A simulator of optical coherent-state evolution in quantum key distribution systems

Optical and Quantum Electronics (2022) 54:689
https://doi.org/10.1007/s11082-022-04041-8

A simulator of optical coherent-state evolution in quantum key distribution systems

Carlo Caputo[1] · Mario Simoni[1] · Giovanni Amedeo Cirillo[1] · Giovanna Turvani[1] · Maurizio Zamboni[1]

Received: 22 November 2021 / Accepted: 19 July 2022

Abstract
Quantum key distribution (QKD) is believed to represent a viable solution to achieve theoretically unconditionally secure key generation. However, the available optical systems for experimental QKD, based on photon transmission, are flawed by non-idealities that ultimately limit the achievable performance. Classical simulation of the optical hardware employed in these systems may take on a determining role in engineering future QKD networks. In this article, attempts for developing a QKD simulator based on low-computational-cost models of the employed hardware are presented. In particular, the simulation infrastructure targets polarization-based QKD setups with faint laser sources, whose behaviour can be described by semiclassical coherent states and Mean Photon Number (MPN) per beam. The effects of passive optical components on the photonic qubit evolution are described by Jones matrices, whose coefficients, for some commercial devices, are stored in an *ad-hoc* library. Realistic eavesdropping attacks and non-idealities, such as optical losses, fibre attenuation, polarization misalignment and limited efficiency of single-photon detectors, are also taken into account. The infrastructure allows the user to describe the desired QKD configuration and it provides in output the MPN at the receiver and two fiducial performance parameters: Quantum Bit Error Rate (QBER) and secure key rate. The comparison of the simulation results with experimental data in the state-of-the-art literature highlights that this work is a step forward towards the definition of compact models for the hardware-dependent simulation of quantum-assisted communication networks.

Keywords Quantum-assisted communication · Quantum key distribution · Simulation · Faint lasers · Coherent states · Polarization · Quantum information

✉ Mario Simoni
mario.simoni@polito.it

✉ Giovanna Turvani
giovanna.turvani@polito.it

Extended author information available on the last page of the article

Published online: 13 September 2022

1 Introduction

Cybersecurity is a fundamental part of our life: all of our personal information are online, banks handle our money, which has become mostly digital. Even our memories and knowledge are entrusted to the network. For these reasons, cryptography and cryptosystems, the pillar of cybersecurity, must evolve to deal with the latest decryption methods, thus ensuring that private information or messages cannot be read by third parties. Two kinds of cryptosystems are mainly consolidated:

1. Symmetric, where the same private key is used for encryption and decryption;
2. Asymmetric, where a *public key* and a *private key* are used to encrypt and decrypt a message respectively.

A consolidated cryptosystem is the asymmetric Rivest-Shamir-Adleman (RSA) (Rivest et al. 1978), based on the prime numbers factoring of large numbers, from 2048 bits onwards, an operation that is extremely hard for classical computers. However, more powerful traditional computers and algorithms executable on quantum computers may put at risk most of these cryptography methods in a couple of decades, or even less. The Shor's algorithm (Shor 1994) is the most famous example of such a kind of algorithm: it is capable to factorise an integer number in its prime factors in polynomial time, thus making ciphers breaking extremely efficient (Djordjevic and Zhang 2004). The upcoming possibility of running Shor's algorithm on many-qubit quantum computers is expected to jeopardise asymmetric cryptography algorithms. For this reason, the exchange of secure data in the quantum era will require the adoption of post-quantum (Bernstein and Lange 2017) algorithms, computationally hard for quantum computers, or symmetric cryptography, which shifts the security requirements from the algorithm to the distribution of private keys.

Quantum mechanics can help in distributing keys which are, from a theoretical point of view, unconditionally secure. In fact, the superposition principle, the no-cloning theorem (Wootters and Zurek 1982) and the entanglement can be exploited for generating keys extremely hard to be detected. All quantum-based methods for key generation belong to Quantum Key Distribution (QKD) (Renner 2008; Gisin et al. 2002). The most consolidated QKD protocol is the one proposed by Charles Bennet and Gilles Blassard in 1984 (BB84) (Bennett and Brassard 1984), characterised by the absence of entanglement requirement, thus practically simplifying the implementation. Figure 1 shows the ideal protocol, without any eavesdropper, generating the key `1011`. Information is encoded on the polarization of single photons, which substantially behaves as a qubit, and two users, Alice and Bob, exploit two non-orthogonal bases—one associated with horizontal and vertical polarizations (H/V), the other with those diagonal and anti-diagonal (D/A)—to transmit and receive photons sequentially. Alice randomly chooses the transmission basis for each photon to be sent to Bob through the quantum channel, while Bob measures in an arbitrarily chosen basis, too. According to the quantum uncertainty principle for qubit measurements, Bob would know exactly the polarization of the photon transmitted by Alice only if he chose the same basis of hers. After repeating the protocol multiple times, Alice and Bob compare on a classical channel the bases at each iteration, without declaring the values. This operation is ideally sufficient for both Alice and Bob to get the value of each key bit, because—considering what already said about uncertainty principle for measurements—the choice of the same basis for transmission and detection ensures to Bob the recognition of the bit transmitted by Alice.

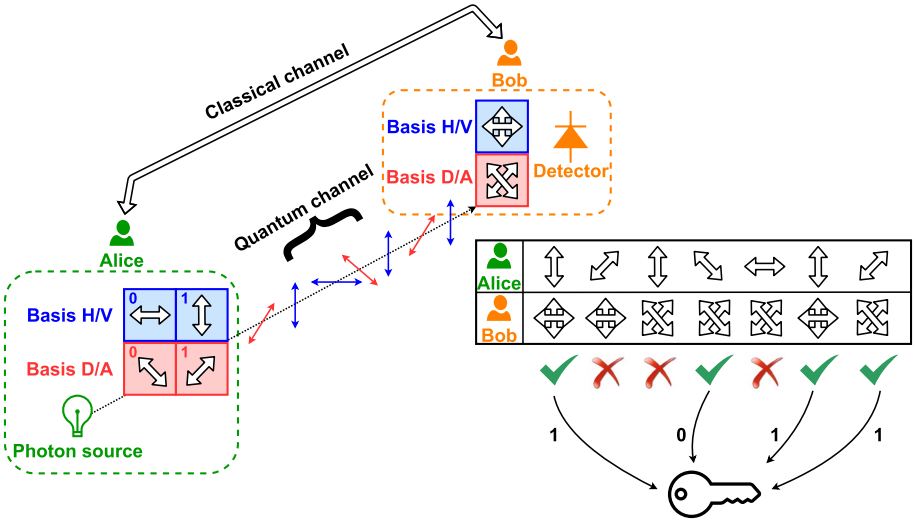

Fig. 1 Schematic representation of BB84 protocol

In general, QKD requires single-photon generation, manipulation, transmission and detection, in particular polarization manipulation with passive optical components. Apart from the possibility of having an eavesdropper on the quantum channel, ideal conditions for implementing the protocol in a practical scenario cannot be easily achieved, because of the limitations of real hardware. For example, single-photon sources are not nowadays highly reliable (Lounis and Orrit 2005) and they must be necessarily approximated. A consolidated approach is exploiting **faint lasers** (Al-Kathiri et al. 2008; Molotkov and Potapova 2016). As observable in Fig. 2, coherent light emitted by a pulsed laser can be seen as a packet of photons; each packet tries to overcome an attenuator, sufficiently opaque to force an output packet with at most one photon. Unfortunately, this is not a high-quality single-photon source, since the number of photons in a packet is probabilistic and described by a **descending Poissonian probability distribution** with mean value lower than 1, thus implying non-null probabilities of emitting no photons or more than one photon. In addition to the difficulties in generating single photons, other non-ideality phenomena—such as the losses of passive optical components

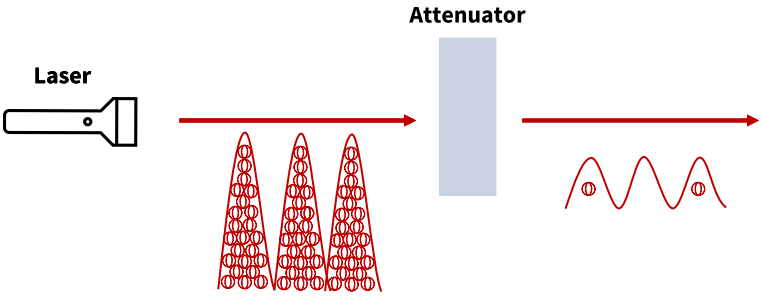

Fig. 2 Schematic representation of a faint laser

for manipulating polarization, undetection of photon detectors and optical fibre attenuation and polarization misalignment—induce further deviations from ideality.

Even though the performance of real hardware for quantum and quantum-assisted communication is generally limited, frameworks for developing applications are already available. In particular, simulators, allowing users to develop applications and protocols for quantum networks and quantum internet, are developed by academic research teams. Among them, it is important to remind (Coopmans et al. 2021) and (Dahlberg and Wehner 2018) from TU Delft, (Diadamo et al. 2021) from Technische Universität München, the Quantum Internet Simulation Package (QUISP) (Matsuo et al. 2020) from Keio University and the Simulator for Quantum Networks and Channels (`SQUANCH`) (Bartlett 2018) from Stanford University. These infrastructures permit to design and evaluate the performance of quantum and quantum-assisted communication in a protocol scenario. Moreover, some of these, e.g. NetSquid and `SQUANCH`, also introduce qubit errors and noisy channels, but in a hardware-independent scenario, where all the non-idealities are considered as abstract operators affecting qubits.

The research described in this article tries to respond to the need of integrating hardware non-idealities in a simulation scenario, to evaluate the effects of real available infrastructures on the performance of a protocol. In particular, considering that currently available QKD and quantum network systems are mainly based on coherent light manipulation—such as the ones proposed in Allati and Baz (2015), Allati et al. (2011) and Lütkenhaus (2000)—a **preliminary coherent state-based simulator of BB84 QKD systems**, consisting of faint lasers and non-ideal optical devices, is here presented, with the whole mathematical formalism for simulation and reliability estimation of the protocol. The simulation methodology is substantially the same adopted for quantum computing technologies in Simoni et al. (2022), Cirillo et al. (2019) and Cirillo et al. (2020)—where the performance of a quantum computer were evaluated depending on degrees of freedom related to the control and physical parameters of hardware affecting qubits—and it has been implemented in MATLAB environment. It is important to repeat that this work is currently focusing on hardware non-idealities, so only experimentally plausible eavesdropper attacks are taken into account.

A **theoretical overview** of the quantum-mechanical description of coherent light emitted by faint lasers and **of the polarization manipulation** in terms of Jones calculus is reported in Sect. 2, as well as a description of the fundamental **data structure** of the simulator itself. Section 3 and Sect. 4 describe the **non-ideal optical devices and channels** required for the BB84 protocol, according to the notation of the simulator. Section 5 details the **simulation of a BB84 setup** described in the state of the art, proving that the results obtained with the simulator are compatible with the experimental ones. Moreover, in order to prove the capability of the simulator of handling many physical degrees of freedom, the simulation results with different single-photon detectors and optical fibre lengths are provided and compared. Section 6 discusses the behaviour of the simulator in presence of **beam splitter attack** (Sect. 6.1) and **polarization misalignment** effects (Sect. 6.2). Finally, future perspectives are discussed in Sect. 7.

2 Theoretical foundations

The optical simulator is based on the use of **coherent states** that fit very well with the description of the coherent light emitted by attenuated lasers, the light source most employed in current QKD systems. A generic coherent state is defined by the complex number α, which is associated with the mean photon number in the pulse μ through the

relation $\mu = |\alpha|^2$ (Gazeau 2009). Equivalently, α is linked to the electric field amplitude of the electromagnetic wave. Moreover, α uniquely locates the coherent state in the optical phase space; in practice, the length of the phasor that represents the state is equal to $|\alpha|$ (Fox 2006).

