



## Practical analysis of decoy method in QKD over underwater optical fiber

**Bacco, Davide; Ribezzo, Domenico; Zahidy, Mujtaba; De Lazzari, Claudia; Vagniluca, Ilaria; Petitjean, Antoine; Lemmi, Gianmarco; Occhipinti, Tommaso; Cataliotti, Francesco Saverio; Oxenløwe, Leif K.**

*Total number of authors:*  
12

*Published in:*  
Quantum Computing, Communication, and Simulation III

*Link to article, DOI:*  
[10.1117/12.2647846](https://doi.org/10.1117/12.2647846)

*Publication date:*  
2023

*Document Version*  
Publisher's PDF, also known as Version of record

[Link back to DTU Orbit](#)

*Citation (APA):*  
Bacco, D., Ribezzo, D., Zahidy, M., De Lazzari, C., Vagniluca, I., Petitjean, A., Lemmi, G., Occhipinti, T., Cataliotti, F. S., Oxenløwe, L. K., Xuereb, A., & Zavatta, A. (2023). Practical analysis of decoy method in QKD over underwater optical fiber. In P. R. Hemmer, & A. L. Migdall (Eds.), *Quantum Computing, Communication, and Simulation III* Article 124460D SPIE - International Society for Optical Engineering.  
<https://doi.org/10.1117/12.2647846>

---

### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

# PROCEEDINGS OF SPIE

[SPIDigitalLibrary.org/conference-proceedings-of-spie](https://SPIDigitalLibrary.org/conference-proceedings-of-spie)

## Practical analysis of decoy method in QKD over underwater optical fiber

Davide Bacco, Domenico Ribezzo, Mujtaba Zahidy, Claudia De Lazzari, Ilaria Vagniluca, et al.

Davide Bacco, Domenico Ribezzo, Mujtaba Zahidy, Claudia De Lazzari, Ilaria Vagniluca, Antoine Petitjean, Gianmarco Lemmi, Tommaso Occhipinti, Francesco Saverio Cataliotti, Leif K. Oxenløwe, André Xuereb, Alessandro Zavatta, "Practical analysis of decoy method in QKD over underwater optical fiber," Proc. SPIE 12446, Quantum Computing, Communication, and Simulation III, 124460D (8 March 2023); doi: 10.1117/12.2647846

**SPIE.**

Event: SPIE Quantum West, 2023, San Francisco, California, United States

# Practical analysis of decoy method in QKD over underwater optical fiber

Davide Bacco<sup>a,b</sup>, Domenico Ribezzo<sup>c,d</sup>, Mujtaba Zahidy<sup>e</sup>, Claudia De Lazzari<sup>b</sup>, Ilaria Vagniluca<sup>b</sup>, Antoine Petitjean<sup>c</sup>, Gianmarco Lemmi<sup>c,d</sup>, Tommaso Occhipinti<sup>b</sup>, Francesco Saverio Cataliotti<sup>a,c</sup>, Leif K. Oxenløwe<sup>e</sup>, André Xuereb<sup>f</sup>, and Alessandro Zavatta<sup>b,c</sup>

<sup>a</sup>Dipartimento di Fisica, Università degli Studi di Firenze, Firenze, Italy

<sup>b</sup>QTI S.r.l., 50125, Firenze, Italy

<sup>c</sup>Istituto Nazionale di Ottica del Consiglio Nazionale delle Ricerche (CNR-INO), 50125 Firenze, Italy

<sup>d</sup>Università degli Studi di Napoli Federico II, Napoli, Italy

<sup>e</sup>Center for Silicon Photonics for Optical Communication (SPOC), Department of Electrical and Photonics Engineering, Technical University of Denmark, Kgs. Lyngby, Denmark

<sup>f</sup>Department of Physics, University of Malta, Msida MSD 2080, Malta

## ABSTRACT

Quantum key distribution (QKD) is the first commercial application of the second quantum revolution. Although QKD systems have already been developed and implemented all around the world, some open challenges are limiting the overall deployment of this technology (limited key rate, limited link distance, etc.). By improving the current QKD protocols, it is possible to increase the final secret key generation rate. In this work, we compare 1-decoy with 2-decoy methods in BB84 protocol over an underwater optical fiber link connecting Malta to Italy, showing that 2-decoy can achieve more than twice the key rate of 1-decoy method.

