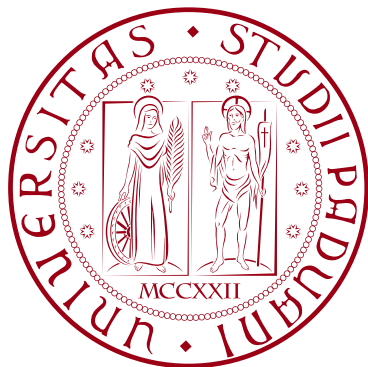




UNIVERSITÀ DEGLI STUDI DI PADOVA

DEPARTMENT OF INFORMATION ENGINEERING

PH.D. SCHOOL IN INFORMATION ENGINEERING

INFORMATION SCIENCE AND TECHNOLOGY

XXXVIII CYCLE

Advances in real-world applications of Quantum Key Distribution

Author:

Alberto DE TONI

Supervisor:

Prof. Paolo VILLORESI

Co-Supervisor:

Prof. Giuseppe VALLONE

Dr. Luca CALDERARO

Ph.D. School Coordinator:

Prof. Fabio VANDIN

UNIVERSITÀ DEGLI STUDI DI PADOVA

Department of Information Engineering

Ph.D. School in Information Engineering

Information Science and Technology

XXXVIII Cycle

Advances in real-world applications of Quantum Key Distribution

by Alberto DE TONI

Abstract

The increasing demand for unconditionally secure communication in an era of growing computational power has positioned Quantum Key Distribution (QKD) as a critical technology for future cybersecurity infrastructures. However, transitioning QKD systems from laboratory environments to robust, high-performance, real-world applications presents challenges in terms of speed, stability, scalability, and security. This thesis addresses these challenges through a multi-faceted investigation into the practical advancement of QKD systems. First, we introduce a complete theoretical model for Sagnac-based optical modulators, which are crucial components for stable quantum state encoding. We propose and experimentally validate novel modulation strategies, including a symmetric balanced scheme, that overcome the inherent repetition-rate limitations of traditional asymmetric designs. This innovation enables the development of high-speed, calibration-free encoders that mitigate environmental noise and patterning effects, achieving modulation rates exceeding 1.5 GHz. Second, leveraging this advanced hardware, we present the design and demonstration of a complete, high-performance, polarization-based QKD system developed for the QUANGO project. The system, implementing an efficient three-state decoy protocol, was rigorously tested over both optical fiber and a 620-meter urban free-space link. The results demonstrate exceptional performance, achieving a sustained Secret Key Rate (SKR) of over 1 Mb/s with a Quantum Bit Error Rate (QBER) below 1.5% in daylight free-space operation, validating its suitability for both terrestrial and future satellite-to-ground quantum networks. Third, we detail the deployment and long-term operational analysis of VenQCI, a 4-node metropolitan QKD network in Italy. This network integrates our QKD platform with commercial telecom infrastructure, utilizing resource-efficient optical switching to connect multiple nodes. A two-month analysis of the production network confirms its long-term stability and reliability, demonstrating continuous, automated key delivery for securing 100 Gbps MACsec-encrypted classical data links. Finally, we conduct a comprehensive security analysis of the *iPognac* encoder against Trojan-Horse Attacks (THAs). By modeling and experimentally executing attacks in both strong- and weak-light regimes, we characterize the system's vulnerabilities. We quantify the effectiveness of practical countermeasures, demonstrating that a combination of standard passive optical components and active monitoring can provide robust security, requiring over 65 dB of attenuation to render such side-channel attacks ineffective. Collectively, this work provides a significant contribution to the field by advancing QKD technology from the component level to deployed networks, paving the way for scalable and secure quantum communication infrastructures.

Acknowledgements

Thanks to Concessioni Autostradali Venete (CAV) s.p.a., that funded this PhD, in collaboration with ThinkQuantum s.r.l. that provided the means for my research on the field.

Thanks to my peers, my supervisors and all the other colleagues from academia. Your help has been invaluable.

Contents

Abstract	iii
Acknowledgements	v
List of Acronyms	xix
1 Fundamentals of cryptography	1
1.1 Classical cryptography	1
1.1.1 Secret-key authentication	2
1.1.2 Public-key and secret-key cryptography	3
1.2 Quantum cryptography	3
1.2.1 Quantum Key Distribution	4
1.2.2 Entropies in QKD	5
Shannon Entropy	6
Rényi Entropies	6
Max- and Min-Entropy	7
Quantum conditional min-entropy	7
Smooth Entropies	8
1.2.3 Secret-key rate, Yield, QBER	8
1.2.4 Practical QKD: approximations for the BB84 protocol	9
1.2.5 Unconditional security	10
1.2.6 Quantum Mutual Information and Holevo Bound	11
1.2.7 Fiber-based and satellite-based QKD	12
1.3 Decoy state QKD	14
1.3.1 Two decoy states	16
1.4 Three-state one-decoy <i>Efficient</i> -BB84	18
1.4.1 Secret Key Rate of the protocol	18
1.5 Post-processing	20
1.5.1 Parameter Estimation	21
1.5.2 Error-Correction algorithms	24
1.5.3 Privacy Amplification	25
1.6 Attacks in QKD	27
1.6.1 Trojan-Horse Attack	29
1.7 Other QKD protocols	29
2 Devices and components in Optics	31
2.1 Polarization Maintaining Fibers	31
2.2 Phase Modulators	32
2.3 Beam splitters	33
2.4 Polarizing Beam Splitters	34
2.5 Encoders for QKD	35
2.5.1 Roberts' intensity modulator	35

2.5.2	iPOGNAC polarization encoder	36
2.5.3	iPOGNAC as an Intensity Modulator	38
3	Software for real-time analysis of QKD systems	41
3.1	Objective	41
3.2	The software	42
3.2.1	Clock-recovery algorithm	44
3.3	Considerations	48
4	General model and modulation strategies for Sagnac-based encoders	51
4.1	Introduction	51
4.2	Principles of Sagnac modulators	52
4.2.1	Symmetric configuration	55
4.3	Sagnac polarization modulators	56
4.4	Sagnac intensity modulators	60
4.4.1	Pulse generation with symmetric configuration	61
4.5	Maximizing the repetition rate	61
4.5.1	Time-shifted modulation	63
4.5.2	Differential modulation	63
4.5.3	Balanced modulation	63
4.6	Conclusion	64
5	GHz-rate polarization-based DV-QKD system	65
5.1	Definition of the project	65
5.2	Introduction	66
5.3	Introduction to the system	67
5.3.1	Description of the free-space terminals	68
5.4	Results	70
5.4.1	Results of the fiber link in lab	70
5.4.2	Results of the free-space link	71
5.5	Conclusions	73
6	Long-term analysis of efficient-BB84 4-node network with optical switches in metropolitan environment	75
6.1	Introduction	75
6.2	Description of the devices	76
6.2.1	QuKy by ThinkQuantum s.r.l.	76
6.2.2	Node orchestration and link switching	77
6.3	Methods	77
6.3.1	Analysis of link performances	77
6.3.2	Description of the network (VenQCI)	77
6.4	Results	79
6.5	Conclusions	81
7	Trojan-Horse attack on the iPognac	85
7.1	Introduction	85
7.2	Methods	86
7.2.1	Description of the system	86
7.3	Theoretical Model	88
	Optimal POVM	88
	Fixed POVM	90
7.4	Strong light regime	93

7.4.1	CW laser attack	93
7.4.2	Pulsed laser attack	95
7.4.3	Results for the Strong Light Regime	96
7.5	Weak light regime	97
7.5.1	Results for the Weak Light Regime	98
7.6	Comparison of the attacks	99
7.7	Countermeasures	99
7.8	Conclusion	102
8	Conclusions	103
A	Appendix: Trojan-Horse attack on the iPognac	105
	Bibliography	107

List of Figures

1.1	A construction of two rotating disks with a Caesar cipher that can be used to encrypt or decrypt the code. [observablehq.com, 07/2025]	2
1.2	Example of one-time pad application: encryption and decryption. [Researchgate, 07/2025]	2
1.3	Working principle of the BB84 protocol. [Researchgate, 07/2025]	5
1.4	Binary Entropy function. [Wikipedia, 07/2025]	7
1.5	Key generation rate with different light sources: weak coherent state (WCS), heralded single-photon source (HSPS), and 2LS source (2LSS) with $\sigma = \Gamma/2$ and $P = 20$. [131]	10
1.6	Comparison of the time complexities between Shor's algorithm and the best current classical algorithm for primes factorization. [sharkyspool.home.blog, 07/2025]	11
1.7	Satellite and fiber communication efficiencies. [68]	13
1.8	Examples of polarization state (a) and phase state (b) encoders. [121]	13
1.9	Performances of decoy state QKD with respect to basic implementation. [73]	15
1.10	Example of an OFDR trace of Bob's Plug-&-Play QKD system. Each peak appears 3 times, because the incoming and reflected light both split in two, following the short and long path of the interferometer. For instance, one can notice that the long arm of the interferometer is about 11.5 meters longer than the short arm. [44]	29
2.1	Core examples of polarization maintaining fibers. [abalone-tech.com, 07/2025]	31
2.2	Working principle of an electro-optic phase modulator. [researchgate.net, 07/2025]	32
2.3	Free-space beam splitter schematics. [midopt.com, 07/2025]	33
2.4	Free-space polarizing beam splitter schematics. [altechna.com, 07/2025]	34
2.5	Intensity modulation. (a) Schematic of the Sagnac-based IM with a coupling ratio $R : T$. (b) Transmission (T) with voltage (V) for an interferometer-based IM. Power deviations for identical voltage shifts (ΔV) for signal states ("s") (ΔP_2) and decoy-states ("v") (ΔP_1) are given. The red dotted line shows the output of the proposed low extinction ratio interferometer. [98]	35
2.6	Scheme of the iPOGNAC polarization encoder. [9]	36
2.7	Scheme of an intensity modulator composed of an iPOGNAC polarization modulator followed by a polarizer rotated at an angle θ . [27]	38
2.8	Theoretical intensity ratio response of the system as a function of the iPOGNAC polarization phase modulation $\Delta\phi$ for different polarizer rotation angles θ . [27]	39
3.1	quTAG by qutools GmbH. [qutools.com, 08/2025]	42
3.2	Screenshot of the software during the testing of a QKD setup running in real-time.	43
3.3	Detail of the software showing the QBER and total detections. Logging widget on the right.	44
3.4	Widget to control an electrical amplifier.	44

3.5	Comparison between the old and new algorithm in terms of computation time performance, calculated on a fixed experimental set of data.	46
3.6	Before (left) and after (right) the frequency adjusting performed by the clock-recovery algorithm. The y-axis represents the time modulo-period in ps of each timetag (in this example the period being 1 ns) while the x-axis represents the time in ps of each timetag. The red line represents the fitted linear-regression line on the un-synchronized data.	48
4.1	Polarization and intensity modulator based on the Sagnac scheme. ϕ -mod indicates the electro-optic phase modulator, while the white arrow indicates the direction of the RF microwave signal. ΔL quantifies the asymmetry of the phase modulator within the Sagnac loop. For symmetric configuration $\Delta L = 0$	53
4.2	Phase $\phi_s(t)$ for rectangular driving signal $s(t)$. We considered the case $\tau_d \geq \tau_s + \tau_{\text{mod}}$ and $\tau_s \geq 2\tau_{\text{mod}}$. The signal $s(t)$ is reported in units of V_0 , while $\phi_s(t)$ is given in unit of $\frac{V_0}{V_\pi}$. For simplicity we set $t_0 = 0$	55
4.3	Modulations proposed in this work, characterized by signal $s(t)$ (top) and phase response $\phi(t)$ of the configuration (bottom). From left to right: a) time-shifted modulations for the asymmetric configuration (for $\tau_s \geq 2\tau_{\text{mod}} + \tau_{\text{op}}$); b) differential asymmetric modulations (for $\tau_s \geq \tau_{\text{op}}$); c) differential symmetric modulation (for $\tau_s \geq \tau_{\text{op}}$); d) balanced symmetric modulations (for $\tau_s \geq \tau_{\text{op}}$). For the asymmetric configuration we choose $\tau_d = \tau_s + \tau_{\text{mod}}$, while for the symmetric configuration we have $\tau_d = 0$. It should be noted that the voltage required to apply a $\pi/2$ phase on the optical pulse for the symmetric differential configuration is higher than all others by a gain factor of g_V defined in Eq. (4.12).	57
4.4	Generated states at 1.5 GHz of repetition rate using the symmetric balanced configuration and projected on the Y basis, with a polarization extinction ratio of $\text{PER}_Y = 23.147 \pm 0.003$ dB observed between the $ L\rangle$ and $ R\rangle$ states.	59
4.5	Experimental data showing the behavior of the time-shifted asymmetric modulation varying τ_s (bottom) and V (top).	59
4.6	Comparison between the differential and balanced symmetric modulation for (a) polarization modulator and (b) intensity modulator.	60
4.7	Example of pulse generation through carving using the Sagnac intensity modulator in symmetric configuration. Despite the realistic scenario presenting a "dip" in the center of the pulse, it is only when perfect symmetry is achieved that the intensity reaches zero, otherwise resulting similarly to the ideal case.	61
4.8	Experimental data testing the pulse generation model proposed in sec. 4.4.1.	62
5.1	Partners within the QUANGO project.	66

5.2	Scheme of the setup. The source is composed by a DFB laser generating optical pulses that go through an isolator (ISO), then inside a free-space-coupled (the coupling of the input fiber is tilted by 45° to proceed with the $ D\rangle$ state) beam-splitter (BS): the beam gets reflected into the Sagnac loop, consisting of a polarization-beam-splitter (PBS) and a phase-modulator (ϕ -Mod), and travels back to be transmitted, through a polarizer (POL), into the polarization modulation stage, which consists in the same pieces except the polarizer. After travelling through the channel, the pulses reach the receiver, consisting on a D-WDM filter, a fiber BS, two polarization-controllers (PC), two PBSs and four detectors, one for each polarization state (namely L,R,D,A). The output is analyzed by a time-to-digital-converter (TDC) that is synchronized by the same system-on-a-chip (SoC) that is used to generate the light pulses and control the modulation of the signal.	68
5.3	Testbed illustration. (A) Aerial view of the 620 m free-space channel between DFA and DEI in Padova. Data from Google Earth [©2025 Google]. (B) Schematic of the Tx node at DFA, connected to LUX through a deployed fiber network. It is also shown the render of the 3D model of the enclosure hosting the optical terminal. (C) Schematic of the Rx optical components. It is also shown the render of the 3D model of the receiving telescope. TTM: tip-tilt mirror; CAM: camera; FOM: folding mirror; FSM: fast-steering mirror; DM: dichroic mirror; BF: bulk filter; SMF: single-mode fiber; DWDM: dense wavelength-division multiplexer; PSD: position-sensitive-detector; PM: power meter.	69
5.4	Secret key rate obtained over time for a 1024-symbol sequence in the lab, at 26 dB of total losses. In blue and red, associated with the right axis, the measured QBER on the Z and X basis.	71
5.5	Estimation of the secret key rate for different channel attenuation values. The dashed line represents the asymptotic limit, while the red and green dots represent, respectively, the finite-key analysis using the Hoeffding and Chernoff bounds.	71
5.6	Control OFF and ON scatter plots, with PSD detecting λ_{Coarse} beam's centroid in a $10\ \mu\text{m}$ bin width. The channel attenuation is measured for both scenarios.	72
5.7	Results for the link in free-space with high channel losses (~ 39 dB).	73
5.8	Results for the link in free-space with low channel losses (~ 18 dB).	74
6.1	QuKy by ThinkQuantum s.r.l. [114]	76
6.2	The VenQCI network: VSIX – CavPD (Padova toll booth) – CavVE (Mestre toll booth) – VEGA. Aerial view provided by earth.google.com.	78
6.3	Scheme of the VenQCI network.	78
6.4	For each link, probability distribution of the time required to accumulate and process 500 kB of sifted key. In each graph are present two peaks, one on the right corresponding to the first block after the switching (including the initial base alignment time), and one on the left for the following blocks, which skip this phase (inside the colored area).	79
6.5	RKR and SKR of each link distinguished by line type. The line represents the mean taken on a daily basis.	80
6.6	QBER trend for each 2-node link in a two-month period. Experimental data is represented by a scatter plot, while the average is reported as a line plot.	81
6.7	Plot of the switching mechanism sampled from the long-run. The data represents a period of 2 hours on the 13th of May 2025.	82

6.8	Raw Key Rate by the hour. Box-plot where the middle point of the boxes represents the median data point, the box represents the 25% and the lines the 75% quantiles, meanwhile dots are outliers.	82
6.9	Secret Key Rate by the hour. Box-plot where the middle point of the boxes represents the median data point, the box represents the 25% and the lines the 75% quantiles, meanwhile dots are outliers.	83
7.1	Scheme of the setup for the THA on the <i>iPOGNAC</i> . SM-Fibers in yellow, PM-Fibers in blue, electrical connections in black. The optical power entering inside Alice's setup is indicated as μ_{in} , while the one coming out (subject to the attenuations of the Alice's system and therefore smaller than μ_{in}) is indicated as μ_{out}	86
7.2	Theoretical prediction accuracy with respect to the mean photon number μ_{out} , varying different POVMs, extinction ratios of the projective measurements, efficiencies, and experimental data for comparison.	87
7.3	Theoretical detection probabilities for each state and the total with respect to the mean photon number μ_{out} in the use-case of only two detectors (Extinction Ratio = 8.86 dB).	91
7.4	2D-histogram of the waveform resulting from the oscilloscope, result of the optical modulation in continuous wavefront by the <i>iPOGNAC</i> during the THA, and $ H\rangle$, $ V\rangle$ and $ D\rangle$ symbols separately. All the waveforms presented are calculated by performing a modulo-period operation. In the top plot, the red vertical line shows the detected position of the first symbol in the original waveform.	94
7.5	Waveform with calculated symbol positions and classified symbols for the CWLA. Red dots show the estimated symbol locations, while thresholds are used to classify the symbol as $ H\rangle$, $ V\rangle$, or $ D\rangle$ (if the symbol location is above the threshold up, the symbol is classified as $ V\rangle$, if it is between the thresholds up and down, it is classified as $ D\rangle$, and if it is below the threshold down, it is classified as $ H\rangle$).	95
7.6	Mean of $ H\rangle$, $ V\rangle$, and $ D\rangle$ symbols in time modulo period, result of the optical modulation in pulsed regime by the <i>iPOGNAC</i> during the THA. Data points are reported in purple. Red vertical line shows the detected position of the first symbol in the original waveform. Statistical distributions of these symbols are displayed on the right.	95
7.7	Waveform with calculated symbol positions and classified symbols for the pulsed laser attack. Red dots show estimated symbol locations, thresholds are used to classify the symbol as $ H\rangle$, $ V\rangle$, or $ D\rangle$ (if the symbol is above the threshold H, the symbol is classified as $ H\rangle$, between the thresholds H and D, it is classified as $ D\rangle$, otherwise it is classified as $ V\rangle$).	96
7.8	Results on optimal prediction accuracy based on the mean photon number μ_{out} for the continuous and pulsed laser attack.	96
7.9	Mean photon number μ_{out} at different attenuations set on the VOA. Noise floors thresholds are indicated with horizontal lines. The plateau after 15 dB is due to the noise floor of the power-meter we used to characterized the output power (50 nW).	97
7.10	Prediction accuracy in relation to the mean photon number μ_{out} , after normalizing the average power to 10 W for thermal damages (t) and 1 MW for ablation damages (a), for which the respective countermeasure attenuation is reported at the top.	98

7.11 Attenuation required to counteract the THA presented in this work in different scenarios of input power P_{in} and pulse width ΔT , both for thermal (top) and ablation (bottom) damage limits.	101
--	-----

List of Tables

1.1	Example of transmission with <i>intercept-resend</i> attack (errors in red, sifted in cyan).	6
1.2	Detection of Eve performing a <i>PNS attack</i> using decoy state QKD.	14
1.3	Targets, attacks, and exploited imperfections in QKD systems.	28
4.1	Performance parameters for all implemented modulations, with ΔV the normalized range of voltage required to achieve all states for the three-state BB84 protocol and t_{sym} the minimum period as a function of the setup parameters. The minimum period t_{sym}^* and maximum repetition rate R_{max} were obtained assuming experimentally verified values of $\tau_{\text{mod}} = 320$ ps, $\tau_s = 166.6$ ps, and $\tau_{\text{op}} = 100$ ps.	62
7.1	Truth-table of the detections (clicks) of the symbols in a Geiger-mode detector using two channels.	90
7.2	Detection probabilities for each (Eve Alice) case using Geiger-Mode (G-M) and Photon-Number-Resolving (P-N-R) photodetectors. We considered a more realistic scenario for G-M detectors, introducing also a sub-optimal extinction ratio (ER , in linear scale) coming from the projecting device at Eve's side. We identified as "vac" the vacuum state, where no detector clicks.	92
7.3	Use-cases of the attacks proposed in this work: Photodiode - continuous wave laser attack (PD-CWLA), Photodiode - pulsed laser attack (PD-PLA) and attack using Geiger-mode single-photon detectors (G-M).	99

List of Acronyms

AoA	Angle of Arrival
BB84	Bennett-Brassard 1984 Protocol
BF	Bulk Filter
CAM	Camera
CCW	Counter-Clockwise
CIRC	Circulator
CV-QKD	Continuous-Variable Quantum Key Distribution
CW	Clockwise
CWLA	Continuous-Wave Laser Attack
DEI	Department of Information Engineering
DFA	Department of Physics and Astronomy
DFT	Discrete Fourier Transform
DI-QKD	Device-Independent Quantum Key Distribution
DM	Dichroic Mirror
DV-QKD	Discrete-Variable Quantum Key Distribution
DWDM	Dense Wavelength-Division Multiplexer
EC	Error Correction
ED	Eavesdropper Detector
EOM	Electro-Optic Modulator
ER	Extinction Ratio
FOM	Folding Mirror
FOV	Field of View
FPGA	Field-Programmable Gate Array
FSM	Fast-Steering Mirror
FWHM	Full-Width-at-Half-Maximum
GUI	Graphical User Interface
HCF	Hollow-Core Fiber
HSPS	Heralded Single-Photon Source
IM	Intensity Modulator
IoT	Internet of Things
KMS	Key Management System
LDPC	Low-Density Parity-Check
LEO	Low-Earth Orbit

LIDT	Laser-Induced Damage Threshold
MACsec	Media Access Control Security
MDI-QKD	Measurement-Device-Independent Quantum Key Distribution
MFD	Mode-Field Diameter
MPLS	Multi-Protocol Label Switching
NANF	Nested-Antiresonant Nodeless Fiber
OGS	Optical Ground Station
OSC	Oscilloscope
OTP	One-Time Pad
PC	Polarization Controller
PD	Photodiode
PE	Parameter Estimation
PIC	Photonic Integrated Circuit
PKC	Public-Key Cryptography
PLA	Pulsed Laser Attack
PM	Polarization-Maintaining
PNS	Photon-Number Splitting
PSD	Power Spectral Density / Position-Sensitive Detector
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QUANGO	QUbesat for QUANTum and 5G cOmmunication
RKR	Raw Key Rate
Rx	Receiver
SKC	Secret-Key Cryptography
SKR	Secret Key Rate
SKIP	Secure Key Integration Protocol
SMF	Single-Mode Fiber
SNR	Signal-to-Noise Ratio
SNSPD	Superconducting Nanowire Single-Photon Detector
SoC	System-on-a-Chip
SOP	State of Polarization
TDC	Time-to-Digital Converter
THA	Trojan-Horse Attack
TTM	Tip-Tilt Mirror
Tx	Transmitter
VLAN	Virtual Local Area Network
VOA	Variable Optical Attenuator
WCS	Weak Coherent State
WD	Watchdog Detector
WDM	Wavelength-Division Multiplexer

To the ones who left, to the ones who stayed, to the newcomers.

Chapter 1

Fundamentals of cryptography

1.1 Classical cryptography

Cryptograhpy is the ensamble of techniques for secure communication in the presence of third party adversaries. It is about thinking, developing and analyzing protocols that prevent others from reading private messages, except from the sender (*Alice*) and the receiver (*Bob*). In a world were privacy assumes a fundamental role in everyone's life, cryptography is the invisible hand that prevents the system from falling apart. In more than one scenario, perfect secrecy is of utmost importance in telecommunications: just think about our bank account data being transferred from one office to another. Banks are day by day globally expanding and inevitably require this kind of security, otherwise their clients could loose all their funds at the expenses of an ordinary hacker. The term *Classical* was added after the quantum revolution in order to distinguish it from *quantum* cryptography, and it refers, as the name says, to classical communication, which relies on the *bit* as fundamental element of information. The bit has two fundamental values, 0 and 1, and is usually represented by a high/low electrical voltage or magnetic domains. Reproducibility is one of the fundamental properties of classical communication: information can be copied and, while being useful for amplifying the signal (allowing high SNR long-distance communications), is also a great disadvantage for private communication (this will be discussed later in sec. 1.2). The basic principle behind cryptography is to use an algorithm (or a *cipher*) to transform (i.e., to encrypt) the data into apparent gibberish. The receiver, knowing how the cypher works, can *decrypt* the apparent random message to retrieve the original one. The original data is called *plaintext*, while the encrypted data is called *ciphertext*. For obvious reasons, changing algorithm for every transmission is not practical and instead what is done is using different *keys* for the same cipher. A key is a parameter without which it is difficult, if not impossible, to retrieve the plaintext from the ciphertext. One of the first examples of encryption was found in "*Caesar's cipher*" (fig. 1.1). It consisted on an alphabet shifted right(left) of a random number of letters. Knowing that number, the receiver could rapidly retrieve the original message by re-shifting left(right) the alphabet. Even though it doesn't surely achieve perfect secrecy, for the time it was a big leap forward in cryptography.

Perfectly secret ciphers, although, exist and can be quite easily achieved. The simplest and most famous one is *one-time pad* (OTP), created by combining the ideas of Vernam and Mauborgne in the years 1917-18. It consists in modulo-2 addition (*XOR* operation) of each plaintext bit p_i with each key bit k_i , i.e: $c_i = p_i \oplus k_i$. By knowing the key k , one can easily retrieve the original plaintext p from the ciphertext c by performing another modulo-2 addition with the key (fig. 1.2).

The major drawback of one-time pad is, as the name suggests, that it can be used only once. Otherwise, using the same key k for two plaintext messages p and p' will cause that



FIGURE 1.1: A construction of two rotating disks with a Caesar cipher that can be used to encrypt or decrypt the code. [observablehq.com, 07/2025]

ENCRYPT	
$\oplus$	00110101 Plaintext
	11100011 Secret Key
=	11010110 Ciphertext
DECRYPT	
$\oplus$	11010110 Ciphertext
	11100011 Secret Key
=	00110101 Plaintext

FIGURE 1.2: Example of one-time pad application: encryption and decryption. [Researchgate, 07/2025]

$p \oplus p' = c \oplus c'$ and information (in the Shannon sense) can be extracted. OTP can achieve *unconditional security* if the following circumstances hold:

1. The key must be random (uniformly distributed and independent of the plaintext).
2. The key must be at least as long as the plaintext.
3. The key must never be reused in whole or in part.
4. The key must be kept completely secret by the communicating parties.

1.1.1 Secret-key authentication

An important function of classical cryptography is *authentication*. Authentication is the set of techniques aimed at verifying that a transmitted message arrives unmodified at the receiver: messages modified or created by any other person can be detected and discarded. In order for QKD to work properly, Alice and Bob must talk through an authenticated channel. Otherwise, an *eavesdropper* (Eve) could make Alice believe she's Bob and perform a complete undisturbed communication without Bob receiving any single bit. There are ways of doing authentication, usually coming down to adding redundancy to the original message: any modifications would break that redundancy. The piece of information added to the original message is called "*message authentication code*" (MAC). Before sending a message, Alice attaches a MAC, which she calculates as a function of both the message and the key. On his side, Bob recalculates the MAC from the received message and compares it to the attached MAC. Provided that the shared key is not compromised, he can be confident that the message is legitimate when both MACs match. [121]

1.1.2 Public-key and secret-key cryptography

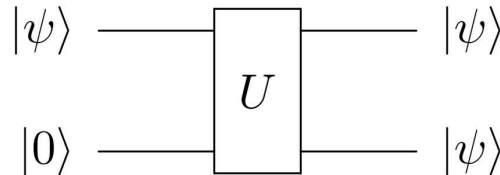
The essential difference between public-key cryptography (PKC) and secret-key cryptography (SKC) is that the first allows anyone to encrypt to a single recipient, while the latter is intended for one-to-one communications. SKC allows role-exchange (Alice can be Bob and viceversa) while PKC has Bob attached to its private key and Alice can be anyone having access to the directory of public keys. This way, in a network of n people, SKC would impose everyone to establish a secret key with everyone else, hence resulting in a potential number $n(n-1)/2$ of different keys. With PKC, only n pairs of private and public keys are needed. For this reason, PKC is usually considered to be more practical than SKC even though the latter is capable of achieving more secrecy. Quantum Key Distribution, which will be discussed in section 1.2.1, is capable of making SKC more feasible. [121]

1.2 Quantum cryptography

Quantum communication's fundamental information unit is the *Qubit* (or *quantum bit*), any two-level quantum-mechanical system in which information can be encoded. Mathematically speaking, a Qubit lies on an Hilbert space $\mathcal{H}$ of dimension 2 and computational basis $\{|0\rangle, |1\rangle\}$. The astounding difference between the bit and the Qubit is that while the first can have only the values 0 or 1, the second can have both $|0\rangle$ and $|1\rangle$ simultaneously thanks to the property of *superposition*. This gives quantum information unique properties that the classical one could not exploit, like the collapse of the wavefunction after a measurement or the uniqueness of the Qubit (also named "*no-cloning theorem*" [127]) which demonstration, for the sake of the simplicity of it, is reported below.

th: it is impossible to create an independent and identical copy of an arbitrary unknown quantum state $|\psi\rangle$.

dem: Let's suppose the perfect cloning machine exists:



i.e. a machine that through a unitary operator U can perform:

$$(\alpha|0\rangle + \beta|1\rangle)_A \otimes |0\rangle_B \xrightarrow{U} (\alpha|0\rangle + \beta|1\rangle)_A \otimes (\alpha|0\rangle + \beta|1\rangle)_B$$

Since it must work also on the singular bases:

$$\begin{aligned} |0\rangle_A \otimes |0\rangle_B &\xrightarrow{U} |0\rangle_A \otimes |0\rangle_B \\ |1\rangle_A \otimes |0\rangle_B &\xrightarrow{U} |1\rangle_A \otimes |1\rangle_B \end{aligned}$$

Yet, when it is applied to the generic state $|\psi\rangle$, due to linearity:

$$\begin{aligned} &(\alpha|0\rangle + \beta|1\rangle)_A \otimes |0\rangle_B = \\ &= (\alpha|0\rangle_A \otimes |0\rangle_B + \beta|1\rangle_A \otimes |0\rangle_B) \xrightarrow{U} (\alpha|0\rangle_A \otimes |0\rangle_B + \beta|1\rangle_A \otimes |1\rangle_B) \\ &\neq (\alpha|0\rangle + \beta|1\rangle)_A \otimes (\alpha|0\rangle + \beta|1\rangle)_B \end{aligned}$$

i.e., the computational bases can be perfectly copied but not the superposition state. Note that the relation is valid for every α, β complex, so the theorem is demonstrated.

//

This theorem has important consequences on quantum cryptography, because it means that the eavesdropper cannot gain information without leaving a trace of its presence. From that the idea of exploiting quantum mechanical observables to exchange the key for encoding/decoding the plaintext. Because of practical uses and the relation with the project of this thesis, I will concentrate on light polarization states as observables.

Light can be used to encode information thanks to its various polarization states ($\uparrow, \rightarrow, \nearrow, \nwarrow, \cup, \cap$: a light beam is linearly polarized "if the electric field vector vibrates in a constant direction" [1], while is said to be elliptically polarized "if the curve traced by the end point of the electric field vector is an ellipse" [1]), that can be put in superposition to generate quantum states: it is only matter of choosing which one is a 0 and which is a 1; for example, using the $+$ basis, $\rightarrow = 0$ and $\uparrow = 1$.

I will use the notation:

$$\begin{aligned} \mathbb{Z} = + &= \{|0\rangle, |1\rangle\} = \{|H\rangle, |V\rangle\} = \{|L\rangle, |R\rangle\} \\ \mathbb{X} = \times &= \{|+\rangle, |-\rangle\} = \left\{ \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\} = \{|D\rangle, |A\rangle\} \end{aligned}$$

Where $\{|H\rangle, |V\rangle\}$ and $\{|L\rangle, |R\rangle\}$, despite representing different states on the Bloch sphere, for the scope of QKD can be used indifferently, because they are both mutually unbiased bases to $\{|D\rangle, |A\rangle\}$. I will cover the matter of encryption of quantum states on section 1.2.1, since quantum cryptography is quite directly correlated with the concept of Quantum Key Distribution [121].

1.2.1 Quantum Key Distribution

BB84 is the first Quantum Key Distribution Protocol that was proposed by Charles Bennet and Gilles Brassard in 1984. It requires two communication channels: an authenticated classical channel, with which Alice can transmit to Bob the ciphertext, and a secret quantum channel, with which the key is sent. Because of the properties above mentioned, BB84 does not prevent an eavesdropper to intercept the key but aims to statistically deduce the presence of it. The key point is, no pun intended, the key sharing: let's see how this works.

1. Alice encodes each key bit in a random basis ($+, \times$) and sends it to Bob;
2. Bob chooses randomly a measurement basis ($+, \times$) for each key element. At the end he will obtain what is called a *raw key*;
3. Alice communicates publicly through the classical channel her encoding bases;
4. Bob discards all the bits that he measured with a wrong basis and communicates the right ones to Alice, in a step called *Reconciliation*;
5. They both have now a key that is most probably smaller than the raw key. This is called *sifted key*;
6. Alice and Bob can perform other actions in order to improve the security of the key (such as *error correction* or *privacy amplification*) or do an analysis in order to understand if a key can be distilled from the shared quantum states.

The process is portrayed below in figure 1.3.

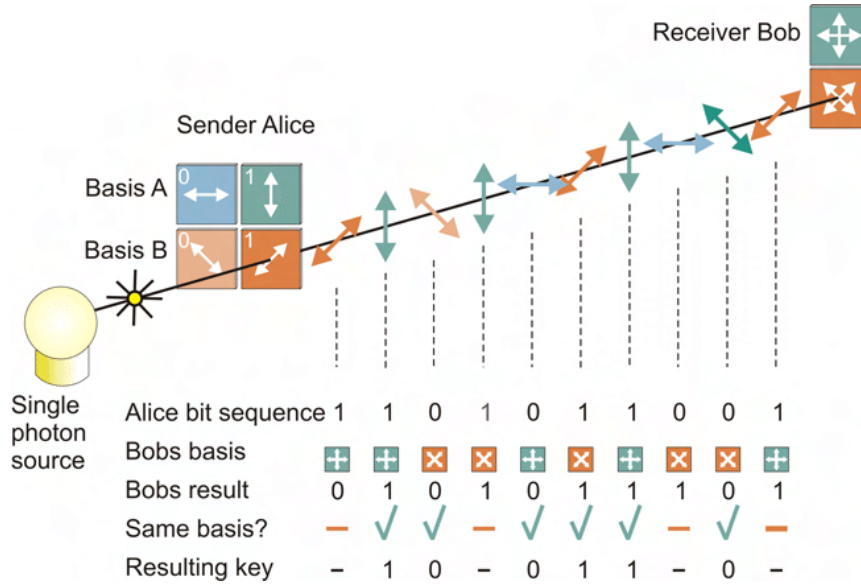


FIGURE 1.3: Working principle of the BB84 protocol. [Researchgate, 07/2025]

How can this protocol get aware of the presence of an eavesdropper? Thanks to the fundamental property of quantum mechanics related to the *collapse of the wavefunction* following a *measurement*. Be aware that Bob has a 50% probability of choosing the right basis of measurement: when he does, he has ideally a 100% probability of receiving the same state Alice sent, otherwise he receives a random state with a 50% probability. After *reconciliation* Bob should expect around a 0% error at his side. Yet, since Eve cannot gain information without introducing some noise in the channel, the simplest attack she can perform (others can be more complex, such as "*phase-covariant cloning*" attack [21]) is the so-called "*intercept-resend attack*", where she *intercepts* and measures Alice's states choosing random bases and *resends* them to Bob hoping she got them all correct. Since Eve has basically took the place of Bob in the original scheme (fig. 1.3) she also has a 50% chance of choosing the wrong basis, which will reflect at Bob's side in a whole 25% error rate after sifting. Alice and Bob can decide whether to discard the key or perform some other operations in order to exclude Eve from the communication. In table 1.1 on the following page is reported an example of transmission in presence of an *intercept-resend* attack. Comparing the situations in which the eavesdropper is present and not, after sifting the case in which Eve intercepts the message gives to Bob an error rate much higher than expected: even though this is only a specific example, this behaviour should reflect in the mean case as a 25% error rate.

1.2.2 Entropies in QKD

One of the key aspects that makes Quantum Key Distribution different from classical protocols is its ability to estimate and bound the amount of information that could have been leaked to a possible adversary. Entropies are useful tools that help into the evaluation of such quantities. In this section is not presented the whole spectrum of the entropies, but only the ones that find a possible use in this thesis.

Alice's bases	+	+	+	×	+	×	×	×	+	+	×	+	+
Alice's transmission	↑	→	→	↗	↑	↖	↖	↗	→	↑	↗	→	↑
	1	0	0	0	1	1	1	0	0	1	0	0	1
Eve's bases	+	+	×	+	×	×	+	+	+	×	×	×	×
Eve's measurement	↑	→	↗	→	↗	↖	→	↑	→	↖	↗	↖	↗
	1	0	0	0	0	1	0	1	0	1	0	1	1
Bob's bases	×	+	+	+	+	×	×	×	+	×	+	+	+
Bob's measurement in Eve's presence	↗	→	↑	→	→	↖	↖	↗	→	↖	↑	↑	↑
	0	0	1	0	0	1	1	0	0	1	1	1	1
Sifted key	/	0	1	/	0	1	1	0	0	/	/	1	1
Bob's measurement out of Eve's presence	↖	→	→	↑	↑	↖	↖	↗	→	↗	→	→	↑
	1	0	0	1	1	1	1	0	0	0	0	0	1
Sifted key	/	0	0	/	1	1	1	0	0	/	/	0	1

TABLE 1.1: Example of transmission with *intercept-resend* attack (errors in red, sifted in cyan).

Shannon Entropy

Shannon Entropy is a quantity that, in reality, applies to a fully classical system. It is helpful, though, in order to define, in a quantitative and operational way, the amount of classical information (in bits) associated with an event.

The Shannon entropy of a discrete random variable X with probability distribution $p_X(x)$ is defined as:

$$H(X) = - \sum_x p_X(x) \log(p_X(x)) \quad (1.1)$$

$H(X)$ represents, under the I.I.D. assumption, how much information we learn on average about X after the realization (i.e.: after the observation of X), or how much uncertainty we have about X before the realization. It has several useful properties, such as the non-negativity, concavity, invariance under permutations or relabeling, or the upper bound $\log |X|$. In the binary case (shown in Fig. 1.4), the Shannon Entropy can be rewritten as:

$$h_2(p) = -p \log_2(p) - (1-p) \log_2(1-p) \quad (1.2)$$

Rényi Entropies

For some applications it can be useful to give more weight to events with high or low information content. Rényi entropies are a family of entropies that generalize Shannon's for this purpose:

$$H_\alpha(X) = \frac{1}{1-\alpha} \log_2 \sum_x P_X(x)^\alpha \quad (1.3)$$

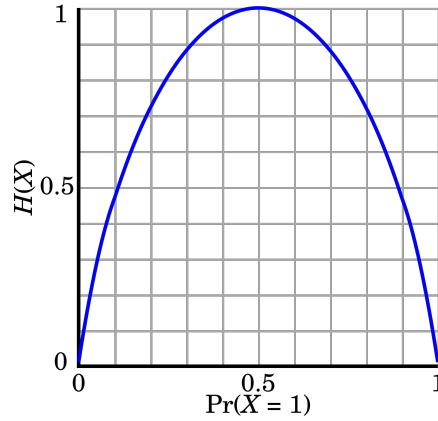


FIGURE 1.4: Binary Entropy function. [Wikipedia, 07/2025]

with $\alpha \in [0, \infty]$. Rényi entropies are monotonically decreasing in α , meaning that $\alpha > 1$ is associated to rare events, while $\alpha < 1$ is associated to more common events. Similarly to the classical case, if one is interested instead in single-shot quantities, it is possible to define the *quantum* version of the Rényi entropies:

$$H_\alpha(\rho) = \frac{1}{1-\alpha} \log \frac{\text{Tr}[\rho^\alpha]}{\text{Tr}[\rho]} \quad (1.4)$$

Max- and Min-Entropy

Another important quantity is the max-entropy $H_{\max}(X) = H_{\frac{1}{2}}(X)$, which gives more weight to events with lower surprisal. The max-entropy has an operational meaning: Shannon's noiseless coding (that states that given a source sampling from X , there exists a compression scheme that allows to store the information using $H(X)$ bits per source symbol) is valid for infinite and independent repetitions of the protocol. If the asymptotic assumption is dropped, $H_{\max}$ gives the minimum number of bits to compress X for a single realization of x . Clearly, since this requirement is more stringent than the asymptotic case, $H_{\max}(X) \geq H(X)$.

Similarly, the Min-Entropy $H_\infty(X) = H_{\min}(X)$ also has an operational meaning: it characterizes the optimal probability of correctly guessing the value of X in a single-trial.

Quantum conditional min-entropy

The quantum conditional min-entropy $H_{\min}(A|B)$ quantifies the uncertainty that we have about the system A after we get some quantum side-information B , for a single repetition of the protocol.

$$\begin{aligned} H_{\min}(A|B)_\rho &= -\inf_{\sigma_B} D_\infty(\rho_{AB} \| \mathbb{1}_A \otimes \sigma_B) \\ &= -\log \min_{\sigma_B} \{\lambda \in \mathbb{R} : \rho_{AB} \leq \lambda \cdot \mathbb{1}_A \otimes \sigma_B\} \end{aligned} \quad (1.5)$$

While the fully quantum $H_{\min}(A|B)_\rho$ provides a general definition, for QKD we are mostly interested in the $H_{\min}(X|B)_\rho$ for the classical-quantum state. In this case, the $H_{\min}(X|B)$ can be expressed in terms of the guessing probability. Considering the c-q state $\rho_{XB} = \sum_x p_X(x) |x\rangle\langle x| \otimes \rho_X^B$ and denoting as $\{E_X\}_x$ a possible POVM on B , then the

guessing probability $p_g(X|B)$ of correctly guessing X having access to the quantum system B is given by:

$$p_g(X|B) = \max_{\{E_x\}} \sum_x p_X(x) \text{Tr} [E_x \rho_X^B] \quad (1.6)$$

$$H_{\min}(X|B) = -\log(p_g(X|B))$$

In a more practical view, Alice and Eve may share a bipartite (pure) state $|\psi\rangle_{AB}$. After Alice's measurement, but before the announcement, Alice's side collapses to the classical register $|x\rangle\langle x|$ with probability $p_X(x)$, where x are the possible outcomes of Alice's measurement. ρ_X^B represents the state on Eve's side after the measurement. The best strategy for Eve to guess X is to find a set of optimal measurements E_X that maximize the overlap with ρ_X^B , to extract as much side-information as possible, and then average over $p_X(x)$.

Smooth Entropies

Up to now only one-shot tasks with no-errors were considered. For example, $H_{\min}(X|E)$ is the amount of randomness that can be extracted from X such that the output is indistinguishable from a uniform distribution. What if the output is allowed to be only ϵ distant from the uniform distribution? To characterize tasks that can tolerate an ϵ -error the quantum conditional smooth entropies $H^\epsilon(A|B)$ must be introduced:

$$H_{\min}^\epsilon(A|B) = \max_{\tilde{\rho} \in \mathcal{B}(\rho)} H_{\min}(A|B)\tilde{\rho} \quad (1.7)$$

$$H_{\max}^\epsilon(A|B) = \min_{\tilde{\rho} \in \mathcal{B}(\rho)} H_{\max}(A|B)\tilde{\rho} \quad (1.8)$$

where $\mathcal{B}(\rho) = \{\tilde{\rho} : D(\rho, \tilde{\rho}) \leq \epsilon\}$ is an ϵ -ball around a subnormalized state ρ ($D(\cdot, \cdot)$ is the purified distance). Smooth entropies are "smoothing" or excluding improbable events associated to the one-shot entropies by optimizing inside a ball ϵ -close around the original state.

