IL NUOVO CIMENTO **48 C** (2025) 171
DOI 10.1393/ncc/i2025-25171-5

COMMUNICATIONS: SIF Congress 2024

Decoy-state quantum key distribution over long-distance optical fiber

GIULIA GUARDA([1])([2])(*)

([1]) *European Laboratory for Non-Linear Spectroscopy (LENS) - 50019 Sesto Fiorentino, Italy*
([2]) *Istituto Nazionale di Ottica del Consiglio Nazionale delle Ricerche (CNR-INO) - 50125 Firenze, Italy*

received 27 January 2025

Summary. — Long distance quantum key distribution links are essential for the development of a widely spread fiber-based quantum network. For instance, it would allow for two remote users to communicate securely without the need for a trusted intermediate node. In this work, we focus on enhancing the receiver side of a quantum key distribution system, deploying state-of-the-art superconducting nanowire single photon detectors with ultra low dark count (< 1 Hz) and very high efficiency ($> 90\%$), achieving a secure key distribution over a 55 dB losses channel with 0.6 bps rate. This result opens new possibilities for long distance secure communications.

1. – Introduction

Quantum key distribution allows the distribution of a random secret key between two or more users, exploiting the laws of quantum physics [1-3]. Quantum Key distribution can be implemented with different protocols, the most known and most widely used being the BB84 protocol [4]. Here, two parties, Alice and Bob, wish to share a secret key. To do so, they communicate both via a quantum and a classical channel. The quantum channel is one-way (from Alice to Bob) and here Alice sends the randomly encoded quantum states to Bob. The classical channel is two-way, and here the two parties perform the post processing algorithms. The unconditional security of the key that the two parties share at the end is ensured by the laws of quantum physics [1, 4, 5]. More specifically, the no-cloning theorem and Heisenberg's uncertainty principle. The no-cloning theorem states that it is impossible to make an identical copy of an unknown quantum state. The uncertainty principle states that there is a precision limit with which certain properties can be measured.

(*) E-mail: guarda@lens.unifi.it

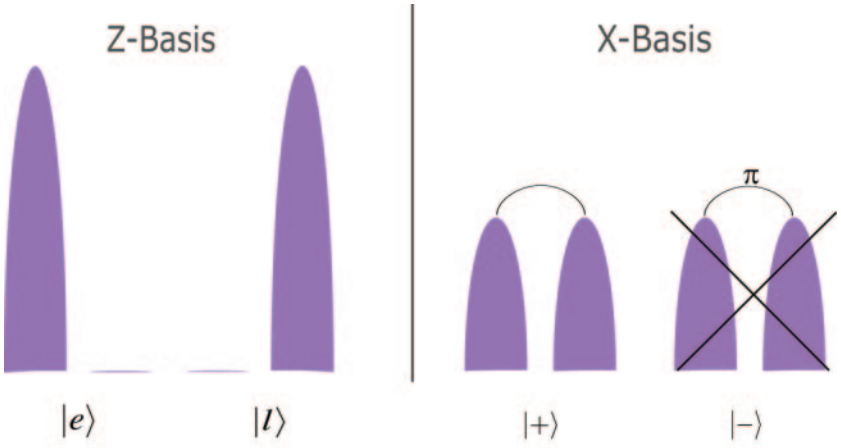

Fig. 1. – Visual representation of the encoding of the quantum states. Z-basis: here the states are labelled as "*early*" and "*late*" state, indicating their position in the time-bin. X-basis: a coherent superposition of the "*early*" and "*late*" states forms the orthogonal basis. Here the states are labelled as $|+\rangle$ and $|-\rangle$, referring to the relative phase between the two time-bins (0 or π). The state $|-\rangle$ is represented for completeness, however is crossed out as it is not generated.

The goal is to connect a long distance link using optical fiber [2]. Here, the main limitation comes from photon absorption in optical fibers [6]. One could adopt many different solutions to overcome the problem. It is possible to act on the protocol and use a more efficient one, for example implementing a protocol with high dimensional states [7]. It is also possible to increase the generation rate on the transmitter's side, sending more quantum states per second [8]. Additionally, one could improve the detection system on the receiver's side. Adopting all three solutions simultaneously would be the optimal idea, however, it might be challenging to realize experimentally. In this work, we focus on the receiver's side and use state-of-the-art superconducting nanowire single-photon detectors (SNSPD) with ultra-low dark count rates (<1 Hz) and high efficiency (> 90%). As a result, we are able to reduce the quantum bit error rate (QBER), hence enabling two main results. First, we are able to distribute a secure key for longer channels, as the ultra-low noise level of these detectors degrades less the measurements. Second, it is possible to achieve a higher secure key rate (SKR) for every channel, compared to less-performing detectors.