**Keywords:** quantum communication, field-trial experiment, quantum cryptography, quantum key distribution, decoy-state method

## 1. INTRODUCTION

Quantum key distribution (QKD) is a method that, exploiting the laws of quantum physics, makes it possible to share fully secure symmetric keys over a quantum channel, i.e., optical fiber, free-space, or underwater links. Currently, quantum networks have been deployed all around the world demonstrating a huge interest from final users.<sup>1,2</sup> More specifically, within Europe, a big infrastructure program like the European Quantum communication Infrastructure has been launched with the goal of creating the first European quantum network.<sup>3</sup> However, big challenges such as limited key generation rate, limited link distance and difficulties in co-propagating quantum and classical light into the same infrastructure, are still restricting a large-scale deployment of this technology.<sup>4</sup>

Improving current quantum protocols employed in commercial systems is a way to increase the key rate generated from QKD systems. More specifically in our work we have theoretically and experimentally investigated the BB84 protocol in the case of decoy-state technique considering one or two levels of decoys (1-decoy versus 2-decoy). In particular, we implemented the three-state BB84 protocol with time-bin encoding using the 1 and 2-decoy methods over a quantum link from Pozzallo (Sicily, Italy) to Malta through a 100 km underwater ultra-low loss optical fiber (20 dB attenuation). The experimental data, in agreement with the theoretical model, clearly show an advantage of the 2-decoy method compared to the 1-decoy one in terms of final key generation rate (1734 bps versus 814 bps). This work represents a direct comparison of these two QKD protocols in a field trial experiment demonstrating the advantage of the 2-decoy method on the practical side.

---

Send correspondence to: [davide.bacco@unifi.it](mailto:davide.bacco@unifi.it)

## 2. METHODS

### 2.1 Decoy-state Method

Nowadays, attenuating a specifically modulated classical laser down to single-photon level is definitely more practical than building a single-photon source;<sup>5</sup> for this reason, a large number of QKD setups, and most of the commercial QKD devices, employs weak coherent pulses as quantum states obtained by attenuating a telecom laser. Nevertheless, this method exposes a QKD system to photon number splitting attacks, i.e. a malicious third party (generally named Eve) could take advantage of multi-photon events (i.e. states made by two or more photons), eavesdropping only one photon of such states without being detected.<sup>6,7</sup> Let us consider a weak coherent state  $|\psi\rangle$  of amplitude  $\alpha$ :

$$|\psi\rangle = |\alpha\rangle |e^{i\theta}\rangle = \sqrt{\mu} |e^{i\theta}\rangle, \quad (1)$$

with the assumption of a randomized phase  $\theta$ . The probability distribution for the number of photons will follow a Poissonian distribution with parameter  $\mu$ , i.e., the probability of having a pulse with  $n$  photons  $p_n$  is:

$$p_n = e^{-\mu} \frac{\mu^n}{n!} \quad (2)$$

where  $\mu$  represents the average number of photons per pulse. To limit the number of multi-photon events,  $p_n$  for  $n \geq 2$  has to be small enough. This happens in the regime of  $\mu \ll 1$ , that ends up in drastic drops of rates and covered distances.<sup>8</sup>

The presence of an eavesdropper in the channel could be schematized as a black box that blocks the single-photon states and, after removing one photon, let the multi-photon states pass. This affects the photon number statistics, but unfortunately, Bob cannot distinguish between single-photon and multi-photon states. To overcome this issue, the decoy-state method was introduced back in 2003;<sup>9</sup> it helps to go beyond the limit of  $\mu \ll 1$ , resulting in improvements in terms of both distance and secret key generation rate. In decoy-state protocol, the intensity of quantum states is randomly chosen from a set. In the sifting stage, Bob uses this information, revealed by Alice at the end of the communication, to check the transmittance of the quantum channel for different intensities. Any discrepancies in the channel transmittance for different intensities indicates an active photon number splitting attack. In the 1(2)-decoy implementation, Alice chooses between 2(3) intensity levels, a main signal, and 1(2) decoy intensities. Both cases boast a big number of theoretical proofs and practical implementations. In this work, we test both 1-decoy and 2-decoy methods showing the higher performances of the 2-decoy method in terms of key rate.<sup>8,10</sup>