A coherent state can be represented as a **sum of Fock states**, the so-called standard form, or using the displacement operator $\hat{D}(\alpha)$ acting on the vacuum state $|0\rangle$ (Rosas-Ortiz 2019):

$$\begin{aligned} |\alpha\rangle &= e^{-\frac{\alpha^2}{2}} \sum_{n=0}^{+\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \\ &= e^{\alpha\hat{a}^\dagger - \alpha^* \hat{a}} |0\rangle = \hat{D}(\alpha)|0\rangle. \end{aligned} \tag{1}$$

Thanks to this last representation, it is possible to propagate the initial state across every component of the system modifying the displacement operator or, in other words, the creation and annihilation operators contained in it.

Furthermore, with this representation, it is possible to take in consideration more than one optical path, a convenient feature when studying complex optical systems. This can be done by involving more subspaces of the Fock space, one per each path. For example, an m-mode Fock space can be written by combining the subspaces in $|n_1, n_2, \ldots, n_m\rangle$.

Another widely used characteristic of the displacement operator is that it can also take in account the polarization of the coherent state (Kučera 2007; C 2011) by considering a two-mode polarization Fock space, with the subspaces associated with the number of photons in horizontal and vertical polarization state $|n_H, n_V\rangle$. For example, a coherent light pulse diagonally polarized, oriented at + 45° from the horizontal axis, can be expressed as (Maitra and Das 2019):

$$\begin{aligned} |\alpha_{+45}\rangle &= \hat{D}(\alpha_{+45^\circ})|0_H, 0_V\rangle \\ &= \exp\left(\frac{\alpha}{\sqrt{2}}(\hat{a}_H^\dagger + \hat{a}_V^\dagger) - \frac{\alpha^*}{\sqrt{2}}(\hat{a}_H + \hat{a}_V)\right)|0_H, 0_V\rangle, \end{aligned} \tag{2}$$

where $\hat{a}_H^{(\dagger)}$ and $\hat{a}_V^{(\dagger)}$ are the annihilation (creation) operators for horizontally and vertically polarized photons, and $|0_H, 0_V\rangle$ is the vacuum state in the two-mode polarization Fock space (Vintskevich et al. 2020).

In general, modifying the creation and annihilation operators contained in $\hat{D}$ for horizontal and vertical components, it is possible to describe the evolution of the coherent state across a generic optical structure, and, consequently, to develop the proposed simulator.

2.1 Propagation in quantum optics

In classical optics, fully polarized light can be described with **Jones calculus**. The light beam is described by a two dimensional Jones vector, which contains the complex components of the electric field phasor (Jones 1942):

$$\begin{pmatrix} |E_x|\, e^{i\phi_x} \\ |E_y|\, e^{i\phi_y} \end{pmatrix}, \tag{3}$$

where the reference system is chosen to align the electric field polarization with the x-y plane (transverse to the direction of the wave vector). In order to determine the evolution of light along an optical path, this vector is multiplied by the Jones matrix associated with the optical device where the light passes through.

Thanks to **canonical quantization**, the equations that describe the evolution of creation and annihilation operators are identical to those of the classical complex amplitudes of the electric field in Jones calculus (Bachor and Ralph 2019; Kučera 2007; Maitra and Das 2019; Prasad et al. 1987). In fact, if an optical component is described by a Jones matrix $J_{component}$, such that its action on the Jones vector is:

$$\begin{pmatrix} E_x^{out} \\ E_y^{out} \end{pmatrix} = J_{component} \begin{pmatrix} E_x^{in} \\ E_y^{in} \end{pmatrix}, \tag{4}$$

it is possible to obtain the quantum description of the component passing to creation (or similarly annihilation) operators:

$$\begin{pmatrix} \hat{a}_H^{out} \\ \hat{a}_V^{out} \end{pmatrix} = J_{component} \begin{pmatrix} \hat{a}_H^{in} \\ \hat{a}_V^{in} \end{pmatrix}. \tag{5}$$

Therefore, a coherent state can be represented as a bi-dimensional vector, analogous of the classical Jones vector, whose components are the coefficients for horizontal and vertical creation operators in the displaced vacuum state representation. They are nothing more than the eigenvalues of the annihilation operators. For example, the state $|\alpha_{+45^\circ}\rangle$ can be written as:

$$\begin{pmatrix} \frac{\alpha}{\sqrt{2}} \\ \frac{\alpha}{\sqrt{2}} \end{pmatrix}, \tag{6}$$

where the two coefficients correspond to those in Eq. 2 for $\hat{a}_H^\dagger$ and $\hat{a}_V^\dagger$.

Then, using the Jones matrix of each component, the state can be propagated through the optical system, and one can obtain the mean photon number, or, equivalently, the electric field intensity in every point of the system. The proposed simulator exploits this vector-based approach since it allows one to evaluate the evolution of information on an optical setup, as shown in Sect. 5.2, taking into account most of the non-ideal phenomena affecting optical devices (as discussed in Sects. 2.2 and 4) and looking for a compromise between computational complexity and physical accuracy. In particular, this approach is expected to reasonably estimate the evolution of coherent state along the whole system, with a total CPU time lower than the corresponding one required for solving density matrix-based master equations.

As an example, the effect of a linear polarizer with horizontal transmission axis on $|\alpha_{+45^\circ}\rangle$ will be Fowles (1989):

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{\alpha}{\sqrt{2}} \\ \frac{\alpha}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{\alpha}{\sqrt{2}} \\ 0 \end{pmatrix}. \tag{7}$$

So, basically, only half of the input photons will be transmitted, and the output state will be completely horizontally polarized.

As aforementioned, this model can also be extended to **multi-mode systems**. In fact, in the context of this simulator, it is important to take into account not only the polarization,

but also the photons paths. This is fundamental in order to consider two-input and two-output optical devices, such as beam splitters. For example, the input state of a beam splitter, given by the coherent light states at the two input ports of the device, can be represented by a four-dimensional vector. This is obtained by the combination of the two-dimensional vectors associated with the polarization in each input path:

$$V = \begin{pmatrix} V_1 \\ V_2 \end{pmatrix} = \begin{pmatrix} \alpha_{H_1} \\ \alpha_{V_1} \\ \alpha_{H_2} \\ \alpha_{V_2} \end{pmatrix}, \tag{8}$$

where $\alpha_{\{H,V\}_k}$ are the eigenvalues of horizontal and vertical annihilation operators in path k.

In this context, "expanded" 4×4 Jones matrices will be involved and the evolution of the states will be written as:

$$\begin{pmatrix} \alpha^{out}_{H_1} \\ \alpha^{out}_{V_1} \\ \alpha^{out}_{H_2} \\ \alpha^{out}_{V_2} \end{pmatrix} = M \begin{pmatrix} \alpha^{in}_{H_1} \\ \alpha^{in}_{V_1} \\ \alpha^{in}_{H_2} \\ \alpha^{in}_{V_2} \end{pmatrix}, \tag{9}$$

As an example, the propagation through a polarizing beam splitter (PBS) is considered. For simplicity, assuming an ideal PBS that completely splits the incoming light in two separate polarized beams, the quantum-mechanical relations are (Maitra and Das 2019; Nagata et al. 2010):

$$\begin{cases} \hat{a}_H = \hat{c}_H \\ \hat{a}_V = \hat{d}_V \\ \hat{b}_H = \hat{d}_H \\ \hat{b}_V = \hat{c}_V \end{cases} \tag{10}$$

where the nomenclature for ports is reported in Fig. 3. If an antidiagonal state enters in the "a" port of a beam splitter, while the other port "b" is left unused, the input state for the beam splitter is:

$$|\alpha\rangle_a \, |0\rangle_b = \exp\left(\frac{\alpha}{\sqrt{2}} (\hat{a}^\dagger_H - \hat{a}^\dagger_V) - \frac{\alpha^*}{\sqrt{2}} (\hat{a}_H - \hat{a}_V) \right)_a |0\rangle_a |0\rangle_b, \tag{11}$$

where the vacuum state $|0_H, 0_V\rangle$ is represented only with $|0\rangle$ to lighten the notation, and the subscripts a and b indicate the input ports. The associated input vectors are:

$$V_a = \frac{\alpha}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \quad V_b = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{12}$$

From Eq. 10, one can obtain the output states:

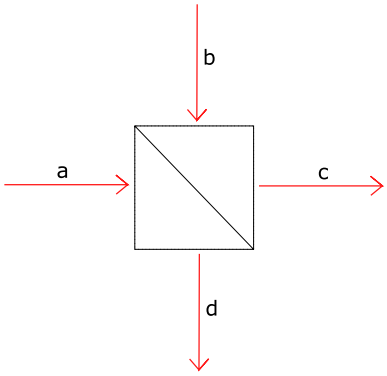

Fig. 3 Naming convention for beam splitter ports

$$
\begin{aligned}
|\beta\rangle_c|\beta\rangle_d = & \exp\left(\frac{\alpha}{\sqrt{2}}\left(\hat{c}_H^\dagger\right) - \frac{\alpha^*}{\sqrt{2}}\left(\hat{c}_H\right)\right)_c \\
& \cdot \exp\left(-\frac{\alpha}{\sqrt{2}}\left(\hat{d}_V^\dagger\right) + \frac{\alpha^*}{\sqrt{2}}\left(\hat{d}_V\right)\right)_d \\
& |0\rangle_c\,|0\rangle_d\,,
\end{aligned}
\tag{13}
$$

Correspondingly, the matrix relation for the PBS (which will be thoroughly presented in Sect. 3.3) permits to obtain the output associated vectors. In the ideal case it results:

$$
\begin{aligned}
\begin{pmatrix} V_c \\ V_d \end{pmatrix} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} V_a \\ V_b \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{\alpha}{\sqrt{2}} \\ -\frac{\alpha}{\sqrt{2}} \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{\alpha}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{\alpha}{\sqrt{2}} \end{pmatrix}
\end{aligned}
\tag{14}
$$

andso:

$$
V_c = \frac{\alpha}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad V_d = -\frac{\alpha}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{15}
$$

These vectors correctly represent the output states reported in Eq. 13, as expected.

2.2 Losses treatment

In general, to consider losses, relations between input and output operators must be modified introducing the **Langevin operators** $\hat{F}$, also called noise operators (Barnett et al. 1998). However, in the case of coherent states, the treatment of losses can be simplified. In fact, passing through linear components, coherent states remain coherent states (Bachor and Ralph 2019). Hence, the input and output relations for creation (or annihilation)

operators are the same of the ideal case, but the reflection and transmission coefficients have a reduced amplitude due to losses, in order to take in account energy dissipation (Barnett et al. 1998).

3 Quantum mechanical relations

After having described the foundations of the theoretical approach, in this section the quantum mechanical relations for the **most used optical components** will be presented. It is important to precise that the components are described by taking into account the minimum number of modes that permits their description. Hence, devices as waveplates, working on single photon paths, are described in terms of their effect on a single photon path with two polarizations.

3.1 Light source

The light emitted by a coherent light source, such as an attenuated laser, can be represented as a coherent state whose alpha factor is equal to the square root of the mean photon number μ contained in the light pulse:

$$|\alpha| = \sqrt{\mu}\,. \tag{16}$$

For example, if the laser produces a light pulse vertically polarized with a mean photon number equal to two, the coefficient of the coherent state will be $\alpha = \sqrt{2}$. Formally, the state is:

$$\begin{aligned} |\Psi\rangle &= D(\alpha_V = \sqrt{2})\,|0\rangle \\ &= \exp\left(\sqrt{2}\left(\hat{a}_V^{\dagger}\right) - \sqrt{2}(\hat{a}_V)\right)|0\rangle \end{aligned} \tag{17}$$

while its vectorial representation is:

$$V = \begin{pmatrix} 0 \\ \sqrt{2} \end{pmatrix} \tag{18}$$

3.2 Waveplates and Pockels cells

Pockels cells (Fig. 4) are voltage controlled waveplates, widely used in QKD systems both for modifying the logical value of the qubit in polarization-encoding systems and for compensating for unwanted polarization deviations. Waveplates and Pockels cells are made of birefringent crystals in which the refractive index depends on polarization and propagation direction of light (Kemp 1969). They are characterized by two axes: ordinary, with refractive index n_0, and extraordinary, with refractive index n_e. As a result, one component of the polarization is retarded with respect to the other; for this reason these types of components are generically called retarders. The effect of the waveplate depends on this retardation and also on the input polarization. The retardation describes the phase shift between the two polarization components, which is given by the following expression:

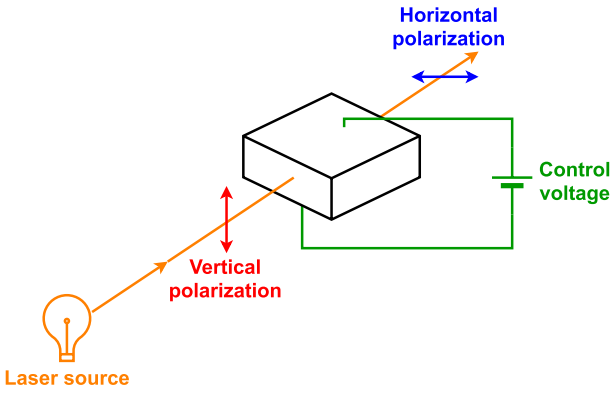

Fig. 4 Schematic representation of Pockels cell changing polarization from vertical to horizontal

$$\theta = \frac{2\pi}{\lambda_0} d\,|n_0 - n_e|, \tag{19}$$

where λ_0 is the wavelength in vacuum, d is the thickness of the plate, and n_0 and n_e the refractive indexes for light polarized along ordinary and extraordinary axis respectively (Hecht 2002).

