PAPERS | JANUARY 01 2025

Simple portable quantum key distribution for science outreach

Special Collection: Celebrating the International Year of Quantum Science and Technology

Pedro Neto Mendes ; Paulo André ; Emmanuel Zambrini Cruzeiro

Am. J. Phys. 93, 69–77 (2025)
https://doi.org/10.1119/5.0204077

Simple portable quantum key distribution for science outreach

Pedro Neto Mendes[a] and Paulo André[b]
Departamento de Engenharia Electrotécnica e de Computadores, Instituto Superior Técnico, 1049-001 Lisbon, Portugal and Instituto de Telecomunicações, 1049-001 Lisbon, Portugal

Emmanuel Zambrini Cruzeiro[c]
Instituto de Telecomunicações, 1049-001 Lisbon, Portugal

(Received 19 February 2024; accepted 22 November 2024)

Quantum key distribution (QKD) has become an essential technology in the realm of secure communication, with applications ranging from secure data transmission to quantum networks. This paper presents a simple, compact, and cost-effective setup for undergraduate tutorial demonstrations of QKD. It relies on using weak coherent pulses, which can be readily produced using an attenuated laser. The system employs the simplified three-state BB84 protocol in free space, with states encoded using linear polarization. Polarization encoding can be done passively or actively, depending on the budget available. Time multiplexing is implemented at the receiver to reduce the number of required detectors. Only two detectors are used to implement measurements on two bases, with a total of four outcomes. The result demonstrates the practicality of the system for free-space quantum communication, and its compact and portable nature makes it particularly suitable for pedagogical demonstrations. This work paves the way for engaging undergraduate students in the field of quantum communication through hands-on laboratory projects.
https://doi.org/10.1119/5.0204077

I. INTRODUCTION

Information security plays a pivotal role in numerous domains, including finance, military, industry, and even at the individual level. Traditional encryption methods, although effective in many scenarios, confront an approaching threat posed by the rapid advancement of quantum computing. These quantum computers have the potential to break through established encryption techniques, thereby raising concerns about the vulnerability of sensitive information.

Quantum key distribution (QKD) has the potential to enable secure encrypted communication. First proposed in 1984,[1] it offers the ability to exchange a secret key between two remote parties with proven security based only on the laws of physics. This key can later be used to communicate messages using protocols like the one-time-pad.

The simplified three-state BB84 protocol makes this QKD more easily implemented in an undergraduate laboratory. Moreover, to render QKD systems more practical, some assumptions can be relaxed; for example, the ideal single-photon source can be replaced by a source of attenuated laser pulses. At first glance, the use of these weak coherent pulses seems to make the system prone to photon number splitting (PNS) attacks. However, this security risk can be overcome with the use of decoy states,[3] which allow the users to determine more easily the presence of an eavesdropper.

These practical choices allow for more compact, cheaper, and simpler setups that can be used in an undergraduate laboratory to explain how these protocols work while at the same time discussing fascinating questions that researchers have to deal with related to security issues and what really is quantum in a light pulse. Additionally, we also use time multiplexing to reduce the number of detectors required to implement the QKD protocol.

Although educational articles exist on QKD implementation and single photon experiments in laboratories,[4–7] here we focus on the use of weak coherent pulses which offer a more straightforward and cost-effective setup, making quantum communication protocols more easily accessible to undergraduate students. This work aims to bridge the gap between theory and practice, providing a valuable educational resource for understanding and implementing secure quantum communication.

In this work, different setups are proposed to implement the communication protocol. The total cost of the experiment was around 27 000 dollars as equipment already acquired was used. If simpler and cheaper equipment is used instead, as suggested, the price can be lowered to around 11 000 dollars (detailed prices in Appendix A).

This paper begins with a review of basic quantum mechanics and the cryptographic protocols considered in Sec. II. Section III provides an overview of the experimental setup and its implementation, followed by a discussion of the results in Sec. IV.

II. THEORY

A. Basic quantum mechanics

A pure quantum bit, or qubit, can be represented by a normalized vector in $\mathbb{C}_2$; that is, the two-dimensional space of complex numbers. In the Dirac notation, such a vector is denoted $|\psi\rangle$. In general, a qubit can be parametrized in spherical coordinates as

$$|\psi\rangle = \begin{pmatrix} \cos\dfrac{\theta}{2} \\ e^{i\varphi}\sin\dfrac{\theta}{2} \end{pmatrix}, \tag{1}$$

where θ is related to how close one is from the $|0\rangle$ (equiv. $|1\rangle$) state, and φ gives a phase that describes a rotation of the state around the z-axis.

The basis we implicitly chose, $|0\rangle, |1\rangle$ is called the Z basis. Other bases for qubits are the X ($|+\rangle, |-\rangle$) and Y ($|R\rangle, |L\rangle$) bases. When encoding a qubit in the linear polarization of light, $|0\rangle$ becomes $|H\rangle$, i.e., a horizontally polarized mode, $|1\rangle$ becomes $|V\rangle$, $|+\rangle$ becomes $|D\rangle$, and $|-\rangle$ becomes $|A\rangle$.

A measurement in quantum mechanics is represented by a set of operators E_k ($C_2 \times C_2$ matrices). Note that there exist more general forms, but in our case, we restrict to rank one projectors, which means they can be written in terms of one vector, i.e., $E_k = |k\rangle\langle k|$. The number of operators, or equivalently of indices k, represents the number of measurement outcomes. In this tutorial, all the measurements we consider have two outcomes. Finally, in quantum mechanics, one computes the probability of obtaining an outcome k when measuring the state $|\psi\rangle$ with measurement E_k using Born's rule, which reads $\text{Prob}(k) = \langle\psi|E_k|\psi\rangle$.

B. One time pad and BB84

The one-time pad is an information-theoretically secure encryption technique, meaning that the encrypted message does not provide information about the original message. This communication method requires a novel, symmetric, and random key in each communication round and these keys cannot be smaller than the message size.

The message m, written in binary code, is combined with the secret key k through modular addition creating the cipher message c ($c = m \oplus k$). The cipher message can be combined with the secret key to recover the original message ($m = c \oplus k$).

The encryption is only secure if the random key can be distributed securely. The BB84 protocol is a quantum key distribution scheme where the emitter (usually referred to as Alice) can share a secret key with the receiver (usually referred to as Bob). These parties are connected through a quantum channel and a classical channel, where they exchange quantum and classical signals. We also consider the possibility that a third party, Eve, may eavesdrop on either channel.