2. – Methods

We implement a three-state efficient BB84 protocol using time bin and phase encoding. The two adopted encoding bases are referred to as Z-basis and X-basis. Here, a time slot (1.68 ns long) is made of two different time bins with an 800 ps time delay separating them [9-11]. Each quantum state consists of two time bins: early and late. The logical bits zero and one can be encoded in the two bases by considering both the temporal component and the phase of the pulses. Mathematically, they are represented as:

$$|0\rangle_{\mathrm{z}} = |\gamma\rangle_{\mathrm{early}}\,|0\rangle_{\mathrm{late}}\ ;\ |1\rangle_{\mathrm{z}} = |0\rangle_{\mathrm{early}}\,|\gamma\rangle_{\mathrm{late}};$$

$$|0\rangle_{\mathrm{x}} = \frac{|0\rangle_{\mathrm{z}} + |1\rangle_{\mathrm{z}}}{\sqrt{2}} \; ; \; |1\rangle_{\mathrm{x}} = \frac{|0\rangle_{\mathrm{z}} - |1\rangle_{\mathrm{z}}}{\sqrt{2}} \; . \tag{1}$$

Here γ represents the amplitude of the weak coherent state. In the Z-basis encoding, depending on whether it is on the early or late time bin, it encodes the logical bits zero or one, respectively. In the X-basis encoding, there is a coherent superposition of the quantum states in the Z-basis and here the information on the phase determines the encoding of the logical bits zero and one. In contrast to the standard BB84 protocol, where both states in the X-basis —$|0\rangle_{\mathrm{x}}$ and $|1\rangle_{\mathrm{x}}$— are generated, in our scheme only the state $|0\rangle_{\mathrm{x}}$ is produced (see fig. 1). This does not harm the security of the protocol [12, 13], however, the X-basis states can be used for security checks only and not for the key generation. The advantages come both in the decreased complexity of the states' generation and also in the need for just two detectors instead of three.

Efficiently generating single photons for use as quantum states remains a significant challenge. Single-photon sources operate at lower repetition rates compared to sources based on attenuated laser pulses [14], which limits the key rate and the maximum achievable communication distance. For this reason, attenuated laser sources are the most commonly chosen method for implementing discrete-variable QKD. Attenuated lasers emit coherent states that follow a Poissonian distribution for the mean photon number per pulse. Although the signal is strongly attenuated below the single-photon level, 0.16 or 0.20 mean photons per pulse, the probability of multi-photon events is reduced but not eliminated. As a result, some pulses may contain two or more photons. These multi-photon events make the system vulnerable to photon-number splitting (PNS) attacks, in which an eavesdropper intercepts one photon from a multi-photon pulse and stores it [1]. Since no measurement is performed on the stored photon, no errors are introduced, and Bob, the receiver, remains unaware of the interception as he still detects one photon [1]. To mitigate the risk of PNS attacks, the most common strategy is to randomly vary the intensity of the pulses, a technique known as the decoy-state method [1]. By reconstructing the photon-number statistics at the end of the protocol, any deviations caused by eavesdropping can be identified, thus ensuring the security of the quantum communication [1].

The upper bound for the secret key length (l) in finite block-size regime is bounded to [15]:

$$l \leq s^l_{Z,0} + s^l_{Z,1}(1 - H_2(\phi^u_Z)) - \lambda_{EC} - \lambda_{sec} - \lambda_{corr}. \tag{2}$$

In eq. (2), $s^l_{Z,0}$ and $s^l_{Z,1}$ are the lower bounds for vacuum and single-photon events. These bounds are estimated in the post-processing algorithms. $H_2(x)$ is the binary entropy, defined as $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$. ϕ^u_Z is the upper bound for the phase error rate, estimated from the interferometer's visibility as $\mathrm{vis}_{\mathrm{X}} = 1 - 2 \cdot \mathrm{QBER}_{\mathrm{x}}$, where QBER is the quantum bit error rate. As only one state is generated in the X-basis, the ϕ^u_Z parameter can only be estimated and not directly measured. λ_{EC} is the amount of disclosed bits during the error correction stage. λ_{sec} and λ_{corr} are functions of the security ($\epsilon_{sec} = 10^{-12}$) and correctness ($\epsilon_{corr} = 10^{-12}$) parameters in the form of: $\lambda_{sec} = 6\log_2(19/\epsilon_{sec})$ and $\lambda_{corr}\log_2(2/\epsilon_{corr})$. These parameters ensure that the key is secret and correct, with a probability of error less than 10^{-12}.