1.2.3 Secret-key rate, Yield, QBER

Discussing privacy needs a mathematical term capable to quantify the amount of secrecy the communication is able to give. Generically speaking, one can define the *secret-key rate* (using perfect reconciliation techniques) as difference between the mutual informations of the parties and the eavesdropper. Or,

$$S(A; B||E) \geq \max\{I(A, B) - I(A, E), I(A, B) - I(B, E)\} \quad (1.9)$$

(knowing mutual information is defined as [2])

$$I(X; Y) = \sum_{x \in X} \sum_{y \in Y} p_{(X,Y)}(x, y) \cdot \log\left(\frac{p_{(X,Y)}(x, y)}{p_X(x)p_Y(y)}\right) = H(X) - H(X|Y)$$

which intuitively means that the two communicating parties are able to perform secret-key distillation whenever Bob has more information than Eve [45]. Note that BB84 is fairly symmetric in Alice and Bob. During reconciliation, they exchange parities to find where their bit differs and they correct such differences. Since these differences are known to the eavesdropper (reconciliation is performed over a public channel) it does not matter whether Alice's or Bob's bits serve as a key. For that reason the (strong) secret-key rate can be formally defined as [121]:

The (strong) secret key rate of X and Y with respect to Z , denoted by $S(X; Y|Z)$, is the maximal rate $R \geq 0$ such that $\forall \epsilon > 0$ and $\forall l \geq N_0(\epsilon)$ there exist a variable K with range $\mathcal{K}$ and a protocol, using public communications over an insecure but authenticated channel, with l independent instances of the variables given: $X_{1\dots l}$ to Alice(Bob), $Y_{1\dots l}$ to Bob(Alice) and $Z_{1\dots l}$ to Eve, such that Alice(Bob) and Bob(Alice) can compute keys K_C and K_D respectively, verifying $\Pr[K_{A(B)} = K \wedge K_{B(A)} = K] \geq 1 - \epsilon$, $I(K; Z_{1\dots l}M) \leq \epsilon$ and $H(K) = \log|\mathcal{K}| \geq l(R - \epsilon)$, with M the collection of messages sent by Alice(Bob) and Bob(Alice) over the insecure channel.

For the specific case of BB84 formula (1.9) evolves in:

$$S \geq q r [Q_1 - Q_\mu f(e_\mu) H_2(e_\mu) - Q_1 H_2(e_1)] \quad (1.10)$$

Where q is a base factor ($q = 1/2$ for BB84 as the probability of each base is 50%), r is the key rate, Q_i is the gain of the channel ($i = 1$ when a click at Bob's side is generated from a single photon event, $i = \mu$ when is generated from a Poisson distribution of parameter μ), f is an efficiency term related to error correction in function of the error rate e_i , and H_2 is the binary Shannon entropy. In summary,

- Q_1 is a term related to the *raw key*;
- $Q_\mu f(e_\mu) H_2(e_\mu)$ is a term related to error correction;
- $Q_1 H_2(e_1)$ is a term related to privacy amplification.

As it can be seen from formula (1.10), the error rate is of utmost importance in the evaluation of the secure key generation rate. Normalizing the error rate with the key rate gives the QBER E_n , which can be mnemonically defined as the "amount of information the eavesdropper is in possession" or, more mathematically, as

$$E_n = \frac{\text{error rate } e}{\text{key rate } r} = p_f + \frac{p_d n q \Sigma f_r t_l}{2} \mu \quad (1.11)$$

where p_f is the probability for a wrong click ($1 - 2\%$), p_d is the probability for a wrong photon signal (Si: 10^{-7} , GaAs: 10^{-5}), n the number of detections, q can be seen as a phase term = $1/2$ (better for optical fibers) or a polarizaton = 1 (better in free space), Σ the detector efficiency, f_r the pulse repeat frequency, t_l the transmission rate (for large distances is usually small) and μ the attenuation for light pulses (for single photons is equal to 1).

Usually the QBER in absence of an eavesdropper is acceptable up to around 11% but mostly close to 2% [3] (other works: [48], [68], [46]). Another important term for secret key distillation is the *Yield* Y_i , that can be described as a probability distribution:

$$Y_i = P_i [\text{Bob's detector clicks} | \text{Alice sent an } i\text{-photon signal}] \quad (1.12)$$

Secret-key rate, QBER and Yield will cover an important role in the *Decoy-States protocol*, which will be discussed in section 1.3.

1.2.4 Practical QKD: approximations for the BB84 protocol

In most of the real-life scenarios, the working conditions for BB84 are too strict to be applied in practice. First of all, single photons sources are not easy to implement other than being too expensive. An alternative solution is using *weak coherent pulses*, i.e. coherent states with a low average number of photons. Using the Fock states notation, a coherent state $|\alpha\rangle$ has an average number of photons equal to $\mu = |\alpha|^2/4N_0$, following a Poissonian distribution

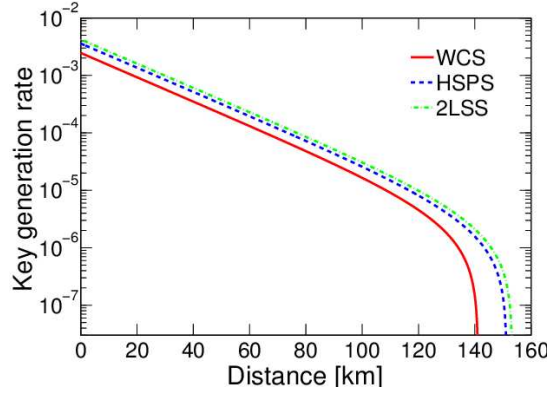


FIGURE 1.5: Key generation rate with different light sources: weak coherent state (WCS), heralded single-photon source (HSPS), and 2LS source (2LSS) with $\sigma = \Gamma/2$ and $P = 20$. [131]

($Pr[n] = \mathcal{P}(\mu) = e^{-\mu} \frac{\mu^n}{n!}$, n number of photons). Hence, by creating a coherent state with $\mu \ll 1$ one rarely creates more than one photon. For instance, when $\mu = 0.1$, the 90.5% of the pulses are empty, 9% are single photon pulses, while the remaining contain more than one photon. Weak coherent pulses are very easy to create using for instance a laser diode, while an attenuator can be also introduced to lower the pulse intensity. The main drawback is that multi-photon pulses carry all the same phase or polarization information and it could be possible for an eavesdropper to detect them, extract the information of one and resend the others to Bob's side through a lossless channel (supposing it exists). This kind of attack is called "*photon-number splitting*" (PNS) and could be in principle undetectable since it does not increase Bob's error rate. By now, the practical use of weak coherent pulses makes them the most favoured by the majority. The advantage of single-photon sources is the longer achievable distances: since no multi-photon pulses are produced, the information carried has better secrecy and can travel farther distances while also providing better robustness against dark counts (fig. 1.5). Real single photon sources are still an active area of research and various approaches are being tested, such as trapped atoms/ions [51], dye molecules in solvent [77], nitrogen-vacancy color centers in diamonds [87], single electrons in p-n junctions [128] or electron-hole pairs in semiconductor quantum dots [55].

1.2.5 Unconditional security

We already seen that some classical algorithms (like OTP) can achieve perfect secrecy in some conditions, which are although not so easy to reproduce in a real-life scenario. For example, in the case of one-time-pad, the four conditions reported in section 1.1 seem logical but truly are not easy to achieve: the true randomness of the key isn't guaranteed with pseudo-random generators integrated in modern computers, the length of the key is often difficult to match the length of the plaintext, and it's also frustrating to use it for one and one message only. Without mentioning that the secrecy of the key along the channel is not an easy task when classical communication is involved. It can be demonstrated that BB84, thanks to the mentioned properties (non-commuting bases, no-cloning theorem, collapse of the wavefunction), can achieve *unconditional security*, i.e. it presents mathematical proofs for perfect secrecy in the following conditions:

- Eve cannot intrude into Alice's and Bob's devices;
- The random number generators must provide true random numbers (not pseudo-random);

- The classical channel is authenticated;
- Devices are trusted and characterized.

Which are much less strict conditions. More sophisticated protocols that want to break free from these constraints exist (like DI-QKD [93] or MDI-QKD [72]), yet they did not find any practical application up to the moment. Another problem with classical public-key cryptographic algorithms is that they often rely on decoding problems that take a long time to be solved with the current methods. Currently, we know that prime numbers factorization, the most common cryptographic methodology, belongs to the NP class but it's not proven that is NP-hard, i.e. that it can be solved in polynomial time. The day a much faster algorithm is found, cryptographic systems would become ineffective. That's exactly what happened with Shor's algorithm in 1997 [106], which is capable of solving prime factorization in a time $O(n^3)$ (belongs to the BQP class [4]) (fig. 1.6), but luckily there was still time to investigate new cryptographic methods before quantum computers were commercially available.

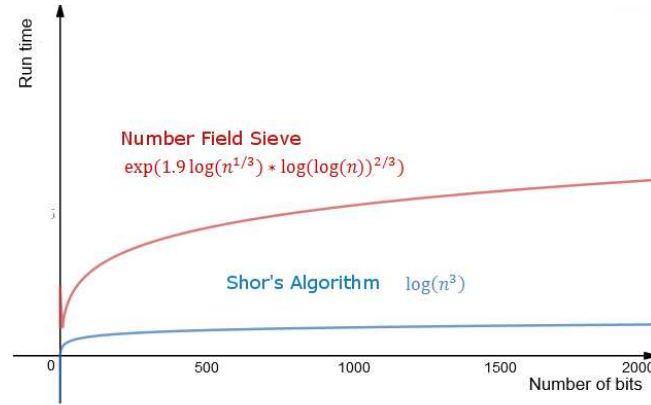


FIGURE 1.6: Comparison of the time complexities between Shor's algorithm and the best current classical algorithm for primes factorization.

[sharkyspool.home.blog, 07/2025]

1.2.6 Quantum Mutual Information and Holevo Bound

Similarly to the classical case, we can define the quantum mutual information, that captures the information shared between two subsystems A and B as:

$$\begin{aligned}
 I(A : B) &= H(A)_\rho + H(B)_\rho - H(A, B)_\rho \\
 &= H(A)_\rho - H(A|B)_\rho \\
 &= H(B)_\rho - H(B|A)_\rho
 \end{aligned} \tag{1.13}$$

In a classical example, for two binary X, Y :

$$I(X : Y) = H(X) - H(X|Y) \leq 1 \quad \text{since } H(X) \leq 1 \text{ and } H(X|Y) \geq 0.$$

This means that no more than 1 bit for use of the channel can be transmitted between Alice and Bob. Instead, for ρ_{AB} , density matrix of the Bell state

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B):$$

$$I(A : B) = 1 - (-1) = 2.$$

It means that one e-bit (Bell state) can be used to transmit 2 classical bits via superdense coding.

The Holevo bound χ allows to put an upper-bound on the maximum amount of information that can be known about a quantum system. Suppose Alice prepares a state ρ_X with $X \in \{0, \dots, n\}$ with probability p_X , and Bob performs a measurement using POVM elements $\{E_Y\}$ with outcome Y , then:

$$H(X : Y) \leq \chi = H(\rho) - \sum_X p_X H(\rho_X) \quad (1.14)$$

with $\rho = \sum_X p_X \rho_X$. This quantity is quite used in characterizing the ability to send classical information with quantum states.

1.2.7 Fiber-based and satellite-based QKD

There are a variety of optical techniques for implementing QKD. The most common class of solutions encode each bit of the secret key onto discrete degrees of freedom of optical signals, and hence is termed collectively as discrete-variable QKD (DV-QKD). An alternative approach employs coherent communication techniques to encode the private information, and is known as continuous-variable QKD (CV-QKD). Both approaches have seen dedicated engineering that has led to increased key generation rates and improved compatibility with current communications infrastructure. However, both approaches face a similar obstacle when attempting to implement wide-scale deployment of QKD: physical communication channels introduce transmission losses that increase exponentially with distance, greatly limiting the secure key rates that can be achieved over long ranges. For any pure-loss channel with transmittance η , it has been shown that the secure key rate per mode of any QKD protocol scales linearly with η for small η . This places a fundamental limit to the maximum distance attainable by QKD protocols relying on direct transmission. To put this into perspective, consider that a conventional telecommunications fiber with an attenuation of 0.18 dB/km stretching over 1000 km has a theoretical transmittance of precisely $\eta = 10^{-18}$ worse in real-world deployments—making the resulting key rates forbiddingly small. The problem remains even if using state-of-the-art fibers which can reach attenuations of 0.142 dB/km. Note that the classical solution of using repeaters along the way by now cannot be exploited for the no-cloning theorem. Quantum repeaters are currently an active area of research and they wouldn't perfectly reproduce the superposition state anyway. Experiments have been reported where QKD was performed for distances of up to 404 km [129], but the resulting key rates remain several orders of magnitude smaller than the requirements for practicable deployment. Sufficiently large key rates can only be obtained over metropolitan-scale networks, where the range is within 100 km. In principle, it is possible to extend the range of QKD by using quantum repeaters. Some proposals for quantum repeaters rely on heralded entanglement generation and purification, while other recent architectures employ logical Qubits capable of quantum error-correction to overcome both operational errors and errors due to loss [40]. The difficulty of constructing such systems, however, is comparable to the challenges faced in building universal quantum computers, with the required technology unlikely to be available in the near future. An alternative, which is viable with the present level of technology, is to use satellites as intermediate trusted nodes for communication between locations on the ground. By placing a satellite above the Earth's atmosphere, direct links can be established between ground stations and the satellite, thus enabling communication between distant points on the planet. Atmospheric attenuation in free space is less significant than in fiber (fig. 1.7), where for instance values of 0.07 dB/km can be achieved at 2400 m above sea-level, with higher

attenuations at lower altitudes and negligible attenuation in the vacuum above the Earth's atmosphere. Note also that polarization encoding is favoured in free-space scenarios

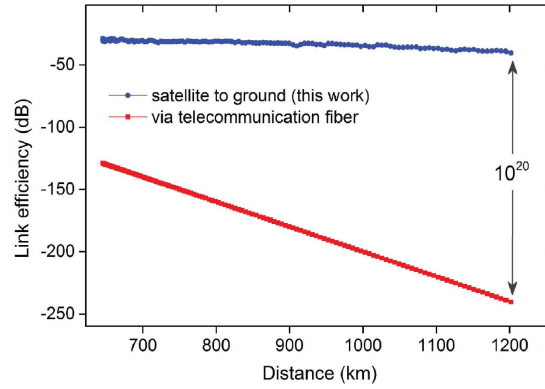


FIGURE 1.7: Satellite and fiber communication efficiencies. [68]

because in optical fibers polarization tends to fluctuate, where instead is preferred phase encoding exploiting Mach-Zehnder Interferometers (fig. 1.8).

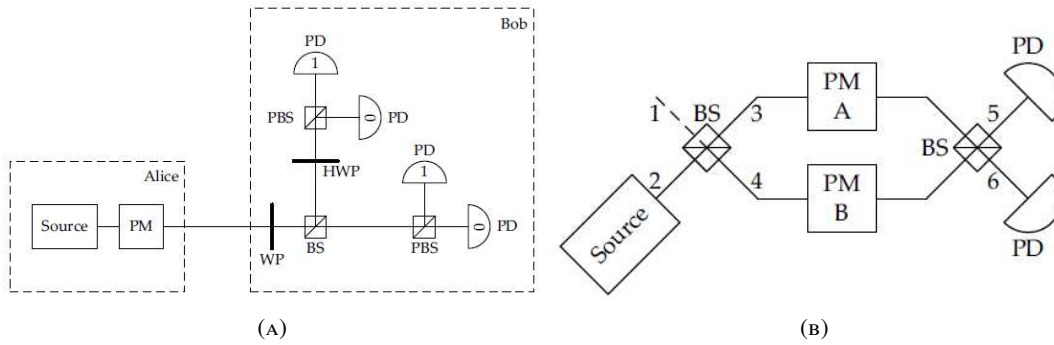


FIGURE 1.8: Examples of polarization state (a) and phase state (b) encoders. [121]

Dominant sources of loss in this case occur due to beam diffraction and the limited size of telescopes at the receiver. However, the overall effect is a greatly reduced amount of loss compared with ground-level transmission, making satellite QKD a promising route to enable secure key generation across global distances. Consequently, a number of efforts are under way to raise the technology readiness level of satellite QKD. These projects range from truck-based tests of pointing and tracking mechanisms, to in-orbit testing of quantum light sources, to full QKD demonstrations using orbiting satellites. Altogether, these efforts will enable global QKD services as well as advanced fundamental experiments.[22]

In the meanwhile, hollow-core optical fibres (HCF), particularly the nested-antiresonant nodeless (NANF) designs, are emerging as an efficient medium for QKD, owing to their ultra-low attenuation, minimal latency, dramatically reduced nonlinearity, and excellent polarization purity-enabling simultaneous transmission of classical and single-photon quantum signals over shared links with minimal crosstalk. Recent trials by British Telecommunications using Lumenisity's CoreSmart HCF cables have demonstrated operation of QKD systems over 6 Km with reduced latency and negligible scattering-induced interference between classical and quantum channels [64]. Concurrently, research culminating in Microsoft-backed deployment of NANF-based HCF in Azure's network, achieving record-low loss (~ 0.091 dB/km at 1550 nm) and deployment of >1200

km (with plans for 15000 km), promises to extend QKD to high-performance, scalable cloud and AI infrastructures [92]. Furthermore, laboratory studies confirm that NANF HCFs exhibit exceptional polarization extinction ratios (−30 to −70 dB across telecom bands) and low dispersion suitable for low-QBER QKD protocols [8], and real-time data-signals transmitted over HCF span-lengths reaching 301.7 km using a novel high-power (37 dBm) HCF line-system achieved full C-band system data-rate of 25.6 Tb/s after 200.5 km with negligible fiber transmission penalty, demonstrating the potential of HCFs to expand unamplified links [13].

1.3 Decoy state QKD

As discussed in section 1.2.4, in standard BB84 protocol, only single photon pulses emitted by Alice are guaranteed to be secure, otherwise opening the channel to PNS attacks. Consequently, the secure key generation rate per signal state emitted by Alice is given by:

$$S \geq Q_\mu \{-H_2(E_\mu) + \Omega[1 - H_2(e_1)]\}$$

with Q_μ the gain of the signal state, E_μ the QBER of the signal state, Ω and e_1 the fraction and QBER of detection events that originated from single-photon arrivals, and H_2 the classic binary Shannon entropy. It is in general complicated to obtain a lower bound on Ω and an upper bound on e_1 . The decoy states idea, proposed by Hwang [57], is capable of performing this type of estimation in an efficient manner. The concept of decoy-state QKD is that Alice prepares a set of additional states (decoy states, in addition to the standard BB84 ones), that are used for detecting eavesdropping attacks only, whereas the standard states are used for key generation only. The difference between the two types of states is their intensities (i.e. their photon number distributions). If they possess the same characteristics, Eve cannot distinguish a decoy-state from a signal-state and the only information Eve can obtain is a signal's number of photons. Therefore, the yield Y_n and QBER e_n depend only on the photon number n , but not from which state (decoy or signal) the signal is from. The most important part of the decoy-state idea can be summarized by the following:

$$Y_n(\text{signal}) = Y_n(\text{decoy}) = Y_n \quad (1.15)$$

$$e_n(\text{signal}) = e_n(\text{decoy}) = e_n \quad (1.16)$$

Here's an example (tab. 1.2):

Yields	Eve absent and $Y_1 = 100\%$	Eve absent and $Y_1 = 0\%$	Eve present
Y_1	100%	0%	0%
Y_2	100%	$P[\mathcal{P}(\mu_2) = 2] \ll 1$	100%
Y_n	100%	$P[\mathcal{P}(\mu_n) = n] \ll 1$	100%
Conclusion:	correct transmission	consistent channel losses	PNS attack

TABLE 1.2: Detection of Eve performing a *PNS attack* using decoy state QKD.

Therefore a PNS attack gives an abnormally high transmission probability when increasing the number of photons from 1 to 2 [70]. The procedure is the following (note that nor Alice or Bob have direct access to the number of photons of each symbol):

1. Alice send a signal-state or a decoy-state randomly;
2. Bob receives the signals and sends an acknowledgement;

3. Alice publicly shares which of the states were decoy- and which were signal-;
4. Alice and Bob calculate the probability of transmission for decoy- and signal- states.

Considering the yield Y_n is given by (transmission efficiency of n -photon signals $\eta_n = 1 - (1 - \eta)^n$, η transmission probability of each photon):

$$\begin{cases} Y_0 = p_{dark} \\ Y_n = \eta_n + p_{dark} - \eta_n \cdot p_{dark} \approx \eta_n + p_{dark} & n \geq 1 \end{cases} \quad (1.17)$$

and the error rates e_n are given by:

$$\begin{cases} e_0 = 1/2 \\ e_n = (e_{detector} \cdot \eta_n + \frac{1}{2}p_{dark})/Y_n & n \geq 1 \end{cases} \quad (1.18)$$

While only a few decoy-states are sufficient, we'll by now consider the case where Alice picks an infinite number of intensities for decoy-states. Imagine Alice varies over all non-negative values of μ in a random and independent manner for each signal, then Alice and Bob can measure the yield Q_μ and the QBER E_μ . Since the relations between the variables $\{Q_\mu, Y_n\}$ and $\{E_\mu, e_n\}$ are linear, given Q_μ and E_μ measured from the experiments, Alice and Bob can deduce with high confidence the variables Y_n and e_n . This means that they can constrain the yields, Y_n and QBER e_n simultaneously for all n . Supposing Alice and Bob know the properties of their channel well, they know what ranges of Y_n and e_n are adequate and any intrusion by Eve that will change these parameters will be caught with a high probability. In summary, the possibility for Alice and Bob of verifying experimentally the values of Y_n and e_n greatly strengthens their eavesdropping detecting possibilities, leading their QKD system to a dramatic improvement (fig. 1.9).

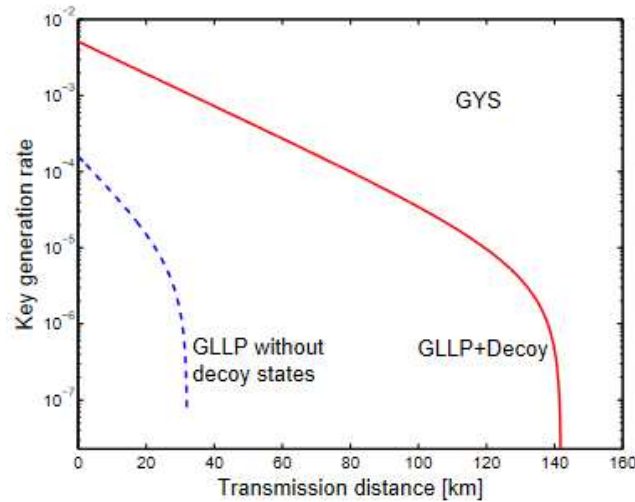


FIGURE 1.9: Performances of decoy state QKD with respect to basic implementation. [73]

Since it's the case of the transmitter we developed, we will assume Alice can prepare phase-randomized coherent states and that she can tune her power for each signal. This can be done by using variable optical attenuators (VOAs). Basically Alice can prepare any Poissonian (with parameter μ) distribution of photon-number states and, also, she can change the parameter μ for each signal.

Consider the gain Q_μ for a coherent state $|\sqrt{\mu}e^{i\theta}\rangle$. Then, being Y_n the yield of an n -photon signal,

$$Q_\mu = Y_0 e^{-\mu} + Y_1 e^{-\mu} \mu + Y_2 e^{-\mu} (\mu^2/2) + \dots + Y_n e^{-\mu} (\mu^n/n!) + \dots \quad (1.19)$$

the QBER E_μ is given by:

$$Q_\mu E_\mu = Y_0 e^{-\mu} e_0 + Y_1 e^{-\mu} \mu e_1 + Y_2 e^{-\mu} (\mu^2/2) e_2 + \dots + Y_n e^{-\mu} (\mu^n/n!) e_n + \dots \quad (1.20)$$

The fraction of Bob's detection events that have originated from single-photon signals emitted by Alice is:

$$\Omega = \frac{Q_1}{Q_\mu} = \frac{Y_1 \cdot \mu e^{-\mu}}{Q_\mu} \quad (1.21)$$

Introducing inefficiency of error correction in eq. 1.15 as $f(e) > 1$:

$$S \geq q \{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1 [1 - H_2(e_1)]\} \quad (1.22)$$

where q is an efficiency term depending on the implementation (1/2 for BB84, because 50% of the times Alice and Bob's bases aren't compatible). Comparing with the GLLP result:

$$S \geq Q_\mu \left\{ -H_2(E_\mu) + \Omega \left[1 - H_2\left(\frac{E_\mu}{\Omega}\right) \right] \right\} \quad (1.23)$$

A much better lower bound on Ω and upper bound on e_1 can be obtained. With this method there is a substantial increase in the net key generation rate from $O(\eta^2)$ to $O(\eta)$ (η overall transmission probability of the channel). [73]

1.3.1 Two decoy states

To lower bound eq. 1.23 one can put a lower bound on Y_1 and an upper bound on e_1 (following extracted from [80]). Intuitively we can exploit only two decoy states for that and consequently for a practical QKD implementation. Let's suppose that Alice and Bob choose two decoy states with expected photon numbers ν_1 and ν_2 which satisfy

$$\begin{aligned} 0 &\leq \nu_2 < \nu_1 \\ \nu_1 + \nu_2 &< \mu \end{aligned} \quad (1.24)$$

where μ is the expected photon number of the signal state.

Lower bound of Y_1 : The gains of $\nu_{1,2}$ are given by

$$Q_{\nu_1} = \sum_{i=0}^{\infty} Y_i \frac{\nu_1^i}{i!} e^{-\nu_1} \quad (1.25)$$

$$Q_{\nu_2} = \sum_{i=0}^{\infty} Y_i \frac{\nu_2^i}{i!} e^{-\nu_2} \quad (1.26)$$

First, Alice and Bob can estimate the lower bound of the background rate Y_0 by $\nu_1 e^{\nu_2} \cdot (1.26) - \nu_2 e^{\nu_1} \cdot (1.25)$:

$$\begin{aligned}
 \nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1} &= \nu_1 \sum_{i=0}^{\infty} Y_i \frac{\nu_2^i}{i!} - \nu_2 \sum_{i=0}^{\infty} Y_i \frac{\nu_1^i}{i!} \\
 &= \nu_1 Y_0 + \nu_1 Y_1 \nu_2 + \nu_1 Y_2 \frac{\nu_2^2}{2} + \nu_1 Y_3 \frac{\nu_2^3}{3!} + \dots - \nu_2 Y_0 - \nu_2 Y_1 \nu_1 - \nu_2 Y_2 \frac{\nu_1^2}{2} - \nu_2 Y_3 \frac{\nu_1^3}{3!} + \dots \\
 &= (\nu_1 - \nu_2) Y_0 + \cancel{Y_1(\nu_1 \nu_2 - \nu_2 \nu_1)} + Y_2(\nu_1 \frac{\nu_2^2}{2} - \nu_2 \frac{\nu_1^2}{2}) + Y_3(\nu_1 \frac{\nu_2^3}{3!} - \nu_2 \frac{\nu_1^3}{3!}) + \dots \\
 &= (\nu_1 - \nu_2) Y_0 - \nu_1 \nu_2 \left(Y_2 \frac{\nu_1 - \nu_2}{2!} + Y_3 \frac{\nu_1^2 - \nu_2^2}{3!} + \dots \right) \leq (\nu_1 - \nu_2) Y_0
 \end{aligned}$$

Thus, a crude lower bound for Y_0 is given by (expliciting Y_0):

$$Y_0 \geq \max \left\{ \frac{\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1}}{\nu_1 - \nu_2}, 0 \right\} = Y_0^L \quad (1.27)$$

where the equality holds when $\nu_2 = 0$ (vacuum decoy). From eq. (1.19) the contribution of multi-photon states in signal state can be expressed¹ by:

$$\sum_{i=2}^{\infty} Y_i \frac{\mu^i}{i!} = Q_{\mu} e^{\mu} - Y_0 - Y_1 \mu \quad (1.28)$$

Combining eq. (1.25), (1.26) under the conditions (1.24):

$$\begin{aligned}
 Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} &= Y_1(\nu_1 - \nu_2) + \sum_{i=2}^{\infty} Y_i \frac{\nu_1^i - \nu_2^i}{i!} \\
 &\leq Y_1(\nu_1 - \nu_2) + \frac{\nu_1^2 - \nu_2^2}{\mu^2} \sum_{i=2}^{\infty} Y_i \frac{\mu^i}{i!} \\
 &= Y_1(\nu_1 - \nu_2) + \frac{\nu_1^2 - \nu_2^2}{\mu^2} (Q_{\mu} e^{\mu} - Y_0 - Y_1 \mu) \\
 &\leq Y_1(\nu_1 - \nu_2) + \frac{\nu_1^2 - \nu_2^2}{\mu^2} (Q_{\mu} e^{\mu} - Y_0^L - Y_1 \mu)
 \end{aligned} \quad (1.29)$$

The lower bound on Y_1 is thus given:

$$\begin{aligned}
 Y_1 &\geq Y_1^{L, \nu_1, \nu_2} \\
 &= \frac{\mu}{\mu \nu_1 - \mu \nu_2 - \nu_1^2 + \nu_2^2} \left[Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2} (Q_{\mu} e^{\mu} - Y_0^L) \right]
 \end{aligned} \quad (1.30)$$

¹Because of the following hold:

$$\begin{aligned}
 \eta_i &= 1 - (1 - \eta)^i \\
 Y_i &= Y_0 + \eta_i - Y_0 \eta_i \simeq Y_0 + \eta_i \\
 \sum_{i=0}^{\infty} \frac{\mu^i}{i!} e^{-\mu} &= 1 \\
 \implies Q_{\mu} &= Y_0 + 1 - e^{-\eta \mu} \quad , \quad E_{\mu} Q_{\mu} = e_0 Y_0 + e_{\text{detector}} (1 - e^{-\eta \mu})
 \end{aligned}$$

And the gain of the single photon state:

$$\begin{aligned} Q_1 &\geq Q_1^{L, \nu_1, \nu_2} \\ &= \frac{\mu^2 e^{-\mu}}{\mu \nu_1 - \mu \nu_2 - \nu_1^2 + \nu_2^2} [Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2} (Q_{\mu} e^{\mu} - Y_0^L)] \end{aligned} \quad (1.31)$$

Upper bound of e_1 : According to eq.(1.20), the QBER of the weak decoy state is given by:

$$E_{\nu_1} Q_{\nu_1} e^{\nu_1} = e_0 Y_0 + e_1 \nu_1 Y_1 + \sum_{i=2}^{\infty} e_i Y_i \frac{\nu_1^i}{i!} \quad (1.32)$$

$$E_{\nu_2} Q_{\nu_2} e^{\nu_2} = e_0 Y_0 + e_1 \nu_2 Y_1 + \sum_{i=2}^{\infty} e_i Y_i \frac{\nu_2^i}{i!} \quad (1.33)$$

An upper bound of e_1 can be obtained directly from these two:

$$e_1 \leq e_1^{U, \nu_1, \nu_2} = \frac{E_{\nu_1} Q_{\nu_1} e^{\nu_1} - E_{\nu_2} Q_{\nu_2} e^{\nu_2}}{(\nu_1 - \nu_2) Y_1^{L, \nu_1, \nu_2}} \quad (1.34)$$

Note that the lower bound on Y_1 is necessary to find the upper bound on e_1 . Having the bounds Alice and Bob can compute finally the key generation rate as:

$$S \geq \{ -Q_{\mu} f(E_{\mu}) H_2(E_{\mu}) + Q_1^{L, \nu_1, \nu_2} [1 - H_2(e^{U, \nu_1, \nu_2})] \} \quad (1.35)$$

1.4 Three-state one-decoy *Efficient-BB84*

A common and simple variation of BB84 is named "*Efficient BB84*" [71], and has Alice and Bob choosing their bases $+$, $\times$ with probability p_+ and $p_{\times} = 1 - p_+$ different from 50%. In a practical environment, the use of one single decoy level (*Lo* and *Hi* for, respectively, low and high mean-photon-number) is enough to guarantee the security of the protocol. The combination of these two factors grants the development of a simplified QKD transmitter that doesn't require much elaborate components, while keeping the costs of the source contained.

1.4.1 Secret Key Rate of the protocol

In this protocol, the base $+$ = $\mathbb{Z}$ is used to generate the key, while the base $\times$ = $\mathbb{X}$ is used as a check-basis to detect Eve.

To give a good estimate on the upper bound of the secret key rate SKR , statistical fluctuations coming from the finite generated key length should be taken into account. The SKR can be defined as the ratio between the secret bits l distilled from the total bits sent N_{tot} scaled by the source repetition rate R :

$$SKR = \frac{l}{N_{\text{tot}}} R \quad (1.36)$$

The critical part of this calculation is the evaluation of l , that can be upper-bounded by

$$l \leq s_{\mathbb{Z}}^l(0) + s_{\mathbb{Z}}^l(1)(1 - H_2(\phi_{\mathbb{X}}^u)) - \lambda_{\text{EC}} - a \log_2 \left(\frac{b}{\epsilon_{\text{sec}}} \right) - \log_2 \left(\frac{2}{\epsilon_{\text{cor}}} \right) \quad (1.37)$$

where $s_{\mathbb{Z}}^l(0)$ is the lower bound of the vacuum events for the $\mathbb{Z}$ basis (where Bob had a detection and the pulse sent by Alice contained no photons), $s_{\mathbb{Z}}^l(1)$ is the lower bound of the single photon detection for the $\mathbb{Z}$ basis (number of detections at Bob's side when the pulse sent by Alice contained only one photon), $\phi_{\mathbb{X}}^u$ is the phase error upper bound for the $\mathbb{X}$ basis (that takes into account the finite size), λ_{EC} is the number of bits disclosed by error correction, a and b are parameters that depend on the choice one-decoy or two-decoy ($a = 6$ and $b = 21$ for the two-decoy approach and $a = 6$ and $b = 19$ for the one-decoy protocol), ϵ_{sec} is a secrecy parameter, ϵ_{cor} is a correctness parameter. $H_2(x)$ is the Binary Shannon Entropy, defined as:

$$H_2(x) = -x \log_2(x) - (1-x) \log_2(1-x) \quad (1.38)$$

Except for ϵ_{sec} and ϵ_{cor} that are arbitrary input parameters, all the others can be derived knowing only the *expected* probability distributions and the *observed* ones, obtained after the sifting operation on the finite block. The *expected* probabilities depend on the mean number of photons for each decoy μ_{Lo}, μ_{Hi} , and their probability of occurrence p_{Lo}, p_{Hi} . The *observed* distributions are related to the total number of qubits received $n_{b,i}$ and the number of qubits received $m_{b,i}$ for each basis $b \in \{\mathbb{Z}, \mathbb{X}\}$ and intensity $i \in \{Lo, Hi\}$.

The first parameters to be computed, the *expected* ones, are the probabilities that Alice sent an n -photon state

$$\tau(n) = \sum_i \tau(n, i) \quad (1.39)$$

where $\tau(n, i)$ is the Poisson arrival distribution for intensity i

$$\tau(n, i) = p_i e^{-\mu_i} \frac{\mu_i^n}{n!} \quad (1.40)$$

The second parameters to be computed are the *observed* uncertainties, i.e., the confidence levels that are necessary to define upper and lower bounds on the total blocks

$$\Delta_n^{\pm}(b, i) = \frac{e^{\mu_i}}{p_i} (n_{b,i} \pm \delta(n_{b,i}, \epsilon_1)) \quad (1.41)$$

and on the errors

$$\Delta_m^{\pm}(b, i) = \frac{e^{\mu_i}}{p_i} (m_{b,i} \pm \delta(m_{b,i}, \epsilon_1)) \quad (1.42)$$

where ϵ_1 is an additional input probability that accounts for the error in the single photon component and

$$\delta(n, \epsilon) = \sqrt{\frac{-n \ln(\epsilon)}{2}} \quad (1.43)$$

is the fluctuation in the block.

With these parameters, it is possible to calculate a tight-upper bound of Bob's detection when Alice sent zero photons on the basis $\mathbb{Z}$ (similarly for $\mathbb{X}$)

$$\hat{s}_{\mathbb{Z}}^u(0) = \min \left(s_{\mathbb{Z}}^u(0), s_{\mathbb{Z}, Lo}^u(0), s_{\mathbb{Z}, Hi}^u(0) \right) \quad (1.44)$$

considering the minimum between the upper bound of

$$s_{\mathbb{Z}}^u(0) = 2 (m_{\mathbb{Z}} + \delta(n_{\mathbb{Z}}, \epsilon_1)) \quad (1.45)$$

and

$$s_{\mathbb{Z},i}^u(0) = 2 (\tau_0 \Delta_m^+(\mathbb{Z}, i) + \delta(n_{\mathbb{Z}}, \epsilon_1)) \quad (1.46)$$

Also, it is necessary to compute the lower-bound

$$s_{\mathbb{Z}}^l(0) = \frac{\tau_0}{\mu_{Hi} - \mu_{Lo}} (\mu_{Hi} \Delta_n^-(\mathbb{Z}, Lo) - \mu_{Lo} \Delta_n^+(\mathbb{Z}, Hi)) \quad (1.47)$$

Consequently, it is possible to calculate Bob's detection when Alice sent one photon in the basis $\mathbb{Z}$ (similarly for $\mathbb{X}$)

$$s_{\mathbb{Z}}^l(1) = \tau_1 \frac{\mu_{Hi}}{\mu_{Lo}(\mu_{Hi} - \mu_{Lo})} \left(\Delta_n^-(\mathbb{Z}, Lo) - \frac{\mu_{Lo}^2}{\mu_{Hi}^2} \Delta_n^+(\mathbb{Z}, Hi) - \frac{\mu_{Hi}^2 - \mu_{Lo}^2}{\mu_{Hi}^2} s_{\mathbb{Z}}^u(0) \frac{1}{\tau_0} \right) \quad (1.48)$$

and the relative detection errors

$$v_{\mathbb{Z}}^u(1) = \frac{\tau_1}{\mu_{Hi} - \mu_{Lo}} (\Delta_m^+(\mathbb{Z}, H) - \Delta_m^-(\mathbb{Z}, L)) \quad (1.49)$$

Another parameter to be computed is the upper bound phase error in the $\mathbb{X}$ basis

$$\phi_{\mathbb{X}}^u = \frac{v_{\mathbb{X}}^u(1)}{s_{\mathbb{X}}^l(1)} + \gamma \left(\epsilon_{\text{sec}}, \frac{v_{\mathbb{X}}^u(1)}{s_{\mathbb{X}}^l(1)}, s_{\mathbb{Z}}^l(1), s_{\mathbb{X}}^l(1) \right) \quad (1.50)$$

where

$$\gamma(a, b, c, d) = \sqrt{\frac{(c+d)(1-b)b}{cd \ln(2)}} \log_2 \left(\frac{c+d}{cd(1-b)b} \frac{21^2}{a^2} \right)$$

The last parameter is the length discarded by error correction, which is

$$\lambda_{\text{EC}} = n_{\mathbb{Z}} f_{\text{EC}} H_2 \left(\frac{m_{\mathbb{Z}}}{n_{\mathbb{Z}}} \right)$$

This section has been slightly based on [99].

1.5 Post-processing

Since the original BB84 protocol, that had many theoretical assumptions, state-of-the-art QKD has improved by introducing new layers of post-processing to distill a secure key. After the quantum transmission phase (and sifting), Alice and Bob hold a pair of bit strings K_A and K_B that are, in general, partially correlated and partially secure. In the classical post-processing, they turn these bit strings into secure keys. The first step is the *parameter estimation*: Alice and Bob have to estimate how many errors are there in their respective bit strings and with this the amount of information that was leaked to Eve during the quantum phase. If the error rate is above a certain threshold, they abort the protocol. Otherwise, they continue with the classical post-processing. Then, they perform *error correction*, where their different bit strings are turned into identical ones. The final part is *privacy*

amplification, where any residual information that Eve may have about the key is removed. In all of these tasks, Alice and Bob use some part of their bit strings to achieve the respective goal. The key point is to find efficient methods such that only a small amount of bits has to be discarded for this purpose. In the following sections, only the finite-key scenario will be treated (being the finite-key the only realistic one).

1.5.1 Parameter Estimation

After the quantum stage of the QKD protocol, in which M symbols have been exchanged, and the sifting phase, Alice and Bob have to estimate the error rate between their strings K_A and K_B and therefore the information that has been leaked to Eve. For example, an estimate of the max-entropy of Alice's string conditioned on Bob's string can be used to prove a lower bound on the min-entropy of Alice's string conditioned on Eve's state, which proves that the protocol is secret (we will see why in the following). Parameter estimation can be dependent on what kinds of assumptions are made in the model of the protocol. However, parameter estimation can be performed for many protocols independently of these assumptions. The secret key rate is defined as:

$$r = \frac{l}{M} \quad (1.51)$$

where l is the length of the finite key. After Alice and Bob have completed the quantum phase of the protocol, they want to make an estimate of the error rate in order to decide whether to abort the protocol because too much information was leaked to Eve or to proceed with transforming their bit strings into a secure key. For this purpose, they use a small sample (of dimension k) of their (sifted) bit strings (of total dimension $N < M$) to estimate a global property, namely the error rate, of those strings. The standard procedure here is that Alice sends a small sample of her string to Bob that he compares to his string. He then tells Alice the error rate he sees. If it is beyond a certain threshold, they abort the protocol, otherwise, they continue. Although Alice and Bob only know the error rate for a small sample of their strings, this information enables them to make statements about the whole strings, which is due to the so-called Chernoff-Hoeffding type bounds. These bounds are statistical inequalities that state that, given a random subset of data, a statistical property of the sample must be close to the statistical property of the whole data. These kinds of bounds are going to be discussed in the following to understand their link with the security of the protocol and how to make use of them in the parameter estimation step. We define a bound known as Serfling inequality:

Lemma (Serfling's Inequality)

For a set of N random variables with values $z_i \in (0, 1)$ (where $i = 1, \dots, N$) the average is defined as:

$$\bar{z} = \frac{1}{N} \sum_{i=1}^N z_i \quad (\text{total average})$$

Suppose to be interested in a sample (without replacement) of size n with values x_i ($i \in \{1, \dots, k\}$) out of the set. The average of the sample is defined as:

$$\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i \quad (\text{sample average})$$

Now let $k = N - n$ and $0 \leq \beta \leq 1$. Then:

$$\Pr(\bar{x} \geq \bar{z} + \beta) \leq e^{-\frac{2\beta^2 nN}{k+1}}$$

In brief, this Lemma states that the probability that the sample average is bigger than the total average is exponentially small in the sample size. Therefore, we can make this probability negligible using a large enough sample.

Suppose that Alice and Bob reveal k bits out of the total N bits of their string in the PE phase. The quantity we are interested in is the probability that the error rate Λ_n in the remaining $n = N - k$ bits, is larger than the error rate Λ_k that Alice and Bob observed in the k sampled bits. This probability is conditioned on the event that the error rate of the sampled bits Λ_k is below a certain threshold $\lambda_{\max}$, since otherwise the protocol is simply aborted. Hence, the quantity we are interested in is:

$$\Pr[\Lambda_n \geq \Lambda_k + \gamma \mid \Lambda_k \leq \lambda_{\max}] \quad (1.52)$$

where γ is some small constant. To define the error rates: first, observe that Alice and Bob's respective key strings can be split into a set of k bits ($K_A^{(k)}$ and $K_B^{(k)}$) that is used as the sample and a set of the remaining n bits ($K_A^{(n)}$ and $K_B^{(n)}$). Furthermore, $K_A^{(k)} \oplus K_B^{(k)}$ denotes the binary addition of the two sample bit strings. Note that the resulting string has 0s at those positions where Alice's and Bob's bits coincide and 1s at positions where their respective bits differ. The *Hamming weight* $|K_A^{(k)} \oplus K_B^{(k)}|$ of the string $K_A^{(k)} \oplus K_B^{(k)}$ is the number of 1s in the string, i.e., the number of errors in their sample bit strings. The error rates are then defined as:

$$\Lambda_n = \frac{1}{n} |K_A^{(n)} \oplus K_B^{(n)}|, \quad \Lambda_k = \frac{1}{k} |K_A^{(k)} \oplus K_B^{(k)}| \quad (1.53)$$

Using the notation $\nu = k/N$, the *total error rate* Λ (i.e., the one that includes both the k sample bits and the remaining n bits) can be written as:

$$\Lambda = \nu \Lambda_k + (1 - \nu) \Lambda_n \quad (1.54)$$

Since the k bits are randomly chosen by Alice and communicated to Bob all at once, they are sampled without replacement as the n remaining bits. Hence, we can apply the Serfling's inequality (S.I.) to the n -size sample of remaining bits. We can now start to derive a bound on the quantity of interest: the first step is to conclude from Bayes' theorem² that:

$$\Pr[\Lambda_n \geq \Lambda_k + \gamma \mid \Lambda_k \leq \lambda_{\max}] \leq \frac{\Pr[\Lambda_n \geq \Lambda_k + \gamma]}{\Pr[\Lambda_k \leq \lambda_{\max}]} \quad (1.55)$$

The term in the denominator on the right-hand side is simply the probability that the protocol passes the check; hence, we will use the notation:

$$p_{\text{pass}} = \Pr[\Lambda_k \leq \lambda_{\max}]. \quad (1.56)$$

² $\Pr(A|B) = \frac{\Pr(B|A) \Pr(A)}{\Pr(B)}$

The term in the numerator can be bounded as follows:

$$\begin{aligned} \Pr [\Lambda_n \geq \Lambda_k + \gamma] &= \Pr [\nu \Lambda_n + \Lambda_n \geq \nu(\Lambda_k + \gamma) + \Lambda_n] \\ &= \Pr [\nu \Lambda_k + (1 - \nu) \Lambda_n + \nu \gamma \geq \Lambda_n + \nu \gamma] \\ &= \Pr [\Lambda_n + \nu \gamma] \end{aligned} \quad (1.57)$$

Using Serfling's Inequality (S.I.), the above can be bounded as:

$$\Pr [\Lambda_n + \nu \gamma] \leq e^{-\frac{2k^2 \nu \gamma^2}{(k+1)N}} := \varepsilon^2 \quad (1.58)$$

Hence, we have

$$\Pr [\Lambda_n \geq \Lambda_k + \gamma \mid \Lambda_k \leq \lambda_{\max}] \leq \frac{e^{-\frac{2k^2 \nu \gamma^2}{(k+1)N}}}{p_{\text{pass}}} = \frac{\varepsilon^2}{p_{\text{pass}}} := \varepsilon_{\text{PE}}^2 \quad (1.59)$$

So, there is a small probability (exponentially small in the sample size k) that the remaining error rates are not compatible with the estimated (sampled) parameters, and it is related to the number of bits k that are used to estimate the relevant statistics of the overall data. There is also a small probability ε_{PE} that the raw keys K_A and K_B obtained (i.e., the ones that pass the PE phase) are not compatible with the estimated parameters. Let us consider the probability distribution

$$\mathcal{P} \equiv P_{K_A, K_B, \Lambda_k}(k_A, k_B, \lambda_k) = \Pr [K_A = k_A, K_B = k_B, \Lambda_k = \lambda_k \mid \Lambda_k \leq \lambda_{\max}] \quad (1.60)$$

and another probability distribution defined by

$$Q \equiv Q_{K_A, K_B, \Lambda_k}(k_A, k_B, \lambda_k) = \begin{cases} \frac{P_{K_A, K_B, \Lambda_k}(k_A, k_B, \lambda_k)}{\Pr[\Lambda_n < \Lambda_k + \gamma \mid \Lambda_k \leq \lambda_{\max}]}, & \text{if } \lambda_n < \lambda_k + \gamma, \\ 0, & \text{otherwise.} \end{cases} \quad (1.61)$$

Note that under the distribution Q we know that $\Lambda_n < \Lambda_k + \gamma \leq \lambda_{\max} + \gamma$ with probability 1.

