POLITECNICO DI TORINO
Repository ISTITUZIONALE

Analysis, Design and Implementation of an End-to-End QKD Link

Original
Analysis, Design and Implementation of an End-to-End QKD Link / Mondin, M.; Daneshgaran, F.; Di Stasio, F.; Arnon, S.; Kupferman, J.; Genovese, M.; Degiovanni, I.; Piacentini, F.; Traina, P.; Meda, A.; Gramegna, M.; Bari, I.; Khan, O.; Khan, M. (NATO SCIENCE FOR PEACE AND SECURITY SERIES. B, PHYSICS AND BIOPHYSICS). - In: NATO Science for Peace and Security Series B: Physics and BiophysicsELETTRONICO. - [s.l] : Springer, 2020. - ISBN 978-94-024-2020-3. - pp. 55-64 [10.1007/978-94-024-2021-0_6]

Availability:
This version is available at: 11583/2906312 since: 2021-10-26T12:13:08Z

Publisher:
Springer

Published
DOI:10.1007/978-94-024-2021-0_6

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright
Springer postprint/Author's Accepted Manuscript

This version of the article has been accepted for publication, after peer review (when applicable) and is subject to Springer Nature's AM terms of use, but is not the Version of Record and does not reflect post-acceptance improvements, or any corrections. The Version of Record is available online at: http://dx.doi.org/10.1007/978-94-024-2021-0_6

(Article begins on next page)

12 October 2024

Analysis, design and implementation of an end-to-end QKD link

TOPICS IN THE DESIGN OF A QKD LINK

M. MONDIN*, F. DANESHGARAN, F. DI STASIO
California State University Los Angeles, 5151 State Uni. Dr., 90032, los Angeles CA, USA

S. ARNON, J. KUPFERMAN
Ben Gurion University of the Negev, P.O.B. 653 Beer-Sheva 8410501 Israel

M. GENOVESE, I. DEGIOVANNI, F. PIACENTINI, P.TRAINA, A. MEDA, M. GRAMEGNA
INRIM, Strada delle Cacce, 91, 10135, Torino, Italy

I. BARI, O. KHAN, M. KHAN
NUCES, 160 Industrial Estate, Hayatabad, Peshawar, Pakistan

*To whom correspondence should be addressed.

Abstract- This manuscript discusses the most relevant aspects of the practical implementation of a long-range Quantum Key Distribution (QKD) link with trusted nodes, achieving the highest possible secret key rate generation within the security and system level constraints. To this purpose, we report on recent pilot studies for the measurements of detection efficiency and source photon statistics for validating the calibration facilities (i) at telecom wavelength for realistic quantum backbone implementation through standard telecommunications grade optical fiber, and (ii) for the telecom and VIS-NIR regime. In addition, since there are circumstances when a fiber optical link may not be available, we will also discuss the characterization of a Free Space Optics (FSO) QKD link. Finally, the manuscript also discusses the problem of information reconciliation in Continuous Variable QKD (CV-QKD) scenarios.

Keywords: Quantum Key Distribution, Detection Efficiency, Free Space Optics, Information Reconciliation.

Book Title Information
© 2005 *Springer. Printed in the Netherlands.*

1. Calibration facilities for realistic quantum backbone implementation: detection efficiency and source photon statistics

The development of fiber based point-to-point quantum networks for absolute secure quantum communication requires the exploitation of the most advanced available quantum technology on the market and of the use of innovative diagnostic tools to prevent possible quantum hacking attacks.

A possible solution for the development of a Quantum Key Distribution (QKD) [1,2] network is the installation of QKD devices on existing optical fiber links connecting metropolitan areas and the secure communication, both classical and quantum, between the most important cities.

The point–to-point connection can be then ensured by the realization of QKD trusted nodes. Nevertheless, metropolitan fiber links are subject to very high losses. It is of utmost importance to exploit state-of-the-art measurements techniques that metrology for quantum technology [3,4] is developing in order to pave the way to implementation of secure practical QKD systems and networks.

In this section, we report on pilot studies for the measurements of detection efficiency and source photon statistics for validating the calibration facilities at telecom wavelength, together with an analogue comparison characterisation in the VIS-NIR regime, and the realisation of pilot measurement comparisons to validate the techniques developed.

