|H\rangle, |V\rangle\}$ and $\mathbb{X} = \{|D\rangle, |A\rangle\}$. It is possible to associate a binary value to the two states composing the basis, for example:

$$|H\rangle \rightarrow 0$$

$$|V\rangle \rightarrow 1$$

$$|D\rangle \rightarrow 0$$

$$|A\rangle \rightarrow 1$$

Then, each round, she picks one basis and a state within such basis. It is fundamental that the choice criterion must be completely *random*, *i.e.*

$$p_{|H\rangle} = p_{|V\rangle} = p_{|D\rangle} = p_{|A\rangle} = \frac{1}{4} \tag{3.1}$$

In an advanced version of BB84, called ''Efficient-BB84'', the probabilities are not uniform: one basis is prepared and measured with high probability, and it called the *key basis*, since the raw key will be derived from it. The other basis, called the *check basis* is needed just to check whether an adversary interfered with the communication.

Bob, when receives a photon, randomly decides whether to measure it in the $\mathbb{Z}$ or $\mathbb{X}$ basis and records the outcome.
If for some photons the preparation and the measurement bases do not coincide (for example, Alice prepares a state in the $\mathbb{X}$ basis while Bob measures in the $\mathbb{Z}$ basis), the sequences of symbols that they have at the end of the round are different, due to the randomness of the measurement of quantum states (as highlighted in section 2.2.1).
For this reason, they perform the *sifting* phase, in which they communicate to each other, through the authenticated classical channel, the basis used for each state. Note that a potential attacker, even eavesdropping on the channel, since it is public, would not be able to retrieve the sequences of Bob and Alice information, as it is not possible infer the quantum states from the bases. However, sifting is a leakage of information that might help a potential attacker. At this point, if no errors occurred during the transmission of quantum states and if we assume that there were no adversary that tried to retrieve the key, Alice and Bob should share

the same sequence of symbols, *i.e.* the key.

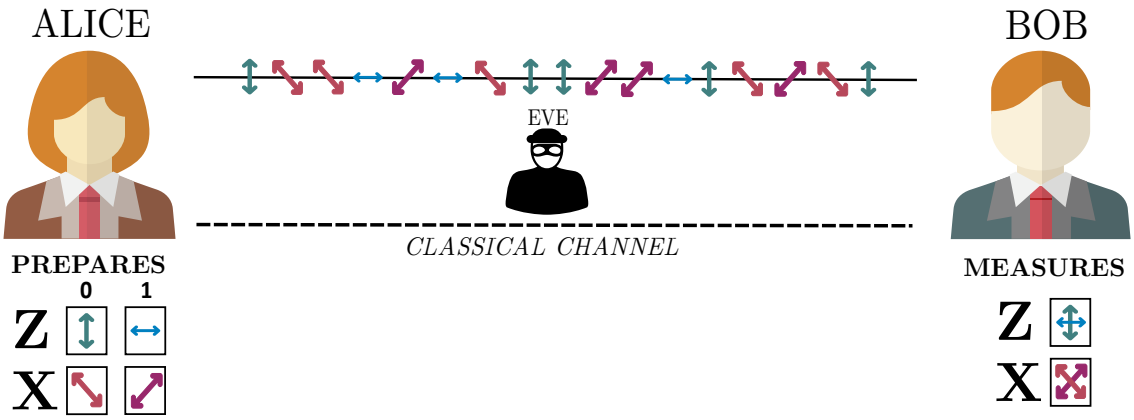

Figure 3.1: The setup of BB84.

Let's now consider the possibility that Eve interfered. Since the states prepared by Alice belong to mutually unbiased bases, she cannot perform a simultaneous and precise measurement on both bases due to the Uncertainty Principle (see section 2.2.2). If she were able to perform a copy of the message transmitted by Alice, in the same fashion as in classical communication, then she could store the copy for herself and send the message to Bob, who would remain unaware of the interference. However, the No-Cloning theorem (see section 2.2.2) prevents her from performing this attack.

Nonetheless, she could still choose the following strategy: intercepting the photon sent by Alice, performing a measurement randomly choosing between the $\mathbb{Z}$ and $\mathbb{X}$ basis, and, according to the outcome, preparing a new state, in the same basis of her measurement, and sending it to Bob. With probability $\frac{1}{2}$ she chooses the correct basis; therefore, she learns the state sent by Alice, prepares the exact same state, and sends it to Bob. Eve knows the correct quantum state without Alice and Bob knowing about her interference. If she chooses the wrong basis, the photon delivered to Bob will be also encoded in the wrong basis: if Bob chooses as measurement basis the same that Alice used to prepare the state (these events are the only relevant after the sifting), and therefore the conjugate of the one chosen by Eve, the probability that he detects an error (*i.e.* he and Alice do not share the same symbol even though they used the same basis), is $\frac{1}{2}$.

Let's suppose that Alice chooses the basis $\mathbb{Z}$ and that she sends $|V\rangle$. Eve tries to guess the preparation basis and chooses $\mathbb{X} = \{|D\rangle, |A\rangle\}$ and performs a measurement. In this case, according to the Born rule, the outcome probabilities $p_{|D\rangle}$ and

$p_{|A\rangle}$ are, respectively,

$$p_{|D\rangle} = |\langle D|V\rangle|^2 = \left|\frac{1}{\sqrt{2}}\left(\langle H|V\rangle + \langle V|V\rangle\right)\right|^2 = \frac{1}{2} \tag{3.2}$$

$$p_{|A\rangle} = |\langle A|V\rangle|^2 = \left|\frac{1}{\sqrt{2}}\left(\langle H|V\rangle - \langle V|V\rangle\right)\right|^2 = \frac{1}{2} \tag{3.3}$$

This means that the state she retrieves is random and wrong. At this point, she prepares a new state according to the outcome she got. Let's suppose that she prepares $|D\rangle$, sends it to Bob, who chooses $\mathbb{Z}$ as a measurement basis, *i.e.* the correct measurement basis. Once again, according to the Born rule, the outcome probabilities of a measurement performed on the state sent by Eve are:

$$p_{|H\rangle} = |\langle H|D\rangle|^2 = \left|\frac{1}{\sqrt{2}}\left(\langle H|H\rangle + \langle H|V\rangle\right)\right|^2 = \frac{1}{2} \tag{3.4}$$

$$p_{|V\rangle} = |\langle V|D\rangle|^2 = \left|\frac{1}{\sqrt{2}}\left(\langle H|H\rangle - \langle H|V\rangle\right)\right|^2 = \frac{1}{2} \tag{3.5}$$

Finally, as stated before, in the case Eve chooses the wrong basis and Bob the correct one, the state prepared by Alice and the state measured by Bob differ with a probability of $\frac{1}{2}$. Moreover, if we consider the choice of the measurement basis of Eve and Bob to be random and independent, the overall probability that Bob gets a wrong outcome while choosing the same basis as Alice is $\frac{1}{4}$. This attack strategy is known as *Intercept-and-Resend* attack.
From these considerations, it is simple to understand that the presence and the intervention of an adversary can be revealed by the QBER (Quantum Bit Error Rate). We want to stress that the QBER might also be deriving from errors introduced by the quantum channel.

In real world applications, it is impossible to assume an errorless quantum channel; however, it is possible to set a threshold on the QBER (Quantum Bit Error Rate) over which the presence of an eavesdropper has to be considered as certain. What to do in that case? It is common to proceed with a step, known as *parameter estimation*, in which Alice and Bob compare a subset of their bits to estimate the quantum bit error rate (QBER). If the error rate exceeds a certain threshold, indicating possible eavesdropping or excessive noise, they may abort the protocol and start a new exchange.

However, in practice, as long as the QBER remains below an acceptable threshold, the protocol proceeds with the classical post-processing.
We have to highlight that it is always possible to perform a *Denial of Service* (DOS) attack in QKD, as any external interference contaminates the quantum communication between the two legitimate users, causing an increase in the error in the channel.

After the sifting, there is a phase known as *advantage distillation*, firstly presented in [30], in which Alice and Bob exploit the classical, authenticated channel to achieve an advantage over Eve (see also [31] and [32]). Subsequently, there is a step known as *information reconciliation*, in which Alice and Bob use classical techniques to correct the errors in the two sequences (by using, for example, the CASCADE protocol [33] or LDPC codes [34]). And finally, the residual information that Eve may have left (note, for example, that in order to correct errors, Alice and Bob have to reveal information about their sequences through the classical channel, which is public) is eliminated by privacy amplification, firstly presented in [35].

3.1.2 Entanglement-based implementation

The description we gave of the BB84 describes a scenario called ''Prepare-and-Measure'' (P&M), in which one of the two parties chooses and prepares the quantum states while the other one effectuates measurements.

Let's now consider a scenario (depicted in figure 3.2) in which the states are prepared by a third, trusted (*i.e.* not under the control of an adversary) entity, that sends them to Alice and Bob, who both measure in the $\mathbb{Z}$ or $\mathbb{X}$ basis. In this case, Alice and Bob are symmetric also from the physical point of view, as they are both receivers. It is fundamental to mention that the source may be placed either at Alice's or Bob's side.

Let's suppose that the source prepares pairs of entangled states, and sends one of them to Alice and the other one to Bob, then it is possible to show that the Prepare-and-Measure implementation is completely equivalent to the Entanglement-based (EB) one.
In fact, let's examine the case in which the state prepared is the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$ and Alice decides to use the basis $\mathbb{X} = \{|+\rangle, |-\rangle\}$ (with $|\pm\rangle \coloneqq \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$) for the measurement: the state on Bob's side, due to the perfect correlation given by the entanglement, collapses into

$$ {}_A\langle \pm | \Phi^+ \rangle_{AB} = |\pm\rangle_B \tag{3.6} $$

We are basically exploiting the property of entanglement according to which, when one of the states of the pair is measured, the other one collapses accordingly. This ensures that the action of Alice (or Bob, it is indifferent) of measuring with a basis on her (his) side corresponds to *preparing* a state in that basis for Bob's (Alice's) side.

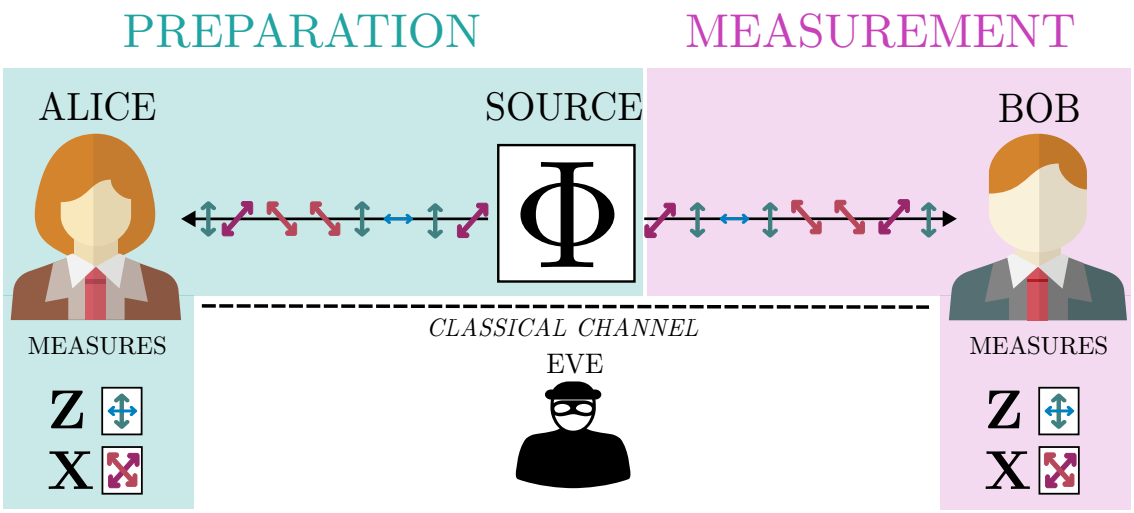

Figure 3.2: The setup of the BB84 in the Entanglement-Based scenario. We highlight the equivalence with the Prepare-and-Measure scenario by considering the source of entangled states and one of the two measurement apparatus (in this case Alice).

Due to the complete equivalence between these two approaches, the Prepare-and-Measure is often used in practical implementations or descriptions (as we did), while the security analysis is typically easier in the Entanglement-Based scenario. Nonetheless, there are some protocols that inherently exploit the Entangled-Based implementation to achieve remarkable results (see [36]).

3.1.3 Assumptions

In order for a QKD protocol to be secure and operate correctly, several assumptions must be satisfied.

- *Validity of quantum mechanics*: no faster-than-light signaling, Uncertainty Principle and No-Cloning theorems hold.
- *Authenticated classical channel*: Alice and Bob share an authenticated classical link so that Eve cannot alter the exchanged messages (although she can listen).

- *Adversary control of the quantum channel*: Eve may manipulate the quantum channel in any way allowed by physics, including introducing loss or delay.
- *No significant side channels in the channel itself*: the only information leakage is through the intentionally transmitted quantum states.
- *Correct state preparation*: the source emits the intended quantum states without unwanted correlations.
- *Trusted photon source and detector model*: Alice and Bob have access to trusted sources and detectors.
- *Truly random number generation*: all random choices (basis selection, bit encoding, privacy amplification) must be unpredictable.

3.2 Information theoretic security

3.2.1 Secret key rate

Intuitively, a round of Quantum Key Distribution succeeds when Alice and Bob are able to exchange some bits in a secure way. The metric that describes this event is known as *secret key rate* (SKR), it is denoted by r and it defines the number of secret bits that can be used as a cryptographic key after the execution of the protocol: a positive secret key rate indicates that the exchange has been successful. Moreover, if the number of states successfully exchanged is n, the length of the key deriving from the execution of the protocol is $l = r \cdot n$. It is common to distinguish the *asymptotic* secret key rate, that is a key rate obtainable by using an infinite number of quantum states, from its *finite-size* version, that must take into account the limited number of quantum states used during the exchange.

A fundamental result is:

Theorem 3.1 (Devetak-Winter [37])**.** *The asymptotic key rate in a QKD protocol (in the case of coherent attacks) is upper bounded by:*

$$r \leq I(A, B) - I(A, E) \tag{3.7}$$

With $I(A, B)$ and $I(A, E)$ we are referring to the mutual information[1] between the two legitimate parties, and between Alice and the eavesdropper, respectively. Following this result, we can intuitively understand that a negative key rate means that we are not exchanging bits in a secure way, and therefore the protocol failed: in fact, the information of Eve about the key $I(A, E)$ would be higher than the information shared between Alice and Bob $I(A, B)$.

If we don't consider the presence of the eavesdropper, the rate would be exactly

$$r \leq C = I(A, B) \tag{3.8}$$

where C is known as channel capacity, a metric widely used in classical telecommunications. Intuitively, the channel capacity can be defined as the maximal amount of information that Alice and Bob are able to share in a *reliable* way *i.e.* in a way in which the receiver is able to retrieve what the transmitter sent.

Now, since our aim is to have also a *secure* communication, we have to take into account the effect of the presence of Eve. Following our intuition, equation 3.1 says that the rate r we are left with is made of the amount of information that Alice and Bob are able to exchange minus the amount of information that Eve is able to retrieve. As outlined before, the quantity $I(A, B)$ is classical (since it is computed on classical key registers held by Alice and Bob) and can be evaluated in a simple way following the definition. On the other hand, Eve is a quantum adversary, which means that she can manipulate quantum states. In the worst-case scenario, the maximal amount of information that Eve can retrieve is bounded by the Holevo bound χ_{EA}:

$$I(E, A) \leq \chi_{EA} = S(\hat{\rho}_E) - \sum_b p_b S(\hat{\rho}_{E|b}) \tag{3.9}$$

where $S(\hat{\rho}_E)$ is the Von Neumann[2] entropy of $\hat{\rho}_E$ and p_b represents the probability distribution related to the outcome that Bob obtains after the measurement. The secret key rate can be derived by evaluating $I(A, B)$ and χ_{AE}. A complete discussion

[1]The mutual information, introduced in Shannon's article [2], is defined as $I(X, Y) = H(X) - H(X|Y)$, where X and Y are random variables and $H(\cdot)$ and $H(\cdot|\cdot)$ are the entropy and the conditional entropy, respectively (in the case of communication, X and Y are the sequences of symbols of the two parties). If the two parties want to communicate, it is clear that they must maximize their mutual information.

[2]It is the quantum version of Shannon entropy and it is defined as $S(\hat{\rho}) = -\mathrm{Tr}[\hat{\rho} \log_2 \hat{\rho}]$

and derivation is presented in [38]. Finally, the secret key rate of BB84 is:

$$r = 1 - h_2(E_z) - h_2(E_x) \tag{3.10}$$

where E_x and E_z are the errors in the $\mathbb{X}$ and $\mathbb{Z}$ respectively, and $h_2(\cdot)$ is the binary entropy. If $E_x = E_z = Q$

$$r = 1 - 2h_2(Q) \tag{3.11}$$

As outlined before, the QBER represents a fundamental parameter. By using the BB84, it is possible to tolerate up to $\approx 11\%$ QBER: over this threshold, the protocol must be aborted, as the secret key rate becomes negative (*i.e.* there has been an intervention from an eavesdropper).

3.2.2 Post-processing

Let's now analyze how the information theoretic quantities $I(A, B)$ and $I(A, E)$ evolve during the post-processing phase. We will refer to figure 3.3 (taken from [39]), in which the raw key of Alice and Bob are represented by the random variables x and y, while the sequence that Alice possesses is denoted as z.

In the first step, randomness and information are shared between A and B, described by their mutual information, which is upper bounded by the entropy of each of the two. However, in this phase, randomness and information are shared also with the eavesdropper: let's consider the worst case, that is the one in which the mutual information between A and E is higher with respect to the one between A and B.

Then, Alice and Bob can perform an *advantage distillation* step: they jointly process blocks of their correlated raw key bits and keep only those blocks that are more reliably correlated. This reduces the length of their raw key, and therefore its entropy, since fewer symbols remain. However, the crucial effect is that the mutual information between Alice and Bob increases relative to Eve's information. An extended treatment of advantage distillation in QKD is presented in [40]. In terms of the graph, the sequences x, y and z are transformed, respectively, into x', y' and c'. Note that now the mutual information between Eve and Alice (*i.e.* what Eve knows about the key) takes into account both z and c', as Eve may have retrieved additional information from the public exchange that happened in the classical channel.

In the *information reconciliation* step, the aim is that the sequence of Alice and

the sequence of Bob coincide; this means that:

$$I(A, B) = H(A) - H(A|B) = H(A) \tag{3.12}$$

because the conditional entropy of two identical random sequences is null. The side effect is that also the eavesdropper gains information, since the error correction procedures employ the classical, public channel to exchange information; therefore, the mutual information $I(A, E)$ increases (this is justified by the intuition that error correction algorithms need to exchange some symbols of the sequences in order to correct errors, and these symbols are shared over the public channel). Once again, in graph 3.3 the random variables are transformed.

Finally, to remove the residual information that the eavesdropper has, we apply the *privacy amplification*, where we typically employ a compression function (see for example [41]). This results in the decrease of the mutual information between Alice and Eve. Of course, this will be reflected also in the shared sequence between Alice and Bob, whose entropy will decrease. Once again, if the symbols are uniformly sampled and i.i.d., the decrease of the entropy coincides with the decrease of the length. Regarding this, it is worth mentioning the fact that a significant fraction of the bits exchanged is discarded throughout the process: some because of channel losses, some because of sifting, and some because of the classical post-processing.

At this point it is possible to evaluate the secret key rate, to determine whether the protocol round was successful or not. In the positive case, the final sequence is random and secure.

3.2.3 Metrics

What are the parameters to evaluate a QKD exchange? Having a positive key ratio basically ensures that we are successfully delivering the key between the two parties, but does not provide any additional information regarding the security against an adversary.

As outlined in the previous section, a positive secret key rate is the indication that the QKD round terminated with the secure sharing of a cryptographic key. However, we need to quantify the security achieved in the execution of the protocol. For this reason, we will provide a formal framework articulated by different definitions, following the presentation given in chapter 5 of [42].

First of all, let's recall that the aim of the security definitions based on the indis-

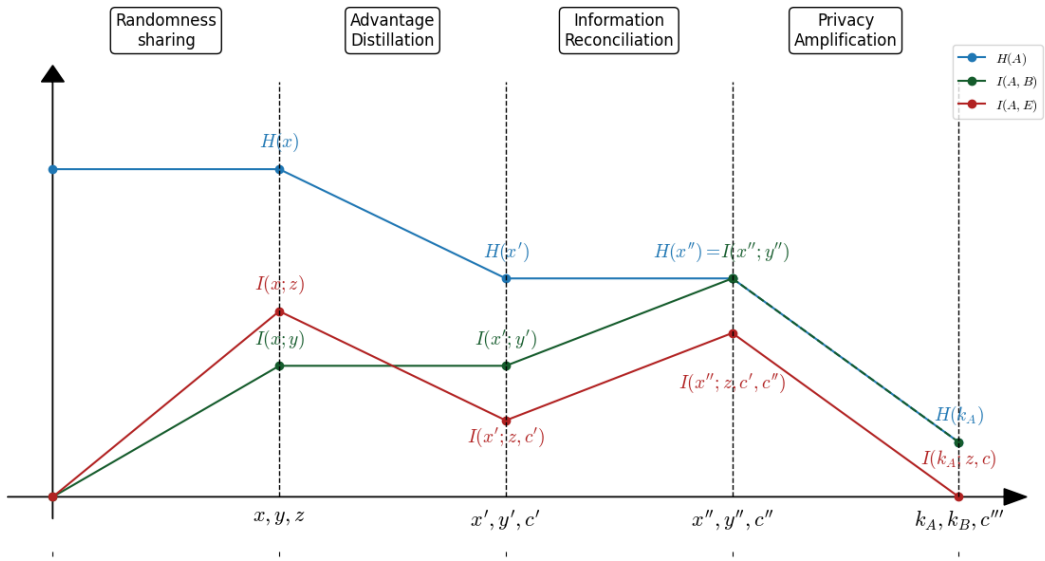

Figure 3.3: The evolution of information theoretic quantities during the post-processing of QKD.

tinguishability is to provide an estimate of the security mechanism based on ''how far'' the mechanism is from its ideal version. The ideal version of a key exchange mechanism is a system that delivers two identical copies of a random cryptographic key to the two intended receivers and delivers useless information to the eavesdropper. Moreover, we want to guarantee that the QKD protocol we are analyzing can be used as a subroutine in another protocol (for example, a One-Time-Pad routine that uses QKD as a subroutine to generate the cryptographic key) and we want that the eavesdropper cannot retrieve the complete key even if he already possesses some bits of it. These requirements are satisfied by the *universal security* definitions, firstly introduced in [43].

The first aspect to take into consideration, however, is the *robustness* of the protocol, that is the capability of being executed (*i.e.* not to be aborted). It is a rather pragmatic concept, yet having the best protocol on paper which never succeeds is completely useless and meaningless.

