Università degli Studi di Napoli *Federico II*

Università di Camerino

Consiglio Nazionale
delle Ricerche

DOTTORATO DI RICERCA IN QUANTUM TECHNOLOGIES

Ciclo XXXIV

Coordinatore: prof. Francesco Tafuri

High-dimensional protocols for practical quantum key distribution over metropolitan fiber links

Settore Scientifico Disciplinare FIS/03

Dottorando
Ilaria Vagniluca

Tutore
Alessandro Zavatta

Anni 2018/2021

Preface

This doctoral dissertation (or thesis) is submitted as final fulfillment of the requirements of the Ph.D. program in "Quantum Technologies", offered by University of Naples "Federico II" and co-financed by University of Camerino and the National Institute of Optics of the National Research Council of Italy (CNR-INO). The Ph.D. educational program, cycle number 34, started in November 2018 and concluded in October 2021, with an overall duration of three years.

The results of the research activity pursued within my Ph.D. and presented in this thesis, have been carried out mainly at the CNR-INO laboratories in Florence (Italy), in close cooperation with the Department of Photonics Engineering from the Technical University of Denmark (DTU Fotonik). Specifically, my experimental work has been based at the CNR-INO main center (Arcetri headquarter) and at the auxiliary CNR-INO facilities located at LENS, the European Laboratory for Nonlinear Spectroscopy of University of Florence, all situated in the Florence metropolitan area. In addition, four months of research activity were carried out abroad, at DTU Fotonik, as a Visiting Ph.D. Student at the High-Speed Optical Communications group, supported by the European Union Erasmus Plus grant "Universities for EU Projects" (SEND Mobility Consortium, from March to July 2019). My work has been mainly supervised by Dr. Alessandro Zavatta from CNR-INO and University of Florence, and by Assistant Prof. Davide Bacco from DTU Fotonik.

The research activity carried out by my group and collaborators has led, during the years of my Ph.D., to the establishment of the Quantum Communication Center at CNR-INO and to the launch of the CNR spin-off company QTI, Quantum Telecommunications Italy.

Furthermore, many results achieved during my Ph.D. emerged from fruitful collaborations with other research groups and institutions, such as the National Institute of Metrological Research of Turin (Italy) and the Department of Applied Physics from University of Geneva (Switzerland).

List of Publications

D. Ribezzo, I. Vagniluca, N. Biagi, *et al.*, "Quantum key distribution network between three countries", manuscript under preparation.

D. Bacco, N. Biagi, I. Vagniluca, T. Hayashi, A. Mecozzi, C. Antonelli, L. K. Oxenløwe, and A. Zavatta, "Characterization and stability measurement of deployed multicore fibers for quantum applications", *Photonics Research*, vol. 9, p. 1992-1997 (2021).

D. Bacco, I. Vagniluca, D. Cozzolino, S. M. M. Friis, L. Høgstedt, A. Giudice, D. Calonico, F. S. Cataliotti, K. Rottwitt, and A. Zavatta, "Towards fully-fledged quantum and classical communication over deployed fiber with up-conversion module", *Advanced Quantum Technologies*, vol. 4, art n. 2000156 (2021).

K. Wang, I. Vagniluca, J. Zhang, S. Forchhammer, A. Zavatta, J. B. Christensen, and D. Bacco, "Round-robin differential phase-time-shifting protocol for quantum key distribution: theory and experiment", *Physical Review Applied*, vol. 15, art. n. 044017 (2021).

I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D. Bacco, "Efficient time-bin encoding for practical high-dimensional quantum key distribution", *Physical Review Applied*, vol. 14, art. n. 014051 (2020).

D. Bacco, I. Vagniluca, B. Da Lio, N. Biagi, A. Della Frera, D. Calonico, C. Toninelli, F. S. Cataliotti, M. Bellini, L. K. Oxenløwe, and A. Zavatta, "Field trial of a three-state quantum key distribution scheme in the Florence metropolitan area", *EPJ Quantum Technology*, vol. 6, art. n. 5 (2019).

Contents

Introduction

Quantum key distribution (QKD) enables the establishment of private keys between remote users, by exploiting a quantum technology rather than the conventional key distribution protocols. Based on the working principles of quantum theory, the secret key bits are generated as a result of a process where information is encoded on a set of quantum states of light, which are then distributed between the users and finally destroyed through quantum measurements. Remarkably, the innovative approach of QKD totally differs from the current technologies for key distribution, as its security can be mathematically derived from the physical laws of quantum mechanics, rather than being based on uncertain assumptions of computational hardness. For this reason, QKD offers the unmatched benefit of not being affected by the present nor future advancements in both classical and quantum computing, whose potential faculties are seriously threatening the current and well-established protocols for key distribution [1–3].

Starting from its first formulation in the 1980s [4, 5], the research field behind QKD has undergone considerable development through the last decades, making it the most advanced among the other emerging quantum technologies, both at the theoretical level as well as in terms of practical implementations. Many QKD protocols have been successfully demonstrated over long transmission distances, often including quantum networks, usually based on fiber optic infrastructures but also involving satellite communications [6–12]. At short distance, when the loss on the quantum signals is negligible, QKD allows the secure distribution of private keys up to tens of megabits per second [13, 14]. In the present digital era, the unmatched security benefits offered by QKD have made its strategic applications of great interest, not only among the academic community, but also involving private companies as well as government institutions, including standardization institutes [15–18].

However, despite the notable advances of the last twenty years, QKD technologies and services are still rarely adopted outside the laboratories. This is mainly due to the high costs of implementation and to the demanding requirements in terms of

environmental disturbances, such as a low noise in the communication channel and a high stability of the optical equipment, necessary to carry out the quantum measurements with sufficient accuracy over the whole acquisition time. Therefore, designing more efficient protocols and introducing alternative solutions for practical QKD, capable of tolerating more noise while maintaining, at the same time, high performances in terms of key generation rate and security, is an essential task towards the establishment of reliable QKD technologies for widespread applications. Moreover, implementing in-field tests of QKD protocols under real-world conditions, is a fundamental step towards making the quantum technologies more and more compatible with the already-existing infrastructures for optical communications.

During the past three years, our research activity has been mainly focused on metropolitan-scale QKD, based on fiber optic links. In particular, we have been able to implement in-field tests of QKD over an installed single-mode fiber in the metropolitan area of Florence [19, 20], where we also addressed the issue of compatibility between the current QKD technologies and classical optical communication, by testing the coexistence of quantum and classical signals multiplexed in the same fiber. In the meanwhile, in the laboratory, we designed and tested novel protocols and setups for practical high-dimensional QKD. In general, high-dimensional protocols [21] enable higher information capacity per quantum signal, which allows the enhancement of the key generation rate as well as the tolerance for the environmental noise. In particular, my research has been focused on high-dimensional QKD with information encoding on time and phase degrees of freedom, being such encoding techniques the most compatible with standard single-mode fibers over metropolitan-scale links. Specifically, we successfully demonstrated an efficient scheme for high-dimensional QKD, requiring a very simplified setup [22], and an improved round-robin protocol with high-dimensional encoding, exhibiting higher tolerance for the noise that typically affects the quantum measurements [23].

In the following Chapters, we will firstly present the fundamental elements of QKD theory, and the experimental tools and methods needed to realize our setups for quantum communication. Next, the contributions of this thesis will be described, analyzing the motivations behind each work and discussing the achieved results.

1

Quantum key distribution: theory and overview

In this Chapter are presented the main elements and working principles of quantum key distribution (QKD). Specifically, the motivations and the theoretical concepts behind this emerging quantum technology, are reported in the first two Sections. Next, the focus is shifted to a specific protocol of QKD, the BB84, although most of the notions discussed for this protocol, such as the eavesdropping strategies and the decoy-state method, can be applied also in other QKD protocols that are relevant for this thesis. In particular, many general concepts apply also in the round-robin protocol for differential-phase-shift QKD, that will be described with more detail in Chapter 4. Then, the discussion of Section 1.3 is focused on some specific variants of the BB84 protocols, that are relevant for this thesis: the asymmetric BB84 protocol with four or three states, with one decoy state and finite-key analysis. The theoretical principles behind high-dimensional QKD are presented in Section 1.4, where we discuss also the BB84 variant with four-dimensional encoding. In conclusion, a brief overview on the other QKD protocols, and on the state of the art of current QKD implementations, is presented in the last Section of this Chapter.

1.1 Motivations

Private keys are widely used in many digital applications of the information technology. These secret strings of bits serve, on one hand, for authentication purposes, by enabling the recognition of the legitimate users that are allowed to access some service or product. On the other hand, private keys are also employed in encryption algorithms for encoding (and decoding) the confidential information, that is transmitted through public networks or untrustworthy channels. Indeed, when a secret

message is properly encrypted, it becomes meaningless for whoever is intercepting it, except for the legitimate owners of the encryption key, i.e., the only ones allowed to recover the original message.

Some typical examples of every day use of private keys are electronic mail and messaging applications, cloud computing, pay television and streaming services, e-commerce, home banking and secured payment transactions. Private keys (short-term session keys) are also established within the HTTPS protocol, widely used on the Internet to protect the authentication, the integrity and privacy of the data flow between the client and the server when accessing a website, especially important over insecure networks such as public Wi-Fi access points [24].

The practical effectiveness of private-key cryptography is strongly related to the efficiency of the encryption algorithm and to the size of the key. The longer is the private key, the more difficult is to guess it, since the average amount of attempts necessary to find a N-long random bit sequence (brute-force attack) grows exponentially as 2^{N-1}. This exponential behaviour makes the brute-force attack highly unpractical, since it would require a very long time and a very high budget to be implemented even for relatively small key sizes[1]. It is mathematically proven that information-theoretic security of encrypted communication can be achieved only with the one-time pad (OTP) private-key cryptography [28, 29], which requires, for each message to be sent, a truly-random private key of the same length of the message, to be used only once. Due to these demanding requirements on the private key, the OTP is rarely employed and other private-key cryptosystems are preferred in every day applications, such as those based on the Advanced Encryption Standard or AES (as recommended by the National Institute of Standards and Technology since the early 2000s), which utilizes key sizes of 128, 192 and 256 bits [30, 31].

A fundamental challenge of private-key cryptography, such as AES and OTP cryptography, is the requirement of a random and secret key to be previously distributed among the users, which means that also distant parties must rely on a secure method to exchange such a key over untrustworthy communication channels. This is often referred as the so-called key distribution problem [32].

[1]It has been shown that an exponential speed-up for the brute-force attack is impossible even in quantum computation [25]. For instance, the quantum search algorithm introduced by Grover can provide only a quadratic speed-up as compared with classical search algorithms ($\sim 2^{N/2}$ rather than $\sim 2^N$ average number of attempts) [26]. Therefore, even though we do not know if (or when) quantum search algorithms will ever become practically relevant, doubling the key size is a sufficient countermeasure to preserve the security of private keys [27].

1.1.1 Current key distribution and security issues

Currently, to distribute the private keys between distant users, public-key cryptography (or asymmetric cryptography) is adopted [33]. The central point is the use of asymmetric encryption algorithms to encode the private key: a public key is employed for encoding the secret bits, while a different key is necessary in the decoding process. The decoding key does not need to be distributed since it is randomly generated *in loco* and stored by the user, who publicly discloses the corresponding encoding key, after having it computed from the decoding key. Thanks of the use of one-way algorithms, based on functions that are easy to compute but difficult to invert, the inverse process of computing the decoding key from the public one, is a computationally hard problem. This means that, to retrieve the decoding key, an exponential or sub-exponential amount of steps, with respect to the public-key size, is required with the mathematical algorithms of current knowledge.

Some typical systems of public-key cryptography are the RSA (Rivest, Shamir and Adleman), based on the hard problem of the prime factorization of large integers, and the ECC (Elliptic Curve Cryptography), based on the discrete logarithm problem [34–36]. Currently, the recommended sizes for the public key are 1024, 2048 and 3072 bits for RSA and 160, 224 and 256 bits for ECC [31, 37].

It has to be noted that, in general, asymmetric encryption algorithms are more computational expensive and more resource consuming than private-key (or simply "symmetric") encryption algorithms, which is the reason why public-key cryptography is rarely used for encoding large amounts of information and is rather employed for distributing only the private keys, necessary for authentication purposes or for the more efficient symmetric encryption algorithms, such as the AES cryptography. However, as mentioned above, the security of public-key cryptography is not mathematically provable, since it relies only on our current experience about the present-day technological limitations and costs. Indeed, it has not yet been possible to demonstrate that more efficient mathematical algorithms, capable of solving the above-mentioned hard problems in a shorter (i.e., not exponential) computational time, do not exist in principle. Although such algorithms have not yet been introduced (presumably) on classical computers and supercomputers, it is a matter of fact that quantum algorithms able to provide and exponential speed-up (i.e., from an exponential to a polynomial time) to the resolution of the prime factorization and the discrete logarithm problems, have been developed by Shor in the Nineties [38,39] and experimentally tested in prototypes of small-scale quantum machines [40–43].

This means that, as far as we know today, it is only a matter of time (estimated as ~ 20 years from now [1]) until large-scale quantum computers with enough computational power, or even classical supercomputers, would be able to crack the current key distribution protocols. As a consequence, if somebody starts storing the public keys of the present day, he/she could likely retrieve the corresponding private keys in the next decades, and potentially access to information that will be still confidential at the time.

A partial countermeasure to these threats is offered by post-quantum cryptography [2], which utilizes public-key encryption algorithms based on different kinds of computationally hard problems, to whom the already known quantum algorithms do not provide a more efficient resolution than their classical counterparts. A plan for the selection and standardization of these novel public-key cryptosystems has started in 2016 and it is expected to take several years for the full migration [3, 27]. This approach is more conservative and thus more compatible with the existing infrastructure for key distribution, providing high rates and long transmission distances. However, it does not offer a solution to the above mentioned issue of long-term security.

Based on a totally different approach, QKD offers, on the other hand, a promising and permanent solution to the key distribution problem, since it enables to mathematically evaluate the amount of transmitted information that is secure and thus suitable for establishing the private key [4, 5]. As opposed to standard or post-quantum public-key cryptography, the security of QKD can be derived from the fundamental laws of quantum physics, which is considered the most well-tested theory in human history. In other words, the secrecy of the distributed keys is independent from the amount of resources (present or future, classical or quantum) available to a potential eavesdropper of the keys, as long as the only constrain to the eavesdropping attacks is given by the laws of physics. Furthermore, the combination of QKD and information-theoretic secure schemes for private-key encryption, such as OTP cryptography, makes it possible to achieve unconditional security of communication.

Although the security benefits promised by QKD surely outperforms those offered by post-quantum cryptography, it is more likely (especially from a practical point of view) that both of the two technologies will be combined together, in the near future, to build a modern infrastructure for quantum-safe cryptography. For instance, post-quantum cryptography could be exploited to distribute preferably the short-term private keys, useful to provide also the initial authentication necessary

to perform a QKD protocol [44].

1.2 General concepts

Similarly to the other emerging technologies based on quantum information theory, QKD exploits the non-classical features of single microscopic physical systems, like superposition and entanglement, to perform some practical tasks of information processing.

Specifically, QKD takes advantage of the non-classical properties of single photons or, more generally, quantum states of light, in order to monitor and evaluate any potential eavesdropping activity over the private-key information that is transmitted between distant sites. Before focusing on the specific protocols of QKD that are relevant for this thesis, the more general and fundamental concepts behind this technology and field of study are presented in this section. The concepts here recalled are extensively analyzed in several quantum mechanics and quantum information books [45–47] and in recent review articles of quantum cryptography [44, 48, 49].

1.2.1 Superposition states and features

The working principles of QKD are based on the concept of quantum superposition. According to this principle, a measurement of a physical system prepared in an arbitrary quantum state, generally returns an aleatory output. Therefore, a single act of measuring is not enough to totally identify an unknown quantum state, since no statistics can be obtained from a single measurement output. Moreover, the post-measurement state is said to collapse into the corresponding eigenstate of the measurement operator (or observable), meaning that the act of measurement generally alters the initial state, by causing the loss of its original definition. Therefore, many physical systems, each one prepared in an identical copy of the original state, would be necessary to totally specify an arbitrary quantum state with a given measurement operator.

In the specific case of interest for QKD theory, we can consider an arbitrary quantum state $|\psi\rangle$, normalized to 1, belonging to the two-dimensional Hilbert space. A physical system described by $|\psi\rangle$ is called qubit and the unitary vector state $|\psi\rangle$ can be depicted as an arbitrary dot situated on the surface of the Bloch sphere, whose north and south poles are identified, respectively, with the qubits $|0\rangle$ and

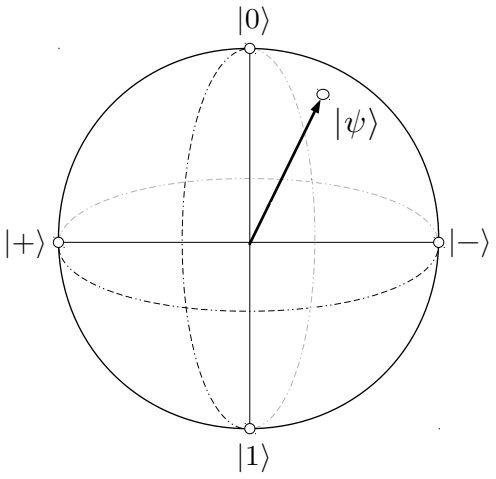


Figure 1.1: The Bloch sphere is used to depict the two-dimensional Hilbert space, whose physical states, or unitary vectors $|\psi\rangle$ (also called qubits) are identified with the dots situated on the spherical surface.

$|1\rangle$ (see Figure 1.1). Being a pure state, $|\psi\rangle$ is surely the eigenstate of a certain observable, and only when that exact observable is measured on $|\psi\rangle$, the measurement output will not be aleatory. Otherwise, if the given observable is, for instance, the Pauli operator $\hat{\sigma}_z$ (whose eigenstates are $|0\rangle$ and $|1\rangle$), the measurement output will be aleatory among the two eigenvalues of $\hat{\sigma}_z$ (± 1, corresponding to $|0\rangle$ and $|1\rangle$ respectively), depending on the probability amplitudes defining $|\psi\rangle$:

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \ , \tag{1.1}$$

where $c_0,\ c_1 \in \mathbb{C}$ and $|c_0|^2 + |c_1|^2 = 1$. By measuring the observable $\hat{\sigma}_z$, $|\psi\rangle$ is said to be projected on the $\mathcal{Z}$ measurement basis, also called computational basis, including the two orthonormal states $\big\{|0\rangle, |1\rangle\big\}$. With only a single measurement available, if the output of the $\mathcal{Z}$ basis projection is (for instance) $|0\rangle$, then it is possible to deduce only that $|\psi\rangle$ is a qubit with $c_0 \neq 0$, i.e., any dot on the Bloch sphere except for the qubit $|1\rangle$, which is the one orthogonal to $|0\rangle$. Therefore, $|\psi\rangle$ can be any qubit which is not orthogonal to $|0\rangle$.

The main idea behind QKD is to take advantage of the superposition principle, by encoding classical information on a given set of non-orthogonal quantum states. Consequently, different bases of the Hilbert space, corresponding to non-commuting observables, have to be involved in a QKD protocol. In particular, considering the $\mathcal{Z}$ basis $\big\{|0\rangle, |1\rangle\big\}$, we see that all the qubits sited on the equator of the Bloch sphere are those exhibiting the maximum uncertainty when projected on the $\mathcal{Z}$ basis, giving equal probabilities of the possible outcomes: $|\langle 0|\psi\rangle|^2 = |\langle 1|\psi\rangle|^2 = 1/2$. Thus, if we pick any couple of opposite vectors lying on the equator to define another basis of

orthonormal states, this basis and the $\mathcal{Z}$ basis are said to be mutually unbiased bases of the two-dimensional Hilbert space. A typical example is the $\mathcal{X}$ basis $\{|+\rangle, |-\rangle\}$, whose states are the eigenvectors of $\hat{\sigma}_x$, and are defined as follows:

$$|\pm\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle \pm |1\rangle\Big) \ . \tag{1.2}$$

In the general case of a d-dimensional Hilbert space, the $\mathcal{Z}$ basis is now composed by d orthornormal states $\big\{|z_0\rangle,\ |z_1\rangle,\ ...,\ |z_{d-1}\rangle\big\}$ and any d-level quantum system can be described by the arbitrary unit vector $|\psi\rangle$, now called qudit, which can be expressed as

$$|\psi\rangle = \sum_{i=0}^{d-1} c_i |z_i\rangle \ , \tag{1.3}$$

where $c_i \in \mathbb{C}$ and $\sum_i |c_i|^2 = 1$. Two d-dimensional bases $\mathcal{Z}$ and $\mathcal{X}$ of the qudit space are said to be mutually unbiased, if the non-orthogonal states $\big\{|z_0\rangle,\ |z_1\rangle,\ ...,\ |z_{d-1}\rangle\big\}$ and $\big\{|x_0\rangle,\ |x_1\rangle,\ ...,\ |x_{d-1}\rangle\big\}$ satisfy the general relation of equal probabilities

$$\Big|\langle z_i|x_j\rangle\Big|^2 = \frac{1}{d} \ , \tag{1.4}$$

with $i, j = 0,\ ...,\ d-1$. Although it is possible to define at most $(d+1)$ mutually unbiased bases in a d-dimensional Hilbert space, only two bases are involved in most QKD protocols, with only few exceptions [50, 51].

In addition to the intrinsic uncertainty of the measurement output, another feature offered by non-orthogonal quantum states is the fact that there is not any cloning operator able to act successfully on a set of states which are not orthogonal. This principle, referred as the no-cloning theorem, implies that the information encoded on a set of non-orthogonal states, as in the case of QKD, can not be duplicated by cloning the quantum states, since this would apply successfully only on a subset of states, keeping the original untouched, but would definitely alter the remaining subset of states, thus introducing detectable errors attributable to eavesdropping activity.

In order to prove that a unitary operator for cloning arbitrary quantum states

can not exist[2], we can consider the unitary transformations

$$\begin{aligned}\hat{U}\Big(|\psi\rangle_A|b\rangle_B\Big) &= \mathrm{e}^{\imath\alpha}|\psi\rangle_A|\psi\rangle_B \ , \\ \hat{U}\Big(|\phi\rangle_A|b\rangle_B\Big) &= \mathrm{e}^{\imath\alpha'}|\phi\rangle_A|\phi\rangle_B \ ,\end{aligned} \tag{1.5}$$

where α and α' are generic phases in $[0, 2\pi)$, A is the physical system prepared in two different states $|\psi\rangle$, $|\phi\rangle$ that we would like to copy and B is an ancillary physical system, prepared in the initial state $|b\rangle$ (normalized), that we would like to turn into the state associated to the system A, while keeping unaltered the state of A, as shown in both transformations. Since $|b\rangle$ is normalized, the product of the initial states is

$$\Big(\langle\phi|_A \ \langle b|_B\Big)\Big(|\psi\rangle_A|b\rangle_B\Big) = \langle\phi|\psi\rangle \ , \tag{1.6}$$

but since $\hat{U}$ is unitary ($\hat{U}^\dagger\hat{U} = \mathbb{1}$), we have also

$$\begin{aligned}\Big(\langle\phi|_A \ \langle b|_B\Big)\Big(|\psi\rangle_A|b\rangle_B\Big) &= \Big(\langle\phi|_A \ \langle b|_B\Big)\hat{U}^\dagger\hat{U}\Big(|\psi\rangle_A|b\rangle_B\Big) = \\ &= \mathrm{e}^{\imath(\alpha-\alpha')} \ \Big(\langle\phi|_A \ \langle\phi|_B\Big)\Big(|\psi\rangle_A|\psi\rangle_B\Big) = \\ &= \mathrm{e}^{\imath(\alpha-\alpha')} \ \Big(\langle\phi|\psi\rangle\Big)^2 \ .\end{aligned} \tag{1.7}$$

However, the equality between Equations 1.6 and 1.7 is satisfied only by $\langle\phi|\psi\rangle = 1$ (implying $|\phi\rangle = \mathrm{e}^{\imath\beta}|\psi\rangle$, i.e., the two physical states are the same, differing only by a global phase β) and by $\langle\phi|\psi\rangle = 0$ (the two quantum states are orthogonal).

As an example, in the specific case of the two-dimensional Hilbert space, we can see that the transformation able to successfully clone the two orthogonal states belonging to the $\mathcal{Z}$ basis,

$$\begin{aligned}|0\rangle_A|b\rangle_B \ &\longrightarrow \ |0\rangle_A|0\rangle_B \ , \\ |1\rangle_A|b\rangle_B \ &\longrightarrow \ |1\rangle_A|1\rangle_B \ ,\end{aligned} \tag{1.8}$$

[2]The unitariety here is required for preserving the norm of the unitary vector states. In other words, it is required for transforming a pure state into another pure state. Remarkably, the no-cloning theorem is also applicable to non-unitary cloning operators: even in this case, cloning non-orthogonal states is only possible at the expense of finite loss of fidelity [45].

can not work for an arbitrary superposition state $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$, not orthogonal to $|1\rangle$ and $|0\rangle$. According to Equation 1.8, we obtain

$$|\psi\rangle_A|b\rangle_B = \Big(c_0|0\rangle + c_1|1\rangle\Big)_A|b\rangle_B \;\longrightarrow\; c_0|0\rangle_A|0\rangle_B + c_1|1\rangle_A|1\rangle_B \;, \tag{1.9}$$

which is clearly different from the desired output

$$\begin{aligned} |\psi\rangle_A|\psi\rangle_B &= \Big(c_0|0\rangle + c_1|1\rangle\Big)_A\Big(c_0|0\rangle + c_1|1\rangle\Big)_B = \\ &= c_0^2|0\rangle_A|0\rangle_B \;+\; c_1^2|1\rangle_A|1\rangle_B \;+\; c_0c_1\Big(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B\Big) \;, \end{aligned} \tag{1.10}$$

implying also that the original state of the system A has been altered by the transformation.

1.2.2 Information and entropy

As already mentioned, QKD enables to mathematically quantify how secure is the private key that is transmitted to the legitimate users. Notably, this is equivalent to the evaluation of how uncertain are the private-key bits, from the point of view of a potential eavesdropper (with unlimited resources and whose only constrain is given by the laws of physics).

The interconnection between information and uncertainty is a fundamental concept in classical information theory: the more uncertain is the outcome of a random variable, the more information is learned when that variable is evaluated. The Shannon entropy measures the amount of bits that are learned, on average, with a single evaluation of a random variable X, considered all its possible outcomes:

$$H(X) = -\sum_x p_x \log_2(p_x) \;, \tag{1.11}$$

where p_x are the probabilities of the possible outcomes x. Notably, if X can return only one output with $p_x = 1$ (no uncertainty), then no information is learned and $H(X) = 0$. Conversely, if the outcomes have all the same probability, the uncertainty is maximum and so is the Shannon entropy, giving $H(X) = \log_2 n$ with n the number of outcomes (and $p_x = 1/n$). Thus, the Shannon entropy defines not only the average content of information that is gained from the evaluation of X, but it also measures the degree of uncertainty about X before learning its value.

In the specific case of a binary variable (only two possible outcomes) it is usual to define the binary entropy function of the probability $h(p)$, being p and $1-p$ the probabilities of the two outcomes:

$$H_{bin}(X) = h(p) = -p\log_2(p) - (1-p)\log_2(1-p) \ . \tag{1.12}$$

Considering now two random variables X and Y, the overall information acquired by evaluating both variables is defined by the joint Shannon entropy,

$$H(X,Y) = -\sum_{x,y} p_{x,y}\log_2(p_{x,y}) \ . \tag{1.13}$$

If X and Y are independent variables, then $p_{x,y} = p_x \cdot p_y$ and their contributions to the joint Shannon entropy simply add to each other, thanks to the properties of log, giving $H(X,Y) = H(X) + H(Y)$. Otherwise, $H(X,Y) \leq H(X) + H(Y)$ generally holds, and the amount of information that the two variables have in common is defined by their mutual information

$$I(X,Y) = H(X) + H(Y) - H(X,Y) \ . \tag{1.14}$$

Considering, for instance, the value of Y already learned, than the amount of uncertainty that is left about the knowledge of X, is given by the conditional entropy,

$$H(X|Y) = H(X,Y) - H(Y) \ , \tag{1.15}$$

which returns zero if X is a given function of Y, while it is maximum (and equal to $H(X)$) if X is independent from Y. Therefore, their mutual information can be equivalently defined as $I(X,Y) = H(X) - H(X|Y)$.

Up to now, classical aleatory variables X, Y have been taken into consideration. However, in order to measure the degree of uncertainty describing the mixtures of quantum states, the Von Neumann entropy has to be evaluated instead of the Shannon entropy:

$$S(\rho) = -\mathrm{tr}\Big(\rho\log_2(\rho)\Big) = -\sum_i \lambda_i \log_2(\lambda_i) \ , \tag{1.16}$$

where ρ is the density operator describing the generic mixed state and λ_i are its eigenvalues. For pure states, $\rho = |\psi\rangle\langle\psi| = \rho^2$ and the uncertainty is zero ($S = 0$),

while for maximum mixtures of states (uniformly mixed states) the uncertainty is maximum and so is S, returning $S = \log_2(d)$ with d the Hilbert space dimension.

1.2.3 Definition of security

According to an ideal protocol of QKD, at the end of the process the two legitimate parties would share the same identical string of ℓ bits, uniformly distributed, as the private key, totally unknown to a potential eavesdropper of the key. In other words, all the possible strings with size ℓ must be equally probable from the point of view of the eavesdropper. Thus, the overall state of the system including all the three parties A, B (or Alice and Bob) and the eavesdropper E (or Eve) can be represented by

$$\rho_{ABE}^{ideal} = \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} \Big(|k\rangle_A\langle k| \otimes |k\rangle_B\langle k| \Big) \otimes \rho_E \ , \tag{1.17}$$

where k is the perfect key string shared by Alice and Bob, $\mathcal{K}$ is the key space with $|\mathcal{K}| = 2^\ell$ possible strings (each having the same probability $1/|\mathcal{K}|$) and ρ_E is the system hold by Eve, totally uncorrelated from the key bits.

In an actual protocol, Alice's string can be slightly different from the one hold by Bob, the possible strings in the key space can occur with not exactly the same probability, and Eve's system can exhibit some little correlation with the private key:

$$\rho_{ABE} = \sum_{k_A, k_B \in \mathcal{K}} \Big(P_{k_A,k_B} |k_A\rangle_A\langle k_A| \otimes |k_B\rangle_B\langle k_B| \otimes \rho_E^{(k_A,k_B)} \Big) \ , \tag{1.18}$$

where k_A, k_B are the key strings hold by Alice and Bob, respectively, with a probability P_{k_A,k_B}.

Consequently, the security of a QKD protocol can be parametrized by its deviaton, ε, from the ideal protocol. Thus, the aim of the security analysis of a QKD protocol is to mathematically prove that ρ_{ABE} and ρ_{ABE}^{ideal} are the same, with an approximation ε. A composable[3] definition of security is given by the trace-distance metric, defined as

$$D(\rho_1, \rho_2) = \frac{1}{2} \mathrm{tr} |\rho_1 - \rho_2| \ , \quad \text{with} \quad |O| \equiv \sqrt{O^\dagger O} \ . \tag{1.19}$$

[3]Here, composability means that the security of the private key is ensured whatever its application may be [48].

Therefore, the private key is said to be ε-secure if the deviation of ρ_{ABE} from ρ_{ABE}^{ideal}, in terms of trace distance, is smaller than ε. Moreover, the private key is said to be ε_{corr}-correct if the probability that Alice's and Bob's strings are different, $P_{k_A \neq k_B}$, is smaller than ε_{corr}. At the same time, the private key is said to be ε_{sec}-secret if the trace-distance deviation between ρ_{AE} and ρ_{AE}^{ideal} (defined analogously as above, as the overall state of Alice an Eve without Bob) is smaller than ε_{sec}. If a QKD protocol is ε_{corr}-correct and ε_{sec}-secret, then it is ε-secure, with $\varepsilon = \varepsilon_{corr} + \varepsilon_{sec}$. The parameters ε_{sec} and ε_{corr} are called, respectively, secrecy and correctness parameters, and in typical QKD protocols are usually taken as small as 10^{-9}.

1.2.4 The secret fraction

In QKD protocols, it is assumed that Alice and Bob are connected via a quantum channel, where quantum states are transmitted, and a classical communication channel, to exchange the instructions necessary to process the key string from the quantum measurements. The quantum channel is, by hypothesis, totally under Eve's control, meaning that she can manipulate the quantum states and take part actively in the quantum communication in place of Alice and Bob. Conversely, the classical channel is assumed to be authenticated[4], thus Alice and Bob are sure to talk to each other and not with Eve, who can not alter their conversation, even though she can listen to it, since no encryption of messages is assumed *a priori*. Therefore, all the communication transmitted in the classical channel is supposed to be public. Furthermore, the quantum channel is typically noisy, thus quantum communication errors can occur even without the presence of eavesdropping activities.

After N rounds of quantum communication between Alice and Bob, an initial raw key of ℓ_R bits (or, more generally, of ℓ_R symbols) is established at both sides, as shown in Figure 1.2. Then, classical post-processing procedures including error correction and privacy amplification, are performed in order to distill, from the raw key symbols, a final string of secure bits of length ℓ, with the help of public conversation between the two parties. The secret fraction r is defined as the amount of secure bits that can be extracted from each symbol of the raw key, in the asymptotic case of large N:

[4]To authenticate the classical channel, Alice and Bob need a private key previously agreed. However, since this authentication is typically required for a short time only (the time necessary to complete the QKD protocol), then a short-term private key, pre-distributed via standard (or, even better, post-quantum) public-key cryptography, is considered suitable for this purpose [44].