Waveplates are classified according to their retardation: **half-waveplates** have $\theta = \pi$ and they rotate the polarization of linearly polarized light (most of the Pockels cells used in QKD systems belong to this category); **quarter-waveplates** have $\theta = \frac{\pi}{2}$ and linearly polarized light oriented at 45° from the fast axis comes out circularly polarized. Similarly, incoming circularly polarized light comes out linearly polarized (Hecht 2002).

As mentioned above, the effect of the retarder depends also on its orientation. Calling δ the orientation of the extraordinary axis (also called fast axis) with respect to the vertical axis, the Jones matrix associated with the retarder is:

$$J_{ret(\theta,\delta)} = \sqrt{t}\begin{pmatrix} \cos^2(\delta) + \sin^2(\delta)e^{-i\theta} & \cos(\delta)\sin(\delta)\left[1 - e^{-i\theta}\right] \\ \cos(\delta)\sin(\delta)\left[1 - e^{-i\theta}\right] & \sin^2(\delta) + \cos^2(\delta)e^{-i\theta} \end{pmatrix}, \tag{20}$$

where t is the transmittance of the retarder, under square root because it is usually related to the transmitted optical power. So, the effect of the retarder is modeled as follows:

$$\begin{pmatrix} \alpha_{H_b} \\ \alpha_{V_b} \end{pmatrix} = J_{ret(\theta,\delta)} \begin{pmatrix} \alpha_{H_a} \\ \alpha_{V_a} \end{pmatrix}, \tag{21}$$

where a and b label the input and output ports of the component. As already mentioned, half-wave Pockels cells are used in QKD systems to vary the photon polarization and consequently the quantum information, changing the qubit value or the encoding basis. Some examples are reported in the following for $t = 1$. A Pockels cell oriented at 45° with respect to the vertical axis can be used to flip the qubit in {H, V} basis, in fact:

$$J_{ret(\pi,\frac{\pi}{4})} \begin{pmatrix} \alpha \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha \end{pmatrix}. \tag{22}$$

On the other hand, a Pockels cell oriented at **22.5**° with respect to the vertical axis can be employed to pass from {H, V} to {A, D} basis:

$$J_{ret(\pi,\frac{\pi}{8})}\begin{pmatrix}\alpha\\0\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}\alpha\\0\end{pmatrix}=\begin{pmatrix}\frac{\alpha}{\sqrt{2}}\\\frac{\alpha}{\sqrt{2}}\end{pmatrix}, \tag{23}$$

in fact the horizontally polarized state becomes diagonally polarized.

Finally, it is possible to prove that the combination of multiple J_{ret} matrices permits to describe a generic rotation of the photon polarization state depending on three angles θ_{U3}, ϕ_{U3} and λ_{U3}:

$$\begin{aligned}J_{ret(-\phi_{U3},0)}J_{ret\left(\pi,\frac{\theta_{U3}}{4}\right)}J_{ret(\pi-\lambda_{U3},0)}&\\=\begin{pmatrix}\cos\left(\frac{\theta_{U3}}{2}\right)&-\sin\left(\frac{\theta_{U3}}{2}\right)e^{i\lambda_{U3}}\\\sin\left(\frac{\theta_{U3}}{2}\right)e^{i\phi_{U3}}&\cos\left(\frac{\theta_{U3}}{2}\right)e^{i(\phi_{U3}+\lambda_{U3})}\end{pmatrix}&\\=J_{ret}^{comb}(\theta_{U3},\phi_{U3},\lambda_{U3}),&\end{aligned} \tag{24}$$

where the suffix of the three angles refers to the fact that the obtained matrix J_{ret}^{comb} corresponds to the $U3$ available in the Qiskit quantum information framework (Abraham 2019) for the arbitrary rotation of single qubits.

3.3 Beam splitters

Non-polarizing beam splitters (BS) and polarizing beam splitters (PBS) are essential components in optical experiments, as also in QKD systems. For example, BS are used to join in a single optical path light beams coming from different sources and, in the detection sub-systems, to randomly select photons and consequently the measurement basis (Bachor and Ralph 2019). PBS are practically always present in the detection units, in front of the detectors, in order to split light in its horizontally and vertically polarized components (Mailloux et al. 2015), or, better to say, in its Transverse Electric (TE) and Transverse Magnetic (TM) modes.

The non-trivial derivation of the quantum mechanical relation for the beam splitters should start considering that, in order to respect energy conservation, creation and annihilation operators must respect the well-known commutators (Gerry and Knight 2004; Loudon 2000):

$$\begin{aligned}\left[\hat{a}_i,\hat{a}_j^\dagger\right]&=\delta_{i,j}\\\left[\hat{a}_i,\hat{a}_j\right]&=0\\\left[\hat{a}_i^\dagger,\hat{a}_j^\dagger\right]&=0,\end{aligned} \tag{25}$$

where i and j label the ports of the component. It is worth recalling that these relations are valid for all optical components, not only for beam splitters. Combining the Jones vectors of inputs and outputs in four dimensional vectors and defining an "expanded" 4×4 Jones matrix for the beam splitter, the quantum mechanical relation results to be:

$$\begin{pmatrix}\hat{c}_H\\\hat{c}_V\\\hat{d}_H\\\hat{d}_V\end{pmatrix}=\begin{pmatrix}\sqrt{t_H}&0&i\sqrt{r_H}&0\\0&e^{i\phi}\sqrt{t_V}&0&ie^{i\phi}\sqrt{r_V}\\i\sqrt{r_H}&0&\sqrt{t_H}&0\\0&ie^{i\phi}\sqrt{r_V}&0&e^{i\phi}\sqrt{t_V}\end{pmatrix}\begin{pmatrix}\hat{a}_H\\\hat{a}_V\\\hat{b}_H\\\hat{b}_V\end{pmatrix}, \tag{26}$$

analogous to the expressions shown in Nagata et al. (2010), Weihs (2001). The subscripts a, b, c and d label the ports of the device, as reported in Fig. 3. ϕ is the difference in phase between horizontally and vertically polarized light. t_H, t_V, r_H and r_V are the transmissivities and reflectivities for each polarization component, under square root because they are related to the power of the light beam. This is the most generic beam splitter matrix and it is possible to get the matrices of characteristic beam splitters from it. For example, a 50:50 non-polarizing beam splitter is used to split in two equivalently beams the incoming light, consequently it has all the terms $t_H = t_V = r_H = r_V = \frac{1}{2}$ and ϕ depends on the specific component. On the other hand, the matrix of an ideal PBS, reported in Eq. 10 and in Eq. 14, can be obtained from Eq. 26 with $t_H = r_V = 1$, $t_V = r_H = 0$ and $\phi = -\frac{\pi}{2}$ and it properly describes the splitting of incoming light in its polarization components. Obviously, real PBSs are intrinsically lossy, so $\sqrt{t_H}, \sqrt{r_V} \lesssim 1$ and $\sqrt{r_H}, \sqrt{t_V} \gtrsim 0$.

4 Quantum channels

The quantum channel is the link between transmitter and receiver that allows one to exchange the qubits, i.e. the properly encoded photons. The two most used solutions are **optical fibers** and **open air**, both with advantages and disadvantages.

The usage of optical fiber as quantum channel has several advantages; it has a low and pretty constant attenuation, slightly dependent on temperature and mechanical vibrations. It also allows one to establish quantum communication systems where an infrastructure already exists.

In the current implementation of the channel model, two main phenomena affecting the photons transmission are taken into account. The first one is **polarization misalignment**, consisting, at quantum mechanical level, in random variations of photons polarization state due to external perturbations on the optical fiber, such as mechanical stresses (bending and twisting) or thermal expansion and contraction.

The model for polarization misalignment in the current version of the simulator is substantially inherited from Xu et al. (2013) and Higgins et al. (2020), where the phenomenon is described in terms of aleatory unitary rotations of the polarization state by an angle $\tilde{\xi}$. In the simulator described in this article, a combination of J_{ret} matrices—responsible of changing α_H and α_V of the input beam—are exploited for the description of misalignment. The input and output ports of the equivalent Pockels cell are related according to the following relation:

$$\begin{pmatrix} \alpha_{H_b} \\ \alpha_{V_b} \end{pmatrix} = J_{ret\left(\pi, \frac{\tilde{\xi}}{2}\right)} J_{ret(\pi,0)} \begin{pmatrix} \alpha_{H_a} \\ \alpha_{V_a} \end{pmatrix}, \tag{27}$$

where $\delta = \frac{\tilde{\xi}}{2}$ describes the random rotations and its value depends on the characteristics of the simulated optical fiber. Those two J_{ret} matrices were chosen to obtain exactly the same matrix for polarization misalignment reported in Xu et al. (2013). In addition to polarization misalignment, **light beam intensity attenuation** along the channel is also taken into account. This phenomenon can be quantum-mechanically described in terms of a reduction of α, thus of the mean numbers of horizontally and vertically-polarized photons:

$$\begin{pmatrix} \alpha_{H_b} \\ \alpha_{V_b} \end{pmatrix} = 10^{-\frac{\sigma_{\text{dB, fibre}} \cdot \text{length}}{20}} \begin{pmatrix} \alpha_{H_a} \\ \alpha_{V_a} \end{pmatrix}, \tag{28}$$

where a and b label input and output ports respectively, and $\sigma_{\text{dB, fibre}}$ is the attenuation of the fiber in dB. The attenuation depends on the communication wavelength; typical values of attenuation are 0.34 dB/km at 1310 nm and 0.19 dB/km at 1550 nm (Corning 2005).

Attenuation of open air quantum channel, employed in quantum-based satellite communication (Liao et al. 2017), can also be evaluated with the same expression reported in Eq. 28. A feature of this channel is that polarization noise is practically absent (Elser et al. 2009), thus implying that open air can be exploited for QKD protocols encoding information onto photon polarization. It is important to remind that $\sigma_{\text{dB, air}}$ is often higher than $\sigma_{\text{dB, fibre}}$ and that at sea level, it tends to fluctuate because of atmospheric conditions and pollution (Kim et al. 2001).

5 System analysis

In order to validate the proposed simulative methodology, the QKD system presented in Wang et al. (2017) will be analysed. It is a **polarization-encoding BB84 system**, where classical and quantum channels coincide in the same optical fiber. The quantum communication sub-system is shown in Fig. 5; the optical paths are labelled in red. Alice's transmitter contains four lasers that, in association with two polarizing beam splitters and a polarization controller (a voltage controlled retarder), generate the four non-orthogonal polarization states. From the top two (labelled A and B) horizontally and vertically polarized photons are generated, while, from the lower two (C and D), coupled with a polarization controller, diagonally and anti-diagonally polarized photons are produced. These two optical paths (1 and 2) are joined in path 3 using a beam splitter. At the end of Alice's subsystem, a Variable Optical Attenuator (VOA) is used to reduce the signal intensity down to quasi single-photon level. In this setup, **decoy state** method is employed to increase the communication security; Alice sends signal states in the 75% of cases whose Mean Photon Number (MPN) is 0.6, weak decoy states in the 12.5% of cases whose MPN is 0.2, and vacuum states in the remaining 12.5% of cases.