According to eq. 1.59, the probability that Λ_n exceeds Λ_k by more than γ (given that the error check is passed) is bounded by $\varepsilon_{\text{PE}}^2$. One can show that the distribution Q is ε_{PE} -close to the distribution $\mathcal{P}$ in terms of the purified distance of probability distributions³.

Indeed, it can be shown (see [115]) that the fidelity of $\mathcal{P}$ and Q is

$$\begin{aligned} F(\mathcal{P}, Q) &= \left(\sum_{k_A, k_B, \lambda_k} \sqrt{P_{K_A, K_B, \Lambda_k}(k_A, k_B, \lambda_k) Q_{K_A, K_B, \Lambda_k}(k_A, k_B, \lambda_k)} \right)^2 \\ &= \Pr [\Lambda_n < \Lambda_k + \gamma \mid \Lambda_k \leq \lambda_{\max}] \\ &= 1 - \Pr [\Lambda_n \geq \Lambda_k + \gamma \mid \Lambda_k \leq \lambda_{\max}] \stackrel{(1.59)}{\geq} 1 - \varepsilon_{\text{PE}}^2. \end{aligned} \quad (1.62)$$

And so, knowing that

$$P^2 := 1 - F \implies F = 1 - P^2 \geq 1 - \varepsilon_{\text{PE}}^2 \quad (1.63)$$

³The purified distance $P(p_x, q_x)$ between two probability distributions $\{p_x\}$ and $\{q_x\}$ can be defined as $P(p_x, q_x) = \sqrt{1 - F(p_x, q_x)}$ where $F(p_x, q_x) = (\sum_x \sqrt{p_x q_x})^2$ is the fidelity. This definition agrees with the one given for density operators; see, for example, the case $\rho = \sum_x p_x |x\rangle\langle x|$ and $\sigma = \sum_x q_x |x\rangle\langle x|$.

at the end we have

$$P(\mathcal{P}, Q) \leq \varepsilon_{\text{PE}}. \quad (1.64)$$

This result means that there is a small failure probability ε_{PE} that the raw keys K_A and K_B obtained are not compatible with the estimated parameters.

1.5.2 Error-Correction algorithms

To be sure that the protocol is correct, an error-correcting code can be introduced to correct any errors between Alice's and Bob's strings. These errors can be due to Eve, noise in the quantum channel, and/or imperfect devices used in the protocol. The task of classical error correction is to correct errors in a string (for example, the communication from a noisy channel), while classical information reconciliation is to turn two strings with correlations into two strings that are the same by possibly changing both of them. However, it is usually easier to consider information reconciliation in the special case of error correction, where Bob corrects his string to make it the same as Alice's (which is called *direct reconciliation*). Alice and Bob can also do *reverse reconciliation* where Alice corrects her string to be the same as Bob's. In this analysis only direct reconciliation will be treated.

Consider the following scenario in the protocol after Parameter Estimation: Alice has a string K_A and Bob has a string K_B that may be different from K_A , while Eve has a quantum state that may have correlations with K_A and K_B . Alice wants to send some function of her raw key to Bob so that Bob can use this information and K_B to reconstruct K_A . What is known from parameter estimation is an estimate of the error rate. The only thing that Bob does not know is where his errors are in his string. Explicit error-correcting codes define what communication is necessary so that Bob can find out where his errors are and correct them.

Two examples of *explicit error-correcting codes* are *low-density parity-check (LDPC) codes* and *polar codes*. These codes provide an important advantage over other codes because being computationally efficient, they can achieve speeds that can be orders of magnitude faster compared to other codes. Both LDPC codes and Polar codes are linear block codes, which means that the message that Alice needs to send to Bob in order for him to correct his errors is given by the multiplication of Alice's string with a matrix.

Independently from the chosen error correction protocol, Alice and Bob have to make sure that the procedure was successful. Since Alice does not have access to Bob's system and Bob does not have access to Alice's system, neither of them can directly check if error correction was successful. One method they can use is applying a *two-universal hash function* to the error-corrected key string, that we still indicate with the symbols K_A and K_B . Alice can (uniformly at random) choose a two-universal hash function $f_{\text{EC}} \in \mathcal{F}$ from a family of such functions and apply it to her key K_A . Alice then sends the function f_{EC} and the evaluation of the function $f_{\text{EC}}(K_A)$ to Bob, who computes the function on his key $f_{\text{EC}}(K_B)$. If the hash values are equal, then with high probability Alice's and Bob's keys are the same.

Definition: δ -almost Two-Universal Hash Functions

Let $\delta > 0$ and let $f \in \mathcal{F}$ be a function $f : \mathcal{K} \rightarrow \mathcal{Z}$ in a family (i.e., a set) $\mathcal{F}$ with input space the alphabet $\mathcal{K}$ and output space the alphabet $\mathcal{Z}$. Then $\mathcal{F}$ is a δ -almost two-universal family of hash functions if

$$\Pr_{f \in \mathcal{F}} [f(k) = f(k')] \leq \delta \quad \text{for any } k \neq k' \in \mathcal{K}. \quad (1.65)$$

- $\mathcal{F}$ is called a two-universal family of hash functions if $\delta = \frac{1}{|\mathcal{Z}|}$.
- A family of two-universal hash functions always exists from $\mathcal{K} = \{0, 1\}^n$ to $\mathcal{Z} = \{0, 1\}^\ell$ for all integers n and ℓ .

Due to the defining property of families of hash functions given in def. 1.65, it is clear that the QKD protocol is ε_{cor} -correct if two-universal hash functions are used with an output space of dimension $|\mathcal{Z}| = 2^{\lceil \log_2 \frac{1}{\varepsilon_{\text{cor}}} \rceil}$, since⁴

$$\Pr [f_{\text{EC}}(K_A) = f_{\text{EC}}(K_B) \mid K_A \neq K_B] \leq 2^{-\lceil \log_2 \frac{1}{\varepsilon_{\text{cor}}} \rceil} \leq 2^{-\log_2 \frac{2}{\varepsilon_{\text{cor}}}} = \varepsilon_{\text{cor}} \quad (1.66)$$

The last inequality (eq. 1.66), together with Bayes' theorem (see footnote 2), implies that

$$\begin{aligned} & \Pr [K_A \neq K_B \mid f_{\text{EC}}(K_A) = f_{\text{EC}}(K_B)] \Pr [f_{\text{EC}}(K_A) = f_{\text{EC}}(K_B)] \\ &= \Pr [f_{\text{EC}}(K_A) = f_{\text{EC}}(K_B) \mid K_A \neq K_B] \Pr [K_A \neq K_B] \end{aligned} \quad (1.67)$$

Where, note, $\Pr [f_{\text{EC}}(K_A) = f_{\text{EC}}(K_B)] = 1$, $\Pr [f_{\text{EC}}(K_A) = f_{\text{EC}}(K_B) \mid K_A \neq K_B] \leq \varepsilon_{\text{cor}}$ and $\Pr [K_A \neq K_B] \leq 1$. Take into account the fact that the protocol aborts when the hashes differ. Therefore, we obtain

$$\Pr [K_A \neq K_B \mid f_{\text{EC}}(K_A) = f_{\text{EC}}(K_B)] \leq \varepsilon_{\text{cor}}. \quad (1.68)$$

This means that Alice's and Bob's strings are the same after error correction if their hash values agree, except with probability ε_{cor} .

Note that this checking procedure is independent of the error rate that Alice and Bob have observed in the PE step and also independent of the chosen error correction code. If the checking procedure succeeds except with probability ε_{cor} , then the whole protocol is ε_{cor} -correct. Despite these results, it is important to know how much information has been leaked to Eve during the error correction phase. Typically, all of the bits of communication sent from Alice to Bob in the EC phase are considered to be leaked bits of information to Eve. The amount of communication depends on the particular error-correcting code used. We indicate with leak_{EC} the number of bits leaked to Eve, to which we have to add the bits needed for the hash function, that are upper bounded by $\log_2 \frac{2}{\varepsilon_{\text{cor}}}$. Hence, if we indicate with C the classical communication about the key that Eve learns from error correction, we have

$$\log_2 |C| = \text{leak}_{\text{EC}} + \log_2 \frac{2}{\varepsilon_{\text{cor}}} \quad (1.69)$$

1.5.3 Privacy Amplification

Privacy amplification is the process of removing any residual information that Eve may have about the key string after all the other steps in the QKD protocol. This can be achieved by using *randomness extractors*: functions "Ext" that take a source of randomness as input, e.g., a string K of length n , as well as a small uniformly random string S (of length d) called a seed and output an almost uniformly random output string Z (of length ℓ) that is longer than the seed:

$$Z = \text{Ext}(K, S). \quad (1.70)$$

To specify the information that the adversary has on Alice's string (it is crucial that this information is limited), the measure we use is the *quantum conditional min-entropy*. For a

⁴Notice that: $\lceil \log_2 \frac{1}{x} \rceil \leq \log_2 \frac{2}{x}$ for all x .

classical–quantum state as

$$\rho_{KE} = \sum_{k \in \mathcal{K}} p_K(k) |k\rangle\langle k| \otimes \rho_E^k, \quad (1.71)$$

that describes Alice’s key K and Eve’s system E , $H_{\min}(K|E)$ tells us how much uniform randomness $Z = \text{Ext}(K, S)$ we can extract from Alice’s random variable K such that Z is independent of Eve’s system E . We define:

Definition: Quantum-proof Strong Randomness Extractor)

A function $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^\ell$ is a (t, ε) -strong quantum-proof randomness extractor if, for all classical-quantum states ρ_{KE} with a classical $K \in \{0, 1\}^n$ with min-entropy $H_{\min}(K|E) \geq t$ and a uniform seed $S \in \{0, 1\}^d$, we have

$$D\left(\rho_{\text{Ext}(K,S)SE}, \frac{\mathbb{1}}{2^\ell} \otimes \rho_S \otimes \rho_E\right) \leq \varepsilon. \quad (1.72)$$

The state $\frac{\mathbb{1}}{2^\ell} \otimes \rho_S \otimes \rho_E$ represents the ideal situation: The key, represented by the maximally mixed state $\frac{\mathbb{1}}{2^\ell}$, is uniformly random, i.e., each 2^ℓ possible ℓ -bit sequence has the same probability. Furthermore, it is independent of the seed S and the state of Eve’s system E , exactly as we required. From the definition of ε -secrecy, we have that the obtained key is ε -secret.

There are two main randomness extractors used for privacy amplification in QKD: the *quantum leftover hash lemma* and the *Trevisan’s extractor*. Informally, the quantum leftover hash lemma shows how much randomness can be extracted from a classical source that has at least a certain amount of conditional smooth min-entropy with a quantum adversary. For QKD this means that we can prove a lower bound on the smooth min-entropy of Alice’s string given Eve’s quantum system.

Lemma: Quantum Leftover Hash Lemma

Let $K \in \mathcal{K}$ be a random variable, E be a quantum system, and let $\mathcal{F}$ be a two-universal family of hash functions from $\mathcal{K} \in \{0, 1\}^n$ to $\mathcal{Z} \in \{0, 1\}^\ell$. Then, for every $\varepsilon > 0$, it holds that

$$D(\rho_{f_{\text{PA}}(K)FE}, \frac{\mathbb{1}}{2^\ell} \otimes \rho_{FE}) \leq \varepsilon + \frac{1}{2} \sqrt{2^{\ell - H_{\min}^\varepsilon(K|E')}} \quad (1.73)$$

where $\rho_{f_{\text{PA}}(K)FE}$ is the state after applying a random two-universal hash function $f_{\text{PA}} \in \mathcal{F}$ to the key K and E' summarizes all information Eve learned about K during the protocol, including the classical communication sent by Alice and Bob over the authenticated channel before privacy amplification.

In contrast to def. 1.72, the quantum leftover hash lemma uses the *smooth conditioned min-entropy* $H_{\min}^\varepsilon(K|E')$ rather than the min-entropy because it gives a tight bound on the maximum amount of uniform randomness that can be extracted from K while being independent of E' . This gives rise to an additional smoothing parameter ε that accounts for the secrecy level.

Notice that if the length ℓ of the final key Z is chosen such that $\ell = H_{\min}^{\varepsilon}(K|E') - 2 \log_2 \frac{1}{\varepsilon_{\text{PA}}}$, with ε_{PA} another smoothing parameter, we have that

$$\frac{1}{2} \sqrt{2^{\ell - H_{\min}^{\varepsilon}(K|E')}} = \frac{1}{2} \sqrt{2^{2 \log_2(2\varepsilon_{\text{PA}})}} = \frac{1}{2} \sqrt{(2\varepsilon_{\text{PA}})^2} = \varepsilon_{\text{PA}} \quad (1.74)$$

and so from the quantum leftover hash lemma (def. 1.73) we have that the protocol is ε_{sec} -secret with $\varepsilon_{\text{sec}} = \varepsilon + \varepsilon_{\text{PA}}$.

It is worth noticing that, instead of bounding from above the trace distance in order to guarantee ε_{sec} -secrecy, we can equivalently try to find a lower bound for the smooth min-entropy $H_{\min}^{\varepsilon}(K|E')$ of Alice's state conditioned on Eve's state.

As stated in Lemma 1.73, E' in $H_{\min}^{\varepsilon}(K|E')$ summarizes all information Eve learned about K during the protocol, including the classical communication sent by Alice and Bob over the authenticated channel in the previous steps of the post-processing. According to the discussion done for the EC step, a maximum of $\text{leak}_{\text{EC}} + \log_2 \frac{2}{\varepsilon_{\text{cor}}}$ bits of information about K are revealed to Eve during the error correction phase.

Hence, by using a chain rule for the smooth min-entropies, we can relate the smooth min-entropy before classical post-processing $H_{\min}^{\varepsilon}(K|E)$ with the min-entropy $H_{\min}^{\varepsilon}(K|E')$ before privacy amplification via

$$H_{\min}^{\varepsilon}(K|E') \geq H_{\min}^{\varepsilon}(K|E) - \text{leak}_{\text{EC}} - \log_2 \frac{2}{\varepsilon_{\text{cor}}} \quad (1.75)$$

Note that by lower-bounding the smooth min-entropy $H_{\min}^{\varepsilon}(K|E)$ Alice and Bob almost fulfill the conditions needed to apply a randomness extractor to K in order to generate the final secret key Z (i.e., the privacy amplification step). Indeed, from def. 1.72 it follows that the randomness extractor is ε -secret if $H_{\min}(K|E) \geq t$, where the min-entropy $H_{\min}(K|E) := H_{\min}^{\varepsilon'}(K|E)$ with $\varepsilon' = 0$. However, a straightforward application of the triangle inequality for the distance between states implies that a corresponding criterion also holds if $\varepsilon' > 0$: indeed if $H_{\min}^{\varepsilon'}(K|E) \geq t$, the use of a (t, ε) -strong quantum-proof extractor will provide a key that is $(\varepsilon + 2\varepsilon')$ -secret.

For having security (i.e., secrecy and correctness) we need that the keys that are put through the hash function f_{PA} in privacy amplification are also correct. If the keys K_A and K_B after error correction are the same (which happens with probability at least $1 - \varepsilon_{\text{cor}}$, then their hashes are guaranteed to be the same, which implies that the protocol is ε_{cor} -secure even after privacy amplification:

$$\Pr[f_{\text{PA}}(K_A) \neq f_{\text{PA}}(K_B)] \leq \Pr[K_A \neq K_B] \leq \varepsilon_{\text{cor}}. \quad (1.76)$$

To conclude, If a bound on the smooth min-entropy can be obtained for the protocol under investigation, then the protocol is $(\varepsilon_{\text{cor}} + \varepsilon_{\text{sec}})$ -secure.

1.6 Attacks in QKD

If assumptions are fulfilled, QKD offers unconditional security. However, practical implementations may deviate from the theoretical models, opening loopholes on the security. In this section, it will be analyzed how these pitfalls have been used to compromise the security of QKD systems and what are the ways to counterattack and prevent such problems. Being it an openly researched field in continuous evolution, only the most known and important attacks will be covered.

Attacks can be reduced to mainly three categories: *individual*, *collective* and *coherent*. These attacks allow to build a model for the attacker and bound the amount of information that it can extract, and hence, the Secret Key Rate. However, these attacks are assuming a perfect implementation of the QKD system and are mainly considered because most of the time the theoretical analysis in the general case is too hard to accomplish. Instead, real-world attacks often rely on the broken assumptions due to the practical implementation. Such assumptions can be:

1. The source emits single-photon states (relaxed with decoy);
2. The states prepared are the ones actually sent;
3. The measurement operators performed are the ones expected;
4. All the state and basis choices are done at random, with no correlations between rounds;
5. Efficiency of the detectors are equal;
6. Detectors only click due to a photon event;
7. Splitting ratio of the devices are constant during the experiment;
8. The decoy levels emitted are the one expected from the protocol;
9. These decoy levels don't fluctuate;
10. There is no leaking of information about state preparation or measurement from the transmitter or receiver: time-difference, spectral difference between different states, or electromagnetic side-channel.

When one or more of these assumptions is broken, a security loophole opens. There are four main families of attacks, targeting different part of the QKD system: *Source*, *Encoder*, *Decoder*, *Detector*. Some examples from each category are reported in Table 1.3.

Target	Attacks	Exploited Imperfections
Source	Source attack [69] Laser injection [43] Distinguishable decoy states [39] Side channels in free-space Alice [85] Intersymbol effect [118] Wavelength-selected [54] Laser injection [54] Laser damage [53]	Nonrandom phase Nonrandom phase under laser injection Pump-current intensity modulation Multiple laser diodes Intensity correlation between neighboring pulses Intensity-related change in wavelength Increased intensity under laser injection Reduced attenuation under high-power illumination
Encoder	Source flaw [31] Phase remapping [43] Trojan-horse [44]	Inaccurate state modulation Incorrect encoding among transition edges of modulation Reflection photon from injected laser
Decoder	Trojan-horse [44] Phase remapping [43] Wavelength-dependent [66] Time shift [42] Efficiency mismatch [42] Dead time [96] After gate [79] Superlinearity attack [79] Detector blinding [86]	Reflection photon from injected laser Incorrect decoding among transition edges of modulation Wavelength-dependent coupling ratio of BS Mismatched detection efficiencies Mismatched detection efficiencies Individual deadtime of each detector Linear mode of SPD Superlinear response of SPD among transition edges Mismatched detection efficiencies and linear mode of SPD
Detector	Backflash attack [109] Timing side channel [20]	Backward-transmitted photons Detector-related detection timing tag

TABLE 1.3: Targets, attacks, and exploited imperfections in QKD systems.

One of the solutions is to develop better QKD protocols that avoid making assumptions on the devices themselves. Some example are Measurement-Device-Independent [72] (where the measurement station is untrusted) and Device-Independent QKD [93] (where both sources and measurements are untrusted).

1.6.1 Trojan-Horse Attack

A very effective attack that it's going to be covered in this section is the so-called *trojan-horse attack* (THA) [44, 62], where Eve injects bright pulses of light back into Alice's transmitter (or receiver). With the right timing, the bright pulses enter in the phase or intensity modulator during Alice's modulation and part of the pulse is scattered back, due to the connectors or other internal reflections (An example of the trace is reported in fig. 1.10). Eve can measure the reflected pulses and infer the modulation performed by Alice. A simple but effective solution is to use attenuators, isolators, circulators or *wavelength-division-multiplexers* (WDM), to prevent the injection of bright pulses in the system. However, the attacker can further increase the injection power up to the damage point. A growing body of research has focused on both theoretical models of THAs and practical countermeasures, including the use of optical isolators, monitoring detectors, and new security proofs that account for side-channel leakage [75, 102, 44]. Despite these efforts, fully characterizing and mitigating THAs remains an open and crucial challenge in the secure deployment of QKD networks [52].

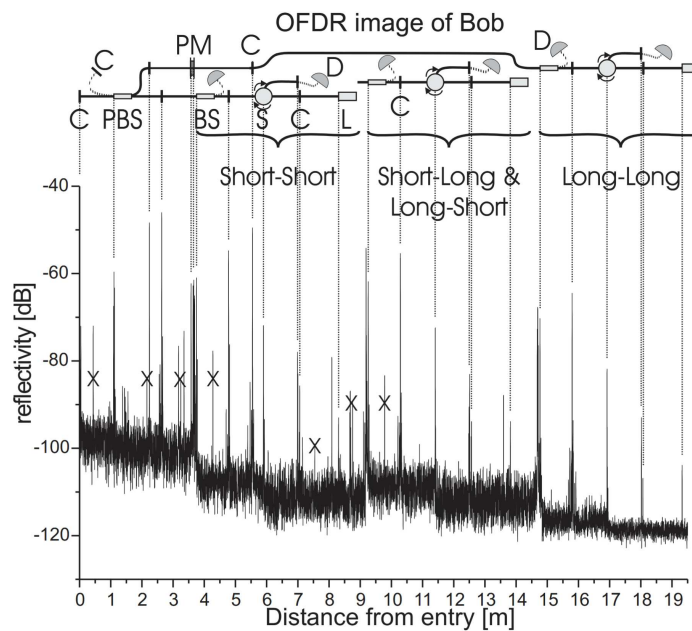


FIGURE 1.10: Example of an OFDR trace of Bob's Plug-&-Play QKD system. Each peak appears 3 times, because the incoming and reflected light both split in two, following the short and long path of the interferometer. For instance, one can notice that the long arm of the interferometer is about 11.5 meters longer than the short arm. [44]

1.7 Other QKD protocols

BB84 isn't the only protocol for QKD: Another incorporates entanglement inside BB84, the E91 protocol [36] (similarly BBM92 [25]): it exploits entangled photons that can be created by the sender (Alice), the receiver (Bob) or someone separate from both, including Eve. The photons are distributed such that the two communicating parties end up with only one

photon from each of the entangled pairs. The idea takes advantage on two fundamental characteristics of entanglement: on one hand, entangled states are theoretically perfectly correlated. If Alice and Bob both measure their particles in the $+$ basis, they obtain the same state with 100% probability. The same is valid for any other complementary and orthogonal polarization (requiring that they have directionality synchronization). On the other hand, any eavesdropping attempt destroys these correlations in a way that can be detected [5]. Just to name a few DI-QKD [93] and MDI-QKD [72], which don't need assumptions over the devices in general, Twin-field QKD [29], which allows to operate beyond the repeater-less bound limit, SARG04 [105], B92 [24], continuous-variable protocols [65] and many others. All of my projects exploited variants of the BB84 protocol with decoy states, so I won't dive deep in the explanations of the other protocols.

Chapter 2

Devices and components in Optics

2.1 Polarization Maintaining Fibers

Polarization-maintaining (PM) fibers are a specialized class of optical fibers designed to preserve the state of polarization (SOP) of light as it propagates through the fiber. Unlike standard single-mode fibers, PM fibers introduce birefringence into their core structure (Fig. 2.1), creating two orthogonal polarization modes with distinct propagation constants. The birefringence is typically achieved by asymmetrically shaping the core or embedding stress rods within the cladding.

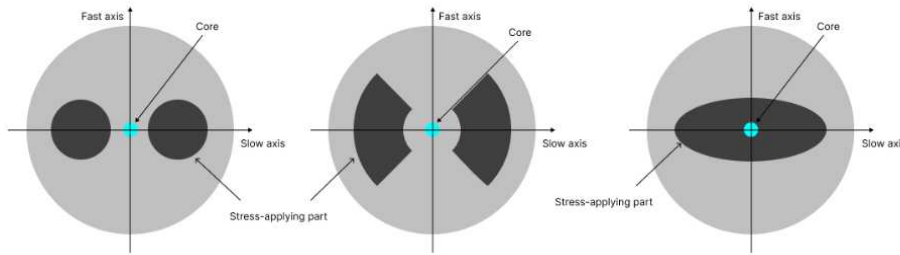


FIGURE 2.1: Core examples of polarization maintaining fibers. [abalone-tech.com, 07/2025]

The birefringence $B = n_{\text{slow}} - n_{\text{fast}}$ in a PM fiber is defined as the difference in effective refractive indices between the fast and slow axes. This birefringence introduces a phase difference $\Delta\phi$ between the two polarization modes over a fiber length L , given by:

$$\Delta\phi = \frac{2\pi BL}{\lambda} \quad (2.1)$$

where λ is the operating wavelength of the light. For PM fibers, the birefringence is engineered to be large enough to prevent coupling between the two polarization modes, ensuring that the light maintains its original SOP.

PM fibers are widely used in applications requiring stable polarization, such as interferometry, fiber optic gyroscopes, and quantum communication systems. They are also critical for coupling light into polarization-sensitive devices, such as electro-optic modulators and polarization beam splitters. The extinction ratio (ER), defined as the ratio of transmitted power in the desired polarization to the undesired polarization, is a key performance metric for polarization evaluation, typically expressed in decibels (dB):

$$(\text{ER})_{\text{dB}} = 10 \log_{10} \left(\frac{P_{\text{desired}}}{P_{\text{undesired}}} \right)$$

This ability to maintain polarization makes PM fibers indispensable for applications requiring high polarization precision and stability in optical systems.

2.2 Phase Modulators

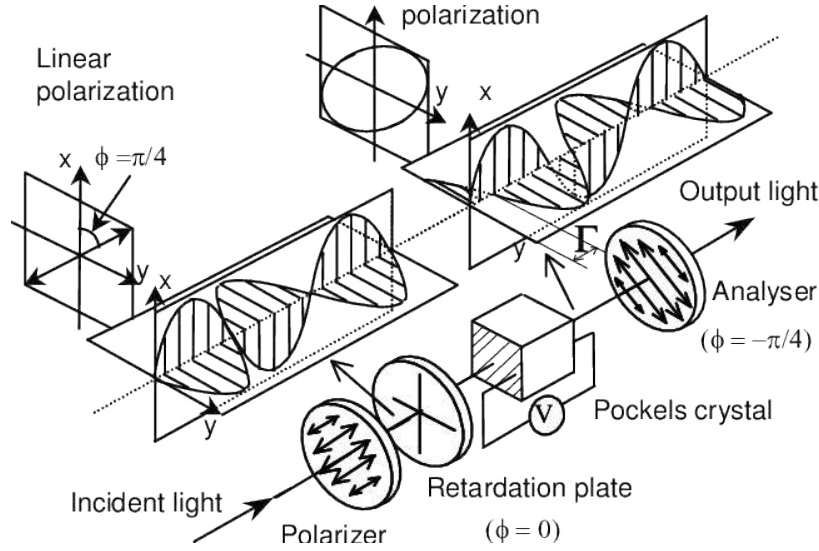


FIGURE 2.2: Working principle of an electro-optic phase modulator.
[researchgate.net, 07/2025]

Phase modulators (Fig. 2.2) are optical devices designed to control the phase of a light wave by introducing a controlled phase shift. This phase shift is typically achieved by exploiting the electro-optic effect, where an applied electric field alters the refractive index of the material through which the light propagates, in the following way:

$$n(E) \simeq n_0 + n_1|E| + n_2|E|^2 \quad (2.2)$$

where n_1 is the Pockel's coefficient and n_2 is the Kerr's coefficient. By varying the voltage across the modulator, the phase of the transmitted light can be precisely adjusted, namely:

$$\Delta\phi(V) = -\pi \frac{V}{V_\pi} \quad (2.3)$$

where V_π is the voltage required to introduce a π -shift in the phase, described as:

$$V_\pi = \frac{d\lambda_0}{Lrn_2} \quad (2.4)$$

where d is the high of the modulation region, L is the length of the modulation region, λ_0 is the wavelength of the material in vacuum and r is a coefficient that depends on the alignment between the direction of propagation of the light and the anisotropic material. Phase modulators are essential components in various optical systems, including interferometers, quantum communication setups, and laser stabilization systems. They

enable fine-tuning of the phase to achieve constructive or destructive interference, which is critical for applications such as signal modulation, beam steering, and frequency control.

These devices are often constructed using materials with strong electro-optic properties, such as lithium niobate (LiNbO_3) or potassium titanyl phosphate (KTP), and are typically configured as waveguides. The ability to modulate the phase at high speeds makes them particularly useful in applications requiring dynamic control of light, such as phase-encoded quantum key distribution or optical coherent communication systems.

2.3 Beam splitters

A beam splitter (Fig. 2.3) is an optical device used to divide an incoming light beam into two separate components: one that is transmitted and another that is reflected. This device is a fundamental component in a wide range of optical experiments and measurement systems, including interferometry, and it plays a critical role in fiber-optic telecommunications. The most common design of a beam splitter is a cubic structure made from two triangular glass prisms that are bonded together at their bases using adhesives such as polyester, epoxy, or urethane. For a 50:50 beam splitter, the adhesive layer is carefully adjusted to ensure that, at a specific wavelength, exactly half of the incident light entering one face of the cube is reflected, while the other half is transmitted. This balance between reflection and transmission is largely attributed to the phenomenon of frustrated total internal reflection.

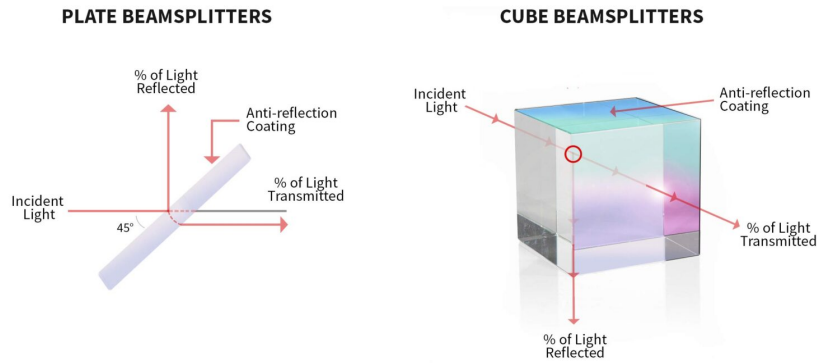


FIGURE 2.3: Free-space beam splitter schematics. [midopt.com, 07/2025]

The beam splitter can be mathematically modeled as a system that transmits a portion T , reflects a portion R , and absorbs a portion A of the incident optical power, satisfying the relation:

$$R + A + T = 1$$

In the special case where the beam splitter is lossless ($A = 0$), it can be described as performing a unitary transformation on the input state $|\psi\rangle$ in a two-dimensional Hilbert space. The output state $|\psi'\rangle$ is then given by:

$$|\psi'\rangle = e^{i\theta_0} \begin{bmatrix} \sqrt{T}e^{i\theta_T} & \sqrt{R}e^{-i\theta_R} \\ \sqrt{R}e^{i\theta_R} & \sqrt{T}e^{i\theta_T} \end{bmatrix} |\psi\rangle \quad (2.5)$$

Beam splitters in fiber optics, often known as fused-fiber couplers, are mounted on single-mode, polarization-maintaining fibers for specialized applications.

2.4 Polarizing Beam Splitters

Polarizing beam splitters (Fig. 2.4) are optical components that separate an incoming light beam into two distinct beams, each characterized by different linear polarization states. In an ideal polarizing beam splitter, the two resulting beams are completely polarized and exhibit orthogonal polarization orientations. However, in practical beam-splitting polarizers, only one of the output beams achieves full polarization, while the other beam is typically a combination of multiple polarization states. Its working principle can be described by the following transfer matrix:

$$U_{\text{PBS}} = \begin{bmatrix} t_H & 0 & 0 & r_V \\ 0 & t_V & r_H & 0 \\ 0 & r_V & t_H & 0 \\ r_H & 0 & 0 & t_V \end{bmatrix}$$

where t_H and t_V are the transmission coefficients for horizontally ($|H\rangle$) and vertically ($|V\rangle$) polarized light, respectively. r_H and r_V are the reflection coefficients for horizontally and vertically polarized light, respectively. For an ideal PBS, $t_H = 1$, $r_H = 0$ (horizontal polarization is fully transmitted), $t_V = 0$, $r_V = 1$ (vertical polarization is fully reflected).

Thus, the matrix simplifies to:

$$U_{\text{PBS}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

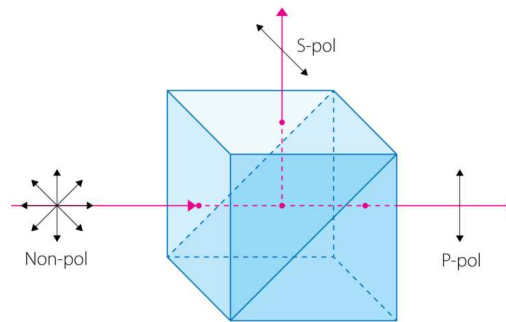


FIGURE 2.4: Free-space polarizing beam splitter schematics. [altechna.com, 07/2025]

Unlike absorptive polarizers, which dissipate the energy associated with the rejected polarization state, beam-splitting polarizers manage this process without absorbing energy. This makes them particularly suitable for handling high-intensity light beams, such as those generated by lasers. Additionally, polarizing beam splitters are advantageous in scenarios

where both polarization components must be simultaneously analyzed or utilized. These devices are often constructed from two prisms made of anisotropic (uniaxial) materials, bonded together, usually with different orientations.

Fiber-based polarizing beam splitters, also referred to as fiber-based polarization beam combiners and splitters, are designed for use with single-mode and polarization-maintaining optical fibers.

2.5 Encoders for QKD

2.5.1 Roberts' intensity modulator

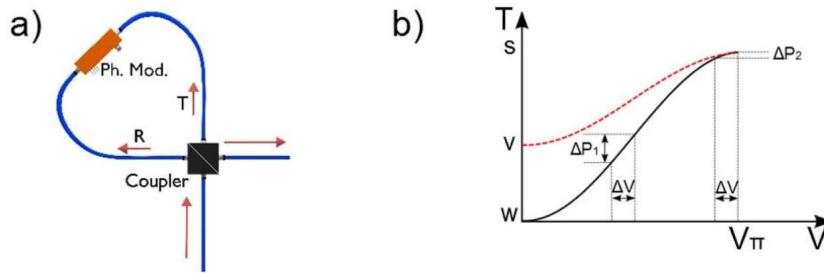


FIGURE 2.5: Intensity modulation. (a) Schematic of the Sagnac-based IM with a coupling ratio $R : T$. (b) Transmission (T) with voltage (V) for an interferometer-based IM. Power deviations for identical voltage shifts (ΔV) for signal states ("s") (ΔP_2) and decoy-states ("v") (ΔP_1) are given. The red dotted line shows the output of the proposed low extinction ratio interferometer. [98]

Roberts' intensity modulator, first proposed in [98], is specifically designed to attenuate optical pulses for the purpose of implementing a one-decoy state protocol. Its primary objective is to establish two distinct intensity levels by selectively applying or omitting modulation. This system (reported simplified in Fig. 2.5) begins with a fast-axis blocking beam splitter, which simultaneously functions as a circulator and interference element. Following the beam splitter, the setup incorporates a polarization-maintaining fiber Sagnac loop paired with a delay line to temporally separate the clockwise (CW) and counter-clockwise (CCW) pulses. In this scheme, one of the pulses is modulated at V_π and subsequently interferes with the other pulse at the beam splitter. The effectiveness of this approach is attributed to the fact that the second intensity level is determined by the beam splitter ratio while maintaining the modulation voltage fixed at V_π . This ensures that the modulation occurs at the peak of the transfer function, where the derivative is zero, thereby minimizing small fluctuations in the electrical voltage that may arise from the input electrical chain. These fluctuations are often caused by the system's parasitic memory, which modifies the shape of the peaks depending on the sequence of symbols used. This phenomenon is known as the patterning effect.

To model the system using principles of quantum mechanics, a mathematical approach can be employed to calculate the intensity modulation. In this representation, the presence of light at the two input and output ports is described by the states $|in\rangle = (1, 0)$ and $|out\rangle = (0, 1)$, respectively. The intensity modulation can be expressed as a function of these states:

$$I(T, \phi) = \langle \text{out} | B(T) J P(\phi) B(T) | \text{in} \rangle = |e^{i\phi}(T - 1) + T|^2 \quad (2.6)$$

where the beam-splitter matrix is given by:

$$B(T) = \begin{bmatrix} \sqrt{T} & i\sqrt{1-T} \\ i\sqrt{1-T} & \sqrt{T} \end{bmatrix} \quad (2.7)$$

the modulation matrix is defined as:

$$P(\phi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix} \quad (2.8)$$

and the matrix describing the inversion of the two paths is:

$$J = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (2.9)$$

2.5.2 iPOGNAC polarization encoder

The iPOGNAC modulator, first introduced in [9], is a device designed to control the polarization state of light. Polarization modulation plays a key role in optics and photonics, as the polarization state conveys critical information and can be utilized in a diverse range of applications. In QKD especially, it can be used for stable, self-compensating polarization encoding: in fact, phase modulators suffer greatly from thermo-optic effects, shifting the V_π in a wide range of values. The Sagnac-loop configuration, though, is able to strongly counteract the dependence on temperature, strongly reducing the number of components needed for the encoder to work.

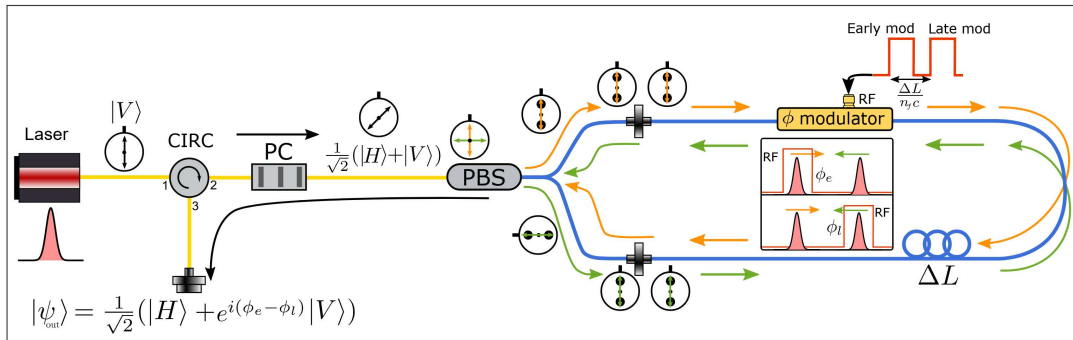


FIGURE 2.6: Scheme of the iPOGNAC polarization encoder. [9]

The iPOGNAC setup (Fig. 2.6) starts with a circulator (CIRC), used to separate the input and output light beams, and a polarization controller (PC), responsible for transforming incoming linearly polarized light into a diagonal polarization state, expressed as $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$. Following this stage, the light is routed to an asymmetric Sagnac interferometer equipped with a polarizing beam-splitter (PBS) and a high-speed phase

modulator (ϕ modulator). In this part of the system, the polarization beam splitter replaces the traditional Sagnac beam splitter, enabling the division of the incoming light into two pulses. The polarization beam splitter is integrated with polarization-maintaining optical fiber outputs, ensuring effective stabilization of the polarization state.

The iPOGNAC has recently evolved substituting the circulator and the polarization controller with a single free-space 50/50 beam-splitter. This configuration takes advantage of the polarization stability offered by free-space optics while benefiting from the flexibility and mature technology associated with fiber-optic components. This change requires all the fibers employed to be polarization maintaining (except the one used for the output), and the one at the input of the beam-splitter to be also fast-axis-blocking and rotated by 45° to ensure the generation of the $|D\rangle$ state.

The central functionality of the iPOGNAC lies in the asymmetry of its interferometer, achieved through a delay line. By temporally separating the clockwise (CW) and counter-clockwise (CCW) pulses, the system enables independent modulation of the two pulses. This allows precise control of the polarization state exiting the device by appropriately adjusting the voltage and timing of the electrical pulses applied to the phase modulator:

$$M(\phi_{\text{CW}}, \phi_{\text{CCW}}) = \begin{bmatrix} e^{i\phi_{\text{CW}}} & 0 \\ 0 & e^{i\phi_{\text{CCW}}} \end{bmatrix} \quad (2.10)$$

Here, ϕ_{CW} and ϕ_{CCW} represent the phases introduced by the modulator to the CW and CCW propagating light pulses, respectively. When a voltage pulse induces a $\pi/2$ phase shift in either the CW or CCW light pulses, the iPOGNAC system produces two orthogonal states, $|L\rangle$ and $|R\rangle$. In contrast, when no phase modulation is applied, the polarization state remains in the diagonal state, $|D\rangle$. These three states are pivotal in QKD protocols, as they facilitate the creation of quantum states required for the one-decoy three-state BB84 protocol.

After modulation, the light pulses travel back through the polarization-maintaining fiber and are redirected to free space. It is important to note that the outputs of the polarization beam splitter are aligned with the slow axis, which induces a rotation in the polarization state:

$$J = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (2.11)$$

This step is essential for the self-compensation of any unintended phase δ caused by the birefringence in the polarization-maintaining optical fiber preceding the loop. The phase compensation is described by:

$$P(\delta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix} \quad (2.12)$$

Compensation ensures spatial and mode filtering precision. Finally, as the pulse reflects through the beam splitter, the horizontal polarization components acquire a phase shift of π , represented by:

$$R = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \quad (2.13)$$

The light is then directed toward the free-space output port. The output state of the system can be expressed as:

$$|\text{out}(\delta, \phi_{\text{CW}}, \phi_{\text{CCW}})\rangle = RP(\delta)JM(\phi_{\text{CW}}, \phi_{\text{CCW}})P(\delta)|D\rangle \quad (2.14)$$

which simplifies to:

$$|\text{out}(\delta, \phi_{\text{CW}}, \phi_{\text{CCW}})\rangle = \frac{1}{\sqrt{2}} \left(e^{i(\phi_{\text{CW}} + \delta)} |H\rangle + e^{i(\phi_{\text{CCW}} + \delta)} |V\rangle \right) \quad (2.15)$$

By ignoring the global phase, this can further be rewritten as:

$$|\text{out}\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle + e^{i(\phi_{\text{CW}} - \phi_{\text{CCW}})} |V\rangle \right) \quad (2.16)$$

2.5.3 iPOGNAC as an Intensity Modulator

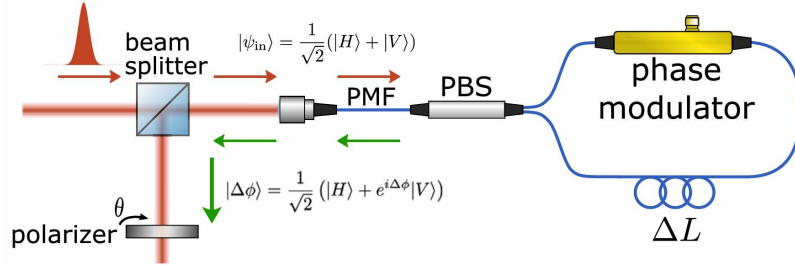


FIGURE 2.7: Scheme of an intensity modulator composed of an iPOGNAC polarization modulator followed by a polarizer rotated at an angle θ . [27]

The iPOGNAC scheme can be utilized also for intensity modulation purposes by performing a projective measurement at the output of the setup, for example by means of a polarizer (Fig. 2.7). The polarizer rotated at an angle θ results in a projection onto the state $|\theta\rangle = \cos(\theta)|H\rangle + \sin(\theta)|V\rangle$ which can be rewritten as $|\theta\rangle = \cos(\theta - \frac{\pi}{4})|D\rangle + \sin(\theta - \frac{\pi}{4})|A\rangle$ to simplify calculations. When the $|D\rangle$ SOP encounters the polarizer, its transmission probability is given by $|\langle\theta|D\rangle|^2 = \cos^2(\theta - \frac{\pi}{4})$, whereas the transmission probability for the $|A\rangle$ state is given by $|\langle\theta|A\rangle|^2 = \sin^2(\theta - \frac{\pi}{4})$. From this, we obtain the intensity ratio value between these two possible states as:

$$\text{IR}(\theta) = \frac{|\langle\theta|A\rangle|^2}{|\langle\theta|D\rangle|^2} = \tan^2(\theta - \frac{\pi}{4}). \quad (2.17)$$

It is clear that the intensity ratio between the two states can be easily tuned to any value by changing the polarizer angle θ (see Figure 2.8), with physical device imperfections

representing the only limit. This feature makes the iPOGNAC-based intensity modulator more flexible than other self-compensating intensity modulators such as the one introduced by Roberts *et al.* [98], which has an intensity ratio that is fixed at construction by the transmissivity and reflectivity of the beam splitter used in their Sagnac interferometer. Tuning this ratio can be crucial to obtain the best performance of the QKD system since a change to the operational scenario could lead to a different optimal setting for the decoy states [27].