Definition 3.1 (ε-robustness)**.** *A protocol is ϵ-robust if, without the interference of an eavesdropper, the probability $p^{\perp}$ that it aborts is:*

$$p^{\perp} \leq \varepsilon \tag{3.13}$$

Intuitively, another requirement for a QKD protocol to be successful is that, at the end of the exchange, Alice and Bob share the same key. Therefore:

Definition 3.2 (ε-correctness)**.** *Let K_A and K_B be the random variables describing*

the keys of Alice and Bob, respectively. Then, the QKD protocol is said to be ϵ-correct if:

$$P(K_A \neq K_B) \leq \varepsilon_{corr} \tag{3.14}$$

Now, let's consider the secrecy of the key. If we start from the idea of the security based on indistinguishability, our aim is to find the distance between the real and ideal version of the key. Regarding the ideal version, Alice's key has to be completely random and Eve must have zero information (*i.e.* correlation) about it. These two requirements are translated into the quantum joint state

$$\hat{\rho}_{AE}^{\text{ideal}} = \hat{\rho}_{\mathbf{1}}^{A} \otimes \hat{\rho}^{E} \tag{3.15}$$

note that $\hat{\rho}_{AE}^{\text{ideal}}$ is a separable state, therefore there is no correlation between the state of Alice and the state of Eve (*i.e.* Eve has no information about Alice's key), and Alice's state is the completely mixed state $\hat{\rho}_{\mathbf{1}} = \frac{1}{2}\mathbf{1}$, that is a state that guarantees a random outcome whatever measurement is performed on it. What about the real state? In this case we have the classical-quantum state

$$\hat{\rho}_{AE}^{\text{real}} = \sum_{k_A} p_{k_A} \left|k_A\right\rangle^A \left\langle k_A\right| \otimes \hat{\rho}_{k_A}^{E} \tag{3.16}$$

Alice's state is classical, as it represents the key she actually possesses, while Eve's state $\hat{\rho}_{k_A}^{E}$ is conditioned on the values that Alice's key takes. To evaluate the distance between $\hat{\rho}_{AE}^{\text{ideal}}$ and $\hat{\rho}_{AE}^{\text{real}}$ we use the *trace distance*, a quantum information metric defined as:

$$T(\hat{\sigma}_1, \hat{\sigma}_2) = \frac{1}{2}\|\hat{\sigma}_1 - \hat{\sigma}_2\|_1 \tag{3.17}$$

We are finally ready to provide the following definition:

Definition 3.3 (ε-secrecy)**.** *A quantum key distribution is said to be ϵ-secret if:*

$$(1 - p^{\perp})\|\hat{\rho}_{AE}^{ideal} - \hat{\rho}_{AE}^{real}\| \leq \varepsilon_{sec} \tag{3.18}$$

An analogous reasoning can be applied by taking into consideration Bob instead of Alice, as the probability that their keys differ is upper bounded by ε_{corr}.
But what about giving a definition that includes both Alice and Bob? If the protocol is ε-secure when we consider Alice, and the states (and therefore the keys) of Alice and Bob are different with probability $(1 - p_{corr})$, what can we say about the *joint state* between Alice and Bob and the state of Eve? We can define, with the same

justifications, the classical quantum state $\hat{\rho}^{\text{real}}_{ABE}$ as

$$\hat{\rho}^{\text{real}}_{ABE} = \sum_{p_{k_A}, p_{k_B}} p_{k_A k_B} \left|k_A k_B\right\rangle^{AB} \left\langle k_A k_B\right| \otimes \hat{\rho}^{E}_{k_A k_B} \tag{3.19}$$

we notice the entanglement between Alice's and Bob's states: this is justified by the fact that they must be strongly correlated. The ideal state $\hat{\rho}^{\text{ideal}}_{ABE}$ is

$$\hat{\rho}^{\text{ideal}}_{ABE} = \hat{\rho}^{AB}_{\mathbf{1}} \otimes \hat{\rho}^{E} \tag{3.20}$$

The evaluation of the trace distance between these two states provides the following definition:

Definition 3.4 (ε-security)**.** *A QKD protocol is ε-secure if:*

$$(1 - p^{\perp}) \| \hat{\rho}^{ideal}_{ABE} - \hat{\rho}^{real}_{ABE} \| \leq \varepsilon \tag{3.21}$$

Following the intuition, if a QKD protocol is ε-secret, which means that the joint state between one of the two parties and the eavesdropper is at least ε_{sec} close (in terms of trace distance) to the ideal state, and it is also ε_{corr}, which means that the probability that Alice's and Bob's state differ is upper bounded by ε_{corr}, one would think that this protocol is also ε-secure, according to 3.4. This result is formalized by the following theorem:

Theorem 3.2. *If a protocol is ε_{corr}-correct and ε_{sec}-secret, then it is ε-secure, with $\varepsilon = \varepsilon_{corr} + \varepsilon_{sec}$.*

The fundamental feature of QKD is that it provides ε-unconditional security. Over the last decades, several security proofs have been presented: in [38] there is one of the most remarkable approaches in the security of BB84.

3.3 Practical implementations

So far, our presentation has been limited to the theoretical side, however Quantum Key Distribution protocols are meant to be deployed and, in the last years, even commercialized. We will proceed by introducing different elements that characterize the challenges to be faced when implementing a QKD protocol in reality, as well as the possible attacks that can be carried out by an adversary.

3.3.1 Quantum channels

As outlined in section 3.1.1, in Quantum Key Distribution the quantum states exchanged are photons. For this reason, the quantum channels employed are optical fibers and free-space links.

Optical fibers

Optical fibers are waveguides that confine and guide light through total internal reflection. The fundamental structure of a fiber consists of a core, with refractive index n_1, surrounded by a cladding, with a refractive index n_2: the refractive indexes respect the crucial relation $n_1 < n_2$. Light entering the core at angles within the fiber's acceptance cone is trapped by repeated reflections at the core-cladding interface, allowing it to propagate over long distances with minimal loss.
In *single-mode fibers*, only the fundamental transverse mode can propagate, which drastically reduces modal dispersion and enables high-bandwidth transmission. In contrast, *multi-mode fibers* allow multiple spatial modes, which increases intermodal dispersion and limits the effective transmission distance. The criterion to distinguish single-mode fibers from multi-mode fibers is the size of the core: a larger core implies the capacity of containing more spatial modes. Typically, the diameter of the core of multi-mode fibers is in the order of hundreds of micrometers, while single-mode fibers have a diameter that is tens of micrometers.

Losses in optical fibers grow exponentially with the distance. From this it follows that the transmittance decreases exponentially with the distance according to:

$$T = 10^{-\frac{\alpha d}{10}} \tag{3.22}$$

The attenuation coefficient α depends on the wavelength and on optical fibers also exhibit characteristic *attenuation windows*, defined as wavelength regions where scattering and absorption are minimal. Common windows include the O-band (1260-1360 nm), the C-band (1530-1565 nm), and the L-band (1565-1625 nm), with standard silica single-mode fibers exhibiting losses below 0.4 dB/km in the C-band.

Among the main advantages of using optical fibers, we must stress the fact that over the last decades there has been an intensive development and research in this field due to their use in classical telecommunications. For this reason, the expertise in this field is remarkable, as well as the widely spread deployment, leading to the opportunity to use the already existing telecommunication infrastructure to implement QKD links.

Free-Space

An alternative to optical fiber transmission is represented by *free-space* quantum channels, in which photons propagate through the atmosphere or in outer space without the guidance of a fiber. In this scenario, the "waveguide" is simply the free-space path between the transmitter and receiver.
Unlike fiber attenuation, which increases exponentially with distance, free-space attenuation is dominated by geometric spreading and atmospheric turbulence, with weather conditions (fog, clouds, rain) having a strong impact on performance.
A remarkable advantage of free-space channels is that, once the signal leaves the atmosphere (as in satellite links), the losses are drastically reduced because propagation occurs in vacuum, where attenuation is negligible. This is the reason why satellite-based QKD is currently considered the most promising solution for intercontinental quantum communication. In this case, satellites can operate as trusted nodes, as repeaters, or even as entanglement sources linking distant ground stations. From a technological point of view, free-space and satellite QKD benefit from decades of development in space optics, pointing and tracking systems, and satellite communications. A significant example is the Micius satellite mission, where Chinese researchers demonstrated QKD over more than 1000 km between ground stations, as reported in [44]. This achievement highlights the feasibility of integrating free-space quantum channels into a global quantum network.

3.3.2 PLOB bound

In the quantum channel, it is never possible to use classical repeaters. This is a rather strong and sharp statement that can be easily justified by considering the BB84 setup. If a technology analogous to classical repeaters (the ones used in telecommunications) existed, the idea of the BB84 would not make any sense. A repeater is a device that receives a signal, eventually amplifies it, and retransmits it. However, the No-Cloning theorem prevents a similar procedure: in fact, an eavesdropper could use the same technology to get the signal generated by the source and retransmit a copy of it to the receiver without being detected.

The fact that there is not the equivalent of classical repeaters for quantum channels represents a major concern. The reason is that, for example, losses in optical fibers increase exponentially with the distance, and therefore the transmittance T exponentially decreases with the distance, significantly limiting the range of QKD.

In 2017, the following fundamental result was presented:

Theorem 3.3 (PLOB bound [45])**.** *The secret key rate r of any repeaterless QKD protocol in a channel with transmittance T is upper bounded by:*

$$r \leq -\log_2(1-T) \tag{3.23}$$

In case of high losses regimes (i.e. $T \approx 0$), it becomes:

$$r \approx 1.44T \tag{3.24}$$

Since $0 \leq T \leq 1$, it is possible to see that it is always possible to achieve a positive key rate r regardless of how low the transmittance is (and therefore regardless of the distance). Nonetheless, maximal achievable distances are considered in case of noise in the channel.

The PLOB bound has become a fundamental benchmark for repeaterless, fiber-based QKD, as it represents the ultimate limit for secret key generation over a lossy quantum channel without trusted intermediate nodes. Approaching, achieving, or even surpassing this bound through innovative techniques has become one of the main drivers of research in fiber-based QKD. This includes the development of novel protocols (see chapter 4) and the design of advanced experimental setups optimized for ultra-low loss and noise resilience. In this context, the achievable communication distance has become a defining performance metric for quantum key distribution systems deployed over optical fiber networks.

At the start of this paragraph we highlighted how the No-Cloning theorem is the reason behind the impossibility of using classical repeaters. However, more than twenty-five years ago, a first proposal for a *quantum* repeater was presented [46], and, nowadays, it is an open research field. Briefly, the main idea is to use an intermediate node C to swap the entanglement between the two distant nodes A and B. This is possible thanks to the use of quantum memories together with a Bell state measurement in C (that actually swaps the entanglement). Among the most relevant experimental realizations, we mention [47] and [48]. However, this technology does not have the required maturity to be used in modern and advanced realizations of QKD systems (for example, it is not efficient enough to tolerate the transmission rates achieved by QKD).

3.3.3 Attacks

Besides the well-known *Intercept-and-Resend* attack, presented in section 3.1.1, several other threats against QKD protocols have been developed over the years. We outline some of them in the following.

Direct Attacks

Attacks can be broadly classified into three categories: *individual*, *collective*, and *coherent* attacks. In *individual attacks*, Eve interacts with and measures each quantum signal independently, without using quantum memory to store the states. These are the easiest to implement technologically but are also the least powerful.

In *collective attacks*, Eve applies the same interaction to each signal, but instead of measuring immediately, she stores her quantum states in a quantum memory. Once the classical post-processing phase begins and basis information is revealed, she can measure all her states, independently and optimally. This increases her information gain compared to individual attacks, though it requires more advanced technology, such as long-term quantum memories.

Finally, in *coherent attacks*, Eve does not restrict herself to independent interactions: she performs an arbitrary joint quantum operation on all intercepted signals and can store the resulting states until after basis reconciliation. Coherent attacks are the most powerful in theory but also the most technologically demanding. All three of these attack types target the quantum states directly, and their practical feasibility is currently limited by the immaturity of quantum memory and large-scale quantum processing technologies.

Side-Channel Attacks

A QKD system can also be targeted ‘‘indirectly’’, via the so-called *side channels*. These attacks exploit imperfections in the physical implementation rather than the fundamental principles of quantum mechanics.

One prominent example is the *Photon-Number Splitting (PNS)* attack. Since generating perfect single-photon states is technologically challenging, many systems use attenuated laser pulses. These sometimes contain more than one photon. If Eve detects a multi-photon pulse, she can split off one photon and forward the others losslessly to Bob. By storing her photon in a quantum memory and measuring it after basis reconciliation, she can obtain the corresponding bit without introducing detectable errors. This vulnerability led to the development of the *decoy-state* method [49], now widely used, whose aim is to use random intensities to detect

PNS attacks.

Several side-channel attacks specifically target the receiver. A typical single-photon receiver uses a *SPAD* (Single-Photon Avalanche Diode) operating in Geiger mode: upon absorbing a photon, it triggers an avalanche of charge carriers that generates a detectable current. If forced into *linear mode* (as in a classical photodiode), the SPAD loses single-photon sensitivity.

In the *blinding attack* [50], Eve sends intense continuous light to the receiver, forcing SPADs into linear mode. She can then send carefully timed bright pulses so that only the detector corresponding to her chosen bit value clicks, effectively dictating Bob's outcomes without raising the quantum bit error rate (QBER).

The *double-click attack* [51] exploits events where both detectors in a measurement basis click simultaneously, which some QKD implementations resolve by assigning a random bit value. By influencing the frequency and timing of double-click events, Eve can bias the randomization process and gain information.

In the *dead-time attack*, Eve exploits the period after a detection during which a SPAD is recovering and cannot register new photons. By sending bright pulses to trigger detections at specific times, she can selectively disable detectors, effectively controlling which ones are active and influencing Bob's measurement results.

Other side-channel strategies target the transmitter rather than the receiver. In these cases, Eve exploits correlations between the prepared quantum states and unintended physical signatures of the source.

One common example is the *Trojan-Horse attack* [52], where Eve injects bright light into Alice's apparatus through the quantum channel. A fraction of this light can be reflected back from internal optical components, such as phase or polarization modulators, carrying information about Alice's encoding settings. If no adequate countermeasures (e.g., optical isolators) are in place, this leakage can reveal the raw key without introducing detectable errors.

Another well-studied case is the *phase-remapping attack* [53]. In phase-encoded QKD systems, modulators require a finite response time to apply the desired phase shift. By slightly adjusting the arrival time of the pulses at Alice's modulator, Eve can cause the applied phase to differ from the intended value, effectively remapping the encoding to a smaller and more distinguishable set of states, which she can then measure with higher accuracy.

Finally, in *wavelength-dependent attacks* [54], Eve exploits the fact that many optical components—such as beam splitters, modulators, and isolators—have wavelength-dependent behavior. By sending light at carefully chosen wavelengths outside the

nominal operating range, Eve can manipulate or probe Alice's internal components without being detected, for instance by changing beam splitter ratios or bypassing isolation.

4

Measurement-Device independent protocols

Referring to the last section of the previous chapter, the impossibility of using repeaters represents a major drawback when it comes to considering the achievable range of a QKD protocol. In addition to this, several side-channel attacks target the receiver side, representing therefore a significant concern for practical QKD implementations. In the following, we will present a groundbreaking protocol, called *Measurement-Device Independent* (MDI) protocol, whose aim is to solve the need to trust the receiver apparatus. Two possible upgrades are then considered, *Twin-Field* (TF), whose performances are able to overcome the PLOB bound, and *Aynchronous-Pairing* (AP). which achieves similar results of TF but avoiding some complex experimental bottlenecks, representing a promising and concrete candidate for practical QKD schemes.

4.1 Measurement-Device-independent QKD

In the canonical QKD assumptions, that we presented in section 3.1.3, there is the need for the devices used in the preparation and in the measurement phases to be trusted, *i.e.* not to be under the control of an adversary. Despite being a reasonable assumption, it is rather restrictive (due to the multitude of side-channel attacks targeting such devices). For this reason, researchers developed an ingenious protocol (see [36]) which could provide a secure key even if all the devices involved (both preparation and measurement devices) were under the control of an adversary: this family of protocols is known as *Device-Independent* (DI) protocol. Unfortunately,

this approach requires advanced technological requirements to be set up: in particular, there is the need to violate a Bell inequality with the devices that must be space-like separated (*i.e.* they cannot influence each other). As a consequence, the Measurement-Device Independent protocol relaxes the constraint on the preparation sources by trusting them, since most of the attacks target the receivers, and not the sources, yet achieving remarkable results. We will present it, referring to the first proposal (see [55]).

4.1.1 A protocol based on Bell basis measurement

In the setup of the MDI protocol (depicted in figure 4.1), both Alice and Bob work as transmitters, while the measurements are performed by a third entity, *Charlie*, that might be under the control of an adversary.

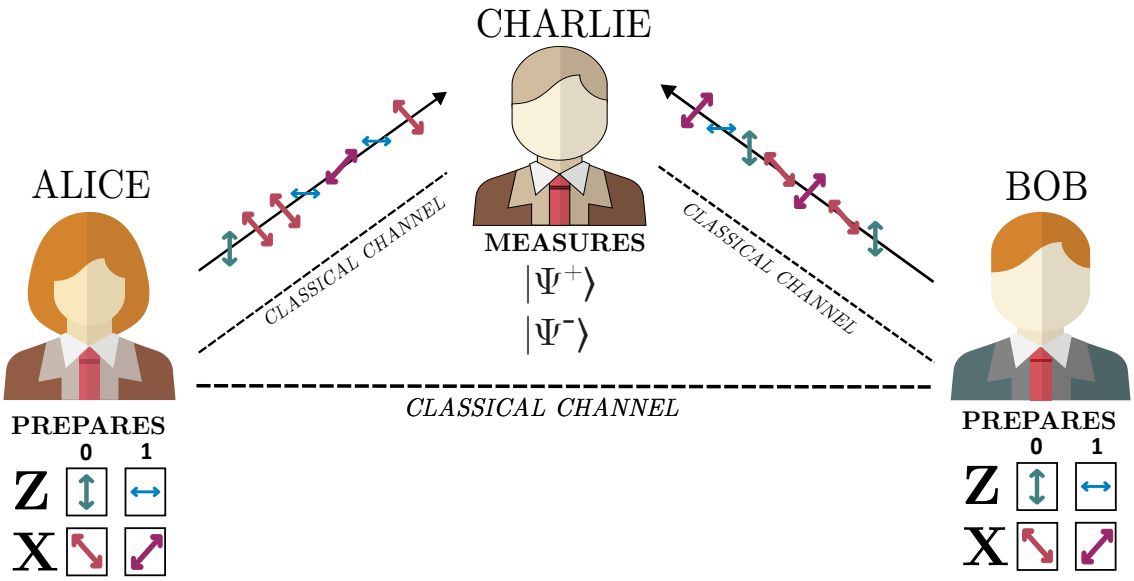

Figure 4.1: The setup of the MDI protocol, where Alice and Bob are both transmitters and Charlie is the receiver, who performs a Bell measurement.

The preparation phase is similar to the one of BB84, as Alice and Bob are randomly preparing four quantum states by choosing between the $\mathbb{Z} = \{|H\rangle, |V\rangle\}$ basis and the $\mathbb{X} = \{|A\rangle, |D\rangle\}$ basis. Subsequently, they send their states to the measurement station, which performs a Bell state measurement, *i.e.* projects the two incoming state into one of the four Bell states $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$. In [55] there is an implementation proposal (shown in figure 4.2) that takes into account just $|\Psi^+\rangle$ and $|\Psi^-\rangle$, which does not affect the security of the protocol.

Let's examine how a Bell basis measurement works by using figure 4.2 as a reference. The quantum states coming from Alice and Bob interfere at a 50:50 beam-

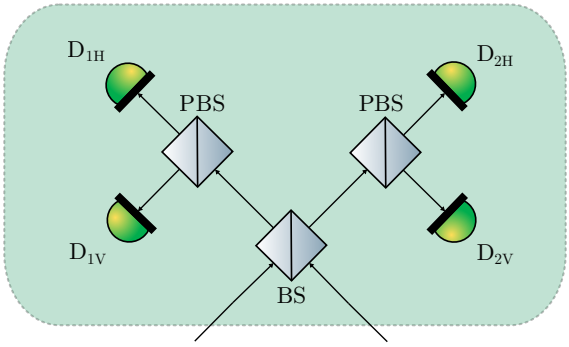

Figure 4.2: The realization of a Bell state measurement with optical components.

splitter, whose outputs are connected to two polarizing beam-splitters (they are a special kind of beam-splitters that split the light according to the polarization it has). At each output of the PBS there is a single photon detector, *i.e.* a device that is triggered whenever an incoming photon arrives. Given this setup, we consider that a detection is *successful* if two photons in orthogonal polarization are detected. In other words, if there is a click of D_{1H} *and* D_{2V} or D_{1V} *and* D_{2H} the outcome of the measurement is the Bell state $|\Psi^-\rangle$, if there is a click of D_{1H} *and* D_{1V} or D_{2V} *and* D_{2H} the outcome of the measurement is the Bell state $|\Psi^+\rangle$. To better justify the motivation behind the choice of the Bell state measurement, let's consider the joint state $|\psi\rangle_{AB} = |\phi\rangle_A |\phi\rangle_B$ that Charlie receives: it is known, since the Bell states constitute a basis for the Hilbert space, that it can be written as a linear combination of them. For example

$$|HV\rangle = \frac{1}{\sqrt{2}} \left(\left|\Psi^+\right\rangle + \left|\Psi^-\right\rangle \right) \tag{4.1}$$

Given the received state, a Bell measurement corresponds to a projection of the state into one of the Bell states, which are entangled states: therefore, a Bell state measurement can be seen as a post-selection entanglement creation. The motivation for creating entanglement is linked to the need to create a correlation between the states sent by Alice and Bob. Of course, by performing such measurement, Charlie cannot learn the polarization of the states received. Once the exchange is over, Charlie communicates over a public channel the outcomes of his measurements. Since the projective measurement is on the states $|\Psi\rangle^+$ and $|\Psi\rangle^-$, the outcome indicates *anticorrelation* between the states sent by Alice and Bob (*i.e.* they are one of the complementary of the other), except in the case in which Charlie's outcome is $|\Psi\rangle^-$ and Alice and Bob chose the $\mathbb{X}$ basis. For this reason, one of them has to perform a bit-flip, to have the same bit (except in the case described before: in that case there is already correlation and no bit flip is needed).

After the bit-flip operation, the post-processing phase is identical to the one of BB84, already presented in section 3.1.1.

A detailed security proof is contained in the supplementary material of [55]. However, let's consider informally the case in which Charlie is under the control of the adversary. If he tries to falsify or forge the outcomes of the Bell state measurement, Alice and Bob are able to detect his behaviour by observing an increase in the error. Therefore, in order not to be detected, the adversary needs to behave properly (*i.e.* he needs to perform a Bell state measurement and communicate the outcome to the users): in this case, the security proof ensures that it is possible to distill a secure key.

4.1.2 Advantages and drawbacks

Achievable distance and SKR

Let's recall the transmittance T of an optical fiber quantum channel, introduced in section 3.3.1:

$$T(d) = 10^{-\frac{\alpha d}{10}} \tag{4.2}$$

which respects $0 \leq T(d) \leq 1$. We can link it with the probability that a photon sent over the quantum channel reaches the receiver; therefore, assuming that the noise is independent of the distance, the secret key rate is proportional to the raw key rate, which is proportional to the distance. Let's now consider a standard Prepare-and-Measure BB84 optical fiber implementation, where the length of the quantum channel is d, and let's define the transmittance on the channel as $T(d)_{BB84}$. It is intuitive that, by employing an MDI setup or an Entanglement-Based BB84 setup with the central station positioned in the middle, the achievable distance doubles. However, the probability of receiving both using these two configurations is the product of the two transmittances:

$$T(d)_{BB84} \cdot T(d)_{BB84} = 10^{-\frac{2\alpha d}{10}} = T(2d)_{BB84} \tag{4.3}$$

that is exactly the transmittance we would be able to obtain with a BB84 Prepare-and-Measure setup with a $2d$ long quantum channel. Therefore, if on the one hand the fact that potentially doubling the distance represents a remarkable feature, on the other hand, the overall transmittance remains the same: this means that the secret key rate keeps scaling linearly with the transmittance. A pictorial representation is shown in figure 4.3.