Alice encodes the secret key in the polarization of photons. Alice and Bob agree in advance that both a vertically polarized photon (V) and a diagonally polarized photon (D) encode the bit 0, while the horizontal (H) and anti-diagonal (A) polarizations encode the bit 1. They also agree to randomly change their polarizer orientations between the V/H basis (called Z) and the D/A basis (called X). The crux of the BB84 protocol is that the photons are sent through the quantum channel, and after the detection is complete, the orientations of the polarizers can be sent "in the open" through the classical channel.

Of course, if Bob measures in the wrong basis, he may get the wrong result, since, for example, a diagonally polarized photon may be measured as either horizontally or vertically polarized, with equal probability. However, if he measures in the same basis, then he will receive the bit that Alice sent. When they send the polarizer orientation information through the classical channel after the measurements are complete, they will know which bits they must agree on, and those will become the secret key.

The presence of an eavesdropper can be detected if Alice and Bob compare a few of the bits in the secret key to test if they all agree. Eve would not know in advance how to set her polarizer, and if both Alice's and Bob's polarizers happened to be oriented in the same basis but Eve's was different, then her measurement would change the polarization of the photon, leaving a 50% chance that Bob would detect the wrong bit.

This is the idea of the BB84 protocol. It works as follows:

(1) **Quantum communication**: Alice creates a binary random key string and for each bit, randomly chooses on which basis to encode the information. She then sends through the quantum channel the respective quantum state. Bob makes a random basis choice, measures the state, and stores the output.
(2) **Sifting**: Alice and Bob share through the classic channel their respective basis choice. They then discard the bits for which the bases do not match and save the rest.
(3) **Post processing**: Alice and Bob estimate how much information was leaked to Eve through the errors on the sifted key, and perform error correction and privacy amplification. The protocol is aborted if Eve's presence is identified.

Table I illustrates a few rounds of communication between Alice and Bob and how errors can appear in the shared key.

The error correction step is necessary to ensure that Alice and Bob share the same string of bits. This is accomplished using protocols like Cascade or LDPCs,[8] which require an estimation of the quantum bit error rate (QBER) and additional information to be shared through the classical channel (e.g., the parity of blocks of the key string). This estimation of the QBER is done by sharing part of the key between Alice and Bob. Finally, both parties run a privacy amplification protocol[9] to ensure that even with the extra information Eve might have intercepted, she cannot reconstruct the secret key. This procedure reduces the size of the key.

The performance of the communication protocol can then be evaluated by some key parameters like the QBER, the secret key rate (SKR), and the transmission distance (given by how much loss the system can tolerate before the SKR becomes negligible).

The QBER can be defined as the ratio of the number of erroneous bits to the total number of bits transmitted over a quantum channel. A lower QBER generally signifies a more secure and reliable QKD system, as it implies fewer errors in the transmitted key bits, increasing the potential for eavesdropping detection and the efficiency of the key generation process.

The SKR is the rate at which secure keys are generated and shared between two parties. It reflects the amount of usable key material produced per second after post-processing, ensuring secure communication. Higher secret key rates indicate more efficient and practical QKD systems.

The transmission distance is the distance at which the communication was performed and is related to the loss as for both free-space and fiber-based setups, the loss increases with the distance. The higher the loss an experimental setup can tolerate, the longer the transmission distance will be.

C. Simplified BB84

The simplified BB84 protocol is a variant of the original BB84 quantum key distribution protocol, designed to streamline the process while maintaining its security features. In the computational basis Z, the protocol runs exactly as the original BB84. However, in the monitoring basis X, the emitter prepares only $|D\rangle$, so that only three preparations are necessary. The protocol then runs similarly to the BB84:

Table I. Shared secret key generated by the BB84 protocol in the presence of Eve. Bold letters show the cases where Alice's and Bob's states should match.

Alice's bit	0	1	1	0	1	0	1
Alice's basis	**Z**	Z	**Z**	Z	X	**X**	**Z**
Alice's state polarization	V	H	H	V	A	D	H
Eve's basis	Z	X	X	Z	X	Z	X
Eve's state polarization	V	D	D	V	A	H	D
Bob's basis	**Z**	X	**Z**	X	Z	**X**	**Z**
Bob's state polarization	V	D	V	A	H	D	H
Sifting							
Shared secret key	0	⋯	1	⋯	⋯	0	1
Errors in key	⋯	⋯	×	⋯	⋯	⋯	⋯

(1) **Quantum communication**: Encoding is randomly done in Z and X bases. The emitter sends $|H\rangle$ and $|V\rangle$ uniformly in the Z basis, while in the X basis, it only emits $|D\rangle$. The receiver measures in X or Z bases with respective probabilities p_X^B and $p_Z^B = 1 - p_X^B$. Basis choice and measurement outcome are recorded.
(2) **Sifting**: Both parties announce their chosen bases for each event. Z basis events are used to generate the raw key, while X basis events are utilized to estimate the presence of an eavesdropper. This step concludes after collecting a predetermined number of raw key bits.
(3) **Post processing**: An error correction algorithm is applied to the block of bits by both parties, during which some bits may be disclosed. Privacy amplification is applied to the block of bits to obtain a secret key.

In the original BB84 protocol, the probabilities p_X^B and p_Z^B were fixed at 50 %, but various protocols and experimental setups can benefit from asymmetric measurement choices. For instance, in the simplified BB84 protocol, one basis monitors for eavesdropping while the other generates the key. Ideally, the monitoring basis measurements should be the minimal value that still allows for a complete monitor of the channel.

For educational purposes focused on understanding the experimental implementation of secure communication through quantum key distribution (QKD), a detailed description of error correction and privacy amplification was omitted. More information and the security analysis can be found in Ref. 10.

III. EXPERIMENTAL IMPLEMENTATION

The objective of this setup is to be practical, compact, and easy to construct. It enables a straightforward experiment for characterizing the setup, providing insights into the protocol's functionality without complete implementation. Additional equipment and effort can then be employed to implement the fully functioning protocol.

We selected the wavelength of 850 nm for the experiment due to its combination of efficient single-photon detection capabilities and the availability of commercial products operating at this wavelength.