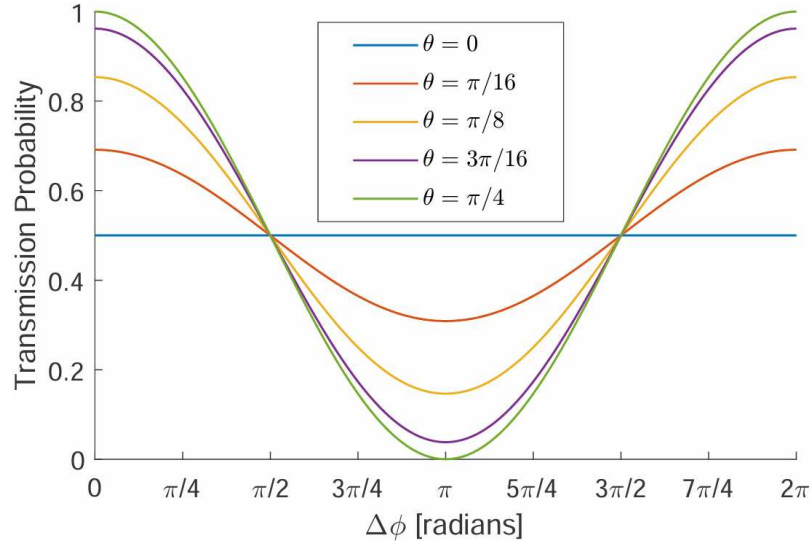


FIGURE 2.8: Theoretical intensity ratio response of the system as a function of the iPOGNAC polarization phase modulation $\Delta\phi$ for different polarizer rotation angles θ . [27]

Chapter 3

Software for real-time analysis of QKD systems

I have contributed to the project by participating in these work packages: design, development, testing.

3.1 Objective

The primary objective of this project was to develop an integrated and interactive tool capable of providing immediate, real-time feedback on QKD systems performances. The goal was to transform the characterization process from a slow, iterative cycle into a dynamic, closed-loop optimization task. To achieve this, the software was designed with the following specific objectives in mind:

- *Real-time Data Visualization:* To provide an immediate, intuitive understanding of the quantum signal by continuously plotting histograms of photon arrival times from multiple detector channels.
- *Live Performance Metrics Calculation:* To automatically compute and display critical QKD performance indicators, most notably the QBER for different bases and the total detection rates, updating them live as new data streams in.
- *Interactive Experimental Control:* To offer a flexible *Graphical User Interface* (GUI) for interactively tuning parameters, such as the position and width of detection gates, synchronization settings, and individual channel delays, allowing for optimization on-the-spot.
- *Hardware Abstraction and Integration:* To create a unified software "roof" for the various laboratory instruments, starting with the Time-to-Digital Converters (TDCs), providing a consistent interface regardless of the underlying hardware.
- *Robust Algorithmic Framework:* To build a platform capable of integrating, testing, and validating complex real-time processing algorithms, such as the *Qubit4Synch* clock-recovery mechanism, in a live experimental environment.
- *Concurrent Data Logging:* To reliably save raw, unprocessed timetag data to disk in parallel with the real-time analysis, ensuring that no data is lost and that comprehensive post-processing and archival is always possible.

The choice of Python 3 with the PyQt6 library (pypi.org/PyQt6) was a deliberate design decision to balance rapid and easy development (both from myself and from my peers) with the performance demands of real-time analysis. Python's scientific computing ecosystem was essential to adapt the laboratory demands, while PyQt6's robust support for

multi-threading was critical for ensuring that the computationally intensive data processing would not render the GUI unresponsive. Ultimately, the objective was not merely to acquire data, but to create a comprehensive command center for lab experimentation that would accelerate research and enable the fine-tuning required to achieve the high-performance results presented in the following chapters.

3.2 The software

The software was primarily designed to collect data from a *Time-to-Digital Converter* (TDC) with N channels, which determines the arrival time, with sub-ns resolution, of the electrical signals coming from the different channels. The software is compatible with several TDC devices; in our laboratory, we mainly use the quTAU and quTAG (Figure 3.1) devices from qutools GmbH.



FIGURE 3.1: quTAG by qutools GmbH. [qutools.com, 08/2025]

Each electrical signal represents the detection of a photon. The data collected by the TDC is represented by a list of detections, containing the channel information and the precise arrival time (time-tag) of the signals. The software then processes the data to display the histogram of detections. A screenshot of the software output during a typical data acquisition is shown in Fig. 3.2.

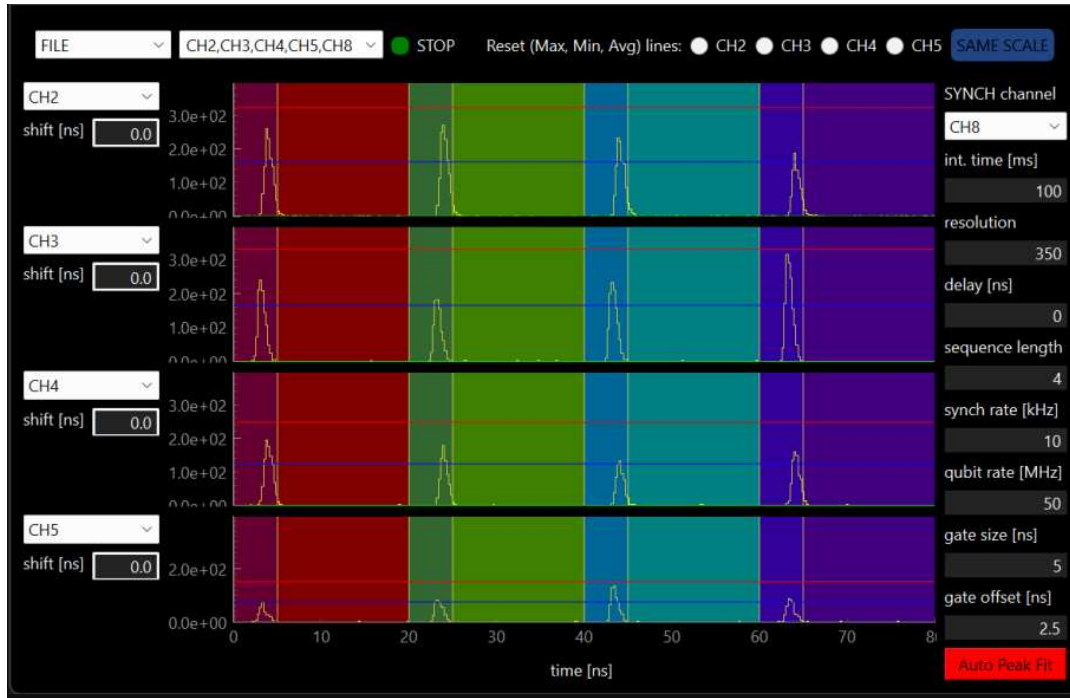


FIGURE 3.2: Screenshot of the software during the testing of a QKD setup running in real-time.

Clicking on "START" begins the acquisition, and it is possible to display the data belonging to the channels selected by the user. It is also possible to set one of the channels as a synchronization channel (especially in the case of the quTAU timetagger by qutools, which has no internal synchronization). Several parameters can be set, such as integration time, sequence length, synchronization rate, and qubit rate (the repetition rate of the source). After these initial settings, it is possible to display the detection histogram in real time (where typical peaks from laser pulses can be observed). It is also possible to manually adjust the individual shifts for each channel to better visualize the QKD sequence pattern. The gate parameters (*gate size* and *gate offset* in Fig. 3.2) can be set to discard detections due to background or detector noise. In this way, only detections occurring within the selected "gate" are considered, while the others are discarded. By comparing the selected detections in the different channels, it is possible to evaluate the QBER, which is related to the security of the final key.

The software also calculates the sum of all detections in a given time interval, corresponding to the total detection rate (four slots, shown in red, green, cyan and purple, are displayed in Fig. 3.3). The detection rate over time and the QBER are displayed at the bottom of Fig. 3.3.

On the right side of Fig. 3.3, a logging feature is also visible. While viewing the synchronized timetags, it is possible to simultaneously save the original timetags in real time, with the option of adding additional "saving functions" and thus store more elements to disk (such as the QBER at a specific time instant). This feature is useful for post-processing and data analysis, as the data can be saved in .bin, .txt, and .csv formats, with the option to add other formats if necessary. Likewise, other "widgets" have been implemented to control other parts of the setup from the same central workstation, such as electrical amplifiers (Fig. 3.4).

This framework has been useful to me, as well as to many of my peers, for evaluating performance during the testing phase of QKD setups.



FIGURE 3.3: Detail of the software showing the QBER and total detections. Logging widget on the right.

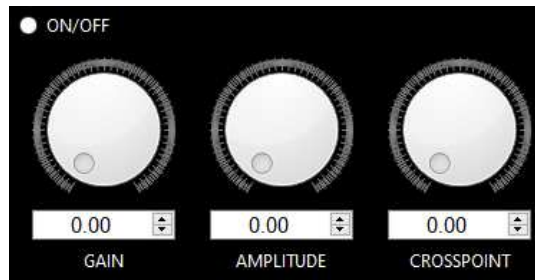


FIGURE 3.4: Widget to control an electrical amplifier.

3.2.1 Clock-recovery algorithm

On this environment, I also worked on programming a clock-recovery algorithm to reconstruct Alice's frequency on Bob's side. I reproduced the "*Qubit4Synch*" algorithm, originally conceived in [28], making it simpler, more intuitive, and more robust by adding an additional noise filtering step not included in the original algorithm. In Figure 3.5, it is possible to assess the performance improvements of the new algorithm compared to the old one. The computation times in the graph that are higher than the integration time (i.e.: higher than 100%) can be associated to the first stage of the algorithm, that has to compute a *Discrete Fourier Transform* (DFT), the slowest part of the code. This part is necessary to perform a coarse estimation of the period at Alice's side, which then will be fine-tuned by the second step of the algorithm, the linear regression stage. In this case, we can model the

arrival of the timetags as a train of Dirac-delta functions $\delta(t)$:

$$s(t) = \sum_{i=1}^N \delta(t - t_i) \quad (3.1)$$

which gives a Fourier transform that can be rewritten as a discrete sum, exploiting the Fourier transform of the Dirac delta $\int e^{j\omega t} \delta(t - t_i) dt = e^{-j\omega t_i}$:

$$s(\omega) = \int e^{j\omega t} s(t) dt = \sum_{i=1}^N \int e^{j\omega t} \delta(t - t_i) dt = \sum_{i=1}^N \int e^{j\omega t} \delta(t - t_i) dt = \sum_{i=1}^N e^{-j\omega t_i} \quad (3.2)$$

Where j is the imaginary number and $\omega = 2\pi f = 2\pi/T$, f frequency and T period of the signal. By calculating the power spectral density (PSD) and taking the *argmax* of it, one can find a broad estimation of the transmitting frequency. The rest follows as a simple linear regression to follow the compression of the period in time.

The novelty in the algorithm consists into performing a filtering on the data using a 2D-histogram on the timetags. As seen in Figure 3.6, after performing a modulo-period operation - when the estimated period is close to matching the real one - the signal appears in the space as a dense cloud of points (timetags). The density of the cloud can therefore give an estimate of where the signal is located before even doing the linear regression. The 2D-histogram divides the space in square blocks (bins), so by choosing an adequate number of bins and filtering out the timetags related to bins with less counts than the maximum divided by a pre-defined *Signal-to-Noise Ratio* (SNR), one can improve the linear regression stage both computationally (since there are less points to include in the calculation) and accurately (since the line is not mediated over points that contribute to the noise). After this, an initial linear regression is performed on these data to filter out timetags at a distance higher than the signal jitter from this line, to then perform an ulterior, more precise linear regression on these data. By iteratively subtracting this line to the timetags, one can stabilize the period at Bob's side, successfully reconstructing Alice's period oscillation in time.

A code snippet can be found below, while in Figure 3.6 the effect of the algorithm on the un-synchronized data can be visualized, before and after the correction at Bob's side.



FIGURE 3.5: Comparison between the old and new algorithm in terms of computation time performance, calculated on a fixed experimental set of data.

```

1 def _qubit4synch(self):
2     if self._current_state == 1:
3         self._state_1() # only call state_1 when needed
4         self._state_2()
5
6 def _state_1(self):
7     """
8     DFT on reduced data for computational performances
9     """
10    self._shift0_ps = 0
11    tauA_ps = 1 / (self._params['bitrate_mhz'] * 1e6) * 1e12 # nominal period at Alice
12    ↪ side in ps
13
14    self._tauB_ps = tauA_ps*(1+3.1e-6) # mean estimation from several data
15
16    Nselection = 400 # select first Nselection timetags
17    self.__tSelection = self._ttags_buffer[:Nselection]
18    L = round((np.max(self.__tSelection) - np.min(self.__tSelection)) / (tauA_ps / 4)) #
19    ↪ length of timestamps with T/4 resolution
20    df = 4 / (tauA_ps * L) # frequency resolution
21    x = 1 / self._tauB_ps + np.arange(-100, 101, 0.5) * df # frequency span
22    y = np.abs(np.sum(np.exp(1j * 2 * np.pi * x[np.newaxis, :] * self.__tSelection[:,
23    ↪ np.newaxis]), axis=0)) ** 2 # DFT evaluation
24    self._tauB_ps = 1 / x[np.argmax(y)] # coarse estimation of period
25
26    X = self.__tSelection
27    tmod = (X + (self._tauB_ps / 2)) % self._tauB_ps - (self._tauB_ps / 2) # bin
28    Y = tmod
29
30    # Calculate the linear regression line
31    p0 = np.polyfit(X, Y, 1)
32    Yfit = np.polyval(p0, X)
33
34    # Find the linear regression line for points within a 'self._params['jitter_ps']'
35    ↪ distance from Yfit
36    indices = np.abs(Y - Yfit) < self._params['jitter_ps']
37    p = np.polyfit(X[indices], Y[indices], 1)
38
39    if np.std(Y) > 2 * self._params['jitter_ps'] and np.std(Y - Yfit) > 2 *
40    ↪ self._params['jitter_ps']:
41        self._params['jitter_ps']:
42        self._shift0_ps = tauA_ps / 2 # ps
43        tmod = (X + self._shift0_ps + (self._tauB_ps / 2)) % self._tauB_ps -
44        ↪ (self._tauB_ps / 2)
45        Y = tmod

```

```

39     p0 = np.polyfit(X, Y, 1)
40     Yfit = np.polyval(p0, X)
41     indices = np.abs(Y - Yfit) < 2*self._params['jitter_ps']
42     p = np.polyfit(X[indices], Y[indices], 1)
43     self._shift0_ps = self._shift0_ps - p[1]
44     else:
45         self._shift0_ps = -p[1]
46
47     self._tauB_ps *= 1+p[0] # better period estimation
48     self.__p0 = np.array([0,0])
49
50     self._current_state = 2
51
52 def _state_2(self):
53     '''
54     2d-histogram filtering and linear regression
55     '''
56     tauA_ps = 1 / (self._params['bitrate_mhz']*1e6)*1e12 # nominal period at Alice side
57     ↪ in ps
58
59     X = self._ttags_buffer - np.polyval(self.__p0, self._ttags_buffer)
60     Y = ((X + self._tauB_ps / 2) % self._tauB_ps) - (self._tauB_ps / 2)
61
62     # Filtering through 2D-histogram
63     hist = histogram2d(Y,X, bins=10, range=[min(X), max(X)], [-self._tauB_ps/2,
64     ↪ self._tauB_ps/2][::-1]) # 2d array
65
66     if np.max(hist)/max([np.min(hist), 0.1]) < 1.2:
67         print('Signal not found. Skipping filterings.')
68         self.ttags_Alice = np.array(X / self._tauB_ps * tauA_ps)
69     else:
70         edges_x = np.linspace(min(X), max(X), len(hist[0])+1)
71         edges_y = np.linspace(-self._tauB_ps/2, self._tauB_ps/2, len(hist)+1)
72         threshold = (np.max(hist) + np.min(hist)) / 2
73         mask = np.zeros_like(X, dtype=bool)
74         for i in range(len(edges_x)-1):
75             for j in range(len(edges_y)-1):
76                 if hist[j, i] > threshold:
77                     mask_x = (X >= edges_x[i]) & (X < edges_x[i+1])
78                     mask_y = (Y >= edges_y[j]) & (Y < edges_y[j+1])
79                     mask = mask | (mask_x & mask_y)
80
81     X1 = X[mask]
82     Y1 = Y[mask]
83
84     if np.std(Y1) > 2*self._params['jitter_ps']:
85         self.ttags_Alice = np.array(X / self._tauB_ps * tauA_ps)
86
87     self._current_state = 1
88     print('returning to state 1 because frequency was lost')
89
90     return
91
92     p = np.polyfit(X1, Y1, 1)
93
94     dY = Y-np.polyval(p, X)
95     X1=X[np.abs(dY)<self._params['jitter_ps']]
96     Y1=Y[np.abs(dY)<self._params['jitter_ps']]
97     p = np.polyfit(X1, Y1, 1)
98
99     self.__p0 = self.__p0 + p
100
101     p2=np.polyfit(X1*1e-12, Y1, 2)
102     dY = Y-np.polyval(p2, X*1e-12)
103     X2=X[np.abs(dY)<2*self._params['jitter_ps']]
104     Y2=Y[np.abs(dY)<2*self._params['jitter_ps']]
105     p2 = np.polyfit(X2*1e-12, Y2, 2)
106
107     self.ttags_Alice = np.array((X - np.polyval(p2, X*1e-12)) / self._tauB_ps * tauA_ps)

```

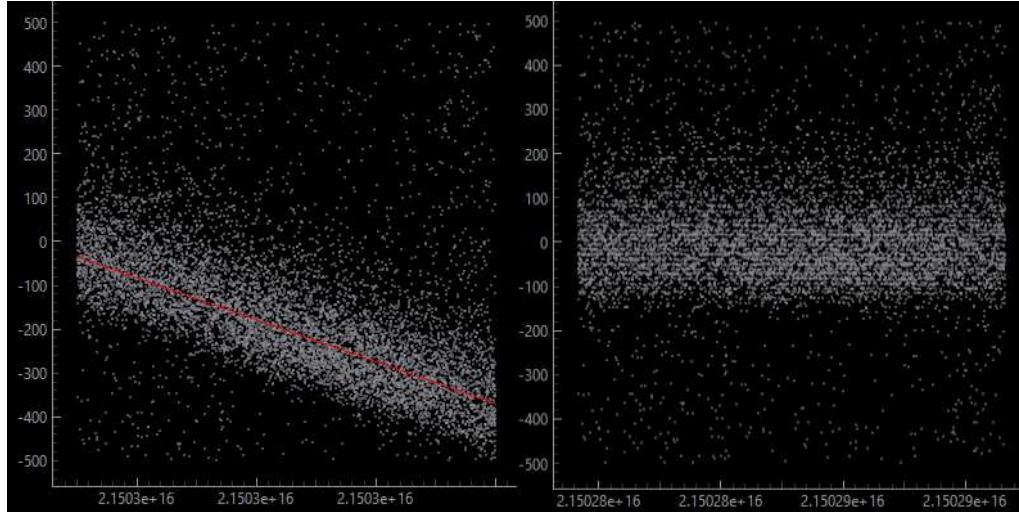


FIGURE 3.6: Before (left) and after (right) the frequency adjusting performed by the clock-recovery algorithm. The y-axis represents the time modulo-period in ps of each timetag (in this example the period being 1 ns) while the x-axis represents the time in ps of each timetag. The red line represents the fitted linear-regression line on the un-synchronized data.

3.3 Considerations

The development of the real-time analysis software described in this chapter represents a critical enabling technology for the experimental work presented in this thesis. While the primary goal was to create a functional tool for data acquisition, its impact and the strategic considerations behind its design merit a more detailed discussion. The most significant contribution of this software was the fundamental shift it enabled in our experimental workflow. Prior to its development, the characterization of QKD systems was a disjointed, multi-stage process: data was first acquired blindly, then processed offline, and only then were the results analyzed. This introduced significant latency between adjusting a physical parameter, such as the bias of a modulator or the alignment of a polarization controller, and observing its effect on key performance metrics like the Quantum Bit Error Rate (QBER). A custom-built software, built ad-hoc with, for example, real-time "histogramming", gating, and QBER calculation, transformed this into an interactive, closed-loop process. This agility proved invaluable during the optimization of the high-speed iPOGNAC modulator (chapter 4 on page 51) and the field-testing phases of the QUANGO project (chapter 5 on page 65). The ability to receive immediate visual feedback allowed for rapid fine-tuning and troubleshooting, drastically reducing the time required to achieve optimal system performance and stability. The choice of Python with the PyQt6 framework was a strategic decision balancing development speed against raw performance. While a lower-level language like C++ could offer higher data throughput, Python's rich scientific ecosystem (including libraries like NumPy and SciPy) was indispensable for the rapid implementation and testing of complex algorithms, most notably the *Qubit4Synch* clock-recovery mechanism. PyQt6 provided the necessary robustness for a responsive Graphical User Interface (GUI) through its mature multi-threading capabilities, ensuring that intensive data processing did not freeze the user interface, a common pitfall in simpler frameworks. This choice represents a trade-off: the system is not designed to be a commercial high-frequency data logger, but rather an advanced laboratory tool where the speed of analysis and algorithmic flexibility are a priority. Looking forward, while the software proved highly effective for its intended purpose, several avenues for future development exist. Its current

architecture is centered around a single, locally connected Time-to-Digital Converter (TDC). A natural extension would be to evolve it into a distributed, network-aware application capable of aggregating and synchronizing data from multiple nodes in a network like VenQCI (chapter 6 on page 75). This would provide a centralized, real-time dashboard for monitoring the health and performance of an entire quantum network. Furthermore, the manual parameter-tuning (e.g., gate positioning, channel delays) could be enhanced through automation. Future versions could incorporate machine learning algorithms to automatically optimize gate parameters or even provide feedback to active optical components, creating a self-optimizing QKD system. Finally, integrating control over a wider range of laboratory instruments (e.g., optical attenuators, laser controllers) would solidify the software's role as a unified command center for complex quantum communication experiments.

Chapter 4

General model and modulation strategies for Sagnac-based encoders

I have contributed to the project by participating in these work packages: design, functional validation, data analysis. Pre-print available at: [26]

4.1 Introduction

A major drawback of both inline and Mach-Zehnder modulators is the bias drift resulting from temperature and environmental fluctuations, thus necessitating active stabilization of the temperature and bias voltage to maintain a stable operating point. Moreover, inline polarization modulators require high operating voltages, coupled with the fact that the birefringence of the waveguide induces polarization mode dispersion (PMD), which reduces the degree of polarization for short pulses.

Sagnac loop-based modulators have recently been proposed as an effective alternative to conventional in-line and Mach-Zehnder modulators. The common path geometry inherently compensates for reciprocal phase shifts, reducing sensitivity to environmental perturbations such as temperature fluctuations and mechanical vibrations. The Sagnac interferometer configuration is exploited to achieve both intensity [98] and polarization modulation [19, 10] while avoiding the need for bias voltage control.

The Sagnac modulator consists of an optical loop (often realized by fiber optics), typically formed using a beam splitter (for intensity modulation) or a polarizing beam splitter (for polarization modulation) with the light entering the input port split into two counter-propagating beams that travel the loop in opposite directions (see Fig. 4.1). By placing an EOM asymmetrically within the loop, the co-propagating and counter-propagating beams arrive at the modulator at different times, allowing them to be modulated independently, thus controlling the relative phase between them.

However, this asymmetry also imposes a limit on the maximal repetition rate of optical pulse transmission. To prevent the counter-propagating component of the pulse N from overlapping with the co-propagating component of pulse $N + 1$, it is necessary that the transmission frequency be lower than a value that depends on the propagation time of the pulse in the modulator and the asymmetry (i.e., its position in the Sagnac loop). Overcoming this limitation by completely removing the asymmetry implies modulating both co-propagating and counter-propagating components at the same time, which presents a significant experimental challenge.

In this work, we introduce a complete model of the Sagnac modulator and propose some useful modulation techniques that can be used for both intensity and polarization

modulation. Moreover, we present a study on the symmetric Sagnac configuration and how its challenges can be tackled with carefully chosen modulation schemes.

4.2 Principles of Sagnac modulators

A traveling-wave electro-optic phase modulator is designed with an optical waveguide in an electro-optic material and an adjacent electrode structure forming a coplanar waveguide for a microwave signal. This configuration allows the optical and electrical pulses to interact continuously along the length where the two waveguides are adjacent. To maximize this interaction, it is crucial to match not only their physical alignment but also their effective refractive indices (or phase velocities). Proper velocity matching ensures that the two waves remain synchronized, enabling effective modulation throughout the device length, as long as both the optical and electrical waves propagate in the same direction, i.e., co-propagating. This structure is particularly advantageous for high-speed applications, as it supports high repetition rates and multiple optical pulses can propagate while interacting primarily with their corresponding electrical pulse. However, traveling-wave modulators can also operate when the optical pulses propagate in the opposite direction to the electrical signal. In this counter-propagating configuration, the interaction between the two waves changes, resulting in a different modulation effect compared to the co-propagating configuration. The reason for this effect must be traced back to the relative motion between the optical and electrical pulses, which alters the effective interaction time and modulation efficiency. This kind of modulator operates by imposing a phase $\phi_s(t)$ on the optical wave in response to an electrical signal $s(t)$, such that

$$\phi_s(t) = \int e^{i\omega t} H(\omega) S(\omega) d\omega, \quad (4.1)$$

where $H(\omega)$ is the transfer function of the modulator and

$$S(\omega) = \frac{1}{2\pi} \int e^{-i\omega t} s(t) dt \quad (4.2)$$

is the Fourier transform for the electrical signal $s(t)$.

Assuming that the velocities of the electrical and the optical waves are equal inside the phase modulator, the transfer function takes a simple but distinct form between the co-propagating (co) and counter-propagating (ct) cases, such that

$$H_{\text{co}}(\omega) = \frac{\pi}{V_\pi}, \quad H_{\text{ct}}(\omega) = \frac{\pi}{V_\pi} \text{sinc}(\tau_{\text{mod}}\omega), \quad (4.3)$$

where $\text{sinc}(x) = \frac{\sin x}{x}$, τ_{mod} is the propagation time of the electrical (or optical) signal inside the modulator, and V_π is the voltage of the electrical signal corresponding to a phase shift of π [12]. Typical values (which can vary depending on the specific commercial device used) are $V_\pi \approx 5V$ and $\tau_{\text{mod}} \approx 320$ ps. The previous relations are obtained for a simplified modulator model (neglecting electrical absorption and bandwidth saturation effects). In particular, we neglected the dependence of V_π on ω (for high frequencies, the value of V_π typically increases).

In the co-propagating configuration, the optical and electrical signals remain synchronized along the modulator, leading to a relatively uniform phase modulation. In contrast, in the counter-propagating case, the imposed phase depends on the angular frequency ω of the electrical signal, effectively acting as a low-pass filter. Because the two waves travel in opposite directions, their overlap occurs only for a very short period of time with respect to

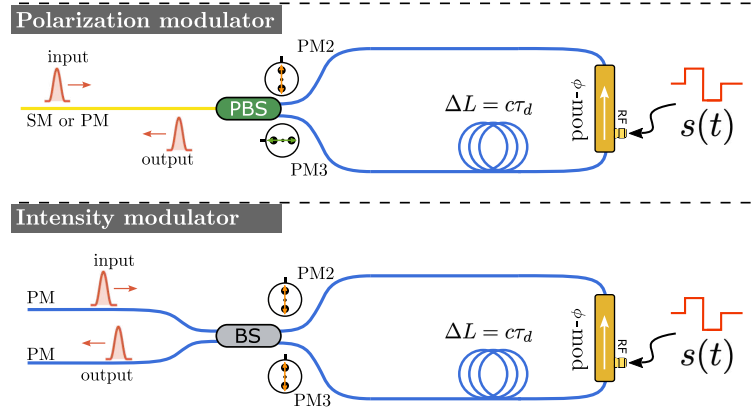


FIGURE 4.1: Polarization and intensity modulator based on the Sagnac scheme. ϕ -mod indicates the electro-optic phase modulator, while the white arrow indicates the direction of the RF microwave signal. ΔL quantifies the asymmetry of the phase modulator within the Sagnac loop. For symmetric configuration $\Delta L = 0$.

the co-propagating overlap time, during which the optical pulse accumulates the entire interaction with the electrical field. This short interaction window makes the counter-propagating scheme more sensitive to the physical length of the waveguide and can lead to less efficient modulation capabilities, implying a higher modulation voltage requirement to impose the same phase with respect to the co-propagating case.

Combining the two transfer functions mentioned above, the model can be applied to describe the transfer function of schemes that use a modulator within a Sagnac loop, as illustrated in Fig. 4.1. When implementing a Sagnac modulator, be it for intensity or polarization modulation, the resulting transfer function can be expressed by combining the two terms of Eq. (4.3) as

$$H_{\text{Sagnac}}(\omega) = \frac{\pi}{V_\pi} e^{i\omega t_0} [1 - e^{-i\omega \tau_d} \text{sinc}(\tau_{\text{mod}} \omega)], \quad (4.4)$$

where $\tau_d = \Delta L/c$ is the time corresponding to the delay line ΔL and t_0 is the overall delay between the electrical and optical signal. Note that if the delay line ΔL is placed before or after the modulator, the sign of τ_d can be inverted.

Through the transfer function $H_{\text{Sagnac}}(\omega)$, using (4.1) it is possible to calculate the phase as a function of time, $\phi_s(t)$, that will be applied to an optical signal when an electrical signal with a given temporal trend $s(t)$ is applied to the modulator. Alternatively, $\phi_s(t)$ can be evaluated by calculating the inverse Fourier transform of the transfer function (for simplicity, we neglect the overall delay t_0)

$$\begin{aligned} h_{\text{Sagnac}}(t) &= \int e^{i\omega t} H_{\text{Sagnac}}(\omega) d\omega \\ &= \frac{2\pi^2}{V_\pi} \left[\delta_D(t) - \frac{1}{2\tau_{\text{mod}}} \Pi\left(\frac{t - \tau_d}{2\tau_{\text{mod}}}\right) \right], \end{aligned} \quad (4.5)$$

where $\delta_D(t)$ is the Dirac-delta and $\Pi(t)$ is the rectangular function

$$\Pi(t) = \begin{cases} 1, & |t| \leq 1/2 \\ 0, & |t| > 1/2. \end{cases} \quad (4.6)$$

The phase $\phi_s(t)$ is therefore obtained from the convolution

$$\begin{aligned}\phi_s(t) &= \frac{1}{2\pi} \int s(t') h_{\text{Sagnac}}(t - t') dt' \\ &= \phi_{co}(t) - \phi_{ct}(t),\end{aligned}\quad (4.7)$$

where

$$\begin{aligned}\phi_{co}(t) &= \frac{\pi}{V_\pi} s(t), \\ \phi_{ct}(t) &= \frac{\pi}{V_\pi} \frac{1}{2\tau_{\text{mod}}} \int_{t-\tau_{\text{mod}}}^{t+\tau_{\text{mod}}} s(t' - \tau_d) dt'\end{aligned}\quad (4.8)$$

represent, respectively, the phase applied to the co-propagating and counter-propagating components, where the latter behaves effectively as the moving average of the electrical signal around τ_d . The two expressions (4.1) and (4.7) are equivalent and can be used to calculate $\phi_s(t)$ starting from the shape of the electrical signal $s(t)$.

The asymmetry between co-propagating and counter-propagating optical signals can be effectively illustrated in the behavior of the modulator when a rectangular wave signal (the typical signal used in the modulators described previously) of duration τ_s is given as the input. For a rectangular signal with maximum voltage V_0

$$s(t) = V_0 \Pi\left(\frac{t - \tau_s/2}{\tau_s}\right), \quad (4.9)$$

the expression for $\phi_{ct}(t)$ in (4.7) can be simplified to a trapezoidal equation

$$\phi_{ct}(t) = \pi \frac{V_0}{V_\pi} \cdot \begin{cases} 0 & t' \leq -\tau_{\text{mod}} \\ \min\left(\frac{t' + \tau_{\text{mod}}}{2\tau_{\text{mod}}}, \frac{\tau_s}{2\tau_{\text{mod}}}\right) & -\tau_{\text{mod}} \leq t' \leq \tau_{\text{mod}} \\ \min\left(1, \frac{\tau_{\text{mod}} + \tau_s - t'}{2\tau_{\text{mod}}}\right) & \tau_{\text{mod}} \leq t' \leq \tau_{\text{mod}} + \tau_s \\ 0 & t' \geq \tau_{\text{mod}} + \tau_s \end{cases} \quad (4.10)$$

with $t' = t - \tau_d$.

To provide a clearer understanding of the output phase $\phi_s(t)$ in response to a rectangular driving signal $s(t)$, Fig. 4.2 shows a representative example corresponding to cases $\tau_d - \tau_{\text{mod}} \geq \tau_s$ and $\tau_s \geq 2\tau_{\text{mod}}$. It can be noted that the phase applied to the co-propagating signal exactly follows the shape of the rectangular wave input signal. For the counter-propagating signal, the phase is modified by the transfer function, resulting in a trapezoidal shape.

If $\tau_s > 2\tau_{\text{mod}}$, the phase ϕ_{ct} increases linearly from the instant $t = t^* \equiv \tau_d - \tau_{\text{mod}}$, reaching its maximum value $\pi V_0/V_\pi$ at time $t = t^* + 2\tau_{\text{mod}}$. From this instant on, the phase remains constant up to the point $t = t^* + \tau_s$ from which it decreases linearly to 0 at time $t = t^* + \tau_s + 2\tau_{\text{mod}}$.

If instead the duration of the electrical signal τ_s satisfies $\tau_s \leq 2\tau_{\text{mod}}$, the phase ϕ_{ct} increases to $\pi \frac{V_0}{V_\pi} \frac{\tau_s}{2\tau_{\text{mod}}}$ at time $t = t^* + \tau_s$, remains constant until $t = t^* + 2\tau_{\text{mod}}$ when it decreases to 0 at $t = t^* + \tau_s + 2\tau_{\text{mod}}$. In general, the maximum phase applied to the counter-propagating optical signal can be written as

$$\phi_{ct}^{\text{max}} = \frac{V_0}{V_\pi} \pi \cdot \min\left(1, \frac{\tau_s}{2\tau_{\text{mod}}}\right). \quad (4.11)$$

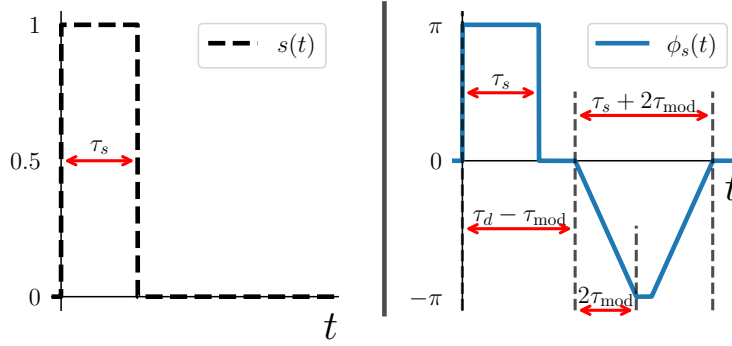


FIGURE 4.2: Phase $\phi_s(t)$ for rectangular driving signal $s(t)$. We considered the case $\tau_d \geq \tau_s + \tau_{\text{mod}}$ and $\tau_s \geq 2\tau_{\text{mod}}$. The signal $s(t)$ is reported in units of V_0 , while $\phi_s(t)$ is given in unit of $\frac{V_0}{V_\pi}$. For simplicity we set $t_0 = 0$.

It is important to emphasize that to achieve the maximum phase modulation under the condition of $\tau_s \geq 2\tau_{\text{mod}}$, the counter-propagating electrical pulse must transfer enough energy to the optical signal along the entire length of the modulator, similar to what occurs in the co-propagating configuration. To fulfill this condition, the optical signal must enter the waveguide when the electrical signal is already present; the latter must have propagated through the entire modulator length, which requires a time τ_{mod} . Moreover, the electrical signal must persist for an additional duration of τ_{mod} , corresponding to the transit time of the optical wave through the modulator. Consequently, the minimum total duration over which the electrical signal must be active is $2\tau_{\text{mod}}$. This can also be considered the minimum condition that allows to inscribe the co-propagation rectangular signal into a counter-propagation trapezoid with the same height. When injecting an optical pulse of width τ_{op} in the Sagnac modulator, to impose a constant phase over the entire pulse, it must hold that $\tau_{\text{op}} \leq \tau_s - 2\tau_{\text{mod}}$. It is worth noting that this particular example of a rectangular electrical signal is an idealization and does not fully represent a real, imperfect, implementation. However, the model as presented is able to take some of these imperfections into account. For example, any electrical waveform generator is limited in bandwidth, which can be easily taken into account by modifying the signal $s(t)$ according to said limitation. This same condition can apply, for example, to bandwidth limits on electrical amplifiers. Another common limitation, caused by imperfect matching of the indices of refraction of both the electrical and optical waveguide of the EOM, is the bandwidth limit within the EOM itself. Taking this effect into account implies modifying the transfer function presented in Eq. (4.4) appropriately.

4.2.1 Symmetric configuration

An interesting case arises when the Sagnac interferometer is operated in a symmetric configuration (i.e., $\tau_d = 0$). In this regime, the asymmetry between co-propagating and counter-propagating interactions discussed in the previous section can be exploited to impose different phase shifts on the two optical components. While both directions are modulated by the same electrical signal, their responses do not cancel out as the counter-propagating component is traveling against the electrical pulse, thus experiencing a different effective modulation voltage compared to the one of the co-propagating component.

In the symmetric configuration, the co- and counter-propagating signals are allowed to interfere. Because of the modulator's asymmetry, the amplitude of the counter-propagating component also depends on the duration of the electrical pulse. Therefore, it is important

that the electrical pulse satisfies $\tau_s < 2\tau_{\text{mod}}$ to prevent the two effects from canceling out within the modulation region. Furthermore, since in this scheme the electrical pulse can be made much shorter, it is advantageous to optimize the throughput by choosing $\tau_s \approx \tau_{\text{op}}$ when performing an optical pulse modulation.

If a standard rectangular electrical pulse, such as the one defined in Eq. (4.9), is used under the condition $\tau_s < 2\tau_{\text{mod}}$, the co- and counter-propagating contributions interfere destructively. In this case, since $\phi_{co}^{\text{max}} = \pi \frac{V_0}{V_\pi}$ and $\phi_{ct}^{\text{max}} = \phi_{co}^{\text{max}} \frac{\tau_s}{2\tau_{\text{mod}}}$ (see eq. (4.11)) the imbalance between the two effects can be pre-compensated by increasing the modulation voltage V_0 by a gain factor of

$$g_V = \left(1 - \frac{\phi_{ct}^{\text{max}}}{\phi_{co}^{\text{max}}}\right)^{-1} = \left(1 - \frac{\tau_s}{2\tau_{\text{mod}}}\right)^{-1}. \quad (4.12)$$

Assuming a sensitive value for commercially available EOMs of $\tau_{\text{mod}} = 320$ ps and the minimum achievable τ_s using a 6 GSa/s digital-to-analog converter ($\tau_s = 166.6$ ps), this corresponds to a gain factor of $g_V \approx 1.35$. This increase in amplification may require cascades of amplifiers that also introduce distortion, decreasing the signal-to-noise ratio.

In this work, we propose a new option for the electrical signal $s(t)$ that overcomes the need for an increase in voltage and fully exploits the integration-like behavior of the counter-propagating component. Thus, this new modulation scheme, defined as *balanced modulation*, uses electrical signals defined as

$$s(t) = V_0 \left[\Pi\left(\frac{t - \tau_s/2}{\tau_s}\right) - \Pi\left(\frac{t - 3\tau_s/2}{\tau_s}\right) \right]. \quad (4.13)$$

This method requires the use of three voltage levels, implying an extra requirement of a digital-to-analog converter or equivalent circuit capable of generating all levels (e.g., two separate voltage signals, an RF voltage inverter coupled with an RF power combiner).

This approach can be used to improve state of the art schemes based on asymmetric Sagnac loops such as, for example, the intensity modulator proposed in [98], the time-bin encoders proposed in [104] and [122], or the polarization encoder proposed in [19].

Moreover, the proposed modulation scheme is applicable to any architecture that exploits a double pass (in opposite directions) of light in the modulator, such as the scheme proposed in [76].

4.3 Sagnac polarization modulators

Any Sagnac polarization modulator [10, 19, 125, 67] is based on a Sagnac interferometer with an EOM inside the loop, where the standard beamsplitter is replaced by a polarizing beam splitter (PBS) to separate the co- and counter-propagating components according to the input polarization state (Fig. 4.1a). For a given electrical signal $s(t)$, an optical pulse is prepared in a diagonal polarization state $|D\rangle = (|H\rangle + |V\rangle) / \sqrt{2}$ (or any balanced superposition of $|H\rangle$ and $|V\rangle$). When this pulse is injected into a Sagnac modulator, the resulting output state is described by

$$|\psi_{\text{out}}(t)\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i\phi_s(t)}|V\rangle), \quad (4.14)$$

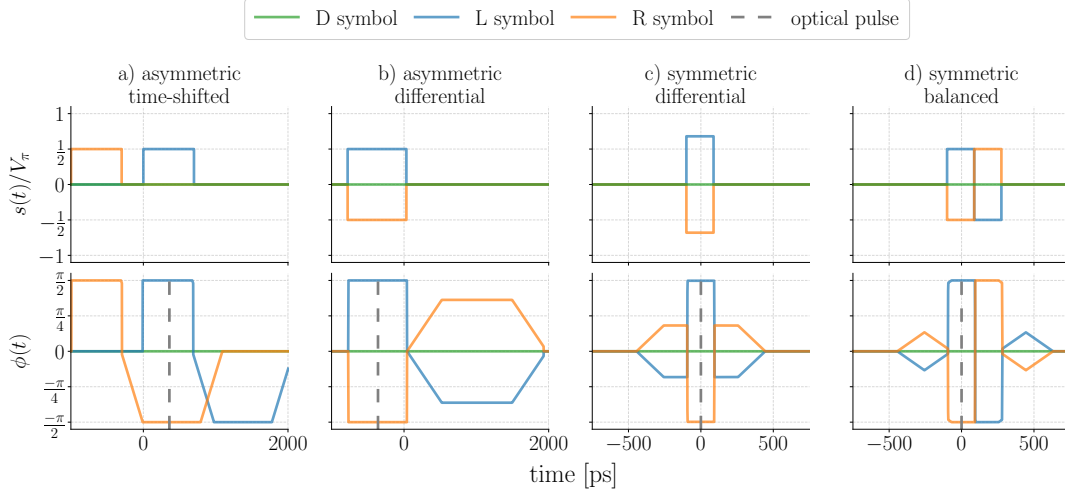


FIGURE 4.3: Modulations proposed in this work, characterized by signal $s(t)$ (top) and phase response $\phi(t)$ of the configuration (bottom). From left to right: a) time-shifted modulations for the asymmetric configuration (for $\tau_s \geq 2\tau_{\text{mod}} + \tau_{\text{op}}$); b) differential asymmetric modulations (for $\tau_s \geq \tau_{\text{op}}$); c) differential symmetric modulation (for $\tau_s \geq \tau_{\text{op}}$); d) balanced symmetric modulations (for $\tau_s \geq \tau_{\text{op}}$). For the asymmetric configuration we choose $\tau_d = \tau_s + \tau_{\text{mod}}$, while for the symmetric configuration we have $\tau_d = 0$. It should be noted that the voltage required to apply a $\pi/2$ phase on the optical pulse for the symmetric differential configuration is higher than all others by a gain factor of g_V defined in Eq. (4.12).

which corresponds to any state belonging to the $X - Y$ equatorial plane of the Bloch sphere. This section is written focusing on a specific iPOGNAC implementation [19] tailored for QKD applications where only three polarization states are required to realize the three-state BB84 protocol [100].

In previous works, Sagnac polarization modulators have been used with a carefully chosen asymmetry in the Sagnac interferometer, allowing for what we will refer to as *time-shifted modulation*. As described in Section 4.2, when using an asymmetric iPOGNAC with a delay line $\tau_d \geq \tau_{\text{mod}} + \tau_s$, asymmetric modulation is achieved by sending a large enough electrical pulse ($\tau_s \geq 2\tau_{\text{mod}}$) to modulate with the same intensity the co-propagating and counter-propagating optical pulses of width $\tau_{\text{op}} \leq \tau_s - 2\tau_{\text{mod}}$. The three symbols are achieved by sending an electrical pulse aligned with the optical co-propagating for $|L\rangle$, shifting the electrical symbol by τ_d for $|R\rangle$, and sending no electrical pulse for $|D\rangle$. Thus, we can define the corresponding $s_i(t)$ required to generate each symbol, with $i = R, L, D$ as

$$\begin{aligned} s_L(t) &= V_{\frac{\pi}{2}} \Pi\left(\frac{t - t_0}{\tau_s}\right), \\ s_R(t) &= V_{\frac{\pi}{2}} \Pi\left(\frac{t - t_0 - \tau_d}{\tau_s}\right), \\ s_D(t) &= 0, \end{aligned} \quad (4.15)$$

where $V_{\frac{\pi}{2}}$ is the half-wave voltage of the phase modulator and t_0 is an arbitrary time such that the phase electrical signal aligns with the optical pulse (Fig. 4.3a).

The asymmetric configuration coupled with the time-shifted modulation allows the creation of three polarization states by only employing two-level signals (i.e., $V = \{0, V_{\frac{\pi}{2}}\}$). This configuration, however, implies a limitation on the maximum achievable repetition rate R of

the modulation (see Section 4.5).