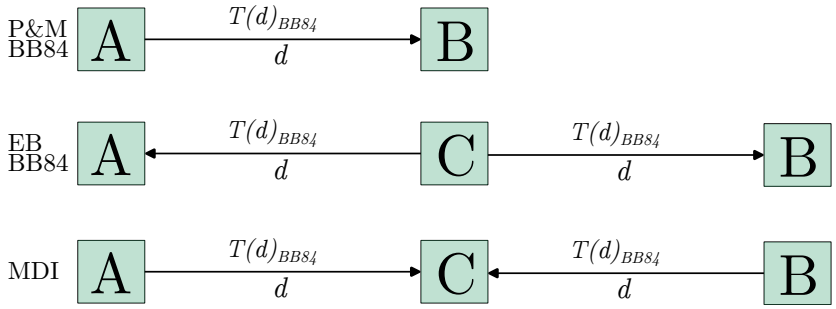

Figure 4.3: The comparison between the transmittance and the achievable distance for P&M BB84, EB BB84 and MDI protocols.

Simultaneous state arrival

The most significant drawback of MDI is represented by the need for the states sent by Alice and Bob to be identical in all their degrees of freedom (for example, they must have the same wavelength) when they arrive at the measurement station Charlie. Among these requirements, they need to arrive simultaneously: in fact, a Bell state measurement can be performed only if the states arrive exactly at the same time at the first BS. If this requirement is not satisfied, meaning that there is a temporal mismatch, the outcome is a mismatch.
This constraint represents a major obstacle to practical realizations, as it requires perfect synchronization from the two sources, as well as the knowledge of the length of the links.

4.1.3 Experimental realization

One of the first experimental realizations of the MDI protocol dates back to 2013, when researchers managed to achieve the generation of a secure key over a 50 km fiber link (see [56]). In this experiment, the time-bin encoding was used instead of using the polarization encoding. Moreover, the authors adopted the decoy states technique (that we introduced in section 3.3.3, as initially suggested in the original paper ([55]), and phase randomization for each pulse (to prevent an eavesdropper from inferring information about the encoding from the phase of the pulses). Nonetheless, we want to stress the remarkable complexity of the source required for the simultaneous arrival of the quantum states at the measurement site. In fact, the two sources share a 1 MHz common time reference to be synchronized, and they use pulses with 2 ns width generated from two different lasers. To achieve the simultaneous arrival of the two states, they monitor the arrival times of the pulses with an 80 GHz oscilloscope and they use an optical delay with < 10 ps resolution to calibrate the timing at one of the two sources. Their accuracy is guaranteed by the fact that the jitter of the pulses (≈ 10 ps) is smaller than the pulse width, and

because the overlap between the two pulses can be adjusted with a precision finer than the pulse width.

A significant advancement was made in 2014, when it was reached, over an optical fiber channel, the distance of 200 km (see [57]). This experiment shares most of the characteristics of the one described previously (time-bin encoding with phase-randomized decoy states), but it uses a time reference of 75 MHz (instead of 1 MHz). In addition to this, the synchronization part is even more complex, as two additional lasers (one per source) are used, together with a feedback control dependent on Charlie's measurement, allowing for the simultaneous arrival of the pulses. With a similar technique, in 2016 researchers were able to reach a record distance of 404 km (see [58]).

As mentioned in the previous section, the simultaneous arrival of the quantum states at the receiver, needed to perform the Bell basis measurement, represents an experimental challenge which decreases the feasibility of practical realizations.

4.2 Twin-Field

In 2018, a novel protocol, called *Twin-Field*, was proposed (see [59]). It took as inspiration the idea of the MDI to make interfere two quantum signals, sent from Alice and Bob, at the receiver's side, Charlie, which can be under the control of an adversary. The Twin-Field protocol maintains several characteristics of the MDI (for example, being measurement-device independent and using a central measurement station) but it achieves the remarkable result of guaranteeing a secret key rate that scales as the *square root* of the transmittance instead of proportional to the transmittance..

4.2.1 Interference

The idea for the setup of TF (depicted in figure 4.4) comes directly from the MDI protocol, in particular the fact that both Alice and Bob act as sources and they send their quantum states to a third entity, Charlie, that is untrusted. However, the measurement stage differs from MDI, since, if the phases of the two sources are coherent, at the intermediary station a first-order interference measurement is performed (unlike the MDI protocol, in which there is a second-order interference measurement).

In the preparation stage, Alice and Bob are generating coherent optical fields (to use the decoy states technique) with a randomized global phase, ρ_A and ρ_B, re-

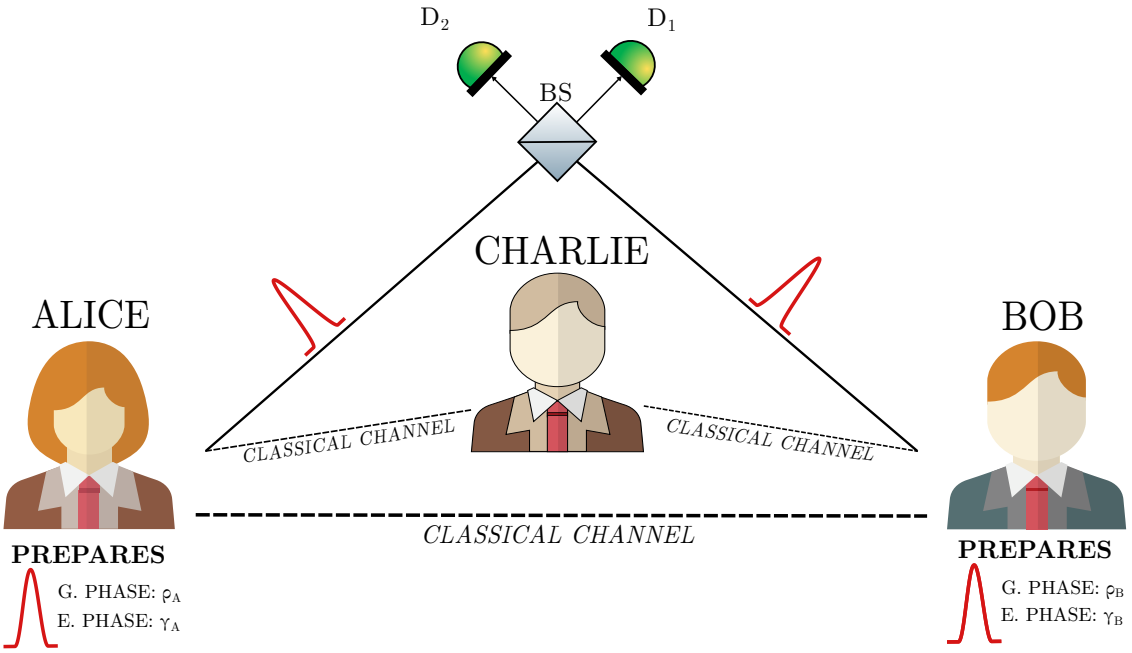

Figure 4.4: The setup of the Twin-Field protocol: Alice and Bob need to choose a global phase and an encoding phase before sending the states to Charlie, who performs an interferometric measurement.

spectively. As highlighted before, the phase randomization is necessary for security reasons. Of course, $\rho_A, \rho_B \in [0, 2\pi)$. Such interval can be divided into M slices $\Delta_k = \frac{2\pi}{k}$, with $k \in \{0, M-1\}$. In the sifting phase, Alice and Bob will also publish the slice of each state sent, keeping only the matching ones (*i.e.* when the global phases that they randomly chose are within the same slice). As mentioned in [59], the optimal number of slices is $M_{opt} = 16$. Subsequently, Alice and Bob apply to the optical field a second phase, the encoding phase γ. This corresponds to selecting the polarization of a state (in the case of a qubit, changing its polarization is exactly applying a phase to it, which corresponds to a rotation of the qubit in the Bloch sphere). We need four states to be encoded, therefore $\gamma_A = \gamma_B = \{0, \frac{\pi}{2}, \pi, \frac{3}{2}\pi\}$.

At this point, Alice and Bob send the prepared states over the quantum channel, directed towards Charlie. The link between Alice and Charlie, as well as the one between Bob and Charlie, can be seen as the arm of an interferometer. The reason is that Charlie, when he receives the two quantum states, performs an interferometric measurement with a beam-splitter. At this point the *relative phase* $\gamma_A - \gamma_B$ is crucial (remember that we are keeping only the fields with the same global phase, therefore $|\phi_A - \phi_B| \approx 0$, with an error up to $\frac{2\pi}{M}$). In fact, we can individuate two cases:

1. $|\gamma_A - \gamma_B| = 0$: Alice and Bob chose the same state.
2. $|\gamma_A - \gamma_B| = \pi$: Alice and Bob chose the same basis but opposite states.

This consideration is useful when we consider the outcome of an interferometric measurement: if we place at the output ports of the beam-splitter two detectors, one will click when the first case happens ($|\gamma_A - \gamma_B| = 0$), while the other one in the second case ($|\gamma_A - \gamma_B| = \pi$). As remarked earlier, we highlight that this measurement (a first-order interference measurement) does not need a coincidence at the receiver's side, but just a click.

After the measurements, Charlie communicates over the public channel which detector clicked at each round and Alice and Bob share the bases they used, making it possible for them to get the key. In fact, if they chose the same state, then the bit in the raw key will be a 0, if they chose the opposite state (obviously within the same basis), the raw bit will be 1. It is worth mentioning that the cases in which they choose different bases are not taken into account (*i.e.* $|\gamma_A - \gamma_B| = \frac{\pi}{2}$ or $|\gamma_A - \gamma_B| = \frac{3\pi}{2}$), exactly like in the standard BB84. However, there is the need for a second basis (otherwise an eavesdropper could easily perform an *Intercept-and-Resend* attack by measuring always in that basis).

4.2.2 Overcoming the PLOB bound

With respect to the MDI protocol, the Twin-Field protocol relaxes the constraint on the simultaneity at the receiver's side, but it requires an additional condition, that is the phase-locking and the phase-tracking of the optical fields in the two arms of the interferometer (it will be analyzed in section 4.2.3). Despite the arguably complex requirements, Twin-Field represents an exceptional advancement in the domain of QKD protocols as it is able to overcome the PLOB bound. In this section, we will provide an informal proof, following the treatment given in the Supplementary Information material of [59].

Transmittance and SKR

The Twin-Field protocol is able to overcome the PLOB bound thanks to the fact that its secret key rate scales as the *square root* of the transmittance (note that in all the protocols presented so far, it scaled linearly with the transmittance, as mentioned in section 4.1.2). This is a counter-intuitive result, as the PLOB bound represents a fundamental limit for the distance achievable by repeaterless quantum communications. However, if we consider the behavior of the intermediary node, we notice that it acts as a quantum repeater, thus allowing for an extended range.

This result can be extrapolated from the security proof of Twin-Field, in which

the secret key rate is derived in an analytical form. The proof is not immediate and involves several steps: in the following, we will highlight informally the main ideas.

The authors use the ingenious strategy of reducing the setup of Twin-Field to a BB84-like setup in order to adapt the security tools and proofs already developed for BB84. Of course, a complete analogy with BB84 is not possible, as in TF the measurement device cannot be trusted. Moreover, as we mentioned during the presentation of the protocol, Alice and Bob share additional information in the post-processing steps, in particular the random global phase they applied to each state; actually, according to the original protocol, they share only the slice containing the global phase, but it is intuitive that, if it is possible to derive a security proof by considering that the eavesdropper knows the precise global phase, it means that disclosing less information (*i.e.* only the slice) will not affect the overall security.

The security proof then takes into account a realization of the protocol in which there is a single source of light that generates a single photon (*i.e.* the Fock state $|1\rangle$) that impinges into a beam -splitter: each output of the BS is connected to the arm of the interferometer. The single-photon source is inaccessible to Eve (since also in TF the sources are considered to be trusted), and the only information she has access to is the difference between the two random global phases $\rho_{AB} = \rho_A - \rho_B$, as it is disclosed in the post-processing. When a single photon impinges in a BS (that they suppose to be 50:50), the joint state of the two outputs is the Bell state $|\Psi^+\rangle$.
If we take into consideration also the encoding phase that Alice and Bob add, the phase applied to the global state will be the *difference* of the two phases. Since all the events in which Alice and Bob choose the same basis are kept, the difference of their phases is either 0 or π, leading to the fact that the joint state available to Eve will be either $|\Psi^+\rangle$ or $|\Psi^-\rangle$. In other words, the security is granted by reducing the setup to a BB84-like scenario and exploiting the entanglement properties to guarantee that the maximal information that Eve can gain regards the correlation between the bits encoded, but not the bits themselves. Fig. 4.5 provides a visual representation of this first part of the security proof.

The proof continues by showing that the security holds also for the actual schemes (and not just for the BB84-like one), removing also the hypothesis of having single photon sources and detectors by taking into account that the transmitter uses weak coherent pulses. Finally, the SKR achieved is (Eq. 3 of [59]):

$$R^{(\neg\rho)}_{\text{TF-QKD}}(\mu, L) = \frac{d}{M}\left[R_{\text{QKD}}\left(\mu, \frac{L}{2}\right)\right]_{\oplus E_M} \tag{4.4}$$

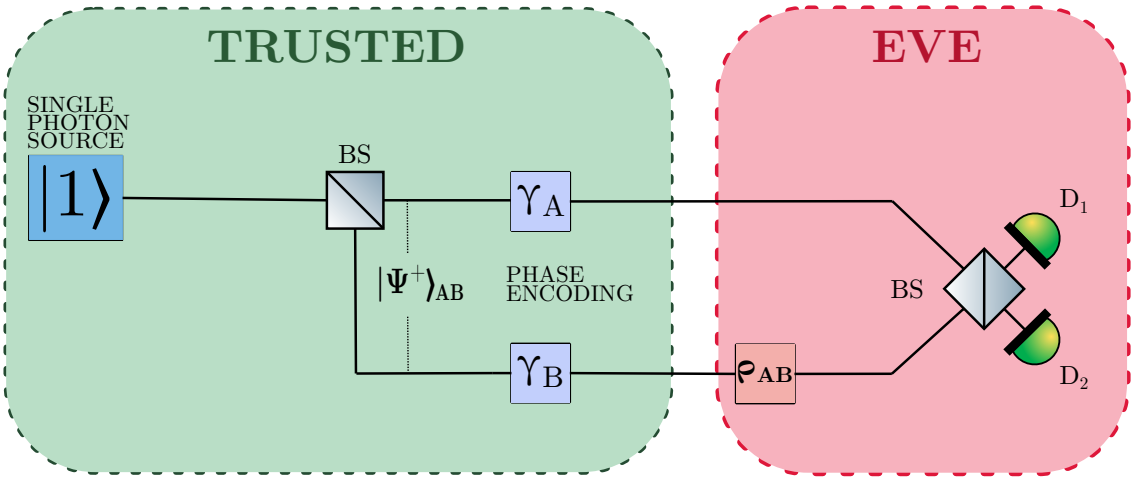

Figure 4.5: The reduction of the TF protocol to a BB84-like setup. The generation of single-photon states and the polarization encoding is considered to be trusted. We assume that Eve controls the measurement site and knows the global phases ρ_{AB}.

If the revelation of the global phases does not bear any meaningful information (represented by $(\neg\rho)$), the key rate of the Twin-Field protocol $R_{\text{TF-QKD}}(\mu, L)$ over a distance L is proportional to the key rate of any other QKD protocol $R_{\text{QKD}}\left(\mu, \frac{L}{2}\right)$ over a distance $\frac{L}{2}$: recalling the relation between the secret key rate and the transmittance, we can say that the SKR of TF scales as the square root of the transmittance. In equation 4.4, with μ we indicate the sum of the intensities of the pulses sent by Alice and Bob, M the number of slices used, d the duty cycle between classical and quantum modalities and $\oplus E_M$ the additional error in the QBER due to phase randomization. As a consequence, it can be proven that the PLOB bound can be overcome, as shown in figure 4.6 (taken from [59]).

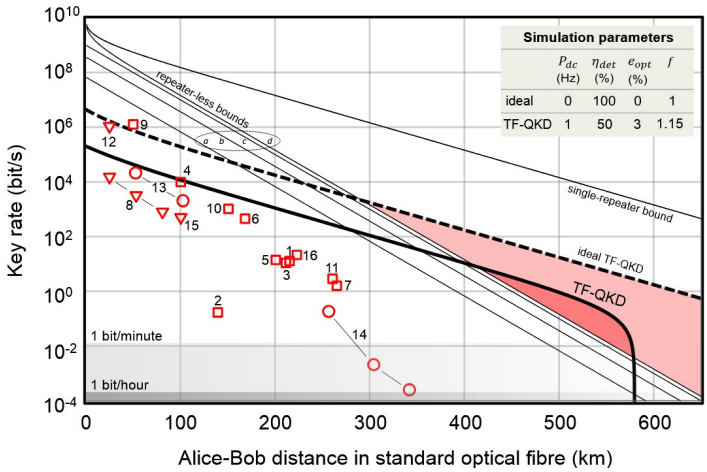

Figure 4.6: Both the ideal version and the realistic versions of TF are able to overcome the repeaterless bounds a (for decoy states MDI), b (for decoy states BB84), c (for standard BB84) and d (secret key capacity).

4.2.3 Phase-locking and phase-tracking

One of the main challenges of the Twin-Field protocol is requiring that, after Alice and Bob apply the respective random phase, the relative phase between the pulses sent must be constant over time: the two optical fields that are traveling in the arms of the interferometer need to be phase-locked. From the experimental point of view, however, it represents a rather complex challenge, especially in the case of transmission over long distances.

Let's consider the experiment described in [60], in which researchers were able to reach the record distance of 1000 km for a QKD exchange over optical fibers.

In the setup, there are two lasers λ_1 and λ_2 at the receiver's side that are locked to an ultrastable cavity using the PDH (Pound-Drever-Hall, see [61, 62]) technique, obtaining an extremely narrow linewidth (in the order of Hz). The two lasers are then combined in a beam-splitter and sent to Alice and Bob.

Alice (Bob) receives the light and demultiplexes it through a DWDM (Dense Wavelength Division Multiplexing) filter. Alice modulates λ_1 with 400 ps pulses in each 1 μs period to get a strong phase reference that is needed to track the phase and prevent it from drifting over long distances. Alice and Bob use as a reference λ_2 (by using an optical phase-locked loop) to generate the quantum signals (this procedure is known as *phase locking).*

The idea of using two different wavelengths for the phase locking and phase tracking was introduced in [63] to prevent Rayleigh scattering over long distance fiber communications. The complexity needed to maintain the phase locked and tracked represents an obstacle for practical realization of long-range QKD systems.

4.3 Asynchronous-Pairing

In the first two sections of this chapter we presented two advanced approaches to QKD that overcome what are, arguably, the major drawbacks of Quantum Key Distribution: the need to trust the measurement device and the difficulty to reach long distance communications due to the impossibility to use repeaters. However, both these schemes, MDI and TF, are extremely complex to implement from the experimental point of view, therefore preventing their use in a possible practical, everyday use of QKD.

In 2022, two research teams proposed independently a third approach that overcomes some drawbacks of the previous two, *i.e.* the need for the simultaneous arrival of quantum states at the receiver (that requires perfect synchronization between the sources) and the phase-locking and phase tracking requirements (highly

complex from the experimental point of view over hundreds of kilometers distances).

4.3.1 Post-measurement interference

The two articles that paved the way for Post-Measurement Pairing QKD come from the Nanjing University researchers ([64]) and from the team of Tsinghua University ([65]). We will present the protocol proposed by the former, called Asynchronous-Pairing QKD (while the latter was named Mode-Pairing QKD).

Let's start by mentioning the two main ideas, advanced by the authors, that served as a starting point for the AP-QKD. Recalling the section 4.1.2, it is easy to understand that the secret key rate of the MDI protocol scales linearly with the transmittance only because there is the need that *both* quantum states arrive at the receiver simultaneously: the probability of this event happening is the product of the probability that each quantum state arrives at the receiver, *i.e.* the product of the transmittance of the two channels. The *adaptive* MDI protocol ([66]) contains an ingenious solution: Alice and Bob send m quantum states in m different channels, simultaneously; Charlie verifies the presence of a quantum state in each channel, that depends on the transmittance and can be certified by a quantum non-demolition measurement (*i.e.* quantum measurement that preserves the state from collapsing, see [67]), and finally links through optical switches Alice's and Bob's channels that actually contain the states, leading to the Bell state measurement. As argued in [66], if m is larger than the inverse of the transmittance of the optical channel, one or more photons arrive at Charlie with high probability, making the key rate scale as the square root of the transmittance. This idea will be crucial in AP-QKD as it introduces the intuition of post-selecting the quantum states.
The second idea is to use time-multiplexing, introduced in [68], that is sending pairs of pulses (from both the senders) and considering their time-arrival window.
Briefly speaking, AP-QKD translates the idea of space multiplexing into time multiplexing, requiring only one optical channel per transmitter and performing the matching part in the post-processing, instead of actively doing it with optical components. In the following, we present a detailed explanation of the protocol proposed in [64].

Protocol description

The result of the merge of the two previous ideas is the preparation of a series of pulses over time. In particular, let's consider having N time bins: for each time bin $i \in \{1, ..., N\}$ Alice (Bob) randomly chooses a global phase θ_A^i (θ_B^i) and a bit value $b_A^i = \{0, \pi\}$ ($b_B^i = \{0, \pi\}$). Then, she (he) chooses an intensity k_A^i (k_B^i) with probability $p_{k_A}^i$ ($p_{k_B}^i$) where $k_A = \{\mu_A, \nu_A, \mathbf{0}_A, \hat{\mathbf{0}}_A\}$ ($k_B = \{\mu_B, \nu_B, \mathbf{0}_B, \hat{\mathbf{0}}_B\}$)[1]. These intensities are linked to the use of decoy states. With these parameters, Alice (Bob) prepares the weak coherent pulse $e^{(\theta_A^i + b_A^i \pi)} \left|\sqrt{k_A^i}\right\rangle$ ($e^{(\theta_B^i + b_B^i \pi)} \left|\sqrt{k_B^i}\right\rangle$) and sends it to Charlie.

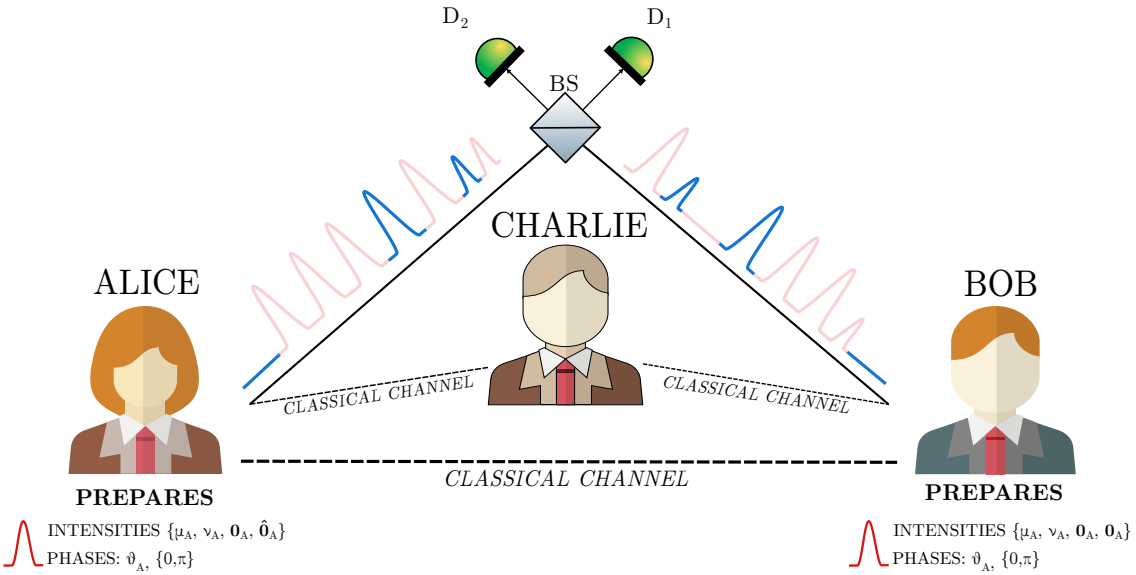

Figure 4.7: The setup for AP-QKD. Alice and Bob choose intensities and phases and the send a train of pulses to Charlie. Only the events that give interference (showed in blue) are kept.