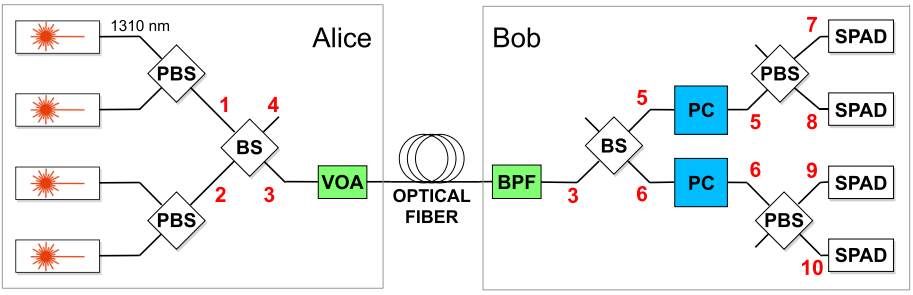

Fig. 5 Schematic of the quantum communication subsystem (Wang et al. 2017). The four lasers, in combination with the polarizing beam splitters (PBS) and a polarization controller (PC), generate one of the four non-orthogonal states (qubit) at a time. The first two light paths (labeled with 1 and 2, in red) are combined using a beam splitter (BS). Then, the light pulse is attenuated down to signal state or weak decoy state through a variable optical attenuator (VOA) and sent to Bob through an optical fiber. At the beginning of Bob's receiver a band pass filter (BPF) is used to filter out the Raman noise. Then, a BS splits the incoming photons in order to select the measurement basis. The other two polarization controllers are used to compensate alterations in the SOP caused by the fiber and, the lower one, also to rotate the light polarization of 45° in order to measure in $\{A, D\}$ basis. The PBSs, in combination with the single-photon avalanche diodes (SPAD), form the effective measurement units

Alice and Bob are connected through an optical fiber, as aforesaid. It has an attenuation equal to 0.33 dB/km at 1310 nm, the quantum communication wavelength used in this system.

At the beginning of Bob's receiver, a 100 GHz bandpass filter centered at 1310 nm is present in order to suppress the noise added by the classical communication, mainly due to Raman scattering. Then a beam splitter is used to randomly select the measurement basis: photons directed in path 5 towards the upper PBS are measured in {H, V} basis; conversely, photons directed in path 6 first pass in a polarization controller that rotates their polarization of 45° and then in the PBS to be measured in {A, D} basis. A polarization controller is present also in path 4 in order to compensate unwanted deviations in the SOP, mainly caused by the optical fiber (polarization misalignment), which are here neglected. It is reminded here that another simulation, reported and commented in Sect. 6.2, takes into account this non-ideality phenomenon. The last element of Bob's sub-system is made by the single-photon detectors, in this case Single-Photon Avalanche Diodes (SPAD). They are a fundamental part of the QKD system because their performance strongly influences the secure key rate and the quantum bit error rate.

5.1 Example of qubit propagation across the system

Employing the formalism presented in Sect. 2, here the propagation of a qubit from Alice's laser to Bob's detector is calculated. It is a concrete example of the simulative methodology, where ideal components will be considered in order to simplify the understanding. Obviously, in MATLAB, the real parameters of the system components will be used in order to evaluate the Quantum Bit Error Rate (QBER) and the secure key rate.

Assuming ideal optical components, α_{L} is the alpha parameter (Eq. 16) for the coherent light emitted by the lasers, while α_{A} is the parameter after the attenuation of the VOA.

The encoding scheme used in these types of systems is the following one: binary "1" corresponds to vertical or diagonal photons, while binary "0" corresponds to horizontal or anti-diagonal photons.

Assuming that Alice wants to send a "1" in the {H, V} basis, she activates laser B, taking the other 3 lasers deactivated. Consequently, after the PBS, the state in path 1 is:

$$|p_1\rangle = \exp\left(\alpha_{\mathrm{L}}\left(\hat{a}_V^{\dagger}\right) - \alpha_{\mathrm{L}}^{*}\left(\hat{a}_V\right)\right)|0\rangle, \tag{29}$$

and its associated vector is:

$$V_1 = \begin{pmatrix} 0 \\ \alpha_{\mathrm{L}} \end{pmatrix}. \tag{30}$$

Instead, in path 2 there is the vacuum state, so the global state is:

$$|p_1\rangle\,|p_2\rangle = \exp\left(\alpha_{\mathrm{L}}\left(\hat{a}_V^{\dagger}\right) - \alpha_{\mathrm{L}}^{*}\left(\hat{a}_V\right)\right)_1 |0\rangle_1 |0\rangle_2. \tag{31}$$

Light from path 1 and path 2 is combined using a 50:50 BS. Using Eq. 26 with $\phi = 0$ and $t_H = t_V = r_H = r_V = \frac{1}{2}$, one obtains that the output state is:

$$
\begin{aligned}
|p_3\rangle\,|p_4\rangle = \exp&\left(\frac{\alpha_{\mathrm{L}}}{\sqrt{2}}\left(\hat{b}_V^{\dagger}\right) - \frac{\alpha_{\mathrm{L}}^*}{\sqrt{2}}\left(\hat{b}_V\right)\right)_3 \\
&\cdot \exp\left(\frac{i\,\alpha_{\mathrm{L}}}{\sqrt{2}}\left(\hat{c}_V^{\dagger}\right) + \frac{i\,\alpha_{\mathrm{L}}^*}{\sqrt{2}}\left(\hat{c}_V\right)\right)_4 \\
&|0\rangle_3|0\rangle_4,
\end{aligned}
\tag{32}
$$

where $\hat{b}$ and $\hat{c}$ are the operators at the output ports. In the following steps the alphabetical order will be followed. Note that the plus in the displacement operator of path four is a consequence of the complex conjugation of the imaginary unit.

This result is confirmed using the matrix relation employed in the simulator:

$$
\begin{aligned}
\begin{pmatrix} \alpha_{H_3} \\ \alpha_{V_3} \\ \alpha_{H_4} \\ \alpha_{V_4} \end{pmatrix} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & i & 0 \\ 0 & 1 & 0 & i \\ i & 0 & 1 & 0 \\ 0 & i & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ \alpha_L \\ 0 \\ 0 \end{pmatrix} \\
&= \frac{\alpha_L}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 0 \\ i \end{pmatrix},
\end{aligned}
\tag{33}
$$

whose result can be written as follows:

$$
V_3 = \frac{\alpha_{\mathrm{L}}}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad V_4 = \frac{\alpha_{\mathrm{L}}}{\sqrt{2}} \begin{pmatrix} 0 \\ i \end{pmatrix}. \tag{34}
$$

Note that the imaginary unit i as vertical component of vector V_4 is only a phase shift of $\frac{\pi}{2}$.

One of the two output states (4) is discarded, while the other one (3) passes through the VOA to obtain a signal or a decoy state that is sent to Bob:

$$
|p_3\rangle = \exp\left(\alpha_{\mathrm{A}}\left(\hat{d}_V^{\dagger}\right) - \alpha_{\mathrm{A}}^*\left(\hat{d}_V\right)\right)|0\rangle. \tag{35}
$$

After the optical fiber and the Raman filter, which in the ideal case do not affect the state, the light pulse reaches Bob's beam splitter. Obviously, in the simulator, the attenuation of these two components is taken in account using Eq. 28. As aforementioned, this last BS separates the photons in order to select the measurement basis. Following the same approach, one can find that the output states of the BS are:

$$
\begin{aligned}
|p_5\rangle\,|p_6\rangle = \exp&\left(\frac{\alpha_{\mathrm{A}}}{\sqrt{2}}\left(\hat{e}_V^{\dagger}\right) - \frac{\alpha_{\mathrm{A}}^*}{\sqrt{2}}\left(\hat{e}_V\right)\right)_5 \\
&\cdot \exp\left(\frac{i\,\alpha_{\mathrm{A}}}{\sqrt{2}}\left(\hat{f}_V^{\dagger}\right) + \frac{i\,\alpha_{\mathrm{A}}^*}{\sqrt{2}}\left(\hat{f}_V\right)\right)_6 \\
&|0\rangle_5|0\rangle_6,
\end{aligned}
\tag{36}
$$

and equivalently, using the matrix relations, the output vectors are:

$$V_5 = \frac{\alpha_A}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix}, \quad V_6 = \frac{\alpha_A}{\sqrt{2}}\begin{pmatrix}0\\i\end{pmatrix}. \tag{37}$$

Photons that reach path 5 are measured in {H, V} basis. In fact, after having crossed the voltage controlled retarder used to compensate polarization drifts (which can be neglected in this ideal example), the coherent state is split in path 7 and 8 by a PBS, obtaining the following states:

$$|p_7\rangle\,|p_8\rangle = \exp\left(\frac{\alpha_A}{\sqrt{2}}\left(\hat{g}_V^\dagger\right) - \frac{\alpha_A^*}{\sqrt{2}}\left(\hat{g}_V\right)\right)_8 |0\rangle_7|0\rangle_8. \tag{38}$$

Equivalently, similarly as done in Eq. 14, their vectorial representation is:

$$V_7 = \begin{pmatrix}0\\0\end{pmatrix}, \quad V_8 = \frac{\alpha_A}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix}. \tag{39}$$

From the previous calculations, one can easily understand that, if all the photons of thelight pulse are directed towards path 5 to be measured in {H, V}, the qubit is correctly measured. In fact, only the SPAD connected to path 8, associated with vertically polarized photons, is triggered. The fact that the vacuum state is present in path 7 indicates that no photon reaches the upper detector, at least in the case of an ideal system. Obviously, in the real case, imperfections in optical components bring some photons to this detector, resulting in occasional erroneous detections.

On the other hand, photons directed towards path 6 are measured in {A, D} basis. In fact, the polarization controller present in this path is always active and primarly used to rotate the state of polarization of the photons of 45°. Applying Eq. 21 (with $\delta = \pi$ and $\theta = \frac{\pi}{8}$ to describe a rotator of 45°) one finds that, after this polarization controller, the state becomes antidiagonal, in fact:

$$V_6' = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} \cdot \frac{\alpha_A}{\sqrt{2}}\begin{pmatrix}0\\i\end{pmatrix} = \frac{\alpha_A}{2}\begin{pmatrix}i\\-i\end{pmatrix}, \tag{40}$$

This rotation will lead to totally random measurements, as expected. In fact, after the PBS, the input path is splitted in a couple of horizontally-polarized and vertically-polarized states, and the global state can be computed similarly as in Eq. 14:

$$\begin{aligned}|p_9\rangle\,|p_{10}\rangle = &\exp\left(\frac{i\,\alpha_A}{2}\left(\hat{i}_H^\dagger\right) + \frac{i\,\alpha_A^*}{2}\left(\hat{i}_H\right)\right)_9 \\ &\cdot \exp\left(\frac{i\,\alpha_A}{2}\left(-\hat{l}_V^\dagger\right) + \frac{i\,\alpha_A^*}{2}\left(-\hat{l}_V\right)\right)_{10} \\ &|0\rangle_9|0\rangle_{10},\end{aligned} \tag{41}$$

Equivalently, using the matrix relation of the PBS, one can easily find that the associated vectors are:

$$V_9 = \frac{\alpha_A}{2}\begin{pmatrix}i\\0\end{pmatrix}, \quad V_{10} = \frac{\alpha_A}{2}\begin{pmatrix}0\\-i\end{pmatrix}. \tag{42}$$

In practice, the mean photon number (i.e. the sum of the square of the components of the associated vectors) reaching the two detectors is equal, and thus the two SPADs have the same probability to be triggered. In other words, a single photon that crosses path 6 is directed in the 50% of cases towards detector C measuring "0", while, in the remaining 50%, towards detector D, measuring "1". So, the measurement in $\{A, D\}$ basis is totally random, as expected.

To sum up, the simulator proposed in this article works in **aggregate way**; launching only once the simulation, the user obtains the mean photon number in every optical path and several useful parameters, such as the light intensity in every point of the system, the transmissivity, the polarization contrast (the probability that the photon hits the erroneous detector), and consequently the measurement probability.

5.2 MATLAB implementation

Since this simulator is mainly based on the matrix calculation, MATLAB results a suitable development environment, simple and efficient.