If more than two voltage levels are available (in particular, $V_{\frac{\pi}{2}}$, 0, and $-V_{\frac{\pi}{2}}$), it is possible to increase the repetition rate by having the electrical pulse aligned with the optical co-propagating in both cases, which we will refer to as *differential modulation* from now on, such that

$$\begin{aligned} s_L(t) &= V_{\frac{\pi}{2}} \Pi\left(\frac{t-t_0}{\tau_s}\right), \\ s_R(t) &= -V_{\frac{\pi}{2}} \Pi\left(\frac{t-t_0}{\tau_s}\right), \\ s_D(t) &= 0, \end{aligned} \quad (4.16)$$

which also removes the requirement for $\tau_s \geq 2\tau_{\text{mod}}$ (Fig. 4.3b), reducing it instead to $\tau_s \geq \tau_{\text{op}}$ so that the entire optical pulse is modulated equally. The same modulation scheme can also be used in a symmetric configuration as presented in Section 4.2.1, requiring an increase in the modulation voltage by a gain factor as described by Eq. (4.12) (Fig. 4.3c).

However, it is possible to remove the requirement for a voltage increase by using *balanced modulation* (Fig. 4.3d), which has electric signals with a shape given by Eq. (4.13), such that

$$\begin{aligned} s_L(t) &= V_{\frac{\pi}{2}} \left[\Pi\left(\frac{t-t_0}{\tau_s}\right) - \Pi\left(\frac{t-t_0-\tau_s}{\tau_s}\right) \right], \\ s_R(t) &= -V_{\frac{\pi}{2}} \left[\Pi\left(\frac{t-t_0}{\tau_s}\right) - \Pi\left(\frac{t-t_0-\tau_s}{\tau_s}\right) \right], \\ s_D(t) &= 0. \end{aligned} \quad (4.17)$$

This modulation scheme not only relaxes the requirement for voltage amplification that is otherwise required, but it also has the property of each symbol being zero-average voltage. In standard commercial AC-coupled amplifiers, the amplification factor is usually dependent on the average signal level (i.e. the DC component). By each symbol begin zero-average voltage, the average signal level is kept at zero independent of the sequence being sent, greatly mitigating patterning effects.

The balanced modulation scheme was tested on a Sagnac polarization modulator when injecting pulsed $|D\rangle$ states at a repetition rate of $R = 1.5$ GHz. By creating a fixed three-states sequence of ‘LRD’ and projecting into the Y and X basis, a polarization extinction ratio (PER) for each basis was obtained as $\text{PER}_Y = 23.147 \pm 0.003$ dB and $\text{PER}_X = 23.981 \pm 0.005$ dB (Fig. 4.4). If this state preparation was used for QKD applications, for example, the intrinsic QBER can be obtained as

$$\text{QBER} = \frac{1}{1 + 10^{\text{PER}/10}}, \quad (4.18)$$

which would correspond to $\text{QBER}_Y \approx 0.5\%$ and $\text{QBER}_X \approx 0.4\%$. Then, the same system was used to emulate a QKD experiment by sending a pseudo-random sequence of 1024 states according to the three-state BB84 protocol [100].

Finally, to compare both modulation schemes applicable to symmetric Sagnac modulators, an iPOGNAC system was used with both the previously mentioned modulation types, injecting continuous wave laser light with a defined $|D\rangle$ polarization to its input port and measuring the projection of the output state on the $|A\rangle$ polarization. To take into account imperfections in the system, the electrical signals $s^*(t)$ were measured using an RTP164B oscilloscope by Rohde & Schwarz after the corresponding amplification stage. The

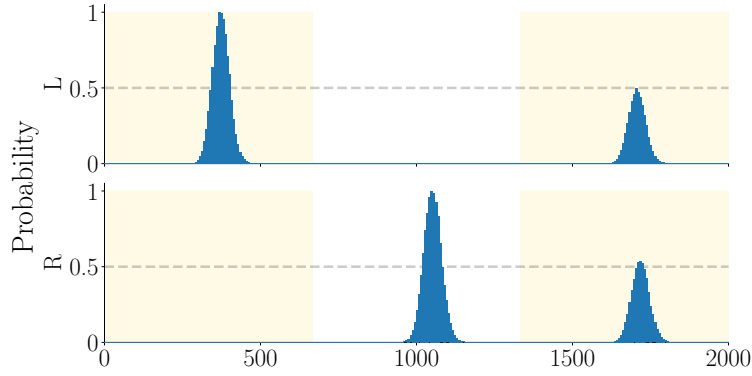


FIGURE 4.4: Generated states at 1.5 GHz of repetition rate using the symmetric balanced configuration and projected on the Y basis, with a polarization extinction ratio of $\text{PER}_Y = 23.147 \pm 0.003$ dB observed between the $|L\rangle$ and $|R\rangle$ states.

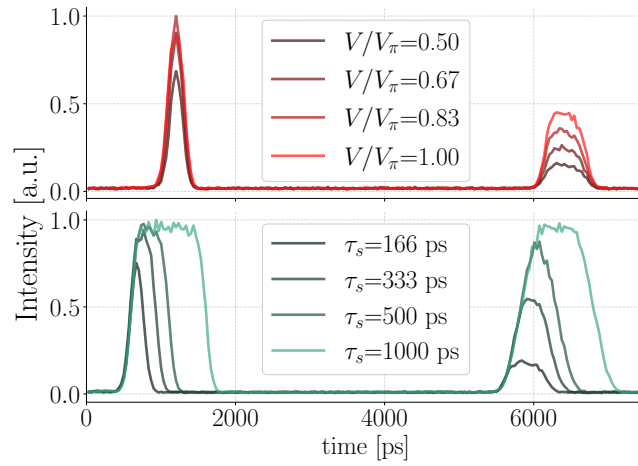


FIGURE 4.5: Experimental data showing the behavior of the time-shifted asymmetric modulation varying τ_s (bottom) and V (top).

maximum voltage used for both cases remained constant to highlight the reduction in applied phase discussed in section 4.2.1 on page 55.

Once the resulting phase difference in the Sagnac interferometer due to the electrical signals, $\phi_s^*(t)$, is obtained, the probability of measuring the system in the state $|A\rangle$ can be written as

$$P_A(t) = \left| \langle A | \left(|H\rangle + e^{i\phi_s^*(t)} |V\rangle \right) \rangle \right|^2 = \sin^2 \left(\frac{\phi_s^*(t)}{2} \right). \quad (4.19)$$

This probability corresponds to the projection onto the chosen state, which can be generalized to any arbitrary measurement basis. In the case of a continuous optical signal, this projection translates into an intensity modulation, effectively carving the light field according to the applied modulation. Figure 4.5 shows the measured relative intensity at the output of a Sagnac polarization modulator, when injecting continuous wave light with fixed $|D\rangle$ polarization and projecting on the $|A\rangle$ state, as a function of τ_s and the modulating voltage, for an asymmetry of $\tau_d = 5$ ns.

To properly compare the expected probabilities with their experimental value, the detection jitter of the single photon detectors used was also taken into account (Fig. 4.6a).

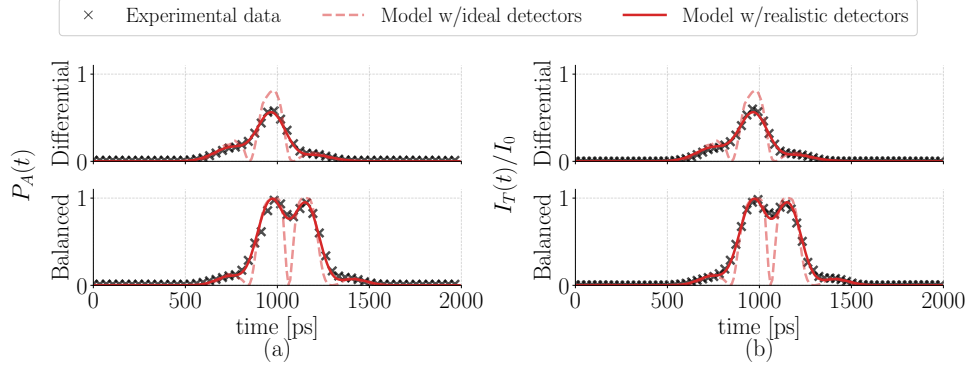


FIGURE 4.6: Comparison between the differential and balanced symmetric modulation for (a) polarization modulator and (b) intensity modulator.

4.4 Sagnac intensity modulators

Sagnac intensity modulators consist of a Sagnac interferometer with an EOM inside the Sagnac loop (Fig. 4.1b). When used in pulsed regime, as presented in Roberts et al. [98], this scheme allows the controllable attenuation of the optical pulses by carefully choosing the modulating voltage and the beamsplitter ratio.

Assuming a time-independent beamsplitter with transmissivity T , for a given time t , the output intensity of a Sagnac interferometer will be given by

$$I_T(T, t) = I_0 \left| e^{i\phi(t)} (T - 1) + T \right|^2, \quad (4.20)$$

with I_0 the intensity at the input port and $\phi(t)$ the phase difference between the two arms of the Sagnac at time t . By combining this with Eq. (4.7), the time-dependent transmission can be obtained, from which the extinction ratio ER can be estimated. Assuming $\phi_s(t) = 0$ for a given time t , and the absolute maximum phase to be $\phi_{\max} = \max |\phi_s(t)|$, the extinction ratio is given by

$$ER(T) = 10 \log_{10} \left| \frac{e^{i\phi_{\max}} (T - 1) + T}{2T - 1} \right|^2. \quad (4.21)$$

As highlighted by Roberts et al., to reduce patterning effects on the system, it proves convenient to set $\phi_{\max} = \pi$, such that the modulation occurs at the peak of the transfer function, where the derivative is zero, reducing small fluctuations of the electrical voltage that could occur in the input electrical chain. It is worth noting that to properly attenuate an optical pulse, the phase $\phi_{\max}$ has to be maintained for the entire duration of the pulse.

Once again, to provide further experimental validation of the proposed model, the same procedure presented in the previous section was done using a Sagnac intensity modulator with a beamsplitter with transmissivity $T = 1/2$, maintaining the same electrical signals $s^*(t)$. For this measurement, instead of projecting to a particular polarization state, we simply measured the output intensity of the modulator, such that

$$I_T(T, t) = I_0 \left| e^{i\phi_s^*(t)} (T - 1) + T \right|^2 = I_0 \sin^2 \left(\frac{\phi_s^*(t)}{2} \right), \quad (4.22)$$

showing the same time dependence as for the polarization case (Fig. 4.6b), with, as before, I_0 the intensity at the input port.

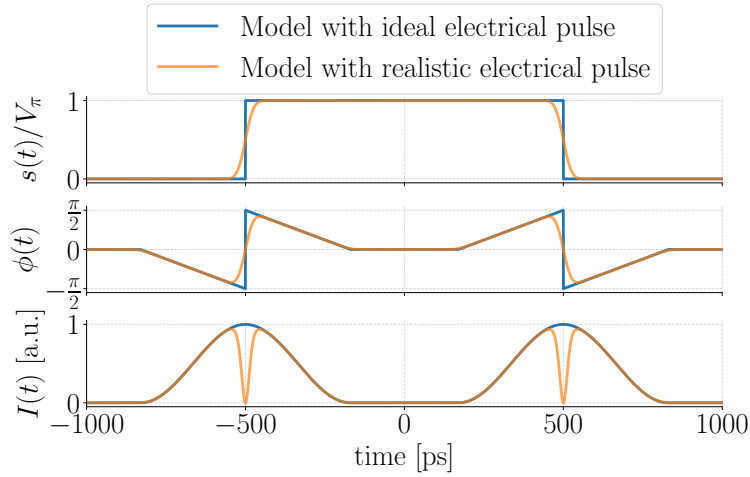


FIGURE 4.7: Example of pulse generation through carving using the Sagnac intensity modulator in symmetric configuration. Despite the realistic scenario presenting a "dip" in the center of the pulse, it is only when perfect symmetry is achieved that the intensity reaches zero, otherwise resulting similarly to the ideal case.

4.4.1 Pulse generation with symmetric configuration

When using a Sagnac intensity modulator in the symmetric configuration, everything exposed in section 4.2.1 is still valid, allowing for an increase in the repetition rate of the intensity modulation when using pulsed light at the input. Moreover, in addition to this, a new application arises from the nature of Sagnac interferometers: *pulse generation* by carving from continuous wave light (demonstrated in [122]). For this regime to occur, the system has to be used in the condition $\tau_s > \tau_d$, which happens automatically in the symmetric configuration, where $\tau_d = 0$.

Assuming an input signal of the form $s(t) = \Pi(t/\tau_s)$, it can be seen that the response function of the phase modulator, given by eq. (4.7), is nonzero only on the rising and falling edge of the electrical pulse (Fig. 4.7). When reaching the beamsplitter at the output, only those nonzero phase points will interfere constructively on the second mode of the beamsplitter, thus generating two optical pulses separated by τ_s . However, when taking into account imperfections in the electrical signal (i.e. not perfectly square), the transition from negative to positive phase difference is 'smoothed', thus creating a 'dip' on the optical pulse due to the transition having a zero-phase-difference point on each of the edges. If pulse shaping is relevant, this can be easily solved by adding a non-zero delay of at least τ_{mod} , such that $\tau_d > \tau_{\text{mod}}$, such that the zero-phase-difference points are removed. The experimental results are shown in fig. 4.8 on the next page.

4.5 Maximizing the repetition rate

Choosing the right modulation type is one of the key metrics to increase the repetition rate of the source. Modulation strongly depends on the geometry of the modulated system: for example, a loop scheme (like the one of the iPOGNAC) has different optimized modulations than an in-line system. This is because, as shown in the previous section, additional inter-symbol interference needs to be taken into account. Here, three different modulation schemes will be covered, one related to an asymmetric Sagnac configuration (time-shifted modulation, see section 4.3 on page 56), one to a symmetric one (balanced modulation, see

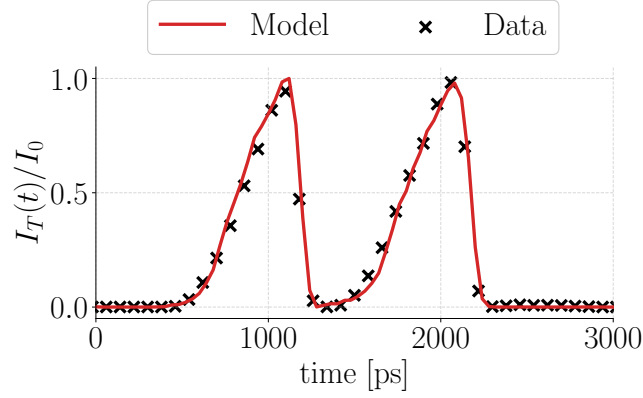


FIGURE 4.8: Experimental data testing the pulse generation model proposed in sec. 4.4.1.

Modulation scheme	ΔV	t_{sym}	t_{sym}^*	R_{max}
Time-shifted	0.5	$5\tau_{\text{mod}} + \tau_{\text{op}}$	1.7 ns	~ 588 MHz
Differential asymmetric	0.5	$2(\tau_{\text{mod}} + \tau_s)$	972 ps	~ 1.03 GHz
Differential symmetric	0.685	$\tau_{\text{mod}} + \tau_s$	486 ps	~ 2.06 GHz
Balanced	0.5	$\tau_{\text{mod}} + 2\tau_s$	652 ps	1.53 GHz

TABLE 4.1: Performance parameters for all implemented modulations, with ΔV the normalized range of voltage required to achieve all states for the three-state BB84 protocol and t_{sym} the minimum period as a function of the setup parameters. The minimum period t_{sym}^* and maximum repetition rate R_{max} were obtained assuming experimentally verified values of $\tau_{\text{mod}} = 320$ ps, $\tau_s = 166.6$ ps, and $\tau_{\text{op}} = 100$ ps.

section 4.2.1 on page 55), and one valid for both (differential modulation, see section 4.3 on page 56 and section 4.2.1 on page 55).

For each modulation format presented in this section, the performance will be estimated through the following performance metrics: t_{sym} , which corresponds to the symbol period and is defined as the minimum time required to concatenate two symbols without experiencing inter-symbol interference in the modulation region, and $\Delta V = (V_{\text{max}} - V_{\text{min}})/V_{\pi}$, which corresponds to the normalized range of voltages necessary for modulation necessary to achieve all the symbols. For the sake of absolute maximum ratings, we will assume that the target optical pulse is smaller than τ_s . These parameters are summarized in Table 4.1, where the modulator length was experimentally estimated as $\tau_{\text{mod}} = 320$ ps and the minimum achievable electrical signal width as $\tau_s = 166.6$ ps to provide a numeric value for all cases.

With each of the proposed schemes, it is possible to increase the repetition rate of the system at the expense of non-ideal modulation, that is, allowing inter-symbol interference. In this regime, the total time required for the response function to a given $s(t)$ is greater than the repetition rate desired for the modulation. Depending on the desired use of the system, this behavior can be tolerated to allow an increase in the overall repetition rate. When using periodic modulation signals, this behavior can be pre-compensated, taking into account the inter-symbol interference terms. However, for applications like QKD where the modulating signal has to be randomly chosen at the qubit repetition rate, this interference leads to randomly distributed imperfect modulation, resulting in a net increase in QBER.

4.5.1 Time-shifted modulation

Time-shifted modulation is achieved when selectively targeting either the co-propagating or counter-propagating optical pulse in an asymmetric Sagnac configuration as described in section 4.3 on page 56. To avoid consecutive symbols from interfering, it is enough to avoid overlap in the modulation region.

As shown in Fig. 4.2, for a given electrical pulse of width τ_s , the total duration of the modulation is determined by both the co-propagating and counter-propagating phase responses. In general, assuming the asymmetry condition $\tau_d \geq \tau_{\text{mod}}$, the total modulation time for a symbol is $t_{\text{sym}} = \tau_s + \tau_d + \tau_{\text{mod}}$, where τ_d is the delay between the co- and counter-propagating contributions, and τ_{mod} is the modulator length.

To avoid overlap between the co-propagating phase response ϕ_{co} and the counter-propagating response ϕ_{ct} , the delay must satisfy $\tau_d \geq \tau_s + \tau_{\text{mod}}$, which ensures that the counter-propagating phase starts only after the co-propagating phase ends. Substituting this condition into the expression for t_{sym} gives the minimum period $t_{\text{sym}} \geq 2(\tau_s + \tau_{\text{mod}})$. A convenient boundary condition is to set $\tau_s \geq 2\tau_{\text{mod}}$, which ensures a sufficiently long pulse relative to the modulator transition time. In this case, the minimum separation between consecutive optical pulses is $t_{\text{sym}} \geq 6\tau_{\text{mod}}$.

If, instead, the Sagnac modulator is used to modulate optical pulses, we can allow interference on the phase response, while keeping the modulation region unaffected. This means that the condition is slightly relaxed since the optical pulse is placed in the middle of the co-propagating in the second slot, meaning that some phase response interference can be tolerated on that region, while keeping the phase modulation of the pulse unaffected. Assuming also the minimum required electrical pulse duration such that the phase applied by the counter-propagating component reaches its maximum value for the entire duration of the optical pulse, that is, $\tau_s = 2\tau_{\text{mod}} + \tau_{\text{op}}$ and a minimum required asymmetry $\tau_d = \tau_s + \tau_{\text{mod}}$, the minimum symbol period becomes $t_{\text{sym}} = 5\tau_{\text{mod}} + \tau_{\text{op}}$.

4.5.2 Differential modulation

When using differential modulation, it is worth distinguishing between the asymmetric and symmetric configurations. For the asymmetric configuration, since now the symbols do not require a temporal shift with respect to each other, the minimum symbol period becomes $t_{\text{sym}} = \tau_d + \tau_{\text{mod}} + \tau_s$, where there is no longer the constraint of $\tau_s \geq 2\tau_{\text{mod}} + \tau_{\text{op}}$, since only the co-propagating component is used for applying the modulation, but still keeping the constraints $\tau_d = \tau_s + \tau_{\text{mod}}$ and $\tau_s \geq \tau_{\text{op}}$, thus obtaining $t_{\text{sym}} = 2(\tau_{\text{mod}} + \tau_s)$.

On the other hand, when utilizing differential modulation with the Sagnac in a symmetric configuration, the minimum symbol period is reduced by τ_d , obtaining instead $t_{\text{sym}} = \tau_{\text{mod}} + \tau_s$, once again with $\tau_s \geq \tau_{\text{op}}$, which increases the maximum repetition rate by a factor of 2 compared to the asymmetric case. However, this increase in repetition rate comes with the cost of increasing the required voltage by a gain factor of $g_V = [1 - \tau_s/(2\tau_{\text{mod}})]^{-1}$ as defined in Sec. 4.2.1.

4.5.3 Balanced modulation

When using balanced modulation, the maximum repetition rate is slightly reduced compared to the differential case in the symmetric configuration, since now it requires the use of two voltage pulses with inverted sign, each with a duration of τ_s . For this case, both positive and negative pulses should last at least the optical pulse width, which implies that the minimum symbol period now becomes $t_{\text{sym}} = 2\tau_s + \tau_{\text{mod}} \geq 2\tau_{\text{op}} + \tau_{\text{mod}}$. However, in comparison to the

differential case, the use of balanced modulation relaxes the condition for higher voltage, making it potentially less costly to implement. It is worth noting that this type of modulation also helps mitigate the patterning effect in amplifiers, because the amplification depends on the average signal level, which in this case is zero and is not influenced by the sequence of consecutive pulses.

4.6 Conclusion

Because of their intrinsic phase stability and architectural flexibility, Sagnac-loop modulation schemes have been, and will continue to be, key components for quantum communications. This work provides a complete, general model for Sagnac-based modulators that generalizes existing schemes and offers a practical framework applicable to a broad class of loop-based modulators in the literature. Additionally, we presented and experimentally validated a symmetric configuration of the Sagnac loop with a differential modulation driving of the EOMs that enables stable operation and allows intensity and polarization modulation as well as the generation of optical pulses directly within the interferometer at higher repetition rates with respect to other traditionally used methods. This combination of theory and practice provides a solid foundation for future photonic and quantum communication applications.

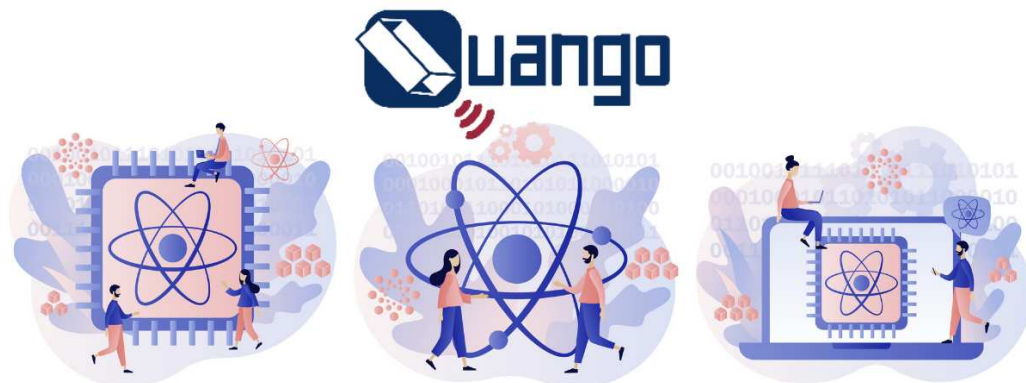
Chapter 5

GHz-rate polarization-based DV-QKD system

I have contributed to the project by participating in these work packages: design, technology development, ground segment, functional validation, and the free-space tests of the source.

5.1 Definition of the project

(The following informations are extracted from [6])



Cybersecurity is the main concern for the digital world of these days. We all share tons of information on the internet, but are still not clear on how well this data is being protected. Aware of this imminent hacking threat of sensitive and utmost important data, the European Commission has, for these past years, put in motion different programs to find solutions on how to protect all communications within the European region. To do this, it is essential to improve and maximize security protocols with its feasible integration into current communication channels, such as 5G, which not only involves ground but also satellite communications.

Quantum Key Distribution (QKD) is an ultra-secure form of encryption that allows data to be transmitted with a very high level of security, and is proving to be a protocol that can be easily integrated into current technologies that are being used to transmit information throughout the European continent. On the other hand, 5G is the fifth generation of wireless connection that is being currently deployed all over the world to enable the Internet of Things (IoT) technology.

Coordinated by University of Padova, in collaboration with the research institutions ICFO, Sorbonne University, University of Malta, and the companies Sateliot, Stellar Project, and Argotec (Figure 5.1), the project aims to design a secure communication network implementing Quantum technologies, 5G communications and nanosatellites. More



FIGURE 5.1: Partners within the QUANGO project.

specifically, the project aims to design a 12U-CubeSat low-earth-orbit satellite constellation, deployed in an orbit in space at 600km, that will combine capabilities for secure communications with QKD and 5G connections. QUANGO (cubesat for QUANTum and 5G cOMmunication) [7] will carry out laboratory demonstrations of critical components, subsystems and payloads and study their implementation feasibility. It will then pioneer the integration of QKD security systems into 5G protocols aiming to create, in the long run, a 5G-QKD satellite constellation that can cover all European areas and offer the maximum security in communications. QUANGO will provide a new paradigm to share the satellite infrastructure required for secure communication based on quantum technologies and for 5G communication. It will help lay the groundwork for the future Quantum European Infrastructure, a pan-European quantum communication infrastructure that uses satellite as well as ground-based solutions to connect and link European regions and cities. Specific objectives of the project include:

- Design of a nano-satellite with both QKD and 5G capabilities for low orbit satellite-to-ground communication.
- Design and development of the quantum payload and ground station.
- Laboratory demonstrations of the critical components and subsystems.
- Theoretical study of future technologies: intersatellite QKD and integration of QKD security into 5G protocols.
- Exploitation and business plan for the 5G-QKD satellite
- Development and integration of a QKD system in the networking infrastructure of a leading bank in an EU member state as a prototypical end user of the 5G-QKD satellite.

As a member of the QUANGO project, the University of Padova was in charge of the development of the quantum payload, providing a stable QKD transmitter together with proofs of free-space testings for depolarization. The source should aim at achieving a repetition rate of 1 GHz, a QBER around 1% and not depolarize in free-space on the long run.

5.2 Introduction

Although protocols such as BB84 and decoy-state variants have been implemented over increasing distances and integrated into field-deployable systems [74, 124], the need for a global secure network calls for more innovative solutions. That is where satellite-based QKD comes into play: unlike traditional fiber optic cables, which can only transmit data over some hundred kilometers due to signal loss [89, 83], satellites offer the potential to establish secure communication links spanning continents (whilst in a fiber the transmission losses increase exponentially with distance, they follow a square-law relationship in free-space) [89, 130, 97].

The groundbreaking work in satellite-based quantum communication has led to remarkable achievements, such as the development and launch of the Quantum Science Satellite "Micius" by the Chinese Academy of Sciences [88]. Micius has not only shown that satellite-based QKD is feasible but has also successfully enabled secure communication links between continents, marking a significant step forward in the quest for a truly global secure communication network.

In this work, we present a three-state polarization-encoded 1550 nm QKD setup that is fit both for fiber and satellite communication. Despite the duality, the system is designed to be space-graded and therefore ready for an integration in a *CubeSat*. We disclose the innovative setup, that includes two *iPOGNACs*, first proposed by Agnesi, Avesani et al. [19], one for polarization encoding and the other for intensity modulation. We show the results of the QKD tests inside the lab, that display an average *Quantum-Bit-Error-Rate* (QBER) of $\sim 0.25\%$ and a *Secret-Key Rate* (SKR) of ~ 467 kb/s at 26 dB of channel attenuation. We discuss the setup used to perform QKD tests on a 620 m free-space link in daylight and show the results, that yield a QBER of $\sim 1.5\%$ and SKR of ~ 1 Mb/s. The novelties presented in this work are: the optical scheme, qubit-based synchronization tested for the first time at 1GHz in free-space, the *iPOGNAC* polarization encoder working at 1GHz and a free-space QKD test running with a QBER around 1.5% using *Superconducting-Nanowire Single-Photon Detectors* (SNSPDs).

5.3 Introduction to the system

We engineered a Quantum Key Distribution source and receiver of polarization-encoded states at 1550 nm with the capability to execute the efficient 3-states 1-decoy BB84 protocol, like described in [47]. Both source and receiver are represented in Fig. 5.2. The source is realized with a gain-switched DFB 1550 nm laser followed by a sequence of two *iPOGNACs*, consisting on a Sagnac loop modulated by an electro-optical phase modulator (EOM). As shown in [9], when the input polarization state for the *iPOGNAC* encoder is $|D\rangle$, this system is capable of creating any polarization state on the equator of the Bloch Sphere such that $|\Psi\rangle = |H\rangle + e^{-i\Delta\phi}|V\rangle$. Thus, by combining one of the *iPOGNAC* encoders with a $|D\rangle$ -aligned polarizer at its output, it is possible to attenuate incoming light pulses by a factor of $\sin^2(\Delta\phi)$, allowing the system to encode decoy states. The attenuated pulses then go through a second *iPOGNAC* stage, in which the polarization is encoded into one of the three states required for the protocol: $|D\rangle$, $|L\rangle$ and $|R\rangle$, corresponding to diagonal, left-hand circular, and right-hand circular polarization states respectively. Both EOMs on the *iPOGNAC* encoders and the pulsed laser are controlled by an FPGA. The encoded signal is then sent through an optical channel (i.e. fiber or free-space), and finally to a standard polarization receiver consisting on a balanced beam-splitter, which performs the random basis choice, with each of its outputs followed by a polarization controller and a polarizing beam-splitter. The polarization controllers were set such that one arm of the beam-splitter projected the incoming photons on the key basis $\mathbb{Z} = \{|L\rangle, |R\rangle\}$, while the other on the check basis $\mathbb{X} = \{|D\rangle, |A\rangle\}$.

The electrical components of the source include a power supply, a laser module comprising a Gooch&Housego AA0701-193400-010-PM900-FCA50 laser and a Meerstetter TEC-1091-NTC-SCREW temperature controller, a variable optical attenuator, a Niclslab XPOW-8AX-CV configurable power supply, an IXblue DR-PL-20-MO amplifier, an IXblue DR-DG-20-MO amplifier, an *iPOGNAC* intensity modulator, an *iPOGNAC* polarization modulator, an IXblue DR-VE-10-MO amplifier and a Xilinx Ultrascale+ FPGA. Both

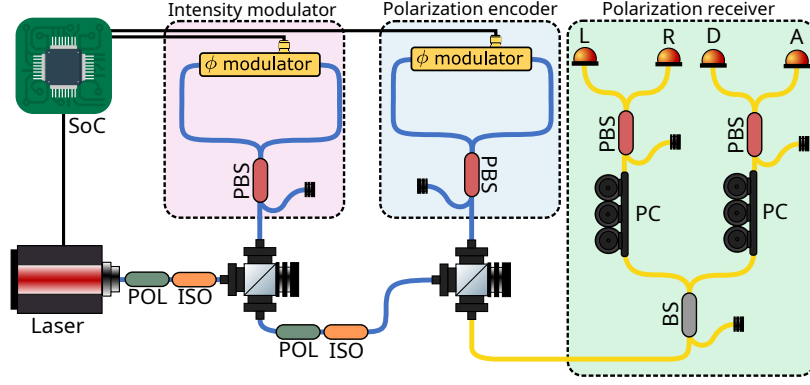


FIGURE 5.2: Scheme of the setup. The source is composed by a DFB laser generating optical pulses that go through an isolator (ISO), then inside a free-space-coupled (the coupling of the input fiber is tilted by 45° to proceed with the $|D\rangle$ state) beam-splitter (BS): the beam gets reflected into the Sagnac loop, consisting of a polarization-beam-splitter (PBS) and a phase-modulator (ϕ -Mod), and travels back to be transmitted, through a polarizer (POL), into the polarization modulation stage, which consists in the same pieces except the polarizer. After travelling through the channel, the pulses reach the receiver, consisting on a D-WDM filter, a fiber BS, two polarization-controllers (PC), two PBSs and four detectors, one for each polarization state (namely L,R,D,A). The output is analyzed by a time-to-digital-converter (TDC) that is synchronized by the same system-on-a-chip (SoC) that is used to generate the light pulses and control the modulation of the signal.

intensity iPOGNACs use IXblue MPZ-LN-20-00-P-P-FA-FA phase modulators and an OZ-Optics FOBS beam splitter as a circulator.

As shown in [19], when the input polarization state for the iPOGNAC encoder is $|D\rangle$, this system is capable of creating any polarization state on the equator of the Bloch Sphere such that $|\Psi\rangle = |H\rangle + e^{-i\Delta\phi}|V\rangle$. Thus, by combining one of the iPOGNAC encoders with a $|D\rangle$ -aligned polarizer at its output, it is possible to attenuate incoming light pulses by a factor of $\sin^2(\Delta\phi)$, allowing the system to encode decoy states. The attenuated pulses then go through a second iPOGNAC stage, in which the polarization is encoded into one of the three states required for the protocol: $|D\rangle$, $|L\rangle$ and $|R\rangle$, corresponding to diagonal, left-handed circular, and right-handed circular polarization states respectively. To achieve GHz repetition rate, both iPOGNAC encoders were built in the symmetric configuration, which through precise electrical signals are able to reach such rates (see chapter 4 on page 51).

Both EOMs on the iPOGNAC encoders and the pulsed laser are controlled by an *Ultrascale+* based system-on-a-chip (SoC). The encoded signal was then sent through an optical channel (i.e. fiber or free-space), and finally to a standard polarization receiver consisting on a balanced beamsplitter, which performs the random basis choice, with each of its outputs followed by a polarization controller and a polarizing beam-splitter. The polarization controllers were set such that one arm of the beam-splitter projected the incoming photons on the key basis $Z = \{|L\rangle, |R\rangle\}$, while the other on the check basis $X = \{|D\rangle, |A\rangle\}$.

5.3.1 Description of the free-space terminals

For the free-space testbed we have located our optical terminals in two buildings of the University, both in the city of Padova. As sketched in Fig. 5.3(A), the transmitter node (Tx) has been installed at the Department of Physics and Astronomy (DFA), shown in Fig.

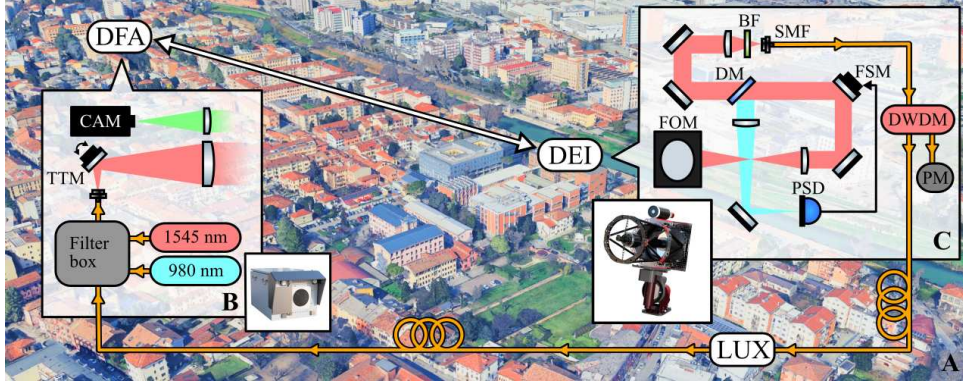


FIGURE 5.3: **Testbed illustration.** (A) Aerial view of the 620 m free-space channel between DFA and DEI in Padova. Data from Google Earth [©2025 Google]. (B) Schematic of the Tx node at DFA, connected to LUX through a deployed fiber network. It is also shown the render of the 3D model of the enclosure hosting the optical terminal. (C) Schematic of the Rx optical components. It is also shown the render of the 3D model of the receiving telescope. TTM: tip-tilt mirror; CAM: camera; FOM: folding mirror; DM: dichroic mirror; BF: bulk filter; SMF: single-mode fiber; DWDM: dense wavelength-division multiplexer; PSD: position-sensitive-detector; PM: power meter.

5.3(B), and connected to the QKD source at Luxor laboratory (LUX) through a network of deployed fibers characterized by $L_{\text{Fiber}}^{\text{Tx}} = 2.75$ dB of losses.

The Tx is composed by a filter box that, by exploiting a fiber wavelength-division multiplexer (WDM), adds other wavelengths to the propagation of the signal: the first one, is at $\lambda_{\text{Coarse}} = 980$ nm, and it is used for coarse pointing the receiver, while the second one, is at $\lambda_{\text{Beacon}} = 1545.32$ nm (C40 of ITU-grid), and it is used at the receiver to monitor the channel efficiency from the power coupled into a single-mode fiber (SMF) during the operations. Once these signals have been multiplexed, they will propagate into a SMF connected to a linear stage and positioned at the rear focal plane of a 2-inch lens, part of our optical terminal. Between the focal plane and the lens, a tip-tilt mirror is present. With the purpose of increasing the pointing accuracy of the system, the tip-tilt mirror is remotely controllable thanks to two linear actuators, allowing for a fine alignment of $2 \mu\text{rad}$ roughly [49]. After the lens, the C-band signals will propagate in free-space as collimated beams of waist $W_0 = 25$ mm, through an enclosure's optical window of diameter 150 mm, minimizing the reflection losses for the exploited wavelengths. From the fiber to the optical window, fixed optical losses are present for an amount of $L_{\text{Optics}}^{\text{Tx}} = 0.7$ dB. The terminal presents also a coarse line, where a camera (CAM) creates an image on a focal plane of a system of lenses with an equivalent focal length of 850 mm, giving a full-angle field of view (FOV) of 8×6.4 mrad². The system is completely tunable from remote, and by controlling an alt-azimuth mount (model Az-GTi by SkyWatcher) it is possible to align the Tx with the receiver.

The receiving node (Rx) is an optical ground station (OGS) located on the roof of the Department of Information Engineering (DEI). The OGS is equipped with a dome (3M by ScopeDome) and a German Equatorial Mount (model Paramount ME-II by Software Bisque) that supports an $f/8$ Ritchey-Chrétien (model PRORC-400 by Officina Stellare) telescope, with an aperture diameter of $D_{\text{Rx}} = 410$ mm and a linear obscuration factor $\alpha = 0.41$. The Rx telescope is equipped on the top flange with an additional coarse telescope $f/12$ Maksutov (model SkyMax 127 by Sky-Watcher), with an aperture of 127 mm, and is equipped with a camera (model ASI 294 MC Pro Color by ZWO) with a

full-angle FOV of $9 \times 13 \text{ mrad}^2$ used as coarse camera.

On the Rx telescope's rear, schematized in Fig. 5.3(C), a $600 \times 600 \text{ mm}^2$ breadboard hosts an optical line for SMF injection, reachable through a 2-inch mirror (FOM) tilted by 45 degrees with respect to the telescope's optical axis. On the breadboard, after the primary focus, a 100 mm focal lens collimates the received beam, forming a pupil of dimension 12.5 mm on the surface of a 1-inch fast-steering mirror (FSM), which is included in the system to address any tip-tilt fluctuation caused by atmospheric turbulence. Following the reflection off the FSM, a dichroic mirror (DM) is placed along the path in order to separate the C-band signals from the coarse one. The 980 nm beacon will be reflected off the DM, and passing through a 300 mm focal lens, directed onto a silicon position-sensitive-detector (PSD) which will record the displacements of the centroid on the focal plane. This information will be used to adjust the voltage applied on the FSM's actuators, minimizing centroid fluctuations as much as possible. The C-band signals, transmitted through the DM, will be coupled into an FC/PC-terminated SMF, located after a bulk bandpass filter (BF). The filter is centered at 1550 nm, with a bandwidth of 40 nm full-width-at-half-maximum (FWHM), and it is placed before the fiber in order to decrease the noise in it. The focal length of the lens in front of the SMF of mode-field diameter (MFD) $10.4 \mu\text{m}$ is chosen to guarantee that the effective focal length of the system satisfies $f_{\text{eff}} = \pi \varnothing \text{MFD} / (4\lambda\beta)$, where $\beta \approx 1.12$, and $\varnothing$ represents the value of the diameter of the received beam experimentally observed at the telescope's aperture. Once in the fiber, the signals will pass through a telecom dense wavelength-division multiplexer (DWDM) with 100 GHz spacing centered at λ_{Beacon} , which is used to separate the C-band beacon from the QKD signals. The C40 output port is connected to a fiber coupled power meter (PM), with which we log the injected power to estimate the channel losses. The QKD signal instead, is connected to a deployed fiber that will end at LUX, where the QKD system is located. From the telescope's focal plane to the plane in front of the fiber we measured $L_{\text{Optics}}^{\text{Rx}} = 1.64 \text{ dB}$ of losses, while for the fibers deployed from DEI to LUX we measured $L_{\text{Fiber}}^{\text{Rx}} = 2.59 \text{ dB}$.

5.4 Results

This section is dedicated to the exposition of the results, first the preliminary ones in the lab (sec. 5.4.1) and then the ones of the testbed in free-space (sec. 5.4.2).

5.4.1 Results of the fiber link in lab

To demonstrate the capabilities of the source for QKD, a fixed pseudo-random sequence of 1024 symbols was generated to simulate a three-state one-decoy BB84 QKD implementation. The system was set-up with typical values [99], such that $\mu = 0.6$ and $\nu/\mu \approx 0.33$, with μ and ν the mean number of photons for signal and decoy pulses, respectively. Moreover, the pseudo-random sequence was generated such that $p_Z = 0.7$ and $p_X = 0.3$, with $p_{Z(X)}$ the probability to generate a state on the key (check) basis.

As a first instance, to highlight the stability of the system's low QBER over long periods of time, the source was ran at a repetition rate of 1 GHz for 1 hour without performing any active nor passive stabilization on any of its components. For this measurement, the secret key rate was estimated along the entire duration, obtaining an average SKR = $467 \pm 6 \text{ kb/s}$ at 26 dB of total losses (Fig. 5.4). This analysis was performed by applying decoy state bounds, taking into account finite size key effects [99]. The average QBER for the entire duration was observed to be $\text{QBER}_Z = (0.38 \pm 0.01)\%$ for the key basis, and $\text{QBER}_X = (0.27 \pm 0.03)\%$ for the check basis.

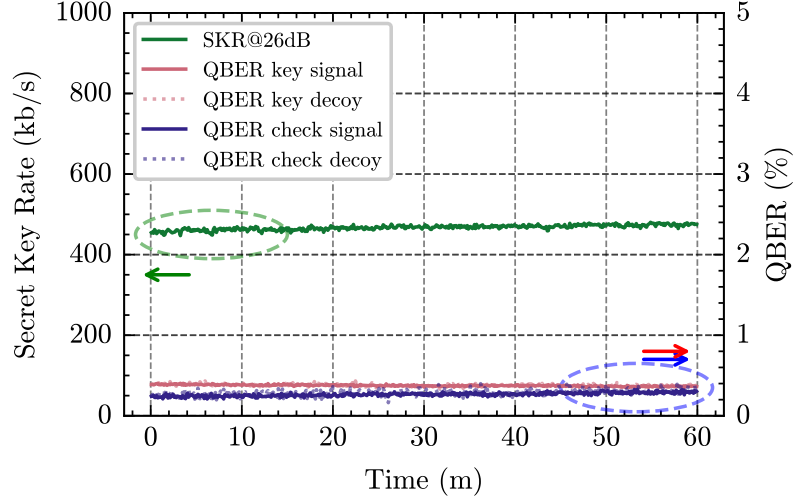


FIGURE 5.4: Secret key rate obtained over time for a 1024-symbol sequence in the lab, at 26 dB of total losses. In blue and red, associated with the right axis, the measured QBER on the Z and X basis.

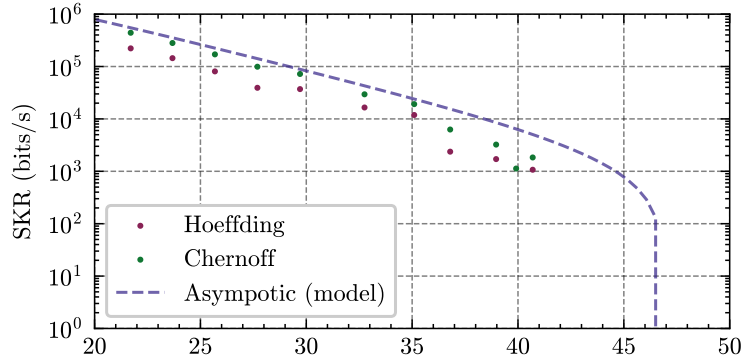


FIGURE 5.5: Estimation of the secret key rate for different channel attenuation values. The dashed line represents the asymptotic limit, while the red and green dots represent, respectively, the finite-key analysis using the Hoeffding and Chernoff bounds.

Then, by placing a variable optical attenuator between the source and the receiver, we performed the same test as before but for different channel attenuation values. For these measurements, the duration was constrained to that for which an entire block of key was sifted for each channel loss value. Following the same procedure, the secret key rate was estimated at multiple loss values (Fig. 5.5).

5.4.2 Results of the free-space link

The trial has been conducted on July 29th, 2025. For this free-space link, we consider as channel attenuation L_{Ch} the losses that are presents from the output of the enclosure's optical window to the optical power measured at the fiber-based PM after the DWDM (as shown in Fig. 5.3(C)).