As a route to the validation of the measurement facilities, four European NMIs (INRIM, PTB, NPL and CMI) started two pilot studies on two key measurands in the 1550 nm region correlated with fibre-based QKD systems, i.e. the detection efficiency of single-photon detectors, and the Glauber second-order auto-correlation function of a pseudo single-photon source. Measurement protocols and procedures were developed on purpose.

Firstly, the pilot study towards a comparison on the measurements of detection efficiency of SPADs in the 1550 nm region, exploited a free-running InGaAs/InP SPAD-based detector. Single-photon avalanche diodes (SPAD) based on InGaAs/InP semiconductor materials are the most exploited detectors in many quantum technologies [5,6]. The successful development of such new technologies and products requires the solution to a number of metrological challenges; for this reason a metrological characterization in terms of detection efficiency, dead time, after pulsing and dark counts of single photon detectors is mandatory. A pilot study to compare different detection efficiency measurement strategies at the wavelength of 1550 nm was performed by four European National Metrology Institutes: CMI, INRIM, NPL and PTB. The device under test was a commercial free-running fibre-coupled InGaAs/InP single-photon detector.

The setup and the reference standard used as well as a detailed estimation of the measurement uncertainty of the detection efficiency was compared. The DUT was a fiber pigtailed free running SPAD (Id Quantique ID220), with nominal detection efficiency of 10% and dead time D of 10 μs. All the participants provided quantum efficiency measurement with the detector illuminated by a pulsed laser source, a commercial short-pulse laser source (ID Quantique, id300), which is based on a Distributed-feedback laser diode at 1550 nm. The measurement was carried out with the common repetition rate of 110 KHz. The exact wavelength of the source is measured with an optical spectrum analyzer (Anritsu MS974 OA). The measurement principle used by all participating laboratories for determining the detection efficiency of the InGaAs/InP SPAD detector was based on the substitution method. In a general scheme, adopted by all the participants, the output of the laser was sent to a device that provide a variable calibrated attenuation to attenuate light at single photon level. The detection efficiency was estimated by comparing the optical power measured by the DUT with the incident mean optical power per laser pulse measured with an analogue calibrated detector. Data are still under analysis but it seems that an excellent agreement (within the uncertainty) is obtained.

Secondly, the pilot study towards a comparison on the measurements of the Glauber second order autocorrelation function in the telecom range achieved a good agreement within the uncertainty. The source used for this test was a CW heralded single-photon source emitting real single photons at 1550nm. The Pilot study was carried on jointly in the INRIM labs.

Single-photon sources represent one of the fundamental tools for quantum information, quantum metrology and related quantum technologies. Because of this, the need for their characterization and standardization is becoming of the utmost relevance. Here, we show a procedure providing a quantitative estimate of the multi-photon component of a CW single-photon source, showing the results achieved in a pilot study [7] for the measurement of the second-order autocorrelation function $g^{(2)}(0)$ of a low-noise heralded single-photon source (HSPS) prototype operating at telecom wavelength , i.e. 1550 nm.

In our setup (Figure 1), our source hosts a CW laser (532 nm) pumping a 10 mm × 1 mm × 10 mm periodically-poled lithium niobate (PPLN) crystal to produce non-degenerate SPDC. Our signal and idler photons, respectively with wavelengths 1550 nm and 810 nm, are filtered and coupled to single-mode fibers (SMF). The detection of an idler photon by the SPCM-AQR silicon single-photon avalanche detector heralds the arrival of a 1550 nm signal photon, addressed to a 20 m long single-mode optical fiber connected to an electro-optical shutter (OS) operated by a fast pulse generator controlled by a field programmable gate array (FPGA). For each heralding signal, the FPGA operates the pulse generator in order to open our HSPS output channel,

i.e. OS channel A, for a time window of 7 ns in correspondence of the passage of a 1550 nm photon.