### 2.2 QKD Protocol

The protocol adopted in our experiment is the efficient three-state BB84 time-bin encoding. In the finite-key regime, the three-state BB84 protocol with decoy method produces a key whose length is bounded to:<sup>11,12</sup>

$$l \geq s_{Z,0}^l + s_{Z,1}^l(1 - H_2(\phi_Z^u)) - \lambda_{EC} - 6 \log_2 \left( \frac{b}{\epsilon_{sec}} \right) - \log_2 \left( \frac{2}{\epsilon_{corr}} \right), \quad (3)$$

with  $s_{Z,0}^l$  and  $s_{Z,1}^l$  being the lower bounds for the vacuum and the single-photon events respectively,  $\phi_Z^u$  is the upper bound of the phase error rate,  $\lambda_{EC}$  represents the number of disclosed bits in the error correction stage,  $H_2(x) = -x \log_2(x) - (1-x) \log_2(1-x)$  is the binary entropy,  $b$  is equal to 19 for the 1-decoy method and 21 for 2-decoy, and  $\epsilon_{sec}$  and  $\epsilon_{corr}$  are the secrecy and correctness parameters respectively, defined as:<sup>13</sup>

$$\begin{aligned} P[S_A \neq S_B] &< \epsilon_{corr}, \\ \mathbf{1}(S_A, S_B; Z, C) &< \epsilon_{sec}, \end{aligned}$$

where  $S_A$  and  $S_B$  are the two sifted keys,  $P[x]$  is the probability of  $x$ ,  $\mathbf{1}(\cdot)$  a generic information measure,  $Z$  is the eavesdropped sequence, and  $C$  is a random variable that represents the exchanged information. The second term denotes the probability  $\epsilon_{sec}$  that Alice's and Eve's strings have a stronger correlation than Alice's and Bob's ones. These parameters have been arbitrarily set as  $\epsilon_{corr} = 10^{-12}$  and  $\epsilon_{sec} = 10^{-12}$ . The phase error rate in the  $\mathbf{Z}$ -basis  $\phi_Z$  can generally be considered equal to the bit error rate in the  $\mathbf{X}$ -basis  $\text{QBER}_X$ ; however, the fact that in the adopted protocol Alice sends only one quantum state in the  $\mathbf{X}$ -basis, makes that the  $\phi_Z$  cannot be directly measured but it needs to be extracted from  $\text{QBER}_X$  as reported in.<sup>14</sup>  $\text{QBER}_X$  is connected to the interferometer visibility  $vis_X$  by  $\text{QBER}_X = (1 - vis_X)/2$ .