In particular, for our horizontal link, we associate the channel losses to the following measurable terms:

$$L_{\text{Ch}} = L_{\text{F}} + L_{\text{Optics}}^{\text{Rx}} + L_{\text{SMF}}, \quad (5.1)$$

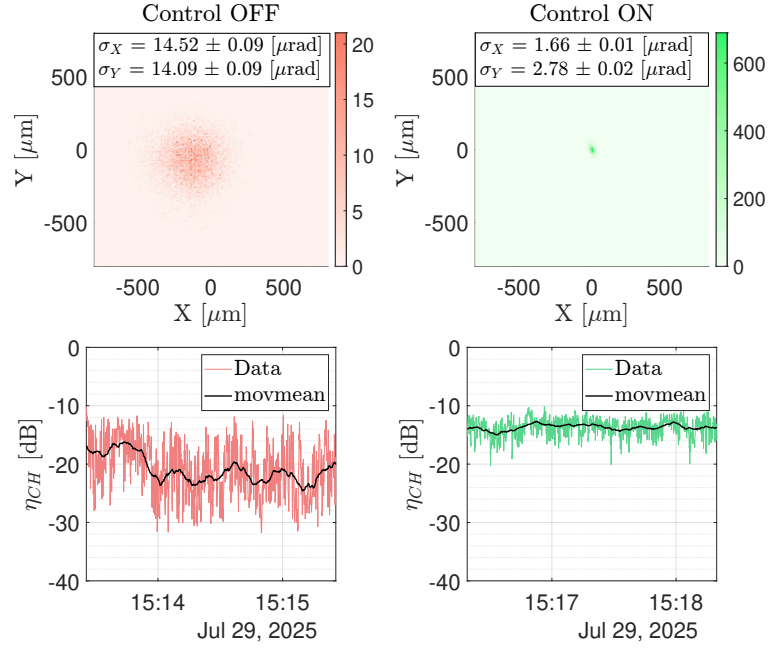


FIGURE 5.6: Control OFF and ON scatter plots, with PSD detecting λ_{Coarse} beam's centroid in a $10 \mu\text{m}$ bin width. The channel attenuation is measured for both scenarios.

where L_F denotes the losses due to atmospheric absorption, pointing error and receiver's collection efficiency, $L_{\text{Optics}}^{\text{Rx}}$ accounts for the insertion losses at the receiver, and L_{SMF} represents the coupling efficiency into SMF. The first term can be measured by placing a PM on the primary focal plane of the receiving telescope, and compare the values with the one measured at the transmitter side. During the experiment, we measured an average of $L_F = 1.9 \text{ dB}$. The system insertion losses, denoted as $L_{\text{Optics}}^{\text{Rx}}$ and already expressed in Section 5.3.1, represent all the losses due to reflections and non-optimal coating of some optical elements. The last term of Eq. 5.1 can be obtained by measuring the optical power in front of the fiber and comparing it with the one measured by the fiber-based PM into the SMF. This quantity highly depends on the atmospheric turbulence, that with its strength can decrease the coupling efficiency. As an example, we show in Fig. 5.6, data collected when the FSM has control OFF (open-loop) and control ON (closed-loop). On the scatters plots, we reported the number of occurrences of the λ_{Coarse} beam's centroid to fall in a bin of $10 \mu\text{m}$ width on the PSD focal plane. Thanks to the FSM feedback, the standard deviation of the angle of arrival (AoA), as seen from the telescope's aperture, can be reduced up to values that range from 3 to $1 \mu\text{rad}$, increasing the occurrences for a single bin. Moreover, the benefit of the FSM implementation allows to obtain a reduction in the measured losses of the channel attenuation of 7 dB.

Two distinct experiments were conducted over a 620 m free-space optical link between the DFA and DEI buildings to assess the performance of the GHz polarization-based QKD source. For both tests, we implemented the Qubit4Synch synchronization protocol [28].

First, we characterized the maximum achievable performance of the system under its nominal link conditions. However, to prevent saturation of the single-photon detectors and the data acquisition hardware due to high photon flux, calibrated optical attenuation was introduced at the receiver. The QKD transmission was operated continuously for one hour under daylight conditions (approximately noon), employing the same system configurations detailed in Section 5.4.1. Throughout the measurement, the system maintained a stable

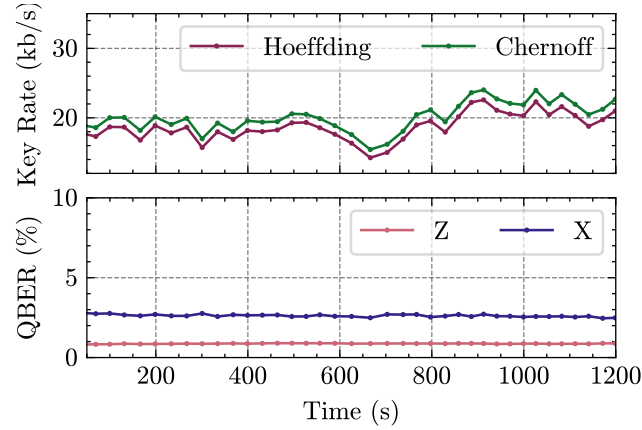


FIGURE 5.7: Results for the link in free-space with high channel losses (~ 39 dB).

quantum bit error rate (QBER) in the key basis of $QBER_Z \approx 0.8\%$. The QBER in the check basis was measured at $QBER_X \approx 2\%$ (see footnote ¹ for details). This configuration yielded a sustained secret key rate exceeding 1 Mb/s, establishing a new benchmark for free-space BB84 QKD systems over this distance.

Subsequently, to emulate the high-loss environment of a satellite-to-ground link, additional attenuation was introduced at the receiver to achieve a total channel loss of approximately 38.7 dB. Even under these conditions, the system demonstrated a low and stable QBER (around 1.5%) in both bases, enabling the generation of a secret key block approximately every 30 seconds, for a total secret key rate of around 20 kb/s.

To address scenarios with constrained acquisition times, such as a low-Earth-orbit satellite pass, we evaluated the performance using different finite-size security analyses. We compared the standard asymptotic bounds [99] with the tighter bounds proposed by Mannelath et al. [81], which are known to yield significantly higher key rates for smaller data block sizes. The performance was assessed for both large (e.g., $\sim 10^7$ bits) and small (e.g., $\sim 10^5$ bits) block sizes. In the evaluated scenarios, a positive secret key of around 20 kb/s was successfully extracted. This result underscores the system's robustness and operational flexibility, demonstrating its capability to be optimized for diverse environments.

5.5 Conclusions

In this work, we have successfully developed and tested a complete, high-performance Discrete-Variable QKD system operating at a 1 GHz repetition rate. The system, based on polarization-encoded states at 1550 nm, exploiting the *iPOGNAC* in its symmetric configuration and implementing the efficient 3-state 1-decoy BB84 protocol, was tested over both a stable fiber link and a 620 m urban free-space optical link. In laboratory fiber tests, the system demonstrated exceptional intrinsic stability, maintaining a low average QBER of $\sim 0.4\%$ over one hour of continuous operation, yielding a secret key rate of 467 ± 6 kb/s at 26 dB of channel loss. Over the free-space link, the implementation of a fast-steering mirror (FSM) to actively compensate for atmospheric turbulence proved crucial, improving channel efficiency by 7 dB. This enabled the system to achieve a sustained secret key rate exceeding 1 Mb/s with a stable key-basis QBER of $\sim 0.8\%$, even during daylight hours, establishing a

¹The slightly elevated $QBER_X$ compared to the results in Section 5.4.1 was attributed to a minor electrical misalignment at the source.

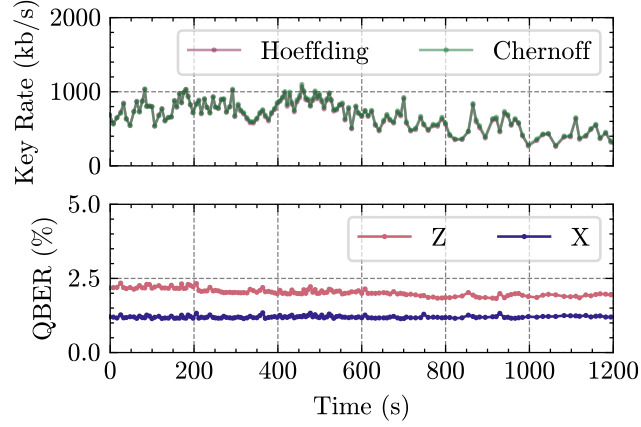


FIGURE 5.8: Results for the link in free-space with low channel losses (~ 18 dB).

new performance benchmark. Furthermore, we demonstrated the system's robustness by emulating a high-loss, satellite-to-ground link scenario. By introducing calibrated attenuation to reach a total channel loss of ~ 38.7 dB, the system successfully generated a secure key at a rate of around 20 kb/s. The application of advanced finite-size security analyses confirmed that a positive key rate could be extracted even with smaller data blocks, highlighting the system's suitability for time-constrained scenarios such as low-Earth-orbit satellite passes. These results collectively validate our platform as a robust, high-performance, and operationally flexible solution, paving the way for future metropolitan and satellite-based quantum communication networks.

Chapter 6

Long-term analysis of efficient-BB84 4-node network with optical switches in metropolitan environment

I have contributed to the project by participating in these work packages: technology deployment, functional validation, testing, logging and data analysis. Pre-print available at: [\[117\]](#)

6.1 Introduction

While point-to-point QKD links have demonstrated secure key exchange over both fiber and free-space optical channels, the integration of QKD into scalable, multi-node networks is essential for widespread adoption in real-world applications, such as secure governmental communication, financial services, and critical infrastructure protection [30].

QKD networks introduce new challenges and design requirements, including efficient key management, routing, and node interoperability. Recent network implementations have adopted efficient-BB84 to improve scalability and performance, enabling more practical deployments across metropolitan and backbone-scale infrastructures [90, 35]. These advancements make efficient-BB84 a promising candidate for future quantum-secure communication networks, particularly in scenarios where channel loss and system complexity must be tightly controlled. Among the other various techniques employed in QKD networks, physical link switching has gained particular attention due to the reduced cost of technology introduction and the possibility of iterative scalability. By changing the wavelength or the lightpath of qubits, different implementations allow for more flexibility both in infrastructure design and on-demand performance.

With this work, we present and analyze VenQCI, a production network designed and realized by the Veneto Region, Concessioni Autostradali Venete (CAV) and University of Padova, the first regional quantum network in Italy, and part of the future Italian quantum communication infrastructure. This network was planned and implemented with industrial usage as the final objective, with ease of maintainability and minimal future expansion cost as key points, leveraging efficient BB84 and link switching. We obtained a stable network that, as of the time of writing, is used for the encryption of traffic data, like highway webcam video streams, and is suitable to support other security applications.

6.2 Description of the devices

In this section we will describe the QKD devices and the network orchestration software employed in the present work.

6.2.1 QuKy by ThinkQuantum s.r.l.



FIGURE 6.1: QuKy by ThinkQuantum s.r.l. [114]

QuKy [114] (see figure fig. 6.1) is a ThinkQuantum QKD platform implementing BB84 for secure key distribution. It integrates a QRNG delivering a direct qubit stream, eliminating key expansion and pseudorandomness, thus enabling high key rates with strong security and robustness.

Compatibility and Flexibility QuKy supports multiple network topologies and key-management protocols, operating over both fiber and free-space optical links for broad deployment options.

Interoperability Alice and Bob require no dedicated pairing: a single unit can interoperate with multiple counterparts, enhancing versatility and scalability.

Protocol QuKy implements *efficient*-BB84 with three polarization states and one decoy level [34], matching BB84 security/performance [110] and yielding higher finite-key rates than two-decoy schemes [99]. Transmitter and receiver fit a 2U 19" rack for easy integration. Phase randomization via laser gain switching [63] and a source-device-independent QRNG [18] (QRN2Qubit) are key components of the system: phase correlations degrade SKR in decoy methods [111], while QRNGs avoid PRNG backdoors [33].

Stability QuKy uses the iPOGNAC encoder [19], an all-fiber, self-compensating Sagnac-loop polarization modulator providing calibration-free, low-error, long-term stable operation. A single-phase modulator, asymmetrically placed in the loop, imparts independent CW/CCW phase shifts to synthesize BB84 states on the Poincaré sphere and passively cancel common-mode drifts. Reported experiments show low QBER over hours in the lab and the field. The hardware can be retimed/rebiased to support time-bin generation [103], continuous-variable modulation [101], and intensity modulation [27].

Synchronization *Qubit4Sync* [28] is a qubit-aided clock-recovery algorithm embedding a sparse, known pattern in the quantum stream so the receiver estimates clock phase/frequency from single-photon timestamps via correlation or ML estimators, then tracks drift adaptively. It is protocol-agnostic, fiber/FSO compatible, reduces Raman crosstalk and side-channels by avoiding bright pilots, and has FPGA/SoC real-time implementations. QuKy uses Qubit4Sync to operate over a single communication channel.

6.2.2 Node orchestration and link switching

As QKD evolves into large-scale quantum networks, a central challenge is the orchestration of QKD nodes. This involves coordinated management of quantum and classical resources such as link scheduling [113], key routing, load balancing, and fault tolerance. Efficient orchestration maximizes utilization of quantum channels, reduces key distribution latency, sustains continuous key availability for secure applications [56], and lowers deployment costs by allowing shared use of existing infrastructure thanks to link switching. The task grows in complexity in heterogeneous networks [82], multi-hop paths, and multiple QKD protocols. Because orchestration is critical to network-wide secure key delivery, several standards have been proposed [38, 37, 59, 60]. Most, however, assume a centralized controller, which introduces a potential single point of failure. The QuKy platform addresses this limitation by extending the ETSI QKD GS 015 interface to support quantum link switching. Here, a node agent can control a local optical switch, selecting outbound ports toward neighboring nodes. This allows a single QuKy to be time-multiplexed across multiple QKD links, reducing hardware demands. After initial configuration, key management systems coordinate directly via a proprietary protocol, removing the need for continuous external management. Crucially, in the case that the central SDQKD controller faults, the cooperating QuKys can keep switching between links and maintain the service operational. This removes the concern of a series of attacks where the controller is involved, as countermeasures to ignore the central management can be implemented, making it infeasible to take down the network.

Two switching policies have been developed: key balancing, where the resources dedicated to each link are defined with a set of ratios of buffered key to keep, and coordinated switching, where the devices follow a clock dictated by the number of key blocks generated (that is, every n blocks generated by each active link, the switching procedure boots). The approach allows for future new policies to be added or modified, allowing finer control over the setup. In the case of optical network maintenance on a fiber link instead, the adjacent nodes skip it after a timeout and try to start the next QKD link in the schedule to keep the service running. This allows for hardware maintenance without having to reconfigure or interact with the QKD devices. Moreover, the switching capability greatly reduces the initial cost of introducing the technology on the network, as a new node can be added to the network with just one QKD-capable device and an optical switch, compared to one QKD device per link.

6.3 Methods

6.3.1 Analysis of link performances

The network was released into production in 2025. To assess the continuous service, we gathered operational use data - comprising Raw and Secret Key Rate (RKR, SKR), QBER, and block-time - for a period of two consecutive months spanning from April to June 2025. The block-time is the time required to accumulate a block of data (see below). This gave us a picture of possible long-term trends in the network. We also batched the data hour by hour to highlight possible daily trends.

6.3.2 Description of the network (VenQCI)

The network here analyzed consists of four nodes: VSIX - Padova toll booth - Mestre toll booth - VEGA (see fig. 6.2 on the next page). Despite another fifth node being present, it is currently being used for research purposes and not in an active production environment,

which is the focus of this analysis. Therefore, we will treat the network as a four-node network in the entirety of the exposition. Each is connected with the following:

- VSIX - Padova toll booth (CavPD): ~ 5 km fiber
- Padova toll booth (CavPD) - Mestre toll booth (CavVE): ~ 20 km fiber
- Mestre toll booth (CavVE) - VEGA: ~ 5 km fiber



FIGURE 6.2: The VenQCI network: VSIX – CavPD (Padova toll booth) – CavVE (Mestre toll booth) – VEGA. Aerial view provided by earth.google.com.

The network architecture involves multiple components coordinately operating to enable secure communication, and it's represented schematically in fig. 6.3. At the edge of the system, the end users' switches are responsible for transporting unencrypted VLAN traffic within the secure perimeter domain. These switches provide connectivity between nodes

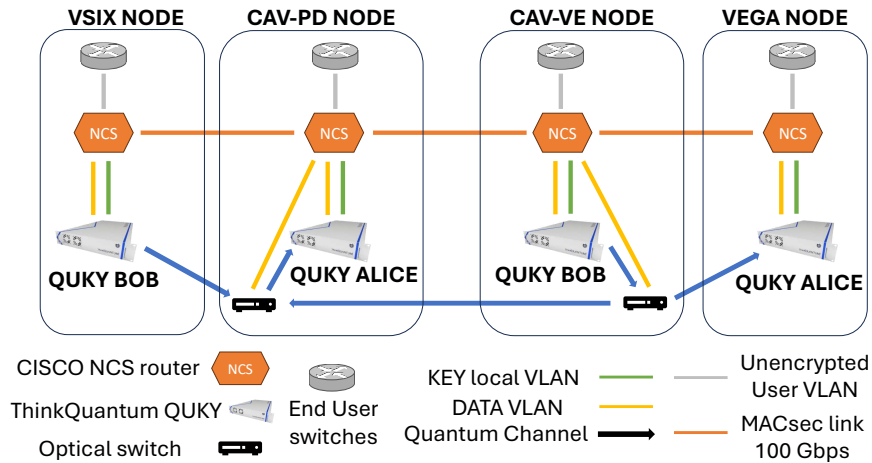


FIGURE 6.3: Scheme of the VenQCI network.

through a *Multi-Protocol Label Switching* [123] (MPLS) network, ensuring high-performance routing capabilities. MPLS is a routing technique that encapsulates packets from various network protocols and defines the paths between the endpoints through which those packets are transported. In the backbone of the network are found the *NCS routers*, manufactured by *CISCO*, that implement the MPLS network over encrypted links. The encryption is provided by *Media Access Control Security* [58] (MACsec), a layer 2

protocol that ensures data confidentiality, integrity, and authenticity. The MACsec encryption keys are derived from symmetric keys distributed via the Quantum Key Distribution (QKD) system. The encrypted MACsec communication is established over a duplex optical link supporting data rates of up to 100 Gbps, utilizing a dedicated single-mode duplex fiber to ensure physical layer security and performance. The QKD infrastructure is implemented using the QuKy platform developed by ThinkQuantum. Within this architecture, the quantum channel—used for the transmission of quantum states—is carried over a dedicated simplex optical fiber. This fiber connects the QKD devices via an optical switch, which is deployed exclusively at intermediate nodes to facilitate dynamic routing of the quantum signal. In parallel, the classical channel required for QKD protocol execution (such as sifting, error correction, and key reconciliation) is implemented via a dedicated VLAN that is transported over the existing MPLS network. Once the QKD process has generated symmetric encryption keys, these keys are delivered to the NCS routers using the SKIP [107] interface. This interface operates over a VLAN that is local to each node, ensuring secure and isolated delivery of data to the encryption devices.

During the booting phase, the MACsec link starts with a pre-shared key until QKD keys are available. Then, MPLS runs over the new established MACsec link and subsequently carries the QKD's CC data. New QKD keys are then generated, and the MACsec link refreshes with a new QKD key of 32B each minute.

6.4 Results

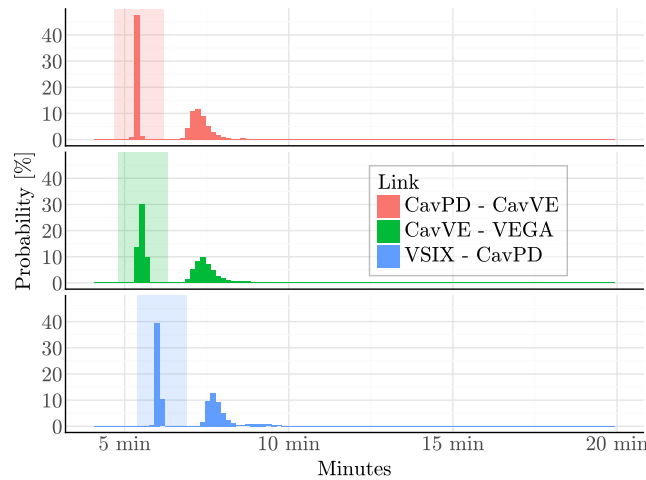


FIGURE 6.4: For each link, probability distribution of the time required to accumulate and process 500 kB of sifted key. In each graph are present two peaks, one on the right corresponding to the first block after the switching (including the initial base alignment time), and one on the left for the following blocks, which skip this phase (inside the colored area).

The QKD post-processing is performed starting from batches of 500 kB of sifted detections, which take, on average, approximately 6 minutes to produce. In fig. 6.4, the distribution of time necessary to complete and process one of these blocks is shown. For each link, two distributions emerge; the one on the right corresponds to the first block created after each switch, while the one on the left, in the highlighted area, corresponds to the following blocks. The former comprises an initial base alignment phase that makes the block take longer with higher variance, while the latter skips this step, leading to more consistent and shorter times. In fig. 6.5 on the following page, we can see the results for both the RKR and SKR, collected

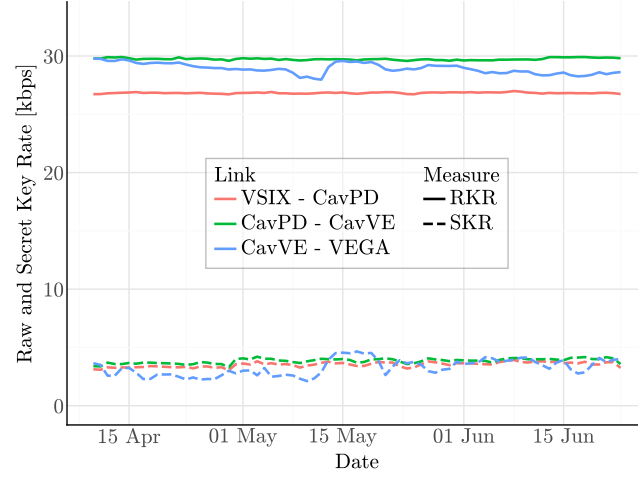


FIGURE 6.5: RKR and SKR of each link distinguished by line type. The line represents the mean taken on a daily basis.

over the two months. The lines represent the daily average computed for each metric. The links connecting CavPD to both VSIX and CavVE seem more stable, whereas the one connecting VEGA to the Mestre toll presents a higher variance both in raw and secret key rate. This, coupled with longer times during data acquisition, points to more significant and less predictable losses that require further investigation in the future. In fig. 6.6 on the next page, we can see the average and the detailed measurements for the QBER, both in the X and Z bases, with the scatter representing the single data points and the line the 3-day average. A zoomed-in visualization of the span of two hours, illustrated in fig. 6.7 on page 82, shows the switching mechanism at work. The paired QKD devices collect measurements until they have enough to create two blocks, after which they coordinate to start the other link as pictured. The figs. 6.8 and 6.9 on page 82 and on page 83 show the box-plot of the data collected grouped by hour, over the months. Here, the middle point of the boxes represents the median data point, the box represents the 25% and the lines the 75% quantiles; meanwhile, dots represent single events where the key rate dropped outside the main trend, because of random fluctuations influenced by the environment. This analysis was done to investigate whether some daily trend would appear, such that it would suggest a correlation between link performance and external factors with daily cycles like highway and railway traffic. Even though there is some fluctuation in the data, we can see how the difference in the median is negligible compared to the interval indicated by the distribution.

After two months, the network has proven to be stable and reliable. VenQCI is well-positioned to sustain future traffic demands due to its robust key generation capacity, currently exceeding 3 kB/s of SKR on all links. Given that a single secure connection like those presented in the introduction consumes just 32 bytes of key material per minute, the network can support a substantial number of simultaneous secure links with bandwidth to spare. This high bit rate not only ensures scalability as the number of users grows, but also provides headroom for more frequent key refresh rates or the integration of additional security services.

The study is limited by the two-month observation window for the full network and by the metropolitan scale of the topology. Future works should extend the monitoring across seasons and maintenance-intensive periods to further quantify resilience, and investigate scalability toward larger, heterogeneous networks with standardized, interoperable orchestration in alignment with emerging ETSI and ITU-T standards. Additionally, in a

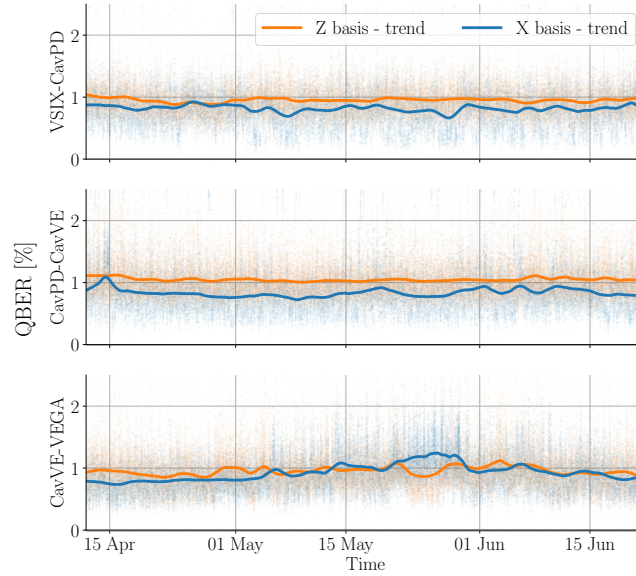


FIGURE 6.6: QBER trend for each 2-node link in a two-month period. Experimental data is represented by a scatter plot, while the average is reported as a line plot.

broader view, adapting to key-demand elasticity will require a new dimensioning of switching schedules, buffering, and post-processing throughput.

This defines a clear path for expansion and increased security in communications within the area. Future plans include the progressive extension of the network and its integration with other segments to form the Italian QCI backbone, enabling a unified, resilient infrastructure at the national scale. The initially reduced cost, made possible by switching, ensures that the project can follow an incremental development model rather than requiring a single, large-scale deployment. Meanwhile, multiple sections of the backbone can be developed in parallel and later connected through the inter-domain interface next to be released as ETSI QKD GS 020. This standard will define a REST-based interface to allow two Key Management Systems (KMS), located in the same trusted node between two network domains, to exchange keys and extend key relay across different implementations and vendors. This staged approach simplifies the process, minimizes upfront investment risks, accelerates time to operational readiness, and allows for adaptation as technological and operational requirements evolve. It would provide a framework for continuous upgrades in performance, security, and interoperability, ensuring the infrastructure remains aligned with broader European quantum communication initiatives. It can also enhance resilience and flexibility by allowing independent domains to collaborate while maintaining their own security policies. This encourages the development of vendor-agnostic deployment of multi-domain QKD networks by permitting standardized, secure key exchange between heterogeneous KMS platforms without requiring end-to-end vendor uniformity.

6.5 Conclusions

We have presented the design, deployment, and operational evaluation of VenQCI, an active four-node quantum key distribution (QKD) network that integrates multiple ThinkQuantum s.r.l. QuKy platforms, which exploit efficient-BB84 one-decoy protocol, iPOGNAC-based polarization encoding, and Qubit4Sync synchronization. The system delivers quantum-derived keys to different infrastructures through ETSI-aligned interfaces and SKIP,

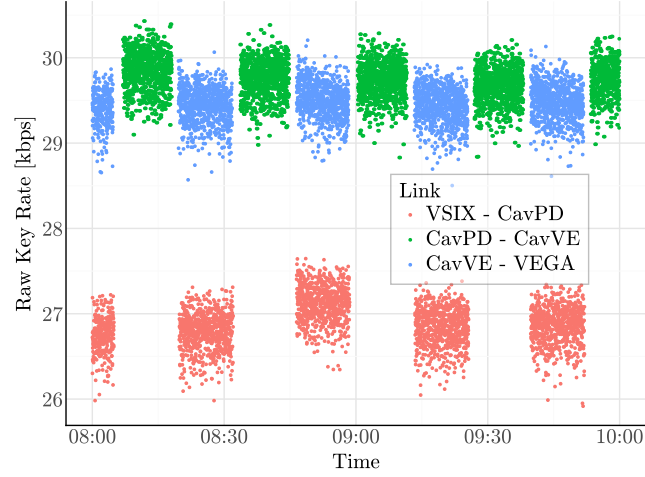


FIGURE 6.7: Plot of the switching mechanism sampled from the long-run. The data represents a period of 2 hours on the 13th of May 2025.

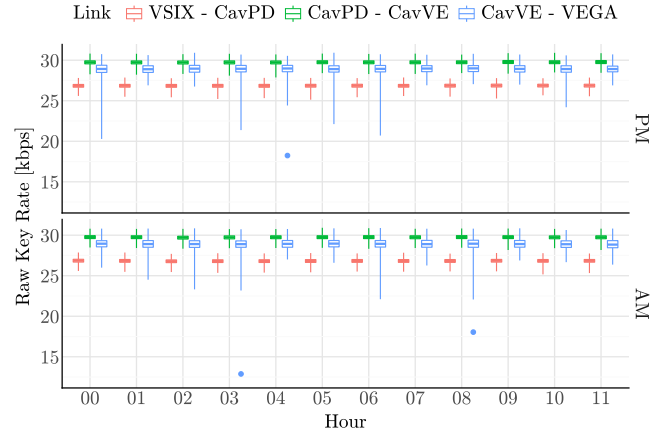


FIGURE 6.8: Raw Key Rate by the hour. Box-plot where the middle point of the boxes represents the median data point, the box represents the 25% and the lines the 75% quantiles, meanwhile dots are outliers.

enabling periodic MACsec re-keying over a 100 Gbps MPLS backbone. Our methodology consisted of a two-month multi-node active operation with dynamic link switching in a metropolitan setting.

The field-test results demonstrate the technical viability and stability of the architecture. The network operation sustained low QBER with elevated raw and secret key generation. Raw-key batches of 500 kB were formed, on average, approximately every six minutes across links, enabling continuous post-processing and stable secret key rates. Analyses by the hour did not reveal statistically significant daily trends, suggesting that environmental dynamics and traffic-induced disturbances on the fibers had a limited impact on key production.

From a networking perspective, we introduced and validated a node-agent-driven quantum link switching mechanism that extends the ETSI QKD GS 015 model. This approach time-multiplexes a single transmitter across multiple neighbors, reducing costs for initial deployment and partially mitigating the risk of a single link sustaining damage. Moreover, coordinated switching preserved service continuity during fiber maintenance without the reconfiguration of QKD endpoints, evidencing practical resilience in operational environments.

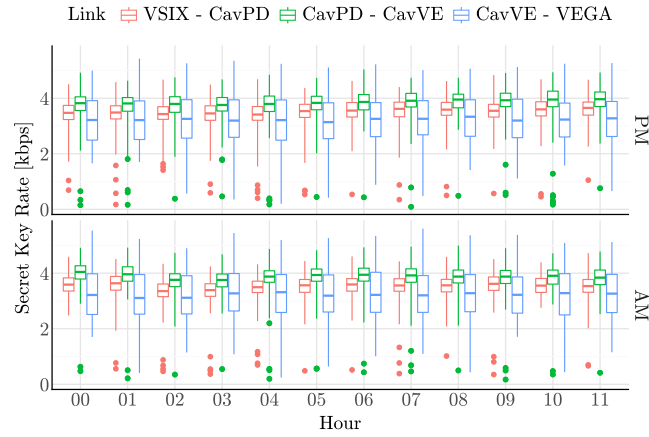


FIGURE 6.9: Secret Key Rate by the hour. Box-plot where the middle point of the boxes represents the median data point, the box represents the 25% and the lines the 75% quantiles, meanwhile dots are outliers.

The system integration across layers was validated end-to-end. QKD-derived keys were consumed for minute-scale 32 B MACsec rekeying, while the MPLS infrastructure dealt with the classical communications once encryption was established. The bootstrapping sequence derived keys as designed, illustrating a promising path for future quantum networks.

In conclusion, the VenQCI network demonstrates that QKD can be operated as a networked utility rather than a point-to-point solution. The system yielded stable secret keys suitable for high-throughput infrastructures. These results provide a practical blueprint for metropolitan-scale quantum-secured services and a foundation for scaling toward larger, interoperable quantum networks.

Chapter 7

Trojan-Horse attack on the iPognac

I have contributed to the project by participating in these work packages: design, development, theoretical model, testing and analysis. Pre-print available at: [116]

7.1 Introduction

Practical security of QKD systems depends critically on the faithful implementation of their underlying quantum protocols. Any deviation or imperfection in components can introduce vulnerabilities that are not covered by theoretical security proofs [32].

One such vulnerability is posed by *Trojan Horse Attacks* (THAs) [44, 62], in which an eavesdropper (Eve) injects bright light into the QKD apparatus, typically at the sender's (Alice's) side, and then analyzes the back-reflected signal to gain information about secret settings, such as basis choices or intensity levels [120, 44, 61]. These attacks exploit the physical layers of the system and, if undetected, can significantly compromise the security of the generated keys without introducing errors that are detectable by Alice and Bob (the receiver) [95].

A growing body of research has focused on both theoretical models of THAs and practical countermeasures, including the use of optical isolators, monitoring detectors, and new security proofs that account for side-channel leakage [75, 102, 44]. Despite these efforts, fully characterizing and mitigating THAs remains an open and crucial challenge in the secure deployment of QKD networks.

In this work, we analyze the practical impact of THAs on the *iPOGNAC*. This analysis is of relevance since many different QKD systems have adopted the *iPOGNAC* since, both for *Discrete-Variable* (DV) QKD, for polarization modulation [16] and time-bin modulation [103], and for *Continuous-Variable* (CV) QKD [101], showcasing the reliability, robustness and effectiveness of the polarization encoder. Other works previously analyzed the impact of THAs on this type of encoder, like [78], but without addressing the possibility of Eve directly exploiting the Sagnac-loop to gain information on the encoded symbol, a scenario in which she can get most of her optical power back.

In this work we perform an analysis of the attack in different regimes: continuous and pulsed laser, high and low mean photon number. We investigate the countermeasures that Alice can adopt in her system to drastically reduce the information leakage at Eve's side, give estimates of the limitations of such defenses and analyze the performances of the different types of THAs in those conditions.

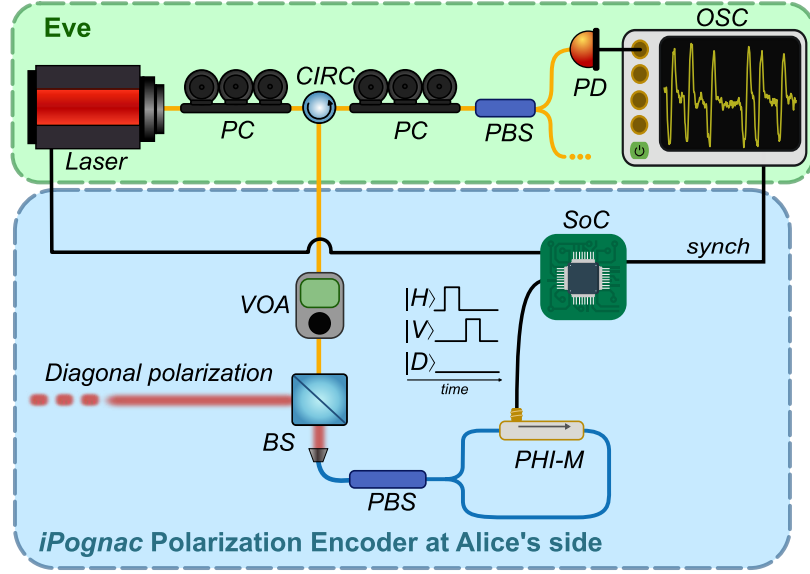


FIGURE 7.1: Scheme of the setup for the THA on the *iPOGNAC*. SM-Fibers in yellow, PM-Fibers in blue, electrical connections in black. The optical power entering inside Alice's setup is indicated as μ_{in} , while the one coming out (subject to the attenuations of the Alice's system and therefore smaller than μ_{in}) is indicated as μ_{out} .

7.2 Methods

Naïve implementation of Sagnac-loop based modulation schemes can be problematic since a significant portion of injected light through a THA can return to the eavesdropper containing an information leakage that can undermine the security of the implemented quantum communication protocol. In fact, the light injected by the eavesdropper traverses the same modulation loop Alice uses to encode her information, meaning that it potentially experiences the same modulation and carries the same information as the QKD signal, allowing the eavesdropper to gain knowledge on the forthcoming symbol.

To analyze the performances of the THA on the iPOGNAC, we divided our work into three stages: an attack in strong-light regime, which comprises a continuous-wave laser attack (CWLA) and a pulsed laser attack (PLA) (both of them make use of photo-diodes as light detectors), a pulsed laser attack in weak-light regime exploiting Geiger-mode detectors such as *Superconducting-Nanowire Single Photon Detectors* (SNSPDs) and an evaluation/analysis on the countermeasures that Alice can take to counteract these attacks. The reasons we chose to study these cases is because high-power attacks are simpler and cheaper to implement, whereas single-photon-level attacks allow for a wider range of countermeasure levels. In the meantime, pulsed attacks permit to concentrate more photons in a single time-span, while CW attacks require less stringent synchronization (more on the motivations for each attack in section 7.6). The stages are reported in the following sections, after a brief description of the setup.

7.2.1 Description of the system

The iPOGNAC polarization encoder is a device designed for stable, low-error, and calibration-free polarization modulation, particularly suited for QKD and quantum communications. Its core innovation lies in its use of a Sagnac interferometer loop, which

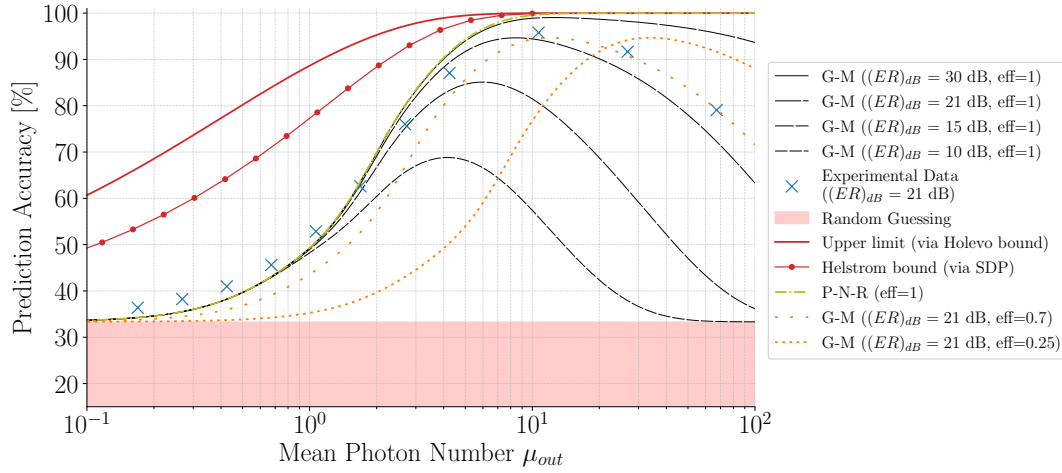


FIGURE 7.2: Theoretical prediction accuracy with respect to the mean photon number μ_{out} , varying different POVMs, extinction ratios of the projective measurements, efficiencies, and experimental data for comparison.

inherently compensates for environmental disturbances such as temperature fluctuations and phase drifts, ensuring long-term operational stability.

Its working principle begins with linearly polarized optical pulses injected into the iPOGNAC. A half-wave plate rotates the polarization to a diagonal state, after which a beam splitter separates the input and output streams. The transmitted light is coupled into a polarization-maintaining fiber (PMF). The light then enters a fiber-based polarization beam splitter (PBS), which initiates the Sagnac loop. Here, the two orthogonal polarization components (horizontal and vertical) travel in opposite directions — clockwise (CW) and counter-clockwise (CCW) — along the slow axis of the PMF. Each component passes through a phase modulator at different times, allowing independent phase control. By applying specific phase shifts to the CW and CCW pulses, the iPOGNAC can generate all the polarization states required for the BB84 QKD protocol, including diagonal, anti-diagonal, and circular polarizations. Experimental results have demonstrated the iPOGNAC's ability to maintain a low QBER over extended periods, both in laboratory and field-trial settings. The device's versatility is further highlighted by its ability to be reconfigured for tasks such as time-bin encoding [103], continuous variable modulation [101] and intensity modulation [27], supporting the development of robust and flexible quantum networks [17, 11].

Regarding the attack, at Eve's side, a 1560 nm laser shines through a *Polarization Controller* (PC) that controls the polarization in input at Alice's side. The light that comes back from Alice's system is redirected using a *Circulator* (CIRC) to another PC and a *Polarizing Beam Splitter* (PBS) that allows the projective measurement on a *Si-Photodiode* (PD) or on the SNSPDs. The output of the PD is displayed using an *Oscilloscope* (OSC), which is also used to store the data to analyze. Alice's setup is composed of a *Variable Optical Attenuator* (VOA) to counteract the THA, and the asymmetric-iPOGNAC, namely a *Beam Splitter* (BS) connected to Alice source on one side to a Sagnac-loop composed of a PBS and a *Phase Modulator* (PHI-M) on the other side. Alice source emits diagonal polarized photons that enter the BS from the left side. For simplification purposes, the whole system (Alice+Eve) is controlled through the same *System-On-A-Chip* (SoC), a *Field-Programmable-Gate-Array* (FPGA) that allows to generate electrical pulses and synchronize everything to the same clock-rate [84]: this holds on the generalized assumption that Eve has access to the system of Alice to exploit the same synchronization signals she uses, or that she can use clock-recovery algorithms to extract the information on the synchronization. The setup of

the experiment is depicted in its entirety in Fig. 7.1. The modulation signals employed work by introducing a delay between the $|H\rangle$ and $|V\rangle$ symbols on the FPGA side: in this sense the Sagnac loop enables to encode the polarization states on the optical signal by fine-tuning this delay (see Fig. 7.4). We care to point out that since Alice is using an attenuator as countermeasure, the light of the THA coming out from her system will experience two times the attenuation set on the VOA. In our setup, the total attenuation experienced by the light coming out from the system Att_{tot} can be described by this equation:

$$(\text{Att}_{tot})_{\text{dB}} = 2(\text{Att}_{VOA} + \Delta A) + 6 + E \quad (7.1)$$

where Att_{VOA} is the attenuation manually set on the VOA (the term we mostly refer to in this work when talking about countermeasures), ΔA is an inefficiency term given by the characterization of the VOA (in our case is 4 dB), 6 dB is the attenuation given by the double crossing of the 50:50 beam splitter, and E are extra losses from coupling inefficiencies, defective components, and so on, in our case corresponding to ~ 1 dB.

7.3 Theoretical Model

This section is dedicated to the calculation of the guessing probability in function of the output mean photon-number μ_{out} . We will cover three cases: using an optimal POVM for the measurement, which gives an upper-bound on the maximum information that can be extracted from the system, while using a fixed POVM, photon-number resolving detectors in the second case and Geiger-mode photodetectors in the third case. All of them are reported in the following sections. Despite the theoretical model being valid both for weak and strong light regimes, the main limitations of the latter mostly come from the limited performances of the devices in use, like the noise floor of the detectors or the oscilloscopes (see sec. 7.4.3 and 7.6).

Optimal POVM

When implementing a THA, Eve will manage to obtain a state that depends on the symbol modulated by Alice. With no lack of generality, we therefore assume that the states that Eve will receive are

$$\begin{aligned} |\psi_1\rangle &= |\sqrt{\mu}\rangle_H \otimes |0\rangle_V && \text{if Alice sends } |H\rangle, \\ |\psi_2\rangle &= |0\rangle_H \otimes |\sqrt{\mu}\rangle_V && \text{if Alice sends } |V\rangle, \\ |\psi_3\rangle &= |\sqrt{\frac{\mu}{2}}\rangle_H \otimes |\sqrt{\frac{\mu}{2}}\rangle_V && \text{if Alice sends } |D\rangle. \end{aligned} \quad (7.2)$$

Optimizing on the POVM F_e employed by Eve, it's possible to extract an upper bound on the quantity of information that is accessible and can be extracted from the system, the so-called *accessible information*:

$$I_{\text{acc}}(A : E) = \max_{\{F_e\}} \sum_{a,e} p(a,e) \log_2 \frac{p(a,e)}{p(a)p(e)} \quad (7.3)$$

with $p(e|a) = \text{Tr}[F_e \rho_a]$ and ρ_a is the density matrix of the received state $|\psi_a\rangle$. Instead, the average probability of correctly guessing a symbol p_g , in this scenario, is given by:

$$p_g = \sum_a p(a) p(e = a|a) \quad (7.4)$$

Assuming the system is symmetric, namely $p(a) = 1/3$, $p(e = a|a)$ and $p(e \neq a|a)$ do not depend on a , then $p(e) = 1/3$ and:

$$p_g^* = \text{Tr}[F_a^* \rho_a] \quad \forall a \quad (7.5)$$

where F_a^* is the optimal POVM. Therefore the accessible information can be related to the guessing probability by:

$$I_{\text{acc}}(A : E) = p_g \log_2(3p_g) + (1 - p_g) \log_2 \frac{3(1 - p_g)}{2} \quad (7.6)$$

While the maximization in (7.3) is in general hard to solve because there is not an explicit closed form for the optimal POVM, the mutual information can be upper-bounded by the so called Holevo bound [126], which expresses the amount of classical information that can be extracted from a quantum system, obtained as a mixture $\rho = \sum_a p_a \rho_a$:

$$\begin{aligned} I_{\text{acc}}(A : E) &\leq \chi(\rho) = S(\rho) - \sum_a p_a S(\rho_a) \\ &= S(\rho) \end{aligned} \quad (7.7)$$

The last equality follows from the fact the state ρ is given by $\rho = \frac{1}{3} \sum_{a=1}^3 |\psi_a\rangle\langle\psi_a|$ and the Von Neumann entropy of a pure state is vanishing (i.e.: $S(|\psi_a\rangle\langle\psi_a|) = 0$). Then, it follows that eq. (7.3) is upper bounded by $S(\rho)$.

Solving this equation can yield an upper bound for the p_g . As a first step we therefore have to calculate $S(\rho)$, that is equal to the Shannon Entropy of the eigenvalues λ_i of the matrix given by $\rho_{ij} = \frac{1}{3} \langle \psi_i | \psi_j \rangle$ (see appendix A):

$$S(\rho) = H(\mu) := - \sum_{i=1}^3 \lambda_i(\mu) \log_2(\lambda_i(\mu)) \quad (7.8)$$

By using eq. (7.7), an upper bound on the guessing probability p_g can be extracted in function of μ by the implicit relation:

$$I_{\text{acc}}(A : E) \leq H(\mu) \quad (7.9)$$

which gives the results reported in fig. 7.2 as a red line.