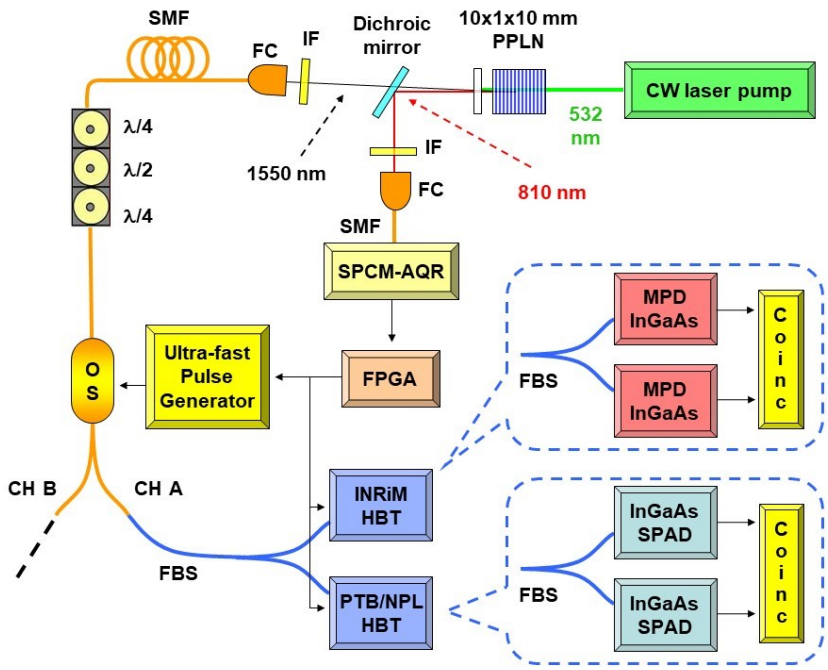

Figure 1 Experimental setup for the joint estimation of the multi-photon component in the emission of a low-noise CW single-photon source in the infrared (1550 nm).

For this joint measurement, the HSPS output is addressed to a 50:50 fiber beam splitter (FBS) whose outputs are sent to two Hanbury Brown & Twiss (HBT) interferometers, one belonging to INRiM and the other to the guest NMI (PTB or NPL), allowing simultaneous data collection between INRiM and the guest NMI to avoid mismatch due to some drift in the HSPS output over time. Every HBT is composed of two infrared InGaAs-InP SPADs, be they free-running or gated (when gated, the SPADs are triggered by the same FPGA signal opening the OS), whose outputs are sent to time-tagging coincidence electronics. Actually, the parameter we evaluate to characterize the emission of our source is $\alpha = \frac{P_{12}^{(ph;ph)}}{P_1^{(ph)} \cdot P_2^{(ph)}} \cong g^{(2)}(0)$, where $P_{12}^{(ph;ph)}$ and $P_i^{(ph)}$ $(i = 1,2)$ are, respectively, the probability of a coincidence count between the two HBT SPADs and the photon count probability for each of the HBT SPADs (dark counts subtracted). After a careful analysis of the setup parameters for a proper evaluation of the uncertainties associated to our measurements, we obtained the results below.

Measurement session	α (INRiM)	α (NPL)	α (PTB)
INRiM - PTB	0.016 ± 0.006	$-$	0.04 ± 0.05
INRiM - NPL	0.013 ± 0.008	0.02 ± 0.02	$-$

Table 1

As visible in the Table 1 above, the results of the whole measurement campaign (involving different measurement setups and data collection methodologies) are all in agreement within the experimental uncertainties reported (coverage factor: k = 1).
This pilot study, involving INRiM (also responsible for the source realization), NPL and PTB, represents a step forward towards a robust procedure for the characterization of this kind of single-photon sources.

Concerning with the pilot study [8,9] towards a comparison on the measurements of the Glauber second order autocorrelation function in the VIS-NIR regime, the source used for this test was a pulsed single photon source based on nitrogen-vacancy in diamond emitting single photons.
In order to establish standard techniques in single-photon metrology, device-independent and reproducible methods for source characterization are needed. Measurement of the $g^{(2)}(0)$ parameter is of utmost importance in characterizing and understanding single-photon sources emission.
In this paragraph we report on the pilot studies, performed by INRIM, NPL and PTB, on the complete characterization of a test source based on a single colour centre in diamond excited in pulsed regime and emitting radiation in the visible range. More details can be found in [7].
This comparison was hosted at INRIM from October 16 to October 29 2017 and was composed of two joint measurements of $g^{(2)}(0)$, on the same emitter: one performed by INRIM and PTB and the other one by INRIM and NPL.
The experimental setup [9] is composed of a laser-scanning confocal microscope whose signal is split by a 50:50 beam-splitter and connected to two measurement devices, i.e. two single-photon sensitive Hanbury Brown & Twiss (HBT) interferometers. The excitation light, produced by a pulsed laser (48 ps FWHM, 560 pJ per pulse) emitting at 532 nm with a repetition rate R= 2.5 MHz was focused by a 100X oil-immersion objective on the nano-diamond (ND) sample hosting an SPS based on a single Nitrogen Vacancy (NV) center of negative charge, with emission in a broad spectral band starting approximately at 630 nm and ending at 750 nm. The optical filters used were a notch filter at 532 nm and two long-pass filters (FEL600 and FEL650). The photoluminescence signal (PL), thus occurring in a 650 nm–750 nm spectral range, was collected by a multimode fiber and split by a 50:50 beam-splitter (BS). As stated above, each end of the BS was connected