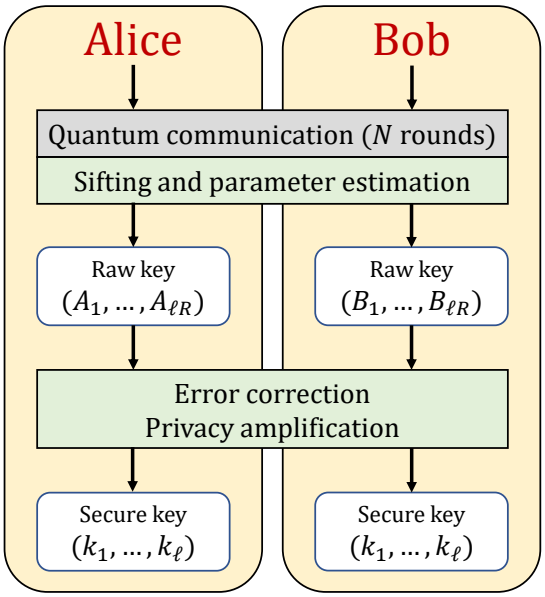


Figure 1.2: Schematic of a QKD protocol. Classical post-processing is used to extract the secure key from the initial raw key. Green rectangles denote operations carried out with the help of public conversations in the classical channel, as opposed to the N rounds of quantum communication, that are performed on the quantum channel.

$$r = \lim_{N\to\infty} \frac{\ell}{\ell_R} \ . \tag{1.20}$$

From a practical point of view, the above definition is analogous to the one involving the secure-key rate K and the raw-key rate K_R, with the two rates given, respectively, in bits and symbols per unit of time:

$$K = K_R \cdot r \ . \tag{1.21}$$

The secret fraction is the most significant quantity in a QKD protocol, and the aim of the security proof is to provide an explicit expression for r, depending on the specific protocol, on the security parameter ε and on some other quantities measured and estimated during the initial part of the protocol.

During error correction, Alice's and Bob's raw keys (which typically differ a little from each other, due to the errors) are processed in order to extract two identical strings (with a failure probability ε_{corr}), by publicly disclosing, at the same time, the minimum amount of information about their raw keys. In the following, one-way classical post-processing is assumed, meaning that one of the two parties is chosen to hold the reference key and to publicly transmit instructions to the other party, who manipulates their raw key according to the established procedure, without giving

any feedback[5]. It has been proven that the fraction of perfectly correlated bits that can be extracted from a list of partially correlated symbols, is bounded by the mutual information between Alice's and Bob's raw keys, defined in Section 1.2.2:

$$I(A,B) = H(A) + H(B) - H(A,B) = H(A) - H(A|B) \ , \tag{1.22}$$

where A and B are the random variables related to Alice's and Bob's raw-key symbols. In the specific case of direct one-way post-processing, where Alice tells Bob how to act on his ray key, then the right side of Equation 1.22 can be read in the following way: the amount of raw-key information that Alice has to sacrifice is at least as large as the uncertainty of Bob about Alice's raw key (assumed that he knows his own raw key). Nonetheless, the theoretical bound $I(A,B)$ is usually not reached by practical codes for one-way error correction, and more accurate estimates on the bits to be lost during the process have to be evaluated for each specific code.

The privacy amplification step is required to bring down Eve's information about the corrected raw key shared by Alice and Bob. Currently, the procedures able to amplify privacy in a provable way are those based on two-universal hash functions, where Alice and Bob apply to their keys a publicly announced function belonging to the two-universal set [44,48]. Afterwards, both Alice and Bob end up with a shorter key, but Eve's knowledge about it has dropped to such a level that the probability that she can guess it correctly is roughly $1/|\mathcal{K}|$, with $\mathcal{K}$ the key space.

The amount of raw key bits to be lost during privacy amplification is the determined by the information leaked in the quantum channel, that depends on the assumptions on Eve's possible strategies. When considering collective attacks on the quantum channel, Eve attacks each round of the quantum communication independently from all the others (yet using the same strategy for every round), by exploiting her ancillary system E. Then, she can keep her ancillae stored in a quantum memory until any later time convenient to her, before measuring them with a collective measurement. For instance, she can wait until the end of classical post-

[5]The theoretical bounds on the secret fraction can be improved when considering two-way post-processing, in which both parties are allowed to send information. Moreover, most of the efficient algorithm for error corrections that are actually implemented (like Cascade, based on the parity-check of key blocks) require two-way communication [44, 48, 52]. However, given the complexity of the mathematical derivation of general bounds for two-way post-processing, the bounds of the one-way case are usually taken into account in most security proofs of quantum key distribution. This is also in agreement with the general assumption of the worst-case scenario, under which the security proofs are usually derived.

processing, in order perform the most convenient measurement, compatible on what she knows from the public conversation between Alice and Bob. Thus, the generic bound for the bit loss during direct one-way privacy amplification, is given by maximizing, among all of Eve's possible measurements, the Holevo quantity $\chi(A, \rho_E)$, which measures the mutual information between Alice's raw key and the state of Eve's ancillae ρ_E:

$$\chi(A, \rho_E) = S(\rho_E) - \sum_a p(a) S(\rho_{E,a}) \ , \tag{1.23}$$

where S is the Von Neumann entropy (given in Equation 1.16), while a denotes the symbols of Alice's raw key, distributed with probability $p(a)$, with $\rho_{E,a}$ the corresponding state of Eve's ancillae, after having attacked the corresponding round of quantum communication ($\rho_E = \sum_a p(a)\rho_{E,a}$).

When considering a more general class of attacks on the quantum channel, called coherent attacks, Eve's ancillary system is subjected to a joint interaction with all the rounds of the quantum communication, instead of an individual (and independent) interaction as it is assumed for collective attacks. Nonetheless, in many cases of interest, it turns out that the bound on the secret fraction is exactly the same as for collective attacks. This is due to the fact that, in many protocols of QKD (yet, not all protocols), including the BB84, the state describing the $N \to \infty$ rounds of quantum communication can be transformed into a tensor product of the states that are related, each one, to a single round. Notably, to do so, the states describing the single rounds have to be uncorrelated. Therefore, Eve has no practical advantage in attacking each round jointly or separately. In a more general framework, the same conclusion can be proven by invoking the exponential De Finetti theorem [48].

To sum up, the general formula for the secret fraction, in a QKD protocol with direct one-way post-processing, is given as follows:

$$r = I(A, B) - \max_{\text{Eve}} \chi(A, \rho_E) \ . \tag{1.24}$$

Notably, if $r \leq 0$, no secure key can be established with the key distribution protocol, that has to be aborted.

1.3 The BB84 protocol

In the previous section, the general concepts behind the working principle of a QKD protocol were presented. From now on, we will focus on a specific family of protocols, based on the first QKD scheme, the BB84 protocol (proposed by Bennet and Brassard in 1984 [4]) and on its later variants.

In the following, after recalling the main steps of the BB84 protocol, we will discuss the possible eavesdropping attacks and corresponding countermeasures to be taken into account in the security analysis. Specifically, the secret key bounds with decoy-state method in a finite-key scenario will be reported, since they are used in the main contributions presented in this thesis. Moreover, the generalization of the BB84 protocol in a high-dimensional Hilbert space will be presented. Most of the notions reported in this section are further analysed in many review articles of quantum key distribution [44,48,49] and in some recent works on BB84 protocol [9,53–57].

In the original BB48 protocol, the four quantum states from $\mathcal{Z}$ and $\mathcal{X}$ bases (as introduced in Section 1.2.1) are used for bit encoding:

$$0 \longrightarrow \begin{cases} |0\rangle \\ |+\rangle \end{cases} \quad , \quad 1 \longrightarrow \begin{cases} |1\rangle \\ |-\rangle \end{cases} \quad . \tag{1.25}$$

Quantum communication: preparation. Alice chooses two uniformly random strings of bits of length N: the bit string $x = x_1...x_N \in \{0,1\}^N$ and the basis string $\beta = \beta_1...\beta_N \in \{0,1\}^N$. Then, she encodes each bit x_i by preparing the corresponding quantum state $\hat{\mathrm{H}}^{\beta_i}|x_i\rangle$, with $\hat{\mathrm{H}}$ the Hadamard unitary operator ($\hat{\mathrm{H}}|0\rangle = |+\rangle$, $\hat{\mathrm{H}}|1\rangle = |-\rangle$). In this way, when $\beta_i = 0$ she encodes the bit x_i in an eigenstate of the $\mathcal{Z}$ basis, when $\beta_i = 1$ she encodes the bit x_i in an eigenstate of the $\mathcal{X}$ basis, in agreement with the the encoding relation 1.25. Then, the N qubits so prepared are forwarded to Bob through the quantum channel.

Quantum communication: measurement. Bob chooses a uniformly random string of bits $\beta' = \beta'_1...\beta'_N \in \{0,1\}^N$. Then, he measures the incoming qubit $|x_i\rangle$ by projecting it on the $\mathcal{Z}$ or $\mathcal{X}$ basis depending on the value $\beta'_i = 0$ or $\beta'_i = 1$, respectively. From this projective measurement, based on the encoding relation 1.25, he obtains the output bit x'_i. Notably, if no errors have occurred,

if $\beta'_i = \beta_i$ the equality $x'_i = x_i$ holds with probability 1, otherwise ($\beta'_i \neq \beta_i$) it holds with probability 1/2, being the bits totally uncorrelated due to the mutually unbiased bases. If, for some reason (e.g., losses in the quantum channel or in the measurement apparatus), the qubit $|x_i\rangle$ does not produce any measurement output, the i-th event is discarded. If, for some reason (e.g., a double click in the measurement apparatus), the qubit $|x_i\rangle$ returns more than one measurement output, the i-th event is not discarded, but it is given a random output $x'_i = 0$ or $x'_i = 1$, with 1/2 probability (random assignment)[6].

Sifting (basis reconciliation). After the N rounds of quantum communication, the exchange of information between Alice and Bob moves to the classical channel. Bob tells Alice which ones of the events $i = 1, ..., N$ were not discarded, and Alice and Bob publicly share their basis strings β and β'. Then, both parties discard all the events with $\beta'_i \neq \beta_i$. The resulting strings of bits, $s = \{x_i \mid \beta'_i = \beta_i\}$ and $s' = \{x'_i \mid \beta'_i = \beta_i\}$, are called sifted keys, and their size, for large N, is typically $\lesssim N/2$, due to the uniform randomness of the basis strings.

Parameter estimation. Alice and Bob pick a random subset of events j from their sifted keys, with 1/2 probability for each event to be picked. This random subset, with typical size $\lesssim N/4$, is used for parameter estimation. To do so, Alice and Bob publicly share their sifted key bits s_j and s'_j, for each j in the selected subset of events. Then, they measure the error rate by evaluating the fraction of wrong events ($s_j \neq s'_j$) within the selected subset. If the outcome is beyond the threshold of maximum tolerable error rate, the protocol is aborted. Otherwise, the protocol can proceed, and Alice and Bob use the experienced error rate to estimate, in the worst-case scenario, the amount of information leaked to Eve. They define, as raw keys, their remaining bits of sifted key that were not included in the selected subset. The raw key size is typically $\ell_R \lesssim N/4$.

It has to be noted that, however, it is not strictly necessary for Alice and Bob to publicly announce a subset of sifted key bits for evaluating the error rate, since it can be precisely estimated also during the following step of error correction, at the cost of disclosing some amount of raw key information [48].

[6]The random assignment is a countermeasure against the security loophole that is opened up when the double-click events are simply discarded (double-click attacks) [58].

Error correction and privacy amplification. Finally, based on the results of the parameter estimation, Alice and Bob perform the error correction code and privacy amplification procedure (as already discussed in Section 1.2.4), in order to distill, from their raw keys, a final secure key of length $\ell \leq \ell_R$.

1.3.1 Eavesdropping strategies

Notably, when the error rate goes beyond a fixed threshold, the protocol is automatically aborted, even if the errors are all resulting from the intrinsic noise in the quantum channel or in the measurement apparatus, and not from an actual eavesdropper. The reason of this is the pessimistic assumption that all experienced errors are due to Eve's activities and not to the channel itself, since the eavesdropper is, by hypothesis, an almighty adversary whose only constrains are the physical laws. Therefore, Eve's attacks can take advantage of the imperfections in the quantum channel (which is totally under her control) and, in the most pessimistic scenario, she can even replace it with an ideal quantum channel introducing no errors[7].

The most trivial strategy among Eve's possibilities in BB84 protocol, is the intercept-and-resend attack [4], where Eve measures the qubits $|x_i\rangle$ with a uniformly random choice of bases $\mathcal{Z}$ and $\mathcal{X}$, and she forwards her projection output $|y_i\rangle$ to Bob. With this strategy she introduces, on average, a 0.25 error rate in the sifted key. As a consequence, even in the case when the 0.25 error rate is simply due to the intrinsic noise in the quantum channel, no secure key can be distributed with the BB84 protocol, that is aborted. Thus, from a practical point of view, the higher is the maximum error rate tolerable in a given protocol, the higher is the intrinsic channel noise that still enables the distribution of a secure key.

The maximum tolerable error rate in the BB84 protocol can be evaluated from the bound for the secret fraction, whose generic expression, under the coherent attack scenario, was given in Equation 1.24. Since the BB84 is based on qubits (two-dimensional Hilbert space) the random variables A, B related to Alice's and Bob's raw keys are binary variables and the Shannon entropy $H(\cdot)$ becomes the binary entropy function $h(\cdot)$, from Equation 1.12. Moreover, since Alice's bit string $x = x_1...x_N$ is uniformly random (i.e., same amount of 0 and 1), then also the raw

[7]Moreover, even in the cases where the measurement devices are previously calibrated, the loss and the noise of the measurement setup are usually included in the quantum channel, since Alice and Bob have no means to distinguish them from those originating from the channel. Consequently, they are attributed to Eve.

keys are uniformly random, assuming that the orthogonal qubits undergo the same loss in the quantum channel (symmetric channel assumption). Thus, $h(A) = h(B) = \log_2 2 = 1$. The amount of bits to be lost during perfect one-way error correction is $h(A|B) = h(B|A) = h(e)$, where e is the error rate, thus giving $I(A, B) = 1 - h(e)$. Furthermore, the amount of information leaked to Eve is also equal to $h(e)$, as she can can acquire information on the raw key only at the cost of introducing errors. Then,

$$r = 1 - 2 \cdot h(e) \tag{1.26}$$

and the error rate threshold[8] to obtain $r \geq 0$, results into $e \leq 0.110$.

However, imperfect error correction is often taken into account, by introducing the term $\text{leak}_{EC}(e) \geq h(e)$ to better estimate the loss of bits during this step. Furthermore, more generally, a decoupling is made between the bit error rate e_{bit} (or qber), related to raw key errors (to be addressed during error correction), and the phase error rate e_{ph}, related to the amount of information leaked to Eve, to be cancelled during privacy amplification:

$$r = 1 - \text{leak}_{EC}(e_{bit}) - h(e_{ph}) \ . \tag{1.27}$$

For instance, the phase error rate in the $\mathcal{Z}$ basis is defined, for the signals measured in $\mathcal{Z}$ basis, as the hypothetical error rate that would be experienced if the same signals were measured in the mutually-unbiased $\mathcal{X}$ basis. In the original BB84, the phase error rate in the $\mathcal{Z}$ basis is equivalent to the bit error rate in $\mathcal{X}$ basis, which, in turn, is assumed to be equal to the bit error rate in $\mathcal{Z}$ basis, hence we have $e_{ph} = e_{bit} \equiv e$ [44].

Notably, the above bounds are valid only when the physical systems carrying the information can be described accurately by the qubits from $\mathcal{Z}$ and $\mathcal{X}$ bases. Unfortunately, this applies to single photons only, and not to generic attenuated pulses of light. If the BB84 is not implemented with a single photon source, then additional eavesdropping attacks must be taken into account in the security proof. In particular, Eve can take advantage of the loss in the quantum channel, by means of beam splitting attacks, since a beam splitter acts on light pulses without introducing errors in the raw key. Moreover, Eve could replace the lossy channel with a lossless one, and put an equivalent beam splitter immediately outside of Alice's setup. In these cases, the channel loss acts as a so-called side channel, i.e., a not-

[8] With two-way classical post-processing, the error rate threshold raises to 0.200 [59].

monitored channel leaking information to Eve and leaving it unnoticed. Conversely, in the single-photon case, channel loss does not leak any information to Eve, since any splitted qubit causes the event to be automatically discarded.

If perfect single-photon sources are not available, then the security proof of the BB84 protocol can be derived under the assumption of a more general source, described by a mixture of Fock states

$$\rho_s = \sum_{n=0}^{\infty} P(n)|n\rangle\langle n| \ . \tag{1.28}$$

Notably, a laser source is not described by ρ_s, being described with good approximation by the coherent state $|\alpha\rangle$ (pure state) that is, instead, a coherent superposition of Fock states:

$$|\alpha\rangle = \mathrm{e}^{-\mu/2} \sum_{n=0}^{\infty} \frac{(\sqrt{\mu}\mathrm{e}^{i\theta})^n}{\sqrt{n!}}|n\rangle \ , \tag{1.29}$$

with $\alpha = \sqrt{\mu}\mathrm{e}^{i\theta}$, where $\mu = |\alpha|^2$ is the mean photon number and θ is the phase [60]. However, the mixture can be obtained by introducing a continuous randomization of the phase in the coherent state:

$$\rho_\mu = \frac{1}{2\pi}\int_0^{2\pi} d\theta \ |\alpha\rangle\langle\alpha| = \mathrm{e}^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}|n\rangle\langle n| \equiv \sum_{n=0}^{\infty} P_\mu(n)|n\rangle\langle n| \ , \tag{1.30}$$

where $P_\mu(n) = |\langle n|\alpha\rangle|^2 = \mathrm{e}^{-\mu}\mu^n/n!$ is the probability distribution of Fock states in the coherent state. The security proof for the BB84 protocol with a source described by ρ_μ, can be derived by considering Eve's optimal strategy, where she acts differently based on the actual photon number of each pulse, that she is able to measure without introducing perturbations on the quantum states (photon-number splitting attacks). The weight of each Fock component in the raw key is then given by $Q_n = P_\mu(n)Y_n$, where the yield Y_n describes Eve's action (or the channel behaviour) on that Fock component. Only the detections coming from single-photon pulses, Q_1, can be taken into account for distilling a provably secure key, since it is the only Fock component to whom Eve's activities produce detectable errors. From multi-photon pulses, Eve can get all the information without introducing errors, thanks to beam splitting. From zero-photon pulses Eve gets no information, since they can give at most a random outcome at Bob's side (due to random dark counts). Therefore, Eve can stop all the pulses with $n = 0$ and split all the pulses with $n \geq 2$, keeping a

photon for herself and forwarding the remaining photons to Bob. Since $\sum_n Q_n = 1$ must hold, she can also stop some (yet not all) of the pulses with $n = 1$, in order to minimize Q_1. So, by assuming that all the experienced errors come from the single-photon pulses, then $e = \sum_n Q_n e_n = Q_1 e_1$ is the overall error rate. Therefore, the bound for the secret fraction becomes [48]

$$r = Q_1 \left[1 - h\left(\frac{e}{Q_1} \right) \right] - \mathrm{leak}_{EC}(e) \ . \tag{1.31}$$

Similarly to the case of channel loss for not-truly single photon sources, other side-channel attacks, often referred as hacking attacks [61], may arise from the weaknesses of practical implementations of the BB84 protocol, which make it deviate from the assumptions of the security proof. A typical example are the Trojan horse attacks, in which Eve can probe and guess the setups of Alice and Bob by injecting some light into them and measuring the reflected signal to acquire extra information on the raw key. To avoid side-channel attacks, any piece of equipment involved in each specific implementation, has to be properly characterized, isolated and protected from the outside. Moreover, *ad-hoc* countermeasures (e.g., additional components or extra characterization), depending on the specific setup, have to be adopted to counteract each hacking attack, once it has been noticed. However, a definitive solution against all the possible side-channel attacks arising from imperfect or untrustworthy components, can be solely found in device-independent and measurement-device-independent protocols of QKD [62–64]. Notably, also conventional cryptosystems for standard key distribution may suffer from side-channel attacks [44].

1.3.2 Decoy-state method

The decoy-state method [65–67] is a very efficient resource for QKD systems lacking of truly single-photon sources, since it enables to detect the photon number splitting attacks from some additional parameters to be estimated during the protocol. As a result, Eve has to put a limit on her beam splitting attacks if she does not want the protocol to be aborted, thus leading to a higher bound for the secret fraction than the one given in Equation 1.31.

In the decoy-state protocol, the phase-randomized source ρ_μ generates attenuated light pulses which are totally identical to each other, except for their mean photon number μ, which is randomly chosen, for each quantum state to be prepared, among

different values ($\mu_k = \mu_1,\ \mu_2,\ \mu_3, ...$). The additional values of μ to be included in the protocol are referred as decoy states, while the pulses belonging to the μ_1 distribution are called signal states. After the N rounds of quantum communication, Alice announces, on the classical channel, the value of μ that was chosen for each round. Bob computes, from his sifted detections, the weight Q_{μ_k} and the error rate E_{μ_k}, related to each intensity:

$$\begin{aligned} Q_{\mu_k} &= \sum_n P_{\mu_k}(n) Y_n = P_{\mu_k}(0) Y_0 + P_{\mu_k}(1) Y_1 + P_{\mu_k}(2) Y_2 + ... \ , \\ E_{\mu_k} Q_{\mu_k} &= \sum_n P_{\mu_k}(n) Y_n e_n = P_{\mu_k}(0) Y_0 e_0 + P_{\mu_k}(1) Y_1 e_1 + P_{\mu_k}(2) Y_2 e_2 + ... \ . \end{aligned} \tag{1.32}$$

In this way, even if Eve measures the actual photon number of each pulse, she can not know which distribution ($P_{\mu_1}(n),\ P_{\mu_2}(n),\ P_{\mu_3}(n), ...$) is the one related to that pulse. Therefore, if she acts differently based only on the value of n, as shown for the no-decoy protocol, she ends up introducing alterations on the experienced distributions at Bob's side, since Bob will observe different channel loss for the different μ intensities. As a result, Eve has to restrain herself in blocking the useful single-photon pulses, from which she can acquire information only at the expense of introducing errors. In addition, from the system of equations 1.32, Alice and Bob can evaluate the quantities Y_n and e_n, so they can accurately estimate the single-photon weight of signal detections $Q_1 = P_{\mu_1}(1) Y_1$, as well as its corresponding error rate e_1. This allows for a more precise bound for the secret fraction [44]:

$$r = Q_1 \Big[1 - h(e_1) \Big] - Q_{\mu_1} \mathrm{leak}_{EC}(E_{\mu_1}) \ . \tag{1.33}$$

Here, only the detection events coming from the signal intensity μ_1 are used to collect the secure key bits, although slightly different bounds, including all the μ_k detections, together with the contribution $Q_0 = P_{\mu_1}(0) Y_0$ coming from zero-photon pulses (or vacuum events), can be derived for decoy-state QKD[9] [48].

Although infinite decoy intensities are necessary to solve exactly the system 1.32, for small intensity values ($\mu < 1$) the contributions from large photon numbers ($n \geq 3$) become negligible, as can be deduced by considering phase-randomized laser sources, where $P_\mu(n) = \mathrm{e}^{-\mu} \mu^n / n!$. Thus, Q_0, Q_1 and e_1 can be estimated,

[9] The Q_0 term is often neglected in the secure key formula, being due to background detections and dark counts [66, 68].

with sufficient accuracy, also in the more practical situations where only few decoy intensities are included in the protocol. In particular, a lower bound for Q_0, Q_1 and an upper bound for e_1 can be derived, also in the cases of two decoy states and only one decoy state, as shown in Ref. [68]. Moreover, the two-decoy protocol asymptotically approaches the theoretical limit of the infinite-decoy protocol, if one of the two decoy intensities is set to zero, with $\mu_1 > \mu_2 > \mu_3 = 0$ (vacuum and weak decoy states) [68].

1.3.3 Finite-key analysis of decoy-state BB84

In practical implementations of QKD, the secure key has to be extracted after a finite number N of quantum communication rounds. As a consequence, during the parameter estimation step of the protocol, all the useful quantities can not be evaluated with total accuracy, but their statistical fluctuations have to be quantified, depending on the finite data size. Since every fluctuating parameter is replaced by its upper or lower estimate by assuming always the worst-case scenario, the extractable secure key is typically shorter than in the asymptotic case $N \to \infty$, that was assumed so far.

Keeping in mind the purposes of this thesis, we will now focus on the asymmetric BB84 protocol, implemented with one or two decoy states, in a finite-key scenario [9, 54–56].

In the asymmetric BB84 protocol [53, 54], the basis choice at Alice's and Bob's side is performed at random with the biased probabilities $p_{\mathcal{Z}}$ and $p_{\mathcal{X}} = 1 - p_{\mathcal{Z}}$. Moreover, only the detection events in the $\mathcal{Z}$ basis, independently from the μ distribution to whom they belong, are used to collect the raw key bits. Specifically, the raw key is collected by random sampling the $\mathcal{Z}$-basis detections, after the sifting process (basis reconciliation). The overall length of the raw key string, $n_{\mathcal{Z}} = \sum_{\mu_k} n_{\mathcal{Z},\mu_k}$, is called post-processing block size. On the other hand, the sifted detections from the $\mathcal{X}$ basis, $n_{\mathcal{X},\mu_k}$, are not included in the raw key, but are publicly disclosed in order to evaluate the amount of errors, $m_{\mathcal{X},\mu_k}$. The errors from $\mathcal{X}$ basis $m_{\mathcal{X},\mu_k}$ are used to estimate the phase error rate in the $\mathcal{Z}$ basis, which is necessary to evaluate the bit loss during privacy amplification, and is generally different from the experienced error rate in the $\mathcal{Z}$ basis, called bit error rate or qber (see Equation 1.27). Specifically, the phase error rate arising from single-photon detections, $\phi_{\mathcal{Z},1}$, quantifies Eve's information on the single-photon events, useful to extract the secure key. Whenever $\phi_{\mathcal{Z},1}$ goes beyond a pre-fixed threshold, the protocol has to be aborted.

In the two-decoy protocol, analyzed in Ref. [54], Alice prepares the three intensities $\mu_k = \mu_1,\ \mu_2,\ \mu_3$ (with $\mu_1 > \mu_2 + \mu_3$ and $\mu_2 > \mu_3 \geq 0$) with the respective probabilities $p_1,\ p_2$ and $p_3 = 1 - p_1 - p_2$. As discussed in the previous Section, the number of detection events corresponding to quantum states with n photons, can be bounded from the system 1.32, by knowing the experienced detections $n_{\mathcal{Z},\mu_k}$ for each intensity μ_k. In particular, the amount of $\mathcal{Z}$-basis detections from vacuum ($n = 0$) and single photon ($n = 1$) events, can be bounded as

$$\begin{aligned} D_{\mathcal{Z},0} \geq D^L_{\mathcal{Z},0} &= \tau_0 \frac{\mu_2 n^-_{\mathcal{Z},\mu_3} - \mu_3 n^+_{\mathcal{Z},\mu_2}}{\mu_2 - \mu_3} \ , \\ D_{\mathcal{Z},1} \geq D^L_{\mathcal{Z},1} &= \frac{\tau_1 \mu_1 \left[n^-_{\mathcal{Z},\mu_2} - n^+_{\mathcal{Z},\mu_3} - \frac{\mu_2^2 - \mu_3^2}{\mu_1^2} \left(n^+_{\mathcal{Z},\mu_1} - \frac{D^L_{\mathcal{Z},0}}{\tau_0} \right) \right]}{\mu_1(\mu_2 - \mu_3) - \mu_2^2 + \mu_3^2} \ , \end{aligned} \tag{1.34}$$

where $\tau_n = \sum_{\mu_k} p_k P_{\mu_k}(n)$, with $P_{\mu_k}(n) = \mathrm{e}^{-\mu_k} \mu_k^n / n!$, is the probability of sending an n-photon state. To compute the bounds from Equation 1.34, the amount of sifted detections $n_{\mathcal{Z},\mu_k}$ has to be corrected in order to take into account its statistical fluctuations, arising from the finite block size $n_{\mathcal{Z}}$:

$$n^{\pm}_{\mathcal{Z},\mu_k} = \frac{\mathrm{e}^{\mu_k}}{p_k} \left[n_{\mathcal{Z},\mu_k} \pm \delta\Big(n_{\mathcal{Z}}, \frac{\varepsilon_{sec}}{21} \Big) \right] , \tag{1.35}$$

with ε_{sec} the secrecy parameter as defined in Section 1.2.3, to be included in the finite-size correction. The correction $\delta(M, \epsilon)$ is derived from Hoeffding's inequality for independent events [69], which holds with probability of at least $(1 - 2\epsilon)$:

$$\delta(M, \epsilon) = \sqrt{\frac{M}{2} \ln \frac{1}{\epsilon}} \ . \tag{1.36}$$

Analogous formulas are used to compute the lower bounds of $D_{\mathcal{X},0}$ and $D_{\mathcal{X},1}$ from the amount of sifted detections in $\mathcal{X}$ basis, $n_{\mathcal{X},\mu_k}$, after having it corrected as in Equation 1.35, with the finite data size $n_{\mathcal{X}} = \sum_{\mu_k} n_{\mathcal{X},\mu_k}$. In addition, also the amount of experienced errors in $\mathcal{X}$ basis must be corrected,

$$m^{\pm}_{\mathcal{X},\mu_k} = \frac{\mathrm{e}^{\mu_k}}{p_k} \left[m_{\mathcal{X},\mu_k} \pm \delta\Big(m_{\mathcal{X}}, \frac{\varepsilon_{sec}}{21} \Big) \right] , \tag{1.37}$$

with $m_{\mathcal{X}} = \sum_{\mu_k} m_{\mathcal{X},\mu_k}$, in order to bound the amount of errors from single-photon events

$$e_{\mathcal{X},1} \leq e^U_{\mathcal{X},1} = \tau_1 \frac{m^+_{\mathcal{X},\mu_2} - m^-_{\mathcal{X},\mu_3}}{\mu_2 - \mu_3} \ . \tag{1.38}$$

The above quantities are necessary to estimate an upper bound to the phase error rate of $\mathcal{Z}$ basis from single-photon events,

$$\phi_{\mathcal{Z},1} \leq \phi^U_{\mathcal{Z},1} = \frac{e^U_{\mathcal{X},1}}{D^L_{\mathcal{X},1}} + \gamma\Big(\frac{\varepsilon_{sec}}{21}, \frac{e^U_{\mathcal{X},1}}{D^L_{\mathcal{X},1}}, D^L_{\mathcal{X},1}, D^L_{\mathcal{Z},1}\Big) \ , \tag{1.39}$$

where the function γ is defined as follows:

$$\gamma(a,b,c,d) = \sqrt{\frac{(c+d)(1-b)b}{cd\ln 2} \cdot \log_2\Big(\frac{c+d}{cd(1-b)ba^2}\Big)} \ . \tag{1.40}$$

Then, by taking the upper and lower bounds of the above quantities, the length of the secure key for the two-decoy protocol can be bounded as

$$\ell \leq D^L_{\mathcal{Z},0} + D^L_{\mathcal{Z},1}\Big[1 - h(\phi^U_{\mathcal{Z},1})\Big] - \lambda_{EC} - \log_2\Big(\frac{2}{\varepsilon_{corr}}\Big) - 6\log_2\Big(\frac{21}{\varepsilon_{sec}}\Big) \ , \tag{1.41}$$

where $\lambda_{EC} + \log_2(2/\varepsilon_{corr})$ are the bit lost during error correction, depending on the correctness parameter ε_{corr} as defined in Section 1.2.3.

In the one-decoy protocol, analyzed in Ref. [55], Alice prepares only two intensities μ_1 and μ_2, with $\mu_1 > \mu_2$ and probabilities p_1 and $p_2 = 1 - p_1$. Even with only one decoy, Alice and Bob can successfully estimate all the parameters required to generate a secure key. Although the two-decoy protocol was found to always outperform the one-decoy protocol in the asymptotic scenario ($N \to \infty$) [68], choosing only one decoy in the asymmetric BB84 with finite-key analysis was proven to be advantageous under some experimental circumstances, including the middle-loss regime [55].

The bound for the secure key length in one-decoy case is similar to Equation 1.41,

$$\ell \leq D^L_{\mathcal{Z},0} + D^L_{\mathcal{Z},1}\Big[1 - h(\phi^U_{\mathcal{Z},1})\Big] - \lambda_{EC} - \log_2\Big(\frac{2}{\varepsilon_{corr}}\Big) - 6\log_2\Big(\frac{19}{\varepsilon_{sec}}\Big) \ , \tag{1.42}$$

where the lower bounds for the vacuum and single-photon events are now evaluated only from μ_1 and μ_2 detections, to be corrected in the finite-key scenario:

$$n^{\pm}_{\mathcal{Z},\mu_k} = \frac{\mathrm{e}^{\mu_k}}{p_k}\left[n_{\mathcal{Z},\mu_k} \pm \delta\Big(n_{\mathcal{Z}}, \frac{\varepsilon_{sec}}{19}\Big)\right] . \tag{1.43}$$

The lower bound on $D_{\mathcal{Z},0}$ has simply the same expression as in the two-decoy protocol,

$$D_{\mathcal{Z},0} \geq D^L_{\mathcal{Z},0} = \tau_0 \frac{\mu_1 n^-_{\mathcal{Z},\mu_2} - \mu_2 n^+_{\mathcal{Z},\mu_1}}{\mu_1 - \mu_2} , \tag{1.44}$$

while the lower bound on $D_{\mathcal{Z},1}$ is found to be

$$D_{\mathcal{Z},1} \geq D^L_{\mathcal{Z},1} = \frac{\tau_1\mu_1}{\mu_2(\mu_1-\mu_2)}\left[n^-_{\mathcal{Z},\mu_2} - \frac{\mu_2^2}{\mu_1^2} n^+_{\mathcal{Z},\mu_1} - \frac{\mu_1^2-\mu_2^2}{\mu_1^2}\frac{D^U_{\mathcal{Z},0}}{\tau_0}\right] , \tag{1.45}$$

where the $D^U_{\mathcal{Z},0}$ is the upper bound on the vacuum events. Unfortunately, this quantity can not be bounded tightly in the one-decoy protocol, but it still can be estimated by considering that, on average, half of the vacuum events give rise to errors. The derivation from Ref. [55] shows that a proper bound can be found by considering the errors $m_{\mathcal{Z},\mu_k}$ arising from only one of the two intensities $\mu_k = \mu_1$ or $\mu_k = \mu_2$, in the following way:

$$D_{\mathcal{Z},0} \leq D^U_{\mathcal{Z},0} = 2\left[\tau_0 m^+_{\mathcal{Z},\mu_k} + \delta\Big(n_{\mathcal{Z}}, \frac{\varepsilon_{sec}}{19}\Big)\right] . \tag{1.46}$$

Again, analogous relations can be derived to compute the bounds from $\mathcal{X}$-basis detections, $D^L_{\mathcal{X},0}$ and $D^L_{\mathcal{X},1}$. The upper bound on the phase error rate is computed in the same way as for the two-decoy protocol,

$$\phi_{\mathcal{Z},1} \leq \phi^U_{\mathcal{Z},1} = \frac{e^U_{\mathcal{X},1}}{D^L_{\mathcal{X},1}} + \gamma\Big(\frac{\varepsilon_{sec}}{19}, \frac{e^U_{\mathcal{X},1}}{D^L_{\mathcal{X},1}}, D^L_{\mathcal{X},1}, D^L_{\mathcal{Z},1}\Big) , \tag{1.47}$$

where γ is defined as in Equation 1.40, while the upper bounds on the erroneous detections in $\mathcal{X}$ basis from single-photon events is analogously obtained as

$$e_{\mathcal{X},1} \leq e^U_{\mathcal{X},1} = \tau_1 \frac{m^+_{\mathcal{X},\mu_1} - m^-_{\mathcal{X},\mu_2}}{\mu_1 - \mu_2} , \tag{1.48}$$

with the corrected errors $m^{\pm}_{\mathcal{X},\mu_k} = \mathrm{e}^{\mu_k}/p_k[m_{\mathcal{X},\mu_k} \pm \delta(m_{\mathcal{X}}, \varepsilon_{sec}/19)]$.