The results just found depict a loose upper bound on the actual, tighter, quantum limit for the distinguishability of a set of states, which is given by the Helstrom bound [50, 126] (originally defined for bi-partite systems), which quantifies the maximum probability p_g^* of identifying the correct state. To compute this limit for the states identified by the density matrices $\{\rho_i\}$, it is possible to express the primal-form optimization problem:

$$\begin{aligned} p_g^* &= \frac{1}{3} \max_{F_a} \sum_a \text{Tr}[F_a^* \rho_a] \\ F_a &\succeq 0 \quad \forall a \quad \text{and} \quad \sum_a F_a = \mathbb{I} \end{aligned} \quad (7.10)$$

This semi-definite program (SDP) is strictly feasible [112] (for instance, the trivial measurement $F_a = \mathbb{I}/3$ satisfies the constraints) which means that the Slater condition for convex optimization is satisfied [23], granting that Strong Duality holds and we can write this as a dual-problem SDP [14]. This method allows us to optimize over all generalized

quantum measurements to find the optimal strategy by finding a Hermitian operator K that solves the following minimization problem (in general computationally simpler to solve):

$$p_g = \min_K \left\{ \text{Tr}(K) \mid K \succeq p_i \rho_i, \quad \forall i \right\} \quad (7.11)$$

where $p_i = \frac{1}{3}$ in our case.

The solution to this program allows to relax the bound on μ with which an eavesdropper can get useful information on the system, and is reported in Fig. 7.2 as a red line with dots.

Fixed POVM

For this attack, we wanted to minimize the amount of detectors whilst still being able to distinguish the symbols, which corresponds to a minimum of two channels, as seen from the truth-table of the detections reported in Table 7.1:

input	detector	CH_1	CH_2
$ H\rangle$		click	no-click
$ V\rangle$		no-click	click
$ D\rangle$		click	click

TABLE 7.1: Truth-table of the detections (clicks) of the symbols in a Geiger-mode detector using two channels.

Based on the table, we can already predict that the minimum amount of photons per symbol required to distinguish all the three symbols is two (therefore the two channels, to be able to distinguish $|D\rangle$). Knowing the probability of a channel to *not click* is described by a

Poissonian distribution $\left(\mathcal{P}_\mu(0) = \frac{\mu^0}{0!} e^{-\mu} = e^{-\mu} \right)$, we can describe the guessing probabilities for each symbol in the following way:

$$\begin{aligned} P(|H\rangle_{out} \mid |H\rangle_{in}) &= P(CH_1 \cap \overline{CH_2}) \\ &\stackrel{i.i.d.}{=} P(CH_1) \cdot P(\overline{CH_2}) \\ &= (1 - e^{-\mu_H \eta}) \cdot e^{-\mu_H \eta \cdot ER} \end{aligned} \quad (7.12)$$

and similarly for $|V\rangle$ and $|D\rangle$:

$$P(|V\rangle_{out} \mid |V\rangle_{in}) = e^{-\mu_V \eta \cdot ER} \cdot (1 - e^{-\mu_V \eta}) \quad (7.13)$$

$$P(|D\rangle_{out} \mid |D\rangle_{in}) = (1 - e^{-\mu_D \eta})^2$$

where η is the efficiency of the detectors and μ_H , μ_V and μ_D are, respectively, the mean photon numbers when sending $|H\rangle$ and projecting the measurement on CH_1 , sending $|V\rangle$ and projecting on CH_2 , and sending $|D\rangle$ - projecting detector should be irrelevant.

Assuming the detectors are equally balanced, i.e. $\mu = \mu_H = \mu_V = 2\mu_D$, and the efficiency is maximum, i.e. $\eta = 1$, the equations can be written as:

$$\begin{aligned}
P(|H\rangle_{out} | |H\rangle_{in}) &= P(|V\rangle_{out} | |V\rangle_{in}) \\
&= (1 - e^{-\mu}) \cdot e^{-\mu \cdot ER}
\end{aligned} \tag{7.14}$$

$$P(|D\rangle_{out} | |D\rangle_{in}) = (1 - e^{-\mu/2})^2$$

Summing the three cases, we obtain the total detection probability we can expect from a certain extinction ratio (i.e.: prediction accuracy). The dependency of the prediction accuracy from mean photon number μ and extinction ratio ER (defined in linear scale as the ratio of $|\alpha|^2$ and $|\beta|^2$ in $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$, and $ER = 10^{-(ER)_{dB}/10}$) can be graphically visualized in Fig. 7.3 and Fig. 7.2.

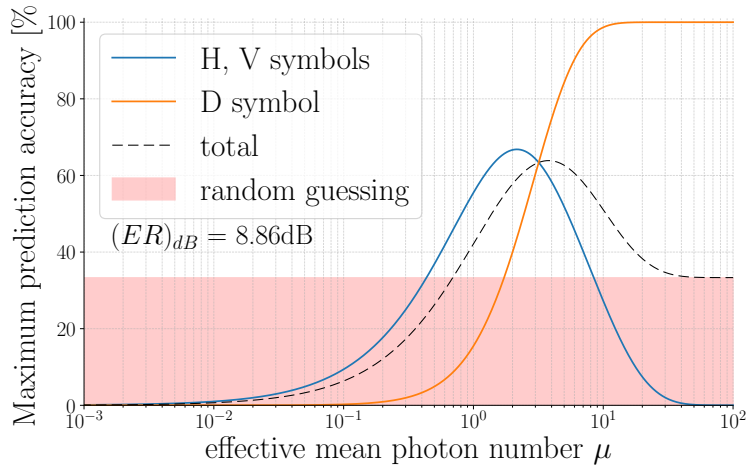


FIGURE 7.3: Theoretical detection probabilities for each state and the total with respect to the mean photon number μ_{out} in the use-case of only two detectors (Extinction Ratio = 8.86 dB).

Let's suppose Eve is in possession of a perfect photon-number-resolving detector with optimal detection efficiency. We can model Eve's approach by describing the back-reflected photons as coherent states of the form:

$$|\Psi_E\rangle = \frac{1}{\sqrt{2}}(|\mu_{out}^H\rangle + e^{i\varphi}|\mu_{out}^V\rangle) \tag{7.15}$$

Where μ_{out} is the mean photon number coming back from Alice's system and φ holds the information on the encoding state given by the phase modulator. At $\mu_{out} = 0$ Eve is forced to randomly guess the symbol, therefore her $P_{guess}^E(0) = 1/3$. Already from $\mu_{out} = 1$, it can be seen that for Eve is more convenient to use two channels for detection, because her $P_{guess}^E(1) = 2/3$, given that if she detects a photon on $|H\rangle$ or $|V\rangle$ her best strategy is to keep the received state, as she will guess correctly two times out of three. Even though she knows that the state she received could also be a $|D\rangle$ state, a random guess between these two symbols will yield a $P_{guess}^E = \frac{1}{2} < \frac{2}{3}$. Intuitively, increasing the number of detectors will just cause an increase in the uncertainty. For $\mu_{out} \geq 2$, we fall into the case described later in Table 7.1, therefore her $P_{guess}^E(\geq 2)$ will depend on the detection probabilities for each channel, namely $\frac{1}{3} (\Pr(H|H) + \Pr(V|V) + \Pr(D|D))$. In tab. 7.2 we listed the detection probabilities $\Pr(\text{Eve}|\text{Alice})$ both for Photon-Number-Resolving and imperfect Geiger-Mode photodetectors, noting as $c(\nu) = (1 - e^{-\nu})$ and $\bar{c}(\nu) = e^{-\nu}$ the functions, respectively,

indicating the probability for a detector to click and not-click. Given the aforementioned

Probability	G-M	P-N-R
$\Pr(H H)$	$c(\mu_{out}) \cdot \bar{c}(\mu_{out}ER)$	$c(\mu_{out})$
$\Pr(V H)$	$c(\mu_{out}ER) \cdot \bar{c}(\mu_{out})$	0
$\Pr(D H)$	$c(\mu_{out}) \cdot c(\mu_{out}ER)$	0
$\Pr(\text{vac} H)$	$\bar{c}(\mu_{out}) \cdot \bar{c}(\mu_{out}ER)$	$\bar{c}(\mu_{out})$
$\Pr(H V)$	$= \Pr(V H)$	0
$\Pr(V V)$	$= \Pr(H H)$	$c(\mu_{out})$
$\Pr(D V)$	$= \Pr(D H)$	0
$\Pr(\text{vac} V)$	$= \Pr(\text{vac} H)$	$\bar{c}(\mu_{out})$
$\Pr(H D)$	$c(\mu_{out}/2) \cdot \bar{c}(\mu_{out}/2)$	$c(\mu_{out}/2) \cdot \bar{c}(\mu_{out}/2)$
$\Pr(V D)$	$= \Pr(H D)$	$= \Pr(H D)$
$\Pr(D D)$	$c(\mu_{out}/2) \cdot c(\mu_{out}/2)$	$c(\mu_{out}/2) \cdot c(\mu_{out}/2)$
$\Pr(\text{vac} D)$	$\bar{c}(\mu_{out}/2) \cdot \bar{c}(\mu_{out}/2)$	$\bar{c}(\mu_{out}/2) \cdot \bar{c}(\mu_{out}/2)$

TABLE 7.2: Detection probabilities for each (Eve|Alice) case using Geiger-Mode (G-M) and Photon-Number-Resolving (P-N-R) photodetectors. We considered a more realistic scenario for G-M detectors, introducing also a sub-optimal extinction ratio (ER , in linear scale) coming from the projecting device at Eve's side. We identified as "vac" the vacuum state, where no detector clicks.

probabilities that Eve correctly guesses a symbol at a certain μ_{out} , we can derive the calculation of the total $P_{\text{guess}}^E(\mu_{out})$ as follows:

$$\begin{aligned}
P_{\text{guess}}^E(\mu_{out}) &= \\
&= \frac{1}{3} \Pr(\langle 0|\mu_{out} \rangle) + \frac{2}{3} \Pr(\langle 1|\mu_{out} \rangle) + \\
&\quad + P_{\text{guess}}^E(\geq 2) \cdot (1 - \Pr(\langle 0|\mu_{out} \rangle) - \Pr(\langle 1|\mu_{out} \rangle)) \\
&= \frac{1}{3} e^{-\mu_{out}(\mu_{out}+1)} \left[\mu_{out}^2 + \right. \\
&\quad + e^{\mu_{out}^2} \left(-2e^{\mu_{out}/2} + 3e^{\mu_{out}} - 1 \right) + \\
&\quad \left. + 2e^{\mu_{out}/2}(\mu_{out}^2 + 1) - e^{\mu_{out}}(\mu_{out}^2 + 2) + 1 \right]
\end{aligned} \tag{7.16}$$

We define the mutual information $I(A : E)$ as follows:

$$\begin{aligned}
I(A : E) &= \sum_{a,e} p(a,e) \log_2 \frac{p(a,e)}{p(a)p(e)} \\
&= \sum_{a,e} p(e|a)p(a) \log_2 \frac{p(e|a)}{p(e)} \\
&= \frac{1}{3} \sum_{a,e} p(e|a) \log \frac{p(e|a)}{p(e)}
\end{aligned} \tag{7.17}$$

being $p(a) = \frac{1}{3}$ since each state ($|H\rangle$, $|V\rangle$, $|D\rangle$) is chosen by Alice with equal probability, while the $p(e|a)$ are given in table 7.2. On the other hand, $p(e)$ can be written case by case,

fixing e , as:

$$\begin{aligned}
 p(e) &= \sum_a p(e|a)p(a) = \\
 &= \begin{cases} \frac{1}{3}(\Pr(H|H) + \Pr(H|V) + \Pr(H|D)) & e = |H\rangle \\ \frac{1}{3}(\Pr(V|H) + \Pr(V|V) + \Pr(V|D)) & e = |V\rangle \\ \frac{1}{3}(\Pr(D|H) + \Pr(D|V) + \Pr(D|D)) & e = |D\rangle \\ \frac{1}{3}(\Pr(\text{vac}|H) + \Pr(\text{vac}|V) + \Pr(\text{vac}|D)) & e = |\text{vac}\rangle \end{cases} \quad (7.18)
 \end{aligned}$$

Intuitively, the mutual information must be upper-bounded by the Holevo bound, which expresses the amount of classical information contained in a quantum system:

$$I(E : A) = \chi(\rho) = S(\rho) \leq \log_2 3 \quad (7.19)$$

Where $\rho = \frac{1}{3}(|\alpha_H\rangle\langle\alpha_H| + |\alpha_V\rangle\langle\alpha_V| + |\alpha_D\rangle\langle\alpha_D|)$. The resulting guessing probability P_{guess}^E is displayed for the ideal photon-number-resolving detector with optimal extinction ratio as a green dot-dashed line, and for the Geiger-mode detector with different detection efficiencies and extinction ratios, in Fig. 7.2.

7.4 Strong light regime

The attack in strong light regime has been performed employing commercially-available photo-diodes. These not only have bandwidths that allow for a full resolution of the spectral response, but can also estimate proportionally the quantity of incoming light, admitting a wide range of attacks, contrarily from the weak light regime where Geiger-mode-type photo-detectors must be employed, limiting the possibilities. We acknowledge the fact that the methods hereby presented are sub-optimal, and don't use all the information available from the total shape of the outputs. Machine-Learning classifiers can be adopted to improve the results. For the scope of this work, more centered on the countermeasures to these types of attacks, we will leave the introduction of Machine-Learning methods as a task for future works.

7.4.1 CW laser attack

For the hacking in continuous regime, we made sure to fine-tune the first PC to enter Alice's setup with the $|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ state. The second, analogously, serves to project the $|D\rangle$ state on the $|H\rangle$ and $|V\rangle$ state by means of the PBS and measure them with the photodiode. The resulting waveform should be equally split above and below the average, as it is visible on the screen of the oscilloscope reported in Fig. 7.5.

By taking that same plot and performing a "modulo-period" operation (in this case the period being 20 ns, since the repetition rate is 50 MHz), we obtain a superposition of the $|H\rangle$ and $|V\rangle$ symbols in the exact location in time where the symbols are (in the timespan of one period) in the original waveform. We perform a 2D-histogram of these data, as for higher attenuations the shapes of the waveform get lost in the noise, obtaining a waveform characterized by the previously-mentioned down-up behavior, like the one depicted in Fig. 7.4. From there we can easily estimate the location of the first symbol in the sequence, which automatically gives us all the following symbol locations by simply increasingly adding the period (20 ns).

After estimating all symbol locations, each symbol is classified as $|H\rangle$, $|V\rangle$, or $|D\rangle$ using thresholds, as shown in Fig. 7.5. The thresholds are chosen modeling the arrival of the

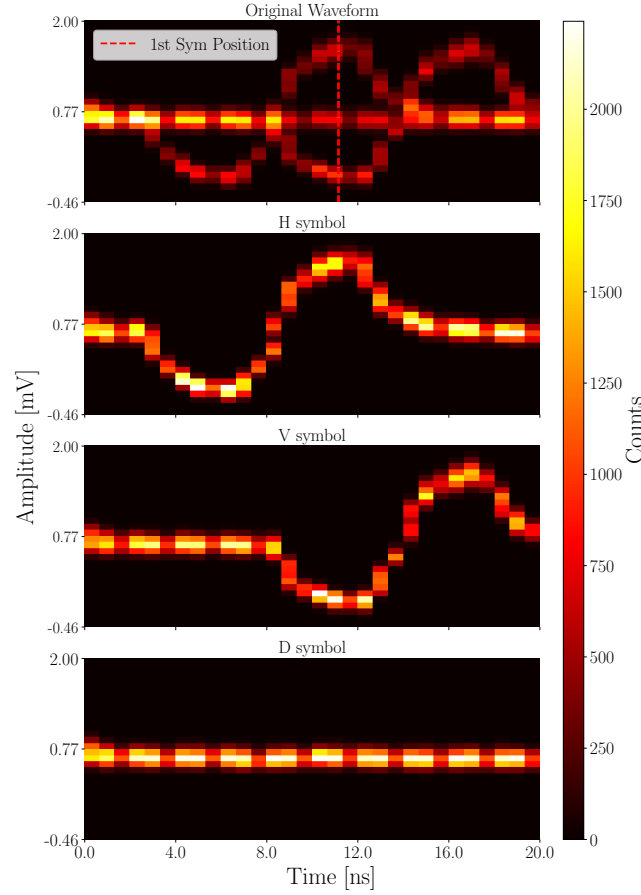


FIGURE 7.4: 2D-histogram of the waveform resulting from the oscilloscope, result of the optical modulation in continuous wavefront by the *iPOGNAC* during the THA, and $|H\rangle$, $|V\rangle$ and $|D\rangle$ symbols separately. All the waveforms presented are calculated by performing a modulo-period operation. In the top plot, the red vertical line shows the detected position of the first symbol in the original waveform.

heights of the symbols as Gaussian distributions with certain mean ν and variance σ^2 and using the *Bayes decision rule for minimum error*, which guarantees the lowest possible probability of error under known distributions and priors [41] and yields that the optimal threshold t^* minimizing the total error is:

$$t^* = \arg \min_t E(t)$$

where $E(t)$ is the error function. In this sense, the best threshold happens to be found in the intersection point between the two Normal distributions, because that's where the likelihood of observing the value x is the same for both the PDFs. In our scenario, the distributions of the $|H\rangle$, $|V\rangle$ and $|D\rangle$ symbols have very similar variances $\sigma_1^2 \simeq \sigma_2^2 = \sigma^2$. Therefore, the optimal threshold t^* can be obtained as the middle point of their averages ν_i :

$$\frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(t^* - \nu_1)^2}{2\sigma^2}\right) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(t^* - \nu_2)^2}{2\sigma^2}\right)$$

Therefore $t^* = \frac{\nu_1 + \nu_2}{2}$.

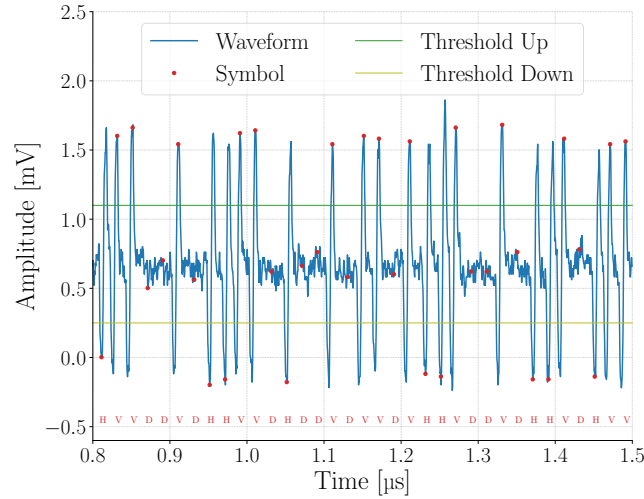


FIGURE 7.5: Waveform with calculated symbol positions and classified symbols for the CWLA. Red dots show the estimated symbol locations, while thresholds are used to classify the symbol as $|H\rangle$, $|V\rangle$, or $|D\rangle$ (if the symbol location is above the threshold up, the symbol is classified as $|V\rangle$, if it is between the thresholds up and down, it is classified as $|D\rangle$, and if it is below the threshold down, it is classified as $|H\rangle$).

7.4.2 Pulsed laser attack

For hacking in pulsed regime, following a method similar to that used in the previous section, a “modulo-period” operation is applied to the waveform, resulting in a superposition of the $|H\rangle$, $|V\rangle$ and $|D\rangle$ symbols, as illustrated in Fig. 7.6 (inside the pulse the three heights are visible, $|V\rangle$ at 0%, $|D\rangle$ at 50% and $|H\rangle$ at 100%). Once the position of the first symbol is estimated by locating the maximum, all symbol positions are determined by iteratively adding the period.

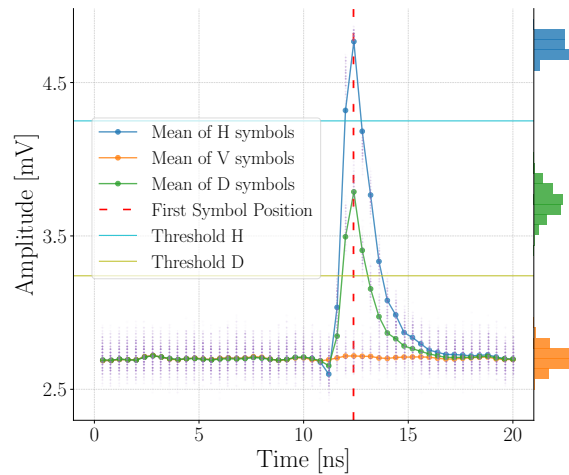


FIGURE 7.6: Mean of $|H\rangle$, $|V\rangle$, and $|D\rangle$ symbols in time modulo period, result of the optical modulation in pulsed regime by the *iPOGNAC* during the THA. Data points are reported in purple. Red vertical line shows the detected position of the first symbol in the original waveform. Statistical distributions of these symbols are displayed on the right.

As shown in Fig. 7.7, each symbol can be classified as $|H\rangle$, $|V\rangle$ or $|D\rangle$ using thresholds,

after all the symbol locations have been determined. Thresholds are chosen using Gaussian distributions of the symbols and Bayes decision rule for minimum error, mentioned in the previous section.

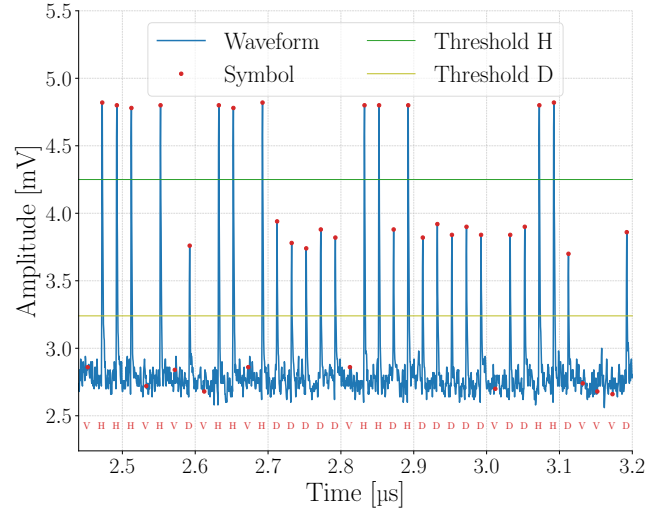


FIGURE 7.7: Waveform with calculated symbol positions and classified symbols for the pulsed laser attack. Red dots show estimated symbol locations, thresholds are used to classify the symbol as $|H\rangle$, $|V\rangle$, or $|D\rangle$ (if the symbol is above the threshold H, the symbol is classified as $|H\rangle$, between the thresholds H and D, it is classified as $|D\rangle$, otherwise it is classified as $|V\rangle$).

7.4.3 Results for the Strong Light Regime

The result of optimal prediction accuracy for continuous and pulsed laser attacks is shown in Fig. 7.8:

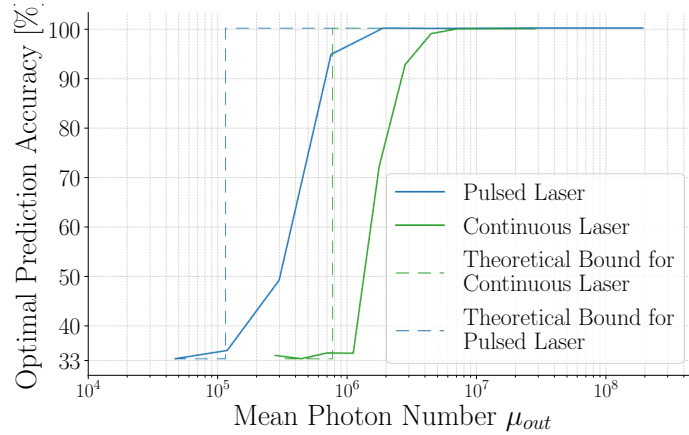


FIGURE 7.8: Results on optimal prediction accuracy based on the mean photon number μ_{out} for the continuous and pulsed laser attack.

For the CW laser, we observed that the sequence can be constructed from the theoretical bound of $\mu_{out} \sim 10^7$, which corresponds up to 8 dBs of attenuation.

From the setup scheme shown in the Fig. 7.1, the laser shines from Eve's side passes through the VOA twice. Consequently, the effective attenuation on Eve's laser is doubled.

Notably, for this test we used an EDFA to increase the optical signal power in the case of the pulsed laser attack, which led to a noticeably higher average power of 60 mW. When compared to the CW case, this amplification allows for a gain of roughly ~ 16.5 dB in the pulsed scenario, which increases Eve's capacity to compromise the transmission.

The mean photon number variation based on the attenuation set on the VOA is shown in Fig. 7.9.

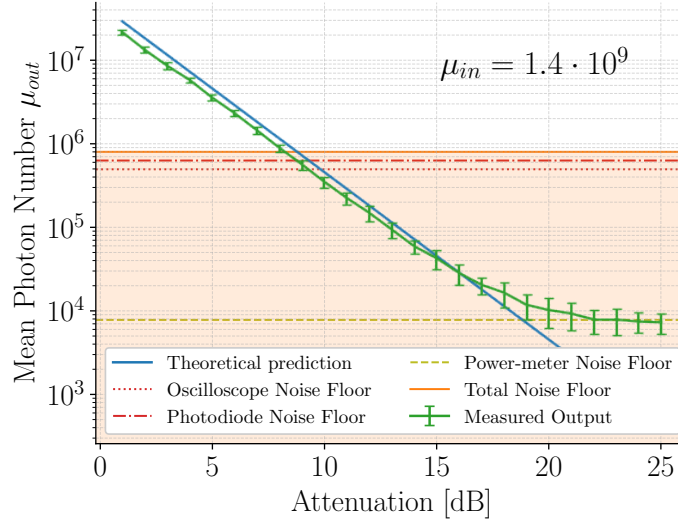


FIGURE 7.9: Mean photon number μ_{out} at different attenuations set on the VOA. Noise floors thresholds are indicated with horizontal lines. The plateau after 15 dB is due to the noise floor of the power-meter we used to characterized the output power (50 nW).

The theoretical output is calculated on the basis of the losses that occur in our setup. The total noise floor is calculated by the *Root Sum Square* (RSS) of the oscilloscope and photodiode standard deviations, namely σ_{osc} and σ_{pd} as follows:

$$\sigma_{total} = \sqrt{\sigma_{osc}^2 + \sigma_{pd}^2} \approx 5 \mu W \quad (7.20)$$

As seen in Fig. 7.9, around 8 dBs, the output power of the CW laser is below the total noise floor, implying that the sequence cannot be predicted after this bound, consistent with the theoretical bound for the continuous laser shown in Fig. 7.8.

7.5 Weak light regime

In Geiger-mode photodetectors like SNSPDs, the duration of time required for the current to fully return to the nanowire or for the voltage to drop to the baseline noise level is known as the detector's dead (reset) time [15]. The detectors we used have a dead time T_{dead} of ~ 20 ns, therefore the maximum achievable repetition rate f_{max} for the pulsed signal can be:

$$f_{max} \approx \frac{1}{T_{dead}} \approx 50 \text{ MHz} \quad (7.21)$$

Given that during the period of dead time the detectors are unable to detect the incoming photons, there is a strong upper bound on the maximum achievable repetition rate, that is not

only given by Eq. 7.21, but also by the saturation of the SPDs. In fact, a repetition rate of 50 MHz would yield meaningful results (i.e.: at least two photons per pulse) only in a situation of maximum saturation of the single channels of the SNSPDs. Since this could lead to irreparable damages to the equipment, we opted to lower the repetition rate to 1 MHz to account for the dead time of the SNSPDs and lower the expected counts.

An alternative to counteract this problem is to exploit multiple channels of the SNSPDs and a $1 \times N$ beam splitter per PBS output. This could lead to an increase in the count rate, at the cost of increasing the number of channels used and at a required temporal alignment at the beginning, hypothetically doubling the maximum frequency with N . Since our analysis wants to tackle the issue with the less components as possible, we won't delve into this possibility, leaving it for future analyses.

7.5.1 Results for the Weak Light Regime

Regarding the THA using SNSPDs as detectors, we measured the extinction ratio $(ER)_{dB}$ of the PBS at our disposal (measuring ~ 21 dB), and predicted the sequence for different levels of attenuation. In Fig. 7.2, not only the experimental results are visible, but also how different ER s highly influence the trend of the theoretical prediction accuracy curve in variation of μ . Our results show that a maximum of $\sim 95\%$ prediction accuracy was achieved in near-perfect conditions of μ .

All these tests were performed in normal conditions of average power to give an estimate of the prediction accuracies. Potentially, real-world attackers can increase the power of their laser up to the maximum possible ratings of the components at their disposal (e.g.: the maximum power a fiber can handle, which normally is around 10 W for continuous regime and 1 MW for pulsed regime [91, 108]). For this purpose, we normalized the average powers of the results to a higher value to show the attenuation levels that are required by Alice to cope with such intensities. The results are collected and shown in Fig. 7.10, where it shows that an attenuation of ~ 60 dB involved in a THA won't lend meaningful results to Eve, even when the eavesdropper is employing single-photon detectors in their setup.

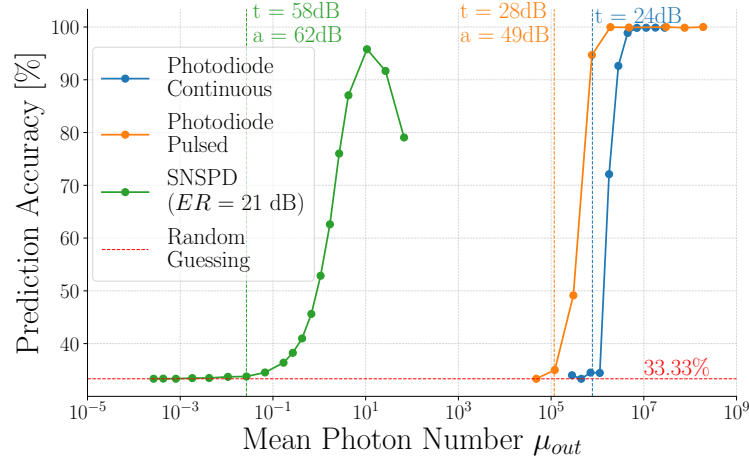


FIGURE 7.10: Prediction accuracy in relation to the mean photon number μ_{out} , after normalizing the average power to 10 W for thermal damages (t) and 1 MW for ablation damages (a), for which the respective countermeasure attenuation is reported at the top.

7.6 Comparison of the attacks

We studied a comparison of the attacks proposed in this work, and collected them based on their complexities in Table 7.3.

regime	complexity	<i>low</i>	<i>medium</i>	<i>high</i>
	<i>strong</i> <i>weak</i>	PD-CWLA	PD-PLA	G-M

TABLE 7.3: Use-cases of the attacks proposed in this work: Photodiode - continuous wave laser attack (PD-CWLA), Photodiode - pulsed laser attack (PD-PLA) and attack using Geiger-mode single-photon detectors (G-M).

The attack in continuous-wave doesn't require the alignment of the pulses with Alice's setup, differently from the pulsed-laser one. Once Alice and Eve are synchronized, achieved either having an electrical connection to Alice's SoC or exploiting clock-recovery algorithms like [28], the continuous stream of photons provides all the information on the symbols being transmitted. Yet, this attack is the least resistant to countermeasures, given that a considerable amount of optical power is wasted in useless information between two subsequent symbols. On the other hand, the pulsed-regime attack requires precise alignment of Eve's pulses with Alice's modulation at the beginning of the transmission. Once that is achieved, though, the stream is straightforward and the use of photo-diodes (that can have bandwidths in the order of 2-20 GHz) guarantees every symbol of the sequence can be identified. It is important to acknowledge that all the results of the strong light regime are dependent on the total noise floor shown in Eq. 7.20 and Fig. 7.9, sum of the ones of the photo-diode and the oscilloscope. Improving the performances of these two components, it is possible to counteract more attenuation and reconstruct the sequence with better accuracies in strong light regime. As shown in Fig. 7.10, we might conclude that the pulsed-laser attack yields meaningful results for just some dBs of attenuation more than the continuous-wave attack. In reality, achieving higher peak powers is much easier than achieving higher average powers, for example using an *Erbium-Doped Fiber Amplifier* (EDFA), or by reducing the duty-cycle of the pulses. Another advantage is that using a pulsed laser one can work closer to the thermal upper limit imposed by silica SM fibers, which is 1 MW for pulsed lasers [108, 91]. In comparison to the photo-diode used in the strong light scenario, attacks using SNSPDs are notably more complex, as reported in Table 7.3. The main reason for this complexity is the interaction of many parameters that control the reliability and efficiency of SNSPDs. Moreover, key performance indicators such as the extinction ratio after the states are measured (which dependency is shown in Fig. 7.2), dark count rate, jitter time, reset time, etc. must be carefully optimized in tandem to ensure accurate and efficient single-photon detection [119]. Better results on the prediction accuracy, using the same POVM, can be obtained by exploiting photon-number-resolving single-photon detectors, as we discussed in sec. 7.3.

7.7 Countermeasures

Up to now we only considered passive countermeasures that involved attenuation at the entrance of Alice's setup using a VOA. This is because we investigated different types of THA counterattacks and categorized the most common defenses in:

- **Passive**

1. Filtering (using a *Wavelength Division Multiplexer* filter in Alice's transmission band);
 2. Isolation (using an Isolator or a Circulator at Alice's output);
 3. Attenuation (using Optical Attenuators at Alice's output);
- **Active**
 1. *Watchdog* detectors (exploiting a Circulator connected to a detector at Alice's output).

Passive countermeasures can be all traced back to the attenuation type, since all of them can be overcome sending enough optical power [94, 120]. By measuring input and output power on different off-the-shelf components, we calculated for passive filtering and isolation to correspond to an approximate ~60 dB of optical attenuation. The results that we reported confirm that even using SNSPDs as a mean of attack is not enough to get useful results on a real-world-scenario QKD setup, since the transmission rates are generally higher (transmission frequencies higher than 50-100MHz are sufficient with state-of-the-art equipments) and an isolator is often sufficient to block the incoming light in Alice's system. Furthermore, reducing back-reflections is a proactive measure that enhances overall security. This can be achieved by using angle-polished connectors (FC/APC) instead of flat connectors (FC/PC), eliminating open ports, and fusing connections where possible. These methods can limit attack opportunities regardless of the spectral characteristics of individual components [61].

An active countermeasure system can also be used, exploiting what are usually known as "Watchdog" detectors. These are devices that measure the light impinging in Alice's setup by means of a Circulator situated at the output of the system. These are particularly helpful because an attacker can be immediately spotted by measuring its optical power (that is generally high). There are three cases a Watchdog detector (WD) and an eavesdropper detector (ED) can face:

1. *The noise floor of the WD is lower than the one of the ED*: in this case the attacker is caught and the communication terminates;
2. *The noise floor of the WD is higher than the one of the ED*: in this case Alice could not perceive the presence of the attacker and can be hacked;
3. *The noise floors of the WD and of the ED are comparable*: in this case the attacker is surely spotted, since it needs to shoot much higher power to cope with Alice's setup internal attenuations.

Therefore, an eavesdropper should aim at using detectors with very low noise level (such as single-photon detectors) to counteract the use of Watchdog detectors. Despite that, the effectiveness of both monitoring detectors (as well as the other passive countermeasures) can be limited by their spectral responsiveness, potentially allowing attacks at wavelengths where their sensitivity is negligible [61]. In this sense, having Eve sending short pulses could limit the visibility of the Watchdog detector, not triggering the power measure. In conclusion, a near-optimal countermeasure to a THA can be achieved by mixing all of the proposed above.

We now try to estimate a lower bound on the attenuation required to counteract these attacks based on the assumption that the *Laser-Induced Damage Threshold* (LIDT) of the system is set at 10 W for thermal damages and 1 MW for ablation damages. As shown in Fig. 7.2, a mean photon number of $\mu_{out} \sim 5 - 8$ photons per symbol is sufficient for Eve to obtain a successful attack with a prediction accuracy higher than 80% in good conditions of extinction ratio. In order to have full security on the iPOGNAC, a stricter bound can be

placed at $\mu_{out} < 0.1$ photons per symbol to get Eve's prediction accuracy closer to the random guessing limit of 33%. Therefore, we can give an estimate on the countermeasures that can be taken in these conditions. Assuming a total loss inside the iPOGNAC (excluded the VOA) in the best case (not accounting coupling losses or imperfections in the components) of $\Delta P \simeq 6$ dB, we can derive the amount of attenuation at the output that can counteract the attack:

$$A_{dB} = \frac{1}{2} \left(10 \log_{10} \left(\frac{\mu_{in}}{\mu_{out}} \right) - \Delta P \right) \quad (7.22)$$

Where the $1/2$ is because of the optical pulse crossing two times the attenuation imposed by the VOA, and μ_{in} is solely dependent by parameters of the attacker:

$$\mu_{in} = \frac{\lambda P_{in} \Delta T}{hc} \quad (7.23)$$

where h is Planck's constant ($6.6261 \text{E-}34$ J·s), c is the speed of light in vacuum ($2.9979 \text{E}8$ m/s), while P_{in} , λ and ΔT are respectively the optical power in watts, the wavelength and the width of the pulse of Eve's laser in seconds. In Fig. 7.11 the required levels of attenuation required to counteract different levels of P_{in} are shown. With ~ 65 dB of attenuation, i.e. ~ 130 dB of isolation, at the output, we can consider the iPOGNAC to be secure against the types of THA presented in this work, which is in line with what presented by Lucamarini et al. in [75]. On average, the output power coming out of current QKD systems employing the iPOGNAC revolves around $\mu \simeq 10^5$ photons per symbol, therefore already requiring an attenuation of around 50 dB to reach a typical mean photon number of 0.6 photons per symbol. As we have shown with our work, this is already a reasonable amount of countermeasure that deprives Eve of a lot of information. In order to be completely secure from this types of attacks, adding an isolator at the output (which, when traveled in the opposite direction adds an attenuation of at least 30 dB) can be a good habit for state-of-the-art QKD systems in general.

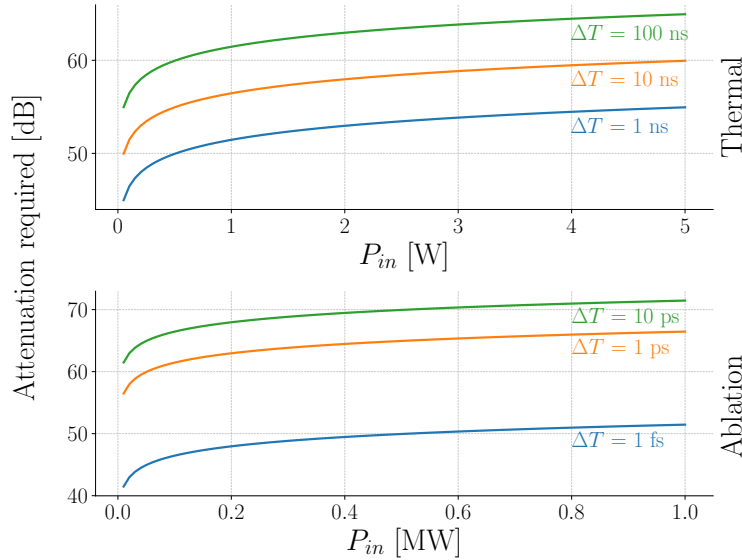


FIGURE 7.11: Attenuation required to counteract the THA presented in this work in different scenarios of input power P_{in} and pulse width ΔT , both for thermal (top) and ablation (bottom) damage limits.

7.8 Conclusion

We analyzed different methodologies to approach Trojan-Horse Attacks that can be executed on a QKD setup that exploits three-state efficient-BB84 and a modulation scheme like the one of the *iPOGNAC*, a self-compensating all-fiber polarization encoder first proposed in [19]. We proposed two different categories of attack, in strong and weak light regime, where in the former the detection can be done exploiting photo-diodes while in the latter higher-efficiency single-photon detectors must be used. Even though the attack types are different in the two regimes (utilizing a more deterministic approach in one and a more probabilistic one depending on the mean-photon-number in the other) we estimated that the weak regime can be considered successful with countermeasures that comprise attenuations ~ 30 dB higher than the ones required in the strong light regime, allowing to detect the sequence even in conditions of extremely low average power. However, the prediction accuracy is not as stable and deterministic as in the strong regime because of the detector types (the ones we adopted are Si-Photodiodes). Using photodiodes, in fact, the prediction accuracy follows a shape similar to an "inversed sigmoid function", from 100% to 33.33% (equivalent to a random guessing), while for single-photon detectors the prediction accuracy is highly limited by the saturation of the detectors and the extinction ratio of the polarization states.

We've shown that an effective and immediate Trojan Horse Attack is possible in continuous waveform regime (without having to adjust the delays between a light pulse and the modulation of Alice), that the same kind of attack in pulsed regime can overcome more easily higher defense layers, and that attacks are also possible at higher attenuation levels using single-photon detectors with high sensitivity like SNSPDs. We investigated different types of countermeasures that can be applied to the setup that can limit the leaked information at Eve's side with ease. In a broader sense, we've estimated that having more than 65 dB of attenuation (~ 130 dB of isolation) at Alice's output is many cases a good habit to limit the effects of Trojan Horse Attacks like the ones proposed, and that this can be improved in combination with wavelength filtering or optical isolation. We gave an estimate of the theoretical mutual information that can be extracted by the attack in weak regime, both in an hypothetical scenario using an optimal POVM, using perfect photon-number-resolving detectors and in a more realistic scenario using SNSPDs. For future works, we are planning the implementation of a Machine-Learning classifier to distinguish the states in strong light regime.

Chapter 8

Conclusions

This thesis has embarked on a journey to advance the practical applicability of Quantum Key Distribution. The research presented has addressed critical challenges spanning from the deployment, to the long-term operation, and security hardening of QKD systems. Through a combination of theoretical modeling, hardware innovation, and in-field demonstrations, this work has contributed to push the technological readiness of QKD for practical, large-scale deployment. The principal findings and contributions are summarized in the following paragraphs.

A core contribution of this work was the development of a versatile and complete model for Sagnac loop-based modulators, which form the heart of our stable quantum state encoders. We generalized the behavior of these interferometers to describe both polarization and intensity modulation, accounting for the distinct interactions of co- and counter-propagating signals within a traveling-wave electro-optic modulator. Building on this model, we introduced and experimentally validated several novel modulation schemes designed to overcome the repetition rate limitations imposed by traditional asymmetric Sagnac configurations. The most significant of these is the *balanced modulation* technique. This approach successfully removes the need for a physical asymmetry in the loop, allowing for a dramatic increase in the maximum achievable symbol rate. We demonstrated robust operation at 1.5 GHz, achieving a high polarization extinction ratio (> 23 dB) and a low intrinsic QBER ($< 0.5\%$). This method not only enhances speed but also improves system stability by mitigating voltage-dependent patterning effects, offering a clear path toward multi-GHz, calibration-free encoders for next-generation QKD systems.

Within the framework of the QUANGO project, we engineered a complete, high-performance QKD system tailored for both fiber-optic and free-space channels. The system implements a polarization-based, three-state, one-decoy efficient-BB84 protocol, featuring our advanced iPOGNAC encoder and a qubit-based synchronization protocol (Qubit4Synch). The system's performance was rigorously validated in two key scenarios. In laboratory fiber tests, it demonstrated exceptional stability, maintaining a low average QBER of approximately 0.4% and generating a secret key rate of 467 kb/s over a channel with 26 dB of loss. More significantly, the system was deployed over a 620-meter urban free-space link. By integrating active atmospheric turbulence compensation, we achieved a sustained secret key rate exceeding 1 Mb/s with a stable QBER around 1.5% during daylight operation. Furthermore, we successfully emulated a high-loss satellite-to-ground link scenario (39 dB), generating a positive key rate of approximately 20 kb/s. These results confirm the system's robustness and operational flexibility, establishing it as a viable payload for future terrestrial and satellite-based quantum communication networks.

A major achievement of this research was the deployment and analysis of the VenQCI network, a four-node metropolitan QKD network that represents one of Italy's first steps

toward a national quantum communication infrastructure. This network integrates our QKD platform with existing classical telecommunication hardware, demonstrating the practical feasibility of hybrid quantum-classical systems. A key innovation in this network is the use of automated, node-agent-driven optical link switching. This architecture allows a single QKD device to service multiple links in a time-multiplexed fashion, significantly reducing the hardware cost and complexity of network expansion. Our two-month-long analysis of the network in full production mode confirmed its remarkable long-term stability and resilience. The system provided continuous, uninterrupted secure keys to refresh a 100 Gbps MACsec-encrypted classical data link, with no significant performance degradation or daily trends observed. This in-field validation proves that QKD technology has matured to the point where it can be operated as a reliable, automated utility within a real-world, mission-critical environment.

Beyond performance and deployment, ensuring the practical security of QKD hardware against side-channel attacks is paramount. This thesis presented a thorough investigation into the vulnerability of the iPOGNAC encoder to Trojan-Horse Attacks. We developed a theoretical model to predict Eve's potential information gain and conducted a series of experimental attacks under various conditions, including continuous-wave and pulsed lasers in both strong-light (photodiode-based) and weak-light (SNSPD-based) regimes. Our findings show that a naive implementation is indeed vulnerable. However, we demonstrated that practical and readily available countermeasures are highly effective. We quantified the security provided by standard passive components, such as optical isolators and filters, and active "watchdog" detectors. Our analysis concludes that an overall attenuation of approximately 65 dB at the system's output is sufficient to reduce Eve's information gain to negligible levels, rendering the attack ineffective. This result provides a concrete security parameter for hardening QKD systems, ensuring their resilience against one of the most-cited hardware-level threats.