For each time bin i, the receiver measures the interference of the two signals; the events that are considered meaningful are only single clicks (double-click events and no-click events are discarded). In fact, in AP-QKD the measurement performed is a second-order interferometric measurement (like in MDI).
Following the notation in [64], we define with $\{k_A, k_B\}$ a successful detection event: in this case, Charlie communicates which of his two detectors clicked.

At this point, we introduce the temporal pairing window T_c and we differentiate between two cases (depicted in fig. 4.8):

[1]They need to satisfy $\mu > \nu > \mathbf{0} = \hat{\mathbf{0}} = \mathbf{0}$. The last two values are called *preserve* and *declare* vacuum respectively. The first one is used as a decoy level to compose the raw key, the second one to estimate errors related to the vacuum. Moreover, we will refer to μ as *signal* and to ν as *decoy*.

- *case-1*: given a successful detection at time t, it is possible to find at least another successful event in the interval $[t - T_c, t + T_c]$
- *case-2*: given a successful event at time t, there is no other successful detection in the temporal window $[t - T_c, t + T_c]$.

This distinction is fundamental if we relate it to the fact that, in AP-QKD, phase tracking and phase locking are not employed: the idea, explained formally in the next section, is that, if two pulses arrive within a small time interval, their relative phase drifts are low enough not to compromise the QBER significantly. On the other hand, nothing can be said about case-2 events, in which basically the lack of another signal as a reference for the phase makes it impossible to keep track of it. Authors suggest discarding these events as long as the occurrences are under a preset threshold Λ (preset before the realization of the exchange): if not, Alice and Bob should abort and restart the protocol.

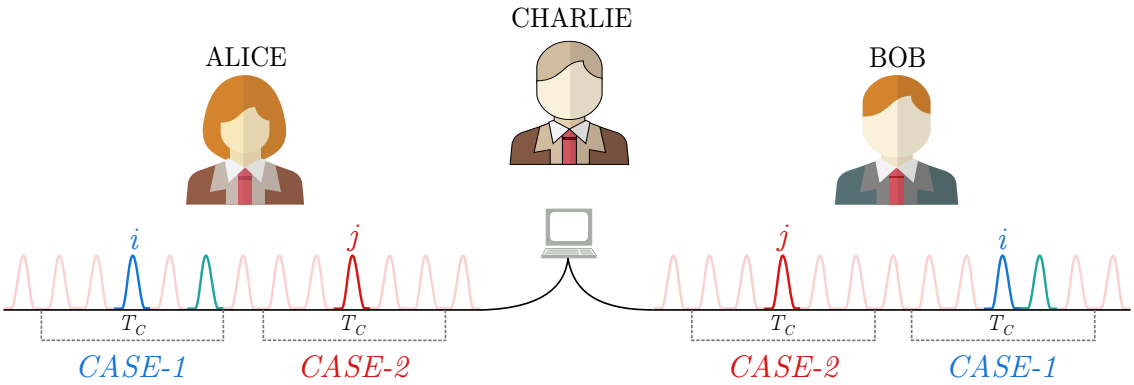

Figure 4.8: The visual representation of the two cases in AP-QKD: in the time-bin i (in blue) we have a successful detection and a case-1: for both Alice and Bob there is another successful detection within the time window T_C. The detection of the time bin j (in red) is a case-2 event, as it is the only successful detection in the time window T_C

The core of the AP-QKD protocol lies in the post-processing stage, since the bit encoding of the raw key is performed *after* the measurement phase. Let's consider case-1 events in which Alice and Bob have chosen either a decoy state (ν) or a declared vacuum state ($\hat{\mathbf{0}}$): in these cases, they publicly announce both the intensities and the phases over the authenticated public channel, and the corresponding data are excluded from key generation. The candidate data for the $\mathbb{Z}$ basis are therefore those not publicly announced, namely

$$\{\mu_A, \mu_B\}, \quad \{\mu_A, \mathbf{0}_B\}, \quad \{\mathbf{0}_A, \mu_B\}, \quad \{\mathbf{0}_A, \mathbf{0}_B\}$$

Alice processes her signals by attempting, for each pair of time bins (i, j), to match a signal pulse μ_A^i with a vacuum $\mathbf{0}_A^j$. If a match is found, she sets her raw

bit to 0 if $i < j$ and to 1 if $i > j$; if no such pairing exists, the event is discarded. She then communicates the indices (i, j) to Bob. Upon receiving this information, Bob compares his own intensity choices k_B^i, k_B^j: if $k_B^i = k_B^j$, he publicly announces this and discards the event; otherwise, he assigns his bit according to

$$0 \quad \text{if } (k_B^i, k_B^j) = (\mu_B, \mathbf{0}_B), \qquad 1 \quad \text{if } (k_B^i, k_B^j) = (\mathbf{0}_B, \mu_B).$$

As a result, the only events that contribute to the raw $\mathbb{Z}$-basis key are

$$\begin{aligned}
&\{\mu_A^i \mathbf{0}_A^j,\ \mu_B^i \mathbf{0}_B^j\} \\
&\{\mu_A^i \mathbf{0}_A^j,\ \mathbf{0}_B^i \mu_B^j\} \\
&\{\mathbf{0}_A^i \mu_A^j,\ \mu_B^i \mathbf{0}_B^j\} \\
&\{\mathbf{0}_A^i \mu_A^j,\ \mathbf{0}_B^i \mu_B^j\}
\end{aligned}$$

which constitute the meaningful $\mathbb{Z}$-basis contributions to the raw key prior to error correction and privacy amplification.

All the events that have been publicly communicated through the channel, *i.e.* those involving detection of states with ν or $\hat{\mathbf{0}}$ intensities, are used to provide an estimate of the phase error, which is a crucial step since AP-QKD avoids phase-locking and phase-tracking. In particular, they use the information about the global phase difference $|\varphi^i - \varphi^j|$ between two time bins. This procedure is presented in detail in [64].

Finally, following the finite-key security analysis for MDI-QKD ([69]), the authors show that the length of the final key is given by

$$l = \lfloor s_{0,\mu_B}^Z \rfloor + \lfloor s_{11}^z \rfloor (1 - h_2(\lceil \phi_{11}^z \rceil) - \lambda_{EC} - \Delta \tag{4.5}$$

The first term, s_{0,μ_B}^Z, accounts for the secure contribution of vacuum-signal events (Alice sends a vacuum while Bob sends a signal), which can be estimated via decoy-state analysis and safely bounded from below.
The second term, $s_{11}^Z(1 - h_2(\phi_{11}^Z))$, represents the contribution of single–single photon events: here s_{11}^Z is the lower bound on the number of detections when both Alice and Bob emit single photons, obtained from decoy-state statistics, while ϕ_{11}^Z is the corresponding phase error rate, inferred from $\mathbb{X}$-basis measurements and bounded from above. The factor $1 - h_2(\phi_{11}^Z)$ quantifies the fraction of extractable secrecy from these events after accounting for phase errors.

The third term, λ_{EC}, denotes the information leakage during error correction, typically estimated as $\lambda_{EC} = f\, n_Z\, h_2(Q_Z)$ where n_Z is the number of sifted $\mathbb{Z}$-basis bits, Q_Z the observed error rate, and $f \leq 1$ the error correction efficiency (it is greater than 1 because the error correction codes do not achieve the Shannon bound, meaning that they are less performant).
Finally, Δ collects the finite-size corrections, ensuring that the key length remains secure despite the use of finite data blocks.

We want to highlight that the raw key rate heavily depends on the pairing rate, *i.e.* the average number of pairs generated per pulse. Referring to the Mode-Pairing protocol, which is similar to the AP-QKD in the pairing technique, as it uses a pairing window (determined by a certain number of pulses) instead of a time window, it is possible to link the pairing window length to the pairing rate. In particular, as the authors highlight in equation 5 of [65], in an ideal case (*i.e.* a pairing window with infinite length), the pairing rate (and therefore the raw key rate) scales as the square root of the transmittance of the quantum channel, matching the performance of the TF protocol. If, on the other hand, the smallest possible pairing window is considered (*i.e.* a window of unitary length), equation 6 shows that the pairing and raw key rates scale as the transmittance of the channel: this result is expected, since using a pairing window of unitary length corresponds to implementing the time-bin MDI protocol, whose key rate scales linearly with the transmittance.

4.3.2 How to avoid phase-locking and phase-tracking

As mentioned earlier, the most remarkable characteristic of AP-QKD is to propose a solution to the most concerning issue, at least from the experimental point of view, of TF-QKD: the phase locking of two remote lasers. We will follow Section III of [64] to show that the use of a (small) temporal window is the way to avoid controlling the phase.

Let's start by recalling the global phase difference between two time bins $|\varphi^i - \varphi^j|$, where φ^i is defined as:

$$\varphi^i = \theta_A^i - \theta_B^i - \phi^i \tag{4.6}$$

The global phase difference of a time bin is the difference between the phases chosen in the preparation step by Alice and Bob ($\theta_A^i - \theta_B^i$) minus the term $\phi^i = \phi_A^i - \phi_B^i$, which considers the evolution of the phase between the transmitters and the receiver. At the receiver's side, $\phi^i = 2\pi\upsilon(t^i - l^i/s)$, where υ is the frequency of the

laser employed, t^i is the temporal index of the time bin i, l^i is the length of the fiber between the source and transmitter, and s is the velocity of light in the fiber. Following this definition, the difference $\phi_A^i - \phi_B^i$ can be expressed as:

$$\phi^i = \phi_A^i - \phi_B^i = 2\pi\delta\upsilon^i t^i - \frac{2\pi}{s}(\delta\upsilon^i l^i - \upsilon^i \delta l^i) \tag{4.7}$$

where $\upsilon^i = (\upsilon_A^i + \upsilon_B^i)/2$, $l^i = (l_A^i - l_B^i)/2$, $\delta\upsilon^i = \upsilon_A^i - \upsilon_B^i$ and $\delta l^i = l_A^i - l_B^i$. The same equation can be obtained for the time bin j. The key idea of AP-QKD is to guarantee phase correlation by considering pulses that are close in temporal terms rather than applying an active phase control. The price paid is a small increase in the QBER.

Let's now suppose that phase-locking is used to prove that there is no need for phase-tracking. In this case, $\delta\upsilon = 0$ since $\upsilon_A^{i(j)} = \upsilon_B^{i(j)} = \upsilon^{i(j)}$. Therefore $\phi^j - \phi^i = (\phi_A^j - \phi_B^j) - (\phi_A^i - \phi_B^i)$ becomes:

$$\phi^j - \phi^i = (\phi_A^j - \phi_B^j) - (\phi_A^i - \phi_B^i) = \frac{2\pi}{s}(\upsilon^j \delta l^j - \upsilon^i \delta l^i) \tag{4.8}$$

As claimed by the authors of [64], if T_c is in the order of tens of microseconds, the dominant term in equation 4.8 is the drift due to the length of the fiber, which has been estimated to be 0.4 rad per 50 μs (the drift of commercially available narrow-band lasers is small, within such a time window). This drift is causing a $\approx 1\%$ error in the interference, allowing the execution of the protocol without a phase-tracking technique. Notably, one may be concerned by the fact that, by choosing a small time window, the amount of events useful for post-processing (*i.e* case-1 events) is not enough: the authors claim that with an average intensity of $\bar{\mu} = 0.5$, a frequency of 1 GHz over 400 km of ultralow loss fibers and transmittance of the channel 70% there are ≈ 9.3 detections per window, which are sufficient for the correct execution of the protocol.

By considering an even smaller T_c (in the order of few tens of microseconds), the difference of the phases is due to the difference of the independent lasers of Alice and Bob. We can express this difference as:

$$\phi^j - \phi^i = 2\pi\delta\upsilon(t^j - t^i) \tag{4.9}$$

If $\upsilon = 100$ kHz, with $T_c = 1$ μs it is possible to obtain $\phi^j - \phi^i \approx 0.1\pi$, which corresponds to an interference error rate of 2.4%. To keep the frequency difference $\delta\nu$ small without resorting to active phase-locking, the authors propose periodic cal-

ibrations rather than continuous feedback. Two practical methods are suggested: the first one is a beat-note measurement between Alice's and Bob's lasers, adjusting their temperatures to minimize $\delta\nu$; the second one a Hong–Ou–Mandel–based feedback approach, as used in time-bin MDI-QKD, exploiting interference visibility as an alignment signal. Experimental measurements with commercial NKT and RIO lasers show average frequency offsets of ~ 145 kHz and ~ 92.5 kHz, which can be further reduced to $\lesssim 100$ kHz via occasional adjustments. Simulations of the bit error rate in the $\mathbb{X}$ basis as a function of the matching window T_c reveal that errors grow with both $\delta\nu$ and T_c, motivating choices such as $T_c = 1$–20 μs and $\delta\nu \lesssim 100$ kHz to keep the error low enough for security. Under these conditions, and without any phase tracking or locking, the protocol's performance still surpasses the PLOB bound (for example, with $F = 1$ GHz, $T_c = 20$ μs, and $\delta\nu = 100$ kHz, secure transmission extends beyond 270 km, and with higher repetition rates and shorter T_c, distances exceed 380 km). The increased $\mathbb{X}$-basis error is fully accounted for in the phase-error upper bound within the key-rate formula, ensuring the protocol remains secure.

4.3.3 Experimental implementations

Shortly after the presentation of Post-Measurement Pairing protocols, two research teams realized the corresponding experimental implementations.

The first one ([70]) was able to overcome the PLOB bound without the need for phase tracking nor phase locking. The protocol chosen to accomplish such result was the AP-QKD one.
Their setup made use of cutting-edge lasers with an extremely narrow bandwidth (1 Hz), centered at a wavelength of 1550.12 nm, stabilized with the already mentioned PDH technique. The encoding was performed with off-the-shelf intensity and phase modulators. The quantum channel was constituted by ultralow loss fibers (with ≈ 0.160 dB/km), while the measurement was performed with SNSPD (Superconducting Nanowire Single Photon Detectors).
The results they achieved were astounding, as they managed to break the record of the distance reached by an MDI protocol (508 km, with approximately 40 secure bits per second), as well as to overcome the PLOB bound, with a secret key rate of 5 kbit/s on a distance of 308 km. Nonetheless, their use of extremely advanced instruments, in particular 1 Hz linewidth lasers, results in an expensive and complex realization (due to the frequency stabilization of the laser at the Hz level).

The implementation of a version of the Mode-Pairing protocol was proposed

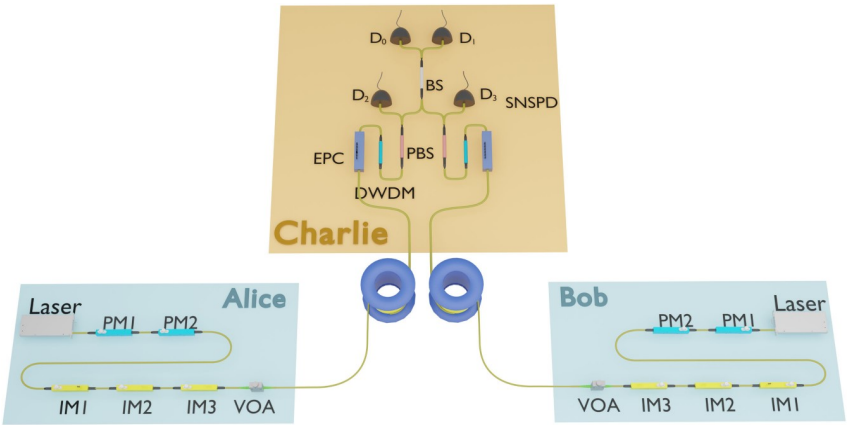

Figure 4.9: The typical setup of a Post-Measurement Pairing QKD implementation.

in [71]. Among the main differences in the setup with respect to the previous experiment, we have to mention the use of off-the-shelf lasers and of a phase-tracking technique. In particular, a part of the pulses sent by Alice and Bob are bright pulses with no modulation to estimate (after the measurement, with a Maximum Likelihood technique) the phase differences. Regarding the lasers, they make use of commercial lasers with 2 kHz of linewidth, centered at 1550.12 nm. To perform the encoding, they use an off-the-shelf intensity modulator and two Sagnac loops, followed by three phase modulators and an optical attenuator.
They were able to reach over 400 km of transmission length (even though having a secret key rate of less than 1 bit/s), yet not managing to overcome the PLOB bound.

Other proposals include a hybrid source (see [72]), a wavelength division multiplexing approach ([73]) in which pulses with different wavelengths can be effectively paired (in the original version of the protocol, they were discarded), that was extended to multi-user networks in [74]. In [75] the authors show the feasibility of employing post-measurement pairing QKD in an already deployed quantum communications infrastructure of hundreds of kilometers links.

A relevant, recent approach ([76]), dating back to May of the current year, manages to overcome the PLOB bound by implementing a MP-QKD protocol with commercial lasers and phase-tracking performed with Fast-Fourier Transform techniques. Through these estimates, researchers were able to apply phase corrections in the post-processing step. Remarkably, they were able to reach a SKR of almost 50 bit/s over 400 km of fiber links, surpassing the PLOB bound by using commercial lasers. We report (in figure 4.9) from the original paper the setup that they employed, which is similar to all the Post-Measurement Pairing QKD implementations.

We will conclude this section by analyzing the setup. At the transmitter side, each user employs a laser source that generates coherent optical pulses, which are then shaped using a series of intensity modulators (IMs) to produce the required signal, decoy, and vacuum states for secure key generation. We want to underline the role of intensity modulators: if the laser operates in continuous mode, one of them is needed to chop the continuous light into a train of pulses. The other two are needed to implement the decoy states technique. In particular, they are involved in the selection of the intensity of the pulse. For this reason, it is typically required a high extinction ratio to ensure maximal suppression when a *vacuum* state is emitted.
Phase modulators (PMs) encode the quantum information by applying relative phase shifts to the pulses. The optical signals are transmitted through fibers to Charlie, where they are first processed by a dense wavelength division multiplexer (DWDM) to properly route the channels. Polarization fluctuations are compensated by an electronic polarization controller (EPC).
A polarizing beam-splitter splits the incoming light from Bob and Alice and directs it towards two Superconducting Nanowire Single-Photon Detectors (SNSPDs), whose outcomes are used for delay and polarization compensation. The other two outputs of the PBS are recombined with a BS, which is connected to two other SNSPDs channels, used to generate the quantum interference measurement results.

5

High-efficiency source

This thesis resumes the efforts put to develop from scratch a source apparatus for AP-QKD. In particular, with respect to the state-of-the-art implementations, presented in section 4.3.3, the initial objective was to simplify the setup to pursue a step towards the practical use of AP-QKD. Specifically, our effort aimed at reducing the number of optical components needed for the encoding part (typically, the implementations consist of several intensity and phase modulators) and at using commercially available lasers.

5.1 Intensity modulation with one Sagnac loop

As outlined earlier, the current experimental implementations of AP-QKD typically use, for the source, three off-the-shelf intensity modulators. With respect to other QKD implementations, in AP-QKD the laser needs to have a high coherence time, leading to the impossibility to use the gain-switching technique: instead, we need to carve a continuous wave laser, and this operation results in low extinction ratio.

The need for a high extinction ratio is justified by the use of the decoy states technique, specifically by the fact that a high extinction ratio between the vacuum states and the "signal" and "decoy"states (*i.e.* states with non-zero intensity) is required. Our aim was to perform intensity modulation by employing a single Sagnac loop. In the following, we provide a theoretical proof that shows the feasibility of this idea.

5.1.1 Theoretical outline

Let's consider a beam-splitter with two inputs and two outputs: in one output branch, there is a phase modulator, *i.e.* a device that applies a phase φ to the incoming light, and in the other branch, there is a delay line of length ΔL. The two branches are then connected together to form a loop. This structure, that exploits the Sagnac effect ([77], [78]) is called a "Sagnac loop", distinguishing it from the "Sagnac mirror", that does not contain active optical elements. A pictorial representation of a Sagnac loop is shown in figure 5.1.

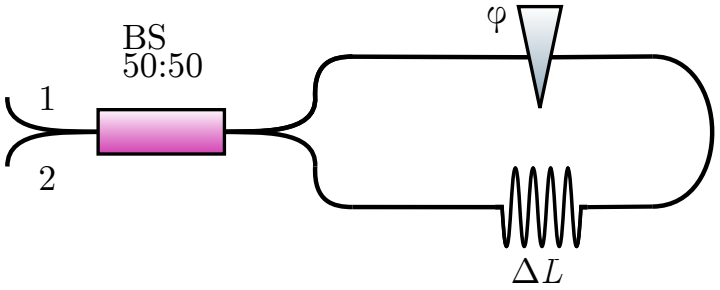

Figure 5.1: The optical design of a Sagnac loop: the light enters from the input 1 and gets divided in the two paths. In one branch a phase φ is applied by a phase modulator, in the other one there is a delay line of length ΔL. The two branches are then united to close the loop.

Let's evaluate now the outputs 1 and 2 (that we indicate with $[E_1, E_2]^T$) when light is entering just from the input 1 (which means $[I_1, I_2]^T = [1, 0]^T$). The BS is characterized by its *scattering matrix*

$$\mathcal{S}_{BS} = \begin{bmatrix} \sqrt{T} & i\sqrt{R} \\ i\sqrt{R} & \sqrt{T} \end{bmatrix} \tag{5.1}$$

, as well as the phase modulator, which reads

$$\mathcal{S}_{\varphi} = \begin{bmatrix} e^{i\varphi_1} & 0 \\ 0 & e^{\varphi_2} \end{bmatrix} \tag{5.2}$$

. Therefore, after the two optical fields are recombined, they can be described by

$$\left(\begin{bmatrix} e^{i\varphi_1} & 0 \\ 0 & e^{\varphi_2} \end{bmatrix} \begin{bmatrix} \sqrt{T} & i\sqrt{R} \\ i\sqrt{R} & \sqrt{T} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right)^{\dagger} \tag{5.3}$$

We are considering the Hermitian conjugate as the modes are switched before re-entering in the BS. It yields:

$$\begin{bmatrix} -ie^{-i\varphi_2}\sqrt{R} \\ e^{-i\varphi_1}\sqrt{T} \end{bmatrix} \tag{5.4}$$

Therefore, the output fields $[E_1, E_2]^T$ can be evaluated by considering the last transformation applied by the BS, that is:

$$\begin{bmatrix} E_1 \\ E_2 \end{bmatrix} = \begin{bmatrix} \sqrt{T} & i\sqrt{R} \\ i\sqrt{R} & \sqrt{T} \end{bmatrix} \begin{bmatrix} -ie^{-i\varphi_2}\sqrt{R} \\ e^{-i\varphi_1}\sqrt{T} \end{bmatrix} \tag{5.5}$$

$$= e^{-i\varphi_1} \begin{bmatrix} i\sqrt{RT}(1+e^{i\Delta\varphi}) \\ T - e^{i\Delta\varphi}R \end{bmatrix} \tag{5.6}$$

Where $\Delta\varphi = \varphi_1 - \varphi_2$. Given the analytical expression of the output fields, we can calculate the corresponding powers:

$$P_1 = |i\sqrt{RT}(1+e^{i\Delta\varphi})|^2 \tag{5.7}$$

$$= RT|1+e^{i\Delta\varphi}|^2 \tag{5.8}$$

$$= 2RT(1+\cos(\Delta\varphi)) \tag{5.9}$$

and

$$P_2 = |T - e^{i\Delta\varphi}R|^2 \tag{5.10}$$

$$= T^2 \left|1 - \frac{R}{T}e^{i\Delta\varphi}\right|^2 \tag{5.11}$$

$$= T^2 \left(1 - 2\frac{T}{R}\cos(\Delta\varphi) + \frac{T^2}{R^2}\right) \tag{5.12}$$

$$= T^2 + R^2 - 2\cos(\Delta\varphi)RT \tag{5.13}$$

Let's now consider for each output the *extinction ratio* ER, defined as the ratio between the maximum and the minimum power achievable.
From equation 5.9 the maximum and the minimum powers, considering output 1, are, respectively:

$$P_1^{\max} = 4RT \tag{5.14}$$

$$P_1^{\min} = 0 \tag{5.15}$$

$P_1^{\max}$ is achieved when $1+\cos(\Delta\varphi) = 2$, *i.e.* $\Delta\varphi = 0$, while it is possible to reach $P_1^{\min}$ with $\Delta\varphi = \pi$, leading to a theoretical extinction ratio of:

$$\mathrm{ER}_1 = \frac{P_1^{\max}}{P_1^{\min}} = \infty \tag{5.16}$$

It is important to highlight that, in the output 1 of the BS, the maximum extinction ratio can be achieved only by applying a phase of π inside the Sagnac loop. Yet, an

extreme precision is needed to obtain a high extinction ratio, as it is possible to see from figure 5.2 and tab. 5.1. However, in a non-ideal scenario, there are phenomena such as cross-talks and reflections that prevent it from reaching an infinite value.

