Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione

Corso di Dottorato in Ingegneria dell'Informazione
Scienza e tecnologia dell'Informazione

XXXII Ciclo

Practical and secure quantum randomness generation and communication

Supervisore:
Prof. Giuseppe Vallone

Coordinatore:
Prof. Andrea Neviani

Dottorando: Marco Avesani

How dare we speak of the laws of chance?
Is not chance the antithesis of all law?
— Joseph Bertrand

Abstract

Quantum mechanics has profoundly revolutionized the field of physics and our understanding of nature. Many effects predicted by quantum mechanics and with no classical analog such as wave-particle duality, the coherent superposition of quantum states, the uncertainty principle, entanglement, and non-locality, are in deep contrast with our general common sense and yet they survived to any experimental verification. Interestingly, when these peculiar quantum effects are studied within the framework of Information Theory, they provide advantages for tasks such as computation, communication, and cryptography.

This thesis work studies how quantum resources can be exploited to develop and implement practical protocols for secure communication and private randomness generation. In particular, the work is focused on those protocols that offer an optimal compromise between security and performances and that are realizable with the current technology.

The thesis is divided into three main sections: in the first introductory section, Chapter 1 describes some basic notions about quantum mechanics and quantum information theory.

The second section is entirely focused on the study of private and secure randomness generation with quantum resources. In particular, Semi-Device-Independent protocols are studied since they provide a high level of security without scarifying performances.

Chapter 2 describes the general framework of quantum random number generation (QRNG), the different types of quantum random number generators, comparing their pro and cons. Then it gives a brief introduction to the different entropy measures that will be considered in the thesis. Finally, it describes the steps and procedures needed to analyze the security of any quantum random number generation protocol.

Chapter 3 describes a new Source-Device-Independent (Source-DI) protocol for quantum random number generation. The protocol exploits the quadratures of the electromagnetic field and the structure of the POVM implemented by heterodyne detection to generate private and secure random numbers. In the first section it is described the theoretical working principle, and the security is proved against general attacks. Then the actual experimental

fiber implementation is described together with the post-processing procedure. In Section 3, the results are presented, showing that with this protocol it is possible to achieve secure generation rates up to 17.4 Gbps, the current record for this type of generators. Finally, some ongoing work related to the real-time operation and the miniaturization of the prototype are discussed.

In this work I've contributed to the design of both the protocol and the experiment. I've contributed to the experimental implementation, to the data analysis, to the security proof and to the writing of the manuscript [1].

Chapter 4 describes a new numerical tool for the analysis of the security of both trusted and Source-DI QRNG. The tool exploits a new formulation of the conditional quantum min-entropy for systems with unknown states but trusted measurement. This new formulation is expressed as a Semidefinite optimization problem, and both the primal and dual forms are analytically derived. Finally the results of this new method are first compared to scenarios where tight bound are known and then to scenarios where only suboptimal bound are known. In the first case compatible results are obtained, while in the second case the new method retrieves significantly higher rates.

In this work I've contributed to the development of the alternative SDP formulation for the min-entropy. I've written the software that performs the optimization and I've performed all the simulations. I've contributed to the writing of the manuscript, which will be be sent soon to an e-print server.

Chapter 5 describes a new protocol to certify, in a Source-DI way, unbounded randomness from finite-dimensional quantum systems. In particular, the first section describes the advantages offered by POVM respect to projective measurements for the certification of randomness. Then the tool described in Chap 4 is employed to derive tight bounds on the secure generation rates for POVM with different structures. Then, thanks to the numerical results, an analytic bound (that coincides with the numeric one) is derived for some symmetric POVM. Finally, the last section describes the experimental implementation of the protocol with an heralded single-photon source and symmetric POVM with 3,4 and 6 outcomes. In all the cases the results are compatible with the theory and show the exact scaling as a function of the number of POVM elements, showing that in the limit of infinite outcomes, unbounded randomness generation is possible

In this work I've contributed to the design of both the protocol and the experiment. I've contributed to the security proof and to the numerical simulations. I've contributed to the experimental realization of the setup, to the data analysis and to the writing of the manuscript, which will be be sent soon to an e-print server.