1.3.3.1 The three-state protocol

In the three-state and simplified version of BB84 protocol [9, 56, 57], Alice prepares the states $|0\rangle$ and $|1\rangle$ in the $\mathcal{Z}$ basis and only the state $|+\rangle$ in the $\mathcal{X}$ basis. Bob measures the projection on both states of $\mathcal{Z}$ basis, to collect the raw key data, and only the projection on state $|-\rangle$ of $\mathcal{X}$ basis, in order to estimate and monitor the phase error rate. The security analysis of this protocol, with one decoy state in a finite-key regime, is reported in Ref. [56] and it is derived in the specific case of time-bin encoding, where the states from $\mathcal{Z}$ basis are defined by the early and late time bins, respectively, with the $\mathcal{X}$ basis projection implemented by observing the interference of the two time bins, in the so called monitoring line [9, 57].

The protocol is structured analogously to the asymmetric BB84 with four states, described in the previous Section. The secret key formula for the one-decoy implementation is the same as in Equation 1.42, with the lower bound of vacuum and single-photon events on $\mathcal{Z}$ basis to be computed in the same way as for the four-state protocol, as reported in Equations 1.44, 1.45 and 1.46. However, the estimation of $\phi_{\mathcal{Z},1}$ becomes more complex, due to the lack of projections into the other state of $\mathcal{X}$ basis:

$$\phi_{\mathcal{Z},1} \leq \phi^U_{\mathcal{Z},1} = \phi^U_{\mathcal{X},1} + \gamma\Big(\frac{\varepsilon_{sec}}{19}, \phi^U_{\mathcal{X},1}, D^L_{\mathcal{Z},1}, D^L_{n(e,\mathcal{Z}\mathcal{Z}),1}\Big) \ , \tag{1.49}$$

where γ is the same function as defined in Equation 1.40, while the quantity $\phi^U_{\mathcal{X},1}$ is computed as

$$\begin{aligned} \phi^U_{\mathcal{X},1} &= \frac{\alpha}{2}\frac{D^U_{n(l,+),1}}{D^L_{n(e,\mathcal{Z}\mathcal{Z}),1}} \\ &+ \max\Bigg[0, \Big(1 + \frac{\alpha}{2}\frac{D^U_{n(l,+),1}}{D^L_{n(e,\mathcal{Z}\mathcal{Z}),1}} - \beta\frac{D^L_{n(l,0)+n(l,1),1}}{D^L_{n(e,\mathcal{Z}\mathcal{Z}),1}} - \alpha\frac{D^L_{n(e,0+)+n(e,+1),1}}{D^L_{n(e,\mathcal{Z}\mathcal{Z}),1}}\Big)\Bigg] \ , \end{aligned} \tag{1.50}$$

with $\alpha = p^2_{\mathcal{Z}}/[4(1-p_{\mathcal{Z}})]$ and $\beta = p_{\mathcal{Z}}/4$ depending on the probability that Alice chooses the $\mathcal{Z}$ basis. In Equations 1.49 and 1.50, the upper and lower bounds for single-photon events are considered by distinguishing different cases, denoted by the subscript $n(b, j)$. Here, b defines the events when Bob measures the b time bin in the monitoring line (either early $b = e$, or late $b = l$), while j (j = 0, 1, +, 00, 11, 0+, +1) denotes the state, or the sequence of states, that are sent by Alice. Moreover, $n(e, \mathcal{Z}\mathcal{Z}) = n(e, 00) + n(e, 11)$ is used to simplify the notation. Based on these considerations, the lower bounds $D^L_{n(b,j),1}$ are computed in the same way

as shown in Equation 1.45, where the amounts of corresponding detections $n(b,j)^{\pm}_{\mu_k}$ have to be included, after applying the correction δ as given in the four-state BB84 with one decoy. Moreover, as shown in Equation 1.45, the computation of each lower bound $D^{L}_{n(b,j),1}$ requires the corresponding upper bound on vacuum events, $D^{U}_{n(b,j),0}$, that can be derived as follows:

$$D^{U}_{n(b,j),0} = \frac{p(j)}{p(01)} n(e,01) + \delta\left(\frac{p(j)}{p(01)} n(e,01), \frac{\varepsilon_{sec}}{19}\right) , \tag{1.51}$$

with the finite-key correction δ given by Equation 1.36. On the other hand, the upper bounds $D^{U}_{n(b,j),1}$ are computed as

$$D^{U}_{n(b,j),1} = \frac{\tau_2}{\mu_1 - \mu_2}\left[n(b,j)^{+}_{\mu_1} - n(b,j)^{-}_{\mu_2}\right] . \tag{1.52}$$

1.4 High-dimensional quantum key distribution

All the notions on the BB84 protocol reported so far, can be extended in the more general scenario when the two mutually unbiased bases of quantum states, to be prepared and measured by Alice and Bob, belong to a d-dimensional Hilbert space [51, 70], as shown in Equations 1.3 and 1.4. In this case, each qudit is used to encode a symbol, corresponding to $\log_2(d)$ bits of information. For instance, if $d = 4$ the quantum states from $\mathcal{Z}$ basis can be represented by $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$, each encoding one of the four symbols 00, 01, 10 and 11, where every symbol corresponds to a string of two classical bits. Consequently, Alice's and Bob raw keys are composed, uniformly at random, by the d possible symbols encoded on the qudits, and the Shannon entropies $H(A) = H(B)$ associated to their random variables, are bounded by $\log_2(d)$. Similarly to the qubit-based BB84, the secret fraction for the d-dimensional BB84 under coherent attacks, implemented with a perfect single photon source and one-way post-processing, can be evaluated as

$$r_d = \log_2(d) - \mathrm{leak}_{EC}(e_{bit}) - H_d(e_{ph}) , \tag{1.53}$$

with $\mathrm{leak}_{EC}(e_{bit}) \geq H_d(e_{bit})$, where H_d is d-dimensional entropy function, defined as $H_d(x) = -x\log_2[x/(d-1)] - (1-x)\log_2(1-x)$ [71]. Notably, the error rates e_{bit} and e_{ph} now refer to symbol errors.

The fist advantage of using qudits as information carrier in place of qubits, is

the larger information efficiency [21], as for each photon (or weak pulse) detected by Bob in the right basis, $\log_2(d) \geq 2$ bits of information are added to the raw key. The larger information gain per photon allows for an optimized exploitation of the photon budget at Alice's side, useful when the state preparation rate is limited by the repetition rate of the source. At the same time, when the measurement setup is limited in bandwidth, the larger information efficiency enables to partially overcome the effects of saturation regime at Bob's side. A second advantage of high-dimensional encoding in QKD is the higher threshold value for the error rate that is tolerated by the protocol, i.e., the maximum error rate that still enables the generation of a secure key [21, 71]. For instance, let's consider the ideal BB84 protocol with one-way post-processing and $\text{leak}_{EC}(e_{bit}) = H_d(e_{bit})$, with $e_{bit} = e_{ph} \equiv e$. As already mentioned in Section 1.3.1, for $d = 2$ the threshold value for the error rate is 0.110 (Equation 1.26). However, for $d = 4$, the threshold raises to 0.189, and its value keeps increasing with d. The reason for this is that, in general, eavesdropping attacks have a larger effect on qudits, in terms of introduced errors. For example, with the intercept-resend attack performed during the BB84 protocol with $d = 2$, Eve causes an average error rate of 0.25 in the raw key bits, because even if she chooses the wrong basis she still has 1/2 probability to get the same bit as Alice's. However, for $d = 4$, when she chooses the wrong basis she has only 1/4 probability to retrieve the right symbol, thus she introduces, on average, a symbol error rate of 0.375 in the raw key [70]. As a consequence, high-dimensional protocols for QKD generally exhibit higher tolerance to the noise affecting the quantum channel.

On the other hand, since the projective measurement on a d-dimensional basis returns d possible outcomes, random counts such as those arising from vacuum events, give rise to errors with $(1 - 1/d)$ probability, which clearly increases with d. Since vacuum events become more and more frequent with the increasing loss of the quantum channel, this different behaviour among the protocols with different dimension is expected to be enhanced for longer channel distances, where the random counts are more likely to produce errors in high-dimensional measurements. As a result, exploiting the qudits instead of qubits is a convenient approach for improving QKD at relatively short distances, with the quantum channel affected by noise but exhibiting relatively low loss [21, 72].

1.4.1 Finite-key analysis of the four-dimensional protocol with decoy states

The finite-key analysis for the asymmetric BB84 protocol with four states and decoy-state method, reported in Section 1.3.3, can be easily adapted to the more general case with $2d$ states. The structure of the d-dimensional protocol is mostly the same as for $d = 2$, except for the fact that Alice creates a uniformly random list of symbols by picking among d different symbol values, and she selects accordingly the quantum states to be prepared among $2d$ different qudits, belonging to the mutually unbiased $\mathcal{Z}$ and $\mathcal{X}$ bases. At the same time, Bob obtains d possible outcomes from the projective measurement on each basis. Again, the two bases are selected at random with probabilities $p_{\mathcal{Z}}$ and $(1 - p_{\mathcal{Z}})$, and all the sifted detections in the $\mathcal{Z}$ basis (from all the intensities μ_k) are used to extract the secure key, while all the sifted detections in $\mathcal{X}$ basis are publicly announced and used to estimate the phase error rate, in order to quantify and bound Eve's information about the raw key.

From now on, we will focus on the four-dimensional protocol with eight states ($d = 4$) and with only one decoy intensity μ_2 (with $\mu_1 > \mu_2$). Therefore, the bound for the secure key can be obtained in an analogous way as already done for the two-dimensional BB84 with one decoy intensity (Equation 1.42):

$$\ell_{4\mathrm{D}} \leq 2D^L_{\mathcal{Z},0} + D^L_{\mathcal{Z},1}\Big[2 - H_4(\phi^U_{\mathcal{Z},1})\Big] - \lambda_{EC} - \log_2\Big(\frac{2}{\varepsilon_{corr}}\Big) - 6\log_2\Big(\frac{19}{\varepsilon_{sec}}\Big)\,, \quad (1.54)$$

where a factor $2 = \log_2(4)$ has been included in front of the vacuum and single-photon contributions, while H_4 denotes the entropy function in four dimensions, $H_4(x) = -x\log_2(x/3) - (1-x)\log_2(1-x)$ [22]. All the lower and upper bounds are computed in the same way as in the four-state protocol with one decoy (Equations 1.43, 1.44, 1.45, 1.47 and 1.48) with the only exception of the upper bound on vacuum events (Equation 1.46), that was estimated by considering that on average, for $d = 2$, 1/2 of the vacuum events give rise to erroneous detections. In $d = 4$, having four possible outcomes, errors arise on average from 3/4 of the vacuum events. Therefore, Equation 1.46 becomes

$$D_{\mathcal{Z},0} \leq D^U_{\mathcal{Z},0} = \frac{4}{3}\left[\tau_0 m^+_{\mathcal{Z},\mu_k} + \delta\Big(n_{\mathcal{Z}}, \frac{\varepsilon_{sec}}{19}\Big)\right]\,, \quad (1.55)$$

with all the terms defined as in Section 1.3.3.

1.5 Overview on quantum key distribution protocols

The last two Sections of the current Chapter have been mainly focused on a specific protocol of quantum key distribution, the BB84, although most of the discussed concepts can be extended to other QKD protocols. Nonetheless, there is no denying that the BB84 protocol, together with its multiple and efficient variants, is the most studied and developed protocol for QKD. Notably, the introduction of decoy-state technique in 2005 has boosted the advancement of practical implementations of BB84 protocols with phase-randomized laser sources, paving the way towards many record-breaking experiments on QKD [7–9, 13, 14, 73–75]. Specifically, recent demonstrations of decoy-state BB84 have achieved high rates of secure key generation (up to 13.7 Mbit/s in 2018 [14]) and long transmission distances, both in fiber-based links (more than 400 km in 2018 [9]) as well as in free-space links ($\sim$ 1200 km from satellite to Earth in 2017 [7]). Moreover, a four-dimensional version of decoy-state BB84 has demonstrated 26.2 Mbit/s of key generation rate in 2017 [13]. The most common degrees of freedom to be exploited in BB84 protocols are polarization [7,8,76], phase [14,73,75] and time bin [9,13,57]. For high-dimensional protocols, the orbital angular momentum, path encoding and time-energy encoding are also employed [77–81].

From a more general point of view, the BB84 protocol and its variants belong to the category of discrete-variable (DV) QKD protocols, based on single-photon sources and single-photon counters, and another distinction is made between prepare-and-measure DV protocols and entanglement-based DV protocols [5, 82], even though the former are often replaced by the latter when deriving the security proofs. With respect to the security level against side-channel attacks, another distinction within the DV family is made between decoy-state protocols and measurement-device-independent (MDI) protocols [63, 64], which offer, in principle, provable security against all possible hacking attacks addressed to untrustworthy devices in the detection setup. In addition, device-independent protocols can guarantee security with totally uncharacterized devices [62], yet they are still not feasible with current technology. On the other hand, practical implementations of MDI protocols have improved notably [6, 83–85] and moreover, an efficient version of MDI QKD, called twin-field, has been introduced in 2018 [86], with the potential to largely extend the boundaries of the transmission distance affordable by QKD [11, 87–89].

As opposed to DV protocols, continuous-variable (CV) QKD is based on coherent sources and homodyne or heterodyne detection schemes [90]. Although they can boast a cheaper and high-bandwidth detection setup, the performances of CV protocols are generally lower than those of DV-QKD, especially at long transmission distances [91].

The last and third family of QKD protocols is called distributed-phase-reference (or DPR) QKD. Similarly to DV protocols, they require single-photon counters in the measurement setup and decoy states at the source. However, the information is encoded in the relative attributes of consecutive pulses, rather than in some degree of freedom of each pulse separately, and the security monitoring is performed by exploiting the properties of coherent states, such as the phase coherence after the transmission. Within the DPR family, a distinction is made between differential-phase-shift (DPS) protocols, which exploit the relative phase of subsequent pulses, and coherent-one-way (COW) protocols, which exploit also different time bins [92, 93]. Based on DPS QKD, a novel protocol called round-robin DPS, has been recently introduced [94]. This protocol and its peculiar features will be presented with more details in Chapter 4.

2

Tools and methods

In this Chapter are presented the tools and methods adopted in the experimental works of QKD reported in this thesis. It is important to remark that the research work and QKD experiments that will be presented in the following Chapters, are mainly focused on the practical implementation of the quantum communication part of the QKD protocol, including the preparation and measurement of quantum states of light. Therefore, the aim of the current Chapter is to describe the experimental setups for quantum communication, with all the optical and electronic components, together with the methods of data collection and analysis, that have been adopted in the main contributions presented in this thesis. Before doing so, a brief overview is reported in order to focus on the main field of application of the research work of this thesis, that is fiber-based QKD over metropolitan infrastructures.

2.1 Fiber-based communication on metropolitan scales

The research activity presented in this thesis is focused on the practical implementation of QKD protocols over fiber optic links, typically connecting pairs of nodes of a metropolitan fiber network. The typical distances covered by metropolitan-scale links are of the order of tens of kilometers, corresponding to the low and middle-loss regime of the quantum channel (up to $\sim 25\,\mathrm{dB}$ of attenuation). Standard single-mode fibers (SMF), in compliance with the recommendations of the International Telecommunication Union (ITU), are mostly deployed in metropolitan infrastructures for optical communications. Such infrastructures are considered suitable also for the implementation of quantum communication protocols, and multiple in-field demonstrations of QKD networks have been successfully carried out in the past, in

Europe [95, 96], UK [10], Japan [97] and China [12, 98]. However, in order to reach the full integration of quantum communication technologies in the already-existing fiber networks, many practical challenges have still to be addressed: low rate of secure key generation, high costs of implementation and low tolerance for the noise, both in the communication line as well as in the experimental apparatus. Therefore, finding novel solutions to address such issues is an essential requirement to enable the widespread use of QKD protocols in every-day life applications.

Standard SMF for telecom applications usually support the infrared wavelengths ranging from 1260 nm to 1625 nm. Within this spectral region, the wavelengths in the C-band (from 1530 nm to 1565 nm) propagate with the lowest attenuation, with a nominal transmission loss of around 0.2 dB/km at 1550 nm. However, the already deployed fibers typically exhibit higher loss due to multiple connections, bend losses or imperfect splicing. Moreover, even dark fibers (i.e., fiber links without transmitted signals nor amplifiers) may exhibit substantial noise, detectable at the single-photon level, due to the environmental conditions. Although the background noise coming from the sun light is usually negligible for fiber cables installed underground (yet it can still affect the transmitting and receiving setups, if they are not shielded properly), cross-talk noise may arise from the nearby and non-dark fiber cables assembled in the same bundle. The situation gets much worse if the fiber dedicated to quantum communication is not dark, but it carries both classical and quantum signals by means of multiplexing techniques. Due to the infinitely higher power of classical light in comparison with quantum signals, even a smallest fraction of it evading the imperfect multiplexing is capable to induce enough noise to prevent the quantum communication from being feasible. In addition, the classical intense signals are likely to induce nonlinear effects in the fiber material (silica), such as Brillouin and Raman scattering [99], which make the conventional multiplexing techniques insufficient to safeguard the quantum communication. Furthermore, other sources of noise and instability may arise from the thermal expansion, from the chromatic dispersion and from the polarization drifts in standard SMF. However, these last effects can be generally compensated and, moreover, they do not affect every QKD implementation. Specifically, polarization drifts affect only the polarization-dependent devices in the receiver apparatus, while the broadening of laser pulses due to chromatic dispersion is usually negligible at the typical metropolitan distances [99].

As it will be shown in the next Chapters, the experimental works presented in this thesis propose different protocols and practical solutions, in order to address the current issues of implementing QKD in such realistic conditions of loss and noise,

that can be typically found in metropolitan fiber links.

2.2 Time-bin and phase encoding

For quantum communication based on single-mode fibers, time-bin and relative-phase encoding are often preferred over polarization encoding, as they usually do not require the compensation of polarization drifts in the quantum channel [44, 48]. Moreover, as opposed to the polarization degree of freedom, whose corresponding Hilbert space has a fixed dimension of $d = 2$, multiple time bins can be exploited to prepare qudits for high-dimensional protocols, as it will be shown in details in the following Chapters.

In the simplest case of qubits ($d = 2$), two identical time bins are defined as the early bin, t_0, and the late bin, t_1, and the generic time-bin state can take the form

$$|\psi\rangle = c_e|e\rangle + c_l|l\rangle \ , \tag{2.1}$$

with $c_e,\ c_l \in \mathbb{C}$ and $|c_e|^2 + |c_l|^2 = 1$, while $|e\rangle = |1\rangle_{t_0}|0\rangle_{t_1}$ and $|l\rangle = |0\rangle_{t_0}|1\rangle_{t_1}$ denote the states where a single photon occupies the time bin t_0 or t_1, respectively. Such qubits can be approximated by weak laser pulses, as discussed in Section 1.3.1. Notably, if we set $|c_e| = |c_l| = 1/\sqrt{2}$, the information will be encoded only on the relative phase between the two bins, and the four non-orthogonal states for BB84 protocol can be defined by the relative phases 0, $\frac{\pi}{2}$, π, $\frac{3}{2}\pi$ (phase encoding). Otherwise, different amplitudes can be set to each time bin to form mutually-unbiased bases of states. It is usual to identify the $\mathcal{Z}$ basis of the time-bin space as the so called time-of-arrival basis, which for $d = 2$ just includes the early and late states: $\{|e\rangle, |l\rangle\}$. The projection on the time-of-arrival basis is the most simple to implement, as it requires just a single-photon detector with sufficient sensitivity to distinguish the time difference, τ, between the two time bins. Then, the $\mathcal{X}$ bases is composed by the superposition states $(|e\rangle \pm |l\rangle)/\sqrt{2}$, where both bins are equally combined with 0 or π relative phase, respectively. The projection on $\mathcal{X}$ basis requires a setup able to distinguish between the two relative phases, that is an unbalanced interferometer with a delay line equal to τ. Michelson interferometers as well as Mach-Zehnder interferometers are both suitable for this purpose. Since the observed interference between the two time bins can be either constructive (0 phase) or destructive (π phase), two single-photon detectors are necessary to monitor the possible arrival of

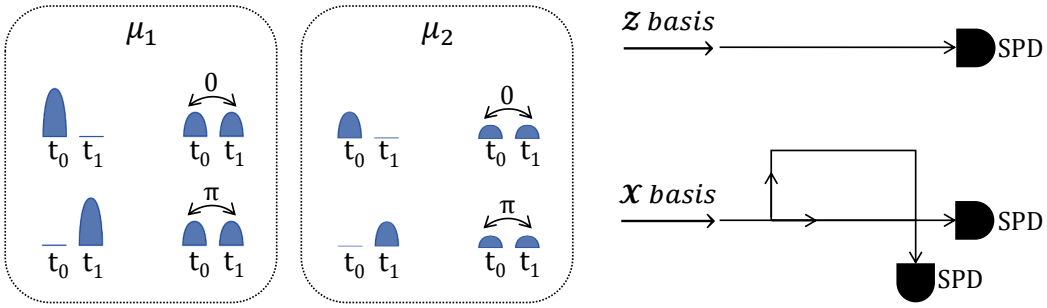


Figure 2.1: Quantum states to be prepared and measured in the four-state BB84 protocol with encoding on two time bins (t_0, t_1) and one decoy state (with $\mu_2 < \mu_1$). For each intensity value, the $\mathcal{Z}$ basis is reported on the left and the $\mathcal{X}$ basis on the right. The former includes the early and late time-bin states, while the latter includes superposition states of both bins with 0 and π relative phases. In the right side of the Figure, the experimental setup necessary to perform the projections on the two bases is depicted schematically (SPD: single-photon detector). A SPD measuring the arrival time of the pulse is sufficient to project on the $\mathcal{Z}$ basis. For $\mathcal{X}$ basis measurements, a Mach-Zehnder interferomenter can be adopted, with a delay line equivalent to the time difference between t_0 and t_1.

the photon from one of the two outputs of the interferometer. This is depicted in Figure 2.1, showing the quantum states to be prepared in a decoy-state BB84 with time bin encoding, together with the measurement setup to project on the two bases. More generally, Figure 2.2 illustrates schematically the experimental setup that we used to test different QKD protocols with time and phase encoding, as described with more details in the following sections.

2.3 The transmitter

As can be deduced from the building blocks in Figure 2.2, in our setups the experimental equipment of the transmitting unit (Alice) is composed of standard fiber-based devices and electronic components from the telecom industry, all of common use in optical communications. In the following, we describe in details the optical setup, including the laser source and the electro-optic modulators, and the electronic FPGA board (field programmable gate array), which drives the pulse carving as well as the amplitude and phase modulation, necessary to perform the high-speed encoding on time and phase, with decoy-state method.

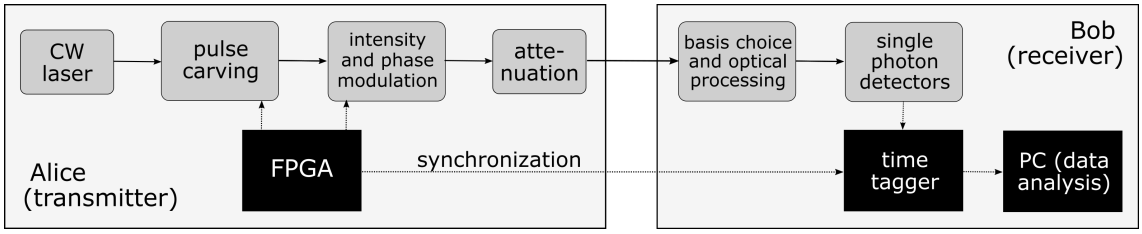


Figure 2.2: Schematic depiction of the experimental setup implemented in the contributions of this thesis, in order to test different QKD protocols with time and phase encoding. Grey blocks represent the optical equipment in the experimental apparatus, while black boxes represent electronic devices and computers. Solid arrows stand for fiber optic (SMF) cables, while dashed arrows stand for coaxial or USB cables.

2.3.1 Optical setup

In our setups, the source is a continuous wave (CW) laser emitting in the C-band, with a fiber-coupled output. Specifically, we use the CoBrite-DX1 lasers from ID Photonics, whose output wavelength can be tuned in the whole bandwidth of the C-band window. The pulse carving is implemented with high-speed intensity modulators, based on the carving pattern signal provided by the FPGA, as reported in Figure 2.3 and described in the following Section. Similarly, the subsequent step of amplitude and phase modulation is performed by means of intensity and phase modulators, respectively, driven by proper square signals provided by the FPGA. All the electro-optic modulators are based on lithium niobate waveguides (with fiber-pigtailed inputs and outputs), whose optical path can be controlled by means of electric signals [100]. In particular, the voltage amplitude required to impress a π phase shift in the phase modulator, which is based on a simple waveguide, is defined as V_π. In the intensity modulator, based on a Mach-Zehnder waveguide, V_π is the voltage that produces the highest extinction ratio at the interference output. For all modulators, $V_\pi \approx 6\,\mathrm{V}$ and all the driving signals provided by the FPGA (see Figure 2.3) need to be amplified and properly tuned to reach a peak-to-peak value as close as possible to V_π. Together with the bias voltage to be applied to the intensity modulators, setting the right amplitude V_π in the driving signals is a crucial task in the transmitter setup, since it can introduce errors in the preparation of quantum states. Moreover, the first step of pulse carving is especially critical for time-bin encoding, being likely to leave some photons out of the pulse shape, due to the finite extinction of the intensity modulator. For this reason, in our setups we usually exploit two cascaded intensity modulators, both dedicated to pulse carving. This

requires the two modulators to be precisely time-aligned, which is accomplished by finely adjusting the electrical delay on the second modulator. Furthermore, also the polarization of the input laser into all the lithium niobate waveguides needs to be properly aligned, along the axis whose refractive index exhibits the strongest dependence to the applied voltage, since any different polarization direction is not properly modulated and gives rise to errors in the preparation of quantum states.

Notably, since the coherence time of the CW laser ($\sim 10\,\mu s$) is much greater than the time bin duration defined in our setups ($\tau \simeq 840\,ps$), the carved pulses sited on consecutive time bins all have, by default, 0 relative phase. This means that also subsequent quantum states are coherent in phase, thus an active system for phase randomization is needed, in order to match the security assumptions of decoy-state QKD (which also require the quantum states to be uncorrelated in order to ensure security under coherent attacks). Active phase randomization can be fulfilled with additional phase modulation of the quantum signals [83]. Moreover, it has been shown that discrete phase modulation with only ~ 10 random phases can provide good results very close to the continuous phase randomization [101]. To implement such multiple levels of phase, a phase modulator driven with a proper digital-to-analog converter has to be included in our the experimental setup. Alternatively, continuous phase randomization can be achieved with a pulsed laser source operating in gain-switching mode, where every pulse originates from a new process of spontaneous emission with intrinsically random phase [102]. Nonetheless, due the experimental scope of our works, we do not carry out the phase randomization of quantum states in most of the contributions presented in this thesis, as it would not affect the obtained results.

To complete the optical setup at the transmitter, an attenuator is needed to bring the laser power down to the quantum regime, with a mean photon number per state, μ_k, lower than 1. The attenuation needs to be properly characterized in order to set the μ_k values required by the QKD protocol. The optimal parameters are evaluated, for each different experiment, with numerical simulations of the QKD protocol under the expected experimental conditions. Notably, the ratio between the different μ_k intensities, together with their probabilities of preparation p_k, are already set in the previous step of intensity modulation, while the final and overall attenuation only determines the average value $\bar{\mu} = \sum_k p_k \mu_k$. Such quantity can be computed and monitored from the optical power P_{out} at the output of the transmitter setup, which is directly evaluated from the known attenuation. Specifically, $\bar{\mu} = P_{out}\lambda d\tau/(hc)$, where hc/λ is the photon energy and $1/(d\tau)$ is the state preparation rate, in the

generic case of d time bins per quantum state.

2.3.2 Electronic FPGA board

As shown in Figure 2.2, the role of the FPGA board is to drive the electro-optic modulators with the electric signals for carving the laser and for modulating the amplitude and phase of the laser pulses, and also to provide a reference signal to be sent to the receiver for synchronization purposes. The first task of driving the modulators is what determines the quantum states to be prepared, including Alice's basis choice and the intensity value μ_k to be sent into the quantum channel. The second task of transmitting the synchronization signal can be included in the public communications that are required in the QKD protocol, to be performed in a classical authenticated channel connecting Alice and Bob.

In our setups we use the Intel/Altera Stratix V GX evaluation board, which exhibits a maximum clock frequency of 12.5 GHz. This internal clock frequency allows the generation of electrical pulses with a minimum full-width half-maximum of ≈ 80 ps. Such pulses compose the carving pattern, necessary for driving the high-speed intensity modulators that carve the laser pulses out of the CW source. In the carving pattern, as shown in Figure 2.3, consecutive pulses occupy different time bins, with a temporal separation of $\tau \simeq 840$ ps. Moreover, some time bins in the pattern are left empty, meaning that the carving signal already includes the time-bin encoding. Afterwards, the carved pulses need to be properly modulated in amplitude an phase: to do so, the squared patterns depicted in Figure 2.3 are provided by the FPGA board. In each squared pattern, the voltage is switched between two different levels, therefore such signals can be used to drive the amplitude modulation between two intensity values (as required for the one-decoy protocol) and to apply a phase difference of 0 or π with the phase modulator. To compose the required patterns for amplitude and phase modulation, pseudo-random binary sequences (PRBS) are used by the FPGA. Such sequences are periodic strings of two-level symbols (or bits) that are pseudo-randomly generated [103]. The periodicity of the PRBS is exploited to produce the carving and squared patterns, and to generate the synchronization signal to be transmitted to the receiver. Specifically, in our implementations we use a PRBS with a period of 4095 symbols (PRBS-12, being $4095 = 2^{12} - 1$), and a symbol duration of 2τ, for generating a reference pulse at the beginning of every new period of the sequence. In this way, the synchronization signal has a frequency of $(2\tau \cdot 4095)^{-1} \simeq 145$ kHz. Notably, the same PRBS-12 with 2τ symbol-width can be

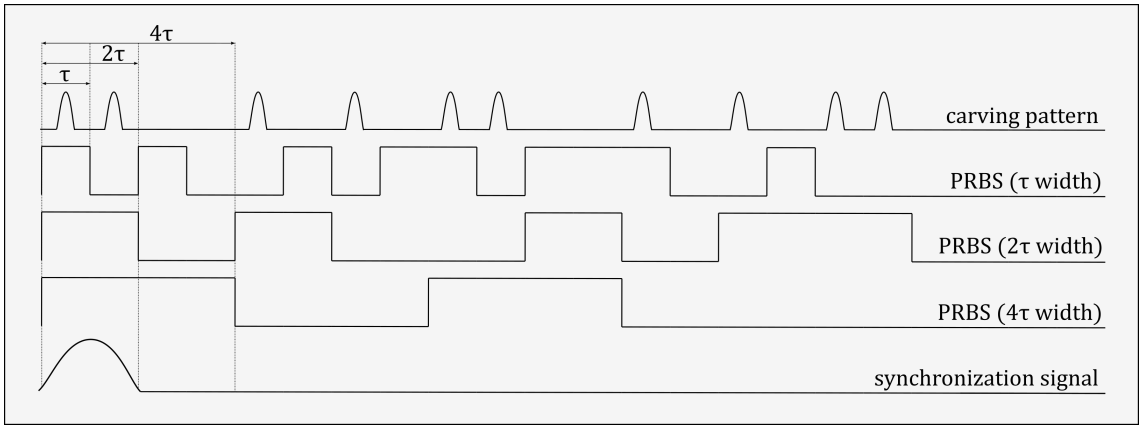


Figure 2.3: Here are reported the electric signals provided by the FPGA board in our QKD setups. The carving pattern and the squared signals, properly derived from pseudo-random binary sequences (PRBS) with different symbol widths, are used to drive the intensity and phase modulators in the transmitter setup, necessary to select and prepare the quantum states to be sent. In our setups, the time-bin duration is $\tau \simeq 840\,\text{ps}$ and every pattern repeats itself after $2 \cdot 4095$ time bins. The synchronization signal, with a frequency of $(2\tau \cdot 4095)^{-1} \simeq 145\,\text{kHz}$, provides the receiver with a time reference necessary for identifying the starting point of each sequence.

used to derive the squared pattern necessary for modulating the amplitude in a two-dimensional time-bin protocol (where a quantum state has 2τ duration). Differently, the squared pattern needed to modulate the phase of each time bin is derived from a PRBS-12 with a symbol width equal to τ, and such pattern is repeated twice in order to fit the whole synchronization period. Furthermore, the squared pattern necessary to perform the one-decoy modulation in a four-dimensional protocol, where each state is defined by $d = 4$ time bins, is derived from a PRBS-7 with symbol width equal to 4τ, repeated 17 times and properly cut in order to fit the synchronization period.

Notably, in a real implementation of QKD, total randomness is required in the preparation of quantum states. To do so, commercial systems make use of quantum random number generators [104]. However, this is not the purpose of our experimental work. Moreover, the use of a fixed and pseudo-random sequence of quantum states that periodically repeats itself (while generating a reference signal at every new period) is a very convenient method that really simplifies the acquisition of experimental data, since the FPGA board can run independently without need to communicate with the software for data analysis.