### 3. EXPERIMENTAL SETUP

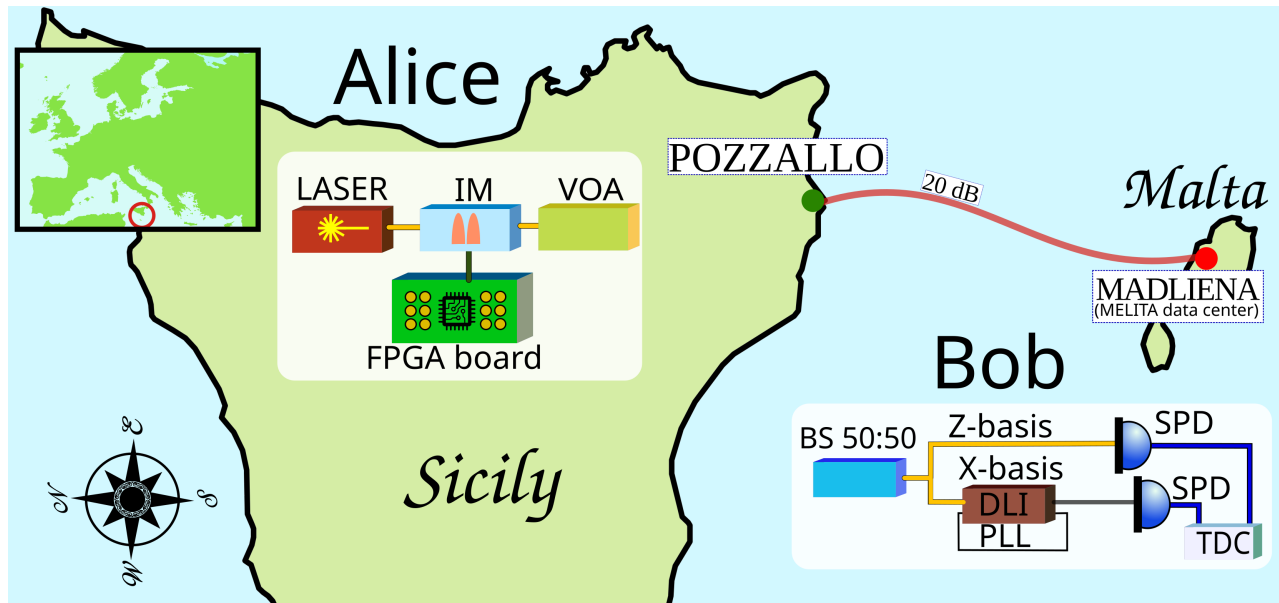


Figure 1. **Geo-localization of the interested area and scheme of the setup.** The quantum states are produced by carving and attenuating a continuous wave C-band laser. An FPGA board controls the intensity modulator (IM) in charge of the carving and generates a synchronization signal at 145 kHz, that travels on a different fiber (service channel); finally, a variable amount of optical attenuation (VOA) is used for achieving the required number of photons per pulse. The receiver setup starts with a 50:50 beam splitter (BS 50:50), that acts as basis choice sending half of the photons directly toward an SPD (Z basis) and routing the other half toward an unbalanced Mach-Zehnder interferometer - or delay line interferometer (DLI). The DLI introduces a time delay equivalent to 800 ps to one of the two arms. This is the time necessary for the X-basis pulses to overlap and interfere. In addition, light from a classical source, with frequency slightly different from the quantum signal, is injected from the output of the interferometer; this counter-propagating signal is detected with a photo-diode, monitored and utilized to stabilize the interferometer acting as a feedback signal on a phase shifter (phase lock loop - PLL). Finally, the interferometer output is detected by a commercial InGaAs single photon detector. A time-to-digit converter (TDC) produces the timestamps of the detection events utilized by a computer for the data analysis.

The implemented QKD link connects Malta to Italy through an underwater optical channel. The link is formed by an ultra-low loss pair of 96 km long optical fibers deployed under the Mediterranean Sea and connecting Malta to Sicily. The fibers show an attenuation of around 20 and 21 dB. Hence, the fiber exhibiting lower loss has been employed for distributing the quantum states while the other one has been utilized as a service channel (distribution of a synchronization signal, parameter estimation, etc.). The transmitter is located in the Melita service room of Pozzallo, in the south of Sicily, and the receiver is located in the Melita data center of Madliena, Malta. The pulses encoding the qubits are created by carving a continuous-wave C-band laser via an intensity modulator driven by a 595 MHz signal generated by a field programmable gate array (FPGA); finally, the pulses are attenuated in order to reach the single-photon level. In Malta, the quantum states are measured by two InGaAs single photons detectors (SPD). A 50-50 beam splitter is used to re-direct the incoming qubits to the two mutually unbiased bases. For the Z-basis, an SPD measures the time of arrival of the photons. To extract information of the states prepared in the X basis, an unbalanced interferometer makes the phase measurement possible. More details about the setup can be found in the caption of fig. 1.

For simplicity, Alice prepares the quantum states only in two different intensity levels: in the 1-decoy method, one represents the signal and the other the decoy, while when Bob analyzes the data adopting his 2-decoy method post-processing routines, the vacuum state (no transmission) is assumed as second decoy.<sup>8</sup> This choice guarantees the fairer possible comparison between the two methods.

## 4. RESULTS

In Fig. (2d) the trends for the secret key rate (SKR) versus channel attenuation for the 1-decoy and 2-decoy case is reported. The measured SKR values for our 20 dB channel loss are reported, which completely match the theoretical model. With a final key rate of 1743 bps, the 2-decoy method makes two times more than the 1-decoy, which reaches a key rate of 814 bps. Finally, in Fig. (2a), (2b), and (2c), the histograms of the three states generated for the protocol and measured after the channel is reported: early and late form the Z-basis states, and the only state produced in the X-basis respectively.

$\text{QBER}_Z(\%)$	2.7
$\text{QBER}_X(\%)$	7.5
$\mu_1$	0.27
$\mu_2$	0.075
$\mu_3$	0
$p_{\mu_1}$ (1-decoy)	0.11
$p_{\mu_1}$ (2-decoy)	0.09
$p_{\mu_2}$ (2-decoy)	0.25
$n_Z$	$10^7$
DCR (Hz)	2500
$p_{ZA}$ (%)	90
$p_{ZB}$ (%)	50
$\tau_f$ (ps)	80
SKR (1 decoy, bps)	814
SKR (2-decoy, bps)	1734

Table 1. **Set parameters and measured values for the setup.** In the table are reported: the measured QBERs in the two bases, the set numbers of photons per pulse  $\mu_1, \mu_2, \mu_3$ , the probability for Alice of sending  $\mu_n$   $p_{\mu_n}$ , the block size  $n_Z$ , the detector dark count rate  $DCR$ , the probability  $p_{ZA}$  and  $p_{ZB}$  of choosing Z-basis for Alice and Bob respectively, the time filters size  $\tau_f$ , and the achieved secret key rate SKR.