This setup is divided into two parts as seen in Appendix A, two optical breadboards of 60 × 60 cm^2 (Thorlabs, B6060A), the emitter, and the receiver. These breadboards were selected because they were already available in our laboratory but smaller breadboards could be used. The emitter is capable of sending weak coherent pulses[11] in three different polarization states ($|H\rangle$, $|V\rangle$, $|D\rangle$). The receiver in turn is capable of measuring on two different bases, Z and X.

A. Emitter

The goal of the emitter is to create three different quantum states. These will be weak coherent states with a chosen average number of photons per pulse and a chosen polarization. All states will have the same average number of photons with different polarization, $|H\rangle$, $|V\rangle$, and $|D\rangle$.

As seen in Fig. 1, the pulses are generated by directly modulating the vertical-cavity surface-emitting laser (VCSEL) (Roithner, VC850M2-MODULE) using a function generator (FC) (AIM-TTI, TG330). We opted for these components as they were readily available in the laboratory. Alternatively, a simple 850-nm laser and any function generator or driver capable of producing pulses could suffice. The pulse length and number of photons depend on different experimental parameters and will be explained later.

The pulses are directed through a polarization beam splitter (PBS) (Thorlabs, PBS102), with the reflected power monitored by a power meter (Thorlabs, S120VC). This monitoring is used to estimate the number of photons emitted. The transmitted light is horizontally polarized and focused into an electro-optic modulator (EOM) (Thorlabs, EO-AM-NR-C1) with the input polarization properly aligned with respect to the crystal axes. This allows a fast (kHz) and active choice of polarization modulation.

While this setup requires a high-voltage amplifier (HVA) (Thorlabs, HVA200) to operate, an alternative option is the resonant EOM (Thorlabs, EO-PM-R-20-C1), which eliminates the need for a high-voltage amplifier.

The EOM creates distinct polarization states by applying varying voltages at the input. The specific voltage values required for the three different states necessary for the protocol depend on the alignment of the EOM crystal, which functions as a variable waveplate, effectively rotating the polarization of the light passing through it.

To achieve the desired polarization states within the available voltage range, a quarter-wave plate (QWP) (Thorlabs, WPQSM05-850) followed by a half-wave plate (HWP) (Thorlabs, WPHSM05-850) and another QWP can be employed to correct the output states of the EOM to match the targeted ones, simplifying the alignment. Additionally, due to our laser spot size being larger than the aperture of the EOM, we opted to utilize lenses (Thorlabs, LA1257-B) to minimize losses in this component.

These voltages are supplied by an arbitrary function generator (Agilent, 33250A), triggered by the first function

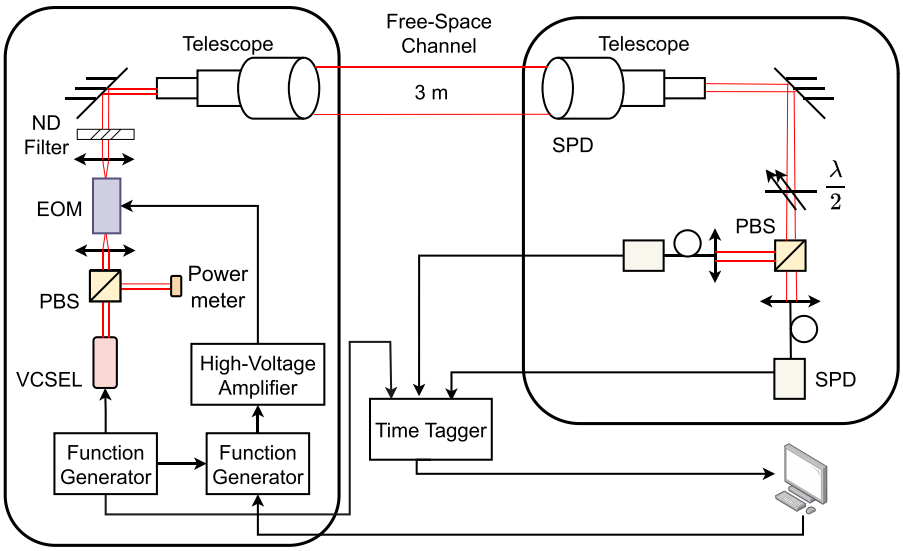

Fig. 1. Simplified setup. Black arrows illustrate signal propagation between the devices. EOM: electro-optical modulator; ND filter: neutral density filters; PBS: polarizing beam splitter; SPD: single photon detector; VCSEL: vertical-cavity surface-emitting laser; $\lambda/2$: half-wave plate.

generator, and the high-voltage amplifier. Alternatively, other function generators can be utilized if they allow the adjustment of the output voltage for each pulse and can be triggered externally. This flexibility enables encoding any bit sequence into photon polarization using the Z basis or the state in the X basis.

Figure 2 illustrates the electrical pulses employed for modulating the devices. The blue dashed pulses represent the modulation of the EOM, responsible for polarization rotation. In this depiction, two distinct states are evident: the high voltage maintains horizontal polarization, while the low voltage pulse rotates it to a vertical orientation. Any slight distortion observed in the figure is attributable to impedance mismatch.

The purple solid pulses are utilized to modulate the VCSEL to switch the laser on and off. The synchronization shown in the figure demonstrates the simultaneous modulation of these two types of pulses: blue dashed line for polarization control and purple solid line for laser activation. This

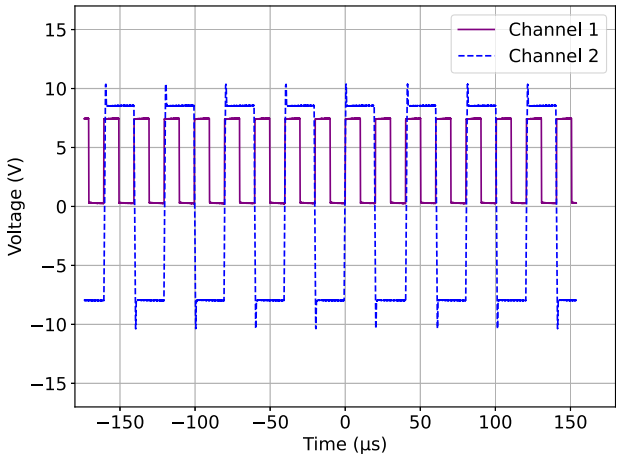

Fig. 2. (Color online) Electrical pulses seen in the oscilloscope. The purple solid pulse (channel 1) is used to modulate the VCSEL. The blue dashed pulse (channel 2) is used to modulate the EOM to encode information in the pulses.

synchronization enables independent polarization control for each light pulse. In this case, the pulse duration was 10 μs and the repetition rate was 50 kHz.