2.4 The receiver

As already mentioned in Section 2.2, in time-bin encoded QKD the quantum measurements are carried out by observing the time of arrival and the relative phase of the incoming quantum signals, which generally requires single-photon detectors and interferomenters. The optical setup depends on the specific QKD protocol that is tested in our experiment, as it will be shown in the next chapters. In general, a projective measurement can be divided into an initial step of basis choice and optical processing (which may include an interferometer) and a final step of single-photon detection, as depicted in Figure 2.2. Every "click" signal returned from a single-photon detector denotes the occurrence of a quantum state projection. The signals returned from all the single-photon detectors are collected by a time tagging unit, which also receives the synchronization signal sent by Alice's FPGA board. Then, the computer acquires the time tags via USB connection and proceeds to the real-time data analysis, as described in Section 2.4.2.

Concerning the experimental setup at the receiver, in our implementations we use both fiber-based devices as well as equipment for free-space optics. Specifically, the Mach-Zehnder interferomenters are realized in free-space in most of our implementations. Rarely, we make use of a fiber-based Mach-Zehnder with a free-space delay line. In both cases, the relative phase between the two arms is adjusted and stabilized by tuning a piezoelectric transducer, that is mounted on a mirror included in the long arm. In addition, the relative phase can be also adjusted by finely tuning the output wavelength of the CoBrite laser source. Notably, the use of free-space propagation causes additional insertion loss in the measurement setup, due to the imperfect coupling with the fibers. A totally fiber-based interferometer would be more compact and would bring less loss, but it requires precise fiber splicing to set the right delay in the long arm. Moreover, fiber-based implementations exhibit much more instability of the interference and therefore, they continuously require an active stabilization of the phase drifts, as we do in some of our works.

2.4.1 Single-photon detectors

The single-photon detectors used in our setups are semiconductor-based devices, called single-photon avalanche diodes or SPADs. In particular, the SPADs based on p-n junctions made of InGaAs/InP (indium gallium arsenide/indium phosphide) enable the photoelectric effect in the near-infrared spectrum from 900 nm to 1700 nm,

thus including the telecom C-band [105]. The junction is biased with a reverse voltage well above the breakdown threshold, in a way that even a single charge carrier is able to trigger an exponentially-growing avalanche of carriers, that is sensed by an internal circuit and used to produce a standard "click" signal. After every click event, the avalanche current is quenched by lowering the voltage below the breakdown threshold, causing the detector to be inactive for the time interval necessary to reset the normal conditions of operation. Such time interval, during which the SPAD can not detect the incoming photons, is called dead time t_D and it affects the observed count rate of the detector, which can be estimated by

$$\mathcal{R} \simeq \frac{\mathcal{R}_{ns}}{1 + \mathcal{R}_{ns} \cdot t_D} \ , \tag{2.2}$$

where $\mathcal{R}_{ns} = \eta_d \mathcal{F}$ is the expected count rate of the ideal detector without dead time, which is directly proportional to the incoming photon flux $\mathcal{F}$, through the photon-detection efficiency η_d. Notably, if $\mathcal{R}_{ns} \gg 1/t_D$, the observed count rate approaches its maximum value $1/t_D$ and the detector is said to work in saturation regime.

Actual single-photon detectors suffer from noise counts, which also affect the observed count rate $\mathcal{R}$. SPAD detectors are usually cooled down with a Peltier cooler, in order to reduce the random dark counts arising from the thermally-generated carriers. Another source of noise is the afterpulsing, caused by the carriers that get trapped during an avalanche and are subsequently released (thus triggering a second avalanche) with a fluctuating delay time. The afterpulsing probability becomes negligible for sufficiently long dead times, such that all trapped carriers are released when the detector is inactive. Furthermore, another relevant parameter for time-bin encoding is the timing jitter, that quantifies the statistical fluctuations of the time delay between the arrival of the photon and the generated click signal.

In our experiments, we mainly use fiber-coupled InGaAs/InP SPADs from ID Quantique and Micro Photon Devices, operating in free-running mode. Such devices offer a maximum detection efficiency $\eta_d = 0.20 \div 0.25$ (at 1550 nm) and a timing jitter below 200 ps. We usually set the dead time as $t_D = 20\,\mu$s in order to reduce the afterpulsing probability to a few percent, with a dark count rate ranging from 100 Hz to 3 kHz, depending on the specific device. Although higher efficiency and count rates can be achieved with superconductive single-photon detectors (i.e., more expensive devices that require cryostats for cryogenic cooling [106]), the performances offered by commercial SPADs at the telecom wavelenghts are sufficient to enable metropolitan-scale QKD.

2.4.2 Data acquisition and analysis

During the acquisition, the time tagger transmits the collected time tags to a computer, where a Matlab or Python software performs the data analysis in real time by processing, one by one, every buffer of transmitted data. In particular, we use the quTAG time tagger from Qutools, which marks each detection event by returning the time difference, in picoseconds, between the tagged event and the last reference signal received from the FPGA board. This enables to compare the detection events with the fixed sequence of quantum states prepared at the transmitter: all the events that are projected in the wrong basis are discarded (sifting), while the amount of not discarded detections returning the wrong outcome determines the error rates of the QKD setup. To compute the error rates and the sifted detection rates, we consider only the detection events that occur within a temporal interval, of about 200 ps, that is defined around the centre of each time bin. All the clicks that have occurred outside this time interval are discarded. This post-selection of detection events allows to improve the signal-to-noise ratio, since random dark counts, afterpulses and carving errors are more likely to be discarded by the temporal filter.

A graphical user interface is used to display, in real-time, the overall count rates of the detectors, the sifted detection rates and the computed error rates, as well as the estimated μ_k intensities. Monitoring these real-time data allows us to refine the experimental settings at both the transmitter and the receiver, such as the applied voltage to the optical modulators and the visibility optimization in the interferometers. Moreover, histograms of the observed pulse shape in the time-bin window are computed and displayed for each detector, in order to evaluate the timing jitter of the experimental setup, but also to monitor the time drifts introduced by the fiber links, which need to be compensated by adjusting the position of the post-selection temporal filter.

In most of our experiments, time tags are continuously collected for several minutes or tens of minutes, in order to acquire enough statistics of the experimental results. During the acquisition time, the observed fluctuations of the error rates, sifted detection rates and μ_k intensities are generally of a few percent. Based on the measured rates from the acquired data, the useful parameters of the QKD protocol are estimated and used to extrapolate the achievable secure key rate, by computing the theoretical bounds presented in the previous Chapter. In some cases we performed continuous acquisitions over several hours, by realizing an automatic system for self-stabilization of the quantum measurements, as described in Chapter 5.

3

High-dimensional QKD with efficient time-bin encoding

The first contribution to be presented in this thesis concerns an experimental work that was carried out in 2019, mostly during my external stay as guest Ph.D. at the Danish Technical University (DTU), in collaboration with the research group of High-Speed Optical Communications at DTU Fotonik. In addition, the Department of Applied Physics from University of Geneva contributed to the theoretical definition of the QKD protocol that was tested in this experimental work. The results were published in Ref. [22] and were presented as an oral contribution at QCRYPT 2020, the 10^{th} international conference on quantum cryptography.

The aim of this work is to test an efficient version of the four-dimensional QKD protocol with time-bin encoding, by taking advantage of a simplified and cost-effective setup that, despite its simplicity, still enables the doubling of the key generation rate in comparison with an analogous two-dimensional protocol, with a comparable equipment in terms of complexity and costs. In the following, the motivations behind this work and the experimental results are presented.

3.1 Time-encoded qudits

High-dimensional encoding for quantum communication can take advantage of multiple degrees of freedom of photons, such as time, energy, path, orbital angular momentum and combinations of them[1], in order to enlarge the Hilbert space dimension [13,21,77–81,107]. Nonetheless, as already mentioned in the previous Chapters,

[1] As opposed to the above-mentioned degrees of freedom, polarization-encoded quantum states live in a two-dimensional Hilbert space, thus they have to be combined with other degrees of freedom in order to enlarge the space dimension [21].

time-bin encoding is the most practical choice for high-dimensional QKD based on the conventional and widespread single-mode fibers (SMF). This is because multiple time bins can be easily involved in the definition of high-dimensional quantum states, without need to resort to other different degrees of freedom, such as orbital angular momentum and path encoding (which require free-space propagation or air-core fibers, and multi-core fibers, respectively, to be distributed [77, 79–81]), or energy encoding (which requires a source for parametric down-conversion [78, 107]). Conversely, more conventional equipment (such as attenuated laser sources, optical modulators and interferometers) based on standard SMF cables, is sufficient to prepare, measure and distribute the time-encoded qudits. The main drawback of using time-bin encoding is that, given a fixed repetition rate at the source, the actual state preparation rate (or symbol rate) decreases by increasing the dimension d, since the time duration of a single qudit becomes longer as it occupies d time bins. Nonetheless, as already pointed out as a general result, high-dimensional protocols with large d are more damaged by the random noise counts in the measurement setup, resulting in a reduction of the maximum distance affordable by QKD. Furthermore, from a practical point of view, as d increases the preparation and measurement of qudits require, in general, a complex setup with a larger amount of expensive resources, especially at the receiver, who has to perform projective measurements on two mutually-unbiased bases of d orthogonal states. In the specific case of time-bin encoding, this usually requires an increasing amount of cascaded interferometers, with practical issues of loss and stability [13, 108, 109]. In the following, we will focus on the time-encoded QKD protocol with $d = 4$.

3.1.1 The four-dimensional protocol

In the four-dimensional time-bin encoding, $d = 4$ time bins (t_0, t_1, t_2, t_3) are involved in the definition of each quantum state. It is convenient to represent the qudits in the time-of-arrival basis $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$, that is the particular basis of orthogonal states where only one time bin is occupied in each state (see Figure 3.1). Then, all the unbiased bases with respect to the time-of-arrival basis, must have all of the four bins equally combined in each state, with different phase relations among the bins. An example is given by the following set of orthogonal states:

$$|f_m\rangle = \frac{1}{2}\sum_{j=0}^{3} \mathrm{e}^{\imath\frac{\pi}{2}mj}|j\rangle \ , \tag{3.1}$$

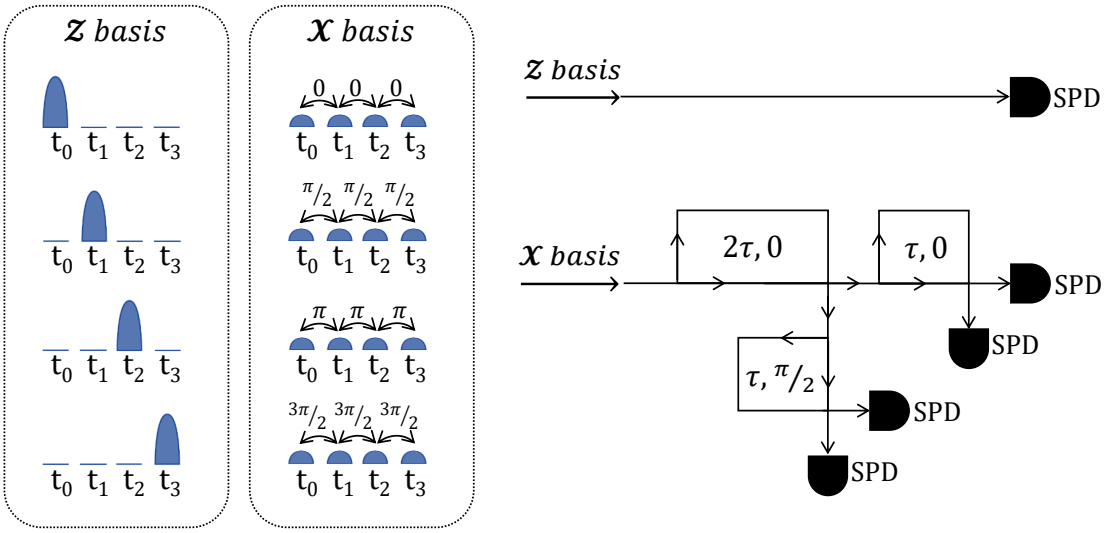


Figure 3.1: The conventional choice of mutually-unbiased bases in the four-dimensional time-bin protocol: the time-of-arrival basis $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ ($\mathcal{Z}$), and the Fourier basis $\{|f_0\rangle, |f_1\rangle, |f_2\rangle, |f_3\rangle\}$ ($\mathcal{X}$). This choice leads to a very unbalanced implementation of the measurement setup, as a cascade of three interferometers, with different delay lines (τ, 2τ) and phase shifts (0, $\frac{\pi}{2}$), equipped with four single-photon detectors (SPD), is necessary to perform the $\mathcal{X}$ basis projection.

with $m = 0$, 1, 2 and 3. In this set of states, also called the Fourier basis, each qudit is denoted by a different phase shift between the consecutive bins, as illustrated in Figure 3.1. The choice of unbiased bases from Figure 3.1 is adopted in the QKD experiment from Ref. [13], where the authors demonstrate a record-breaking rate of secure key generation of 26.2 Mbit/s with a fiber channel of 4 dB loss. The protocol is a BB84 variant with finite-key analysis and two decoy intensities (vacuum and weak decoy) and the receiver is equipped with superconducting single-photon detectors. The time-of-arrival basis can be directly measured with a single detector, even though the beam is split into four different detectors in Ref. [13], in order to reduce the saturation effect. The projection on the other basis is much more complex, as it requires a tree of cascaded interferometers (with different delay lines and phase shifts) and four single-photon detectors, as depicted in Figure 3.1. Here, τ is the time-bin duration, equivalent to 400 ps in the cited work. The first interferometer with 2τ delay (and 0 relative phase between the two arms) is used to produce the interference between non-consecutive bins, while the two subsequent interferometers, both having τ delay, are used to observe the interference between consecutive bins. Notably, $|f_0\rangle$ and $|f_2\rangle$ states exit the 2τ interferometer from the first output (0 relative phase), while $|f_1\rangle$ and $|f_3\rangle$ are directed to the second output (π relative phase).

Then, the first (or second) output is analyzed with the τ-delay interferometer having 0 (or $\frac{\pi}{2}$) relative phase. As a result, the detection signal returned from one of the four outputs of the two τ-delay interferometers, denotes the occurred projection on the corresponding $|f_m\rangle$ state.

Despite the simplicity of the time-of-arrival basis, whose preparation and measurement is straightforward, the states from the Fourier basis are much more difficult to prepare, since four different levels of phase modulation (0, $\frac{\pi}{2}$, π, $\frac{3}{2}\pi$) are required, and also to measure, since three interferometers have to be optimized and stabilized simultaneously. While the four-level signal necessary for phase modulation can be provided with proper electronics, the simultaneous stabilization of the three interferometers, which are also cascaded, can be very challenging [108]. Moreover, four different detectors are required to complete the projection on the Fourier basis. This rises considerably the implementation costs, given that a single-photon detector is the most expensive device of the experimental equipment, even when using semiconductor-based devices in place of superconducting detectors. Furthermore, using more detectors brings more detection events arising from the random dark counts, considering also the higher amount of vacuum events due to transmission loss in the interferometric setup. Notably, using a different setup would lead to an approximately unbiased basis with respect to the arrival time, as shown in Ref. [110].

In the end, the choice of the time-of-arrival basis in the four-dimensional protocol leads to a very unbalanced implementation of the two unbiased bases, requiring an experimental setup whose complexity and costs are considerably higher, in comparison with standard QKD with two-dimensional encoding [57, 76, 111].

3.2 Proposed setup and experimental results

In our work [22], we experimentally test a time-bin QKD protocol with $d = 4$, without using the time-of-arrival basis. Conversely, we exploit time-encoded qudits where two time bins are combined in both bases, with only 0 or π relative phases. Such bases are depicted in Figure 3.2 and can be expressed as follows:

$$\mathcal{Z} = \frac{1}{\sqrt{2}} \begin{pmatrix} |0\rangle + |1\rangle \\ |0\rangle - |1\rangle \\ |2\rangle + |3\rangle \\ |2\rangle - |3\rangle \end{pmatrix} , \qquad \mathcal{X} = \frac{1}{\sqrt{2}} \begin{pmatrix} |0\rangle + |2\rangle \\ |0\rangle - |2\rangle \\ |1\rangle + |3\rangle \\ |1\rangle - |3\rangle \end{pmatrix} , \tag{3.2}$$

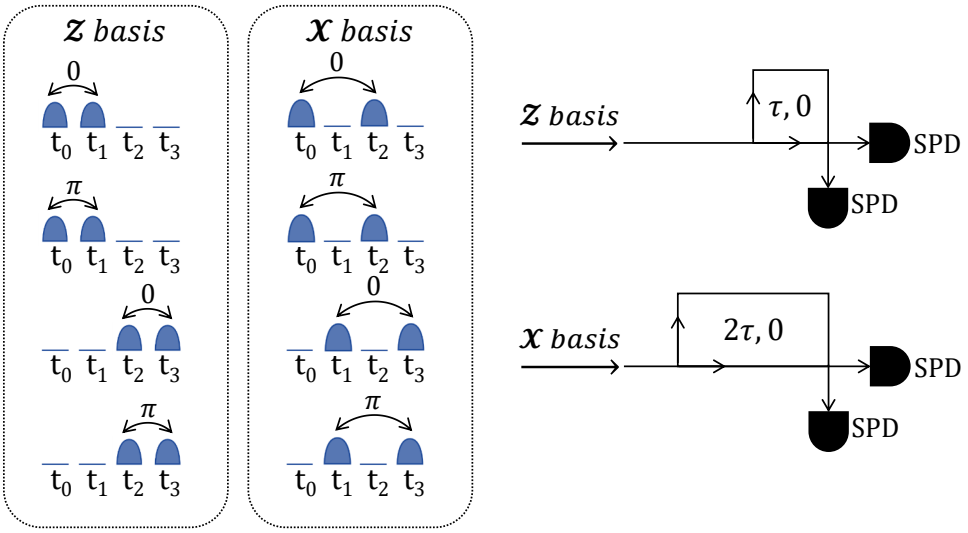


Figure 3.2: The two unbiased bases that are tested in our efficient time-bin protocol. Here, superposition states of two bins are taken in both $\mathcal{Z}$ and $\mathcal{X}$ basis, thus making the two bases very similar to implement, both in the preparation as well as in the measurement setup. Two independent interferometers with different delay lines (τ, 2τ), each one equipped with two single-photon detectors (SPD), are sufficient to carry out all the projective measurements.

where $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ denote the time-of-arrival basis. These two sets of states are mutually unbiased, as they satisfy the general relation 1.4. The choice of taking superposition states of two time bins, makes the two unbiased bases very similar to each other, both in the preparation as well in the measurement setup. At the transmitter side, after the carving of the pulse pattern, the phase has to be modulated between two levels only, that can be done by using a proper squared signal as described in Section 2.3.2. At the receiver, a single interferometer with τ or 2τ delay, respectively, is sufficient to project on the $\mathcal{Z}$ basis (defined by pairs of consecutive bins) or on the $\mathcal{X}$ basis (defined by pairs non-consecutive bins). As shown in Figure 3.2, the two interferometers are independent from each other, and their outputs are directly monitored with single-photon detectors. Differently from the Fourier basis, now each detector measures also the time bin at which the interference occurs, thus enabling to distinguish between the two states defined by the same phase shift but involving different pairs of time bins. For instance, when measuring the first and third states from $\mathcal{Z}$ basis with the τ-delay interferometer, the same detector will click but with different arrival times t_1 and t_3, respectively. The same holds for $\mathcal{X}$-basis projection with the 2τ interferometer, where interference is observed at the time bins t_2 and t_3, depending on the incoming state. Notably, now both the arrival

time and the relative phase are combined in the definition of each qubit, as opposed to the conventional choice of bases, where each state was defined, instead, by only one degree of freedom, arrival time or relative phase.

In our experimental work, we further simplify the receiver setup, by taking advantage of the independence of the two interferometers, each one corresponding to a different basis projection. The main idea is that the smaller interferometer (with τ delay) can be nested inside the bigger one (2τ delay), in a way that the short arm is in common between the two interferometers, while the long arm is switched between two different paths, corresponding to the τ and 2τ delay lines, respectively, that are selected depending on the basis to be measured. In this way, only two single-photon detectors, instead of four, are necessary at the receiver setup (which also becomes more compact), at the cost of implementing an active basis choice at Bob's side, achievable with high-speed modulators or optical switches. Notably, despite their overlap, the two interferometers can be controlled and stabilized independently from each other, by acting on the two independent delay lines in the long arms.

Our implementation of the four-dimensional protocol is reported in Figure 3.3a. Here, we use two nested Mach-Zehnder interferometers that are assembled in a totally free-space setup. The two different delay lines (τ and 2τ) are selected by means of polarizing beam splitters (PBS). Consequently, the basis choice at Bob's side is performed by aligning the incoming signals along one of the two orthogonal polarizations defined by the PBS. This can be achieved by using a polarization modulator. However, we do not include such modulator in our setup, but we replace it with a manual polarization controller (PC), as shown in Figure 3.3a.

A final comment is on the actual differences between of the two bases, from an experimental point of view. Despite the close resemblance in the preparation and measurement, we observe a modest increase in the experienced errors when measuring the $\mathcal{X}$ basis, in comparison with the $\mathcal{Z}$ basis. This is mainly due to the longer interferometer associated to $\mathcal{X}$-basis projections, which is intrinsically less stable than the shorter one. Another contribution is the timing jitter of the detectors, since the time bins observed in the $\mathcal{X}$-basis projection (t_2, t_3) are closer than those observed for $\mathcal{Z}$ basis (t_1, t_3).

3.2.1 Comparison with binary-encoded QKD

In our work, the proposed scheme for efficient time encoding is experimentally tested by performing an asymmetric BB84 protocol in four dimensions, with one decoy

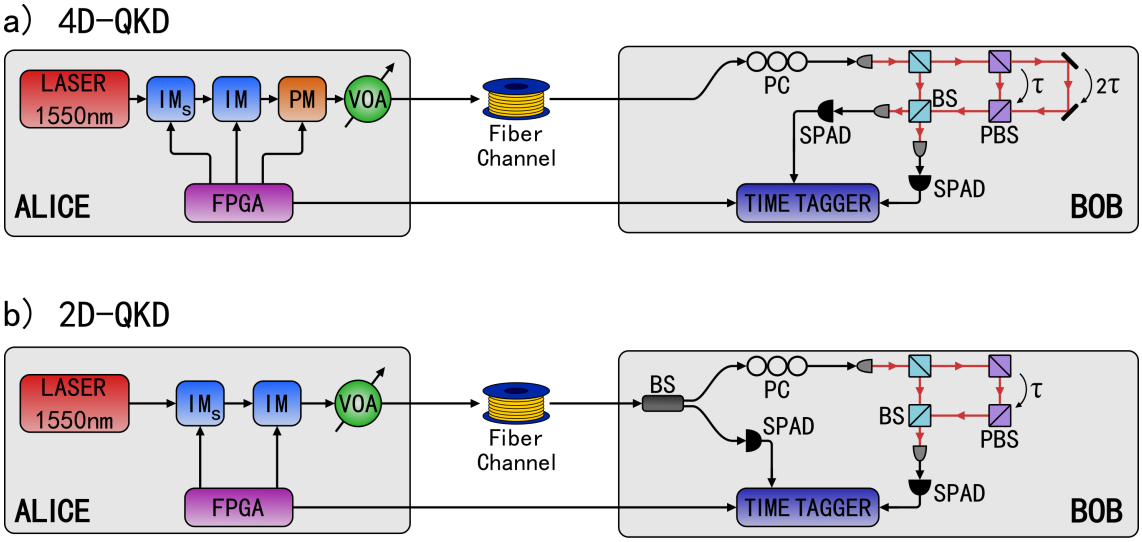


Figure 3.3: This Figure from our work [22] illustrates the experimental setup used to test the two time-encoded protocols that are compared in our work: (a) the four-dimensional protocol with efficient encoding and (b) the simplified BB84 in two dimensions with three states. IM: intensity modulator, PM: phase modulator, VOA: variable optical attenuator, FPGA: field programmable gate array board, PC: polarization controller, BS: beam splitter, PBS: polarizing beam splitter, SPAD: single-photon avalanche diodes, based on fiber-coupled InGaAs/InP detectors. The functioning of our experimental setup is further described in Sections 2.3 and 2.4 of Chapter 2.

state and finite-key analysis. The security analysis for this protocol, reported in Section 1.4.1, is based on previous works on two-dimensional protocols with one and two decoys, in a finite-key regime, as discussed in Chapter 1. In order to assess and benchmark our QKD scheme, a two-dimensional protocol is also tested in the same work, by employing mostly the same experimental equipment, as illustrated in Figure 3.3b. Specifically, we opted to test the simplified three-state BB84 with time-bin encoding and one decoy state [9,56,57], that is described in Section 1.3.3.1 of Chapter 1. The reason for this choice is that also the three-state protocol is an efficient version of the four-state protocol[2], whose time-encoded states are depicted in Figure 2.1 of Chapter 2. Similarly to our four-dimensional setup, the three-state protocol requires only two single-photon detectors, instead of three as shown in Figure 2.1, because Bob measures the $\mathcal{X}$ basis by projecting only on $|-\rangle$ state, while

[2]Despite its cost-effectiveness, it has been shown that the secure key rate achievable with the three-state protocol is close to the one achievable with the four-state BB84 [56]. Moreover, the three-state protocol was implemented in the record-breaking experiment of QKD with more than 400 km of ultra-low-loss fiber link [9].

Alice prepares only $|+\rangle$ state from $\mathcal{X}$ basis. Therefore, only one detector is needed to monitor a single output of the interferometer, while another detector directly measures the arrival time for $\mathcal{Z}$-basis projection, as shown in Figure 3.3b. As a result, the two setups reported in Figure 3.3 are very close in terms of complexity and costs, since the additional equipment required in the four-dimensional setup just includes two devices from the telecommunication industry: the phase modulator at the transmitter and the polarization switcher at the receiver. Moreover, both protocols are implemented with only one decoy state, they offer the same level of security against general attacks in the quantum channel, and take into account one-way post-processing and finite-size effects in the secure key generation.

The functioning of our experimental setup at the transmitter (Alice) and the receiver (Bob) is further described in the previous Chapter (see Sections 2.3 and 2.4). It should be remarked that, although two different carving patterns (both custom) are provided by the FPGA for testing the two time-encoded protocols, the same time bin duration ($\tau \simeq 840\,\text{ps}$) is set in both cases. Consequently, the state preparation rate (or symbol rate) at the transmitter is $1/(2\tau) \simeq 595\,\text{MHz}$ for qubits and $1/(4\tau) \simeq 297.5\,\text{MHz}$ for qudits. This enables a fair comparison between the two protocols, which takes into account the slower symbol rate in the high-dimensional case. In addition, due to the same bin duration, the same interferometer with the shorter delay line is used to project both the qudits on $\mathcal{Z}$ basis as well as the qubits on $\mathcal{X}$ basis. In the latter case, the polarization direction of the incoming signals is kept fixed along the direction that is reflected by the PBS[3]. Bob's basis choice in the two-dimensional protocol is performed passively, with a fiber-based beam splitter. The overall loss of the τ-delay and 2τ-delay interferometer is 2.3 dB and 2.5 dB, respectively, due to imperfect beam splitting and fiber to free-space coupling, which lower the visibility of interference.

3.2.2 Results and discussion

The two QKD protocols are tested for different loss of the quantum channel, by propagating the quantum signals through some spools of SMF with different lengths, up to 145 km (31.5 dB loss). The experimental results are reported in Table 3.1 and in Figure 3.4. The first task to be fulfilled when testing each protocol is finding the optimal experimental parameters, such as the basis choice probabilities ($p_{\mathcal{Z}}$ and

[3]Notably, the two PBS in Figure 3.3b could be replaced with standard mirrors, when testing the two-dimensional protocol.

	two-dimensional protocol						**four-dimensional protocol**					
SMF dB	μ_1	μ_2	$p_{\mathcal{Z}}^B$	qber %	$\phi_{\mathcal{Z},1}^U$ %	SKR bit/s	μ_1	μ_2	$p_{\mathcal{Z}}^B$	qber %	$\phi_{\mathcal{Z},1}^U$ %	SKR bit/s
5.1	0.07	0.03	0.5	1.1	6.6	15 k	0.10	0.05	0.7	3.4	3.9	37 k
14	0.12	0.06	0.9	1.1	9.2	12 k	0.20	0.10	0.7	3.4	4.6	24 k
23	0.26	0.14	0.5	1.4	8.9	5.1 k	0.21	0.10	0.7	4.9	5.7	5.5 k
31.5	0.31	0.15	0.5	2.3	13.6	0.53 k	0.18	0.08	0.5	7.9	7.2	0.42 k

Table 3.1: Experimental parameters and results of our work [22]. The two protocols are tested with different channel lengths of single-mode fiber (SMF), by setting the optimal parameters such as the mean photon number of signal (μ_1) and decoy (μ_2) states, and the basis choice probability at the receiver ($p_{\mathcal{Z}}^B$). From the acquired data, we compute the error rate in $\mathcal{Z}$ basis (qber) and the upper bound on the phase error rate ($\phi_{\mathcal{Z},1}^U$), necessary to extrapolate the achievable secure key rate (SKR), by evaluating the theoretical bounds reported in Chapter 1.

$p_{\mathcal{X}} = 1 - p_{\mathcal{Z}}$) and the signal and decoy intensities (μ_1, μ_2), that maximize the achievable secure key rate, at each different channel loss. The decoy probability (0.5) and the basis choice at the transmitter ($p_{\mathcal{Z}}^A = 0.9$) are kept fixed for both protocols at all channel lengths. The basis choice probability at the receiver ($p_{\mathcal{Z}}^B$), together with μ_1 and μ_2 values, are optimized by simulating the protocols under the expected experimental conditions, and are reported in Table 3.1. The numerical simulations return the expected secure key rate achievable with our setup, as a function of the channel loss, as reported in Figure 3.4b with solid lines. To estimate the secure key rate, the secure key length is computed from the theoretical bounds for finite-key analysis as discussed in Chapter 1, by setting, for both protocols and for every channel loss, a post-processing block size of 10^7 symbols, with a correctness and secrecy parameters of $\varepsilon_{sec} = \varepsilon_{corr} = 10^{-9}$.

The acquired experimental data are analysed in order to evaluate the detection rates and the error rates in both bases. The symbol error rate experienced in $\mathcal{Z}$ basis, or qber, is reported in Table 3.1 and in Figure 3.4a, together with the upper bound on the phase error rate for single-photon events, $\phi_{\mathcal{Z},1}^U$, that is computed from the experimental data, and whose value depends also on the experienced error rate in $\mathcal{X}$ basis. As can be deduced from Figure 3.4, the error rates generally increase

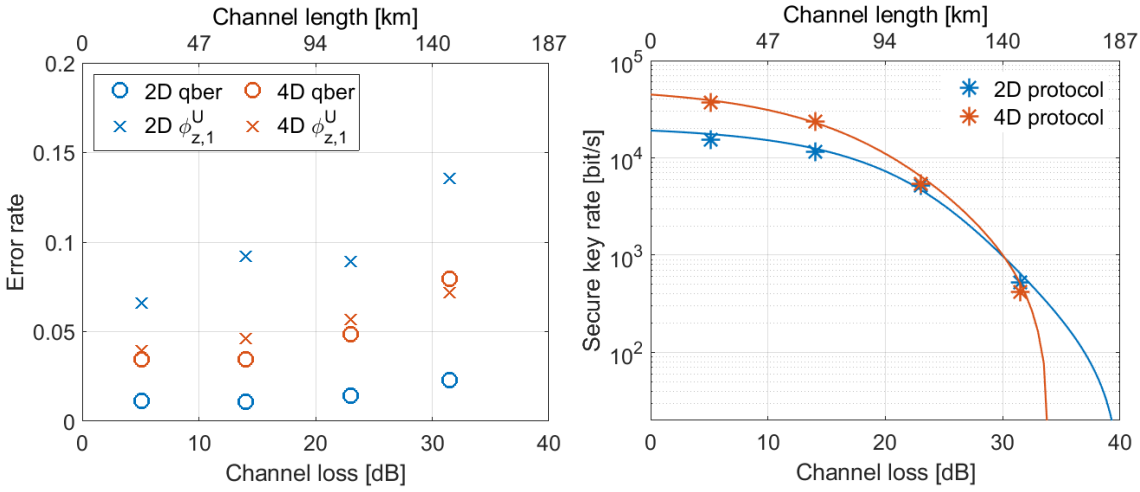


Figure 3.4: Experimental results of our work [22], obtained at different loss of the quantum channel, corresponding to different lengths of SMF. The tested fiber spools exhibit an average attenuation of 0.214 dB/km. Figure (a) shows the experienced error rates from the two protocols, as reported in Table 3.1. Figure (b) shows the secure key rate achievable from the acquired data, together with the simulated behaviour (solid lines), as a function of the channel loss, that is expected with our experimental setup.

with the channel loss, due to the progressive reduction of the signal-to-noise ratio at the receiver: as the detectors gradually exit from the saturation regime, the random noise counts and the modulation errors in the state preparation, become more and more frequent in the overall detected events. Concerning the two different protocols, it is not surprising that the qber measured in $\mathcal{Z}$ basis is better in the two-dimensional case, where it is related to a direct measurement of arrival time. Differently, in the four-dimensional protocol the experienced errors in $\mathcal{Z}$ basis arise both from time errors as well as interference errors. From an experimental point of view, measuring the relative phase is typically more challenging than measuring only the time of arrival, as interferometric measurements require an optimal and stable visibility of interference, which depends on the internal phase drifts but also on the optimal balance of the two arms in terms of temporal delay and power. Therefore, a totally time-of-arrival measurement usually returns less errors than a combination of interference ad arrival time, in agreement with the experienced qbers from two $\mathcal{Z}$-basis measurements. Accordingly, one would expect a comparable error rate in the $\mathcal{X}$ basis from the two protocols, being the interference the main source of errors in both cases. However, the experienced $\phi^U_{\mathcal{Z},1}$ is worse in the two-dimensional

case. We believe that this result is due to the fact that only one output of the interferometer, the one related to destructive interference ($|-\rangle$ state projection), is monitored in the two-dimensional protocol, while both outputs are monitored in the four-dimensional setup. As a consequence, from a practical point of view, the optimization of the interference during the data acquisition is more challenging in the two-dimensional case. Otherwise, in four-dimensional measurements, the visibility can be maximized more efficiently, thus resulting into less interference errors. Furthermore, it is worth noting that the error rates qber and $\phi^U_{\mathcal{Z},1}$, are close to each other in the four-dimensional case, where the two bases have a similar structure, as opposed to the two-dimensional protocol, where the bases are highly unbalanced due to the involvement of the time-of-arrival basis.