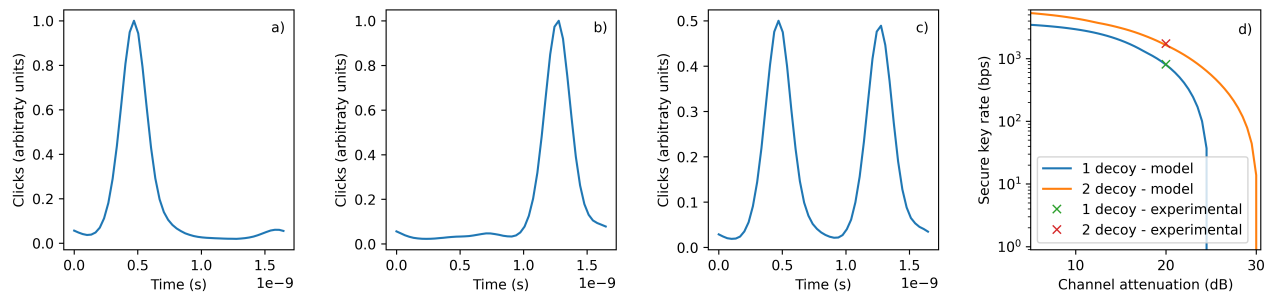


Figure 2. **a, b, c) Quantum states histogram.** The histograms show the shape of the states early (Z-basis), late (Z-basis) and their superposition (X-basis) respectively. The x-axis represents the time duration of one qubit (1.68 ns). The pulses broadness is due to the timing jitter of the detection stage (i.e., time-tagger and single-photon detectors), while imperfections in the carving stage make the basis step not flat. By adding a second intensity modulator it is possible to produce a cleaner signal: it should be taken into account to hold off the QBER for channels showing higher attenuation. **d) Secret key rate versus channel attenuation.** The blue and orange lines show the simulated trends of the secret key rates at different channel attenuation for the 1-decoy method and 2-decoy method respectively. The error probabilities for X and Z basis have been extrapolated from the Z-basis QBER and X-basis visibility in the actual channel (20 dB). The red and green points are the key rates achieved in the channel with the one and two decoy method respectively.

## 5. DISCUSSION

In a world where quantum computers cannot be anymore considered futuristic ideas belonging to physics laboratories, the necessity of finding secure methods to exchange sensitive data became a primary concern. In terms of security, QKD has no rivals: only a system based on quantum physics laws can guarantee the robustness of communications not only against immediate threats but also against every possible attack invented in the future. However, today's QKD cannot guarantee key rates comparable to classical competitors such as post-quantum algorithms, and it works only on limited distances. Efforts towards making these two factors less detrimental is today's priority of every research in this field; twin field QKD<sup>15</sup> and high dimensional protocols<sup>16–20</sup> are just some examples that go in this direction.

In this paper, we used a time-bin encoding QKD setup to compare the final secret key rate employing 1-decoy and 2-decoy methods. It is worth emphasizing that our implementation of a 2-decoy method has no necessity of modifying the setup since the second decoy is  $\mu_3 = 0$ , which corresponds to not sending any state, making possible such big improvements in terms of key rate with essentially no costs. This, to a great extent, paves the way for making QKD an accessible technology for every type of user.

## 6. ACKNOWLEDGEMENTS

This work was partially supported by the Center of Excellence SPOC - Silicon Photonics for Optical Communications (ref DNR123), the Innovationsfonden (No. 9090-00031B, FIRE-Q) the EraNET Cofund Initiatives QuantERA within the European Union's Horizon 2020 research and innovation program (grant agreement No. 731473, project SQUARE), by the NATO Science for Peace and Security program (Grant No. G5485, project SEQUEL) and the programme Rita Levi Montalcini QOMUNE (PGR19GKW5T).