to a separate HBT setup used for the joint measurement. In particular each faciliy was composed of:

- INRiM: a fused 50:50 fibre beam-splitter connected to two Excelitas SPCM-AQR-14-FC single-photon avalanche detectors (SPADs). Single and coincidence counts were sampled via ID Quantique *ID800* time-to-digital converter (60 ps time resolution).
- NPL: a fused 50:50 fibre beam-splitter connected to two Perkin-Elmer SPCM-AQR-14-FC single-photon avalanche detectors (SPADs). Coincidence counts were sampled via PicoQuant *HydraHarp 400* multichannel picosecond event timer (1 ps time resolution).
- PTB: a fused 50:50 fibre beam-splitter connected to two Excelitas SPCM-AQR-14-FC single-photon avalanche detectors (SPADs). Single and coincidence counts were sampled via PicoQuant *HydraHarp 300* multichannel picosecond event timer (4 ps time resolution).

The validity of the technique is demonstrated by compatibility of the results obtained by the three partners (see Table 2), demonstrating a system-independent (and unaffected by the non-ideality of the apparatus), estimate of $g^{(2)}(0)$, emission lifetime ($\tau = 15.34 \pm 0.08$) ns and their uncertainty.

	INRIM	**PTB**
$g^{(2)}(0)$	0.079 ± 0.009	0.076 ± 0.007
	INRIM	**NPL**
$g^{(2)}(0)$	0.065 ± 0.005	0.068 ± 0.005

Table 2

This study will greatly benefit the single-photon metrology community, as well as rapidly-growing quantum-technology-related industries. The main results of this study was the development of a standardized measurement technique as well as an uncertainty estimation procedure.

2. Hacking and security in free-space QKD system

This section reviews the challenge that arise in a realistic implementation of a free space quantum key distribution (QKD) system. QKD exploits quantum mechanics to achieve secure communication, by enabling two parties to produce and to share secret key to encrypt and decrypt messages. Practical QKD systems have been constructed deployed all over the world. However, while in theory QKD systems are secure there are still opportunities for attacks on the system, since actual devices have non ideal physical characteristic hat can be exploited. We focus here on one attack that exploits a detector non ideal physical characteristic, called backflash or Breakdown

flash hacking. Many QKD systems use very sensitive detector, which detection is typically done using single photon avalanche photodiodes (SPADs). In this type of system Alice sends a photon to Bob and he use his SPAD detector to detect the photon. However, due to unwanted phenomena or side effects, sometime the detector also emit a secondary photon which the eavesdropper (Eve) could detect and achieve information from it. This secondary emission is called backflash, and its physical characteristics depend on the structure of the detector. This is not a new phenomenon and has already been identified in the past for silicon and InGaAs/InP detectors [10, 11]. A single photon avalanche photodiodes (SPADs) detector is operated in a Geiger mode. In Geiger mode, the photo diode detector is reverse-biased above the breakdown voltage. As a result, signal photoelectrons can create an avalanche in high probability. In addition in low probability around 0.4% backflash photon is created [12]. In conventional SPAD the nominal detection efficiency is about 10 %, as a results the backflash could contain at least 0.04 photons emerging from the devices. This may result in a considerable amount of information leakage that has to be considered in practical QKD implementations generate a self-sustaining discharge.