The secure key rate (SKR), extrapolated from the experimental data acquired in each scenario, is reported in Table 3.1 and in Figure 3.4b. Our results show an improvement of the achievable SKR up to 23 dB loss, corresponding to 105 km of SMF channel. Conversely, at longer fiber channels, the SKR achievable in the four-dimensional protocol drops off more quickly than in the binary-encoded protocol, due to the more damaging effect of random noise counts in the experienced error rates, as discussed in Section 1.4. According to the simulations of our experimental setup (solid lines in Figure 3.4b), a positive SKR can be extrapolated up to 34 dB loss and up to 39 dB loss in the four- and two-dimensional case, respectively. At short channel distances, instead, when the detectors are more saturated and the weight of random noise counts is lower, we demonstrate a higher SKR of 2.4 and 2.0 times, respectively, at 5.1 dB loss (25 km) and 14 dB loss (65 km). Furthermore, it is interesting to notice that the amount of secure key bits that can be extracted from each quantum state, is larger in the four-dimensional protocol at all the experimental points, i.e., at least up to 31.5 dB loss. This quantity, that measures the photon information efficiency at each channel loss, is evaluated from the ratio of the obtained SKR with the rate of state preparation, that is twice faster in the two-dimensional case, due to the halved temporal duration of qubits in comparison with the qudits. At 31.5 dB of channel loss, the amount of extractable secure bits from each single qudit is 1.4×10^{-6}, while it is 8.9×10^{-7} from each qubit. Consequently, the lower SKR obtained in the four-dimensional protocol is just a consequence of the fact that we have a halved symbol rate at the transmitter, in comparison with the two-dimensional case.

3.2.3 Final comments

In the experimental work described in this Chapter, we successfully demonstrate a efficient and cost-effective protocol for high-dimensional QKD with time-bin encoding, able to run with a simplified and compact setup, whose complexity and costs are comparable with those of standard and binary-encoded QKD.

A first comment is on the implementation of real-time basis choice in the four-dimensional receiver, that is not carried out in our work since we replace the polarization modulator with a manual polarization controller. An additional modulator is likely to increase the insertion loss in the receiver setup, at least of 2 dB. Moreover, extra errors might be introduced by imperfect modulation, due to the incoming signals that are not properly directed into the desired delay line. By considering the additional insertion loss and the typical extinction ratio of high-speed optical modulators (> 20 dB), it is likely to expect a lower SKR achievable by the four-dimensional protocol at long distances (23 dB and 31.5 dB loss). Nonetheless, an improvement of the SKR, in comparison with the binary-encoded protocol, is still expected at short distances, in the saturation regime of detectors.

Secondly, it would be useful to optimize, for each channel loss, all the constant parameters of the experimental setup (such as the probabilities of basis choice and decoy preparation at the transmitter side), in order to maximize the SKR and the transmission distance achievable by the two protocols. Moreover, it would be interesting to test the two protocols with two decoy intensities, instead of only one decoy. Although it has been shown that, for the two-dimensional protocol, the one-decoy implementation can be even more advantageous than the two-decoy implementation [55], the same conclusion has not yet been proven for the four-dimensional case. Therefore, our four-dimensional setup might be more favored by the two-decoy technique, thus enabling it to outperform the binary-encoded protocol at longer distances. Furthermore, the overall performance of the two-decoy implementation of our four-dimensional setup, equipped with superconducting single-photon detectors, could be compared with the work from Ref. [13], where the conventional time-bin encoding in four dimensions is implemented, with two decoy states, in order to achieve the record-breaking SKR of 26.2 Mbit/s at 4 dB loss.

Finally, due to the higher robustness to noise expected with high-dimensional QKD (as discussed in Section 1.4), it would be interesting to test, at short distances, the four-dimensional and the binary-encoded protocols under the same conditions of increasing noise in the quantum channel. Such a trial under real-world circumstances

could promote, even more, the research of efficient solutions for high-dimensional QKD based on single-mode fiber links.

4

High-dimensional version of the round-robin QKD

In this Chapter it is presented another main contribution of this thesis, concerning a theoretical and experimental work that was carried out at the Danish Technical University (DTU) and at the CNR-INO headquarter of Florence. In addition to the High-Speed Optical Communications group from DTU Fotonik, the Beijing University of Posts and Telecommunications (China) contributed to the research work, and in particular to the theoretical analysis of the QKD protocol here presented. The results were published in Ref. [23].

In this work, we propose an improved version of the round-robin protocol for differential-phase-shift QKD. As it will be shown in the next Section, the round-robin protocol is really peculiar, as it offers the unmatched benefit of not requiring the monitoring of the quantum channel, in order to bound the information leakage to a potential eavesdropper. The main idea behind our contribution, presented in Section 4.2, is to enlarge the Hilbert space dimension of the original round-robin protocol, by including the information encoding on the time-bin degree of freedom. Our proposed protocol, referred as the round-robin differential phase-time-shifting QKD, is demonstrated to be more noise tolerant, in comparison with its original version. Specifically, through numerical simulations we show that our protocol can successfully distribute a secure key, even in the condition when the interference disturbances are such to make unfeasible the original round-robin QKD. In order to test our theoretical results, the outcomes of a proof-of-principle experiment are reported and discussed in the same work.

4.1 The round-robin protocol

The round-robin protocol, introduced in 2014 [94], directly evolves from differential-phase-shift (DPS) QKD [92, 112–114], where a secure key is extracted from the process of encoding and decoding on the relative phase shifts, 0 or π, defined between consecutive weak pulses, that are continuously transmitted from Alice to Bob. Differently, in the round-robin DPS protocol, the relevant phase shifts are not only those between adjacent pulses, but are decoded circularly, by defining separate packets of L weak pulses. The protocol, illustrated in Figure 4.1, is structured as follows:

(I) Alice prepares packets of L weak pulses, with a mean photon-number per pulse μ and a mean photon-number per packet $\nu = \mu L$. She sets a random phase shift between the consecutive pulses in each packet, by choosing uniformly at random between the two values 0 and π. Then, she sends the pulse packets to Bob.

(II) Upon receiving each packet, Bob chooses a random number $r \in \{1, 2, ..., L-1\}$, then he consequently sets a delay-line equivalent to r pulses, by adjusting his Mach-Zehnder interferometer, monitored with single-photon detectors. As shown in Figure 4.1, the split packet interferes with itself, by returning a detection signal at the b-th position in the packet. This means that the a-th and b-th pulses in the packet, with $b = a + r$ and $a, b \in \{1, 2, ..., L\}$, have interfered with each other. Based on the measurement result (0 or π), Bob collects one bit of raw key. He discards all the events returning no clicks, or more than one click, within his observation window, whose duration depends on the random r (as shown in Figure 4.1).

(III) After having repeated the above process many times, Bob announces the indices a and b (or equivalently, b and r) related to each detection event. In this way, Alice can recover the relative phase information that, together with Bob's measurements results, constitutes the raw key string, respectively at each side.

(IV) In conclusion, standard post-processing procedures of error correction and privacy amplification are performed to extract the secure key.

As shown above, in the round-robin protocol the raw key bit to be extracted from each packet is determined by the random delay choice at the receiver. This makes it really hard for Eve to correctly guess it, since she is unable to learn, in principle, all the relative phases between each pair of weak pulses included in the packet. In particular, as shown in Ref. [94], the amount of raw key information that Eve can access is bounded by L and ν, which are experimental parameters to be decided by Alice

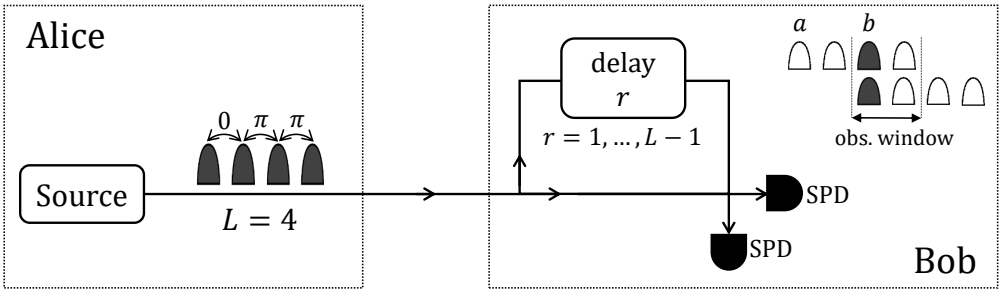


Figure 4.1: Schematic depiction of the round-robin DPS protocol. Here, Alice prepares a packet of $L = 4$ weak pulses, with random phase shifts between consecutive pulses $(0, \pi)$. Bob picks a random number $r \in \{1, 2, ..., L-1\}$ (here, $r = 2$) and consequently adjusts the delay line of his Mach-Zehnder interferometer, monitored with single-photon detectors (SPD). The detection event occurs at the b-th position within Bob's observation window, meaning that the a-th and b-th pulses in the packet (with $b = a + r$) have interfered with each other. Based on the interference output (0 or π), Bob collects a bit of raw key. He publicly announces the indices a and b, hence enabling Alice to recover the relative phase information as a bit of her raw key.

and Bob. Remarkably, this is what makes the round-robin approach totally different from the other QKD protocols, where the information leakage is determined, instead, from some experimental result describing the channel disturbances, such as the experienced error rate. Conversely, in round-robin QKD, the information leaked to Eve can be computed from the users own settings, regardless of the disturbance that she causes on the quantum signals. As a consequence, the amount of bits to be lost during the privacy amplification does not depend on the channel behaviour, and goes to zero in the limit of large packet size L. The authors of Ref. [94] show, indeed, that in the asymptotic limit of large raw-key size, the generic bound for the secret fraction from Equation 1.27, becomes

$$r = 1 - \mathrm{leak}_{EC}(e_{bit}) - h\left(\frac{1}{L-1}\right) \tag{4.1}$$

for the round-robin protocol with a single-photon source [94]. Notably, the bit error rate on the raw key (e_{bit}, or qber) only affects the bit loss during the error correction procedure (leak_{EC}), but it is not necessary to evaluate the phase error rate, that is bounded as $e_{ph} \leq 1/(L-1)$. More generally, for an L-pulse packet containing n photons, the bound becomes $e_{ph} \leq n/(L-1)$, meaning that also the multi-photon components can be used, with sufficiently large L, to generate the secure key[1]. As

[1]As opposed to the other QKD protocols such as the BB84, as discussed in Section 1.3.1. Here, the multi-photon components can not be used for key extraction, since Eve can access all

a result, the round-robin DPS can tolerate, in principle, a higher e_{bit} than the other QKD protocols, thus making it feasible also in the more demanding conditions of high environmental noise [115, 116]. Moreover, without the need of monitoring the potential information leakage, there is no need to sacrifice a random subset of the raw key, for estimating the parameters (together with their statistical fluctuations) required to bound e_{ph}. This also reduces the expected impact of finite-size effects.

The main practical challenge of implementing the round-robin protocol is the random delay-line to be actively selected at the receiver, requiring high-speed optical switches and other electro-optical components. The higher is L, the more random delays have to be included in the interferometer. Nonetheless, experimental demonstrations of round-robin DPS have successfully tested the protocol with large packet sizes, up to $L = 128$ [117–119].

Since the information decoding in round-robin QKD is based on interferometric measurements (as in the other DPS protocols), the main contribution to the bit error rate e_{bit} is due to interference misalignment or unstable visibility, which cause the wrong detector to click. Poor visibility of interference is often due to the imperfect fabrication of the variable-delay interferometer, to the lack of an active feedback system for interference stabilization and also to environmental disturbances. Although the round-robin protocol can in principle tolerate a high e_{bit} by making the information leakage close to zero, the interference misalignment can still prevent to successfully distribute a secure key in many practical circumstances, under unstable experimental environments which degrade the interference visibility. Therefore, designing an improved protocol able to tolerate more interference errors, is essential to enable the use of round-robin QKD in many real-world applications.

4.1.1 Improved security bounds

Recently [116], the bound on the secure key length achievable with the round-robin QKD has been improved, by providing a tighter estimation of the information leaked to Eve, I_{AE} (i.e., the last term in the right side of Equation 4.1).

In the cited work [116], the authors evaluate I_{AE} by deriving Eve's optimal strategy under a collective attack scenario. Under this assumption, as shown in Chapter 1, the information leakage can be bounded by maximizing the Holevo quantity given in Equation 1.23, where the density matrix of Eve's ancilla has to be evaluated for

the information from these components without introducing any detectable errors (and errors are essential to estimate the information leakage in these protocols).

each different symbol of the raw key, i.e., $\rho_{E,0}$ and $\rho_{E,1}$ in the present case. As already mentioned in Chapter 1, the same security bound can be extended to the more general scenario of coherent attacks, if the transmitted packets are totally uncorrelated from each other. Similarly to the other protocols such as the BB84, this condition is satisfied also in the round-robin QKD, by assuming the randomization of the global phase of each L-pulse packet. Moreover, the phase randomization of the source enables to analyze independently all the different Fock components (or photon numbers n), and to derive the information leakage from each n separately, based on the probability distribution $P(n)$ describing the source.

The main steps of the security analysis proposed in the cited work [116], are reported in the Appendix A.1. The main idea of the authors is that some mixed components arising in Eve's density matrix can be ignored, being the relative phases of the different pulses in the packet totally random. Consequently, in order to compute the Holevo bound, Eve's density matrix can be notably simplified, by ignoring all the components that do not give any useful information about the relative phase between the pulses of interest a and b (where a, b are publicly announced during the protocol). As a result, Eve's information in the generic case of n photons per L-pulse packet, with $L \geq n+1$, can be bounded as

$$I_{AE} \leq \max_{x_1,\ldots,x_{n+1}} \left\{ \frac{\sum_{m=1}^{n} \varphi\big[(L-m)x_m, m x_{m+1}\big]}{(L-1)} \right\}, \tag{4.2}$$

with the function $\varphi(x,y) = -x\log_2(x) - y\log_2(y) + (x+y)\log_2(x+y)$. To evaluate the bound under Eve's optimal strategy, the quantity between parenthesis has to be maximized over the non-negative real parameters x_m, satisfying $\sum_{m=1}^{n+1} x_m = 1$. Remarkably, for the Fock components satisfying the constrain $n < L-1$, $I_{AE} < 1$ always holds, meaning that they can be used for key extraction [116]. Furthermore, the upper bound on I_{AE} from Equation 4.2 depends only on the users settings and not on the channel behaviour, although an even tighter bound can be derived by including the experienced error rates [116].

4.2 High-dimensional improvement with time-bin encoding

In our work [23], we propose an improved version of the round-robin DPS protocol, where an extra bit of raw key can be extracted from each L-pulse packet, by exploiting the additional encoding on the time-bin degree of freedom.

The inspiration for our proposal comes from a previous work of the research group from DTU Fotonik, published in Refs. [120, 121], where they developed a high-dimensional-like protocol by including the time-bin encoding in DPS QKD. Such protocol, derived under the framework of differential-phase-reference QKD, is called differential phase-time shifted (DPTS). Accordingly, the high-dimensional version of the round-robin DPS that is discussed here, is named round-robin DPTS protocol. Such protocol is illustrated in Figure 4.2 and is structured as follows:

(I) Similarly to the round-robin DPS protocol, Alice prepares packets of L weak pulses, with a mean photon-number per pulse μ and a mean photon-number per packet $\nu = \mu L$. In addition, each L-pulse packet is given a temporal profile, by choosing at random between two different sets of temporal patterns, the X basis and the Z basis (shown in Figure 4.2). In this way, each L-pulse packet is defined by the time-bin positions occupied by the L pulses (i.e., nonempty bins) and by the positions of the remaining L empty bins. The temporal duration of each bin (empty or nonempty) is quantified as τ. Specifically, Alice encodes a temporal bit of information (0, 1) by preparing the corresponding temporal profile, X_0 and X_1 or Z_0 and Z_1, depending on her random basis choice. Then, she also sets a random phase shift (0, π) between the consecutive pulses in the packet. Finally, she sends the pulse packets to Bob.

(II) As in the round-robin DPS protocol, Bob chooses a random number $r \in \{1, 2, ..., L-1\}$ for each incoming L-pulse packet. However, after having picked r, he also chooses at random between the two temporal delays, $2r\tau$ and $(2r-1)\tau$, to be set on his Mach-Zehnder interferometer. The two choices correspond to measure the incoming packet accordingly to the X basis or the Z basis, respectively. From the interference output, Bob can deduce the pair of pulses $a, b \in \{1, 2, ..., L\}$ (with $b = a + r$) that have interfered, analogously to the round-robin DPS protocol. Notably, here a and b are the pulse indices rather than their time-bin positions, as shown in Figure 4.2. Moreover, Bob collects two bits from each detection event: the

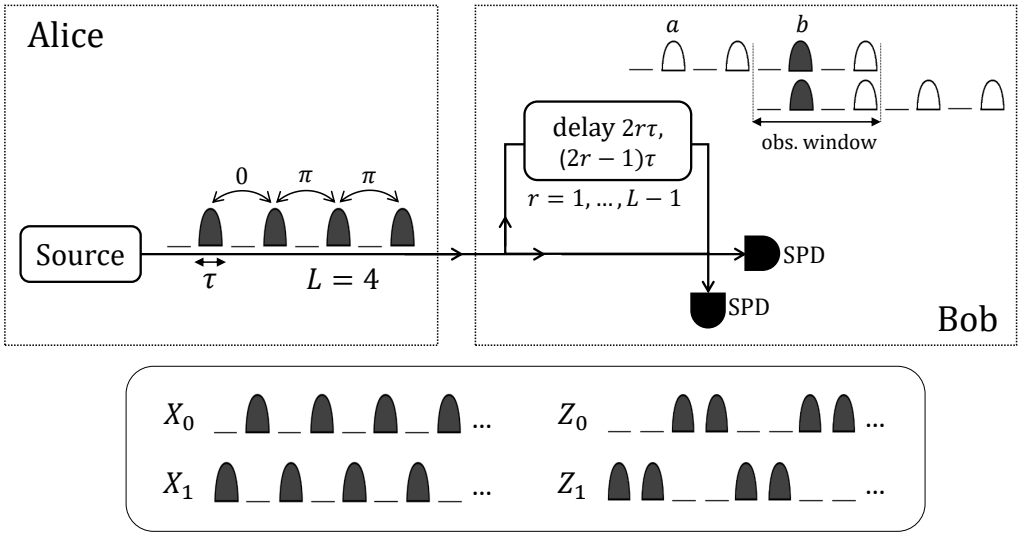


Figure 4.2: Schematic depiction of our proposed protocol, the round-robin DPTS. Alice prepares a packet of $L = 4$ weak pulses, with random phase shifts between consecutive pulses (0, π). She encodes an extra bit in her packet, by selecting one of the four temporal profiles reported in the bottom part of the Figure. Here, she has randomly selected the X basis and she consequently encodes a random temporal bit, 0, by preparing the X_0 pattern. Bob picks a random number r, in order to adjusts his Mach-Zehnder interferometer, monitored with single-photon detectors (SPD). Then, he randomly sets a delay-line of $2r\tau$ or $(2r-1)\tau$ depending on his random basis choice, X or Z, respectively, with τ the time-bin duration. Here, he picks $r = 2$ and he selects the X basis ($2r\tau$ delay-line). A detection event is expected within Bob's observation window, which depends on the basis he has selected. From his measurement result, Bob deduces that the a-th and b-th pulses in the packet, with $b = a + r$, have interfered with each other, as shown in the top-right corner of the Figure. Based on the interference output (0 or π) and on the time-bin position of the interference, Bob collects two bits of raw key. Then, he publicly announces his basis choice and the pulse indices a and b, hence enabling Alice to recover the time and relative phase information as two bits of raw key. All the events related to different basis choices are discarded.

phase-encoded bit from the interference output (0 or π) and the time-encoded bit from discerning the temporal pattern, X_0 or X_1 (and Z_0 or Z_1, depending on his basis choice). In particular, the time-encoded information is acquired by observing the time-bin position at which the interference occurs, i.e., the interference time of arrival. Furthermore, as in the round-robin DPS, Bob discards all the events returning no clicks, or more than one click, within his observation window.

(III) After having repeated the above process many times, Alice and Bob publicly disclose the temporal basis (X or Z) that was selected for each event. Consequently, they discard all the events corresponding to a different choice of temporal basis. Bob then announces the pulse indices a and b related to each detection event,

thus enabling Alice to recover the relative phase information. As a result, for each successful detection event, Alice and Bob collects two bits of raw key.

(IV) In conclusion, standard post-processing procedures of error correction and privacy amplification are performed to extract the secure key.

As shown here, the central point of the round-robin DPTS protocol is the additional bit encoded in the temporal profile of each L-pulse packet. Notably, the security of the time-encoded information is ensured by the random choice of two temporal bases X and Z, in a similar way as in the BB84 protocol. This allows us to derive the security analysis for the round-robin DPTS protocol in a very similar way as done in Ref. [116] for the round-robin DPS, as it will be shown in Sections 4.2.1 and 4.2.2. Then, the expected performances of our protocol are benchmarked against the original round-robin QKD (Section 4.2.3). In conclusion, a proof-of-concept experiment of the round-robin DPTS is presented in Section 4.2.4.

4.2.1 Security analysis

To compute the upper bound on the leaked information I_{AE} under collective attacks, we follow the same derivation as in Ref. [116], that was presented in Section 4.1.1. Again, the main idea is to simplify Eve's density matrix in order to compute the Holevo bound (Equation 1.23 from Chapter 1) with only the relevant components, useful to acquire information on the raw key. The main difference in our derivation is that, being the round-robin DPTS a four-dimensional protocol, the raw key collected at Alice's and Bob's sides is composed of four different symbols: hence, the density matrices to be evaluated are now $\rho_{E,00}$, $\rho_{E,01}$, $\rho_{E,10}$ and $\rho_{E,11}$.

The main steps of our security analysis are presented in the Appendix A.2 and are further described in our work [23]. In the general case of an L-pulse packet with n photons, we derive that with $L \geq 2(n+1)$, Eve's information can be bounded as

$$I_{AE} \leq \max_{x_1,\dots,x_{n+1},y_1,\dots,y_{n+1}} \left\{ \frac{1}{\frac{1}{2}(L-1)+\frac{1}{2}(L/2-1)} \left[\sum_{m=1}^{n} f\big[(L-m)x_m, m x_{m+1}\big] + \frac{(L-n-1)x_{n+1}}{8} + \sum_{m=1}^{n} f\Big(\frac{L/2-m}{2} y_m, \frac{m}{2} y_{m+1}\Big) + \frac{(L/2-n-1)y_{n+1}}{16} \right] \right\}, \tag{4.3}$$

with $f(x,y) = -\frac{x}{4}\log_4\frac{x}{4} - \frac{y}{4}\log_4\frac{y}{4} + \frac{x+y}{4}\log_4\frac{x+y}{2}$ and the non-negative real parameters x_i, y_i, satisfying $\sum_{m=1}^{n+1} x_i = 2$ and $\sum_{m=1}^{n+1} y_i = 2$ [23].

As in the round-robin DPS protocol, this upper bound on I_{AE} allows to distribute a secure key without the need to monitor the quantum channel. Moreover, we demonstrate that $I_{AE} < 1$ always holds for the L-pulse packets with $n < L/2-1$ [23]. It is worth noting that such threshold level for the photon number is lower than in the round-robin protocol ($n < L-1$), because of the information leakage of the time-encoded bit from the multi-photon packets. In the round-robin DPTS, indeed, Eve can opt to measure her ancillary states in different ways, in order to acquire both the temporal and phase information, or the temporal information only, from the multi-photon packets. In particular, the leakage of temporal information is larger for Z basis states, because of the lower amount of interfering pulses in comparison with X basis [23]. Consequently, in our derivation we find that the information acquired by Eve from Z basis states, in the case of $r = 1$ delay, does not depend on L and thus, it can not be bounded for the multi-photon packets. Therefore, we have to discard the $r = 1$ delay for Z basis states, in order to bound I_{AE} in the general n-photon case (Equation 4.3). However, in the single-photon case, or by using decoy-state method (as we do in the proof-of-concept experiment), it is possible to bound I_{AE} without excluding the $r = 1$ delay for Z basis [23]. Furthermore, by assuming a phase-randomized laser source, it is possible to treat the contributions to I_{AE} from each photon-number separately, and also to extend the above security bounds to the more general scenario of coherent attacks.

4.2.2 Secure key rate and symbol error rate

By using the upper bound on I_{AE} derived in the previous Section, we can evaluate the secure key rate achievable with the round-robin DPTS protocol, implemented with a phase-randomized laser source, with a mean photon number per packet equal to $\nu = \mu L$. Specifically, by using the same derivation as shown in Refs. [94] and [116], we quantify the amount of secure key bits that can be extracted from each L-pulse packet, in the asymptotic limit of $N \to \infty$ rounds of quantum communication:

$$S = 2Q\left[1 - H(A|B) - \frac{e_{src}}{Q} - \left(1 - \frac{e_{src}}{Q}\right)I_{AE}\right], \tag{4.4}$$

where Q is the probability to have a successful detection event, $H(A|B)$ is the conditional entropy between Alice's and Bob's raw keys (which depends on the error rate), while e_{src} is the probability that the photon number n of an L-pulse packet is greater than a threshold value n_{th}. Accordingly to Equation 4.4, the multi-photon packets that Alice prepares with $n > n_{th}$, are discarded in the secure key generation. As in the round-robin DPS [116], the values of ν and n_{th} have to be optimized for the different experimental conditions, in order to maximize the secure key rate. In comparison with the secure key formula from Ref. [116], the 2 prefactor is added as two bits of raw key are generated from each successful detection event.

In order to simulate the probability Q and the symbol error rate, we assume an overall loss of η (including the quantum channel and the measurement setup) and a dark count probability per time bin equal to p_d. Moreover, the probability that an incoming quantum signal hits the wrong detector is quantified by $e_{\text{mis}} = (1 - V)/2$, with V the visibility of interference. In the round-robin DPS, a successful detection event occurs when only one click arises in the observation window, which includes $(L-r)$ time bins of τ duration. A single click occurs if only one photon exists among the interfering $(L-r)$ pulses, with a probability $\mathrm{e}^{-(L-r)\eta\mu}(L-r)\eta\mu$. At the same time, no dark counts arise from the two detectors in the remaining bins, with probability $(1 - p_d)^{2(L-r)-1}$. Otherwise, if there is no photon among the interfering pulses, a single click may arise from a dark count, occurring in only one of the observed bins, with overall probability $\mathrm{e}^{-(L-r)\eta\mu} \times 2(L - r)p_d(1 - p_d)^{2(L-r)-1}$. Consequently, in the round-robin DPS we have [116]

$$Q_r = \mathrm{e}^{-(L-r)\eta\mu}(L - r)(1 - p_d)^{2(L-r)-1}\big(\eta\mu + 2p_d\big) \tag{4.5}$$

and a wrong detection event may arise from an dark count, if it occurs in the wrong detector (1/2 probability), or from the incoming photon hitting the wrong detector, because of interference errors (e_{mis} probability):

$$E_rQ_r = \mathrm{e}^{-(L-r)\eta\mu}(L - r)(1 - p_d)^{2(L-r)-1}\big(\eta\mu e_{\text{mis}} + p_d\big) \ . \tag{4.6}$$

Then, all the possible delays are included, giving $Q = \sum_{r=1}^{L-1} Q_r/(L - 1)$ and $EQ = \sum_{r=1}^{L-1} E_rQ_r/(L - 1)$. In the round-robin DPTS, a successful detection event occurs when a single click is observed in the right measurement basis, X or Z. Therefore, we have

$$Q = \frac{1}{2}Q_X + \frac{1}{2}Q_Z \ , \tag{4.7}$$

with $Q_X = \sum_{r=1}^{L-1} Q_{X,r}/(L-1)$ and $Q_Z = \sum_{r=2}^{L-1}\big(Q_{Z,r,e}+Q_{Z,r,o}\big)/(L-2)$. As discussed in the previous section, since we are evaluating the round-robin DPTS with no decoy states, the $r = 1$ delay is not included in Z basis. Moreover, the even and odd values of r have to be distinguished to evaluate $Q_{Z,r,e}$ and $Q_{Z,r,o}$, respectively. Similarly to the round-robin DPS, the probabilities are computed as

$$\begin{aligned}
Q_{X,r} &= \mathrm{e}^{-(L-r)\eta\mu}(L-r)(1-p_d)^{4(L-r)-1}\left(\frac{1}{2}\eta\mu + 4p_d\right) , \\
Q_{Z,r,e} &= \mathrm{e}^{-(L/2-r/2)\eta\mu}(L/2-r/2)(1-p_d)^{2(L-r)-1}\left(\frac{1}{2}\eta\mu + 4p_d\right) , \\
Q_{Z,r,o} &= \mathrm{e}^{-[L/2-(r-1)/2]\eta\mu}\big[L/2-(r-1)/2\big](1-p_d)^{2(L-r)+1}\left(\frac{1}{2}\eta\mu + 4p_d\right) ,
\end{aligned} \tag{4.8}$$

since the amount of the observed time bins is $2(L-r)$ when measuring the X basis, while it is $2(L/2-r/2)$ and $2[L/2-(r-1)/2]$ when measuring the Z basis, respectively with even and odd values of r. Moreover, the $1/2$ factor is added because half of the time bins observed are empty and invalid for distilling key bits. In a similar way as done for the DPTS protocol [120], we can distinguish three different contributions to the overall symbol error rate:

$$\begin{aligned}
E_{X,r}^{(\mathrm{I})} Q_{X,r} &= \mathrm{e}^{-(L-r)\eta\mu}(L-r)(1-p_d)^{4(L-r)-1}\left(\frac{1}{2}\eta\mu e_{\mathrm{mis}} + p_d\right) , \\
E_{X,r}^{(\mathrm{II})} Q_{X,r} &= E_{X,r}^{(\mathrm{III})} Q_{X,r} = \mathrm{e}^{-(L-r)\eta\mu}(L-r)(1-p_d)^{4(L-r)-1} p_d
\end{aligned} \tag{4.9}$$

for X basis, and

$$\begin{aligned}
E_{Z,r,e}^{(\mathrm{I})} Q_{Z,r,\mathrm{e}} &= \mathrm{e}^{-(L/2-r/2)\eta\mu}(L/2-r/2)(1-p_d)^{2(L-r)-1}\left(\frac{1}{2}\eta\mu e_{\mathrm{mis}} + p_d\right) , \\
E_{Z,r,e}^{(\mathrm{II})} Q_{Z,r,e} &= E_{Z,r,e}^{(\mathrm{III})} Q_{Z,r,e} = \mathrm{e}^{-(L/2-r/2)\eta\mu}(L/2-r/2)(1-p_d)^{2(L-r)-1} p_d , \\
E_{Z,r,o}^{(\mathrm{I})} Q_{Z,r,o} &= \mathrm{e}^{-[L/2-(r-1)/2]\eta\mu}\big[L/2-(r-1)/2\big](1-p_d)^{2(L-r)+1}\left(\frac{1}{2}\eta\mu e_{\mathrm{mis}} + p_d\right), \\
E_{Z,r,o}^{(\mathrm{II})} Q_{Z,r,o} &= E_{Z,r,o}^{(\mathrm{III})} Q_{Z,r,o} = \mathrm{e}^{-[L/2-(r-1)/2]\eta\mu}\big[L/2-(r-1)/2\big](1-p_d)^{2(L-r)+1} p_d
\end{aligned} \tag{4.10}$$

for Z basis. The (I) contribution to the symbol error rate is analogous to the round-robin DPS case, as it is related to the occurrence of a click in the wrong detector, due to the interference misalignment causing the photon to hit the wrong detector

(probability e_{mis}) or due to a dark count arising in the right time bin, but in the wrong detector. Therefore, the (I) probability quantifies the occurrence of errors on the phase-encoded bits of raw key. The (II) contribution is related to a dark count arising in the right detector but in the wrong time bin, thus introducing errors in the time-encoded bits. Here, Bob mistakes the X_0 (or Z_0) temporal profile for the X_1 (Z_1) profile, or the other way round, but he correctly retrieves the right phase shift between the a-th and b-th pulses in the packet. The (III) contribution, whose probability is equivalent to the (II) contribution, is related to a dark count occurring in the wrong detector and in the wrong time bin, thus resulting into an error in both the collected bits of raw key. Each contribution (i)=(I),(II),(III) is averaged over the possible delay values, returning $E_X^{(\mathrm{i})}Q_X = \sum_{r=1}^{L-1} E_{X,r}^{(\mathrm{i})}Q_{X,r}/(L-1)$ and $E_Z^{(\mathrm{i})}Q_Z = \sum_{r=2}^{L-1}\big(E_{Z,r,e}^{(\mathrm{i})}Q_{Z,r,e} + E_{Z,r,o}^{(\mathrm{i})}Q_{Z,r,o}\big)/(L-2)$. Then, $E^{(\mathrm{i})} = \big(E_X^{(\mathrm{i})} + E_Z^{(\mathrm{i})}\big)/2$ denotes the single contribution to the overall symbol error rate, given by $E = \sum_{\mathrm{i}} E^{(\mathrm{i})}$. Analogously to the DPTS protocol [120], it is convenient to treat the raw key strings by using a base-4 logarithm and then multiply the result by 2 to obtain the secure key bits, as done in Equation 4.4. Accordingly, the conditional entropy is given by [120]

$$H(A|B) = -(1-E)\log_4(1-E) - \sum_i E^{(\mathrm{i})}\log_4 E^{(\mathrm{i})} \ . \tag{4.11}$$

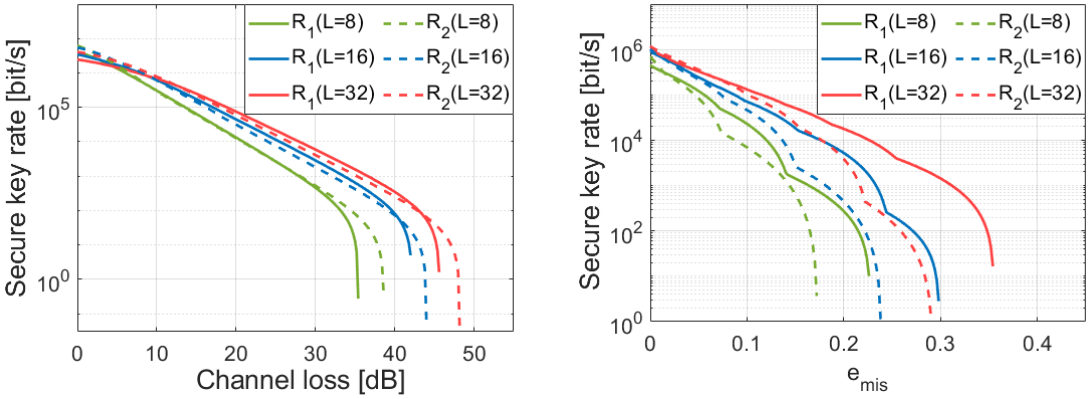
As shown in the error rate contributions, the interferometer imperfections only affect the errors of the phase-encoded bit in the round-robin DPTS protocol, while they do not affect the time-encoded bit. Consequently, the round-robin DPTS can tolerate a lower visibility of interference in comparison with the round-robin DPS, as the time-encoded bit in the packet remains correct when the visibility decreases, as discussed in the following Section. On the other hand, the higher dimensionality of the protocol makes it more vulnerable to the random dark counts, as the observed time window is typically larger than in the round-robin DPS, thus resulting into a higher probability to introduce some sort of error in the raw key bits.