In order to automate the simulations, a series of MATLAB functions have been developed to easily describe and simulate a generic QKD system, but, in principle, it is possible to study any optical experiment based on coherent light where it is prominent to analyse the state of polarization. A function for each passive optical component has been developed; it contains the matrix relation of the component that allows one to compute the propagation of the coherent light state, from input to output. The matrix takes into account the non-idealities of the component mainly through the transmission and reflection coefficients reported in the datasheets. It is important to precise that no information about the values of ϕ of BS and PBS is usually available. For this reason, it is assumed equal to 0 and $-\frac{\pi}{2}$ for BS and PBS respectively, according to the matrices employed in the ideal simulation described in Sect. 5.1.

Each function contains also a sort of **library** storing the list of parameters necessary for the simulation. The functions for Pockels cells, non-polarizing and polarizing beam splitters are precompiled with the parameters of some commercial components. In this way, the real components can be quickly inserted in the simulation of a QKD system by their name, without having to rewrite their parameters every time. Moreover, being this structure fully modular, the user can freely add components to the libraries. For example, to insert a beam splitter in a simulation, the user can write:

```
[V_c,V_d]=beamsplitter_known(V_a, V_b,
          BS_Name)
```

where "BS_Name" recalls one of the saved beam splitters, and the vectors V are the bi-dimensional vectors that describe the coherent state in a certain optical path: in this case V_a and V_b are the input vectors, instead V_c and V_d are the output vectors. So, after having described the QKD optical system using these functions and initialised the vectors linked to the coherent states emitted by the light sources, the user can launch the simulation obtaining the α eigenvalues for every light state in every optical path, similarly as in the example of Sect. 5.1, with the difference of being able to consider the non-idealities of the components.

The presence of the libraries allows the user to **quickly insert and compare different optical components**, observing how the performance of the system varies. This is very

useful from an engineering point of view because it allows one to easily do a **cost-benefit analysis during the design phase of the system**, choosing the components that guarantee acceptable performance in the desired working region. An example of this methodology will be shown in Sect. 5.4, where the system discussed at the beginning of Sect. 5 will be simulated by comparing different SPADs.

5.3 Quantum bit error rate and secure key rate estimation

After having described the system in a MATLAB script, it is possible to calculate the parameters that define the efficiency of the system: QBER and secure key rate. It shall be highlighted that, since the proposed simulator works in an aggregate way, the finite size effect is neglected. Hence, the results are obtained in the asymptotic limit.

5.3.1 Quantum bit error rate

First, the quantum bit error rate must be calculated because it is necessary to evaluate the secure key rate. It is a fundamental parameter since it defines if the communication is secure or not; it can be shown that, if QBER $< 11\%$, Alice and Bob can obtain a secure private key, after having carried out error correction and privacy amplification procedures (Shor and Preskill 2000).

Before introducing the expression for the QBER, it is convenient to define some usefull concepts widely used in literature to analyse the performance of the system and to calculate QBER and key rate. First of all, the yield Y_i of a light pulse made by i-photons is the probability of detection at Bob's side, given that Alice sends an i-photon pulse (Ma et al. 2005). When Alice sends a vacuum state, i.e. she does not send photons to Bob, the yield Y_0 is linked to dark counts, hence to the background noise (such as Raman noise in this case) and especially to the dark counts of the photon detectors. According to Ma et al. (2005, 2006), the theoretic expression for the yield of a generic i-photon state when an infinite number of decoy states are used is:

$$Y_i = Y_0 + \eta_i - Y_0\eta_i \cong Y_0 + \eta_i, \tag{43}$$

where η_i is the transmittance of the i-photon state, which is given by:

$$\eta_i = 1 - (1 - \eta)^i. \tag{44}$$

η is the overall transmittance, obtained considering the power attenuation caused by the quantum channel (in this case the optical fiber, with an attenuation equal to 0.33 dB/km), the optical components at Bob's side and also the photon detection efficiency of the detectors (Wang et al. 2017). The overall transmittance for every optical path is easily obtainable in the MATLAB simulator: assuming that Alice sends to Bob a photon vertically polarized, it is sufficient to make the ratio between the mean photon number reaching the correct detector and the mean photon number leaving Alice's apparatus, multiplied by the photon detection efficiency (PDE):

$$\eta = PDE \cdot \frac{\text{path\_det}(1)^2 + \text{path\_det}(2)^2}{\text{path\_Alice}(1)^2 + \text{path\_Alice}(2)^2}, \tag{45}$$

where path_X^2 are the components of the "quantum" Jones vector used to calculate the mean photon number in horizontal (1) and vertical (2) polarization states.

Returning to the QBER, its expression in BB84 QKD systems, widely used in literature (Wang et al. 2017; Ma et al. 2005, 2006), is the following one:

$$E_\mu = \frac{1}{Q_\mu}\left[e_{\text{vac}} Y_0 + e_{\text{opt}}\left(1 - Y_0\right)\left(1 - e^{-\eta\mu}\right)\right], \tag{46}$$

where:

- Q_μ: the probability of a detection event when Alice sends a signal state. It is also called **signal gain**, and it is equal to (Ma et al. 2005):

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} = Y_0 + 1 - e^{-\eta\mu}, \tag{47}$$

  where μ is the signal mean photon number. In general, the aforementioned Y_0 can be easily obtained by the datasheet of the detector or by making hardware level simulations (for example using Verilog-A models, as in Xu et al. (2018)). In this case, also the Raman noise contributes to Y_0 because the classical communication happens on the same fiber used as quantum channel. Y_0 is assumed equal to 2.45×10^{-6}, considering the dark count probability per clock cycle of the used detector (equal to 1×10^{-6}) plus the Raman noise probability reported in the reference article (Wang et al. 2017). The transmittance η is computed using the simulator;
- e_{vac}: the **error rate of the background**. Dealing with the BB84 protocol, it is usually considered completely random, consequently e_{vac} is assumed equal to 0.5 (Ma et al. 2005);
- e_{opt}: the probability that the photon hits the erroneous detector, due to a **finite polarization contrast**. It fixes the QBER at small communication lengths. In this system setup, it is mostly caused by the polarizing beam splitter. This parameter can be easily computed with the simulator; it is sufficient to divide the light intensity reaching the wrong detector by the total light intensity reaching the pair of detectors:

$$e_{\text{opt}} = \frac{\text{path\_i}(1)^2 + \text{path\_i}(2)^2}{\text{path\_c}(1)^2 + \text{path\_c}(2)^2 + \text{path\_i}(1)^2 + \text{path\_i}(2)^2}, \tag{48}$$

  where the subscripts "i" and "c" stay for incorrect and correct detectors, respectively. Unfortunately, since no details are given regarding the optical components used in this experimental setup, this parameter is obtained by the fit of the theoretical QBER plot shown in the article, which gave $e_{\text{opt}} = 1.2$. In general, this parameter is independent from the quantum channel length, and it ranges between 0.5 and 3.3 (Ma et al. 2005), therefore the fitted value is reasonable.

The comparison of simulated and experimental values is shown in Fig. 6; the simulations well approximate the experimental values, slightly underestimating them between 50 km and 75 km and overestimating them beyond this point. This discrepancy is attributable to the fact that the optical components used in this system are not mentioned. In particular the parameter e_{opt}, connected to the quality of the used optical components, strongly influences the QBER fixing its minimal value when the quantum channel length tends to zero.

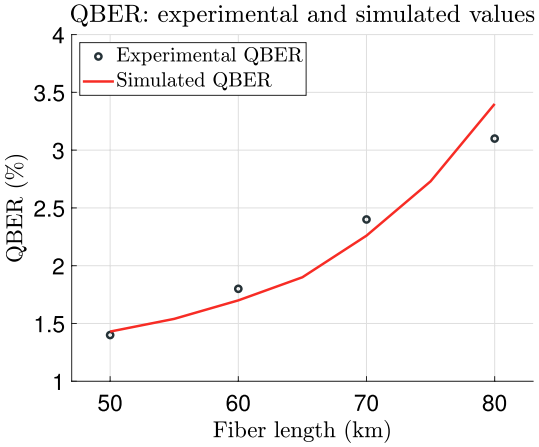

Fig. 6 Comparison between the experimental QBER and the simulated one

5.3.2 Secure key rate

To determine a worst-case scenario, it is useful to evaluate the lower bound of the secure key rate. According to Ma et al. (2005), the lower bound for the secure key rate per clock cycle in a BB84 protocol can be calculated as follows:

$$R = q\{-Q_\mu f \cdot H_2(E_\mu) + Q_1^{LB}[1 - H_2(e_1^{UB})]\}. \tag{49}$$

The parameters in the formula are:

- q: is the probability that Alice emits a signal state (0.75, as reported in the article) and Alice and Bob choose the same basis (0.5). Hence $q = 0.75 \times 0.5 = 0.375$;
- f: the **inefficiency of the error correction**, which is 1.25 in this system;
- H_2: the **binary entropy function**, equal to:

$$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x) \tag{50}$$

- E_μ: the **QBER of the system**;
- Q_1^{LB}: is the **lower bound for single-photons signal states**. Considering that in the setup of Wang et al. (2017) a two-decoy state-protocol is adopted, with a vacuum decoy state and a weak decoy state, its values is calculated using the following formula (Ma et al. 2005):

$$Q_1^{LB} = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right), \tag{51}$$

  where μ is the MPN for signal state, while ν the MPN for the weak decoy state. Q_ν is the weak-decoy state gain, calculated as in Eq. 47;
- e_1^{UB}: the upper bound for the quantum error rate due to single photon. Considering the two decoy state-protocol, it can be estimated with the following formula (Ma et al. 2005):

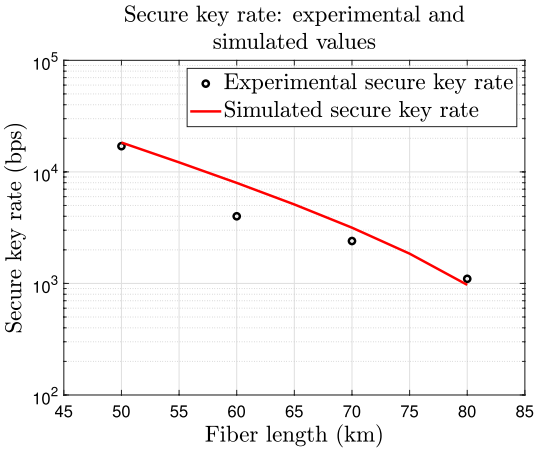

Fig. 7 Comparison between the experimental secure key rate and the simulated one

Table 1 List of the parameters employed in the simulation

Variable	Value	Source	Simulable
Y_0	2.45×10^{-6}	Wang et al. (2017)	–
η	Variable	Simulator	Yes
μ	0.6	Wang et al. (2017)	–
ν	0.2	Wang et al. (2017)	–
e_{vac}	0.5	Literature	–
e_{opt}	0.012	Wang et al. (2017)	Yes
q	0.375	Wang et al. (2017)	–
f	1.2	Wang et al. (2017)	–

$$e_1^{UB} = \frac{E_\nu Q_\nu e^\nu - e_0 Y_0}{Y_1^{LB}\nu}. \tag{52}$$

In this formula Y_1^{LB} is the lower bound for the single-photon yield, calculated with the following equation (Ma et al. 2005):

$$Y_1^{LB} = \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right). \tag{53}$$

The list of the parameters employed in the simulations is reported in Table 1. The simulated secure key rate is shown in Fig. 7, where the black dots represent the experimental values. The simulated curve, in red, tends to slightly overestimate the key rate also because the previously calculated QBER was lower than the experimental one. Nevertheless, since the simulated and the experimental values show the same trend, one can be reasonably optimistic about the accuracy of the proposed modelling methodology.

Considering the few information given by the researchers, the presence of Raman noise, and the simplifications introduced by this simulator, the results are satisfactory. Probably, having a more detailed description of the system would allow the proposed simulator to provide more accurate results.

5.4 Comparison of different SPADs

The possibility to easily observe how the performance of the system varies changing its components is a very useful feature of this simulator; it allows one to perform all the needed cost-benefit analysis during the design phase of the system.