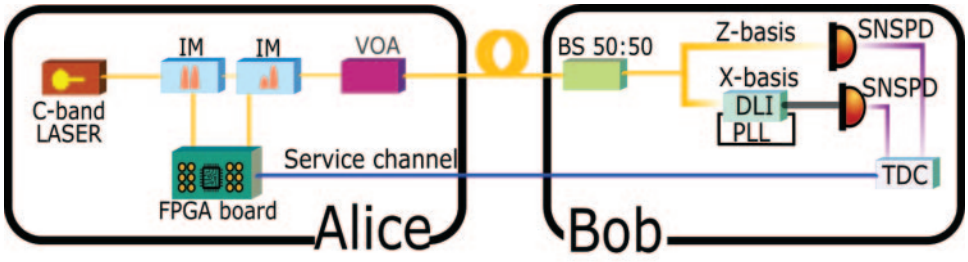

Fig. 2. – Experimental setup. ALICE: a C-band laser passes through two intensity modulators (IMs), both controlled by a field-programmable gate array (FPGA). The laser's intensity is reduced to the single-photon level using a variable optical attenuator (VOA). The quantum states are transmitted to Bob via a single-mode fiber, which serves as the quantum channel. The FPGA also provides clock synchronization. BOB: a 50/50 beam splitter (BS) randomly selects the detection basis. For Z-basis detection, the signal is directed to a superconducting nanowire single-photon detector (SNSPD). For X-basis detection, the signal passes through an imbalanced Mach-Zehnder interferometer (iMZI), which is stabilized using a phase-locked loop (PLL). The output is then detected with a second SNSPD. Data collection is managed by a time-to-digital converter (TDC).

3. – Experimental setup

Figure 2 shows the architecture of the setup used in this work. Alice, the transmitter, is embedded in a 2U rack box and it generates the quantum states. The states are generated with a repetition rate of 595 MHz, carving a continuous-wave laser at 1545.32 nm. The field programmable gate array (FPGA) drives two intensity modulators (IMs). The first IM carves the laser signal into the pulse sequence. For driving the IM, the FPGA generates an electrical signal following a pre-loaded binary sequence of length $l = 2^{13} - 1 = 8191$. This sequence determines the on-off pattern of the pulses. The second IM adjusts the intensity of the pulses using a three-level electrical signal. This adjustment fulfills two key roles. First, it ensures proper encoding by setting the intensity of pulses in the Z-basis to be twice that of the X-basis, as required by the normalization of the quantum state to 1. Second, it generates the two different intensity levels for signal and decoy states as requested by decoy-state method. This dual-modulation scheme provides precise control over both the temporal structure and the intensity of the pulses, enabling secure and efficient implementation of the protocol. The quantum states are encoded in the Z- and X-bases with probabilities $p_Z^A = 0.5$ and $p_X^A = 0.5$, respectively. Once the pulses are created, a variable optical attenuator (VOA) brings their intensity down to the single-photon level. Finally, the states are sent to the receiver end, Bob, via a single-mode optical fiber, *i.e.*, the quantum channel.

The receiver, Bob, is also embedded in a 2U rack box. The module is made of a 50/50 beam splitter for the random detection base choices. Here $p_Z^B = 0.5$ and $p_X^B = 0.5$ are set. The detection in the Z-basis goes straight to the superconducting nanowire single-photon detector (SNSPD), and the arrival time of the photon is recorded. For the detection in the X-basis, the quantum state has to pass through an imbalanced Mach-Zehnder interferometer (iMZI). Here the two pulses in the quantum state are overlapped by the delay line between the two arms of the interferometer, allowing for the phase measurement. The iMZI requires active stabilization, implemented with a phase-locked