As it will be shown in the last Section of this Chapter, where we present a proof-of-principle experiment of the round-robin DPTS, the three contributions to the symbol error rate actually have a different weight in a practical implementation of the protocol, as the relative phase measurements are typically more affected by errors, in comparison with the measurements of arrival time.

4.2.3 Comparison with the original protocol

In order to benchmark our proposed protocol against the original round-robin QKD, we perform numerical simulations of the secure key rate (SKR) achievable with the two protocols, under the same experimental conditions, by using the asymptotic formulas as reported in Equation 4.4 and in Ref. [116]. In both cases, the information leakage I_{AE} is bounded without monitoring the quantum channel. Moreover, in order to make a fair comparison, we consider a time-bin duration $\tau = 1\,\text{ns}$ in both protocols and we evaluate the SKR in bit/s, rather than in bit/pulse or bit/packet, as the L-pulse packets have a different time duration in the two cases (τL and $2\tau L$ in round-robin DPS and DPTS, respectively, given the same L and τ). In our simulations, the overall loss determining the probability Q of successful events, is $\eta = t\eta_d$, with t the transmission of the quantum channel and $\eta_d = 0.85$ the detection efficiency of superconducting single-photon detectors, exhibiting a dark count probability per time-bin of $p_d = 1.6 \times 10^{-8}$. The obtained SKR data, simulated with different experimental parameters, are reported in Figure 4.3 for the round-robin DPTS (R_1, solid line) and for the round-robin DPS (R_2, dashed line). The mean photon-number per packet $\nu = \mu L$ and the photon-number threshold n_{th} are optimized, for both the protocols, in order to maximize the SKR achievable under each different condition of loss, visibility and packet size $L = 8,\ 16,\ 32$.

As shown in Figure 4.3a, in the conditions of high visibility of interference ($V = 0.97$ and $e_{\text{mis}} = (1 - V)/2 = 0.015$) the SKR of the two protocols is comparable, in the low and middle loss regime. Here, the benefits introduced by the high-dimensionality of round-robin DPTS (i.e., the higher photon-information efficiency and the higher amount of tolerable I_{AE}), are counterbalanced by the lower rate of packet per second and by the basis sifting, which causes half of the events to be discarded. Moreover, we do not take into account the saturation effects in the receiver setup, which would favour the round-robin DPTS, but whose extent is negligible under the simulated conditions of incident photon flux and low dead time of superconducting detectors. As a result, the two bits gained for each successful detection event do not bring a relevant improvement in the final SKR. The improvement is even lower in the case of small packet size ($L = 8$), as the round-robin DPTS is more hindered by the lower threshold $n < L/2 - 1$, necessary to keep I_{AE} below 1. Consequently, for a given L, the mean photon number per packet ν has to be kept lower than in the round-robin DPS (where, instead, $n < L - 1$), thus resulting into a lower signal-to-noise ratio at long transmission distances, where the SKR of round-



(a) $e_{\text{mis}} = 0.015$ (interference visibility 97%).

(b) 10 dB channel loss (up to 50 km of SMF).

Figure 4.3: In this Figure from our work [23], we report the simulated secure key rate (SKR) achievable with our proposed protocol, the round-robin DPTS (R_1, solid line) and with the original version of the protocol, the round-robin DPS (R_2, dashed line) [116]. Both protocols are simulated with a phase-randomized laser source (with no decoy states) and the information leakage is bounded without monitoring the quantum channel. In Figure (a) is reported the simulated SKR, as a function of channel loss, achievable in the condition of high visibility of interference, for different packet sizes. In Figure (b) is reported the simulated SKR, as a function of the interference misalignment e_{mis}, achievable with a quantum channel of 10 dB loss (corresponding to 50 km of transmission distance in single-mode fibers).

robin DPTS drops off more quickly than that of the round-robin DPS. Nonetheless, a practical solution to improve the achievable distance of both the protocols is to implement decoy-state method (see Section 1.3.2), as we discuss in the Supplemental Material of our work [23]. Moreover, when implementing decoy-state method in the round-robin DPTS, the $r = 1$ delay can be included in Z basis measurements, which also improves the SKR.

However, the optimal conditions of visibility considered in Figure 4.3a are actually difficult to maintain in practice, especially for a variable-delay interferometer, as shown in the recent experiments of round-robin QKD [117–119]. Therefore, it is interesting to simulate the two protocols in the condition of increasing probability of interference errors[2], e_{mis}, as shown in Figure 4.3b, for a given channel loss of 10 dB. The same plot is reported in our work [23], also in the condition of 20 dB loss. In both cases, the round-robin DPTS outperforms the original protocol. The round-robin DPS, indeed, relies only on the phase-encoded information, which is

[2]When simulating the secure key rate as a function of e_{mis}, the behaviour of the plotted lines is due to the optimization of the experimental parameters ν and n_{th}, as shown also in Ref. [116].

more and more affected by interference errors, as the visibility decreases. On the other hand, the round-robin DPTS exploits the additional encoding on the time of arrival, which is not influenced by the interferometer imperfections, being affected only by the random dark counts arising in the detectors. As a result, our proposed protocol returns a positive SKR even in the most challenging conditions, when the interference disturbances prevent a secure key from being distributed with the original round-robin QKD. Furthermore, it is worth noticing that, at 10 dB channel loss, when the visibility decreases below 60% ($e_{\text{mis}} \geq 0.2$), the round-robin DPS with $L = 32$ (red dashed line) is outperformed by the round-robin DPTS with $L = 16$ (blue solid line).

As a final comment, we remark that our simulations return the SKR achievable by the two protocols, in the asymptotic regime. It would be interesting to include the finite-size effects in the security analysis of the round-robin DPTS, as it has been done very recently for the round-robin DPS [122, 123].

4.2.4 Proof-of-principle experiment

To conclude this Chapter, we report the results of a proof-of-principle experiment of the round-robin DPTS protocol, also included in our work [23]. Our aim is to assess the different contributions to the symbol error rate, such as the phase errors and the time errors, that typically emerge in a practical implementation of the protocol. Differently from the simulated conditions of the previous Section, we employed InGaAs/InP single-photon detectors, with $\eta_d = 0.2$ efficiency and $p_d = 3 \times 10^{-8}$ dark count probability per time bin[3].

In our proof-of-concept experiment, we prepare the quantum states of the round-robin DPTS protocol with $L = 4$, with one decoy state, and we perform the measurements with only $r = 1$, i.e., with 2τ delay for X basis and with τ delay for Z basis. The experimental setup is analogous to the one reported in Figure 3.3a of the previous Chapter (see also Sections 2.3 and 2.4 for more details). To prepare the different temporal profiles of the two bases, a continuous-wave laser source at 1550 nm is followed by two cascaded intensity modulators, driven with a proper carving pattern. Then, a phase modulator, driven with a pseudo-random squared signal, is employed for encoding the two phase shifts 0 and π. Another intensity

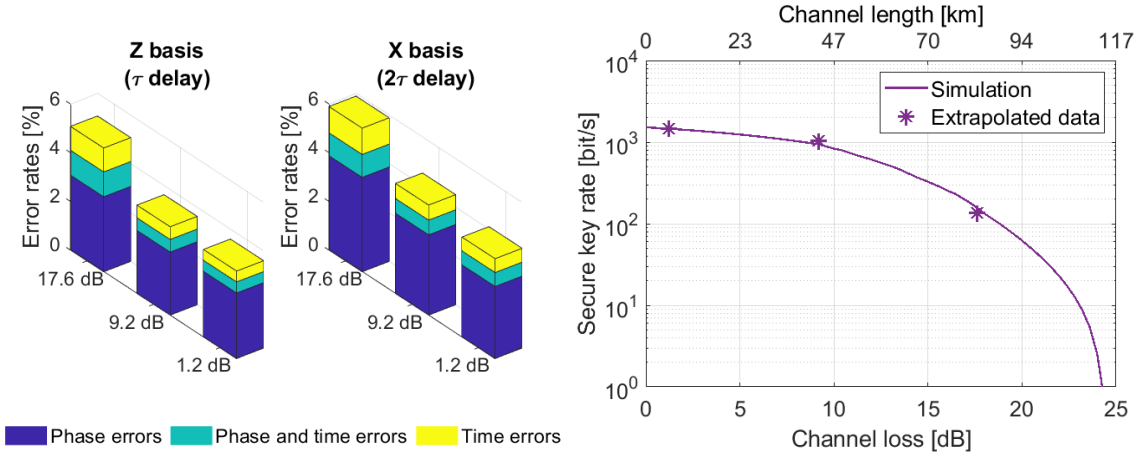
[3]Such value for p_d is obtained, from the observed dark count rate (150 Hz), after applying a post-selection of the detection events, that are processed with a temporal filter of 200 ps around the center of each time bin, as described in Section 2.4.2.

modulator is used to implement the one-decoy method. Both basis choice and decoy preparation are performed with 50% probability, while the time-bin duration is $\tau \simeq 840\,\text{ps}$, as each L-pulse packet is defined by eight time bins. Our transmitting unit allows the preparation of approximately 72.7×10^6 packets per second, with the two different intensity levels $\mu_1 L$ and $\mu_2 L$. After being propagated over single-mode fiber spools of different lengths (6 km, 43 km and 80 km), the L-pulse packets reach the receiver apparatus. Here, two independent and free-space interferometers, with τ and 2τ delay lines, are nested into each other by means of polarizing beam splitters, as described in Section 3.2. The delay choice is performed actively, with a manual polarization controller. A detection event occurs when a single click arise among the six observed time bins, in X basis, and among the four observed time bins, in Z basis. The experimental parameters and results are reported in Table 4.1 and in Figure 4.4. In particular, for each different channel length we measured the different contributions $E^{(\text{I})}$, $E^{(\text{II})}$ and $E^{(\text{III})}$ to the symbol error rate, defined in Equations 4.9 and 4.10, that are observed in both bases with $r = 1$ delay. As can be seen from Table 4.1 and Figure 4.4a, the main contribution arises from interference errors, $E^{(\text{I})}$, which leads to around 70% of all erroneous detections. The other two contributions, related to time errors ($E^{(\text{II})}$) and phase and time errors ($E^{(\text{III})}$), are almost equal to each other (accordingly to theory) and do not depend on the interference visibility, but only on the dark count rate. As a result, they are notably lower than $E^{(\text{I})}$ in a practical implementation of the QKD protocol, leading together to only 30% of all erroneous detections. The reason for this is that, from a practical point of view, retrieving the time-encoded information is generally more straightforward than retrieving the phase-encoded information, as already pointed out in Chapter 3. As a consequence, the additional encoding on the time of arrival, results into a notably practical advantage for the round-robin DPTS protocol, over the round-robin DPS, which makes our proposed scheme successful also in more demanding conditions of interferometric disturbances, which prevent the original protocol from being feasible.

As can be seen from our experimental results, when the channel loss increases the random dark counts become more frequent in the detection events, thus increasing all of the three contributions to the symbol errors. Moreover, the experienced errors are generally higher for X basis, due to multiple factors: the larger amount of observed time bins (which increases the occurrence of dark counts), the higher instability of interference due to the longer delay line, and the higher occurrence of temporal errors induced by the timing jitter of the detectors.

quantum channel		μ_1	μ_2	$E^{(\mathrm{I})}$	$E^{(\mathrm{II})}$	$E^{(\mathrm{III})}$
6 km	1.2 dB	0.020	0.010	2.8 %	0.51 %	0.51 %
43 km	9.2 dB	0.034	0.016	2.9 %	0.56 %	0.57 %
80 km	17.6 dB	0.031	0.015	3.5 %	1.0 %	1.0 %

Table 4.1: Experimental parameters and results of our proof-of-concept experiment of the round-robin DPTS, with $L = 4$ and one decoy state. For each different length of single-mode fiber, we optimize the $\mu_1 L$ and $\mu_2 L$ intensities and we measure the L-pulse packets with $r = 1$, i.e., with 2τ delay for X basis and τ delay for Z basis. Here are reported the three different contributions to the symbol error rate observed in our experiment, as discussed in Section 4.2.2, and averaged for both bases and intensity values.



(a) Experienced symbol error rates.

(b) Simulated secure key rate.

Figure 4.4: This Figure from our work [23] shows the results of our proof-of-concept experiment of the round-robin DPTS, with $L = 4$ and one decoy state. Figure (a) shows the three different contributions to the symbol error rate observed for the two different bases, also reported (averaged) in Table 4.1. Figure (b) shows the secure key rate expected with our experimental setup, that is evaluated by simulating the remaining delay values $r = 2$ and $r = 3$.

To conclude, we evaluate the performances of our experimental setup for round-robin DPTS QKD, with $L = 4$ and one decoy state, by simulating the expected secure key rate achievable when including all the delay values ($r = 1,\ 2,\ 3$). The results of our simulation are reported in Figure 4.4b.

5

From laboratory tests to in-field implementations

In this final Chapter of the thesis, we present a set of experimental works on QKD that have been carried out by exploiting installed links of single-mode fibers. Specifically, we performed in-field tests of time-encoded QKD over a metropolitan fiber link situated in Florence [19, 20], directly accessible from the CNR-INO facilities located at LENS, the European Laboratory for Non-linear Spectroscopy of University of Florence. The High-Speed Optical Communications group from DTU Fotonik contributed to these works. During these field trials, we address two main practical challenges: on one hand, the automatic stabilization of the experimental apparatus of the transmitting and receiving units, necessary to enable long-term quantum communication; on the other hand, the coexistence of quantum and classical signals co-propagated through the same fiber, by means of dense-wavelength division multiplexing in the telecom C-band.

Based on our in-field tests in Florence, a public demonstration of metropolitan-scale QKD was later performed in Trieste [124]. Furthermore, a similar setup for the self-stabilization of the experimental apparatus was also tested on a deployed link in L'Aquila, based on a multi-core optical fiber [125].

5.1 Field trial of time-encoded quantum communication

In the work published in Ref. [19], we present an in-field test of time-encoded QKD on a metropolitan fiber link deployed in Florence, achieved with a self-stabilized experimental setup able to run autonomously for several hours. This work was

the first field trial of a QKD setup to be implemented over an installed fiber in Italy; other metropolitan demonstrations of fiber-based QKD were later performed in Padua [126] and in Trieste [124]. Moreover, the point-to-point fiber link that we tested in Florence is actually a portion of a huge fiber network of about 1700 km, connecting the whole Italian peninsula, from the Turin National Institute of Metrological Research (INRiM) to Matera Space Center. Such fiber infrastructure, currently employed by INRiM for time-standard dissemination from the atomic clock in Turin, acts as the proper environment for the future implementation of a large-scale quantum network, referred as the Italian Quantum Backbone [127].

The experimental setup of our QKD field trial is depicted in Figure 5.1. The metropolitan link is a dark single-mode fiber of about 20 km, connecting the laboratory at LENS, in Sesto Fiorentino, with a telecom datacenter situated more downtown. As shown in Figure 5.1, a standard fiber-based mirror is placed at the telecom datacenter in order to drive the light back to the LENS laboratory, where it is collected with an optical circulator and sent to the receiving unit. The total length of a round-trip in the metropolitan fiber is 40 km, with an overall transmission loss of 21 dB. Our loop-back configuration surely increases the loss of the quantum channel; at the same time it enables to keep both Alice's and Bob's setups in the same room at LENS. As it will be described in the following, this allows to test the QKD protocol under two different scenarios. In the first situation, we totally dedicate the fiber to quantum signal propagation, by exploiting electronic synchronization between Alice's FPGA board and Bob's time tagging unit, as we usually do in the other works. Notably, electronic synchronization requires Alice and Bob to be placed nearby. In the second situation, the synchronization signal is optically delivered, by using a second laser source (continuous wave laser), whose intensity is modulated, driven by the synchronization signal provided by the FPGA board. In this configuration, illustrated in Figure 5.1, the optical synchronization signal is propagated in the same metropolitan fiber, together with the quantum signal. To do so, we exploit a dense-wavelength division multiplexing (DWDM) scheme in the C-band, which allows to separate the two different wavelengths incoming at the receiver setup, by means of a DWDM demultiplexer[1]. Specifically, we employed a 200 GHz DWDM filter, able to split the odd channels of the ITU-T grid, from channel 21 (1560.61 nm) to channel 51 (1536.61 nm). Based on the laser sources available and on the intrinsic noise of the fiber link (discussed in the next Section), we set

[1]Notably, the 200 GHz DWDM demultiplexer, with 16 outputs, introduces an insertion loss of about 3 dB. To reduce the insertion loss, a two-output filter can be employed in place of our device.

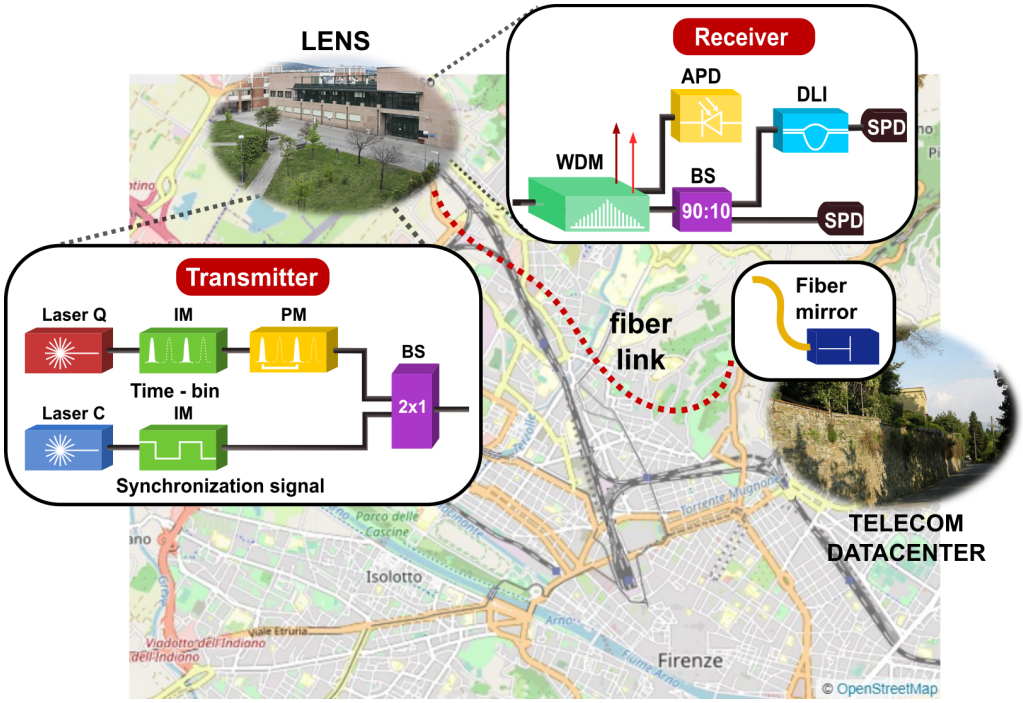


Figure 5.1: This Figure, inspired from our work [19], illustrates the QKD field trial performed in Florence. A metropolitan dark-fiber link of about 20 km connects the LENS laboratory to a telecom datacenter. Here, a fiber-based mirror is placed in order to drive the light back to the laboratory, where both the transmitter and the receiver are located. Two different laser sources are used to prepare the quantum states and the optical synchronization signal, that are multiplexed in the same fiber by exploiting two different wavelengths in the C-band. At the receiver, the two signals are separated with a demultiplexer and the classical light is detected with an avalanche photodiode. The quantum signals are sent to the measurement setup, and Bob's basis choice is performed passively with a 90/10 beam splitter. The QKD scheme that we test is the three-state BB84 with time-bin encoding and one decoy, described in Section 1.3.3.1 (theory) and Section 3.2.1 (experiment). Laser Q: laser quantum; Laser C: laser classical, IM: intensity modulator, PM: phase modulator, BS: beam splitter, WDM: wavelength division multiplexing filter, APD: avalanche photodiode, DLI: delay-line interferometer, SPD: single-photon detector. The transmitter and receiver apparatus is further described in Sections 2.3 and 2.4 of Chapter 2.

the quantum signal to ITU-T channel 21 and the synchronization signal to ITU-T channel 51. To reduce the noise induced by the classical synchronization signal on Bob's single-photon detectors, due to imperfect filtering and nonlinear generation, we decrease its launch power down to -29 dBm. Consequently, an avalanche photodiode (APD) is employed in Bob's setup for detecting the synchronization signal, to be used as a time reference for the time-tagging unit. Furthermore, an additional wavelength filter is placed in front of Bob's setup for quantum measurements, to

further reduce the noise induced by the classical signal, also due to the directivity of the optical circulator.

5.1.1 Characterization of the installed fiber link

As mentioned above, the metropolitan link that we test is a dark fiber, meaning that no optical amplifiers are placed along the path and that no data traffic is present, except for the signals involved in our QKD setup. However, if we put a single-photon detector at one end of the fiber, we can still detect an incoming photon flux, as reported in Figure 5.2. Here, we connect the single-photon detector directly to the different outputs of the 200 GHz DWDM filter situated in the receiver setup (Figure 5.1), with all the laser sources turned off. Since the optical fiber is installed underground and, hence, it is supposed to be shielded from solar light during the whole length, we deduce that the extra clicks observed (in addition to the detector dark counts) could be mainly due to interfiber cross-talk, i.e., background photons leaked from the non-dark fibers arranged in the same bundle, in the metropolitan link. As we observe no extra count rate at the DWDM output corresponding to ITU-T channel 21, we decide to set the wavelength of the quantum signal to 1560.61 nm. In this way, we avoid the additional disturbance in the quantum measurements caused by the background noise affecting the fiber link.

Regarding the loss of the quantum channel, we measured 21 dB of attenuation for a total round-trip in the metropolitan fiber (40 km), including the reflection at the fiber mirror and the two passages in the optical circulator. Notably, the average loss of this fiber channel (more than 0.5 dB/km) is significantly higher than what is typically exhibited by fiber spools of the same length (around 0.21 dB/km), like those that we use to test QKD protocols in the laboratory, as reported in Figures 3.4b and 4.4b of the previous Chapters. Since we can reasonably neglect the loss of the fiber mirror and the optical circulator (less than 1 dB overall), we assume that the observed extra loss could be due to multiple factors, such as bending loss and low-quality connections and splicing, as commonly found in deployed fibers dedicated to standard optical communications. Notably, the extra attenuation typically exhibited by the already-installed fibers, together with the presence of environmental noise in the link as discussed above, contributes to make in-field QKD more challenging, in comparison with the laboratory tests implemented with fiber spools of the same length.

Figure 5.3 shows the results of other characterization measurements that we

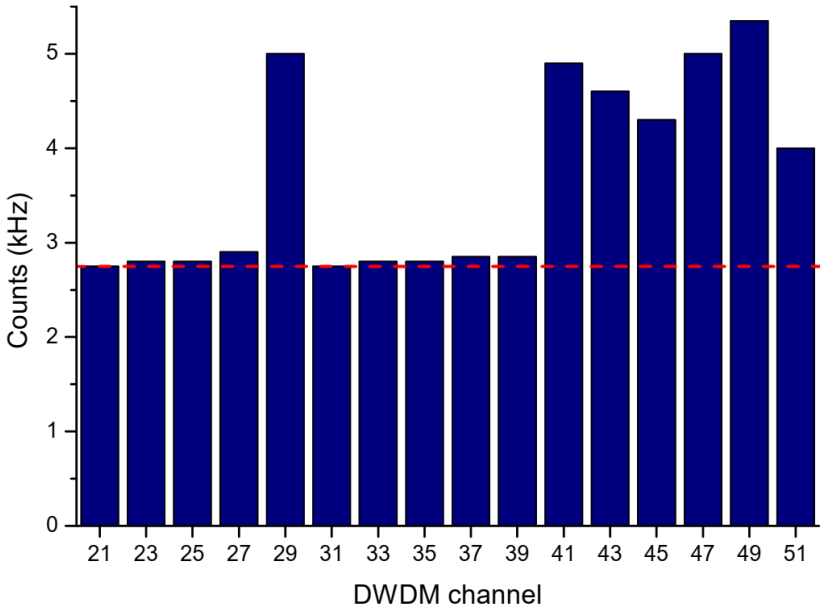
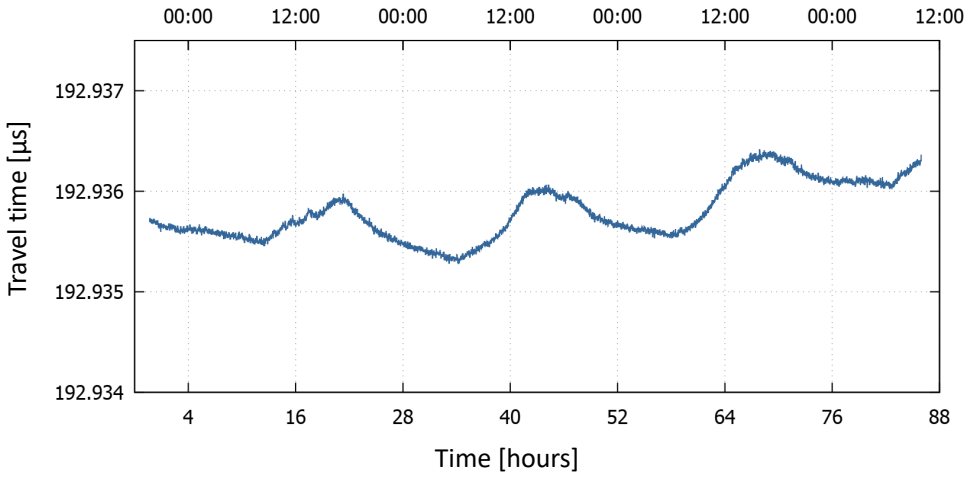


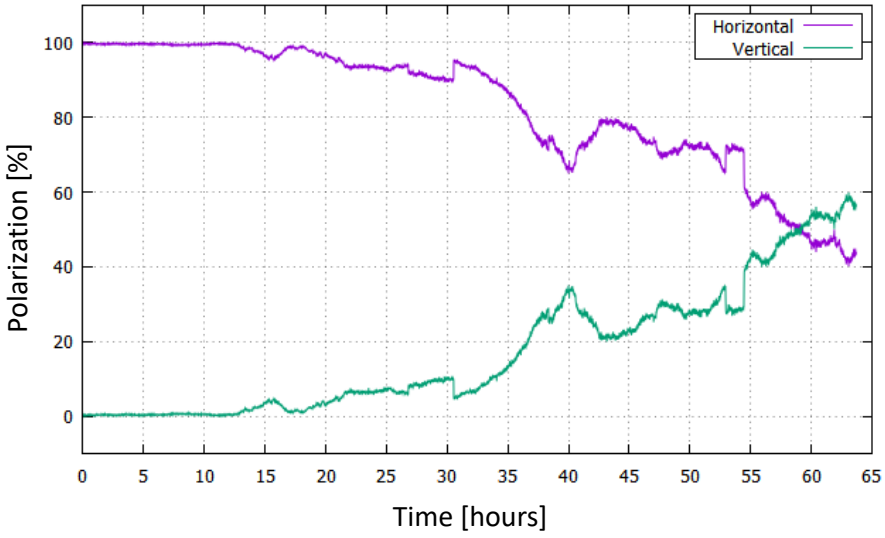
Figure 5.2: Observed count rate at the outputs of the 200 GHz DWDM filter placed at the receiver setup (Figure 5.1), denoting the intrinsic noise of the dark fiber link at the different wavelengths of the ITU-T grid, from channel 21 (1560.61 nm) to channel 51 (1536.61 nm). The red dashed line denotes the dark count rate of the single-photon detector.

perform on the metropolitan fiber: the long-term drifts of the travel time (a) and of the polarization direction (b). Specifically, in Figure 5.3a is reported the round-trip travel time of a laser pulse at 1550 nm, injected into the fiber link through the optical circular. The travel time of the pulse is continuously measured during a long-term acquisition of more than three days (as shown by the top x-axis of the Figure, denoting the local time). The temporal drift becomes significant ($\sim$ 10 ps) after around 10 minutes; moreover, its long-term oscillations seem to follow the same periodicity of the day and night, which suggests that a portion of the fiber link is affected by thermal expansion. The amplitude of the daily fluctuation ranges from 400 ps to 800 ps and needs to be monitored in our long-term acquisitions of QKD, as it causes the drift of the central position of the time bins observed at the receiver setup[2]. Due to such drift, we have to continuously adjust the position of the post-processing temporal filter (of 200 ps) that we apply to our detection events, around the center

[2]Since the time-tagger returns the time differences based on the incoming synchronization signal, the long-term drifts of the travel time in the fiber are more important when the synchronization signal is electrically delivered and hence, it is not affected by the same temporal fluctuations of the quantum signals.



(a)



(b)

Figure 5.3: Long-term characterizations of the metropolitan fiber link installed in Florence: (a) daily oscillations of the round-trip travel time, (b) temporal drifts of the polarization rotation induced by the propagation in the optical fiber. The periodicity of the observed oscillations of the travel time suggests that a portion of the fiber link is subjected to thermal expansion. Such drift has to be compensated at the receiver, who has to continuously adjust the position of the temporal filter used to post-select his detection events. On the other hand, the polarization drifts induced by the fiber link only affect the polarization-dependent devices in the receiver setup.

of each time bin (with duration $\tau \simeq 840\,\text{ps}$), in order to improve the signal-to-noise ratio, as discussed in Section 2.4.2. This adjustment is performed automatically, by monitoring the histogram of the observed pulse shape in the time-bin window, that is computed in real-time from the single-photon detection events, acquired from each data buffer of the time-tagging unit.

Furthermore, Figure 5.3b shows the fiber link stability in terms of polarization. Here, the light travelling back from the metropolitan fiber is collected with a polarizing beam splitter, which allows to evaluate the ratio between the horizontal and vertical components. At the beginning of the acquisition, the polarization is totally aligned with the horizontal direction (the vertical component is less than 0.3%); after 13 hours the vertical component has reached a fraction of 1%, and after 58 hours the polarization becomes equally distributed between the two directions (50%). Based on our experience, the polarization rotation induced by the installed fiber is more stable than in the fiber spools tested in the laboratory, if they are not properly thermalized. Although the stability of polarization does not directly affects the time-bin QKD scheme that is tested in our field trial [19], it can still influence the polarization-dependent devices at the receiver setup. This is the case of the up-conversion-assisted receiver discussed in Section 5.2.1, but also the case of active basis choice based on polarization modulation, as discussed in our proposed setup for high-dimensional QKD with efficient time-bin encoding (Section 3.2).