In order to present this feature, the QBER of the system presented in Sect. 5 is simulated again, changing only the detectors. It is interesting to observe how the maximum achievable communication distance, where the QBER reaches the 11%, changes. For consistency, it was decided to compare only single photon avalanche diodes, the same type of detectors employed in the original setup.

The original detectors are able to work up to 625 MHz, with a PDE equal to 10% and a dark count rate of 1×10^{-6} (Wang et al. 2017). The original QBER, simulated with these parameters, is plotted in black. The SPAD developed by Zhang et al. (2010) is the only one of the comparison that offers better results. In fact, it is a very performing detector, able to work up to 2.23 GHz, with a PDE of 14% when the dark count probability per gate is approximately 1×10^{-6}. Its simulation is reported in red. The SPAD presented in Jiang et al. (2017) allows one to obtain a QBER very similar to the original one. In fact it is a SPAD able to work up to 1.25 GHz, with 10% of PDE when the dark count probability per gate is 1.6×10^{-6}. Its simulation is plotted in orange. The other two SPADs selected for the comparison give worse performance. The detector presented in Ruggeri et al. (2015) is able to work up to 1.3 GHz, with a very high PDE (30%) which corresponds to an equally high dark count probability per gate (2.2×10^{-5}). Its simulation is reported in blue. The worst results are obtained using the detector of Scarcella et al. (2014). It can work up to 1.3 GHz, with a PDE of about 6% and a corresponding dark count probability per gate of 2×10^{-5}. Its results are plotted in green.

From this comparison, it is clear how the single-photon detectors are crucial components in QKD systems. The best detector (red) permits to establish secure communications up to 106 km, approximately, versus the 67 km achievable with the worst one (green).

With the presented simulator it is possible to repeat this kind of comparison for each component, looking for the desired compromise between costs and performance.

6 Additional results

The target experimental setup of Wang et al. (2017) and the related article do not include a discussion on eavesdropping attacks nor on fiber polarization misalignment. Therefore, to validate the proposed coherent state-based simulator by comparing its results with the experimental ones of Wang et al. (2017), Sect. 5 does not consider attacks or polarization misalignment effects. However, the simulation methodology proposed in this article is sufficiently generic to model these phenomena, as discussed in the following.

6.1 Beam splitter attack

Even though an ideal QKD exchange allows Alice and Bob to share an unconditionally secure key, real-world setups, as discussed in the previous sections, are flawed by several non ideal phenomena. The latter can be exploited by an eavesdropper, conventionally known as Eve, to steal information about the key, for instance, through a so-called **intercept**

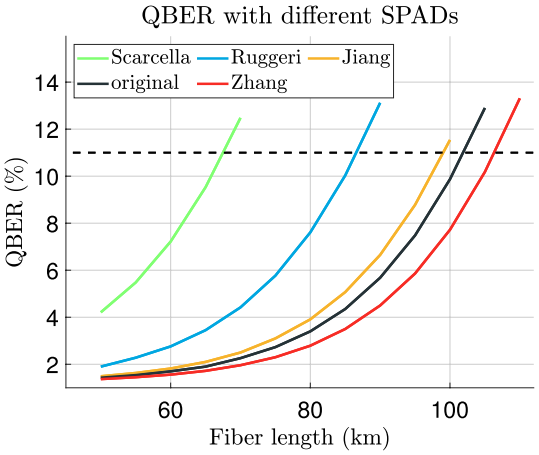

Fig. 8 Simulated QBER of the system (Wang et al. 2017) comparing different SPADs. The black line represents the original QBER, simulated using the information about the detector reported in the reference article (Wang et al. 2017).

and resend attack (Bennet et al. 1992). Several attacks exploit the fact that currently available QKD setups mainly use attenuated coherent lasers as photon sources. Therefore there will be some pulses consisting of more than one photon, and Eve can try to steal photons from the quantum channel. Among the most analysed attacks directed towards coherent states, one can cite the **photon number splitting attack** (Calsamiglia et al. 2001) and the **beam splitter attack** (Bennet et al. 1992; Calsamiglia et al. 2001; Allati and Baz 2015; Ramos and Karlsson 2004). The former is a theoretical attack in which Eve carries out a quantum non-demolition measurement on every pulse received from Alice to count the number of photons: for every pulse containing more than one photon, Eve deterministically takes away a single photon, which she stores in a quantum memory, waiting for Alice and Bob to declare the chosen basis for every pulse. Conversely, the latter is an experimentally feasible attack on current physical setups, to which this section is devolved. In a beam splitter attack, Eve introduces a beam splitter (Fig. 9) in the quantum channel with transmittance t_e towards Bob and reflectance r_e towards herself: varying these parameters, she can control the percentage of photons that are deviated towards herself. Since Eve aims

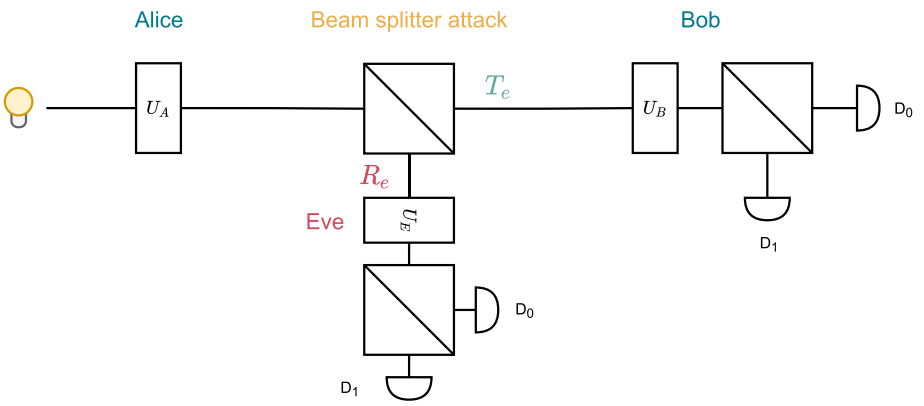

Fig. 9 Schematic representation of a beam splitter attack. t_e and r_e represent the transmission and reflection coefficients of the beam splitter added by Eve. U_A, U_B and U_E symbolically represent the Pockels cell used to choose the basis

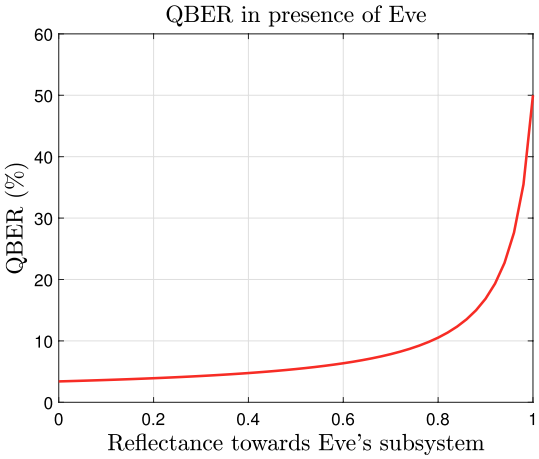

Fig. 10 Simulated QBER of the system (Wang et al. 2017) under beam splitter attack, as a function of the beam splitter reflectance r_e towards Eve's subsystem. The fiber length is fixed at 80 km

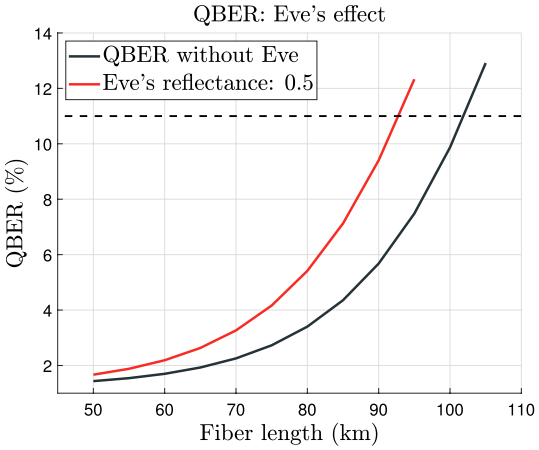

Fig. 11 Simulated QBER of the system (Wang et al. 2017) under beam splitter attack, as a function of fiber length. The red line shows the QBER when Eve uses a beam splitter with reflectance equal to 0.5: as expected, it is higher respect to the case without eavesdropper, and, consequently, the 11% QBER threshold is reached at a shorter fiber length

to maximise the cases for which both she and Bob measure at least one photon, it is clear that the optimum, from Eve's perspective, is to choose $r_e = t_e = 0.5$ (Ramos and Karlsson 2004).

To simulate the effect of a beam splitter attack—while preserving the low-complexity low-CPU-time hardware-oriented approach of the proposed methodology—the same QKD network of Fig. 5 and the same methodology of Sect. 5 are employed, with the only additional assumption that Eve places a beam splitter halfway between Alice's variable optical attenuator and Bob's bandpass filter. The presence of Eve's beam splitter reduces the efficiency η of the setup, thus leading to an exponential increase of the QBER, according to Eq. 46. Indeed, the QBER is a function of the efficiency, which in turn becomes a function of Eve's reflectance r_e. Figure 10 shows the exponential dependence of the QBER on r_e. It shall be highlighted that, as expected, when $r_e = 1$, then $E_\mu = 0.5$. As a matter of fact, if all photons are rerouted towards Eve, Bob's measurements are exclusively due to background noise (modelled by e_{vac}), and no information is shared between Alice and Bob.

Figure 11 reports the simulated behaviour of QBER as a function of the fiber length, when $r_e = t_e = 0.5$ (best choice for Eve). Comparing Fig. 11 with Fig. 8, it can be stated

that the increase of the QBER due to Eve's attack reduces the maximum length of the fiber that guarantees QBER $< 11\%$, as expected from the above discussion.

6.2 Fiber polarization misalignment

Analogously to the beam splitter attack, the QKD setup in Fig. 5 and the simulation methodology of Sect. 5 permit to evaluate the effects of polarization misalignment along the fiber. A schematic representation of the simulated optical system is shown in Fig. 12. The most interesting part is undoubtedly the central one, where channel is highlighted: the effects of random polarization rotations are described in terms of a sequence of equivalent Pockels cells characterized by the random angle $\delta = \frac{\tilde{\xi}}{2}$ (Eq. 27), located exactly in the middle of the channel, whose total length is equal to L, and which is, as usual, affected by the intensity attenuation phenomenon (Eq. 28).

The information available in Xu et al. (2013) is useful not only for the construction of the model based on the effective Pockels cell, but also to choose the $\tilde{\xi}$ value in all the executed simulations. In particular, in that reference, the random angle is assumed to belong to a normal distribution with mean number equal to 0 and standard deviation λ_{std}—which is related to the misalignment error $e_{\text{mis}} = \sin^2(\lambda_{\text{std}})$ employed in the reported results—thus implying that the aleatory angle is considered between $-3\lambda_{\text{std}}$ and $+3\lambda_{\text{std}}$ (99.73% of the normal distribution). For these reasons, in order to consider a worst-case simulative scenario, the effects of polarization misalignment in the setup of Fig. 5 are examined for $\tilde{\xi} = +3\lambda_{\text{std}}$, with different e_{mis} values (thus different $\tilde{\xi} = +3\sin^{-1}(\sqrt{e_{\text{mis}}})$).

Figure 13 shows the simulated behaviour of the secure key rate as a function of the misalignment error $0 \leq e_{\text{mis}} \leq 0.08$ for a channel length equal to 75 km. It is possible to ascertain, as expected from theory, that a higher rotation implies a more significant reduction of the secure key rate. In particular, $e_{\text{mis}} = 0.08$ reduces the plotted quantity by about five times, with respect to the case in which misalignment error is totally absent.

The available model of polarization misalignment also permits to evaluate the effects of this phenomenon on the maximum secure achievable distance, i.e. the channel length where QBER overcomes 11%. Figure 14 shows the QBER as a function of fiber length, with different constant polarization misalignment values. As expected, when the polarization misalignment error increases, the maximum secure achievable distance decreases. In particular, with the simulation setup under analysis, a polarization misalignment $e_{mis} \simeq 0.08$ reduces this distance by more than 10 km with respect to the corresponding value with $e_{mis} = 0$, which is slightly higher than 100 km.