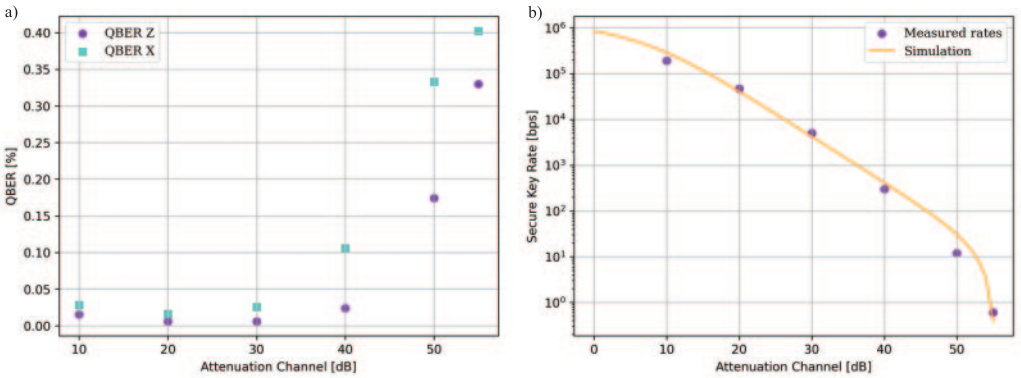

Fig. 3. – (a) Quantum bit error rate trend of the QBER as a function of the channel attenuation in both the Z-basis (purple circles) and X-basis (blue squares). (b) Secure key rate as a function of channel attenuation the orange line represents the expected SKR, the purple circles show the SKR corresponding to the acquired data for different channel attenuations.

loop (PLL). This consists of a monitor signal at 1550.00 nm entering from the iMZI output and counter-propagating with respect to the quantum states path, a piezo-controlled phase shifter, and an Indium Gallium Arsenide (InGaAs) photodetector. The laser is attenuated in such a way that the output power is at most −30 dBm. A proportional-integral-derivative (PID) controller, acting on the phase shifter, is in charge for keeping the phase difference of the two interferometer arms constant. As the PLL wavelength is just slightly different from the quantum states one, locking the phase of the monitoring signal enables concurrent phase locking for the quantum signal. Both the input and output port of the interferometer are equipped with a dense wavelength division multiplexer (DWDM) in charge for combining and dividing the two signals. The hardware is supported by an auto-tuning software that hinders drifts of the setup. However, in a fiber interferometer, the PID alone struggles to lock the interferometer onto a certain phase value for long time intervals (minutes or hours) due to the great instability of fiber-based devices. Typically, when it is observed that the PID begins to lose the optimal locking point, it is recalibrated manually. Our receiver is aided by an autotuning software, capable of recalibrating the interferometer each time the visibility value drops below a threshold, *i.e.*, the system can no longer extract a key. Based on a minimization algorithm, the drawback lies in the slow speed of this process; however, the automation of this step allows for data acquisition for potentially unlimited durations. At the output of the iMZI, the signal is sent to the SNSPD.

The detectors are made of niobium nitride (NbN), and their efficiency is optimized by the incorporation of a distributed Bragg reflector (DBR) optical cavity [16]. To minimize the influence of background dark counts, a 10 nm wide optical filter, centered at 1550 nm, was integrated into the system. The bias current was adjusted to a working point corresponding to a dark count rate (DCR) of 1 Hz, ensuring operation below the onset of the intrinsic dark count rate's exponential rise [17].

The signals are recorded using a time-to-digital converter (TDC). The classical bidirectional channel is made of a coaxial and an ethernet cable. It used for clock synchronization during data acquisition and for post-processing algorithms such as error correction and privacy amplification.

TABLE I. – *Secure key rate. Measured values of the secure key rate for different channel attenuation.*

Attenuation	10 dB	20 dB	30 dB	40 dB	50 dB	55 dB
Secure key rate	190 kbps	47 kbps	5 kbps	300 bps	12 bps	0.6 bps

4. – Results and discussion

Figure 3 presents the measured quantum bit error rate (QBER) and secure key rate (SKR). In fig. 3(a), the QBERs for both the Z- and X-bases are shown. As expected, the QBER in the X-basis is consistently higher than in the Z-basis. This difference arises because measurements in the Z-basis are direct, involving fewer sources of error. In contrast, X-basis-encoded qubits undergo a more complex decoding process prior to detection, making them more prone to intrinsic errors.

Figure 3(b) shows the trend of the expected SKR as a function of the channel attenuation and the measured SKR data for several channel attenuations. The measured values for each attenuation points are also reported in table I. The expected curve is generated based on the models described in refs. [12, 18]. These models require input parameters such as the attenuation losses, the QBER in both bases, the click rate in the Z basis, and the detector's non-ideal characteristics, including its efficiency, dark count rate, and hold-off time.