The research presented in this thesis proposes a solid foundation for several future directions:

- *Hardware Advancement:* The symmetric Sagnac modulator design can be optimized for even higher repetition rates and integrated into photonic integrated circuits (PICs) to drastically reduce the size, weight, power, and cost of QKD systems.
- *Satellite QKD:* The next step for the QUANGO project is the integration of the QKD payload into a CubeSat platform for a low-Earth-orbit (LEO) satellite demonstration, which would represent a major milestone towards a global quantum network.
- *Network Scaling and Interoperability:* The VenQCI network can be expanded to include more nodes and heterogeneous QKD technologies. Future work should focus on implementing advanced, dynamic key-routing and management protocols that align with emerging ETSI and ITU-T standards to ensure interoperability between different quantum networks.
- *Advanced Security Analysis:* While we addressed THAs, further investigation into other potential side-channel vulnerabilities (e.g.: timing, spectral, and power side-channels) is necessary. The development of machine-learning-based monitoring systems could provide real-time threat detection and automated defense mechanisms.

In conclusion, this thesis has demonstrated that through careful design, rigorous testing, and an approach that considers components, systems, and networks, Quantum Key Distribution is no longer a futuristic promise but a present-day reality. The advances detailed here contribute to the state-of-the-art with solutions that will shape the secure communication infrastructures of tomorrow.

Appendix A

Appendix: Trojan-Horse attack on the iPognac

In this section we show how to compute the Von Neumann entropy of the state ρ received by Eve, where $\rho = \frac{1}{3} \sum_{j=1}^3 |\psi_j\rangle\langle\psi_j|$ and the states $|\psi_j\rangle$ are defined in eq. (7.2). The Von Neumann entropy of ρ is equal to the Shannon entropy of its eigenvalues. Therefore, we need to evaluate the eigenvalues of ρ .

Since the three states $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$ are linear independent they can be considered as the first three elements of the basis. Since the Hilbert space is infinite dimensional, we can complete the basis with orthonormal vectors $\{|\psi_4\rangle \dots |\psi_\infty\rangle\}$ that are orthogonal to the subspace defined by $|\psi_j\rangle$ with $(j = 1, 2, 3)$.

Since ρ has support only in the three-dimensional subspace span by $\{|\psi_j\rangle\}$, we can restrict our attention to such subspace, in which the basis elements ρ_{jk} of ρ are given by the following equation:

$$\rho|\psi_k\rangle = \sum_j \rho_{jk} |\psi_j\rangle \quad (\text{A.1})$$

since $\rho = \frac{1}{3} \sum_{j=1}^3 |\psi_j\rangle\langle\psi_j|$ we have that:

$$\rho|\psi_k\rangle = \frac{1}{3} \sum_{j=1}^3 |\psi_j\rangle\langle\psi_j | \psi_k\rangle = \sum_{j=1}^3 \left(\frac{1}{3} \langle\psi_j | \psi_k\rangle \right) |\psi_j\rangle$$

Comparing with (A.1) it is clear that:

$$\rho_{jk} = \frac{1}{3} \langle\psi_j | \psi_k\rangle$$

Therefore, the matrix ρ in the $\{|\psi_j\rangle\}$ basis is given by:

$$\rho = \frac{1}{3} \begin{pmatrix} 1 & e^{-\mu} & e^{-\mu(1-\frac{1}{\sqrt{2}})} \\ e^{-\mu} & 1 & e^{-\mu(1-\frac{1}{\sqrt{2}})} \\ e^{-\mu(1-\frac{1}{\sqrt{2}})} & e^{-\mu(1-\frac{1}{\sqrt{2}})} & 1 \end{pmatrix} \quad (\text{A.2})$$

where the diagonal elements $\langle\psi_i|\psi_i\rangle$ correspond to the squared norms of the vectors. Since coherent states are normalized, these are all equal to 1. The components ρ_{ij} can be evaluated by recalling the general scalar product between two single-mode coherent states is

$$\langle\alpha|\beta\rangle = \exp\left(\alpha^*\beta - \frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}\right) \quad (\text{A.3})$$

Therefore:

$$\begin{aligned}
 \langle \psi_1 | \psi_2 \rangle &= \langle \sqrt{\mu} | 0 \rangle_H \langle 0 | \sqrt{\mu} \rangle_V = e^{-\mu} \\
 \langle \psi_1 | \psi_3 \rangle &= \langle \sqrt{\mu} | \sqrt{\frac{\mu}{2}} \rangle_H \langle 0 | \sqrt{\frac{\mu}{2}} \rangle_V = e^{-\mu(1-\frac{1}{\sqrt{2}})} \\
 \langle \psi_2 | \psi_3 \rangle &= \langle 0 | \sqrt{\frac{\mu}{2}} \rangle_H \langle \sqrt{\mu} | \sqrt{\frac{\mu}{2}} \rangle_V = e^{-\mu(1-\frac{1}{\sqrt{2}})}
 \end{aligned} \tag{A.4}$$

and the other terms are evaluated by using the relation $\langle \psi_j | \psi_i \rangle = \langle \psi_i | \psi_j \rangle^*$.

Calculating the eigenvalues of the matrix ρ , we obtain:

$$\lambda_1(\mu) = \frac{1}{3} - \frac{e^{-\mu}}{3} \tag{A.5}$$

$$\lambda_{2,3}(\mu) = \frac{1}{3} + \frac{e^{-\mu}}{6} \left(1 \pm \sqrt{1 + 8e^{\sqrt{2}\mu}} \right) \tag{A.6}$$

Using the eigenvalues just found, we can calculate the Shannon entropy of the ensemble state ρ as:

$$H(\mu) := - \sum_{i=1}^3 \lambda_i(\mu) \log_2(\lambda_i(\mu)) \tag{A.7}$$

Bibliography

- [1] URL: <https://www.fiberoptics4sale.com/blogs/wave-optics/101402566-polarization-states>.
- [2] URL: <https://quantdare.com/what-is-mutual-information/>.
- [3] URL: <https://www.quantiki.org/wiki/bb84-and-ekert91-protocols>.
- [4] URL: <https://en.wikipedia.org/wiki/BQP>.
- [5] URL: https://en.wikipedia.org/wiki/Quantum_key_distribution#E91_protocol:_Artur_Ekert_.281991.29.
- [6] URL: <https://www.icfo.eu/newsroom/news/4945-quantum-communications-with-nanosatellites-and-5g-protocols>.
- [7] URL: <https://quango.dei.unipd.it/>.
- [8] Ivi Afxenti et al. “Polarization purity and dispersion characteristics of nested antiresonant nodeless hollow-core optical fiber at near- and short-wave-IR wavelengths for quantum communications”. In: *Optics Express* 32.20 (Sept. 2024), p. 34471. ISSN: 1094-4087. DOI: [10.1364/oe.529331](https://doi.org/10.1364/oe.529331). URL: <http://dx.doi.org/10.1364/OE.529331>.
- [9] Costantino Agnesi et al. “All-fiber self-compensating polarization encoder for quantum key distribution”. In: *Optics Letters* 44.10 (May 2019), p. 2398. ISSN: 1539-4794. DOI: [10.1364/ol.44.002398](https://doi.org/10.1364/ol.44.002398). URL: <http://dx.doi.org/10.1364/OL.44.002398>.
- [10] Costantino Agnesi et al. “All-fiber self-compensating polarization encoder for quantum key distribution”. In: *Optics letters* 44.10 (2019), pp. 2398–2401.
- [11] Costantino Agnesi et al. “In-field comparison between G.652 and G.655 optical fibres for polarisation-based quantum key distribution”. In: *IET Quantum Comm.* 5.4 (2024), pp. 567–574. DOI: <https://doi.org/10.1049/qtc2.12095>. URL: <https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/qtc2.12095>.
- [12] Rod C Alferness. “Waveguide electrooptic modulators”. In: *IEEE Transactions on Microwave Theory Techniques* 30 (1982), pp. 1121–1137.
- [13] A. Ali et al. “Unrepeated HCF Transmission over spans up to 301.7 km”. In: *Optical Fiber Communication Conference (OFC) Postdeadline Papers 2025*. Optica Publishing Group, 2025, Th4A.3. DOI: [10.1364/OFC.2025.Th4A.3](https://doi.org/10.1364/OFC.2025.Th4A.3). URL: <https://opg.optica.org/abstract.cfm?URI=OFC-2025-Th4A.3>.
- [14] Antonio Assalini, Gianfranco Cariolaro, and Gianfranco Pierobon. “Efficient optimal minimum error discrimination of symmetric quantum states”. In: *Physical Review A* 81.1 (Jan. 2010). ISSN: 1094-1622. DOI: [10.1103/physreva.81.012315](https://doi.org/10.1103/physreva.81.012315). URL: <http://dx.doi.org/10.1103/PhysRevA.81.012315>.
- [15] Claire Autebert et al. “Direct measurement of the recovery time of superconducting nanowire single-photon detectors”. In: *Journal of Applied Physics* 128.7 (Aug. 2020). ISSN: 1089-7550. DOI: [10.1063/5.0007976](https://doi.org/10.1063/5.0007976). URL: <http://dx.doi.org/10.1063/5.0007976>.
- [16] Marco Avesani et al. “Deployment-Ready Quantum Key Distribution Over a Classical Network Infrastructure in Padua”. In: *Journal of Lightwave Technology* 40.6 (Mar. 2022), 1658–1663. ISSN: 1558-2213. DOI: [10.1109/jlt.2021.3130447](https://doi.org/10.1109/jlt.2021.3130447). URL: <http://dx.doi.org/10.1109/JLT.2021.3130447>.
- [17] Marco Avesani et al. “Resource-effective quantum key distribution: a field trial in Padua city center”. In: *Opt. Lett.* 46.12 (2021), pp. 2848–2851. DOI: [10.1364/OL.422890](https://doi.org/10.1364/OL.422890). URL: <http://opg.optica.org/ol/abstract.cfm?URI=ol-46-12-2848>.
- [18] Marco Avesani et al. “Source-device-independent heterodyne-based quantum random number generator at 17 Gbps”. In: *Nature Communications* 9.1 (Dec. 2018). ISSN: 2041-1723. DOI: [10.1038/s41467-018-07585-0](https://doi.org/10.1038/s41467-018-07585-0). URL: <http://dx.doi.org/10.1038/s41467-018-07585-0>.

- [19] Marco Avesani et al. “Stable, low-error, and calibration-free polarization encoder for free-space quantum communication”. In: *Opt. Lett.* 45.17 (2020), pp. 4706–4709. DOI: [10.1364/OL.396412](https://doi.org/10.1364/OL.396412). URL: <https://opg.optica.org/ol/abstract.cfm?URI=ol-45-17-4706>.
- [20] Adomas Baliuka et al. “Deep-learning-based radio-frequency side-channel attack on quantum key distribution”. In: *Physical Review Applied* 20.5 (Nov. 2023). ISSN: 2331-7019. DOI: [10.1103/physrevapplied.20.054040](https://doi.org/10.1103/physrevapplied.20.054040). URL: <http://dx.doi.org/10.1103/PhysRevApplied.20.054040>.
- [21] Karol Bartkiewicz et al. “Experimental Eavesdropping Based on Optimal Quantum Cloning”. In: *Physical Review Letters* 110.17 (2013). ISSN: 1079-7114. DOI: [10.1103/physrevlett.110.173601](https://doi.org/10.1103/physrevlett.110.173601).
- [22] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. “Progress in satellite quantum key distribution”. In: *npj Quantum Information* 3.1 (2017). ISSN: 2056-6387. DOI: [10.1038/s41534-017-0031-5](https://doi.org/10.1038/s41534-017-0031-5).
- [23] Aharon Ben-Tal and Arkadi Nemirovski. *Lectures on Modern Convex Optimization: Analysis, Algorithms, and Engineering Applications*. Society for Industrial and Applied Mathematics, Jan. 2001. ISBN: 9780898718829. DOI: [10.1137/1.9780898718829](https://doi.org/10.1137/1.9780898718829). URL: <http://dx.doi.org/10.1137/1.9780898718829>.
- [24] Charles H. Bennett. “Quantum cryptography using any two nonorthogonal states”. In: *Phys. Rev. Lett.* 68 (21 1992), pp. 3121–3124. DOI: [10.1103/PhysRevLett.68.3121](https://doi.org/10.1103/PhysRevLett.68.3121).
- [25] Charles H. Bennett, Gilles Brassard, and N. David Mermin. “Quantum cryptography without Bell’s theorem”. In: *Phys. Rev. Lett.* 68 (5 1992), pp. 557–559. DOI: [10.1103/PhysRevLett.68.557](https://doi.org/10.1103/PhysRevLett.68.557).
- [26] Federico Berra et al. *General model and modulation strategies for Sagnac-based encoders*. 2025. arXiv: [2510.11873](https://arxiv.org/abs/2510.11873) [physics.optics]. URL: <https://arxiv.org/abs/2510.11873>.
- [27] Federico Berra et al. “Modular source for near-infrared quantum communication”. In: *EPJ Quantum Technology* 10.1 (July 2023). ISSN: 2196-0763. DOI: [10.1140/epjqt/s40507-023-00185-y](https://doi.org/10.1140/epjqt/s40507-023-00185-y). URL: <http://dx.doi.org/10.1140/epjqt/s40507-023-00185-y>.
- [28] Luca Calderaro et al. “Fast and Simple Qubit-Based Synchronization for Quantum Key Distribution”. In: *Phys. Rev. Appl.* 13 (5 2020), p. 054041. DOI: [10.1103/PhysRevApplied.13.054041](https://doi.org/10.1103/PhysRevApplied.13.054041). URL: <https://link.aps.org/doi/10.1103/PhysRevApplied.13.054041>.
- [29] Jiu-Peng Chen et al. *Twin-Field Quantum Key Distribution over 511 km Optical Fiber Linking two Distant Metropolitans*. 2021. arXiv: [2102.00433](https://arxiv.org/abs/2102.00433) [quant-ph].
- [30] Yu-Ao Chen et al. “An integrated space-to-ground quantum communication network over 4,600 kilometres”. In: *Nature* 589.7841 (2021), pp. 214–219.
- [31] Guillermo Currás-Lorenzo et al. “Security of high-speed quantum key distribution with imperfect sources”. In: *Optica Quantum* (Oct. 2025). ISSN: 2837-6714. DOI: [10.1364/opticaq.569424](https://doi.org/10.1364/opticaq.569424). URL: <http://dx.doi.org/10.1364/OPTICAQ.569424>.
- [32] Guillermo Currás-Lorenzo et al. *Security of high-speed quantum key distribution with imperfect sources*. 2025. arXiv: [2305.05930](https://arxiv.org/abs/2305.05930) [quant-ph]. URL: <https://arxiv.org/abs/2305.05930>.
- [33] Jean Paul Degabriele et al. *Backdoors in Pseudorandom Number Generators: Possibility and Impossibility Results*. Cryptology ePrint Archive, Paper 2016/577. 2016. URL: <https://eprint.iacr.org/2016/577>.
- [34] Yu-Yang Ding et al. “Polarization variations in installed fibers and their influence on quantum key distribution systems”. In: *Optics Express* 25.22 (Oct. 2017), p. 27923. ISSN: 1094-4087. DOI: [10.1364/oe.25.027923](https://doi.org/10.1364/oe.25.027923). URL: <http://dx.doi.org/10.1364/OE.25.027923>.
- [35] J. F. Dynes et al. “Cambridge quantum network”. In: *npj Quantum Information* 5.1 (Nov. 2019). ISSN: 2056-6387. DOI: [10.1038/s41534-019-0221-4](https://doi.org/10.1038/s41534-019-0221-4). URL: <http://dx.doi.org/10.1038/s41534-019-0221-4>.
- [36] Artur K. Ekert. “Quantum cryptography based on Bell’s theorem”. In: *Phys. Rev. Lett.* 67 (6 1991), pp. 661–663. DOI: [10.1103/PhysRevLett.67.661](https://doi.org/10.1103/PhysRevLett.67.661).
- [37] ETSI. *Quantum Key Distribution (QKD); Control Interface for Software Defined Networks*. Tech. rep. ETSI GS QKD 015 V2.1.1. European Telecommunications Standards Institute

- (ETSI), 2021. URL: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/015/02.01.01_60/gs_QKD015v020101p.pdf.
- [38] ETSI. *Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks*. Tech. rep. ETSI GS QKD 018 V1.1.1. European Telecommunications Standards Institute (ETSI), Apr. 2022. URL: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/018/01.01.01_60/gs_qkd018v010101p.pdf.
- [39] Maxim Fadeev et al. “Optical-pumping attack on a quantum key distribution laser source”. In: *Opt. Express* 33.22 (2025), pp. 47001–47012. DOI: [10.1364/OE.562406](https://doi.org/10.1364/OE.562406). URL: <https://opg.optica.org/oe/abstract.cfm?URI=oe-33-22-47001>.
- [40] Austin G. Fowler et al. “Surface Code Quantum Communication”. In: *Physical Review Letters* 104.18 (2010). ISSN: 1079-7114. DOI: [10.1103/physrevlett.104.180503](https://doi.org/10.1103/physrevlett.104.180503).
- [41] Keinosuke Fukunaga. *Introduction to Statistical Pattern Recognition*. Second. San Diego: Academic Press, 2000. ISBN: 9780122698514.
- [42] C.-H. F. Fung et al. “Security proof of quantum key distribution with detection efficiency mismatch”. In: *Quantum Information and Computation* 9.1–2 (Jan. 2009), 131–165. ISSN: 1533-7146. DOI: [10.26421/qic9.1-2-8](https://doi.org/10.26421/qic9.1-2-8). URL: <http://dx.doi.org/10.26421/QIC9.1-2-8>.
- [43] Chi-Hang Fred Fung et al. “Phase-remapping attack in practical quantum-key-distribution systems”. In: *Physical Review A* 75.3 (Mar. 2007). ISSN: 1094-1622. DOI: [10.1103/physreva.75.032314](https://doi.org/10.1103/physreva.75.032314). URL: <http://dx.doi.org/10.1103/PhysRevA.75.032314>.
- [44] N. Gisin et al. “Trojan-horse attacks on quantum-key-distribution systems”. In: *Physical Review A* 73.2 (Feb. 2006). ISSN: 1094-1622. DOI: [10.1103/physreva.73.022320](https://doi.org/10.1103/physreva.73.022320). URL: <http://dx.doi.org/10.1103/PhysRevA.73.022320>.
- [45] Nicolas Gisin et al. “Quantum cryptography”. In: *Reviews of Modern Physics* 74.1 (2002), 145–195. ISSN: 1539-0756. DOI: [10.1103/revmodphys.74.145](https://doi.org/10.1103/revmodphys.74.145).
- [46] I. H. Lopez Grande et al. “Adaptable transmitter for discrete and continuous variable quantum key distribution”. In: *Opt. Express* 29.10 (2021), pp. 14815–14827. DOI: [10.1364/OE.425382](https://doi.org/10.1364/OE.425382).
- [47] Fadri Grünenfelder et al. “Simple and high-speed polarization-based QKD”. In: *Applied Physics Letters* 112.5 (Jan. 2018). ISSN: 1077-3118. DOI: [10.1063/1.5016931](https://doi.org/10.1063/1.5016931). URL: <http://dx.doi.org/10.1063/1.5016931>.
- [48] Fadri Grünenfelder et al. “Performance and security of 5 GHz repetition rate polarization-based quantum key distribution”. In: *Applied Physics Letters* 117.14 (2020), p. 144003. ISSN: 1077-3118. DOI: [10.1063/5.0021468](https://doi.org/10.1063/5.0021468).
- [49] Alberto Guerrini. *Design optomeccanico di un sistema ottico per QKD in spazio libero*. Tesi di Laurea Triennale, Dipartimento di Ingegneria dell’Informazione, Università degli Studi di Padova. 2022. URL: <https://hdl.handle.net/20.500.12608/49721>.
- [50] Carl W. Helstrom. “Quantum detection and estimation theory”. In: *Journal of Statistical Physics* 1 (1969), pp. 231–252. URL: <https://api.semanticscholar.org/CorpusID:12758217>.
- [51] D B Higginbottom et al. “Pure single photons from a trapped atom source”. In: *New Journal of Physics* 18.9 (2016), p. 093038. ISSN: 1367-2630. DOI: [10.1088/1367-2630/18/9/093038](https://doi.org/10.1088/1367-2630/18/9/093038).
- [52] Sanzida Hoque, Abdullah Aydeger, and Engin Zeydan. *Exploring Post Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design*. 2024. arXiv: [2404.10602](https://arxiv.org/abs/2404.10602) [cs.CR]. URL: <https://arxiv.org/abs/2404.10602>.
- [53] Anqi Huang et al. “Laser-Damage Attack Against Optical Attenuators in Quantum Key Distribution”. In: *Physical Review Applied* 13.3 (Mar. 2020). ISSN: 2331-7019. DOI: [10.1103/physrevapplied.13.034017](https://doi.org/10.1103/physrevapplied.13.034017). URL: <http://dx.doi.org/10.1103/PhysRevApplied.13.034017>.
- [54] Anqi Huang et al. “Laser-seeding Attack in Quantum Key Distribution”. In: *Physical Review Applied* 12.6 (Dec. 2019). ISSN: 2331-7019. DOI: [10.1103/physrevapplied.12.064043](https://doi.org/10.1103/physrevapplied.12.064043). URL: <http://dx.doi.org/10.1103/PhysRevApplied.12.064043>.

- [55] Daniel Huber et al. “Semiconductor quantum dots as an ideal source of polarization-entangled photon pairs on-demand: a review”. In: *Journal of Optics* 20.7 (2018), p. 073002. DOI: [10.1088/2040-8986/aac4c4](https://doi.org/10.1088/2040-8986/aac4c4).
- [56] Emilio Hugues-Salas et al. “Monitoring and Physical-Layer Attack Mitigation in SDN-Controlled Quantum Key Distribution Networks”. In: *Journal of Optical Communications and Networking* 11.2 (Jan. 2019), A209. ISSN: 1943-0639. DOI: [10.1364/jocn.11.00a209](https://doi.org/10.1364/jocn.11.00a209). URL: <http://dx.doi.org/10.1364/JOCN.11.00A209>.
- [57] Won-Young Hwang. “Quantum Key Distribution with High Loss: Toward Global Secure Communication”. In: *Physical Review Letters* 91.5 (2003). ISSN: 1079-7114. DOI: [10.1103/physrevlett.91.057901](https://doi.org/10.1103/physrevlett.91.057901).
- [58] “IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security”. In: *IEEE Std 802.1AE-2018 (Revision of IEEE Std 802.1AE-2006)* (2018), pp. 1–239. DOI: [10.1109/IEEESTD.2018.8585421](https://doi.org/10.1109/IEEESTD.2018.8585421).
- [59] ITU-T. *Control and management for quantum key distribution network*. Tech. rep. ITU-T Recommendation Y.3804. International Telecommunication Union - Telecommunication Standardization Sector (ITU-T), 2020. URL: <https://www.itu.int/rec/T-REC-Y.3804>.
- [60] ITU-T. *Quantum key distribution networks – Software-defined networking control*. Tech. rep. ITU-T Recommendation Y.3805. International Telecommunication Union - Telecommunication Standardization Sector (ITU-T), 2022. URL: <https://www.itu.int/rec/T-REC-Y.3805>.
- [61] Nitin Jain et al. “Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution Systems”. In: *IEEE Journal of Selected Topics in Quantum Electronics* 21.3 (May 2015), 168–177. ISSN: 1558-4542. DOI: [10.1109/jstqe.2014.2365585](https://doi.org/10.1109/jstqe.2014.2365585). URL: <http://dx.doi.org/10.1109/JSTQE.2014.2365585>.
- [62] Nitin Jain et al. “Trojan-horse attacks threaten the security of practical quantum cryptography”. In: *New Journal of Physics* 16.12 (Dec. 2014), p. 123030. ISSN: 1367-2630. DOI: [10.1088/1367-2630/16/12/123030](https://doi.org/10.1088/1367-2630/16/12/123030). URL: <http://dx.doi.org/10.1088/1367-2630/16/12/123030>.
- [63] Toshiya Kobayashi, Akihisa Tomita, and Atsushi Okamoto. “Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser”. In: *Physical Review A* 90.3 (Sept. 2014). ISSN: 1094-1622. DOI: [10.1103/physreva.90.032320](https://doi.org/10.1103/physreva.90.032320). URL: <http://dx.doi.org/10.1103/PhysRevA.90.032320>.
- [64] BT Research Labs and Lumenity. “BT conducts world’s first trial of quantum-secure communications over hollow core fibre cable”. In: (2025). Demonstrated QKD over 6 km HCF with low latency and negligible crosstalk.
- [65] Andrew M. Lance et al. “No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light”. In: *Phys. Rev. Lett.* 95 (18 2005), p. 180503. DOI: [10.1103/PhysRevLett.95.180503](https://doi.org/10.1103/PhysRevLett.95.180503).
- [66] Hong-Wei Li et al. “Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources”. In: *Physical Review A* 84.6 (Dec. 2011). ISSN: 1094-1622. DOI: [10.1103/physreva.84.062308](https://doi.org/10.1103/physreva.84.062308). URL: <http://dx.doi.org/10.1103/PhysRevA.84.062308>.
- [67] Yang Li et al. “High-speed robust polarization modulation for quantum key distribution”. In: *Opt. Lett.* 44.21 (2019), pp. 5262–5265. DOI: [10.1364/OL.44.005262](https://doi.org/10.1364/OL.44.005262). URL: <https://opg.optica.org/ol/abstract.cfm?URI=ol-44-21-5262>.
- [68] Sheng-Kai Liao et al. “Satellite-to-ground quantum key distribution”. In: *Nature* 549.7670 (2017), 43–47. ISSN: 1476-4687. DOI: [10.1038/nature23655](https://doi.org/10.1038/nature23655).
- [69] H.-K. Lo and J. Preskill. “Security of quantum key distribution using weak coherent states with nonrandom phases”. In: *Quantum Information and Computation* 7.5–6 (July 2007), 431–458. ISSN: 1533-7146. DOI: [10.26421/qic7.5-6-2](https://doi.org/10.26421/qic7.5-6-2). URL: <http://dx.doi.org/10.26421/QIC7.5-6-2>.
- [70] Hoi-Kwong Lo. “Decoy State Quantum Key Distribution (QKD)”. In: *University of Toronto* (Center for Quantum Information and Quantum Control, Dept. of Electrical & Comp. Engineering (ECE) & Dept. of Physics).

- [71] Hoi-Kwong Lo, H.F. Chau, and M. Ardehali. “Efficient Quantum Key Distribution Scheme And Proof of Its Unconditional Security”. In: *Journal of Cryptology* 18 (Apr. 2005), pp. 133–165. doi: [10.1007/s00145-004-0142-y](https://doi.org/10.1007/s00145-004-0142-y).
- [72] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. “Measurement-Device-Independent Quantum Key Distribution”. In: *Physical Review Letters* 108.13 (2012). issn: 1079-7114. doi: [10.1103/physrevlett.108.130503](https://doi.org/10.1103/physrevlett.108.130503).
- [73] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. “Decoy State Quantum Key Distribution”. In: *Physical Review Letters* 94.23 (2005). issn: 1079-7114. doi: [10.1103/physrevlett.94.230504](https://doi.org/10.1103/physrevlett.94.230504).
- [74] M. Lucamarini et al. “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters”. In: *Nature* 557.7705 (May 2018), 400–403. issn: 1476-4687. doi: [10.1038/s41586-018-0066-6](https://doi.org/10.1038/s41586-018-0066-6). url: <http://dx.doi.org/10.1038/s41586-018-0066-6>.
- [75] M. Lucamarini et al. “Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution”. In: *Physical Review X* 5.3 (Sept. 2015). issn: 2160-3308. doi: [10.1103/physrevx.5.031030](https://doi.org/10.1103/physrevx.5.031030). url: <http://dx.doi.org/10.1103/PhysRevX.5.031030>.
- [76] I Lucio-Martinez et al. “Proof-of-concept of real-world quantum key distribution with quantum frames”. In: *New Journal of Physics* 11.9 (2009), p. 095001.
- [77] Svetlana Lukishova et al. “Single-Photon Source for Quantum Information Based on Single Dye Molecule Fluorescence in Liquid Crystal Host”. In: *Molecular Crystals and Liquid Crystals - MOL CRYST LIQUID CRYST* 454 (Sept. 2006). doi: [10.1080/15421400600653977](https://doi.org/10.1080/15421400600653977).
- [78] Tingting Luo et al. “Security analysis against the Trojan horse attack on practical polarization-encoding quantum key distribution systems”. In: *Physical Review A* 109.4 (Apr. 2024). issn: 2469-9934. doi: [10.1103/physreva.109.042608](https://doi.org/10.1103/physreva.109.042608). url: <http://dx.doi.org/10.1103/PhysRevA.109.042608>.
- [79] Lars Lydersen et al. “Superlinear threshold detectors in quantum cryptography”. In: *Physical Review A* 84.3 (Sept. 2011). issn: 1094-1622. doi: [10.1103/physreva.84.032320](https://doi.org/10.1103/physreva.84.032320). url: <http://dx.doi.org/10.1103/PhysRevA.84.032320>.
- [80] Xiongfeng Ma et al. “Practical decoy state for quantum key distribution”. In: *Physical Review A* 72.1 (2005). issn: 1094-1622. doi: [10.1103/physreva.72.012326](https://doi.org/10.1103/physreva.72.012326).
- [81] Vaisakh Mannalath, Víctor Zapatero, and Marcos Curty. “Sharp Finite Statistics for Quantum Key Distribution”. In: *Phys. Rev. Lett.* 135 (2 2025), p. 020803. doi: [10.1103/1735-x48g](https://doi.org/10.1103/1735-x48g). url: <https://link.aps.org/doi/10.1103/1735-x48g>.
- [82] V. Martin et al. “The Madrid Testbed: QKD SDN Control and Key Management in a Production Network”. In: *2023 23rd International Conference on Transparent Optical Networks (ICTON)*. IEEE, July 2023, 1–4. doi: [10.1109/icton59386.2023.10207295](https://doi.org/10.1109/icton59386.2023.10207295). url: <http://dx.doi.org/10.1109/ICTON59386.2023.10207295>.
- [83] Vicente Martin et al. “Quantum technologies in the telecommunications industry”. In: *EPJ Quantum Technology* 8.1 (July 2021). issn: 2196-0763. doi: [10.1140/epjqt/s40507-021-00108-9](https://doi.org/10.1140/epjqt/s40507-021-00108-9). url: <http://dx.doi.org/10.1140/epjqt/s40507-021-00108-9>.
- [84] Eric Monmasson and Marcian N. Cirstea. “FPGA Design Methodology for Industrial Control Systems—A Review”. In: *IEEE Transactions on Industrial Electronics* 54.4 (2007), pp. 1824–1842. doi: [10.1109/TIE.2007.898281](https://doi.org/10.1109/TIE.2007.898281). url: <https://ieeexplore.ieee.org/document/4267891>.
- [85] Sebastian Nauerth et al. “Information leakage via side channels in freespace BB84 quantum cryptography”. In: *New Journal of Physics* 11.6 (June 2009), p. 065001. issn: 1367-2630. doi: [10.1088/1367-2630/11/6/065001](https://doi.org/10.1088/1367-2630/11/6/065001). url: <http://dx.doi.org/10.1088/1367-2630/11/6/065001>.
- [86] Carlos Navas-Merlo and Juan Carlos Garcia-Escartin. “Detector blinding attacks on counterfactual quantum key distribution”. In: *Quantum Information Processing* 20.6 (June 2021). issn: 1573-1332. doi: [10.1007/s11128-021-03134-9](https://doi.org/10.1007/s11128-021-03134-9). url: <http://dx.doi.org/10.1007/s11128-021-03134-9>.

- [87] Boris Naydenov and Fedor Jelezko. “Single-Color Centers in Diamond as Single-Photon Sources and Quantum Sensors”. In: Jan. 2014, pp. 303–318. ISBN: 978-3-319-15635-4. DOI: [10.1007/4243_2014_78](https://doi.org/10.1007/4243_2014_78).
- [88] Jianwei Pan. “Quantum Science Satellite”. In: *Chinese Journal of Space Science* 34.5 (2014), p. 547. ISSN: 0254-6124. DOI: [10.11728/cjss2014.05.547](https://doi.org/10.11728/cjss2014.05.547). URL: <http://dx.doi.org/10.11728/cjss2014.05.547>.
- [89] Laurent de Forges de Parny et al. “Satellite-based quantum information networks: use cases, architecture, and roadmap”. In: *Communications Physics* 6.1 (Jan. 2023). ISSN: 2399-3650. DOI: [10.1038/s42005-022-01123-7](https://doi.org/10.1038/s42005-022-01123-7). URL: <http://dx.doi.org/10.1038/s42005-022-01123-7>.
- [90] M Peev et al. “The SECOQC quantum key distribution network in Vienna”. In: *New Journal of Physics* 11.7 (2009), p. 075001. DOI: [10.1088/1367-2630/11/7/075001](https://doi.org/10.1088/1367-2630/11/7/075001). URL: <https://dx.doi.org/10.1088/1367-2630/11/7/075001>.
- [91] Pavel Peterka et al. “High-power laser testing of calcium-phosphate-based bioresorbable optical fibers”. In: *Optical Materials Express* 11.7 (June 2021), p. 2049. ISSN: 2159-3930. DOI: [10.1364/ome.428490](https://doi.org/10.1364/ome.428490). URL: <http://dx.doi.org/10.1364/OME.428490>.
- [92] Marco Petrovich et al. “Broadband optical fibre with an attenuation lower than 0.1 decibel per kilometre”. In: *Nature Photonics* (Sept. 2025). ISSN: 1749-4893. DOI: [10.1038/s41566-025-01747-5](https://doi.org/10.1038/s41566-025-01747-5). URL: <http://dx.doi.org/10.1038/s41566-025-01747-5>.
- [93] Stefano Pironio et al. “Device-independent quantum key distribution secure against collective attacks”. In: *New Journal of Physics* 11.4 (2009), p. 045021. ISSN: 1367-2630. DOI: [10.1088/1367-2630/11/4/045021](https://doi.org/10.1088/1367-2630/11/4/045021).
- [94] Anastasiya Ponosova et al. “Protecting Fiber-Optic Quantum Key Distribution Sources against Light-Injection Attacks”. In: *PRX Quantum* 3.4 (Oct. 2022). ISSN: 2691-3399. DOI: [10.1103/prxquantum.3.040307](https://doi.org/10.1103/prxquantum.3.040307). URL: <http://dx.doi.org/10.1103/PRXQuantum.3.040307>.
- [95] Bing Qi. “Trustworthiness of detectors in quantum key distribution with untrusted detectors”. In: *Phys. Rev. A* 91 (2 2015), p. 020303. DOI: [10.1103/PhysRevA.91.020303](https://doi.org/10.1103/PhysRevA.91.020303). URL: <https://link.aps.org/doi/10.1103/PhysRevA.91.020303>.
- [96] Yong-Jun Qian et al. “Robust countermeasure against detector control attack in a practical quantum key distribution system”. In: *Optica* 6.9 (Sept. 2019), p. 1178. ISSN: 2334-2536. DOI: [10.1364/optica.6.001178](https://doi.org/10.1364/optica.6.001178). URL: <http://dx.doi.org/10.1364/OPTICA.6.001178>.
- [97] Ji-Gang Ren et al. “Ground-to-satellite quantum teleportation”. In: *Nature* 549.7670 (Aug. 2017), 70–73. ISSN: 1476-4687. DOI: [10.1038/nature23675](https://doi.org/10.1038/nature23675). URL: <http://dx.doi.org/10.1038/nature23675>.
- [98] G. L. Roberts et al. “Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution”. In: *Optics Letters* 43.20 (Oct. 2018), p. 5110. ISSN: 1539-4794. DOI: [10.1364/ol.43.005110](https://doi.org/10.1364/ol.43.005110). URL: <http://dx.doi.org/10.1364/OL.43.005110>.
- [99] Davide Rusca et al. “Finite-key analysis for the 1-decoy state QKD protocol”. In: *Applied Physics Letters* 112.17 (Apr. 2018). ISSN: 1077-3118. DOI: [10.1063/1.5023340](https://doi.org/10.1063/1.5023340). URL: <http://dx.doi.org/10.1063/1.5023340>.
- [100] Davide Rusca et al. “Security proof for a simplified Bennett-Brassard 1984 quantum-key-distribution protocol”. In: *Phys. Rev. A* 98 (5 2018), p. 052336. DOI: [10.1103/PhysRevA.98.052336](https://doi.org/10.1103/PhysRevA.98.052336). URL: <https://link.aps.org/doi/10.1103/PhysRevA.98.052336>.
- [101] Mattia Sabatini et al. “Hybrid encoder for discrete and continuous variable QKD”. In: (2025). arXiv: [2408.17412 \[quant-ph\]](https://arxiv.org/abs/2408.17412). URL: <https://arxiv.org/abs/2408.17412>.
- [102] Shihan Sajeed et al. “Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing”. In: *Physical Review A* 91.3 (Mar. 2015). ISSN: 1094-1622. DOI: [10.1103/physreva.91.032326](https://doi.org/10.1103/physreva.91.032326). URL: <http://dx.doi.org/10.1103/PhysRevA.91.032326>.
- [103] Davide Scalcon et al. “Cross-Encoded Quantum Key Distribution Exploiting Time-Bin and Polarization States with Qubit-Based Synchronization”. In: *Advanced Quantum Technologies* 5.12 (Oct. 2022). ISSN: 2511-9044. DOI: [10.1002/qute.202200051](https://doi.org/10.1002/qute.202200051). URL: <http://dx.doi.org/10.1002/qute.202200051>.

- [104] Davide Scalcon et al. “Low-error encoder for time-bin and decoy states for quantum key distribution”. In: *npj Quantum Information* 11.1 (2025), p. 22.
- [105] Valerio Scarani et al. “Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations”. In: *Phys. Rev. Lett.* 92 (5 2004), p. 057901. DOI: [10.1103/PhysRevLett.92.057901](https://doi.org/10.1103/PhysRevLett.92.057901).
- [106] Peter W. Shor. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”. In: *SIAM Journal on Computing* 26.5 (1997), 1484–1509. ISSN: 1095-7111. DOI: [10.1137/S0097539795293172](https://doi.org/10.1137/S0097539795293172).
- [107] Rajiv Singh et al. *Secure Key Integration Protocol (SKIP)*. Internet-Draft draft-cisco-skip-01. Work in Progress. Internet Engineering Task Force, Mar. 2025. 24 pp. URL: <https://datatracker.ietf.org/doc/draft-cisco-skip/01/>.
- [108] Arlee V. Smith et al. “Optical Damage Limits to Pulse Energy From Fibers”. In: *IEEE Journal of Selected Topics in Quantum Electronics* 15.1 (Jan. 2009), 153–158. ISSN: 1077-260X. DOI: [10.1109/jstqe.2008.2010331](https://doi.org/10.1109/jstqe.2008.2010331). URL: <http://dx.doi.org/10.1109/JSTQE.2008.2010331>.
- [109] Jialei Su et al. “Quantifying the Upper Limit of Backflash Attack in Quantum Key Distribution”. In: (Jan. 2025). arXiv: [2501.09984](https://arxiv.org/abs/2501.09984) [quant-ph].
- [110] Kiyoshi Tamaki et al. “Loss-tolerant quantum cryptography with imperfect sources”. In: *Physical Review A* 90.5 (Nov. 2014). ISSN: 1094-1622. DOI: [10.1103/physreva.90.052314](https://doi.org/10.1103/physreva.90.052314). URL: <http://dx.doi.org/10.1103/PhysRevA.90.052314>.
- [111] Yan-Lin Tang et al. “Source attack of decoy-state quantum key distribution using phase information”. In: *Physical Review A* 88.2 (Aug. 2013). ISSN: 1094-1622. DOI: [10.1103/physreva.88.022308](https://doi.org/10.1103/physreva.88.022308). URL: <http://dx.doi.org/10.1103/PhysRevA.88.022308>.
- [112] Armin Tavakoli et al. “Semidefinite programming relaxations for quantum correlations”. In: *Reviews of Modern Physics* 96.4 (Dec. 2024). ISSN: 1539-0756. DOI: [10.1103/revmodphys.96.045006](https://doi.org/10.1103/revmodphys.96.045006). URL: <http://dx.doi.org/10.1103/RevModPhys.96.045006>.
- [113] Andrey Tayduganov et al. “Optimizing the deployment of quantum key distribution switch-based networks”. In: *Optics Express* 29.16 (July 2021), p. 24884. ISSN: 1094-4087. DOI: [10.1364/oe.427804](https://doi.org/10.1364/oe.427804). URL: <http://dx.doi.org/10.1364/OE.427804>.
- [114] ThinkQuantum. *QUKY - Quantum Key Distribution Platform*. <https://www.thinkquantum.com/quky/>. 2021.
- [115] Marco Tomamichel et al. “Tight finite-key analysis for quantum cryptography”. In: *Nature Communications* 3.1 (Jan. 2012). ISSN: 2041-1723. DOI: [10.1038/ncomms1631](https://doi.org/10.1038/ncomms1631). URL: <http://dx.doi.org/10.1038/ncomms1631>.
- [116] Alberto De Toni et al. *Countermeasures for Trojan-Horse Attacks on self-compensating all-fiber polarization modulator*. 2025. arXiv: [2510.16868](https://arxiv.org/abs/2510.16868) [quant-ph]. URL: <https://arxiv.org/abs/2510.16868>.
- [117] Alberto De Toni et al. *Long-term analysis of efficient-BB84 4-node network with optical switches in metropolitan environment*. 2025. arXiv: [2510.16867](https://arxiv.org/abs/2510.16867) [quant-ph]. URL: <https://arxiv.org/abs/2510.16867>.
- [118] Daniil Trefilov et al. “Intensity correlations in decoy-state BB84 quantum key distribution systems”. In: *Optica Quantum* 3.5 (Sept. 2025), p. 417. ISSN: 2837-6714. DOI: [10.1364/opticaq.549690](https://doi.org/10.1364/opticaq.549690). URL: <http://dx.doi.org/10.1364/OPTICAQ.549690>.
- [119] Sangita Tripathy, Kriti Tyagi, and Pratiksha Pratap. “A comprehensive study of various superconductors for superconducting nanowire single photon detectors applications”. In: *iScience* 27.10 (2024), p. 110779. ISSN: 2589-0042. DOI: <https://doi.org/10.1016/j.isci.2024.110779>. URL: <https://www.sciencedirect.com/science/article/pii/S2589004224020042>.
- [120] Artem Vakhitov, Vadim Makarov, and Dag R. Hjølme. “Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography”. In: *Journal of Modern Optics* 48.13 (Nov. 2001), 2023–2038. ISSN: 1362-3044. DOI: [10.1080/09500340108240904](https://doi.org/10.1080/09500340108240904). URL: <http://dx.doi.org/10.1080/09500340108240904>.
- [121] Gilles Van Assche. *Quantum Cryptography and Secret-Key Distillation*. Cambridge: Cambridge University Press, 2006. DOI: [10.1017/CB09780511617744](https://doi.org/10.1017/CB09780511617744).

- [122] Kannan Vijayadharan et al. “A Sagnac-based arbitrary time-bin state encoder for quantum communication applications”. In: *arXiv preprint arXiv:2506.08971* (2025).
- [123] Arun Viswanathan, Eric C. Rosen, and Ross Callon. *Multiprotocol Label Switching Architecture*. RFC 3031. Jan. 2001. doi: [10.17487/RFC3031](https://doi.org/10.17487/RFC3031). URL: <https://www.rfc-editor.org/info/rfc3031>.
- [124] Shuang Wang et al. “Twin-field quantum key distribution over 830-km fibre”. In: *Nature Photonics* 16.2 (Jan. 2022), 154–161. issn: 1749-4893. doi: [10.1038/s41566-021-00928-2](https://doi.org/10.1038/s41566-021-00928-2). URL: <http://dx.doi.org/10.1038/s41566-021-00928-2>.
- [125] Ze-Xu Wang et al. “10 GHz robust polarization modulation towards high-speed satellite-based quantum communication”. In: *EPJ Quantum Technology* 12.1 (2025), p. 47.
- [126] Christian Weedbrook et al. “Gaussian quantum information”. In: *Reviews of Modern Physics* 84.2 (May 2012), 621–669. issn: 1539-0756. doi: [10.1103/revmodphys.84.621](https://doi.org/10.1103/revmodphys.84.621). URL: <http://dx.doi.org/10.1103/RevModPhys.84.621>.
- [127] W. Wootters W. Zurek. “A single quantum cannot be cloned”. In: *Nature* 299 (1982), 802–803. doi: <https://doi.org/10.1038/299802a0>.
- [128] Xiulai Xu, D. A. Williams, and J. R. A. Cleaver. “Electrically pumped single-photon sources in lateral p-i-n junctions”. In: *Applied Physics Letters* 85.15 (2004), pp. 3238–3240. doi: [10.1063/1.1803624](https://doi.org/10.1063/1.1803624). eprint: <https://doi.org/10.1063/1.1803624>.
- [129] Hua-Lei Yin et al. “Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber”. In: *Physical Review Letters* 117.19 (2016). issn: 1079-7114. doi: [10.1103/physrevlett.117.190501](https://doi.org/10.1103/physrevlett.117.190501).
- [130] Juan Yin et al. “Satellite-based entanglement distribution over 1200 kilometers”. In: *Science* 356.6343 (June 2017), 1140–1144. issn: 1095-9203. doi: [10.1126/science.aan3211](https://doi.org/10.1126/science.aan3211). URL: <http://dx.doi.org/10.1126/science.aan3211>.
- [131] Huaixiu Zheng, Daniel Gauthier, and Harold Baranger. “Decoy-State Quantum Key Distribution with Nonclassical Light Generated in a One-dimensional Waveguide”. In: *Optics letters* 38 (Mar. 2013), pp. 622–4. doi: [10.1364/OL.38.000622](https://doi.org/10.1364/OL.38.000622).