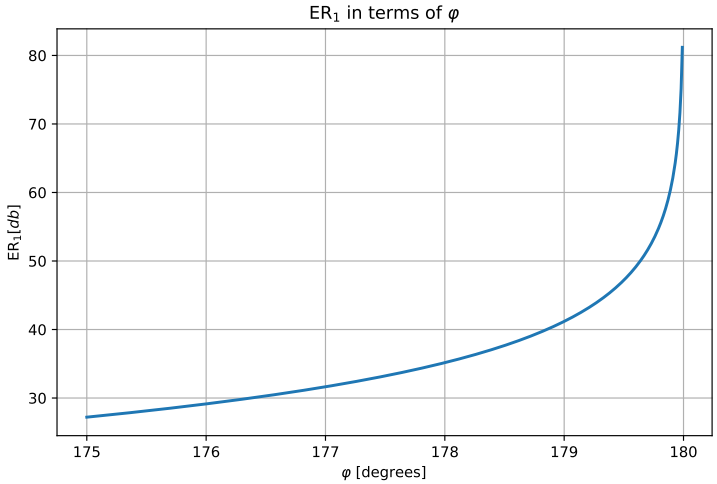

Figure 5.2: The extinction ratio (expressed in dB) achievable in output 1 in terms of the phase φ applied.

Regarding output 2, from equation 5.13 we have:

$$P_2^{\max} = 1 \tag{5.17}$$

$$P_2^{\min} = (T - R)^2 = (1 - 2T)^2 \tag{5.18}$$

where we exploited the fact that $R + T = 1$. Therefore:

$$\mathrm{ER}_2 = \frac{P_2^{\max}}{P_2^{\min}} = \frac{1}{(1 - 2T)^2} \tag{5.19}$$

It is easy to observe that we reach the maximum extinction ratio when $T = 0.5$, *i.e.* when the beam-splitter is a perfect 50:50 BS. If not, the achievable extinction ratio decreases rapidly, as figure 5.3 shows.

It is clear that, in order to obtain a high extinction ratio from the Sagnac loop we need either an extreme precision in the phase φ applied (as table 5.1 shows), or an almost perfect 50:50 beam splitter (see table 5.2 for a list of extinction ratios achievable in terms of the splitting error).

Since our experimental setup was designed to measure the extinction ratio of both channels (more details in sections 5.2 and 5.3), we show how to derive $\Delta\varphi$ and T from ER_1 and ER_2, respectively.

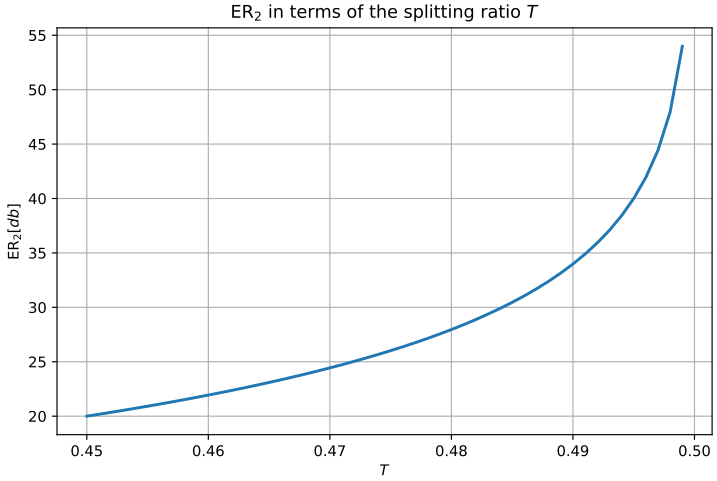

Figure 5.3: The extinction ratio (expressed in dB) achievable in output 2 in terms of splitting ratio T of the beam-splitter.

ER_1	Phase error [rad]	Phase error [°]
20 db	0.2003	11.478°
30 db	0.0632	3.624°
40 db	0.0200	1.145°
50 db	0.0063	0.362°
60 db	0.0020	0.114°
70 db	0.0006	0.036°
80 db	2e-04	0.011°
90 db	6.32e-05	0.003°

Table 5.1: The precision needed in setting the phase to π (expressed both in radiants and degrees) to achieve different values of extinction ratio.

Starting from the output labeled as 1 in figure 5.1, the definition of ER_1 is:

$$ER_1 = \frac{P_1^{max}}{P_1^{min}} \tag{5.20}$$

If no phase modulation is applied, *i.e.* if $\Delta\varphi = 0$, we have the maximum power:

$$P_1^{max} = 4RT \tag{5.21}$$

On the other hand, when we apply a phase modulation $\Delta\varphi$, aiming at reaching π, we have the minimum power:

$$P_1^{min} = 2RT\,(1 + \cos(\Delta\varphi)) \tag{5.22}$$

ER_1	Splitting error
20 db	0.09090
30 db	0.03065
40 db	0.00990
50 db	0.00315
60 db	0.00099
70 db	0.00031
80 db	9.993e-05
90 db	3.162e-05

Table 5.2: The extinction ratio achieved in terms of the distance from the perfect splitting ratio $T = 0.5$.

This leads to the ratio:

$$\mathrm{ER}_1 = \frac{P_1^{max}}{P_1^{min}} = \frac{2}{1 + \cos(\Delta\varphi)} \tag{5.23}$$

Therefore it is possible to calculate the phase modulation applied as

$$\Delta\varphi = \cos^{-1}\left(\frac{2}{\mathrm{ER}_1} - 1\right) \tag{5.24}$$

By following an analogous reasoning and recalling equation 5.13, we can easily observe that the maximum power is achieved when we are modulating the phase, therefore:

$$P_2^{max} = T^2 + R^2 - 2\cos(\Delta\varphi)RT \tag{5.25}$$
$$= 2T^2(1 + \cos(\Delta\varphi)) - 2T(1 + \cos(\Delta\varphi)) + 1 \tag{5.26}$$

In equation 5.26 we wrote it in terms of T exploiting $T + R = 1$. On the other hand the minimum power is reached with no modulation at all, leading to

$$P_2^{min} = T^2 + R^2 - 2RT \tag{5.27}$$
$$= (T - R)^2 \tag{5.28}$$
$$= (T - (1 - T))^2 \tag{5.29}$$
$$= 4T^2 - 4T + 1 \tag{5.30}$$

The extinction ratio can be expressed as:

$$\mathrm{ER}_2 = \frac{2T^2(1 + \cos(\Delta\varphi)) - 2T(1 + \cos(\Delta\varphi)) + 1}{4T^2 - 4T + 1} \tag{5.31}$$

If we solve for T, we retrieve the second-order equation:

$$T^2(4\mathrm{ER}_2 - 2\cos(\Delta\varphi) - 2) - T(4\mathrm{ER}_2 + 2\cos(\Delta\varphi) + 2) + \mathrm{ER}_2 - 1 = 0 \quad (5.32)$$

that leads to:

$$T = \frac{(4\mathrm{ER}_2 + 2\cos(\Delta\varphi) + 2)}{2[4\mathrm{ER}_2 - 2\cos(\Delta\varphi) - 2]} \pm \quad (5.33)$$

$$\pm \frac{\sqrt{[4\mathrm{ER}_2 + 2\cos(\Delta\varphi) + 2]^2 - 4[4\mathrm{ER}_2 - 2\cos(\Delta\varphi) - 2](\mathrm{ER}_2 - 1)}}{2[4\mathrm{ER}_2 - 2\cos(\Delta\varphi) - 2]} \quad (5.34)$$

Since we are interested only in the value splitting ratio, choosing the + or the − sign in the solution is totally indifferent, since the other choice corresponds to deriving R.

5.2 First setup

We will now describe the first version of the setup adopted to measure the extinction ratio of the Sagnac loop. The setup is shown in figure 5.4

The light source was a laser (see section 5.2.1) driven by 20 MHz electrical signals that were 250 ps wide. This operation was carried out by generating a squared electrical signal with an FPGA (Field Programmable Gate Array) with an peak-to-peak voltage of approximately 0.5 V and it was amplified with an RF amplifier with a maximum electrical power gain of 29 dB and 23 GHz bandwidth.
The optical pulse (shown in figure 5.4 in red with an arrow directed to the right) then entered the circulator, a three-port optical component. In a circulator, if light enters from port 1 gets directed to port 2, while if light enters from port 2, then it is not reflected in port 1 but exits from port 3.
Subsequently, the pulse entered the beam splitter (from the port labelled 1 in figure 5.4) and got split into two pulses: one that travelled the loop clockwise and the other one counter-clockwise.
Regarding the clockwise pulse, it encountered the phase modulator, controlled by an electric amplified signal with a frequency of 10 MHz. The anticlockwise signal travels across the delay (with $\Delta L \approx 2$ m) and is recombined with the clockwise signal.

According to the theoretical framework presented in section 5.1.1, if there is no phase modulation applied (*i.e.* $\Delta\varphi = 0$) and the beam-splitter perfectly splits in

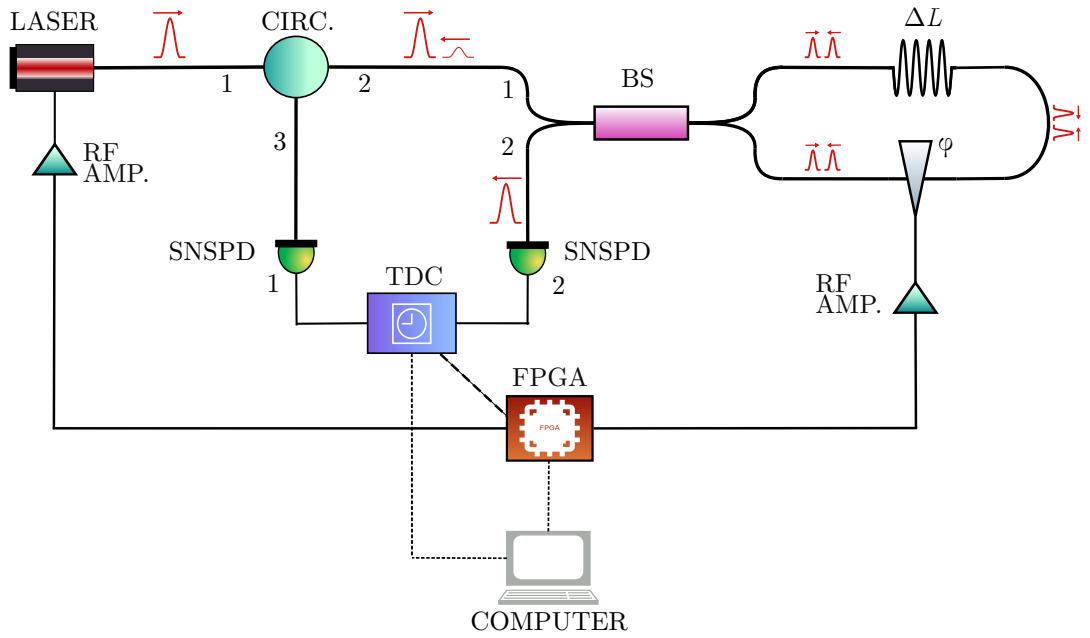

Figure 5.4: The initial version of the setup. The laser is driven by the amplified signals sent by the FPGA, controlled by the computer. The pulses enter the circulator and then they are directed towards the Sagnac loop. Two SNSPDs are put in correspondence of port 3 of the circulator and port 2 of the beam-splitter: the events they detect are transformed by the TDC into timestamps and sent to the computer. Abbreviations: FPGA (Field Programmable Gate Array), SNSPD (Superconducting Nanowire Single Photon Detector), RF AMP (Radio-Frequency Amplifier), TDC (Time-to-Digital), CIRC. (Circulator).

half the light (*i.e.* $T = R = 0.5$), all the light coming from the Sagnac loop goes from the output port labelled 1 to the circulator, where it enters from port 2 and exits from port number 3.
On the other hand, if the phase modulator applies a phase of $\Delta\varphi = \pi$, all the light of the Sagnac loop exits from the output number 2 of the beam-splitter (this event is depicted with the pulses with the arrow directed to the left in figure 5.4: at the beam-splitter output we have a "big" pulse, while on the circulator output a "small", that indicates non-idealities of the setup, since it should be completely suppressed). By applying a modulation signal with half of the frequency of the laser pulse, we are able to collect one modulated and one non-modulated signal for each modulation period (that is twice the period of the pulse). This allows a comparison between the two and the calculation of the extinction ratio.

Finally, each output of the setup is connected to one channel of a Superconducting Nanowire Single Photon Detector (SNSPD); the single-photon detection events are translated into timestamps by an Time-to-Digital (TDC) converter (called also Time-Tagger). We were able to control the real-time counts of each channel of the SNSPD thanks to a GUI (Graphical User Interface) connected to the TDCs, which

provided the real-time incoming number of photons over an adjustable number of periods, as well as a visual representation of the shape of the pulses. The interface was modified in order to display the real-time extinction ratio in each SNSPD channel by exploiting the data analysis technique that we introduce in section 6.1. Finally, the interface provided a way to store the timetags of a variable amount of time in `.bin` format.

The fibers connecting each component, up to the detectors, were PM fibers. The fibers connecting the setup to the detectors were single-mode (SM) fibers, connected to polarization controllers. Moreover, each component was carefully stabilized and fixed to the optical table by means of tape, to avoid polarization or light intensity drifts due to mechanical movements.

A 10 MHz clock was generated by the FPGA and shared with the Time-Tagger.

5.2.1 Laser

The laser that we employed is an Eblana EP1550-DM-H, a DFB semiconductor laser that emits light with a wavelength around 1550 nm. Its basic operation relies on a current injected into the diode, which produces stimulated emission when the carrier density exceeds a certain threshold. All the technical details can be found in the datasheet [79]. Moreover, it has a 100 kHz linewidth, far from being as narrow (and therefore we can consider it "practical", at least from the point of view of the cost) as cutting-edge lasers (in [70] the researchers use lasers with 1 Hz linewidth).

For modulation, the laser can be driven with a combination of a DC bias and a Radio-Frequency (RF) signal. When the DC bias is near or slightly above the threshold current, applying a sufficiently strong RF signal can drive the instantaneous current below and above the threshold periodically. This produces the gain-switching, a regime in which the laser emits a train of optical pulses corresponding to the moments when the carrier density rapidly crosses the threshold. In practice, gain-switching allowed us to generate short optical pulses without using an external modulator.

5.2.2 Single Photon Detectors

The single photon detection was performed with Superconducting Nanowire Single Photon Detectors (SNSPDs), a cutting-edge technology that ensures remarkable performance.

SNSPDs require cryogenic operation at temperatures typically in the order of 1 K in order to maintain the superconducting state of the nanowire. When a photon is absorbed, its energy breaks Cooper pairs, creating a localized resistive hotspot. Since the nanowire is biased with a current just below its critical value, the formation of the hotspot redistributes the current; if the local current density exceeds the reduced critical current, the superconducting state collapses locally and the wire switches into a resistive state. This resistive transition produces a transient voltage pulse, which is detected by the readout electronics and registered as a single-photon event. Once the hotspot cools and the superconducting state is restored, the detector resets and becomes ready to detect subsequent photons.

State-of-the-art commercial realizations integrate the nanowires in closed-cycle cryogenic platforms and achieve system detection efficiencies exceeding 95%, timing jitter on the order of tens of picoseconds, and ultra-low dark count rates, in some cases below one count per second. In comparison, InGaAs/InP avalanche photodiodes operated in Geiger mode (SPADs) typically suffer from lower detection efficiency, higher timing jitter and significantly higher dark count rates. By contrast, SNSPDs are free-running and support much higher maximum count rates. The principal limitation of SNSPDs remains the requirement for cryogenic refrigeration and the associated system complexity, yet their superior performance makes them the detectors of choice for demanding applications such as QKD (their cost, however, prevents them from being used in commercial applications).
Nonetheless, we have to mention that, in the efforts toward practical QKD realizations, they represent a non-negligible element, as their complexity and cost certainly represent an obstacle.

5.3 Theory of operation

As mentioned earlier, the two possible ways to achieve a high extinction ratio by using a Sagnac loop are either extreme precision in the phase modulation step or a beam splitter whose splitting ratio is as close as possible to 50:50. For this reason, in our initial efforts, we did not choose one way instead of the other, but we rather tried both in order to explore which one was the most promising.
In particular, we tried to reach a phase modulation of π by means of an electro-optical phase modulator and, in parallel, to investigate potential solutions to fine-tune the splitting ratio of the beam splitter. Among them, temperature, physical compression, and, later, different wavelengths.
In the following, we explain in detail such operations.

5.3.1 Electro-optical phase modulation

The tool we used to control the phase in the Sagnac loop was an iXBlue MPZ-LN-10 electro-optical modulator. The working principle of this component is directly linked to the Pockels effect (see chapter 11 of [80]). This effect exploits the property of certain materials to linearly change their refractive index when an electric field is applied, in our case the Lithium Niobate ($LiNbO_3$). The change in the refractive index determines a difference in the speed of the light crossing the material, hence resulting in a change of the phase.

Our aim was to control it with electrical signals at a frequency of 10 MHz, to obtain the effect of having one modulated and one unmodulated pulse each two laser pulses. For this reason, we exploited the FPGA to generate the electrical signals. This was not sufficient, though, as the phase modulator needs between 6 V and 8V voltage to apply a phase modulation of π, while the peak-to-peak voltage of the signals generated by the FPGA was smaller than 0.5 V.

For this reason we decided to use an RF amplifier, the Photline DR-DG-20-HO ([81]). Its maximum power (small signal) gain G^{dB}_{max} is reported to be 29 dB, and can be tuned to a range of 3 dB by adjusting the amplification voltage V_{amp}, with $0\ \text{V} \leq V_{amp} \leq 2\ \text{V}$. Since

$$G^{dB} = 10 \log_{10} \left(\frac{P_{out}}{P_{in}} \right) \tag{5.35}$$

and it is known that the relation between the electrical power and the voltage is quadratic, it yields:

$$G^{dB} = 10 \log_{10} \left(\frac{V^2_{out}}{V^2_{in}} \right) = 20 \log_{10} \left(\frac{V_{out}}{V_{in}} \right) \tag{5.36}$$

Therefore

$$V_{out} = 10^{\frac{G^{dB}}{20}} \cdot V_{in} \tag{5.37}$$

resulting in

$$V_{out} \leq 10^{\frac{G^{dB}_{max}}{20}} \cdot V_{in} \tag{5.38}$$

A fundamental parameter to set was the delay between the laser pulses and the modulation pulses, *i.e.* the electric signals that drive the electro-optical phase modulator. The reason is quite easy to understand, as it is necessary to match the "modulation window", that is the amount of time, corresponding to the width of

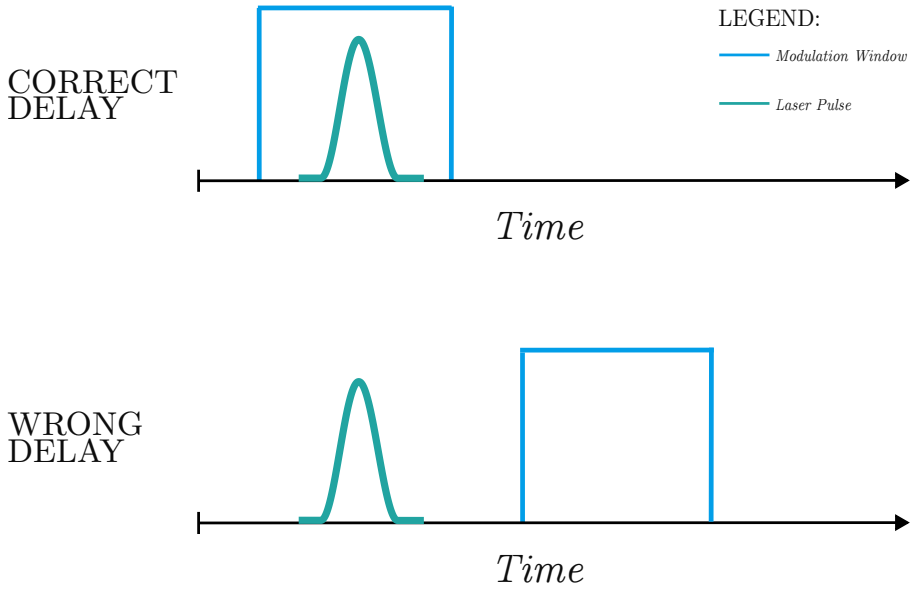

Figure 5.5: A schematic representation of the tuning of the delay operation. When the delay between pulse of the laser and the signal that controls the electro-optical phase-modulator is correct, we obtain the modulation effect as they are overlapped in time (meaning that the phase-modulator applies a phase oh π when the laser pulse crosses it). If the delay is wrong, meaning that the application of the phase is not synchronized with the laser pulse, no phase modulation is obtained.

the signal that controls the phase modulator, with the arrival time of the pulse: a wrong setting of this parameter results in no phase modulation.

Thanks to the real-time interface, we were able to find the optimal starting time with a temporal scan over a pulsing period: in fact, with no modulation applied, a channel displayed two peaks over two periods while the other one did not detect light (as predicted by the theoretical framework). The sign of the correctness of the starting time chosen was the effect of seeing a peak over two periods in both channels, that is, the effect of the phase modulation. At that point, a final fine-tuning operation of both the starting time and the width of the window allowed us to obtain the modulation effect. A schematic representation is shown in figure 5.5

5.3.2 Temperature control

As mentioned in the introduction of this section, we selected the temperature as a means through which the splitting ratio could have been modified, providing a way to fine-tune it to reach the optimal value of 0.5. In the literature, there are several examples (see for example [82], [83]) that discuss and demonstrate that the behavior of fused beam-splitters depends on their working temperature, due to their fabrication principle (see section 6.3).