A deviation from the expected behavior is observed at a channel attenuation of 10 dB. This discrepancy is evident in both the QBER and SKR plots. In the QBER plot, the value at 10 dB attenuation exceeds that at 20 dB for both detection bases. Similarly, in the SKR plot, the measured SKR at 10 dB is slightly lower than the expected value for that channel. We attribute this discrepancy to the software communication library of the TDC, suggesting it is a software-related issue rather than a hardware malfunction. Specifically, when the click rates exceed 1 MHz, the time tagger's timing jitter demonstrates anomalous behavior, which impacts the signal-to-noise ratio in the detection process. To mitigate this effect, the mean photon number per pulse has been intentionally reduced below the optimal value.

5. – Conclusions

In this work, we use state-of-the-art SNSPDs with high efficiency ($> 90\%$) and low dark count rate (< 1 Hz) to establish a secure communication link over a 55 dB channel losses, equivalent to 340 km in ultra low-loss optical fiber. This work paves the way towards long distance quantum communication, moving toward the establishment of a fiber-based quantum network.

* * *

This research paper has been realized with the support of Domenico Ribezzo, Daniela Salvoni, Ciro Bruscino, Pasquale Ercolano, Mikkel Ejrnaes, Loredana Parlato, Giovanni P. Pepe, Alessandro Zavatta and Davide Bacco.

REFERENCES

[1] Pirandola S., Andersen U. L., Banchi L., Berta M., Bunandar D., Colbeck R., Englund D., Gehring T., Lupo C. *et al.*, *Adv. Opt. Photon.*, **12** (2020) 1012.
[2] Wehner S., Elkouss D. and Hanson R., *Science*, **362** (2018) eaam9288.
[3] Gisin N., Ribordy G., Tittel W. and Zbinden H., *Rev. Mod. Phys.*, **74** (2002) 145.
[4] Lo H. W., Curty M. and Tamaki K., *Nat. Photon.*, **8** (2014) 595.
[5] Scarani V., Bechmann-Pasquinucci H., Cerf N. J., Dušek M., Lütkenhaus N. and Peev M., *Rev. Mod. Phys.*, **81** (2009) 1301.
[6] Pomarico E., Sanguinetti B., Gisin N., Thew R., Zbinden H., Schreiber G., Thomas A. and Sohler W., *New J. Phys.*, **11** (2009) 113042.
[7] Zahidy M., Ribezzo D., De Lazzari C., Vagniluca I., Biagi N., Müller R. *et al.*, *Nat. Commun.*, **15** (2024) 1651.
[8] Sax R., Boaron A., Boso G., Atzeni S., Crespi A., Grunenfelder F., Rusca D. *et al.*, *Photon. Res.*, **11** (2022) 1007.
[9] Ribezzo D., Zahidy M., Vagniluca I., Biagi N., Francesconi S., Occhipinti T. and Bacco D., *Adv. Quantum Technol.*, **6** (2023) 2200061.
[10] Ribezzo D., Zahidy M., Lemmi G., Petitjean A., De Lazzari C., Vagniluca I., Conca E., Tosi A., Occhipinti T., Oxenløwe L. K., Xuereb A., Bacco D. and Zavatta A., *Phys. Rev. Appl.*, **20** (2023) 044052.
[11] Guarda G., Ribezzo D., Occhipinti T., Zavatta A. and Bacco D., *Phys. Rev. A*, **110** (2024) 042605.
[12] Rusca D., Boaron A., Grunenfelder F., Martin A. and Zbinden H., *Appl. Phys. Lett.*, **112** (2018) 171104.
[13] Masahito H. and Ryota N., *New J. Phys.*, **16** (2014) 063009.
[14] Grunenfelder F., Boaron A., Rusca D., Martin A. and Zbinden H., *Appl. Phys. Lett.*, **117** (2020) 144003.
[15] Boaron A., Boso G., Rusca D. *et al.*, *Phys. Rev. Lett.*, **121** (2018) 190502.
[16] Li H., Yang X., You L., Wang H., Hu P., Zhang W., Wang Z. and Xie X., *AIP Adv.*, **8** (2018) 115022.
[17] You L., *Nanophotonics*, **9** (2020) 2673.
[18] Rusca D., Boaron A., Curty M., Martin A. and Zbinden H., *Phys. Rev. A*, **98** (2018) 052336.