## REFERENCES

- [1] Yu-Ao Chen, Qiang Zhang, Teng-Yun Chen, Wen-Qi Cai, Sheng-Kai Liao, Jun Zhang, Kai Chen, Juan Yin, Ji-Gang Ren, Zhu Chen, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 589(7841):214–219, 2021.
- [2] Domenico Ribezzo, Mujtaba Zahidy, Iliaria Vagniluca, Nicola Biagi, Saverio Francesconi, Tommaso Occhipinti, Leif K Oxenløwe, Martin Lončarić, Ivan Cvitić, Mario Stipčević, et al. Deploying an inter-european quantum network. *Advanced Quantum Technologies*, page 2200061, 2022.
- [3] European quantum communication infrastructure (euroqci) initiative.
- [4] Davide Bacco, Iliaria Vagniluca, Daniele Cozzolino, Søren MM Friis, Lasse Høgstedt, Andrea Giudice, Davide Calonico, Francesco Saverio Cataliotti, Karsten Rottwitt, and Alessandro Zavatta. Toward fully-fledged quantum and classical communication over deployed fiber with up-conversion module. *Advanced Quantum Technologies*, 4(7):2000156, 2021.
- [5] Ghulam Murtaza, Maja Colautti, Michael Hilke, Pietro lombardi, Francesco Cataliotti, Alessandro Zavatta, Davide Bacco, and Costanza Toninelli. Efficient room-temperature molecular single-photon sources for quantum key distribution. *Optics Express*, (<https://doi.org/10.1364/OE.476440>).
- [6] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.
- [7] Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. Advances in quantum cryptography. *Advances in optics and photonics*, 12(4):1012–1236, 2020.
- [8] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical review letters*, 94(23):230504, 2005.
- [9] Won-Young Hwang. Quantum key distribution with high loss: toward global secure communication. *Physical review letters*, 91(5):057901, 2003.
- [10] Davide Rusca, Alberto Boaron, Fadri Grünenfelder, Anthony Martin, and Hugo Zbinden. Finite-key analysis for the 1-decoy state qkd protocol. *Applied Physics Letters*, 112(17):171104, 2018.

- [11] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussi eres, Ming-Jun Li, et al. Secure quantum key distribution over 421 km of optical fiber. *Physical review letters*, 121(19):190502, 2018.
- [12] Charles Ci Wen Lim, Marcos Curty, Nino Walenta, Feihu Xu, and Hugo Zbinden. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A*, 89:022307, Feb 2014.
- [13] Matteo Canale. *Classical processing algorithms for Quantum Information Security*. PhD thesis, Department of Information Engineering, University of Padova, 2014.
- [14] Alberto Boaron, Boris Korzh, Raphael Houlmann, Gianluca Boso, Charles Ci Wen Lim, Anthony Martin, and Hugo Zbinden. Detector-device-independent quantum key distribution: Security analysis and fast implementation. *Journal of Applied Physics*, 120(6):063101, 2016.
- [15] Marco Lucamarini, Zhiliang L Yuan, James F Dynes, and Andrew J Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705):400–403, 2018.
- [16] Quantum cryptography using larger alphabets. *Physical Review A*, 61(6):062308, 2000.
- [17] Iliaria Vagniluca, Beatrice Da Lio, Davide Rusca, Daniele Cozzolino, Yunhong Ding, Hugo Zbinden, Alessandro Zavatta, Leif K Oxenl owe, and Davide Bacco. Efficient time-bin encoding for practical high-dimensional quantum key distribution. *Physical Review Applied*, 14(1):014051, 2020.
- [18] M Zahidy, D Ribezzo, C De Lazzari, I Vagniluca, N Biagi, T Occhipinti, LK Oxenl owe, M Galili, T Hayashi, C Antonelli, et al. 4-dimensional quantum key distribution protocol over 52-km deployed multicore fibre. In *European Conference and Exhibition on Optical Communication*, pages Th3C–6. Optica Publishing Group, 2022.
- [19] Beatrice Da Lio, Daniele Cozzolino, Nicola Biagi, Yunhong Ding, Karsten Rottwitt, Alessandro Zavatta, Davide Bacco, and Leif K Oxenl owe. Path-encoded high-dimensional quantum communication over a 2-km multicore fiber. *npj Quantum Information*, 7(1):1–6, 2021.
- [20] Davide Bacco, Nicola Biagi, Iliaria Vagniluca, Tetsuya Hayashi, Antonio Mecozzi, Cristian Antonelli, Leif K Oxenl owe, and Alessandro Zavatta. Characterization and stability measurement of deployed multicore fibers for quantum applications. *Photonics Research*, 9(10):1992–1997, 2021.