Therefore, we decided to place the beam-splitter on a Peltier cell, controlled by a Meerstetter TEC-1091 controller.
A Peltier cell, is composed of multiple semiconductor elements arranged in pairs of n-type and p-type materials, electrically connected in series and thermally in parallel. These semiconductors are positioned between two ceramic plates that provide both electrical insulation and mechanical support. When a continuous current passes through the module, heat is absorbed on one side (the cold junction) and released on the opposite side (the hot junction) due to the Peltier effect (see [84]). The direction of heat transfer is determined by the polarity of the current, so reversing it switches the hot and cold sides.
We were able to fully control the temperature of the Peltier cell thanks to the TEC-1091, which was monitoring the temperature of the beam-splitter through a thermistor. This information was fed to a feedback system that, thanks to a PID controller, adjusted the correct value of the current needed to reach the wanted temperature.

Subsequently, we noticed that simply placing the beam-splitter upon the Peltier cell did not yield sufficient performance in terms of insulation from the ambient temperature: for this reason, we managed to build a thermal insulation recipe to avoid the effects of the ambient on the entire temperature control system.

5.4 Second setup

The second version of the setup differs from the first one on two points: the laser employed, and the use of two additional intensity modulators before the circulator; one of them is an off-the-shelf intensity modulator, and the other one is a Sagnac loop (in order to increase the extinction ratio of the carved pulses). This implementation led to the possibility of having a wide range of wavelengths at our disposal (thanks to the laser chosen, see section 5.4.1). The setup is shown in figure 5.6.

The laser was a PurePhotonics PPCL590, chosen because of the possibility of being tuned in a broad range of wavelengths (between 1521.79 nm and 1565.49 nm). The continuous light emitted by the laser (sketched in figure 5.6 as a horizontal line) enters an optical isolator. An isolator is a two-port optical component whose purpose is to avoid that the light entering from the output exits from the input (eliminating therefore all the light that is reflected from subsequent components of the setup, and preventing it from reaching the laser). On the other hand, the light that enters from the input port exits from the output port with minimal losses.
The continuous light then reaches the intensity modulator, in which it is carved in

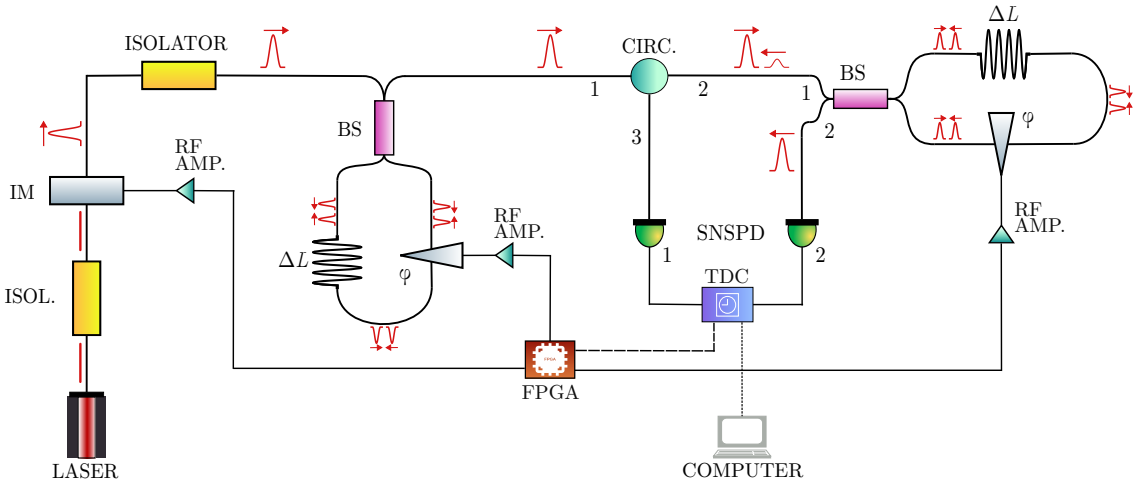

Figure 5.6: The second version of the setup. The light is emitted in continuous by a laser in continuous mode, passes through an optical isolator (that avoids reflections) and is carved into pulses by an off-the-shelf intensity modulator, controlled by an amplified electric signal originated from the FPGA. After a second optical isolator, the pulses reach a Sagnac loop that applies a π modulation (driven by the amplified electrical signals generated by the FPGA). Finally, the pulses arrive at the circulator: from this point, the second setup is completely identical to the first one, shown in figure 5.2.

order to create a train of narrow pulses with frequency 2 MHz, therefore one order of magnitude smaller than the frequency used in the first setup. This choice was determined by the necessity of avoiding light reflections from consecutive pulses in the setup. The pulses then enter the Sagnac loop (after another optical isolator), in which the phase modulator is controlled with 2 MHz electrical signals and the RF amplifier between the FPGA and the phase-modulator of the first Sagnac loop is tuned in order to reach V_π. In practice, we are modulating all the pulses entering the Sagnac loop, in fact the light exits only from the second input of the BS. Our aim is to suppress all the light components outside the temporal window of the pulse, *e.g.* after-pulses, to enhance the splitting ratio of the pulse itself. From the output of the first Sagnac loop, the setup is the same as we described in section 5.2, with the only exception that the phase-modulator of the second Sagnac loop is driven with electrical signals with a frequency of 1 MHz, to maintain the idea of having one modulated and one unmodulated pulse for each two laser pulse periods.

5.4.1 Laser

The laser that we employed is a PurePhotonics PPCL590, a continuous-wave tunable laser module equipped with an integrated acetylene (C_2H_2) gas cell for frequency stabilization. The laser operates in continuous mode and does not support gain-switching (for this reason, we needed to carve the pulses with the intensity modulator). Its wavelength can be tuned across multiple discrete points in the

C-band (that goes from $\approx$ 1530 nm to $\approx$ 1565 nm). A portion of the output is routed through the gas cell, and the transmitted power is monitored to lock the laser frequency at the half-absorption point, where the slope of the absorption line is maximal. Initially, the laser approaches this point in a "dither mode" and then switches to "whisper mode", in which a piezoelectric transducer continuously adjusts the frequency to maintain the lock. Briefly, this laser allowed us to tune to precisely the wavelength of the light entering the setup. All the details can be found in [85]. We want to stress that its linewidth is in the order of 10 kHz, unlike the lasers employed in [70] for example, that had a linewidth of 1 Hz.

6 Results

In this section, we will present the results obtained by using two different types of beam-splitters, preceded by an outline of the data analysis that we performed to retrieve them. These results have been achieved by the second setup we described in section 5.4 using two different types of beam-splitters, one based on micro-optics splitting techniques and the other one on fused fibers.

6.1 Data analysis

Before arriving at the results obtained, we want to describe, step-by-step, the procedure that allowed us to calculate the extinction ratios from the raw `.bin` files that contained the timestamps of the SNSPD detections.

The analysis begins by loading the raw `.bin` files, where the detection timestamps are encoded as 64-bit integers, and the corresponding channel information is stored using 8 bits. Once the data is loaded, the total acquisition time is calculated, and the pulsing period T of the source is defined.
We then select only the timestamps corresponding to the SNSPD channel of interest. At this point, all timestamps are folded modulo one or two periods, effectively mapping the events into a reduced temporal window corresponding to exactly one or two pulsing cycles. This step aligns events that occur in successive periods, allowing the analysis on a restricted time window.
After folding, we determine the maximum timestamp value within the selected interval. This value is then used to define the range for constructing a histogram of detection events. The histogram bins show the timestamps within the reduced

period(s), providing a clear visualization of how detection events are distributed temporally within a single (double) pulsing cycle(s). We can plot the resulting histograms (figures 6.1 and 6.2 for instance).

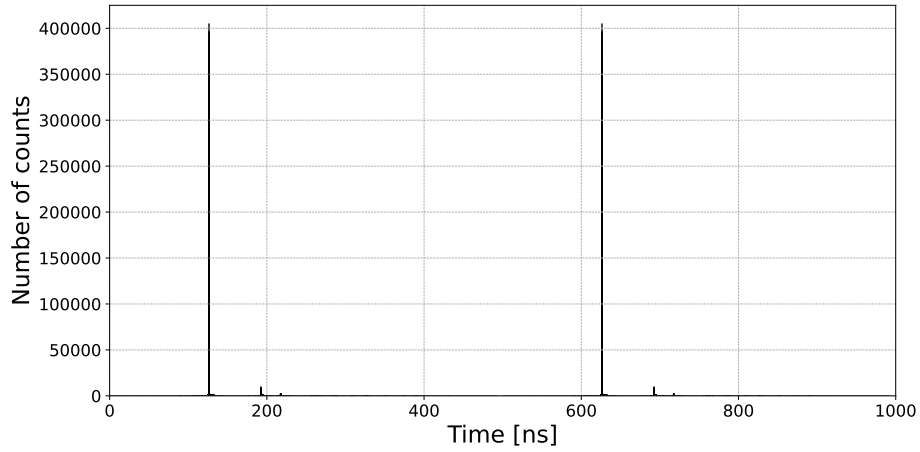

Figure 6.1: The histogram with the number of timestamps detected by the SNSPDs without applying any phase modulation, over two periods (with a pulsing frequency of 2 MHz). It is possible to clearly see two identical pulses, one per period.

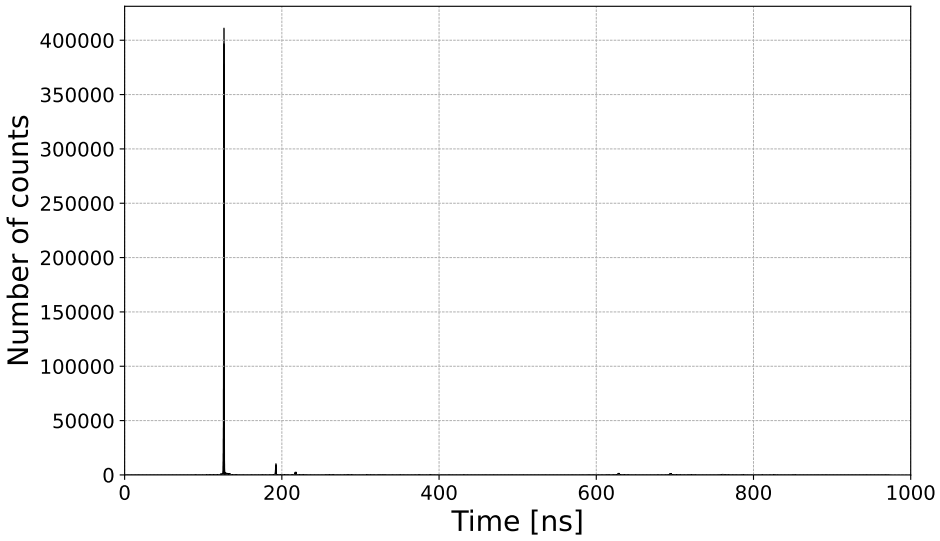

Figure 6.2: The histogram with the number of timestamps over two periods considering a pulsing frequency of 2 MHz (and a modulation frequency of 1 MHz). With respect to figure 6.1 it is possible to see the effect of the modulation: the second peak has been suppressed.

The successive step is to consider the peak of the histogram and an arbitrary temporal window around it. Since from the GUI we observed that the pulse width was in the order of a few ns, we decided to choose the width of this window to be

10 ns. In this interval, we fit a Gaussian on the bins that compose the histogram, as it is possible to see from figure 6.3.

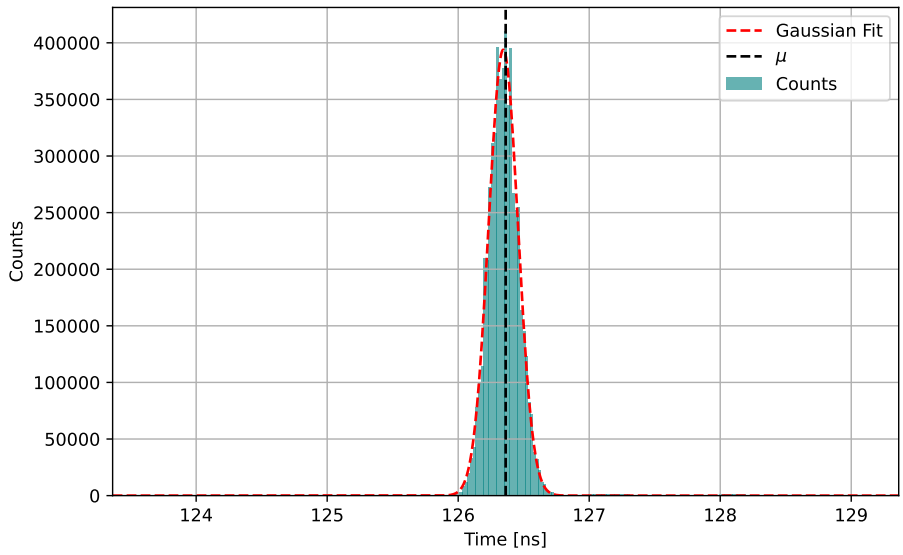

Figure 6.3: The fitting of a Gaussian function near the peak.

The Gaussian fit allowed us to retrieve the mean μ and the standard deviation σ. Thanks to these parameters, we can choose a temporal window of arbitrary width $[\mu - \alpha \cdot \sigma, \mu + \alpha \cdot \sigma]$ where α is a multiplicative factor that we can decide. We want to underline the necessity of the Gaussian fit, that allows us to have a clear representation of the shape of the pulse as well as precise time references (μ and σ).

The last point left is to choose α and compute, through a mask, the number of counts in the window $[\mu - \alpha \cdot \sigma, \mu + \alpha \cdot \sigma]$ and in the window $[\mu \pm T - \alpha \cdot \sigma, \mu \pm T + \alpha \cdot \sigma]$: briefly, with this operation we are summing the number of single-photon detections around the primary peak (*i.e.* the optical power) and one period before or after (it depends on whether the primary peak is in the first period or in the second). By taking the ratio between the two sums means calculating the extinction ratio on the channel. A visual representation of the temporal window is shown in figure 6.4. An important remark is that the extinction ratio is independent of the width of the window, as long as it is the same for the main peak and the secondary peak, obviously. In all the derivations of the extinction ratio that we will present in the following, we used $\alpha = 1$.

Once we calculated the extinction ratio, we were able to derive the modulation applied and the splitting ratio, by employing the result of the theoretical deriva-

tion presented in section 5.1.1. As mentioned in section 5.2, we implemented this procedure also in the GUI to have a real-time visualization of the extinction ratio.

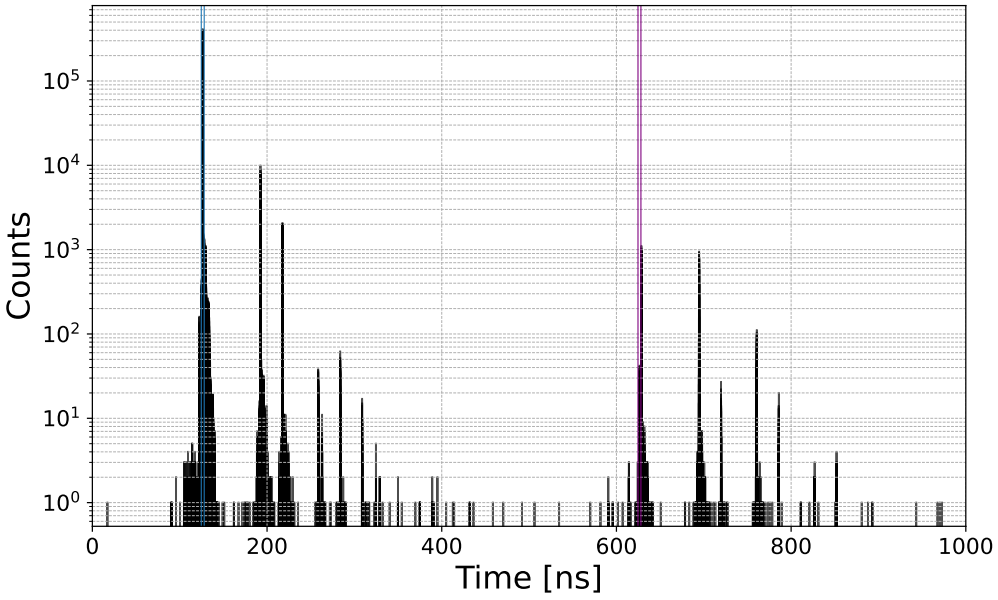

Figure 6.4: The histogram of the counts over two pulsing periods with a logarithmic scale in the y axis. It is possible to see the two temporal windows of width ≈ 3.36 ns (corresponding to $\sigma = 0.112$ ns and $\alpha = 15$ - chosen to have a clear graphical representation) determined to sum the number of counts and derive the extinction ratio. The blue one is centered around the main peak, the purple one is one period after, centered around the modulated peak.

Moreover, from figure 6.4 we can observe that having an afterpulse in the main peak, as in our case (it is also evident from the Gaussian fit shown in 6.3) does not represent a problem in terms of the calculation of the extinction ratio, as the window we are choosing completely avoids it.

Finally, we mention the fact that the GUI automatically created another `.bin` file when the previous one reached the dimension of 50 MBytes. In case of long measurements, we merged together the `.bin` files to create only one `.bin` file, and we performed the analysis described above on that file.

6.2 Micro-Optics beam-splitter

There are different techniques to realize a fiber-based beam-splitter. Our first choice was to use a device whose splitting mechanism was based on micro-optics techniques. In particular, the light arriving from the two input fibers is decoupled (therefore it travels in free-space) and collimated by two lenses. The light is then directed

towards the optical tool that separates it (*e.g.* a prism) and then recoupled into the two output fibers. Briefly speaking, the light is split using free-space techniques. For this reason, one would expect a stable splitting ratio over a wide range of wavelengths, as well as no significative dependence on the temperature. We used a micro-optics BS from Haphit ([86]) whose performance was claimed to be stable in a window of 80 nm centered at 1550 nm.

6.2.1 Extinction Ratios

As outlined before, our aim was to obtain a high extinction ratio from the setup, regardless of the approach used: in particular, we tried both to reach with high precision a phase modulation of π as well as relying on the accuracy of the beam-splitters.

We will start by presenting the results obtained with the phase modulation. As mentioned in section 5.3.1, the crucial element to achieve high precision in the phase modulation was the amplification of the electric signal provided by the FPGA. The reason is that the electro-optical phase modulator needs a specific voltage to apply a phase of π: in our case, the datasheet indicated the range $6 - 8$ V. Therefore, our efforts were concentrated in choosing the perfect amplification of the signal to reach the voltage corresponding to the π phase modulation, that we can call V_π.

The amplification provided by the IXBlue DR-DG-20-HO could be controlled by setting the voltage V_{amp} between 0V and 2V. Moreover, it was possible to control also the cross point by applying a voltage between 0 V and 1.5 V: in this case, we used the typical value of 0.7 V.
Firstly, we measured the extinction ratio achieved by applying a voltage varying between 0 V and 1.2 V with a step of 0.1 V. The plot is shown in figure 6.5.

From the plot, it is clear that the maximum extinction ratio is obtained by applying $0.6\text{V} \leq V_{amp} \leq 0.8\text{V}$. For this reason, we performed a second scan to fine-tune V_{amp}, in this case between 650 mV and 750 mV with a step of 10mV. The results are depicted in figure 6.6.

It is clear from the plot that we were able to reach an extinction ratio of over 45 dB with the phase modulation, by applying $V_{amp} = 0.72\text{V}$. In particular, the exact value is 47.43 dB, which means that, according to the derivation shown in section 5.1.1, $\varphi \approx 3.13308$ rad ($\varphi \approx 179.5122°$) with an error with respect to π of ≈ 0.008505 rad ($\approx 0.4873°$), achieving a precision of more than 99.7 %.

We want to remark that this result is independent of the splitting ratio of the beam-splitter, and therefore of the beam-splitter itself, meaning that, with the ex-

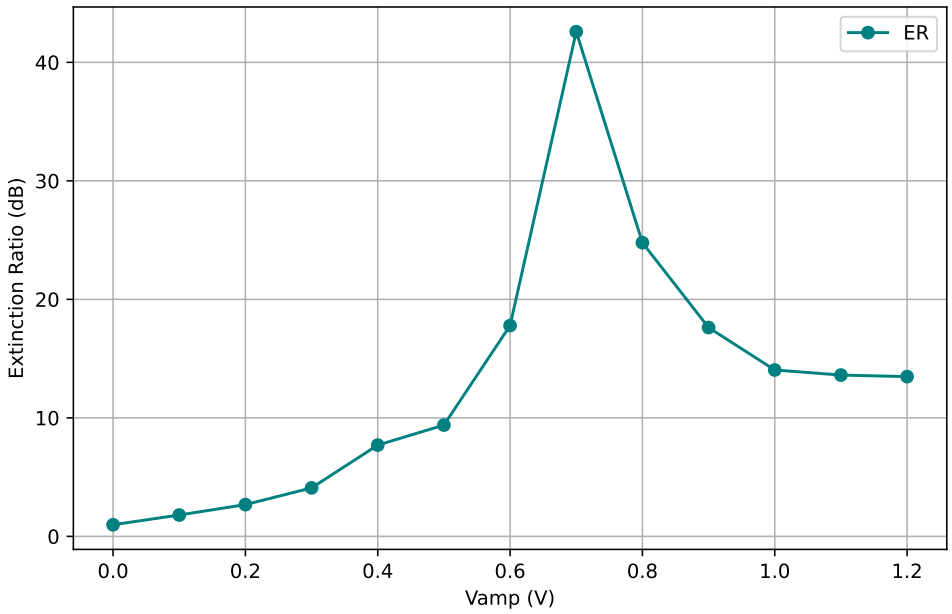

Figure 6.5: The extinction ratio achieved for different values of 0 V $\leq V_{amp} \leq$ 1.2 V measured with steps of 100 mV. From this graph it is clear that the amplification needed by the electric signal applied to the phase modulator to reach V_π is around 700 mV.

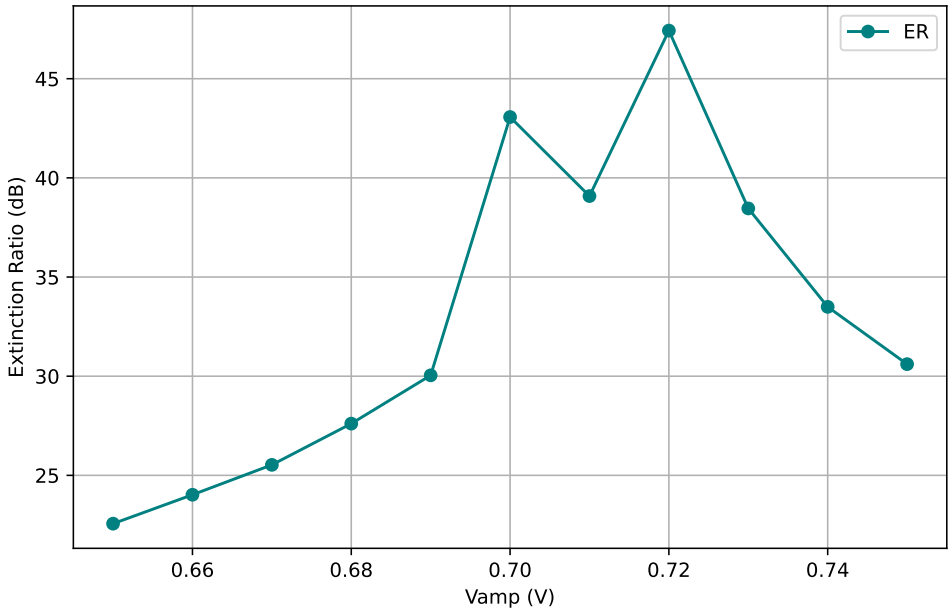

Figure 6.6: The extinction ratio achieved with the fine-tuning of V_{amp}. In particular, the scan was performed for 650 mV $\leq V_{amp} \leq$ 750 mV with a step of 10 mV. The maximum extinction ratio (therefore the maximum modulation precision) is reached with $V_{amp} = 720$ mV.

act same settings, it can be achieved by using a fused beam-splitter.