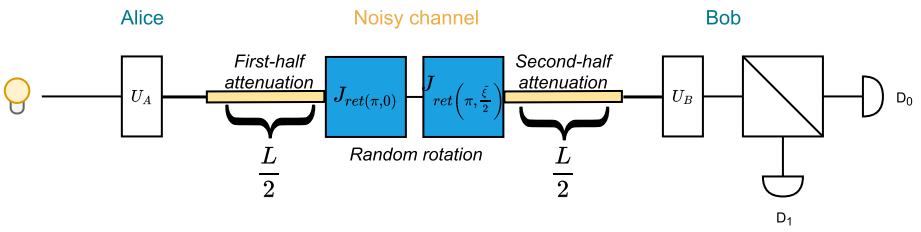

Fig. 12 Schematic representation of a fiber polarization misalignment simulation. The effective Pockels cell used to describe random rotations is located in the middle of a channel with total length L. Simulation also takes into account the intensity attenuation

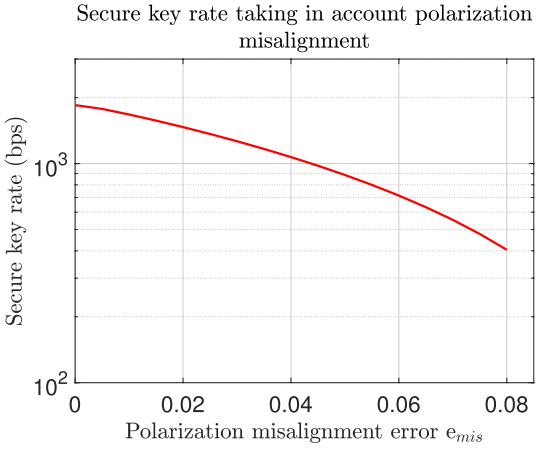

Fig. 13 Simulated secure key rate of the system (Wang et al. 2017) taking in account the polarization misalignment effect. When the polarization error e_{mis} and consequently the rotation angle $\tilde{\xi} = +3\sin^{-1}(\sqrt{e_{\text{mis}}})$ increase, the secure key rate rapidly decreases. The simulations are performed with a quantum channel 75 km long

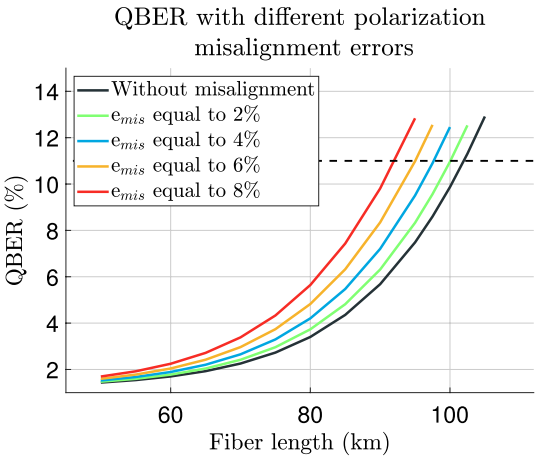

Fig. 14 Simulated QBER of the system (Wang et al. 2017) as a function of the fiber length, taking in account the polarization misalignment effect.When the polarization error e_{mis} and consequently the rotation angle $\tilde{\xi} = +3\sin^{-1}(\sqrt{e_{\text{mis}}})$ increase, the secure communication distance, where QBER is lower than 11%, decreases

7 Conclusions and future perspectives

The theoretical model and the MATLAB implementation discussed in this article represent a necessary starting point for the development of a simulator for the analysis and the design of Quantum Key Distribution systems based on polarization encoding. The simulation of a real system presented in Sect. 5.3 provides reasonable results, which are in good agreement with the experimental QBER and key rate reported in the reference article (Wang et al. 2017). Moreover, the proposed simulator provides a preliminary support for polarization misalignment phenomena, as discussed in Sect. 6. Even though this work does not propose a definitive model for QKD systems, the obtained results are encouraging and represent a first step towards the validation of the reliability of the proposed approach. A comprehensive definitive simulator undoubtedly requires more research; some of the future steps required to approach this goal are reported in the following.

A first step should be the integration of new functions for other passive optical components usually employed in QKD systems, for example mirrors. Moreover, the model of the

quantum channel can be improved and expanded. Indeed, the current version of the simulator only takes into account the attenuation and the polarization misalignment effects of the channel, whereas other channel non-ideal phenomena, such as the frequency dispersion, are neglected. The two phenomena already available could be also evaluated in other simulative scenarios. For example, the model of polarization misalignment based on J_{ret} is sufficiently generic for being employed with probability distributions of $\tilde{\xi}$ different from the normal one inherited from Xu et al. (2013). An interesting use-case could be the simulation of time-correlated aleatory $\tilde{\xi}$ values. Even though the time variable is not explicitly available in the simulator, it could be possible to emulate it with repeated photons transmissions. This approach could also open the way for the future integration in the simulator of "real-time" polarization mismatch compensation procedures based on an iterative methodology, similar to that described in Higgins et al. (2020). This simulative approach could be also exploited for the evaluation of a more generic misalignment based multiple random angles, exploiting the generic J_{ret}^{comb} matrix (Eq. 24). A potential strategy for real-time polarization misalignment compensation is schematized in Fig. 15; this is based on the comparison of the expected transmitted and the received states of photons not encoding information, to obtain an estimation of a triplet of random angles $\theta_{U3,r}$, $\lambda_{U3,r}$ and $\phi_{U3,r}$ associated with the equivalent J_{ret}^{comb} matrix. If this values are available it is possible to apply to the photons state the inverse evolution $J_{ret}^{comb^\dagger} = J_{ret}^{comb}(-\theta_{U3,r}, -\lambda_{U3,r}, -\phi_{U3,r})$ (Abraham 2019), with a set of Pockels cells available to the receiver.

In addition to all possible improvements associated with optical fiber, since open-air QKD is at the root of satellite QKD, the interest in this technology has been recently increasing. Therefore, a detailed analysis should be dedicated to the air used as the quantum channel.

As mentioned above, the photon detection efficiency and the dark count rate of single-photon detectors strongly influence QBER and key rate of QKD systems. Hence, it would be valuable to integrate into the infrastructure a low-level (for instance, circuit-level or hardware-level) simulation tool for photon detectors, as depicted in Fig. 16. A possible approach would be to combine the optical simulator presented in this article with an

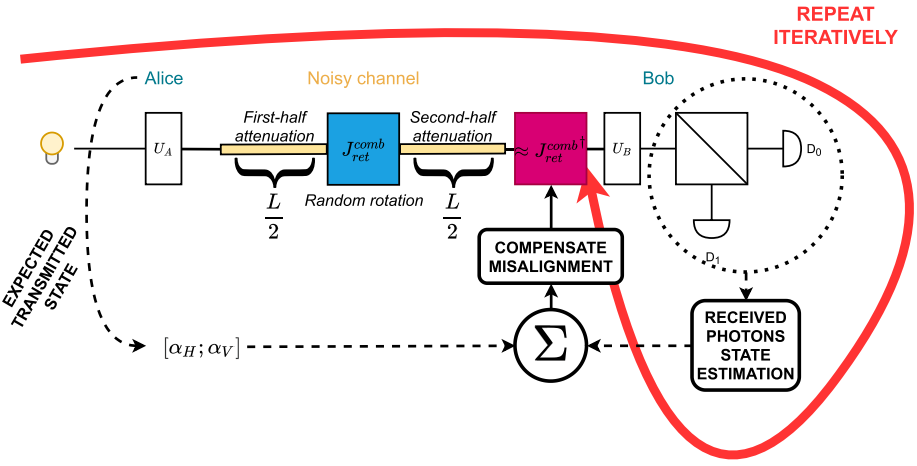

Fig. 15 Schematic representation of a potential iterative procedure for compensating fiber polarization misalignment. Transmitted and received states could be compared to define the rotation angle ξ of the compensation angle available to Bob

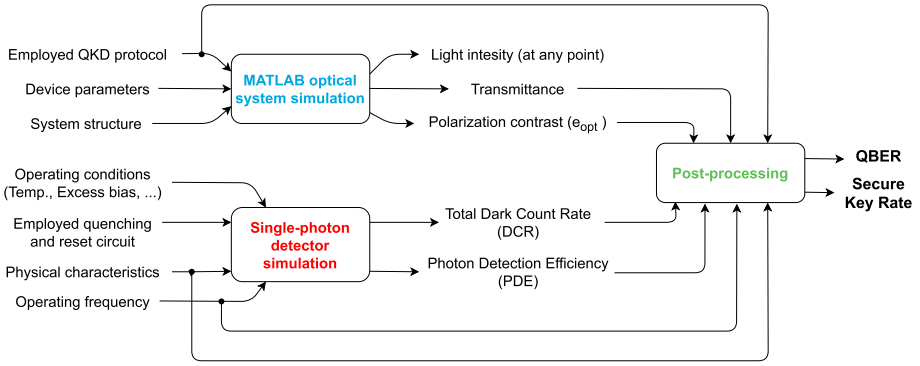

Fig. 16 Flow chart of the simulation framework. The data obtained from the optical simulator and the single-photon detector simulator are combined in a post-processing phase in order to calculate QBER and key rate of the system

analysis tool for photon detectors (based for example on Verilog-A, as the one reported in Xu et al. (2018)), able to evaluate performance of the latter depending on the structure and the operating conditions of the devices. In this way, the user would be allowed to easily estimate and compare the performance of the QKD system, by employing custom detectors and reproducing the real operating conditions.

Currently, as discussed in Sect. 6.1, the simulator supports a preliminary model of the beam splitter attack. The possibility to simulate additional eavesdropper attacks should be another interesting future feature of this simulator.

Thereafter, it will be interesting to broaden the horizons of the simulator, allowing the design of other types of QKD systems, not only based on polarization-encoding. In fact, at the moment, the simulator is suited to analyse systems based on polarization-encoding protocols without entangled photons (such as BB84 or Lucamarini and Mancini 2005). A potential solution would be the evolution of the theoretical model, moving to the density matrix formalism, which is expected to bring at least two main benefits. Firstly, this formalism would allow one to simulate a larger variety of QKD systems, including those that employ real single-photon light sources, such as defect clusters in diamond and quantum dots in solid-state semiconductors. Secondly, it would provide wider support for the simulation of environment interactions and non-ideal phenomena, such as the loss of quantum information due to decoherence and relaxation.

Even though some features must be clearly improved, the activity described in this article could be a good starting point for the development of an accurate simulator of quantum-assisted communication systems, employable by network designers with the awareness of the discrepancies between the simulated results and those expected in an experimental setup.

Funding Open access funding provided by Politecnico di Torino within the CRUI-CARE Agreement.The authors have not disclosed any funding.

Declarations

Conflict of interest The authors declare that no funds, grants, or other support were received during the preparation of this manuscript. The authors have no relevant financial or non-financial interests to disclose.