Subsequently, the photons pass through neutral density filters (Thorlabs, NE50A) to adjust the average photon count per pulse to the desired value before being emitted into the free-space channel via a telescope (Thorlabs, GBE03-B). Filter selection depends on the input power and the specific parameters of the targeted weak coherent pulse and will be explained later.

Alternatively, it is also possible to implement a less costly approach, removing the EOM from the setup as seen in Fig. 3. Instead of one laser, three would be used. Only one laser would be turned on at any time and the path taken by the light would create the respective state. To create the $|H\rangle$ and $|V\rangle$ states, only a PBS would be required. To create the $|D\rangle$ state, a PBS followed by a HWP can be used. This way, the state choice would be done by choosing which laser to turn on instead of by active modulation of the light. The different paths would then be recombined using a 50/50 beam splitter (BS) (Thorlabs, BS011) and the rest of the emitter would work as in the active approach.

This approach has not been tried in the setup at the moment but it is a common approach for emitter setups.[12] This method brings security risks as the lasers can have manufacturing differences (spatial mode, frequency…) and an eavesdropper might take advantage of those but for this work, it can be a solution.

Given that both the emitter and the receiver are situated within the same room, the free-space channel is defined as the distance between the telescopes at each end. While a well-collimated beam and a short free-space channel may render the use of telescopes optional, their inclusion enables easy scalability of the channel length by adjusting the distance between optical tables. The emitter can be seen in Fig. 8 in Appendix A.

B. Receivers

The receiver measures the incoming states on one of two bases. By calculating the QBER, we can detect the presence

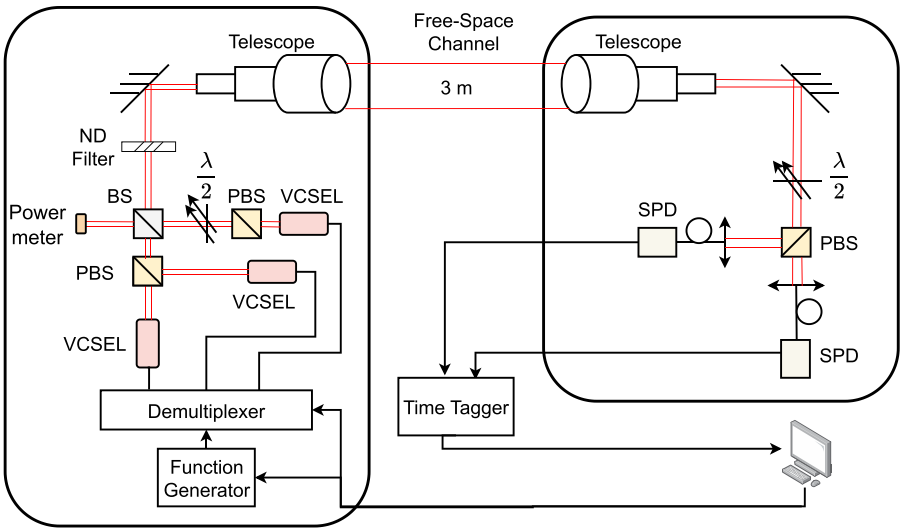

Fig. 3. Simplified setup with a less costly emitter. Black arrows are electrical connections. EOM: electro-optical modulator; ND filter: neutral density filters; PBS: polarizing beam splitter; SPD: single photon detector; VCSEL: vertical-cavity surface-emitting laser; $\lambda/2$: half-wave plate.

of potential eavesdroppers (Eve) and generate secret keys. For educational purposes, it is sufficient to measure on a single basis at a time, rather than switching between two bases. Under these conditions, we can still calculate a QBER for each basis individually and simulate the presence of an eavesdropper.

To accomplish this, as seen in Fig. 1, the light is captured by a telescope and directed through a HWP, followed by a PBS. The angle in the HWP will define if the measurement is on the Z basis or the X basis. Each output of the PBS is then coupled to a fiber and a single-photon detector (SPD) (Excelitas, SPCM-AQRH-10).

The arrival time of the photons is recorded using a time tagger (Swabian Instruments, Time Tagger 20), which offers precision beyond the requirement; a more affordable option such as an electronic circuit or a field programmable gate array microcontroller can be used as described in Refs. 13 and 14. These would be connected to the detectors and would record the time between the trigger signal and both detectors measurements. Additionally, the trigger pulse modulating the laser should be connected to the time tagger for post-processing of the measured data.

The setup can be improved by allowing basis choice in the receiver. To do this with only two detectors, we can use time multiplexing to separate in time the measurements on one basis from the measurements on the other basis. As seen in Fig. 4, we start by adding a non-polarizing BS that will passively make the basis choice because the polarization of photons in one path will be rotated by $\pi/4$. These polarization-rotated photons are also sent through a fiber optic cable to delay their arrival at the detector. The two paths are recombined with a polarizing beamsplitter that measures their polarization state. So now the pulses that arrive without a delay have been measured in the Z basis, while the pulses that arrive with a delay have been measured in the X basis. The size of the delay, which will be discussed in Sec. III C, is sufficient to allow the paths to be distinguished, while not causing overlap between adjacent pulses.

A photograph of the setup used can be seen in Fig. 9 in Appendix A.

C. Parameter selection

To implement the protocol, we need to define the pulse width of the coherent states, the pulse width of the signal modulating the EOM, the repetition rate, the average number of photons, and the time delay for the complete receiver.

The repetition rate will be limited by the high-voltage amplifier as it has a 1-MHz bandwidth. We chose a repetition rate of 50 kHz but a higher or lower value can be chosen.

For the simplified receiver, the pulse width can be chosen freely to be less than the repetition period. Our function generator can only generate square waves, resulting in a pulse width equal to half of the repetition period, 10 μs.

To determine the average number of photons in the weak coherent pulse, it is essential to thoroughly characterize the losses. By measuring the initial power and accounting for losses through various components, we can estimate the average number of photons detected by the receivers.