On the other hand, the extinction ratio deriving from the splitting ratio is heavily dependent on the beam-splitter. Of course, it is possible to obtain an infinite extinction ratio if the beam-splitter splits perfectly the light, while the higher the distance from $T = R = 0.5$, the lower the ER. As we mentioned earlier, from a micro-optics beam-splitter, we expect a stable behavior of the splitting ratio over different conditions. In fact, we firstly tried to act on the splitting ratio by changing the temperature (using a Peltier cell, as explained in 5.3.2), by changing it from 25 °C to 40 °C with a step of 2.5 °C: the plot is shown in 6.7.

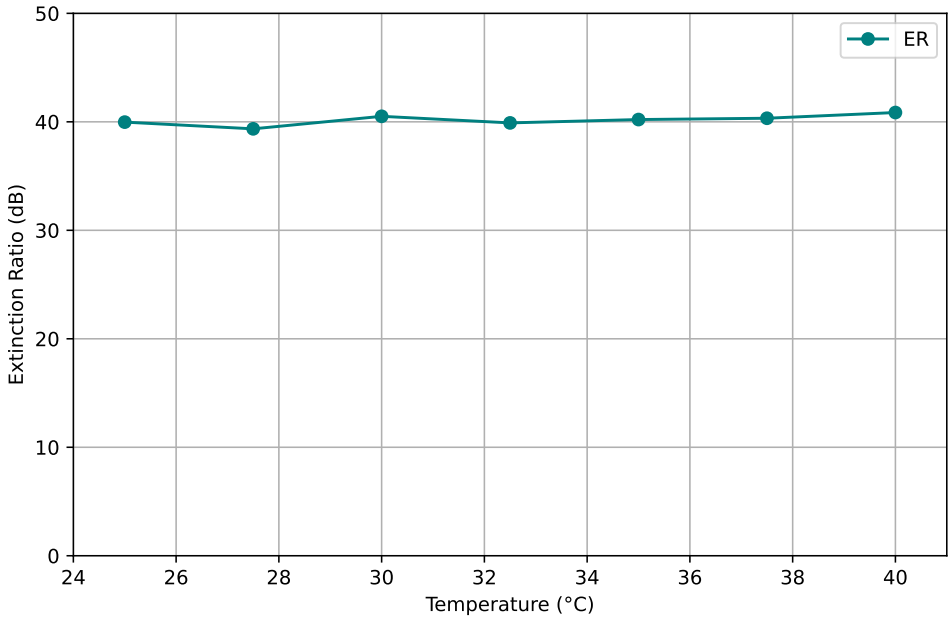

Figure 6.7: The extinction ratio deriving from the splitting ratio of the micro-optics beam-splitter under different temperatures. As expected, the micro-optics beam splitter behaves independently of the temperature, providing an almost constant extinction ratio when different temperatures are applied to it.

Subsequently, we wanted to investigate whether the splitting ratio, and therefore the extinction ratio, exhibited a dependence on the wavelength of the impinging light: we performed a scan between 1565.49 nm and 1529.55 nm with a step of 4.07 nm. The resulting plot is depicted in figure 6.8.

As the plots show, we were able to reach more than 40 dB also by using the beam-splitter splitting ratio.

These two results confirm the fact that the action of the micro-optics beam-splitter is extremely stable even under temperature changes or light with different wavelengths. On the one hand, this is encouraging as we are guaranteed to achieve consistent

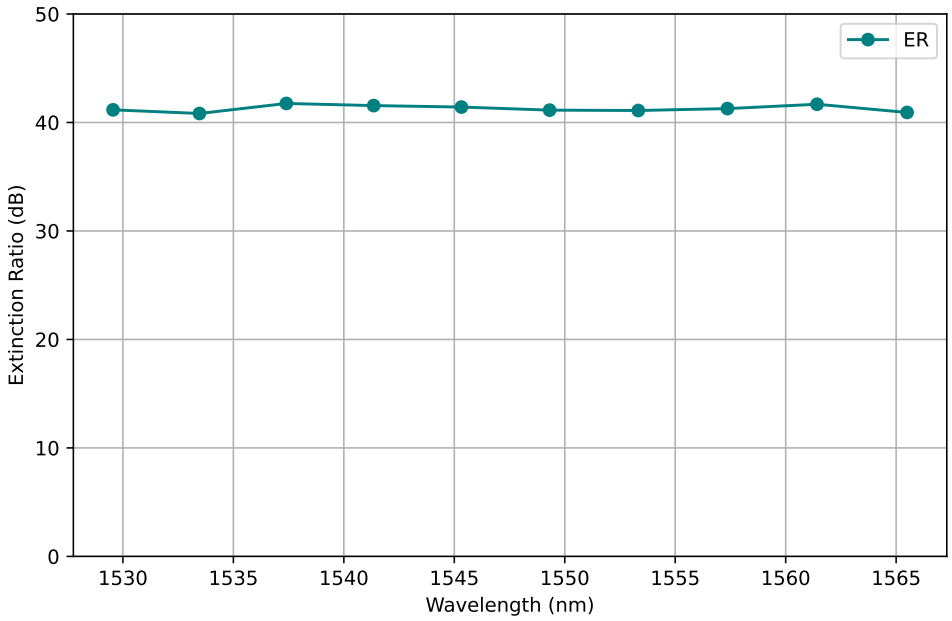

Figure 6.8: The extinction ratio deriving from the splitting ratio of the micro-optics beam-splitter with different wavelengths. Once again, the micro-optics beam-splitter offers stable performance for a wide range of wavelengths, ensuring almost constant extinction ratio from 1529.55 nm to 1565.49 nm.

results under different conditions; on the other hand, it highlights that it can't be done much to enhance or increase the splitting ratio.

6.3 Fused beam-splitter

A second technique used in the realization of fiber beam-splitters exploits the principle of *evanescent field coupling*. During the fabrication process, the cladding of the two input fibers is locally removed, and the fibers are fused together under the application of heat while being simultaneously tapered. This creates an interaction region where the fiber cores are sufficiently close for their guided modes to overlap, enabling the transfer of optical power through evanescent coupling. The coupling ratio is determined by the interaction length and taper geometry, allowing precise control of the output splitting ratio. For these reasons, we chose to use in our setup also a fused beam-splitter, the Thorlabs PNH1550R5A2 [87], with the aim of controlling the splitting ratio both through the temperature and the wavelength.

6.3.1 Wavelength Depedence

During preliminary experiments with the beam splitter in combination with the Eblana laser (see section 5.2.1), the measured extinction ratio did not match the expected value derived from an ideal 50:50 splitting ratio. This suggested a possible wavelength dependence of the BS. Although specified as a 50:50 device at 1550 nm, our results indicated that the splitting ratio at this wavelength deviated significantly from the nominal value.

To investigate this, we implemented a very intuitive experiment in which a tunable continuous-wave laser (the PurePhotonics PPCL590, see section 5.4.1) was the source of light entering the beam-splitter (after being attenuated by a few passive optical attenuators). At the two outputs of the BS, we measured the light intensity by means of two powermeters (*i.e.* devices that measure the optical power).

The result, depicted in figure 6.9, shows that the splitting ratio follows a linear, increasing trend with respect to the wavelength. According to the linear fit, the BS reaches $T = R = 0.5$ when the light enters it with a wavelength of 1564.02 nm.

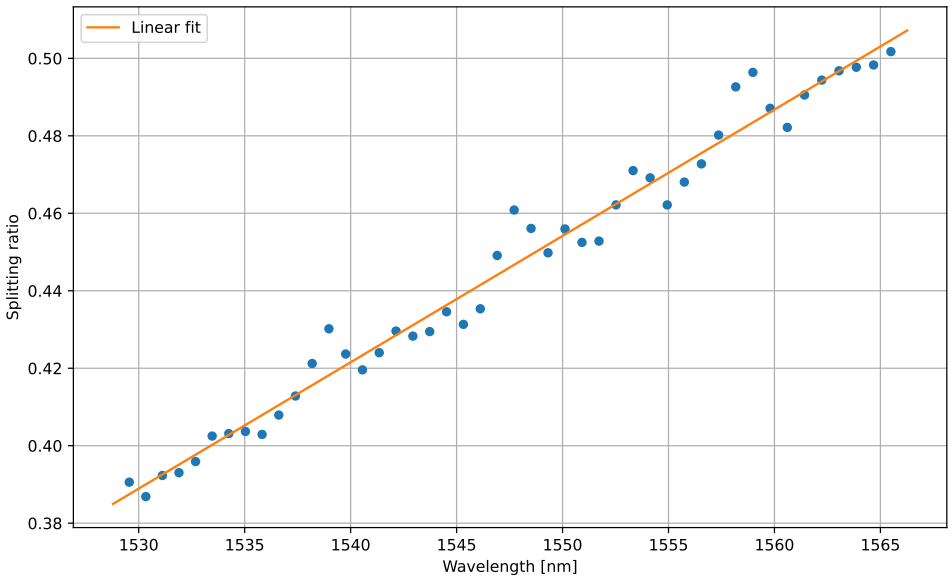

Figure 6.9: The experimental results of the splitting ratio of the fused beam-splitter in the range of wavelengths from 1529.16 nm to 1565.49 nm.

In the following step, we wanted to determine the extinction ratio achievable by the BS.
We used the same continuous-wave tunable laser to provide the input light, which was passed through an optical isolator and circulator before entering a Sagnac loop.

No phase modulation was applied, so the relative phase shift was $\Delta\varphi = 0$. The setup is shown in figure 6.10.

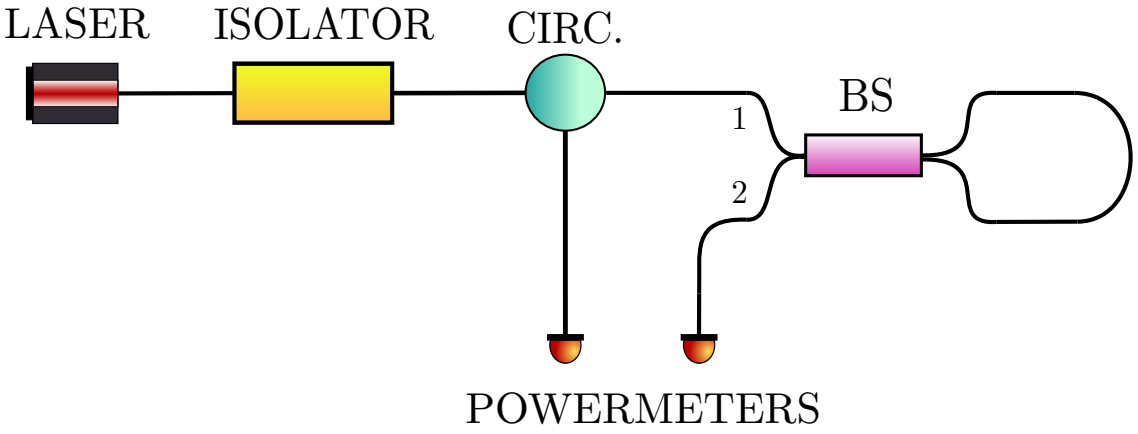

Figure 6.10: The setup used to calculate the extinction ratio (and the splitting ratio) by the BS employing continuous light and two powermeters.

According to the theoretical framework (presented in section 5.1.1), the output powers at the circulator and the second output port of the BS are given by:

$$P_1 = 4RT \tag{6.1}$$

$$P_2 = (T - R)^2 \tag{6.2}$$

For an ideal 50:50 BS ($R = T = 0.5$), the ratio $\frac{P_1}{P_2} = \frac{4RT}{(T-R)^2}$ corresponds exactly to the maximum extinction ratio achievable at the output 2 of our setup (see figure 5.4), as we obtain the same equation (equation 5.19). In the practical experiment, all measured optical powers were normalized with respect to the laser input power to mitigate the effects of laser intensity fluctuations.

The PurePhotonics PPCL590 was tuned in the same wavelength range (from 1529.163 nm to 1565.49 nm) with a step of ≈0.817 nm. We developed an automated procedure that involved, at each wavelength step, turning on the laser, waiting for its stabilization, and recording the optical powers with the two powermeters. For each setting, 10 sequential measurements were acquired over a fixed interval and stored in a `.txt` file. After acquisition, the laser was turned off before moving to the next step.

By using the extinction ratio, we can derive the relative splitting ratio, as shown in section 5.1.1. In figure 6.12 we show the splitting ratio that we derived from the measurement from the extinction ratio and the splitting ratio that we actually measured, already shown in figure 6.9. It is clear that they both follow the same linear trend.

From the graphs shown in figure 6.9, 6.11 and 6.12, it is clear that the splitting

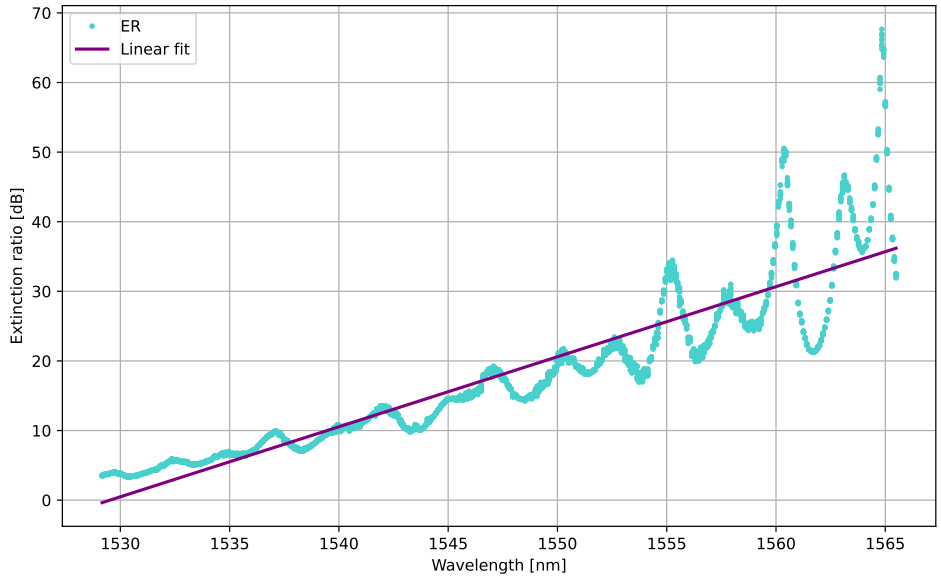

Figure 6.11: The extinction ratio achievable by the fused beam-splitter in the range of wavelengths from 1529.16 nm to 1565.49 nm measure with the setup shown in figure 6.10.

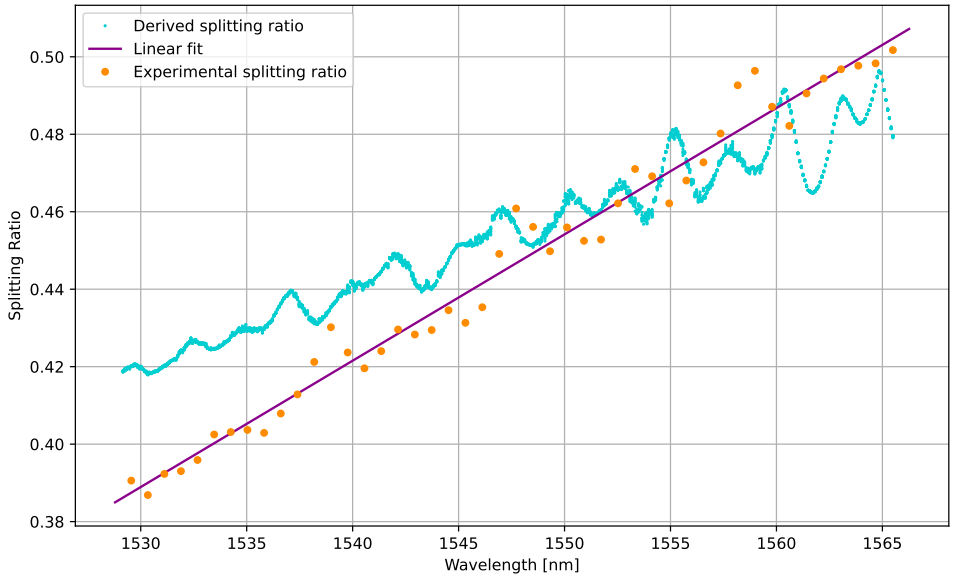

Figure 6.12: The splitting ratio of the fused beam-splitter (in orange) and the splitting ratio derived from the extinction ratio (in turquoise).

ratio (and therefore the extinction ratio) grows linearly with the wavelength in the considered range. However, we noticed the presence of "ripples" that deviate significantly from a linear fit. First, we verified that they were not due to oscillations

of the laser optical power by measuring the emitted power over a long interval of time, which turned out to be constant. Moreover, we observed similar effects in the datasheets of some optical components, although we did not have time to investigate this further. In particular, the isolator and the circulator used in the setups of figure 6.10 and figure 5.6 were the same. A future investigation may address whether this behavior is caused by a single component (and which one) or by their combination.

6.3.2 Extinction Ratios

Let's start this section by recalling the fact that the extinction ratio obtained with the phase modulation (introduced in section 6.2.1) is independent of the extinction ratio, and thus it is independent of the type of beam-splitter. For this reason, in this section we will deal only with the extinction ratio achievable by the splitting ratio.

The wavelength dependence that we introduced in the previous section justified a measure of the extinction ratio achievable by the setup with the light being emitted at different wavelengths. The range of wavelengths chosen was from 1537.397 nm to 1565.49 nm with steps of 0.78 nm. Figure 6.13 shows the result.

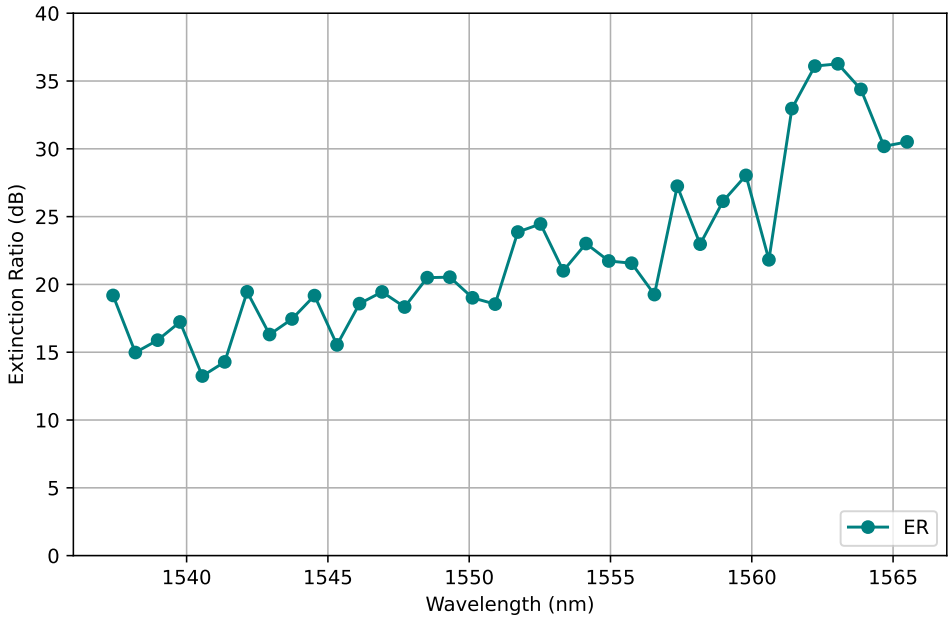

Figure 6.13: The extinction ratio deriving from the splitting ratio of the fused beam-splitter with different wavelengths.

The trend of the plot is expected, as it highlights a peak of the splitting ratio around 1564 nm, which is consistent with the results we obtained by using the continuous light and the powermeters. In particular, the trend is the same: we have an increase of the splitting ratio for increasing wavelengths, with a peak between 1560 nm and 1565 nm.
As a consequence, we decided to restrict the range of the wavelength to perform a second fine-tuning measurement. In this case, we considered the window between 1562.314 nm and 1563.047 nm. The plot in figure 6.14 shows the result.

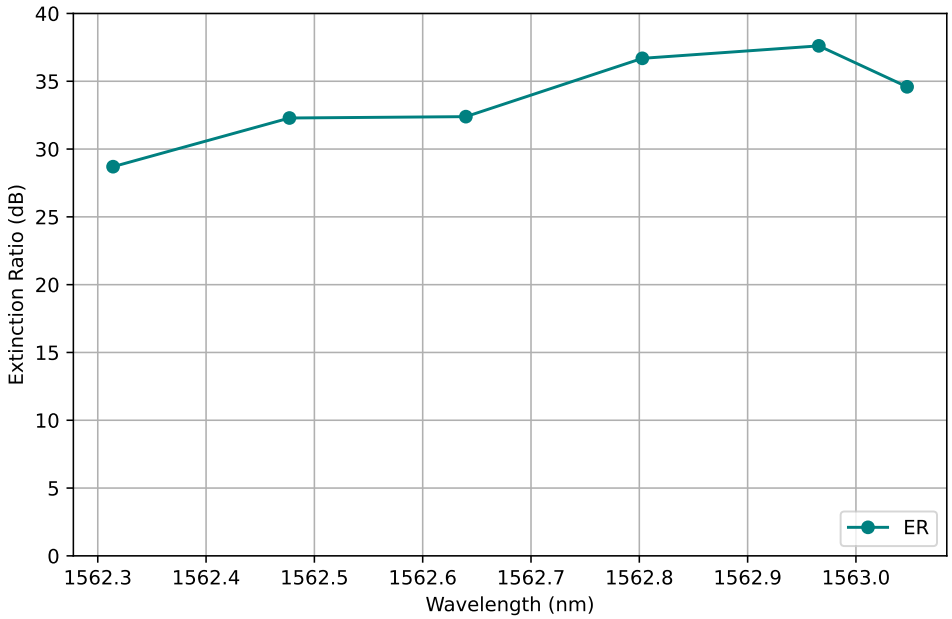

Figure 6.14: The fine-tuning of the extinction ratio with respect to the wavelength for the fused beam-splitter.

With the fine-tuning, we reached 37.61 dB with a wavelength of 1562.965 nm.

As outlined at the beginning of this section, the working principle of the fused beam-splitter suggested to us the possibility of changing the splitting ratio with the temperature, and therefore having a way to fine-tune the extinction ratio of the setup by heating or cooling down the beam-splitter.
For this reason, by using the optimal wavelength derived previously, we performed a scan over different temperatures using the procedure described in section 5.3.2, starting from 25 °C (ambient temperature) up to 40 °C, with a step of 2.5 °C. We show the results in figure 6.15.