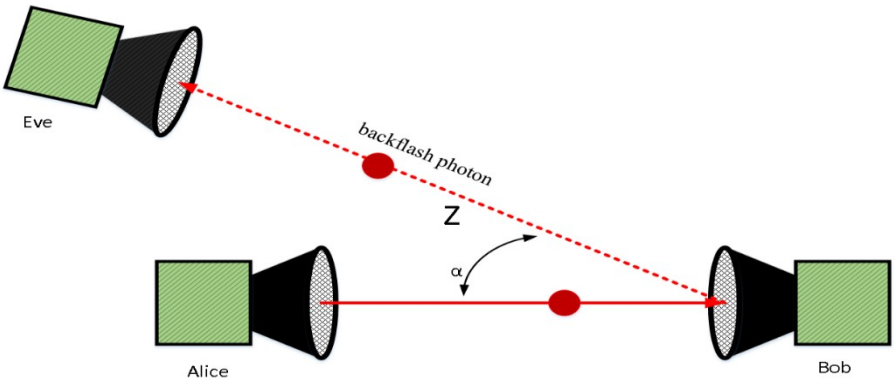

Figure 2 General scheme for use of backflash in eavesdropping

The Backflash spectral distribution, timing and information leakage for the different types of detectors has been measured and characterized in various detectors. The backflash was examined for InGasAs/InP SPADs at telecom wavelength, and for visible silicon SPADs in. The~~ir~~ setup used an attenuated laser sending photons at 155~~5~~0 nm. The back reflected light was analyzed and for the prototype detector this was nearly 10 %, for the commercial one it was around 6 %. Information leakage was affected by detector voltage bias (since higher voltage bias means more carriers in the avalanche. The spectral distribution between 1000 nm and 1600 nm of Backflash for InGaAs SPADs is examined in [12]. In [13] the authors tested commercial silicon SPADs, and demonstrated that an eavesdropper can distinguish detector clicked. Base

on this work it seems that backflash can reveal information about the optical electrical system that the photon propagates One solution to the reduce information leakage by backflash is to insert proper characterized passive optical devices into the system, in particular spectral filters (isolators, spectral filters, circulators), and use short gates and small avalanches. The best solution would be use of superconducting nanowire QKD detector, which would probably have less backflash, but this is not commercially in use at this point.

2.1. BACKFLASH PRINCIPLE

Backflash is a results of secondary photons that are emitted during the avalanche process, due to recombination of electrons and holes in the APD junction [14]. The backflash emission timing and spectrum depend on the detector, so Eve can gain information about the detector and the optical path the photon pass and use it to exploit other weaknesses. For example in a BB84 protocol Eve could know which detector the photon came from [13] because some photons from the vertical polarization detector will be emitted back through the vertical polarizer, and will themselves be vertically polarized.

In Figure 2 we can see the typical scenario under consideration: Alice sends a signal to Bob, and Bob's detector emits backflash through free space, which can then be utilized by Eve. For now, we ignore other optical elements of the system. To study the backflash, we suggest the following a mathematical model describe in the next lines. The probability for Eve to receive a photon due to backflash as a function of pointing direction error angle α and the distance separation between the Bob and Eve and is

$$P_E(\alpha) = \eta_q \frac{K_1 L(\alpha)}{Z^2}$$

where K_1 is a constant, η_q is a quantum efficiency and $L(\alpha)$ is the pointing loss factor (both defined below). The constant K_1 is

$$K_1 = N_B\, \eta_B\, \eta_E \left(\frac{\lambda}{4\pi}\right)^2 L_A G_B G_E$$

L_A represents the atmospheric attenuation, η_E , η_B and G_B , G_E are the optical efficiencies and the telescope gain of the Bob and Eve, respectively. The backflash wavelength is λ, N_B is the probability of backflash due to absorption of photon, and $L(\alpha)$ is the pointing loss factor. The gain of Eve's telescope is $G_E = \left(\frac{\pi D_E}{\lambda}\right)^2$, where D_E represents the aperture diameter for Eve's telescope. The gain of Bob's telescope is given by

$$G_B \approx \phi^{-2} = K_2 \left(\frac{D}{2f}\right)^{-2}$$

D is the detector diameter and f is the equivalent focal length of the optical system and K_2 is a constant. The pointing loss factor is given by

$$L(\alpha) = \exp\{-G_B\, \alpha^2\}$$

We conclude that the closer Eve is, the higher probability to gain a photon. The other factor controlling Eve's probability is pointing loss multiple by gain. This is symmetric around zero, and the probability for Eve to gain a photon increases strongly as this goes to zero. The larger $G_B\alpha^2$, the larger the pointing loss (equation above).