In a secure implementation of the protocol, the average number of photons emitted from the emitter should be low. However, for educational purposes, we may increase this value to simplify the setup, as even with large values of loss, the number of photons arriving at the detector can replicate what would be observed in a secure QKD experiment (single photon regime). This may leave the communication open to attacks.

This means that the use of a non-optimal fiber (or other sources of loss as misalignment) would still allow for the experimental implementation as it would only require an increase in the number of photons sent, to compensate for the extra loss.

Defining P as the initial laser power, ΔT as the pulse width, E_p as the photon energy for this wavelength, and η_s and η_f as the loss of the setup, including here all the losses (components, coupling, channel), and the loss of the filters respectively, the average number of photons measured, $|\alpha|^2$ will be given by

$$|\alpha|^2 = \frac{P\Delta T}{E_p} 10^{-\eta_s+\eta_f/10}. \tag{2}$$

From Eq. (2), the necessary filter loss in dB can be determined. The parameters used in this work were: $\Delta T = 10\,\mu s$, $P = 92\,\mu W$, $\lambda = 850$ nm, $\eta_s = 12.2$ dB (including all the

channel and receiver losses), and $\eta_f = 80$ dB. These values result in a predicted $|\alpha|^2_{Alice} = 39.3$ (weak coherent state emitted by Alice) and $|\alpha|^2_{Bob} = 2.35$ (weak coherent state arriving at the detectors), while the measured value was 2.30 ± 0.05. The measured probabilities of different photon counts were as follows: "0" with a probability of 0.11, "1" with 0.23, "2" with 0.25, and "3" with 0.19.

To implement the complete receiver, time multiplexing for detections is essential. Measurements in one basis must be temporally separated from those in the orthogonal basis to allow for efficient processing. Ideally, this requires a delay larger than the optical pulse width to prevent overlap between the detection windows of delayed and not delayed photons, facilitating the differentiation of measurement bases based on photon arrival time.

To achieve this with only two detectors, measurements on the X basis are deliberately delayed by routing the pulses through a long optical fiber. Despite the lack of refractive index information for the fiber used, typical values generally fall within the range of [1.45, 1.48]. Utilizing an available 2590-m multi-mode optical fiber yields an expected delay of approximately [12.52, 12,77] μs (around 5 ns per meter of fiber). As the number of photons can be adapted in this demonstration, the loss in the fiber is not a concern even though there are more losses than predicted because it is not optimized for the wavelength used.

To verify this delay and assess time-multiplexed detection, a low-photon-count pulse with diagonal polarization is emitted from the emitter. For experimental validation, the BS in the setup (Fig 4) is replaced with a PBS to ensure minimal overlap between delayed and not delayed beams. The horizontal component of the polarized beam traverses a second PBS, reaching only detector 1 after passing through a filter to simulate losses in the alternate path, due to the fiber used. Conversely, the vertical component is directed into the optical fiber for temporal delay. Subsequently, a HWP rotates the polarization at the fiber output to horizontal, guaranteeing that photons exclusively reach detector 2 via a second PBS.

Consequently, clicks registered in detector 1 originate from the non-delayed signal, while those in detector 2 result from the delayed signal.

In Fig. 5, the distribution of photon arrival times relative to the trigger is depicted. Two distinct uniform distributions, centered on different values, are evident. The first, approximately 5.05 ± 0.10 μs, corresponds to the beam directly transmitted to the detector. The second, because it is delayed more than 10 μs, appears in the following pulse statistics and is centered around 17.80 ± 0.10 μs. Bars in gray are clicks in the second detector, while those in black are clicks in the first detector. Both distributions have the same time duration of 10.00 ± 0.10 μs but the delayed distribution has a higher number of photons. This is due to the filter used to mimic the losses in the fiber. The average delay between the two distributions is calculated to be 12.75 ± 0.20 μs.

The observed overlap between the distributions can be attributed to selecting a delay longer than the pulse width. This overlap can be accounted for and filtered out in the post-processing of the data to achieve better discrimination between the basis.

IV. RESULTS AND ANALYSIS

With the previously described setup, communication can be implemented. For simplicity, pre-determined messages can be encoded into the quantum states. The most straightforward message consists of a repeating string of alternating 0 and 1 s throughout the communication ("0101010101…").

A. Simplified receiver

Using the simplified received shown in Fig. 1, the message is transmitted using the quantum states and detected using the HWP set to 0° for the Z basis and 22.5° for the X basis. Since the states are orthogonal, only one detector should register a click for each state sent.

The single photon detectors create an electric pulse when an event is registered. This pulse will generate an event in the connected channel of the time tagger. This way, all the information is registered in the output file of the time tagger, which includes the timestamp, the channel identification, and an error check parameter to access the correct use of the time tagger (missed events). If the FPGA is used instead, the same logic applies.

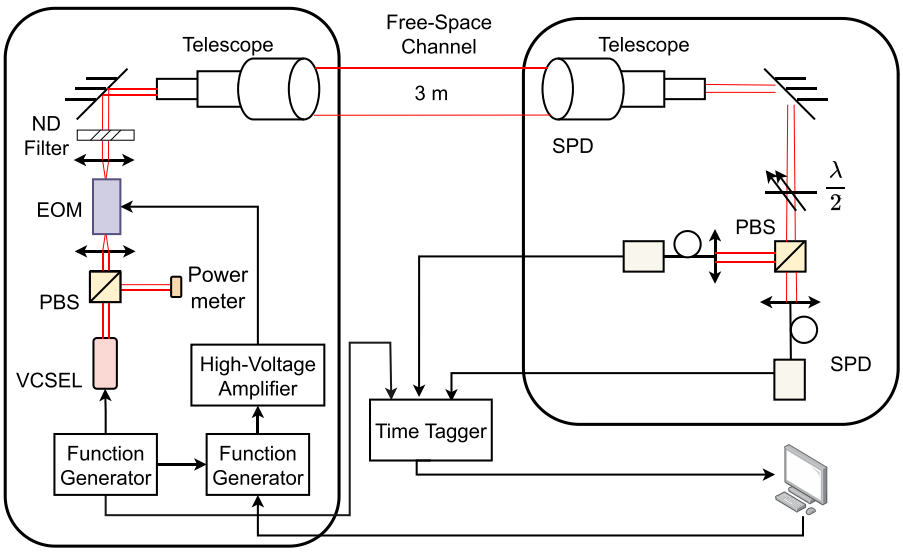

Fig. 4. Complete receiver setup. Black arrows are electrical connections. BS: beam splitter; EOM: electro-optical modulator; ND filter: neutral density filters; PBS: polarizing beam splitter; SPD: single photon detector; VCSEL: vertical-cavity surface-emitting laser; $\lambda/2$: half-wave plate.