5.1.2 Long-term acquisitions

The QKD protocol that we test in our in-field experiment [19] is the simplified three-state BB84 with time-bin encoding and one decoy intensity [9, 56, 57], described in Section 1.3.3.1 (theory) and in Section 3.2.1 (experiment). Similarly to the other QKD setups discussed in this thesis, based on time-bin and phase encoding, an interferometer is required to perform quantum measurements. Specifically, a τ-delay interferometer is needed to observe the interference of the early and late time bins, necessary to carry out the $\mathcal{X}$-basis projection. In order to maintain a low error rate in the $\mathcal{X}$ basis (and consequently, a low phase error rate in the $\mathcal{Z}$ basis) the interference visibility has to be optimized and stabilized during the whole duration of the quantum communication step of the protocol. Depending on the post-processing block-size, whose optimal length is determined by the finite-key analysis of the QKD protocol, the overall acquisition time can require from a few minutes to many hours. To do so, we implement a servo-locking feedback system able to

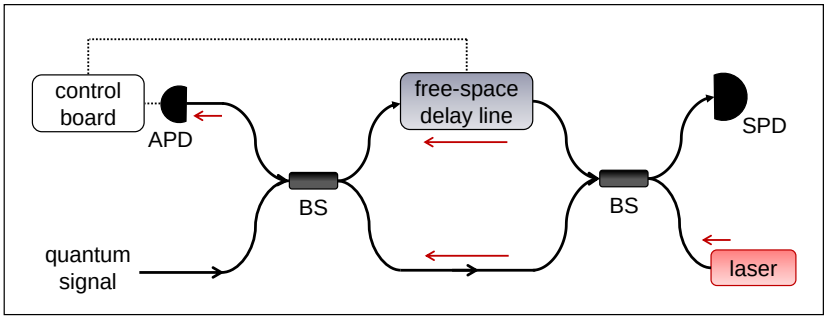


Figure 5.4: Schematic depiction of the servo-locking interferometer implemented for our long-term acquisitions of in-field QKD. An additional laser is injected in the unused output of the Mach-Zehnder interferometer and is collected at the free input. Its interference signal is used by the control board to drive the piezoelectric transducer, mounted in the free-space delay line. BS: beam splitter; APD: avalanche photodiode; SPD: single-photon detector.

automatically adjust the relative phase of the interferometer, without need to interrupt the quantum communication. As shown in Figure 5.4, our setup is composed of a fiber-based Mach-Zehnder interferometer with a free-space delay line, where a piezoelectric transducer is installed for tuning the optical path in the long arm. The applied voltage to the piezoelectric transducer can be manually adjusted, as we do in most of our works. However, to enable long-term acquisition, we make use of an additional laser, that is injected from the unused output of the Mach-Zehnder interferometer, and is collected from the free input with an avalanche photodiode (Figure 5.4). The observed interference signal is used as a feedback signal for a phase lock loop implemented on a control board, where a micro-controller unit consequently drives the voltage of the piezoelectric transducer. In order to reduce the extra noise on the single-photon detectors due to the counter-propagating feedback laser, we set it to a different wavelength of the ITU-T grid (channel 35, 1549.32 nm) and we apply wavelength filtering and proper attenuation. Notably, our system allows to continuously stabilize the interference of quantum signals without need to monitor the error rate in the $\mathcal{X}$-basis, being based on a independent laser propagated through the same interferometer used for quantum measurements. It should be noted that, in a QKD protocol, the error rates are estimated only at the end of the quantum communication step, after having collected all the detection events needed to fill the post-processing block size. Consequently, our stabilization system has the feature to run independently during the whole acquisition time, without need to interrupt it for monitoring the error rates. Moreover, the fact that the quantum projection is independent from the channel behaviour, makes our QKD setup more safeguarded

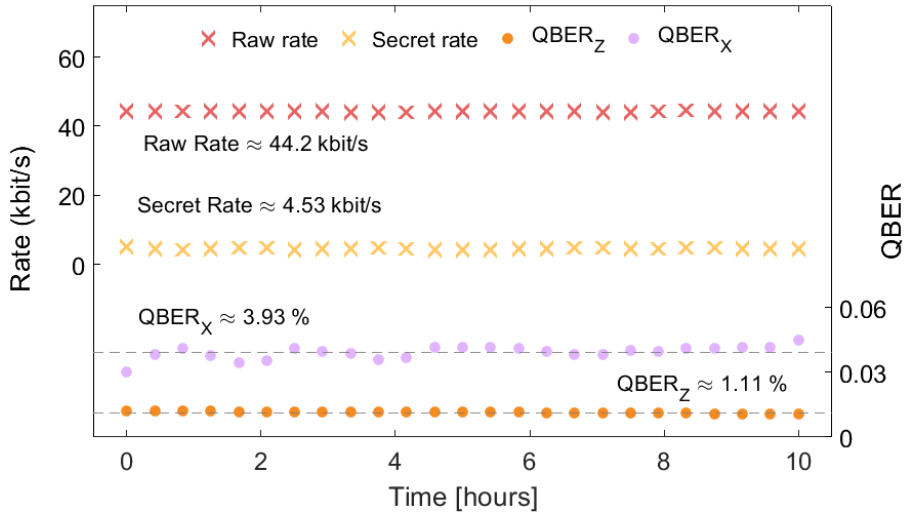
against potential side-channel attacks.

Figure 5.5 shows the results of our long-term acquisitions of in-field QKD. In particular, our setup is demonstrated to run autonomously for more than 10 hours (a) in the configuration with electric synchronization, and for around 4 hours (b) in the configuration with the optical synchronization signal multiplexed in the same fiber. The lower long-term stability of the second configuration is mainly due to the drift of the intensity modulator used to generate the optical synchronization signal, whose bias voltage is not self-adjusted during this experiment. As shown in Figure 5.5b, the optical synchronization signal induces extra noise in the quantum measurements, causing higher error rates in both bases. Moreover, the raw key rate is slightly lower in this configuration, due to the additional wavelength filter placed in front of the quantum measurements, necessary to improve the signal-to-noise ratio when the optical synchronization is delivered. These factors lead to a lower secure key rate achievable in the second configuration (3.40 kbit/s versus 4.53 kbit/s). Notably, the DWDM demultiplexer is present in both cases, as it is needed to filter out the intrinsic noise of the dark fiber link (Figure 5.2).

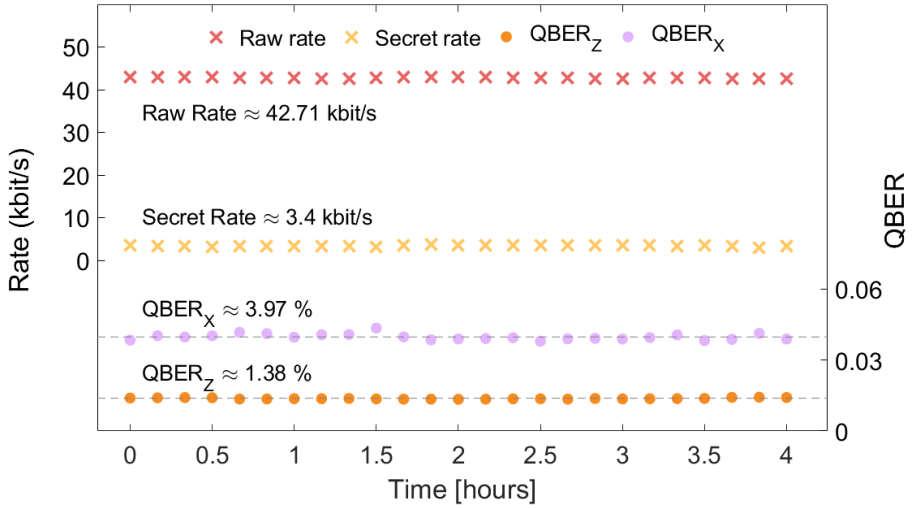
After the field trial in Florence, the servo-locking system used to stabilize the τ-delay interferometer (Figure 5.4), is successfully tested also in the stabilization of an interferometric setup of 25 km, based on a multi-core fiber link installed in L'Aquila [125].

5.2 Dense multiplexing of quantum and classical light

In the QKD field trial presented in the previous Section, we test the co-propagation of quantum and classical signals in the same fiber, by means of a DWDM scheme where the two signals are set to different wavelengths in the C-band. However, as mentioned above, we have to decrease the launch power of the classical signal down to -29 dBm, in order to keep low the introduced errors in the quantum measurements, caused by the extra noise counts affecting the single-photon detectors. Such noise counts originate from nonlinear processes, like Brillouin and Raman scattering [99], leading to the generation of photons with a broad spectrum of wavelengths, that are not filtered out by the wavelength filters. Due to the weakness of the quantum signal, such nonlinear generation has a damaging effect even at the single-photon level, i.e., when the power of the classical signal generating such noise is low: for our



(a) With electric synchronization between Alice's and Bob's stations (only the quantum signals are propagated in the metropolitan fiber link).



(b) With the optical synchronization signal co-propagated in the same metropolitan fiber, together with quantum signals, by means of dense-wavelength division multiplexing.

Figure 5.5: This Figure from our work [19] shows the long-term performance of our in-field test of QKD. With the servo-locking interferometer implemented at the receiver side, our setup can run autonomously for several hours, in the two different configurations (a) and (b). We report the raw key rate and the bit error rates measured in both bases, used to extrapolate the final secure key rate from the theoretical bounds presented in Chapter 1. The experimental parameters for QKD, reported in our work [19], are the following: $\mu_1 = 0.41$, $\mu_2 = 0.15$, $p_Z = 0.9$, $\varepsilon_{sec} = \varepsilon_{corr} = 10^{-9}$, post-processing block size: 10^9 bits.

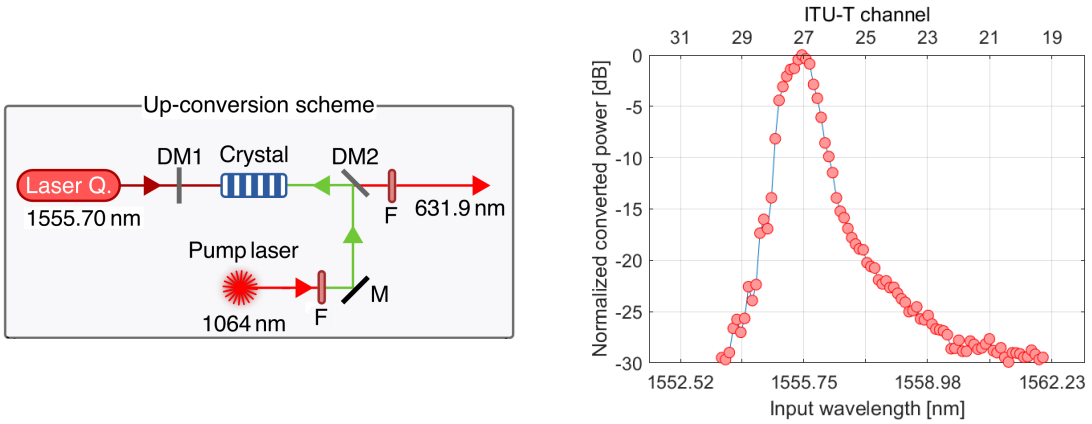
setup of in-field QKD, the maximum tolerable launch power of the synchronization signal is evaluated as $-27\,\mathrm{dBm}$ [19].

In general, the coexistence of classical and quantum communication within the same fiber optic infrastructure is still an open challenge. Most of the QKD implementations, indeed, are accomplished by taking advantage of dark fiber links. However, this choice results into a severe limit to the full deployment of QKD technologies in large-scale applications, due to the high costs of the totally-dedicated fibers for quantum communication. Standard optical communication based on single-mode fibers exploits DWDM techniques for enlarging the capacity of the fiber links; however the simple DWDM method is not enough to enable QKD, as discussed above. Therefore, many solutions have been proposed, to improve the wavelength multiplexing scheme of quantum and classical signals: space and time multiplexing [128], polarization multiplexing [129] and wide-range wavelength multiplexing involving the two telecom windows, the C-band (from 1530 to 1565 nm) and the O-band (from 1260 to 1360 nm) [130]. Moreover, some QKD protocols inherently offer higher tolerance for noise, such as high-dimensional protocols and continuous-variable QKD. Nonetheless, for dense-wavelength multiplexing in the C-band, the most practical solution to enable the co-propagation of quantum and classical communication, is still to decrease the launch power of the classical signals.

In another in-field experiment that we published in Ref. [20], presented in the following Sections, we explore an alternative solution to improve the current DWDM schemes of quantum and classical communication, by taking advantage of a frequency up-conversion detector included in the QKD receiver.

5.2.1 Single-photon detection with frequency up-conversion

Frequency up-conversion [131] is used to turn a telecom wavelength into the visible or near-visible spectrum, where the InGaAs/InP single-photon avalanche diodes (SPADs) can be replaced by the better performing silicon-based SPADs. This process is based on the sum-frequency generation, $\omega_3 = \omega_1 + \omega_2$, enabled by the nonlinear crystals, such as lithium niobate, when illuminated by the two beams ω_1 and ω_2. Such frequency conversions have been demonstrated to preserve the quantum state related to the initial beam [132], which make them suitable for quantum communication applications. Specifically, periodically-poled lithium niobate waveguides (PPLN), induce the frequency conversion $\omega_1 \rightarrow \omega_3$ at the single-photon level, when illuminated with a pump laser ω_2 of some hundreds of milliwatts. The conversion



(a) Setup of the up-conversion module.

(b) Phase matching profile.

Figure 5.6: This Figure inspired from our work [20] describes the up-conversion module that we use to test up-conversion-assisted QKD, under a DWDM configuration of co-propagated quantum and classical light. The experimental setup of the up-conversion module is further described in Ref. [134]. Laser Q.: laser quantum, DM1, DM2: dichroic mirrors, M: mirror, F: wavelength filter.

process is enabled by the phase-matching condition between the three beams, determined by the PPLN geometry and refractive index, and the conversion efficiency can be optimized by tuning the temperature of the crystal, the input wavelengths, their polarization alignment and the power of the pump laser. Notably, the strong pump laser is likely to induce nonlinear generation on its own, such as spontaneous parametric down-conversion and spontaneous Raman scattering [133], which contribute to the overall dark counts of the up-conversion detector.

The up-conversion setup that we test in our work, reported in Figure 5.6, is able to convert the incoming beam at 1555.7 nm to the 631.9 nm visible wavelength, by means of an amplified pump laser emitting at 1064 nm [134]. The noise generated by the pump laser is filtered out by means of cascaded wavelength filters. Then, the up-converted photons are detected with a free-space silicon-based SPAD from Micro Photon Devices, exhibiting $\eta_d = 0.4$ detection efficiency around 630 nm. In order to improve the signal-to-noise ratio of the overall system, we decrease the power of the pump laser, thus causing also a reduction of the achievable conversion efficiency. As a result, the overall detection efficiency of the whole up-conversion-assisted detector (including conversion process, filtering, beam coupling and SPAD) is approximately 2%, while the total dark count rate, including the intrinsic dark counts of the SPAD and the residual noise from the pump laser, is about 11 kHz. One method to improve the performance of the up-conversion detector is to exploit

a longer-wavelength pump laser ω_2, with $\omega_2 < \omega_1$, in order to reduce the nonlinear generation of pump noise at the output wavelength ω_3 [133]. Consequently, we are currently implementing another up-conversion detector for the telecom C-band, with an amplified pump laser at 1950 nm, resulting into an output wavelength of around 864 nm. Such system is expected to achieve up to 30% overall efficiency with less than 200 Hz dark count rate [135–137]. Notably, when increasing the pump wavelength, also the output wavelength increases, leading to a lower probability of being detected by the silicon SPAD, thus a proper trade-off has to be found depending on the specific application and available detectors.

Due to the high selectivity of the phase-matching condition, the up-conversion process acts as an intrinsic and sharp filter in both polarization and wavelength[3] of the incoming beam ω_1. In the meanwhile, the silicon-based SPAD boasts high-performing timing features, such as lower timing jitter and higher maximum count rate, in comparison with the commercial InGaAs/InP SPADs for the telecom bands. Based on these considerations, we investigate the noise tolerance of up-conversion-assisted QKD, in the condition of increasing launch power of a co-propagated laser, multiplexed in the same metropolitan fiber, in a DWDM scheme. In particular, in our work [20] we evaluate the robustness of a QKD receiver equipped with the up-conversion module at 631.9 nm (Figure 5.6), by comparing it with a standard receiver based a commercial InGaAs/InP SPAD and equipped with off-the-shelf filters for wavelength and polarization. Our experimental results are discussed in the next Section.

5.2.2 Experiment and results

The experimental setup that we used in our work [20] is reported in Figure 5.7. Our aim is to compare the performances of the two different QKD receivers, depicted on the right side of the Figure, under a DWDM configuration of quantum and classical light, co-propagated in the same metropolitan fiber. The installed fiber link that we test in this experiment is the same dark fiber of our previous in-field demonstration in Florence [19], hence, the quantum and classical beams are propagated through a full round-trip in the fiber (as light is reflected back at the other end of the link, with a standard fiber-based mirror M). In particular, as shown in Figure 5.7, the

[3]Notably, the up-conversion detector does not act as a temporal or spatial filter of the incoming photons, since the pump beam is a continuous wave laser and the PPLN waveguide is coupled to the same spatial mode that is delivered by single-mode optical fibers.

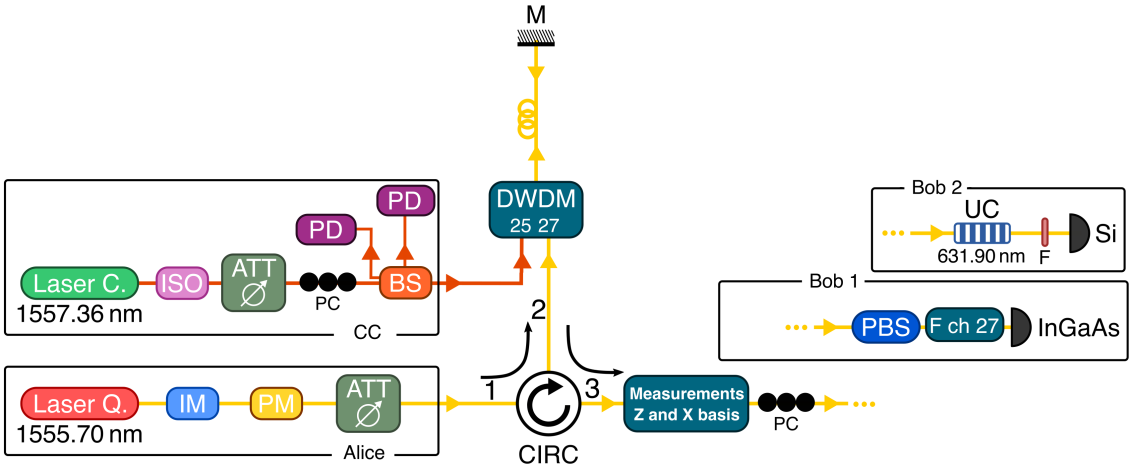


Figure 5.7: This Figure, inspired from our work [20], illustrates the experimental setup that we use to compare the performances of two different QKD receivers, Bob 1 and Bob 2, under the same condition of co-propagated classical laser in a DWDM configuration, through a metropolitan fiber link. Specifically, Bob 1 is a standard receiver based on InGaAs/InP single-photon detectors, equipped with off-the-shelf filters for wavelength and polarization. On the other hand, Bob 2 is our up-conversion-assisted receiver, able to convert the incoming quantum signal at ITU-T channel 27, to the visible wavelength at 631.9 nm, detectable by silicon-based single-photon detectors. The fiber link that we test is the same link used in our field trial of QKD [19], described in Section 5.1. The implemented QKD scheme is the three-state BB84 with time-bin encoding and one decoy, described in Section 1.3.3.1 (theory) and Section 3.2.1 (experiment). Laser Q.: laser quantum; Laser C.: laser classical, CC: classical transmitter, ISO: optical isolator, IM: intensity modulator, PM: phase modulator, ATT: variable optical attenuator, PC: polarization controller, PD: photodiode, BS: beam splitter, CIRC: optical circulator, DWDM: dense-wavelength division multiplexing filter, M: fiber-based mirror, PBS: polarizing beam splitter, F ch 27: 100 GHz wavelength filter around ITU-T channel 27, InGaAs: InGaAs/InP single-photon avalanche diodes, UC: up-conversion module, F: wavelenght filters, Si: silicon single-photon avalanche diodes. The transmitter and receiver apparatuses for QKD are further described in Sections 2.3 and 2.4 of Chapter 2.

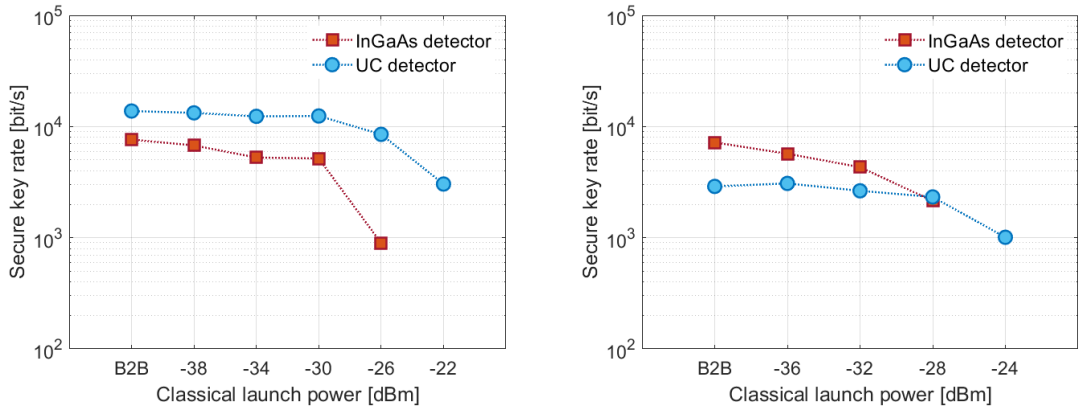
two beams enter the fiber through a DWDM multiplexer, with 200 GHz spacing, and exit the fiber through the same DWDM device, which splits the two wavelengths. Then, the quantum signals are sent to the QKD receiver by means of an optical circulator, while the classical laser is propagated back and partially collected with a photodiode (PD). The remaining power is blocked with an optical isolator (ISO). Another PD is used to monitor the power of the classical laser entering the DWDM. In order to test the performances of our up-conversion setup, the quantum signals are prepared by modulating a laser source emitting at 1555.7 nm, corresponding to channel 27 of the ITU-T grid. The continuous-wave laser for classical light is set to channel 25 of the ITU-T grid, corresponding to 1557.36 nm. The choice of this

wavelength for the classical laser, is based on the experienced behaviour of the overall experimental setup (including the DWDM device and the installed fiber link), in terms of noise. Specifically, we find that when the classical laser entering the fiber (through the DWDM device) is set to ITU-T channel 25, it produces the highest amount of noise observed at the DWDM output corresponding to ITU-T channel 27, i.e., the output connected to the QKD receiver [20]. In this way, we can test the noise tolerance of our QKD setup under the worst-case scenario enabled by our experimental configuration.

The two different setups for single-photon detection that are compared in our work, are denoted by Bob 1 and Bob 2 in Figure 5.7. Bob 1 is based on a commercial InGaAs/InP SPAD from ID Quantique, exhibiting 20% detection efficiency at 1550 nm, and 700 Hz of intrinsic dark count rate at 20 µs dead time. Such settings of efficiency and dead time are needed to optimize the timing jitter (of around 200 ps) while maintaining, at the same time, a low afterpulsing probability. On the other hand, Bob 2 is composed of our home-made up-conversion detector [134], exhibiting an overall efficiency and dark count rate of 2% and 11 kHz, respectively, as mentioned in the previous Section. Despite these lower performances in terms of efficiency and noise, the up-conversion detector outperforms the InGaAs SPAD in terms of timing jitter (34 ps) and dead time (77 ns), thanks to the properties of the silicon-based SPAD from Micro Photon Devices. Notably, the lower timing jitter enables to apply a narrower temporal filter around the center of each time bin, during the post-selection of the detection events, necessary to improve the signal-to-noise ratio. Moreover, the lower dead time allows for a higher maximum count rate of the detection events, thus limiting the saturation effects in the QKD receiver. This means also that a larger block size[4] of detection events can be acquired during the same acquisition time.

As previously mentioned, the up-conversion detector inherently acts as filter of the incoming beam, in polarization and wavelength, as shown by the phase matching profile in Figure 5.6b. Therefore, as reported in Figure 5.7, a polarization controller (PC) is included in the receiver setup, in order to align the incoming quantum signal to the optimal polarization direction. The same feature of polarization filtering is included in Bob 1 setup, by placing a polarizing beam splitter (PBS) in front of the InGaAs detector. Moreover, Bob 1 is equipped with a 100 GHz wavelength filter of ITU-T channel 27, exhibiting a 3 dB bandwidth of 0.64 nm and more than 40 dB

[4]Despite this fact, in our work [20] the two receivers are tested by setting the same post-processing block size of 10^7 raw-key bits.



(a) 3 dB channel loss.

(b) 5 dB channel loss.

Figure 5.8: In this Figure, inspired from our work [20], is reported the secure key rate achievable by the two QKD receivers (standard InGaAs detector and up-conversion-assisted detection module), at two different loss values of the quantum channel, with the increasing launch power of the classical laser injected in the same metropolitan fiber, in a DWDM scheme. The B2B configuration denotes no classical launch power injected in the fiber link. In both cases, the up-conversion module enables to distribute a secure key with a 4 dB higher launch power of the classical laser.

of extinction ratio between ITU-T channels 25 and 27. In this way, we provide the InGaAs receiver with the same advantages that are embodied in the up-conversion process. The overall insertion loss introduced by beam filtering in Bob 1 is around 6 dB. Furthermore, when testing each receiver, the polarization of the classical laser is rotated, at the transmitter side[5], in order to minimize the induced noise in the detection setup: in this way, we can test and compare the properties of polarization filtering of each receiver.

The results of our experiment are reported in Figure 5.8. We test the two detection setups by performing the three-state BB84 with time-bin encoding and one decoy state, as in the previous field trial [19]. However, as opposed to the previous experiment, here only a portion of the metropolitan fiber acts as a quantum channel, while the remaining part is included in the attenuation of the transmitter[6]. In this way we can test the two setups at low channel loss, 3 dB and 5 dB. The reason is that no secure key can be distributed at more than 6 dB channel loss with the up-

[5]Notably, the experienced noise induced by the classical laser at the other outputs of the DWDM device, is found to be independent from the input polarization [20].

[6]The fact that in our experiment, the classical laser is attenuated through several kilometers of fiber propagation, instead of standard optical attenuators, leads to a larger amount of nonlinear noise generated in our setup.

conversion receiver [20], even when the co-propagated classical power is zero, due to the intrinsic noise of the up-conversion module. Such noise, of about 11 kHz, limits the achievable distance by QKD, but can be improved by designing a different setup with long-wavelength pump laser, as already discussed in the previous Section. In general, using different setups with fewer insertion loss at the receiver would enable QKD at higher channel loss, but this is not the purpose of our work, as we aim to test two different detection schemes under the same experimental condition.

Figures 5.8a and 5.8b show the estimated secure key rate at 3 and 5 dB channel loss, respectively, as a function of the effective launch power of the classical laser. Notably, the launch power reported in Figure 5.8 is the classical optical power at the input of the effective quantum channel, hence, it is different from the optical power injected at the DWDM input of ITU-T channel 25. Nonetheless, at both 3 dB and 5 dB channel loss, the up-conversion receiver is demonstrated to be more tolerant to the co-propagated classical laser, as it can afford a 4 dB higher launch power than the InGaAs-based receiver, equipped with off-the-shelf filters. This means that, in a realistic application, the multiplexed data traffic can be more than doubled when using an up-conversion-assisted single-photon detector, with no need to add additional filtering in the QKD receiver. Furthermore, as already mentioned, our up-conversion module for the telecom C-band can still be optimized, as demonstrated in recent works [135–137]. In the end, our work proves that up-conversion-assisted receivers for QKD, combined with multiplexing techniques, have the potential to improve notably the maximum tolerable data traffic co-propagated in the same fiber, under a DWDM scheme in the C-band, essential to achieve the full integration of QKD technologies in the existing infrastructures for optical communications.

5.3 Public demonstrations of in-field QKD

After the field trials in Florence, a similar setup for time-encoded QKD was also tested in Trieste [124], during a public demonstration of metropolitan-scale QKD, performed at the closing ceremony of ESOF 2020 (the EuroScience Open Forum), at the presence of the Italian Prime Minister. This event, conducted in collaboration with University of Trieste and portrayed in the pictures of Figure 5.9, was the first public demonstration of in-field QKD to be performed in Italy. In this case, the transmitting and the receiving stations, connected by a metropolitan link, were situated far apart: the transmitter was placed at ESOF 2020 Auditorium, located

(a) A QKD station placed at the conference Auditorium.

(b) The video-call.

(c) Set up of the QKD apparatus.

Figure 5.9: Pictures of the public demonstration of in-field QKD at ESOF 2020 [124].

in the Old Port of Trieste, while the receiver was placed at the ICT Department of University of Trieste. The two stations were connected through a pair of dark fibers, of about 10 km, belonging to the LightNet fiber network of Trieste. In this QKD implementation, the synchronization signal between the two stations was optically delivered, by exploiting the second fiber. In addition, the post-processing step of the QKD protocol was also implemented, in order to generate a private key, to be used for the secure authentication of a video-call between the Head of University of Trieste, from the ICT Department, and the Italian Prime Minister, attending the ceremony from the stage of ESOF 2020 Auditorium (Figure 5.9).

Another public demonstration of in-field QKD was later performed on August

2021, during the Digital Ministers' Meeting of the G20, held in Trieste. Here, time-encoded QKD was implemented between three different countries (Italy, Slovenia and Croatia) by exploiting a fiber network of multiple nodes, located in Trieste, Postojna, Ljubljana and Rijeka [138].

Conclusions

This thesis presents the main contributions and results achieved during the past three years of my Ph.D. work, mostly carried out at the National Institute of Optics of Florence (CNR-INO, Italy), in close cooperation with the DTU Fotonik at the Technical University of Denmark. In particular, our research activity has been mainly focused on practical quantum key distribution (QKD) based on single-mode fiber links, over metropolitan distances. The aim of our work is to address some open issues of current QKD protocols, which still suffer from high costs of implementation and low tolerance for noise and instability, thus resulting into a serious limit to the full integration of QKD technologies in the already existing infrastructures for fiber-based optical communications.

In the first two contributions presented in this thesis (Chapters 3 and 4) we introduce and test two novel schemes for high-dimensional QKD, both based on time-bin and phase encoding. The preparation of quantum states with such degrees of freedom is the most compatible with fiber-based transmission; moreover, it requires standard equipment for optical telecommunication. In addition, high-dimensional encoding enables to improve the performances of the current QKD setups for binary encoding, at the typical metropolitan distances (i.e., tens of kilometers). In particular, in the work presented in Chapter 3, and published in Ref. [22], we design an efficient encoding scheme for four-dimensional QKD, which boasts a notably simplified receiver in comparison with the conventional time-bin encoding. Our proposed setup requires only two single-photon detectors to carry out all the quantum measurements, thus the amount of expensive resources needed is basically the same as in standard QKD setups for binary encoding. At the same time, our efficient scheme for high-dimensional QKD enables to improve the key generation rate achievable with binary-encoded QKD, up to around 100 km of distance (20 dB channel loss), as we demonstrate by testing the two different QKD protocols in the laboratory, using the same experimental equipment. Next, in the work presented in Chapter 4, and published in Ref. [23], we introduce a high-dimensional version of the

round-robin QKD. The round-robin protocol has the peculiarity of not requiring the monitoring of the quantum channel for estimating the leaked information; however, its performances are typically limited by the environmental noise affecting the quantum measurements, which require optimal and stable visibility to be preserved in a variable-delay interferometric setup. Our proposed protocol exploits the additional encoding in the time-bin degree of freedom, whose measurement is not affected by the quality of interference and, hence, it typically exhibits a low error rate in practical implementations. As a result, our protocol can distribute a secure key also in the condition of high interference misalignment (down to 30% visibility at 10 dB channel loss), where the original round-robin QKD fails. Our results are simulated without relaxing the security assumptions of the original protocol, and are assessed in a proof-of-principle experiment performed in the laboratory.

In the last contributions of this thesis [19, 20], we present the realization of in-field experiments of time-encoded QKD, performed over a metropolitan fiber installed in Florence. In these works we address the practical challenges of implementing QKD under real-world conditions: the extra loss and noise exhibited by the already-installed fibers, the long-term stability of the QKD apparatus and the coexistence of quantum and classical signals co-propagated in the same fiber, by means of dense-wavelength division multiplexing (DWDM) in the C-band. To enable long-term quantum communication over several hours, we implement a servo-locking interferometric setup at the QKD receiver, able to automatically stabilize the quantum measurements with no need to monitor the error rates. Furthermore, we demonstrate an improvement of the current DWDM schemes of quantum and classical light in the telecom C-band, by taking advantage of the properties of a frequency up-conversion detector. Thanks to the intrinsic filtering in polarization and wavelength, and to the higher timing performances of silicon-based single-photon detection, our up-conversion-assisted receiver for QKD is demonstrated to tolerate more classical power (4 dB higher), in comparison with a standard receiver based on InGaAs single-photon detectors and equipped with off-the-shelf filtering devices. In conclusion, we mention a public demonstration of in-field QKD, performed over a metropolitan link in Trieste.

A

Security analysis of the round-robin protocols

In this Appendix are presented the main steps of the security analysis of the round-robin protocols for quantum key distribution, discussed in Chapter 4. More details on the following derivation can be found in Ref. [116] and in our work [23].

A.1 Improved security bounds for the round-robin DPS

Here are reported the main ideas behind the improved security proof for the round-robin protocol, proposed in Ref. [116] and briefly discussed in Section 4.1.1.