It is easy to see that in order to minimize the possibility for an eavesdropper to gain information by means of backflash, Eve should be substantially kept as far as possible, and at as wide an angle as possible away from the line of sight between Alice and Bob.

3. Information Reconciliation considerations

Continuous Variable (CV) Quantum Key Distribution (QKD) can be a viable alternative to its Discrete Variable (DV) counterpart, since CV-QKD does away completely with the requirement of operating with single or at least very low mean photon count per pulse. In CV-QKD Alice and Bob (and possibly Eve) share a set of correlated Gaussian samples. The trick is then to convert the samples into binary bits and use error correction techniques to ensure Alice and Bob's copies of the corresponding label sequence match.

At very low SNR, very little information is carried by the magnitude of the Gaussian samples is extremely low, while the sign contains almost all the information. Quantization of magnitudes of the Gaussian samples at Bob in reverse reconciliation (RR) can then be used to provide side information to Alice, which may be used in an unequal error protection scheme [15].

4. Conclusions

In this paper, we have discussed relevant aspects of the practical implementation of a long-range Quantum Key Distribution (QKD) link with trusted nodes. In particular, we have initially discussed on recent pilot studies for the measurements of detection efficiency and source photon statistics for validating the calibration facilities (i) at telecom wavelength for realistic quantum backbone implementation through standard telecommunications grade optical fiber, and (ii) for the VIS-NIR regime. Second, we discussed the problems that arise in a realistic implementation of a free space QKD

system. Lastly, we briefly commented on information reconciliation problems in CV-QKD systems.

5. Acknowledgements

This research was supported by NATO under the SPS program, project "Analysis, design and implementation of an end-to-end 400 km QKD link". This work received funds also from the projects EMPIR 14IND05 MIQC2, EMPIR 17FUN06 SIQUST, EMPIR 17FUN01 BECOME (the EMPIR initiative is co-funded by the European Union's Horizon 2020 research and innovation program and the EMPIR Participating States).

REFERENCES

[1] C. Bennett, G. Brassard," Quantum cryptography: public key distribution and coin tossing", Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India), pp. 175 – 179 (1984).
[2] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, "Quantum Cryptography", Rev. Mod. Phys, n. 74, pp. 145-195 (2002).
[3] https://www.euramet.org/european-metrology-networks/quantum-technologies/
[4] M. Gramegna et al., "European coordinated metrological effort for quantum cryptography", Proc. SPIE 10674, Quantum Technologies 2018, 106741K (21 May 2018); https://doi.org/10.1117/12.2307841
[5] R. H. Hadfield, Nature Photonics 3, 696–705 (2009)
[6] D. Stucki, et al., Journal of Modern Optics, 48, Issue 13, 1967-1981 (2001)
[7] E. Rebufello et al. "Towards a standard procedure for the measurement of the multi-photon component in a CW telecom heralded single-photon source", Metrologia, vol 56, 025004 (2019).
[8] S. Reichert, "Common Ground", Nature Physics 15, 110 (2019)
[9] E. Moreva et al., "Feasibility study towards comparison of the $g^{(2)}(0)$ measurement in the visible range", Metrologia, vol 56, 015016 (2019).
[10] A. Spinelli and A. L. Lacaita, "Physics and numerical simulation of single photon avalanche diodes", IEEE Transactions on Electron Devices (1997).
[11] A. Meda et alii, "Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution"; Light: Science & Applications - Nature group, n. 6, pp. e16261 (2017).
[12] Y. Shi et alii, "Breakdown flash at telecom wavelengths in InGaAs avalanche photodiodes", Optics express, vol. 25, n. 24, pp. 30388-30394 (2017).
[13] P. V. P. Pinheiro et al. "Eavesdropping and countermeasures for backflash side channel in quantum cryptography", arXiv preprint arXiv:1804.10317 (2018).
[14] A. Lacaita et al., "Photon-assisted avalanche spreading in reach-through photodiodes", Applied physics letters, vol. 62, n. 6, pp. 606-608 (1993).
[15] F. Daneshgaran, M. Mondin e K. Olia, "Permutation modulation for quantization and information reconciliation in CV-QKD systems", in Proceedings of the SPIE, Volume 10409, id. 104090J 10 pp. (2017).