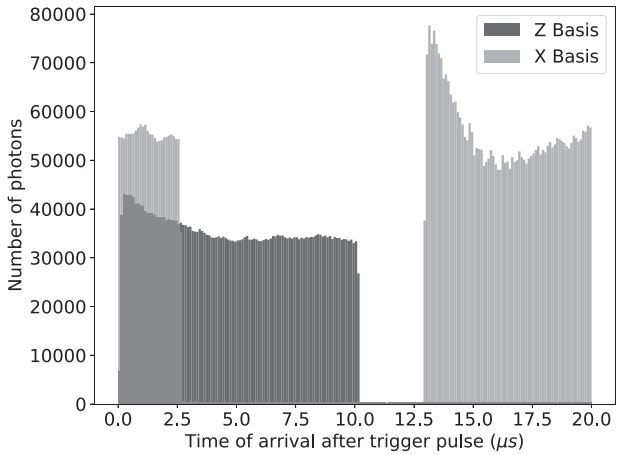

Fig. 5. Histogram of the time of arrival of the photons after the trigger signal. Detector 1 corresponds to the Z basis (in black), while detector 2 corresponds to the X basis (in gray).

TAG #	CHANNEL	TIMESTAMP (ps)	MISSED EVENTS
0	-4	1266764923594	0
1	4	1266774988163	0
2	1	1266777766100	0
3	1	1266777921915	0
4	1	1266780682617	0
5	1	1266782424847	0
6	-4	1266785051746	0
7	4	1266795117875	0
8	2	1266798067729	0
9	2	1266799731859	0
10	-4	1266805178871	0
11	4	1266815240998	0
12	1	1266816548711	0
13	1	1266817793523	0
14	-4	1266825301338	0

Fig. 6. Example of events registered by the time tagger. The "Tag" column registers the event number. The "Channel" column identifies in which channel the event occurred and which device produced the event. The "Timestamp" registers the timing of the event. The "Missed events" column is used to identify problems in the time tagger.

For the Z basis measurement, if the detector connected to the horizontal output of the PBS registers a click, the state sent was $|H\rangle$, while a click in the other detector indicates the state was $|V\rangle$. For educational purposes, it may be advantageous to define a higher average number of photons to ensure consistent detector clicks, simplifying the subsequent analysis. For the X basis, the same logic applies.

In Fig. 6, an illustration of events captured by the time tagger is provided. Channel 4 monitors the modulation of the VCSEL, where event 4 represents a rising edge, indicating the onset of a pulse, while event –4 means a falling edge, denoting the end of the pulse duration. Therefore, the pulse is considered active between a 4 and a –4. The SPD corresponding to the horizontal polarization is connected to channel 1, so its clicks correspond to bit 0. Similarly, the SPD corresponding to the vertical polarization is connected to channel 2, so its clicks correspond to bit 1. When more than one photon is detected in a pulse, if their polarizations do not agree, a guess can be made of the bit sent based on the majority of the detections.

Using this logic, from Fig. 6, the string "010" is recovered, which matches the bits sent for this fraction of the message. By collecting data for 10 s, a message of 500 kbit is sent by Alice and recovered by Bob. By comparing this message to the original, counting the number of different bits, and dividing by the size of the message, the QBER can be found. We measure the QBER to be $(2.5\% \pm 0.4\%)$ on the Z basis, while on the X basis, it is $(2.11\% \pm 0.14\%)$. These error rates are acceptable but could be reduced by addressing the impact of dark counts.

The electrical pulse is relatively wide, limited by the function generator available, and consequently, the detection window, the period during which signals are observed, is also broad. As a result, there's a higher likelihood of dark counts affecting the measured results. To improve this, one could lower the dark counts or reduce the pulse width and the detection window.

While this implementation did not focus on optimizing the SKR, it is still an important figure of merit. As we did not implement an error correction code and privacy amplification protocol we estimated the secret key size using the upper bound provided in Ref. 2.

As we used a weak coherent state with a high number of photons, the corresponding secret key rate is 0. The communication is open to attacks as Eve can capture a few photons each round and recover the entire message. For a secure implementation, the number of photons sent by Alice has to be reduced, and by using a Python package created to estimate the SKR of the simplified BB84 for space-based communication, provided in Ref. 16, we arrived at the optimal secret key rate of 75 bps for an average photon number of 0.87 and parameters reported in Appendix B. This value can be easily improved by increasing the source rate or the communication time window.

Comparing these results to the ones reported in Ref. 2, it can be seen that this setup provides a much lower SKR. For the loss value measured in this experiment and a 625-MHz source, they achieve a QBER of around 3 % and a SKR of around 8 kbps where the result is mainly limited by the detectors used as for low loss values their SKR saturates.

Recent works have shown a SKR of 115.8 Mbps over 10-km standard fiber for a source of 2.5 GHz, proving that high-rate quantum key distribution is possible.[15] There are also commercially available products like the Clavis XGR QKD platform from ID Quantique operating with a 1 Gbit source and generating secret keys at around 12 dB of loss at a rate of 400 kbps.[17]

B. Complete receiver

If the complete receiver is used, the message sent has to have bits encoded in both bases, closer to what is used in a secure QKD setup. The procedure is similar to the simplified receiver; we obtain the data from the time tagger and must recover the message. In this receiver, we have to recover which basis was chosen and the message sent. To recover the basis choice, we look at the number of events delayed and not delayed. This means that the timestamp data shown in Fig. 6 has to be used. If there are more delayed events, events 10 μs after an event in channel 4, the basis chosen is X, and if there are more photons without delay, events between the timestamp of channel 4 and 10 μs after, the basis chosen is Z.

After, we can recover the message as done previously, looking into which detector clicked more. The basis choice can then be compared to Alice's choice and only the events with a basis match are kept. Finally, the QBER is calculated in the same way, by comparing both messages.