Let's start with considering an L-pulse packet containing only a single photon ($n = 1$). Then, the quantum state describing the packet is given by the superposition of a single-photon state in all the bins $i = 1, ..., L$, with different phase factors ± 1, as follows:

$$|\psi\rangle = \frac{1}{\sqrt{L}} \sum_{i=1}^{L} (-1)^{k_i} |i\rangle \ , \tag{A.1}$$

where $k_i = 0, 1$ denotes the relative phase information. Under the hypothesis of collective attacks on the quantum channel, Eve probes each packet separately by making it interact with her ancillary system, initially described by the state $|e_{00}\rangle$. Her general action on the global system $|\psi\rangle|e_{00}\rangle$ can be described by the following transformation:

$$U_{\text{Eve}}|\psi\rangle|e_{00}\rangle = \frac{1}{\sqrt{L}} \sum_{i,j=1}^{L} (-1)^{k_i} c_{ij} |j\rangle|e_{ij}\rangle \ , \tag{A.2}$$

where the bin i has been shifted to the bin j and the ancillary state has turned into $|e_{ij}\rangle$, with the non-negative real parameters c_{ij}, related to the probabilities c_{ij}^2. Then, Eve retains only her ancilla and forwards the single-photon packet to Bob. If Bob witnesses a successful detection event, he obtains the measurement outcomes $a, b \in \{1, 2, ..., L\}$ (with $b = a+r$) and the relative phase factor ± 1, meaning that his quantum state has been projected onto one of the superposition states $(|a\rangle \pm |b\rangle)/\sqrt{2}$, respectively. Notably, these two orthonormal states form a basis. Thus, considering Bob's measurement, the state of the overall system (Bob's photon and Eve's ancilla) can be seen as

$$|\Psi\rangle = \frac{1}{\sqrt{L}} \sum_{i=1}^{L} (-1)^{k_i} \Big(c_{ia}|a\rangle|e_{ia}\rangle + c_{ib}|b\rangle|e_{ib}\rangle \Big) \tag{A.3}$$

and the density matrix of Eve's ancilla, ρ_{Eve}, can be computed as the partial trace of the global system $\rho_\Psi = |\Psi\rangle\langle\Psi|$, which gives

$$\rho_{\text{Eve}} \propto P\left\{ \sum_{i=1}^{L} (-1)^{k_i} c_{ia}|e_{ia}\rangle \right\} + P\left\{ \sum_{i=1}^{L} (-1)^{k_i} c_{ib}|e_{ib}\rangle \right\}, \tag{A.4}$$

where the notation $P\{|x\rangle\} = |x\rangle\langle x|$ is adopted. The main idea of the authors from Ref. [116] is that some mixed components arising in ρ_{Eve}, such as $|e_{ia}\rangle\langle e_{aa}|$ and $|e_{ib}\rangle\langle e_{bb}|$, with $i \neq a, b$, can be ignored, being the phase factors $(-1)^{k_i}$ totally random. Therefore, they do not give Eve any useful information, as she knows only a, b (that are publicly announced) and she aims to guess the relative phase information $k_a \oplus k_b$, while she does not care about the relative phases in the other positions. Consequently, in order to compute the Holevo bound, Eve's density matrix can be simplified into

$$\begin{aligned} \rho_{\text{Eve}} \longrightarrow\ & P\Big\{ (-1)^{k_a} c_{aa}|e_{aa}\rangle + (-1)^{k_b} c_{ba}|e_{ba}\rangle \Big\} + P\Big\{ (-1)^{k_a} c_{ab}|e_{ab}\rangle + (-1)^{k_b} c_{bb}|e_{bb}\rangle \Big\} \\ & + \sum_{i \neq a,b} \Big(c_{ia}^2 |e_{ia}\rangle\langle e_{ia}| + c_{ib}^2 |e_{ib}\rangle\langle e_{ib}| \Big), \end{aligned} \tag{A.5}$$

that, for the two raw key bits $k_a \oplus k_b = 0$ and $k_a \oplus k_b = 1$, gives

$$\begin{aligned}\rho_{E,0} &= P\Big\{c_{aa}|e_{aa}\rangle + c_{ba}|e_{ba}\rangle\Big\} + P\Big\{c_{bb}|e_{bb}\rangle + c_{ab}|e_{ab}\rangle\Big\} \\ &\quad + \sum_{i\neq a,b}\Big(c_{ia}^2|e_{ia}\rangle\langle e_{ia}| + c_{ib}^2|e_{ib}\rangle\langle e_{ib}|\Big)\ , \\ \rho_{E,1} &= P\Big\{c_{aa}|e_{aa}\rangle - c_{ba}|e_{ba}\rangle\Big\} + P\Big\{c_{bb}|e_{bb}\rangle - c_{ab}|e_{ab}\rangle\Big\} \\ &\quad + \sum_{i\neq a,b}\Big(c_{ia}^2|e_{ia}\rangle\langle e_{ia}| + c_{ib}^2|e_{ib}\rangle\langle e_{ib}|\Big)\ .\end{aligned} \tag{A.6}$$

Then, by computing the Holevo quantity (Equation 1.23), and by including all the possible outcomes $a, b \in \{1, 2, ..., L\}$, the upper bound on the information leakage is given by [116]

$$I_{AE} \leq \max_{x_1,x_2}\left\{\frac{\varphi\big[(L-1)x_1, x_2\big]}{(L-1)}\right\}\ , \tag{A.7}$$

with the function $\varphi(x, y) = -x\log_2(x) - y\log_2(y) + (x+y)\log_2(x+y)$ and the non-negative real parameters $x_1 = \sum_i c_{ii}^2$ and $x_2 = \sum_{i\neq j} c_{ij}^2 = 1 - x_1$. Such bound on I_{AE} is tighter than the original one, $I_{AE} \leq h(1/(L-1))$, since it enables to generate a secure key also in the case with $L = 3$, that was not permitted according to the original analysis [116].

With similar derivation, the authors of Ref. [116] evaluate Eve's information in the generic case of n photons per L-pulse packet, with $L \geq n + 1$:

$$I_{AE} \leq \max_{x_1,\ldots,x_{n+1}}\left\{\frac{\sum_{m=1}^{n}\varphi\big[(L-m)x_m, mx_{m+1}\big]}{(L-1)}\right\}\ , \tag{A.8}$$

with the non-negative real parameters x_m, satisfying $\sum_{m=1}^{n+1} x_m = 1$. Remarkably, for the Fock components satisfying the $n < L-1$ constrain, $I_{AE} < 1$ holds, meaning that they can be used for key extraction. Furthermore, the upper bound on I_{AE} from Equations A.7 and A.8 depends only on the users settings and not on the channel behaviour, although an even tighter bound can be derived by including the experienced error rates [116].

A.2 Security analysis of the round-robin DPTS

In order to derive the security analysis of our proposed protocol, the round-robin DPTS, we follow the same steps presented in the previous Section, based on the work on the original round-robin protocol, published Ref. [116]. The density matrices to be evaluated in order to compute the Holevo bound, are now $\rho_{E,00}$, $\rho_{E,01}$, $\rho_{E,10}$ and $\rho_{E,11}$. Our derivation of the simplified density matrices follows the same steps of the previous Section, for each different temporal profile of the round-robin DPTS protocol. Our results are briefly discussed in Section 4.2.1. More details can be found in our work [23].

For an L-pulse packet containing a single photon ($n = 1$), the quantum states of the round-robin DPTS protocol can be expressed as

$$\begin{aligned}
|X\rangle_0 &= \frac{1}{\sqrt{L}} \sum_{i=1}^{L} (-1)^{k_{2i}} |2i\rangle \ , \\
|X\rangle_1 &= \frac{1}{\sqrt{L}} \sum_{i=1}^{L} (-1)^{k_{2i-1}} |2i-1\rangle \ , \\
|Z\rangle_0 &= \frac{1}{\sqrt{L}} \sum_{i=1}^{L/2} \Big((-1)^{k_{4i-1}} |4i-1\rangle + (-1)^{k_{4i}} |4i\rangle \Big) \ , \\
|Z\rangle_1 &= \frac{1}{\sqrt{L}} \sum_{i=1}^{L/2} \Big((-1)^{k_{4i-3}} |4i-3\rangle + (-1)^{k_{4i-2}} |4i-2\rangle \Big) \ ,
\end{aligned} \tag{A.9}$$

where each state is related to the corresponding temporal profile from Figure 4.2, while the coefficients k_{2i}, k_{2i-1}, ... $= 0,\ 1$ denote the relative phases between the nonempty time bins. Again, Eve's general attack on each quantum state can be described by the translation $i \to j$. A successful detection event occurs when Bob projects the incoming states $|X\rangle_0$ or $|X\rangle_1$ onto $(|2a\rangle \pm |2b\rangle)/\sqrt{2}$ or $(|2a-1\rangle \pm |2b-1\rangle)/\sqrt{2}$, respectively, and similarly for $|Z\rangle_0$ or $|Z\rangle_1$ states [23]. The overall state of the system, including Bob's photon and Eve's ancilla used to probe the photon, is derived (for each of the four cases) in an analogous way as shown in the previous Section. Then, we use the same considerations to simplify Eve's density matrices in the four cases (ρ_{X_0}, ρ_{X_1}, ρ_{Z_0}, ρ_{Z_1}), by keeping only the components that are useful to access both the temporal and the relative phase information. The mixed components with $i \neq a, b$, such as $|e_{2i,2a}\rangle\langle e_{2a,2a}|$ and $|e_{2i,2b}\rangle\langle e_{2b,2b}|$ arising in ρ_{X_0} or

$|e_{2i-1,2a-1}\rangle\langle e_{2a-1,2a-1}|$ and $|e_{2i-1,2b-1}\rangle\langle e_{2b-1,2b-1}|$ arising in ρ_{X_1}, can be ignored being the phase factors $(-1)^{2k_i}$ and $(-1)^{2k_i-1}$ totally random (and similarly for ρ_{Z_0} and ρ_{Z_1}). Consequently, for X basis we have

$$\begin{aligned}\rho_{X_0} \rightarrow\ & P\left\{(-1)^{k_{2a}}\tilde{c}_{2a,2a} + (-1)^{k_{2b}}\tilde{c}_{2b,2a}\right\} + P\left\{(-1)^{k_{2b}}\tilde{c}_{2b,2b} + (-1)^{k_{2a}}\tilde{c}_{2a,2b}\right\} \\ & + \sum_{i\neq a,b}\left(c^2_{2i,2a}|e_{2i,2a}\rangle\langle e_{2i,2a}| + c^2_{2i,2b}|e_{2i,2b}\rangle\langle e_{2i,2b}|\right) ,\end{aligned} \tag{A.10}$$

$$\begin{aligned}\rho_{X_1} \rightarrow\ & P\left\{(-1)^{k_{2a-1}}\tilde{c}_{2a-1,2a-1} + (-1)^{k_{2b-1}}\tilde{c}_{2b-1,2a-1}\right\} \\ & + P\left\{(-1)^{k_{2b-1}}\tilde{c}_{2b-1,2b-1} + (-1)^{k_{2a-1}}\tilde{c}_{2a-1,2b-1}\right\} \\ & + \sum_{i\neq a,b}\left(c^2_{2i-1,2a-1}|e_{2i-1,2a-1}\rangle\langle e_{2i-1,2a-1}| + c^2_{2i-1,2b-1}|e_{2i-1,2b-1}\rangle\langle e_{2i-1,2b-1}|\right) ,\end{aligned} \tag{A.11}$$

where $P\{|x\rangle\} = |x\rangle\langle x|$ and $\tilde{c}_{m,k} \triangleq c_{m,k}|e_{m,k}\rangle$. Similar expressions are found for Z basis, even if different cases has to be taken into account separately, such as even r, odd r and $r = 1$ [23]. Then, the four simplified density matrices are evaluated for the two different phase-encoded bits: $\rho_{X_0,0}$ and $\rho_{X_0,1}$ (corresponding to $k_{2a} \oplus k_{2b} = 0$ or 1, respectively), $\rho_{X_1,0}$ and $\rho_{X_1,1}$ (corresponding to $k_{2a-1} \oplus k_{2b-1} = 0$ or 1, respectively) and analogously for $\rho_{Z_0,0}$, $\rho_{Z_0,1}$, $\rho_{Z_1,0}$, $\rho_{Z_1,1}$. Here, the first subscript of the density operators refers to the time-encoded bit in the temporal pattern, while the second subscript refers to the phase-encoded bit in the a-th and b-th pulses of the L-pulse packet. Finally, we compute Eve's density matrices corresponding to the four different symbols included in Alice's and Bob's raw keys, in the following way [120]:

$$\begin{aligned}\rho_{E,00} &= \frac{1}{2}(\rho_{X_0,0} + \rho_{Z_0,0}) , & \rho_{E,10} &= \frac{1}{2}(\rho_{X_1,0} + \rho_{Z_1,0}) , \\ \rho_{E,01} &= \frac{1}{2}(\rho_{X_0,1} + \rho_{Z_0,1}) , & \rho_{E,11} &= \frac{1}{2}(\rho_{X_1,1} + \rho_{Z_1,1}) ,\end{aligned} \tag{A.12}$$

as the two basis are chosen uniformly at random. After evaluating the Holevo bound (Equation 1.23 from Chapter 1), we find Eve's information in the single-photon case:

$$I_{AE} \leq \max_{x_1,x_2,y_1,y_2}\left\{\frac{f\left[(L-1)x_1, x_2\right] + \frac{1}{8}(L-2)x_2 + f\left[\frac{L/2-1}{2}y_1, \frac{1}{2}y_2\right] + \frac{1}{16}(L/2-2)y_2}{\frac{1}{2}(L-1) + \frac{1}{2}(L/2-1)}\right\} , \tag{A.13}$$

with $f(x,y) = -\frac{x}{4}\log_4\frac{x}{4} - \frac{y}{4}\log_4\frac{y}{4} + \frac{x+y}{4}\log_4\frac{x+y}{2}$ and the non-negative real parameters x_1, x_2, y_1, y_2 satisfying $x_1 + x_2 = 2$ and $y_1 + y_2 = 2$ [23].

In the general case of an L-pulse packet with n photons, if $L \geq 2(n+1)$, then Eve's information can be bounded by

$$I_{AE} \leq \max_{x_1,\ldots,x_{n+1},y_1,\ldots,y_{n+1}} \left\{ \frac{1}{\frac{1}{2}(L-1) + \frac{1}{2}(L/2-1)} \left[\sum_{m=1}^{n} f\big[(L-m)x_m, m x_{m+1}\big] + \frac{(L-n-1)x_{n+1}}{8} + \sum_{m=1}^{n} f\Big(\frac{L/2-m}{2} y_m, \frac{m}{2} y_{m+1}\Big) + \frac{(L/2-n-1)y_{n+1}}{16} \right] \right\}, \tag{A.14}$$

with $\sum_{m=1}^{n+1} x_i = 2$ and $\sum_{m=1}^{n+1} y_i = 2$ [23].

Bibliography

[1] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.

[2] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[3] "Post-Quantum Cryptography." `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography`, 2016-2021. National Institute of Standards and Technology, Computer Security Resource Center [Online; accessed on September 2021].

[4] 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*, pp. 175–179, 1984.

[5] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[6] 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, *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Physical review letters*, vol. 117, no. 19, p. 190501, 2016.

[7] 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, *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[8] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, *et al.*, "Satellite-relayed intercontinental quantum network," *Physical review letters*, vol. 120, no. 3, p. 030501, 2018.

[9] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, *et al.*, "Secure quantum key distribution over 421 km of optical fiber," *Physical review letters*, vol. 121, no. 19, p. 190502, 2018.

[10] J. Dynes, A. Wonfor, W.-S. Tam, A. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. Yuan, A. Dixon, J. Cho, *et al.*, "Cambridge quantum network," *npj Quantum Information*, vol. 5, no. 1, pp. 1–8, 2019.

[11] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, *et al.*, "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," *Nature Photonics*, vol. 14, no. 7, pp. 422–425, 2020.

[12] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, 2021.

[13] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, "Provably secure and high-rate quantum key distribution with time-bin qudits," *Science advances*, vol. 3, no. 11, p. e1701491, 2017.

[14] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami, *et al.*, "10-Mb/s Quantum Key Distribution," *Journal of Lightwave Technology*, vol. 36, no. 16, pp. 3427–3433, 2018.

[15] J. Qiu, "Quantum communications leap out of the lab," *Nature*, vol. 508, no. 7497, p. 441, 2014.

[16] A. De Touzalin, C. Marcus, F. Heijman, I. Cirac, R. Murray, and T. Calarco, "Quantum manifesto. A new era of technology," *European Comission*, pp. 1–20, 2016.

[17] G. Lenhart, "QKD standardization at ETSI," in *AIP Conference Proceedings*, vol. 1469, pp. 50–57, American Institute of Physics, 2012.

[18] R. Alléaume, I. P. Degiovanni, A. Mink, T. E. Chapuran, N. Lutkenhaus, M. Peev, C. J. Chunnilall, V. Martin, M. Lucamarini, M. Ward, *et al.*, "World-

wide standardization activity for quantum key distribution," in *2014 IEEE Globecom Workshops (GC Wkshps)*, pp. 656–661, IEEE, 2014.

[19] D. Bacco, I. Vagniluca, B. Da Lio, N. Biagi, A. Della Frera, D. Calonico, C. Toninelli, F. S. Cataliotti, M. Bellini, L. K. Oxenløwe, *et al.*, "Field trial of a three-state quantum key distribution scheme in the Florence metropolitan area," *EPJ Quantum Technology*, vol. 6, no. 1, p. 5, 2019.

[20] D. Bacco, I. Vagniluca, D. Cozzolino, S. M. Friis, L. Høgstedt, A. Giudice, D. Calonico, F. S. Cataliotti, K. Rottwitt, and A. Zavatta, "Toward fully-fledged quantum and classical communication over deployed fiber with up-conversion module," *Advanced Quantum Technologies*, vol. 4, no. 2000156, 2021.

[21] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, "High-dimensional quantum communication: Benefits, progress, and future challenges," *Advanced Quantum Technologies*, vol. 2, no. 12, p. 1900038, 2019.

[22] I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D. Bacco, "Efficient time-bin encoding for practical high-dimensional quantum key distribution," *Phys. Rev. Applied*, vol. 14, p. 014051, Jul 2020.

[23] K. Wang, I. Vagniluca, J. Zhang, S. Forchhammer, A. Zavatta, J. B. Christensen, and D. Bacco, "Round-robin differential phase-time-shifting protocol for quantum key distribution: Theory and experiment," *Phys. Rev. Applied*, vol. 15, p. 044017, Apr 2021.

[24] E. Rescorla, "HTTP over TLS," tech. rep., IETF RFC 2818, 2000. `https://www.ietf.org/rfc/rfc2818.txt`.

[25] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM journal on Computing*, vol. 26, no. 5, pp. 1510–1523, 1997.

[26] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, 1996.

[27] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, *Report on post-quantum cryptography*, vol. 12. US Department of Commerce, National Institute of Standards and Technology, 2016.

[28] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Journal of the AIEE*, vol. 45, no. 2, pp. 109–115, 1926.

[29] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[30] M. A. Wright, "The Advanced Encryption Standard," *Network Security*, vol. 2001, no. 10, pp. 11–13, 2001.

[31] E. Barker, W. Burr, W. Polk, M. Smid, *et al.*, "Recommendation for key management: Part 1 - General (Revision 5)," *NIST Special Publication*, vol. 800, no. 57, 2020.

[32] T. Matsumoto and H. Imai, "On the key predistribution system: A practical solution to the key distribution problem," in *Conference on the Theory and Application of Cryptographic Techniques*, pp. 185–193, Springer, 1987.

[33] L. M. Batten, *Public key cryptography: applications and attacks*. John Wiley & Sons, 2013.

[34] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

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

[36] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.

[37] D. Mahto and D. K. Yadav, "Performance analysis of RSA and elliptic curve cryptography," *Int. J. Netw. Secur.*, vol. 20, no. 4, pp. 625–635, 2018.

[38] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134, Ieee, 1994.

[39] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[40] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature*, vol. 414, no. 6866, pp. 883–887, 2001.

[41] A. Politi, J. C. Matthews, and J. L. O'brien, "Shor's quantum factoring algorithm on a photonic chip," *Science*, vol. 325, no. 5945, pp. 1221–1221, 2009.

[42] E. Lucero, R. Barends, Y. Chen, J. Kelly, M. Mariantoni, A. Megrant, P. O'Malley, D. Sank, A. Vainsencher, J. Wenner, *et al.*, "Computing prime factors with a Josephson phase qubit quantum processor," *Nature Physics*, vol. 8, no. 10, pp. 719–723, 2012.

[43] E. Martin-Lopez, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O'brien, "Experimental realization of Shor's quantum factoring algorithm using qubit recycling," *Nature photonics*, vol. 6, no. 11, pp. 773–776, 2012.

[44] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Reviews of Modern Physics*, vol. 92, no. 2, p. 025002, 2020.

[45] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[46] C. Gerry and P. Knight, *Introductory Quantum Optics*. Cambridge university press, 2004.

[47] S. Barnett, *Quantum information*, vol. 16. Oxford University Press, 2009.

[48] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of modern physics*, vol. 81, no. 3, p. 1301, 2009.

[49] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *et al.*, "Advances in quantum

cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[50] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters*, vol. 81, no. 14, p. 3018, 1998.

[51] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," *Physical Review Letters*, vol. 88, no. 12, p. 127902, 2002.

[52] J. Martínez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martín, "Demystifying the information reconciliation protocol Cascade," *Quantum Inf. Comput.*, vol. 15, no. 5&6, pp. 453–477, 2015.

[53] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *Journal of Cryptology*, vol. 18, no. 2, pp. 133–165, 2005.

[54] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," *Physical Review A*, vol. 89, no. 2, p. 022307, 2014.

[55] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, "Finite-key analysis for the 1-decoy state QKD protocol," *Applied Physics Letters*, vol. 112, no. 17, p. 171104, 2018.

[56] D. Rusca, A. Boaron, M. Curty, A. Martin, and H. Zbinden, "Security proof for a simplified Bennett-Brassard 1984 quantum-key-distribution protocol," *Physical Review A*, vol. 98, no. 5, p. 052336, 2018.

[57] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Simple 2.5 GHz time-bin quantum key distribution," *Applied Physics Letters*, vol. 112, no. 17, p. 171108, 2018.

[58] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Physical Review A*, vol. 61, no. 5, p. 052304, 2000.

[59] D. Gottesman and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications," *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 457–475, 2003.

[60] R. Loudon, *The quantum theory of light*. OUP Oxford, 2000.

[61] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, "Attacks on practical quantum key distribution systems (and how to prevent them)," *Contemporary Physics*, vol. 57, no. 3, pp. 366–387, 2016.

[62] 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.

[63] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar 2012.

[64] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130502, Mar 2012.

[65] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Physical Review Letters*, vol. 91, no. 5, p. 057901, 2003.

[66] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical review letters*, vol. 94, no. 23, p. 230504, 2005.

[67] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Physical review letters*, vol. 94, no. 23, p. 230503, 2005.

[68] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A*, vol. 72, no. 1, p. 012326, 2005.

[69] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journal of the American Statistical Association*, vol. 58, no. 301, pp. 13–30, 1963.

[70] H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," *Physical Review A*, vol. 61, no. 6, p. 062308, 2000.

[71] L. Sheridan and V. Scarani, "Security proof for quantum key distribution using qudit systems," *Physical Review A*, vol. 82, no. 3, p. 030301, 2010.

[72] D. Bacco, B. Da Lio, D. Cozzolino, F. Da Ros, X. Guo, Y. Ding, Y. Sasaki, K. Aikawa, S. Miki, H. Terai, *et al.*, "Boosting the secret key rate in a

shared quantum and classical fibre communication system," *Communications Physics*, vol. 2, no. 1, pp. 1–8, 2019.

[73] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, "Efficient decoy-state quantum key distribution with quantified security," *Optics express*, vol. 21, no. 21, pp. 24550–24565, 2013.

[74] J. F. Dynes, W. W. Tam, A. Plews, B. Fröhlich, A. W. Sharpe, M. Lucamarini, Z. Yuan, C. Radig, A. Straw, T. Edwards, *et al.*, "Ultra-high bandwidth quantum secured data transmission," *Scientific reports*, vol. 6, p. 35149, 2016.

[75] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, "Long-distance quantum key distribution secure against coherent attacks," *Optica*, vol. 4, no. 1, pp. 163–167, 2017.

[76] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Simple and high-speed polarization-based QKD," *Applied Physics Letters*, vol. 112, no. 5, p. 051108, 2018.

[77] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, "High-dimensional quantum cryptography with twisted light," *New Journal of Physics*, vol. 17, no. 3, p. 033033, 2015.

[78] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, *et al.*, "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding," *New Journal of Physics*, vol. 17, no. 2, p. 022002, 2015.

[79] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, "High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits," *npj Quantum Information*, vol. 3, no. 1, p. 25, 2017.

[80] G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. Connolly, A. Przysiezna, E. Gómez, M. Figueroa, G. Vallone, *et al.*, "High-dimensional

decoy-state quantum key distribution over multicore telecommunication fibers," *Physical Review A*, vol. 96, no. 2, p. 022317, 2017.

[81] D. Cozzolino, D. Bacco, B. Da Lio, K. Ingerslev, Y. Ding, K. Dalgaard, P. Kristensen, M. Galili, K. Rottwitt, S. Ramachandran, *et al.*, "Orbital angular momentum states enabling fiber-based high-dimensional quantum communication," *Physical Review Applied*, vol. 11, no. 6, p. 064058, 2019.

[82] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Physical review letters*, vol. 68, no. 5, p. 557, 1992.

[83] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 112, p. 190503, May 2014.

[84] R. Valivarthi, Q. Zhou, C. John, F. Marsili, V. B. Verma, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, "A cost-effective measurement-device-independent quantum key distribution system for quantum networks," *Quantum Science and Technology*, vol. 2, no. 4, p. 04LT01, 2017.

[85] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, *et al.*, "High-speed measurement-device-independent quantum key distribution with integrated silicon photonics," *Physical Review X*, vol. 10, no. 3, p. 031030, 2020.

[86] 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, pp. 400–403, 2018.

[87] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, "Experimental quantum key distribution beyond the repeaterless secret key capacity," *Nature Photonics*, vol. 13, no. 5, pp. 334–338, 2019.

[88] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system," *Physical Review X*, vol. 9, no. 2, p. 021046, 2019.

[89] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, "Proof-of-principle experimental demonstration of twin-field type quantum key distribution," *Physical review letters*, vol. 123, no. 10, p. 100506, 2019.

[90] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical review letters*, vol. 88, no. 5, p. 057902, 2002.

[91] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: principle, security and implementations," *Entropy*, vol. 17, no. 9, pp. 6072–6092, 2015.

[92] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Physical review letters*, vol. 89, no. 3, p. 037902, 2002.

[93] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters*, vol. 87, no. 19, p. 194108, 2005.

[94] T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," *Nature*, vol. 509, no. 7501, pp. 475–478, 2014.

[95] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes, *et al.*, "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, no. 7, p. 075001, 2009.

[96] D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, *et al.*, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, no. 12, p. 123001, 2011.

[97] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, *et al.*, "Field test of quantum key distribution in the Tokyo QKD Network," *Optics express*, vol. 19, no. 11, pp. 10387–10409, 2011.

[98] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, *et al.*, "Metropolitan all-pass and inter-city quantum communication network," *Optics express*, vol. 18, no. 26, pp. 27217–27225, 2010.

[99] F. Mitschke, *Fiber Optics Physics and Technology.* Springer-Verlag Berlin Heidelberg, 2016.

[100] E. L. Wooten, K. M. Kissa, A. Yi-Yan, E. J. Murphy, D. A. Lafaw, P. F. Hallemeier, D. Maack, D. V. Attanasio, D. J. Fritz, G. J. McBrien, *et al.*, "A review of lithium niobate modulators for fiber-optic communications systems," *IEEE Journal of selected topics in Quantum Electronics*, vol. 6, no. 1, pp. 69–82, 2000.

[101] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, "Discrete-phase-randomized coherent state source and its application in quantum key distribution," *New Journal of Physics*, vol. 17, no. 5, p. 053014, 2015.

[102] T. Kobayashi, A. Tomita, and A. Okamoto, "Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser," *Physical Review A*, vol. 90, no. 3, p. 032320, 2014.

[103] N. Benvenuto, G. Cherubini, and S. Tomasin, *Algorithms for communications systems and their applications.* John Wiley & Sons, 2021.

[104] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.*, vol. 89, p. 015004, Feb 2017.

[105] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, "Advances in InGaAs/InP single-photon detector systems for quantum communication," *Light: Science & Applications*, vol. 4, no. 5, pp. e286–e286, 2015.

[106] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, "Superconducting nanowire single-photon detectors: physics and applications," *Superconductor science and technology*, vol. 25, no. 6, p. 063001, 2012.

[107] T. Ikuta and H. Takesue, "Four-dimensional entanglement distribution over 100 km," *Scientific reports*, vol. 8, no. 1, p. 817, 2018.

[108] N. T. Islam, C. Cahall, A. Aragoneses, A. Lezama, J. Kim, and D. J. Gauthier, "Robust and stable delay interferometers with application to d-dimensional time-frequency quantum key distribution," *Physical Review Applied*, vol. 7, no. 4, p. 044010, 2017.

[109] N. T. Islam, C. C. W. Lim, C. Cahall, B. Qi, J. Kim, and D. J. Gauthier, "Scalable high-rate, high-dimensional time-bin encoding quantum key distribution," *Quantum Science and Technology*, vol. 4, no. 3, p. 035008, 2019.

[110] T. Brougham and S. M. Barnett, "Mutually unbiased measurements for high-dimensional time-bin–based photonic states," *EPL (Europhysics Letters)*, vol. 104, no. 3, p. 30003, 2013.

[111] A. Ruiz Alba Gaya, D. Calvo Díaz-Aldagalán, V. García Muñoz, A. Martínez García, A. Ocampo, W. Alexander, R. Chicue, J. Guillermo, J. Mora Almerich, and J. Capmany Francoy, "Practical quantum key distribution based on the BB84 protocol," in *Waves*, vol. 1, pp. 4–14, Instituto de Telecomunicaciones y Aplicaciones Multimedia (iTEAM), 2011.

[112] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," *Phys. Rev. A*, vol. 68, p. 022317, Aug 2003.

[113] K. Wen, K. Tamaki, and Y. Yamamoto, "Unconditional security of single-photon differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 103, p. 170503, Oct 2009.

[114] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. Fejer, K. Inoue, and Y. Yamamoto, "Differential phase shift quantum key distribution experiment over 105 km fibre," *New Journal of Physics*, vol. 7, no. 1, p. 232, 2005.

[115] Z. Zhang, X. Yuan, Z. Cao, and X. Ma, "Practical round-robin differential-phase-shift quantum key distribution," *New Journal of Physics*, vol. 19, no. 3, p. 033013, 2017.

[116] Z.-Q. Yin, S. Wang, W. Chen, Y.-G. Han, R. Wang, G.-C. Guo, and Z.-F. Han, "Improved security bound for the round-robin-differential-phase-shift quantum key distribution," *Nature communications*, vol. 9, no. 1, pp. 1–8, 2018.

[117] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, "Experimental quantum key distribution without monitoring signal disturbance," *Nature Photonics*, vol. 9, no. 12, pp. 827–831, 2015.

[118] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Experimental demonstration of a quantum key distribution without signal disturbance monitoring," *Nature Photonics*, vol. 9, no. 12, pp. 832–836, 2015.

[119] Y.-H. Li, Y. Cao, H. Dai, J. Lin, Z. Zhang, W. Chen, Y. Xu, J.-Y. Guan, S.-K. Liao, J. Yin, *et al.*, "Experimental round-robin differential phase-shift quantum key distribution," *Physical Review A*, vol. 93, no. 3, p. 030302, 2016.

[120] D. Bacco, J. B. Christensen, M. A. U. Castaneda, Y. Ding, S. Forchhammer, K. Rottwitt, and L. K. Oxenløwe, "Two-dimensional distributed-phase-reference protocol for quantum key distribution," *Scientific reports*, vol. 6, no. 36756, pp. 1–7, 2016.

[121] B. Da Lio, D. Bacco, D. Cozzolino, Y. Ding, K. Dalgaard, K. Rottwitt, and L. K. Oxenløwe, "Experimental demonstration of the DPTS QKD protocol over a 170 km fiber link," *Applied Physics Letters*, vol. 114, no. 1, p. 011101, 2019.

[122] T. Matsuura, T. Sasaki, and M. Koashi, "Refined security proof of the round-robin differential-phase-shift quantum key distribution and its improved performance in the finite-sized case," *Physical Review A*, vol. 99, no. 4, p. 042303, 2019.

[123] H. Liu, Z.-Q. Yin, R. Wang, F.-Y. Lu, S. Wang, W. Chen, W. Huang, B.-J. Xu, G.-C. Guo, and Z.-F. Han, "Finite-key analysis for round-robin-differential-phase-shift quantum key distribution," *Optics express*, vol. 28, no. 10, pp. 15416–15423, 2020.

[124] I. Vagniluca, N. Biagi, D. Bacco, and A. Zavatta, "A quantum cryptography system used to encrypt the Italian Prime Minister's videocall at ESOF2020," *Il Colle di Galileo*, vol. 10, no. 1, pp. 43–47, 2021.

[125] D. Bacco, N. Biagi, I. Vagniluca, T. Hayashi, A. Mecozzi, C. Antonelli, L. K. Oxenløwe, and A. Zavatta, "Characterization and stability measurement of deployed multicore fibers for quantum applications," *Photonics Research*, vol. 9, pp. 1992–1997, Oct 2021.

[126] M. Avesani, L. Calderaro, G. Foletto, C. Agnesi, F. Picciariello, F. B. Santagiustina, A. Scriminich, A. Stanco, F. Vedovato, M. Zahidy, *et al.*, "Resource-effective quantum key distribution: a field trial in Padua city center," *Optics Letters*, vol. 46, no. 12, pp. 2848–2851, 2021.

[127] D. Calonico, "A fibre backbone in italy for precise time and quantum key distribution," in *4th ETSI/IQC workshop on quantum-safe cryptography*, 2016.

[128] D. Bacco, B. Da Lio, D. Cozzolino, F. Da Ros, X. Guo, Y. Ding, Y. Sasaki, K. Aikawa, S. Miki, H. Terai, *et al.*, "Boosting the secret key rate in a shared quantum and classical fibre communication system," *Communications Physics*, vol. 2, no. 1, pp. 1–8, 2019.

[129] A. Wonfor, J. Dynes, R. Kumar, H. Qin, W. Tam, A. Plews, A. Sharpe, M. Lucamarini, Z. Yuan, R. Penty, *et al.*, "High performance field trials of qkd over a metropolitan network," *Quantum cryptography (QCrypt)*, 2017.

[130] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, *et al.*, "Integrating quantum key distribution with classical communications in backbone fiber network," *Optics express*, vol. 26, no. 5, pp. 6010–6020, 2018.

[131] L. Ma, O. Slattery, and X. Tang, "Single photon frequency up-conversion and its applications," *Physics reports*, vol. 521, no. 2, pp. 69–94, 2012.

[132] P. Kumar, "Quantum frequency conversion," *Optics letters*, vol. 15, no. 24, pp. 1476–1478, 1990.

[133] J. S. Pelc, L. Ma, C. Phillips, Q. Zhang, C. Langrock, O. Slattery, X. Tang, and M. M. Fejer, "Long-wavelength-pumped upconversion single-photon detector at 1550 nm: performance and noise analysis," *Optics express*, vol. 19, no. 22, pp. 21445–21456, 2011.

[134] S. M. Friis and L. Høgstedt, "Upconversion-based mid-infrared spectrometer using intra-cavity LiNbO 3 crystals with chirped poling structure," *Optics letters*, vol. 44, no. 17, pp. 4231–4234, 2019.

[135] G.-L. Shentu, J. S. Pelc, X.-D. Wang, Q.-C. Sun, M.-Y. Zheng, M. Fejer, Q. Zhang, and J.-W. Pan, "Ultralow noise up-conversion detector and spec-

trometer for the telecom band," *Optics express*, vol. 21, no. 12, pp. 13986–13991, 2013.

[136] F. Ma, L.-Y. Liang, J.-P. Chen, Y. Gao, M.-Y. Zheng, X.-P. Xie, H. Liu, Q. Zhang, and J.-W. Pan, "Upconversion single-photon detectors based on integrated periodically poled lithium niobate waveguides," *JOSA B*, vol. 35, no. 9, pp. 2096–2101, 2018.

[137] N. Yao, Q. Yao, X.-P. Xie, Y. Liu, P. Xu, W. Fang, M.-Y. Zheng, J. Fan, Q. Zhang, L. Tong, *et al.*, "Optimizing up-conversion single-photon detectors for quantum key distribution," *Optics Express*, vol. 28, no. 17, pp. 25123–25133, 2020.

[138] "First intergovernmental quantum communication." `www.units.it/en/news/first-intergovernmental-quantum-communication`, 2021. University of Trieste [Online press release; accessed on October 2021].