This plot highlights an encouraging result: we were effectively able to control the splitting ratio, and therefore the splitting ratio , by changing the temperature of the

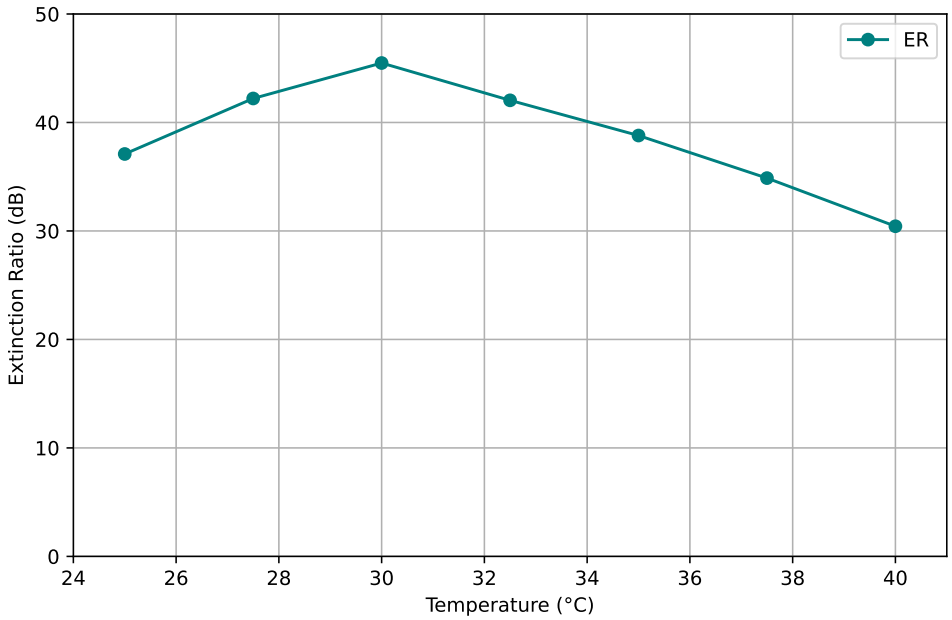

Figure 6.15: The extinction ratio achieved by controlling the splitting ratio of the fused beam-splitter with different temperatures.

beam-splitter (by the means of a Peltier cell). Starting from an extinction ratio of 37.61 dB, measured at 25°C, we achieved 45.48 dB at 30°C, resulting in an increase of almost 8 dB. After the peak, the extinction ratio descended almost linearly. It means that at 30°C we reached the closest point to a 50:50 splitting ratio, and the subsequent increase of the temperature resulted in an overshoot, leading to the decrease of the ER.
Having achieved 45.48 dB of extinction ratio means reaching a splitting ratio of $T = 0.4973$ and $R = 0.5027$, that corresponds to a precision of 99.46%.

7

Conclusion

Quantum Key Distribution is one of the most mature and promising quantum technologies. QKD is a key management security mechanism, meaning that its aim is to generate a random key and to deliver it to two legitimate users, by ensuring that eventual eavesdroppers are not able to retrieve it. As a fundamental feature, QKD achieves *unconditional security*, differentiating itself from the vast majority of mechanisms employed nowadays, able to guarantee only *computational security*.

The security of QKD relies on the properties of quantum mechanics, and in particular on the Uncertainty Principle and on the No-Cloning theorem, by encoding quantum states into photons. Starting from the first proposal by Bennett and Brassard in 1984, there have been massive developments in the last decades, with proposals of commercially available systems on one side and extremely sophisticated protocols on the other side.

Two of the main drawbacks of QKD are the vulnerability of the receivers (as over the years, several side-channel attacks targeting the detectors or other devices at the receiver's side have been proposed) and the range achievable. In particular, the impossibility to use the quantum analogue of classical telecommunication amplifiers significantly limits the distances that can be covered by a QKD link; this limit has been formalized by the PLOB bound.

These two problems found a solution with the proposal of Measurement-Device independent protocols: in particular, it has been shown that a protocol, named Twin-Field, overcomes the PLOB bound (in practice, doubling the achievable dis-

tance) and it is capable of distilling a secure cryptographic key even if the receiver is under the control of an adversary.

The working principle of Twin-Field relies on an interferometric measurement at the receiver's side, ideally placed in the middle between the two users, that work both as transmitters. The experimental implementation carries two major drawbacks regarding the phase of the light transmitted over the two arms of the interferometer: it has to be locked to a precise phase reference (usually provided by the receiver station), and the phases must be tracked (and eventually corrected) when they travel over long distances in optical fibers.

The family of protocols known as Post-Measurement Pairing protocols addresses phase locking and phase tracking by encoding the bits of the cryptographic keys in pairs of pulses that are close from the point of view of the arrival time. This ensures a relaxation on the need for having the phases locked and tracked, yet achieving similar results in terms of distance reached and still being measurement-device independent.
Their practical implementations involve a remarkable number of electro-optical components, as well as expensive lasers, especially the ones that provide the best results.

The aim of this thesis was to describe the efforts and the procedures realized to create an experimental source for Asynchronous-Pairing QKD. In particular, the main objective was to design a high-efficiency source in terms of the extinction ratio needed for practical implementations that employ the decoy states technique.

The technique used to achieve this goal was a Sagnac loop, an optical structure consisting of a beam splitter whose outputs are connected to form a closed loop, inside which an electro-optical phase modulator is placed. The fundamental idea was to control the electro-optical phase modulator by means of signals with half of the frequency of the laser pulses, allowing for a comparison between modulated and unmodulated pulses.

In a Sagnac loop, if the beam-splitter has two inputs, it is possible to differentiate the corresponding extinction ratios, as one depends on the precision of the modulation (*i.e.* the closer to π is the modulation applied, the higher the extinction ratio) and the other one relies on the characteristics of the beam-splitter (the closer to 50:50 is the splitting ratio, the higher the extinction ratio). The topology of the setup used allowed us to measure both.

By tuning the amplification of the electric signal driving the electro-optical phase modulator, we were able to reach an extinction ratio of 47.43 dB. As a remark, we want to highlight that this extinction ratio is independent of the splitting ratio of the beam-splitter in the Sagnac loop, meaning that it can be achieved regardless of the fabrication technique of the beam-splitter itself.
On the other hand, the extinction ratio measured on the other port of the beam-splitter was based on the splitting ratio of the optical device. In our experiments, we used a beam-splitter fabricated with micro-optical techniques and a fused beam-splitter, whose working principle relies on the evanescent field coupling, obtained by simultaneously fusing and tapering two optical fibers together. In addition to achieving high extinction ratios, our study explored the possibility of tuning the beam splitter's splitting ratio by employing light at different wavelengths or by controlling its operating temperature through a Peltier cell.

As expected, the use of the micro-optic beam splitter provided high extinction ratio values (>40 dB), independent of both the wavelength and the applied temperature. In contrast, the fused beam splitter exhibited a marked dependence on the wavelength, requiring fine-tuning to achieve optimal performance. Intuitively, due to its fabrication process, the splitting ratio of the fused beam splitter was also strongly temperature-dependent, which allowed us to adjust it and reach an extinction ratio of 45.48 dB.

With this work, we have shown the feasibility of implementing a high-efficiency source for the Asynchronous-Pairing QKD protocol, reaching extinction ratios above 40 dB through both phase modulation and splitting ratio control. We also observed the opposite behavior of micro-optic and fused beam splitters with respect to wavelength and temperature. In particular, while the micro-optic splitter remains stable under different conditions, the fused splitter is strongly affected by both parameters, offering a practical way to control and tune its performance, especially by adjusting the temperature.

References

[1] J. C. R. Licklider and W. E. Clark, "On-line man-computer communication," in *Proceedings of the May 1-3, 1962, Spring Joint Computer Conference*, ser. AIEE-IRE '62 (Spring). New York, NY, USA: Association for Computing Machinery, 1962, p. 113–128. [Online]. Available: https://doi.org/10.1145/1460833.1460847

[2] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[3] D. Tse, "How claude shannon invented the future," 2020. [Online]. Available: https://www.quantamagazine.org/how-claude-shannons-information-theory-invented-the-future-20201222/

[4] S. Singh, *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*, 1st ed. Doubleday, 1999.

[5] A. Einstein, "Über einen die erzeugung und verwandlung des lichtes betreffenden heuristischen gesichtspunkt," *Annalen der Physik*, vol. 322, no. 6, pp. 132–148, 1905.

[6] M. Planck, "Über das gesetz der energieverteilung im normalspektrum," *Annalen der Physik*, vol. 309, no. 3, pp. 553–563, 1901.

[7] U. Maurer and R. Renner, "Abstract cryptography," in *The Second Symposium on Innovations in Computer Science, ICS 2011*, B. Chazelle, Ed. Tsinghua University Press, 1 2011, pp. 1–21.

[8] B. Pfitzmann, M. Schunter, and M. Waidner, "Cryptographic security of reactive systems: (extended abstract)," *Electronic Notes in Theoretical Computer Science*, vol. 32, pp. 59–77, 2000, workshop on secure architectures and information flow. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1571066104000957

[9] R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols," in *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, 2001, pp. 136–145.

[10] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[11] National Institute of Standards and Technology, "Advanced encryption standard (aes)," U.S. Department of Commerce, FIPS Publication 197, November 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf

[12] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, p. 120–126, Feb. 1978. [Online]. Available: https://doi.org/10.1145/359340.359342

[13] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[14] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[15] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, p. 1484–1509, Oct. 1997. [Online]. Available: http://dx.doi.org/10.1137/S0097539795293172

[16] R. J. McEliece, "A public key cryptosystem based on algebraic coding theory," 1978. [Online]. Available: https://api.semanticscholar.org/CorpusID:56502909

[17] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik*. Berlin: Springer, 1932.

[18] M. Born, "Zur quantenmechanik der stoßvorgänge," *Zeitschrift für Physik*, vol. 37, no. 12, pp. 863–867, 1926.

[19] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Phys. Rev.*, vol. 47, pp. 777–780, May 1935. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRev.47.777

[20] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New high-intensity source of polarization-entangled photon pairs," *Phys. Rev. Lett.*, vol. 75, pp. 4337–4341, Dec 1995. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.75.4337

[21] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, "Ultrabright source of polarization-entangled photons," *Phys. Rev. A*, vol. 60, pp. R773–R776, Aug 1999. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.60.R773

[22] A. Anwar, C. Perumangatt, F. Steinlechner, T. Jennewein, and A. Ling, "Entangled photon-pair sources based on three-wave mixing in bulk crystals," *Review of Scientific Instruments*, vol. 92, no. 4, Apr. 2021. [Online]. Available: http://dx.doi.org/10.1063/5.0023103

[23] H. P. Robertson, "The uncertainty principle," *Phys. Rev.*, vol. 34, pp. 163–164, Jul 1929. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRev.34.163

[24] W. Heisenberg, "Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik," *Zeitschrift für Physik*, vol. 43, no. 3-4, pp. 172–198, 1927.

[25] W. K. Wootters, W. K. Wootters, and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, 1982. [Online]. Available: https://api.semanticscholar.org/CorpusID:4339227

[26] V. Bužek and M. Hillery, "Quantum copying: Beyond the no-cloning theorem," *Phys. Rev. A*, vol. 54, pp. 1844–1852, Sep 1996. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.54.1844

[27] R. Loudon, *The Quantum Theory of Light*, 3rd ed. Oxford: Oxford University Press, 2000.

[28] C. K. Hong, Z. Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," *Phys. Rev. Lett.*, vol. 59, pp. 2044–2046, Nov 1987. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.59.2044

[29] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. IEEE, 1984, pp. 175–179.

[30] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[31] B. Kraus, C. Branciard, and R. Renner, "Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses," *Phys. Rev. A*, vol. 75, p. 012316, Jan 2007. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.75.012316

[32] H.-W. Li, C.-M. Zhang, M.-S. Jiang, and Q.-Y. Cai, "Improving the performance of practical decoy-state quantum key distribution with advantage distillation technology," *Communications Physics*, vol. 5, no. 53, 2022.

[33] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology — EUROCRYPT '93*, T. Helleseth, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 410–423.

[34] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *2009 IEEE International Symposium on Information Theory*. IEEE, Jun. 2009, p. 1879–1883. [Online]. Available: http://dx.doi.org/10.1109/ISIT.2009.5205475

[35] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[36] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, p. 230501, Jun 2007. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.98.230501

[37] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 461, no. 2053, p. 207–235, Jan. 2005. [Online]. Available: http://dx.doi.org/10.1098/rspa.2004.1372

[38] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," *Physical Review Letters*, vol. 85, no. 2, p. 441–444, Jul. 2000. [Online]. Available: http://dx.doi.org/10.1103/PhysRevLett.85.441

[39] N. Laurenti, "Information theoretic key agreement," https://stem.elearning.unipd.it/pluginfile.php/793981/mod_resource/content/4/KeyAgreement.pdf, 2024, lecture 17 of the Information Security course, held by Prof. Nicola Laurenti in the Master's Degree in Cybersecurity at the University of Padova, Italy.

[40] Z. Du, G. Liu, X. Zhang, and X. Ma, "Advantage distillation for quantum key distribution," *Quantum Science and Technology*, vol. 10, no. 1, p. 015050, Dec. 2024. [Online]. Available: http://dx.doi.org/10.1088/2058-9565/ad9d75

[41] M. Canale, F. Renna, and N. Laurenti, "Qkd secrecy for privacy amplification matrices with selective individual attacks," 01 2011, pp. 52 304–52 304.

[42] R. Wolf, *Quantum Key Distribution: An Introduction with Exercises*, ser. Lecture Notes in Physics, vol. 988. Springer, Cham, 2021. [Online]. Available: https://doi.org/10.1007/978-3-030-73991-1

[43] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, "The universal composable security of quantum key distribution," 2004. [Online]. Available: https://arxiv.org/abs/quant-ph/0409078

[44] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, p. 43–47, Aug. 2017. [Online]. Available: http://dx.doi.org/10.1038/nature23655

[45] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, no. 1, Apr. 2017. [Online]. Available: http://dx.doi.org/10.1038/ncomms15043

[46] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, pp. 5932–5935, Dec 1998. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.81.5932

[47] T. van Leent, M. Bock, R. Garthoff, K. Redeker, W. Zhang, T. Bauer, W. Rosenfeld, C. Becher, and H. Weinfurter, "Long-distance distribution of atom-photon entanglement at telecom wavelength," *Phys. Rev. Lett.*, vol. 124, p. 010510, Jan 2020. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.124.010510

[48] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, "Experimental demonstration of memory-enhanced quantum

communication," *Nature*, vol. 580, no. 7801, p. 60–64, Mar. 2020. [Online]. Available: http://dx.doi.org/10.1038/s41586-020-2103-5

[49] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical Review Letters*, vol. 94, no. 23, Jun. 2005. [Online]. Available: http://dx.doi.org/10.1103/PhysRevLett.94.230504

[50] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, vol. 4, no. 10, p. 686–689, Aug. 2010. [Online]. Available: http://dx.doi.org/10.1038/NPHOTON.2010.214

[51] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys. Rev. A*, vol. 74, p. 022313, Aug 2006. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.74.022313

[52] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Physical Review A*, vol. 73, no. 2, Feb. 2006. [Online]. Available: http://dx.doi.org/10.1103/PhysRevA.73.022320

[53] F. Xu, B. Qi, and H.-K. Lo, "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system," *New Journal of Physics*, vol. 12, no. 11, p. 113026, Nov. 2010. [Online]. Available: http://dx.doi.org/10.1088/1367-2630/12/11/113026

[54] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Physical Review A*, vol. 74, no. 2, Aug. 2006. [Online]. Available: http://dx.doi.org/10.1103/PhysRevA.74.022313

[55] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar 2012. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.108.130503

[56] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, "Experimental measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 111, p. 130502, Sep 2013. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.111.130502

[57] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over 200 km," *Physical Review Letters*, vol. 113, no. 19, Nov. 2014. [Online]. Available: http://dx.doi.org/10.1103/PhysRevLett.113.190501

[58] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Physical Review Letters*, vol. 117, no. 19, Nov. 2016. [Online]. Available: http://dx.doi.org/10.1103/PhysRevLett.117.190501

[59] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, p. 400–403, May 2018. [Online]. Available: http://dx.doi.org/10.1038/s41586-018-0066-6

[60] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Experimental twin-field quantum key distribution over 1000 km fiber distance," *Phys. Rev. Lett.*, vol. 130, p. 210801, May 2023. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.130.210801

[61] R. Pound, "Frequency stabilization of microwave oscillators," *Proceedings of the IRE*, vol. 35, no. 12, pp. 1405–1415, 1947.

[62] R. W. P. Drever, J. L. Hall, F. V. Kowalski, J. Hough, G. M. Ford, A. J. Munley, and H. Ward, "Laser phase and frequency stabilization using an optical resonator," *Appl. Phys. B*, vol. 31, no. 2, pp. 97–105, 1983.

[63] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, "600-km repeater-like quantum communications with dual-band stabilization," *Nature Photonics*, vol. 15, no. 7, p. 530–535, Jun. 2021. [Online]. Available: http://dx.doi.org/10.1038/s41566-021-00811-0

[64] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, "Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon

interference," *PRX Quantum*, vol. 3, p. 020315, Apr 2022. [Online]. Available: https://link.aps.org/doi/10.1103/PRXQuantum.3.020315

[65] P. Zeng, H. Zhou, W. Wu, X. Ma, and altri, "Mode-pairing quantum key distribution," *Nature Communications*, vol. 13, no. 1, p. 3903, 2022, open Access.

[66] K. Azuma, K. Tamaki, and W. J. Munro, "All-photonic intercity quantum key distribution," *Nature Communications*, vol. 6, p. 10171, 2015. [Online]. Available: https://doi.org/10.1038/ncomms10171

[67] V. B. Braginsky, Y. I. Vorontsov, and K. S. Thorne, "Quantum nondemolition measurements," *Science*, vol. 209, no. 4456, pp. 547–557, 1980. [Online]. Available: https://www.science.org/doi/abs/10.1126/science.209.4456.547

[68] X. Ma and M. Razavi, "Alternative schemes for measurement-device-independent quantum key distribution," *Physical Review A*, vol. 86, no. 6, p. 062319, 2012. [Online]. Available: https://doi.org/10.1103/PhysRevA.86.062319

[69] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," *Nature Communications*, vol. 5, no. 1, Apr. 2014. [Online]. Available: http://dx.doi.org/10.1038/ncomms4732

[70] L. Zhou, J. Lin, Y.-M. Xie, Y.-S. Lu, Y. Jing, H.-L. Yin, and Z. Yuan, "Experimental Quantum Communication Overcomes the Rate-Loss Limit without Global Phase Tracking," *Phys. Rev. Lett.*, vol. 130, no. 25, p. 250801, 2023.

[71] H.-T. Zhu, Y. Huang, H. Liu, P. Zeng, M. Zou, Y. Dai, S. Tang, H. Li, L. You, Z. Wang, Y.-A. Chen, X. Ma, T.-Y. Chen, and J.-W. Pan, "Experimental mode-pairing measurement-device-independent quantum key distribution without global phase locking," *Physical Review Letters*, vol. 130, no. 3, Jan. 2023. [Online]. Available: http://dx.doi.org/10.1103/PhysRevLett.130.030801

[72] J.-L. Bai, Y.-M. Xie, Y. Fu, H.-L. Yin, and Z.-B. Chen, "Asynchronous measurement-device-independent quantum key distribution with hybrid source," *Optics Letters*, vol. 48, no. 13, p. 3551, Jun. 2023. [Online]. Available: http://dx.doi.org/10.1364/OL.491511

[73] X.-Y. Zhou, J.-R. Hu, J.-J. Wang, Y. Cao, C.-H. Zhang, and Q. Wang, "Enhancing the performance of mode-pairing quantum key distribution by wavelength division multiplexing," *Opt. Express*, vol. 32, no. 10, pp. 18 366–18 378, 2024.

[74] W. Cui, C. Yang, G. Huang, and R. Jiao, "Mode-pairing quantum key distribution based on wavelength division multiplexing in multi-user networks," , vol. 99, no. 8, p. 085112, Aug. 2024.

[75] H.-T. Zhu, Y. Huang, W.-X. Pan, C.-W. Zhou, J. Tang, H. He, M. Cheng, X. Jin, M. Zou, S. Tang, X. Ma, T.-Y. Chen, and J.-W. Pan, "Field test of mode-pairing quantum key distribution," *Optica*, vol. 11, no. 6, p. 883, Jun. 2024. [Online]. Available: http://dx.doi.org/10.1364/OPTICA.520697

[76] L. Zhang, F. Xu, F.-H. Xu, J.-W. Pan *et al.*, "Experimental mode-pairing quantum key distribution surpassing the repeaterless bound," *Physical Review X*, vol. 15, no. 2, p. 021037, May 2025.

[77] G. Sagnac, "L'éther lumineux démontré par l'effet du vent relatif d'éther dans un interféromètre en rotation uniforme," *Comptes Rendus*, vol. 157, pp. 708–710, 1913.

[78] ——, "Sur la preuve de la réalité de l'éther lumineux par l'expérience de l'interféromètre tournant," *Comptes Rendus*, vol. 157, pp. 1410–1413, 1913.

[79] E. Photonics, *EP1550-DM-H Manual*, 2025, available at: https://shop.laserdiodesource.com/wp-content/uploads/2025/04/EP1550_DM_H-1574865896.pdf.

[80] R. W. Boyd, *Nonlinear Optics, Fourth Edition*, 4th ed. USA: Academic Press, Inc., 2020.

[81] iXBlue Photonics, "Dr-dg-20-ho photline driver: 22 gbps high output voltage driver," PDF datasheet, 2015, available online: https://www.hikari-trading.com/ixblue/file/IX052.pdf.

[82] Y. Namihira, T. Kawazawa, and H. Wakabayashi, "Incident polarization angle and temperature dependence of polarization and spectral response characteristics in optical fiber couplers," *Applied Optics*, vol. 30, pp. 1062–1069, 03 1991.

[83] W. Zhu, G. Zhou, Z. Yi, H. You, X. Miao, C. Liu, and D. Wang, "Photo-thermal induced wide-range and high-precision tunable dispersion

turning point in tapered fiber coupler," *Opt. Express*, vol. 33, no. 12, pp. 24 678–24 691, Jun 2025. [Online]. Available: https://opg.optica.org/oe/abstract.cfm?URI=oe-33-12-24678

[84] D. D. Pollock, "Thermoelectric phenomena," in *CRC Handbook of Thermoelectrics*, D. M. Rowe, Ed. CRC Press, 1995, ch. 2.

[85] P. Photonics, *PPCL590 Manual*, 2021, available at: https://www.purephotonics.com/wp-content/uploads/Manual-PPCL590-v1.pdf.

[86] HaphiT, "Pm filter coupler (fpfc) — specifications and ordering information," PDF brochure, 2023, available online: `https://www.haphit.com/pdf/FPFC_PM_Filter_Coupler.pdf`.

[87] Thorlabs, "Polarization-maintaining fiber optic coupler (1550 ± 15 nm, 50:50 split, 25 db per, fc/apc)," PDF brochure, 2023, available online: `https://www.haphit.com/pdf/FPFC_PM_Filter_Coupler.pdf`.

Acknowledgments

This work would not have been possible without my two supervisors, Marco Avesani and Yoann Piétri. Your patience, guidance, and knowledge supported me throughout this experience, and I want to thank you deeply. I am also grateful to the QuantumFuture group for welcoming me so warmly and for providing help whenever I needed it. It was a real pleasure to spend six months in the lab with you. Finally, I would like to thank Prof. Giuseppe Vallone for introducing me to the world of quantum communications and for giving me the opportunity to develop my thesis within the QuantumFuture group.

I ricordi di questi cinque anni saranno legati alle persone che mi hanno circondato. Vorrei ringraziare, in particolare, Alberto, Alessia, Daniele, Mattia, Mattia, Melissa, Nicola e Nicolò per tutte le serate, i viaggi e le esperienze incredibili passate insieme.

L'inizio e la fine del mio percorso universitario coincidono con l'inizio e la fine dell'avventura come istruttore nel *Dolo1909Pianiga*. Non ci sarebbe abbastanza spazio per ringraziare tutte le persone meravigliose incontrate in questi cinque anni. Voglio esprimere la mia gratitudine agli *Esordienti 2009*, agli *Esordienti 2010*, agli *Esordienti 2012* e ai *Pulcini 2014* per tutto il tempo che abbiamo condiviso, in campo e fuori.
Un ringraziamento speciale ad Alessandro, mentore, collega e amico.

Infine, vorrei ringraziare la mia famiglia per il supporto costante che mi hanno dato e che mi continuano a dare. Un ringraziamento particolare a Roberto, Giovanna ed Emanuele.