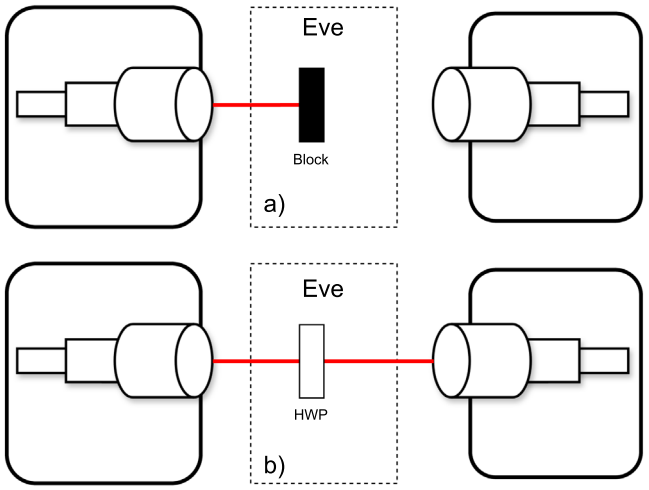

Fig. 7. Design of Eve simulation experiments. (a) The free space channel is blocked. (b) A HWP is used to rotate the basis.

This is a simplified way to estimate the QBER where the whole message is shared between Alice and Bob, not just a fraction. This is followed again by the post-processing to generate the secret key.

C. Simulating Eve

To simulate the presence of Eve, one can create a very simple experiment. If we periodically block the free space channel during the communication phase, we can simulate an attack where Eve removes photons from the channel. This will stop all detection, leading to an increase in the QBER. For example, if for no detection we assume bit 0 was sent, the message recovered while Eve is blocking the channel would be an infinite string of 0 s.

Another possible approach is to use a HWP to rotate the state polarization. If we use an HWP at 22.5°, we can simulate an Eve that always chooses the wrong measurement basis, increasing the QBER to around 50% as the message recovered would be random (the measurement is made on X basis while the state was encoded on the Z basis, for example). This gives intuition on an intercept and resend attack where the basis choice is always wrong. The change in the experimental setup can be seen in Fig. 7.

These simple experiments show that Eve's presence in the channel leads to an increase in the QBER that can be detected aborting the communication and discarding the key generated as it was not secure.

Table II. Equipment prices in February 2024 except for the power meter, FPGA, and the resonant EOM, which the price corresponds to November 2024.

Designation	Distributor	Model	Qt	Unit price ($)
VCSEL	Roithner	VC850M2	1	75
FC	AIM-TTI	TG330	1	500
PBS	Thorlabs	PBS102	2	222
BS	Thorlabs	BS011	1	205
EOM	Thorlabs	EOAM-NR-C1	1	2999
HVA	Thorlabs	HVA200	1	3000
Arbitrary FC	Agilent	33250A	1	2975
ND Filter	Thorlabs	NE50A	3	60
Telescope	Thorlabs	GBE03-B	2	576
HWP	Thorlabs	WPHSM05-850	1	507
SPD	Excelitas	SPCM-AQRH-10	2	3110
Power meter	Thorlabs	PM120D	1	1556
Time Tagger	Swabian	Time Tagger 20	1	10 000
FPGA	Digilent	Arty S7	1	125
Resonant EOM	Thorlabs	EO-AM-R-20-C1	1	3482

Table III. Parameters used for SKR optimization.

Parameter	Value
Signal intensity	0.79
Probability of sending signal	0.75
Decoy intensity	0.02
Probability Alice sends an Z basis signal	0.5
Probability Bob measures an Z basis signal	0.5
Loss	12 dB
Communication time	10 s
Correctness parameter (ϵ_C)	10^{-15}
Secrecy parameter (ϵ_S)	10^{-9}
Intrinsic Quantum Bit Error Rate	10^{-3}
Extraneous count probability	10^{-3}
After pulse probability	10^{-3}
Source repetition rate	100 kHz

V. CONCLUSION

In summary, this work has demonstrated a practical, compact, and cost-effective QKD setup suitable for undergraduate tutorial demonstrations. By using weak coherent pulses, the simplified three-state BB84 protocol, and time multiplexing, the

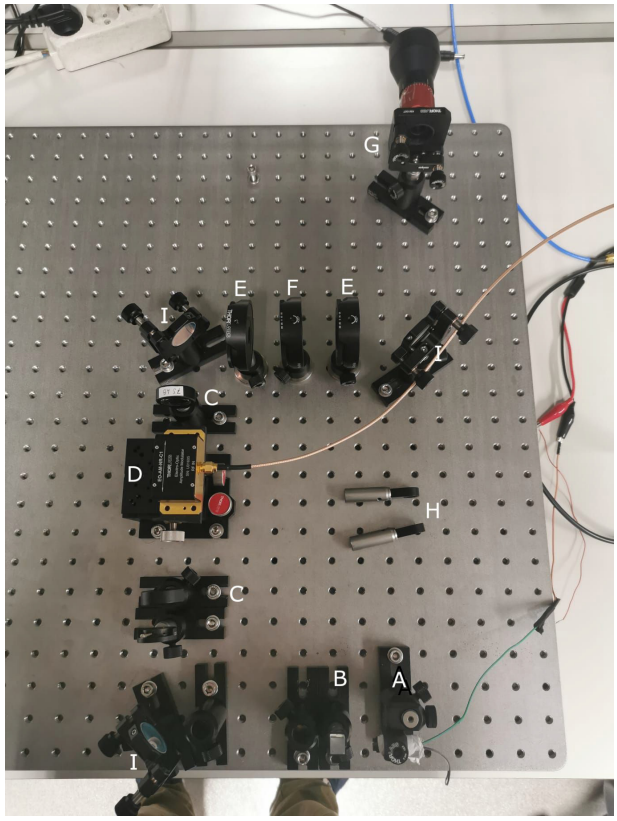

Fig. 8. Photo from the emitter setup. (a) VCSEL. (b) PBS. (c) Lens. (d) EOM. (e) QWP. (f) HWP. (g) Telescope. (h) ND filters. (i) Mirror.