References

Abraham, H., AduOffei., Akhalwaya, I.Y., Aleksandrowicz, G., Alexander, T., Alexandrowics, G., Arbel, E., Asfaw, A., et al.: Qiskit: an open-source framework for quantum computing (2019)

Al-Kathiri, S., Al-Khateeb, W., Hafizulfika, M., Wahiddin, M.R., Saharudin, S.: Characterization of mean photon number for key distribution system using faint laser. In: 2008 International Conference on Computer and Communication Engineering, pp. 1237–1242 (2008). https://doi.org/10.1109/ICCCE.2008.4580803

Allati, A.E., Baz, M.E.: Quantum key distribution using optical coherent states via amplitude damping. Opt. Quantum Electron. **47**, 1035–1046 (2015). https://doi.org/10.1007/s11082-014-9959-2

Allati, A.E., Hassouni, Y., Metwally, N.: Communication via an entangled coherent quantum network. Phys. Scr. **83**, 065002 (2011). https://doi.org/10.1088/0031-8949/83/06/065002

Bachor, H.-A., Ralph, T.C.: A Guide to Experiments in Quantum Optics. Wiley, 3rd edition, (2019)

Barnett, S.M., Jeffers, J., Gatti, A., Loudon, R.: Quantum optics of lossy beam splitters. Phys. Rev. A **57**, 2134–2145 (1998). https://doi.org/10.1103/PhysRevA.57.2134

Bartlett, B.: A Distributed Simulation Framework for Quantum Networks and Channels (2018). arXiv:1808.07047

Bennet, C.H., Bessette, F., Brassard, G., Smolin, J.: Experimental quantum cryptography. J. Cryptol. (1992). https://doi.org/10.1007/BF00191318

Bennett, C.H., Brassard, G.: "Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, (India), p. 175 (1984). https://arxiv.org/abs/2003.06557

Bernstein, D.J., Lange, T.: Post-quantum cryptography. Nature **549**(7671), 188–194 (2017). https://doi.org/10.1038/nature23461

Calsamiglia, J., Barnett, S.M., Lütkenhaus, N.: Conditional beam-splitting attack on quantum key distribution. Phys. Rev. A **65**, 012312 (2001). https://doi.org/10.1103/PhysRevA.65.012312

Cirillo, G.A., Turvani, G., Simoni, M., Graziano, M.: Advances in molecular quantum computing: from technological modeling to circuit design. In: 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 132–137, IEEE, (2020)

Cirillo, G.A., Turvani, G., Graziano, M.: A quantum computation model for molecular nanomagnets. IEEE Trans. Nanotechnol. **18**, 1027–1039 (2019)

Coopmans, T., Knegjens, R., Dahlberg, A., Maier, D., Nijsten, L., de Oliveira Filho, J., Papendrecht, M., Rabbie, J., Rozpedek, F., Skrzypczyk, M., Wubben, L., de Jong, W., Podareanu, D., Torres-Knoop, A., Elkouss, D., Wehner, S.: Netsquid, a discrete-event simulation platform for quantum networks. Commun. Phys. **4**, 1–15. (2021). https://doi.org/10.1038/s42005-021-00647-8

Corning, Corning SMF-28e, Optical Fiber Product Information, http://www.tlc.unipr.it/cucinotta/cfa/datasheet_SMF28e.pdf. Accessed Jan 2005

Dahlberg, A., Wehner, S.: SimulaQron: a simulator for developing quantum internet software. Quantum Sci. Technol. **4**, 015001 (2018). https://doi.org/10.1088/2058-9565/aad56e

Diadamo, S., Nötzel, J., Zanger, B., Beşe, M.M.: QuNetSim: a software framework for quantum networks. IEEE Trans. Quantum Eng. **2**, 1–12 (2021). https://doi.org/10.1109/TQE.2021.3092395

Djordjevic, I.B., Zhang, Y.: Photon angular momentum based multidimensional quantum key distribution. In: 2014 16th International Conference on Transparent Optical Networks (ICTON), pp. 1–4 (2014). https://doi.org/10.1109/ICTON.2014.6876370

Elser, D., Bartley, T., Heim, B., Wittmann, C., Sych, D., Leuchs, G.: Feasibility of free space quantum key distribution with coherent polarization states. New J. Phys. **11**(4), 045014 (2009). https://doi.org/10.1088/1367-2630/11/4/045014

C, M. et al.: Passive preparation of BB84 signal states with coherent light, Prog. Inf. **8** (2011). https://www.nii.ac.jp/pi/n8/8_57.pdf
Fowles, G.: Introduction to Modern Optics. Dover Publications, New York (1989)
Fox, M.: Quantum Optics, an Introduction. Oxford, (2006)
Gazeau, J.-P.: Coherent States in Quantum Physics, 1st edn. Wiley, Berlin (2009)
Gerry, C., Knight, P.: Introductory Quantum Optics. Cambridge University Press (2004). https://doi.org/10.1017/CBO9780511791239
Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**, 145–195 (2002). https://doi.org/10.1103/RevModPhys.74.145
Hecht, E.: Optics. Reading, Mass: Addison-Wesley, 4th edition (2002)
Higgins, B.L., Bourgoin, J.-P., Jennewein, T.: Numeric estimation of resource requirements for a practical polarization-frame alignment scheme for quantum key distribution (QKD). Adv. Opt. Technol. **9**(5), 253–261 (2020). https://doi.org/10.1515/aot-2020-0016
Jiang, W.-H., Liu, J.-H., Liu, Y., Jin, G., Zhang, J., Pan, J.-W.: 1.25 GHz sine wave gating InGaAs/InP single-photon detector with a monolithically integrated readout circuit. Opt. Lett. **42**(24), 5090–5093 (2017). https://doi.org/10.1364/OL.42.005090
Jones, R.C.: A new calculus for the treatment of optical systems. IV. J. Opt. Soc. Am. **32**, 486–493 (1942). https://doi.org/10.1364/JOSA.32.000486
Kemp, J.C.: Piezo-optical birefringence modulators: new use for a long-known effect. J. Opt. Soc. Am. **59**(8), 950–954 (1969). https://doi.org/10.1364/JOSA.59.000950
Kim, I.I., McArthur, B., Korevaar, E.J.: Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications. Opt. Wirel. Commun. **III**(4214), 26–37 (2001). https://doi.org/10.1117/12.417512
Kučera, P.: Quantum description of optical devices used in interferometry. Radioengineering **16**(3), 4 (2007)
Liao, S.-K., Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., Yin, J., Shen, Q., Cao, Y., Li, Z.-P., et al.: Satellite-to-ground quantum key distribution. Nature **549**(7670), 43–47 (2017). https://doi.org/10.1038/nature23655
Loudon, R.: The Quantum Theory of Light. OUP Oxford (2000)
Lounis, B., Orrit, M.: Single-photon sources. Rep. Prog. Phys. **68**(5), 1129 (2005). https://doi.org/10.1088/0034-4885/68/5/r04
Lucamarini M, Mancini S.: Secure deterministic communication without entanglement. Phys. Rev. Lett. **94**(14), 140501 (2005). https://doi.org/10.1103/PhysRevLett.94.140501
Lütkenhaus, N.: Security against individual attacks for realistic quantum key distribution. Phys. Rev. A **61**, 052304 (2000). https://doi.org/10.1103/PhysRevA.61.052304
Ma, X., Qi, B., Zhao, Y., Lo, H.-K.: Practical decoy state for quantum key distribution. Phys. Rev. A **72**, 012326 (2005). https://doi.org/10.1103/PhysRevA.72.012326
Ma, X., Fung, C.-H.F., Dupuis, F., Chen, K., Tamaki, K., Lo, H.-K.: Decoy-state quantum key distribution with two-way classical postprocessing. Phys. Rev. A **74**, 032330 (2006). https://doi.org/10.1103/PhysRevA.74.032330
Mailloux, L.O., Morris, J.D., Grimaila, M.R., Hodson, D.D., Jacques, D.R., Colombi, J.M., Mclaughlin, C.V., Holes, J.A.: A modeling framework for studying quantum key distribution system implementation nonidealities. IEEE Access **3**, 110–130 (2015). https://doi.org/10.1109/ACCESS.2015.2399101
Maitra, A., Das, S.S.: Generalized Theoretical Approach for Analysing Optical Experiments. arXiv repository [quant-ph], (2019). https://arxiv.org/abs/1905.01112v1
Matsuo, T., Durand, C., Satoh, R., Van Meter, R., Shigeya, S., Nagayama, S., Satoh, T., Tatetani, N., Nakai, M., Metwalli, S. et al.: QuISP–Quantum Internet Simulation Package (2020). [online] https://aqua.sfc.wide.ad.jp/quisp_website/
Molotkov, S., Potapova, T.: Faint laser pulses versus a single-photon source in free space quantum cryptography. Laser Phys. Lett. **13**(3), 035201 (2016). https://doi.org/10.1088/1612-2011/13/3/035201
Nagata, T., Okamoto, R., Hofmann, H.F., Takeuchi, S.: Analysis of experimental error sources in a linear-optics quantum gate. New J. Phys. **12**, 043053 (2010). https://doi.org/10.1088/1367-2630/12/4/043053
Prasad, S., Scully, M.O., Martienssen, W.: A quantum description of the beam splitter. Opt. commun. **62**(3), 139–145 (1987). https://doi.org/10.1016/0030-4018(87)90015-0
Ramos, R.V., Karlsson, A.: Software for analysis of eavesdropping strategies in photonic quantum cryptographic systems. J. Opt. Commun. **25**(3), 110–119 (2004). https://doi.org/10.1515/JOC.2004.25.3.110
Renner, R.: Security of quantum key distribution. Int. J. Quantum Inf. **6**(01), 1–127 (2008). https://doi.org/10.1142/S0219749908003256

Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**, 120–126 (1978). https://doi.org/10.1145/359340.359342

Rosas-Ortiz, O.: Coherent and squeezed states: introductory review of basic notions, properties, and generalizations. In: Integrability, Supersymmetry and Coherent States, pp. 187–230, (2019). https://doi.org/10.1007/978-3-030-20087-9_7

Ruggeri, A., Ciuffolini, M., Calandri, N., Sanzaro, M., Scarcella, C., Boso, G., Tosi, A.: High stability InGaAs/InP single-photon detector with Gigahertz sinusoidal gating. In: Single Photon Workshop 2015, CHE,(2015). http://hdl.handle.net/11311/984145

Scarcella, C., Boso, G., Ruggeri, A., Tosi, A.: InGaAs/InP single-photon detector gated at 1.3 GHz with 1.5% afterpulsing. IEEE J. Sel. Topics Quantum Electron **21**(3), 17–22 (2014). https://doi.org/10.1109/JSTQE.2014.2361790

Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134, IEEE (1994). https://doi.org/10.1109/sfcs.1994.365700

Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441 (2000). https://doi.org/10.1103/PhysRevLett.85.441

Simoni, M., Cirillo, G.A., Turvani, G., Graziano, M., Zamboni, M.: Towards compact modeling of noisy quantum computers: a molecular-spin-qubit case of study. J. Emerg. Technol. Comput. Syst. (2022). https://doi.org/10.1145/3474223

Vintskevich, S.V., Grigoriev, D.A., Miklin, N.I., Fedorov, M.V.: Entanglement of multiphoton two-mode polarization fock states and of their superpositions. Laser Phys. Lett. **17**, 035209 (2020). https://doi.org/10.1088/1612-202x/ab72a1

Wang, L.-J., Zou, K.-H., Sun, W., Mao, Y., Zhu, Y.-X., Yin, H.-L., Chen, Q., Zhao, Y., Zhang, F., Chen, T.-Y., Pan, J.-W.: Long-distance copropagation of quantum key distribution and terabit classical optical data channels. Phys. Rev. A **95**, 012301 (2017). https://doi.org/10.1103/PhysRevA.95.012301

Weihs, G., Zeilinger, A.: Photon Statistics at Beam Splitters: An Essential Tool in Quantum Information and Teleportation. (2001). https://copilot.caltech.edu/documents/16791/weihs_zeillinger_photon_statistics_at_beamsplitters_qip.pdf

Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature **299**(5886), 802–803 (1982). https://doi.org/10.1038/299802a0

Xu, F., Curty, M., Qi, B., Lo, H.-K.: Practical aspects of measurement-device-independent quantum key distribution. New J. Phys. **15**, 113007 (2013). https://doi.org/10.1088/1367-2630/15/11/113007

Xu, Y., Zhao, T., Li, D.: An accurate behavioral model for single-photon avalanche diode statistical performance simulation. Superlattices Microstruct **113**, 635–643 (2018). https://doi.org/10.1016/j.spmi.2017.11.049

Zhang, J., Eraerds, P., Walenta, N., Barreiro, C., Thew, R., Zbinden, H.: 2.23 GHz gating InGaAs/InP single-photon avalanche diode for quantum key distribution. In: Itzler MA, Campbell JC (eds.) Advanced Photon Counting Techniques IV, vol. 7681, pp. 239 – 246, International Society for Optics and Photonics, SPIE, (2010). https://doi.org/10.1117/12.862118

Authors and Affiliations

Carlo Caputo[1] · Mario Simoni[1] · Giovanni Amedeo Cirillo[1] · Giovanna Turvani[1] · Maurizio Zamboni[1]

Carlo Caputo
carlo.caputo@studenti.polito.it

Giovanni Amedeo Cirillo
giovanni_cirillo@polito.it

Maurizio Zamboni
maurizio.zamboni@polito.it

[1] Department of Electronics and Telecommunications, Politecnico di Torino, Corso Castelfidardo, 39, 10129 Turin, Italy