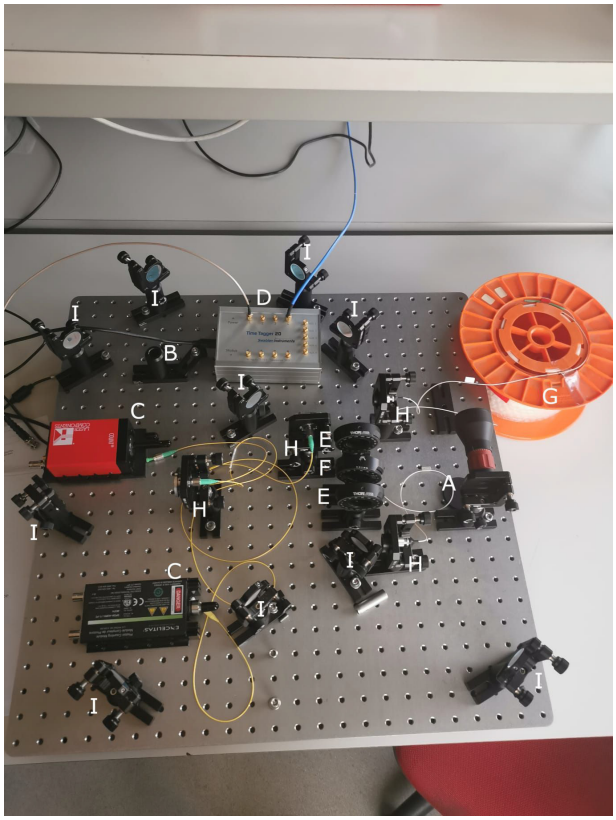

Fig. 9. Photos from the complete receiver setup. (a) Telescope. (b) PBS. (c) SPD. (d) Time tagger. (e) QWP. (f) HWP. (g) Delay fiber. (h) Fiber couplers. (i) Mirror.

complexity of the setup can be reduced and QKD demonstrations can be easily implemented, making the setup more accessible and manageable within educational environments.

ACKNOWLEDGMENTS

The authors acknowledge insightful discussions and valuable feedback provided by our colleagues Preeti Yadav, Gonçalo Teixeira, and José Senart, whose contributions significantly enhanced the depth and clarity of this paper. E.Z.C. acknowledges funding by FCT/MCTES—Fundação para a Ciência e a Tecnologia (Portugal)—through national funds and when applicable co-funding by EU funds under the project Nos. UIDB/50008/2020 and 2021.03707. CEECIND/CP1653/CT0002. The authors thank the support from the European Commission (EC) through project No. PTQCI (DIGITAL-2021-QCI-01).

AUTHOR DECLARATIONS

Conflict of Interest

The authors have no conflicts to disclose.

APPENDIX A: EQUIPMENT PRICE

Here we compile the prices and quantities of the essential components to implement the emitter and complete receiver. It does not include all the equipment necessary, i.e., fibers, mechanical supports, and more.

Table II shows the prices of the equipment used as well as the price of the cheaper solutions. The FPGA can replace the use of both FC and the time tagger. The resonant EOM does not require an HVA to function.

In Figs. 8 and 9, the experimental setups used can be seen.

APPENDIX B: PARAMETERS FOR SKR OPTIMIZATION

The parameters used for the optimization of the SKR for this setup are shown in Table III.

Note: This paper is part of the special issue celebrating the International Year of Quantum Science and Technology.
[a)]ORCID: 0009-0004-1924-0407.
[b)]ORCID: 0000-0002-6276-4976.
[c)]emmanuel.zambrinicruzeiro@gmail.com, ORCID: 0000-0003-3418-9131.

[1]C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theor. Comput. Sci. **560**, 7–11 (2014).
[2]F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Simple and high-speed polarization-based QKD," Appl. Phys. Lett. **112**(5), 051108 (2018).
[3]X. Ma, B. Qi, Y. Zhao, and H. K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**(1), 012326 (2005).
[4]A. Bista, B. Sharma, and E. J. Galvez, "A demonstration of quantum key distribution with entangled photons for the undergraduate laboratory," Am. J. Phys. **89**(1), 111–120 (2021).
[5]B. J. Pearson and D. P. Jackson, "A hands-on introduction to single photons and quantum mechanics for undergraduates," Am. J. Phys. **78**(5), 471–484 (2010).
[6]W. Rueckner and J. Peidle, "Young's double-slit experiment with single photons and quantum eraser," Am. J. Phys. **81**(12), 951–958 (2013).
[7]E. J. Galvez, "Resource letter SPE-1: Single-photon experiments in the undergraduate laboratory," Am. J. Phys. **82**(11), 1018–1028 (2014).
[8]J. S. Johnson, M. R. Grimaila, J. W. Humphries, and G. B. Baumgartner, "An analysis of error reconciliation protocols used in quantum key distribution systems," J. Defense Model. Simul. **12**(3), 217–227 (2015).
[9]R. Renner, "Security of quantum key distribution," Int. J. Quantum Inform. **06**(01), 1–127 (2008).
[10]A. Boaron, B. Korzh, R. Houlmann, G. Boso, C. C. W. Lim, A. Martin, and H. Zbinden, "Detector-device-independent quantum key distribution: Security analysis and fast implementation," J. Appl. Phys. **120**(6), 063101 (2016).
[11]Jean-Pierre Gazeau, *Coherent States in Quantum Physics*, 1st ed. (Wiley, 2009).
[12]H. Ko, B. S. Choi, J. S. Choe, K. J. Kim, J. H. Kim, and C. J. Youn, "High-speed and high-performance polarization-based quantum key distribution system without side channel effects caused by multiple lasers," Photonics Res. **6**(3), 214–219 (2018).
[13]D. Branning, S. Bhandari, and M. Beck, "Low-cost coincidence-counting electronics for undergraduate quantum optics," Am. J. Phys. **77**(7), 667–670 (2009).
[14]E. J. Galvez, C. H. Holbrow, M. J. Pysher, J. W. Martin, N. Courtemanche, L. Heilig, and J. Spencer, "Interference with correlated photons: Five quantum mechanics experiments for undergraduates," Am. J. Phys. **73**(2), 127–140 (2005).
[15]Wei Li *et al.*, "High-rate quantum key distribution exceeding 110 Mb s^{-1}," Nat. Photonics **17**(5), 416–421 (2023).
[16]The code is available on the Github page https://github.com/QuLab-IT/QuantSatSimulator.git.
[17]See https://www.idquantique.com/quantum-safe-security/products/clavis-xgr-qkd-platform/ for Clavis XGR QKD.