Chapter 6 describes a new implementation for a Semi-DI QRNG protocol. The protocol does not make any assumption on the source or the measurement device but assumes a lower-bound on the overlap between the emitted states. Here, the general protocol is described, and a new implementation with heterodyne detection is discussed. The main

advantage of such implementation is that relaxes the requirement of an active phase stabilization, which can be compensated in post-processing. The second section analyzes the security and the expected rate for this configuration, while the next section describes the experimental implementation with fiber optical components. In the last section, the results are presented, showing that, despite a finite amount of noise and a non-perfect efficiency of the detectors, randomness can be extracted and the results are compatible with a model that takes into account the inefficiencies.

In this work I've contributed to the design of both the protocol and the experiment. I've contributed to the numerical simulations of the Heterodyne SDI implementation. I've contributed to the experimental realization of the setup, to the FPGA programming, to the data analysis and to the writing of the manuscript, which will be be sent soon to an e-print server.

Then the third and last section is focused on the experimental implementation of quantum communication protocols, in particular, Quantum Key Distribution.

Chapter 8 describes the design and experimental implementation of a complete prototype for daylight free-space QKD at telecom wavelength. The prototype, developed in collaboration with the Italian Space Agency (ASI), has been tested with two transmitters: a fiber-based one, realized with only commercial components and a second one, developed in collaboration with Scuola Sant'Anna di Pisa, that exploits the Silicon Photonics technology. The prototype also features a single mode fiber injection system and superconducting nanowire single-photon detectors. It has been tested in a 145m long free space link in the urban area of Padova, demonstrating for both the sources, a successful daylight free-space QKD run at telecom wavelength. This prototype is the first step towards the development of a complete QKD system for satellite applications.

In this work I've contributed to the design of the whole experiment. I've contributed to the building of the discrete QKD source and to the characterization of the integrated source. I've contributed to the electronic front-end of both sources and to the experimental implementation of the QKD analyzer. I've contributed to the software that controls the state analyzer. I've participated to the field test and I've contributed to the writing of the manuscript [2]

Chapter 9 describes a new fiber-based polarization encoder for QKD. The encoder is characterized by a Sagnac geometry that greatly improves the stability of the modulator and reduces the required driving power. The first section describes the working principle of the encoder, and then the experimental implementation at 800nm is presented. The experimental results indeed show high stability and a low intrinsic error.

In this work I've contributed to the design of the QKD transmitter and to the experimental realization. I've contributed to the data analysis and to the writing of the manuscript [3].

Chapter 10 describes a new synchronization method for QKD that does not require any auxiliary time reference. The method works by sending a shared public qubit sequence at

pre-established times. Moreover, the public qubit sequence can also be used to compensate fluctuations of the channel and align in real-time the polarization reference frames of the two users. After describing the setup, based on the POGNAC transmitter, the self-synchronization working principle is explained and its robustness to noise is discussed. Then, the last section describes the experimental results, showing a record-low intrinsic QBER for the POGNAC transmitter and an high robustness of the self-synchronization method with respect to losses.

In this work I've contributed to the design of the experiment and to the experimental realization. I've contributed to the data analysis and to the writing of both manuscripts. [4, 5]

Finally, Chapter 11 describes the implementation of a Bell test based on time-bin entanglement, which is not affected by the detection loophole. The first section describes a theoretical analysis of time-bin entanglement schemes and their description with the language of POVM operators. Then the experimental implementation, based on fast optical switches controlled by a PID feedback loop is presented. Finally, the results show that the presented method is able to obtain a Bell violation that is not affected by the post-selection loophole.

In this work I've mainly contributed to the electronic fronted of the experiment and to the realization of the PID controller. I've contributed to the writing of the manuscript [6].

Sommario

La meccanica quantistica ha profondamente rivoluzionato il campo della fisica e la nostra comprensione della natura. Molti effetti previsti dalla meccanica quantistica e senza analoghi classici, come la dualità onda-particella, la sovrapposizione coerente degli stati quantistici, il principio di incertezza, l'entanglement e la non-località, sono in profondo contrasto con il nostro senso comune ma tuttavia sono sopravvissuti a qualsiasi verifica sperimentale. È interessante notare che, quando questi effetti quantistici peculiari sono studiati nel quadro della Teoria dell'Informazione, offrono vantaggi per compiti come il calcolo, la comunicazione e la crittografia.

Questo lavoro di tesi studia come le risorse quantistiche possono essere sfruttate per sviluppare e implementare protocolli pratici per la comunicazione sicura e la generazione di numeri casuali privati. In particolare, il lavoro è focalizzato su protocolli che offrono un compromesso ottimale tra sicurezza e prestazioni e che sono realizzabili con la tecnologia attuale.

La tesi è divisa in tre sezioni principali: nella prima sezione introduttiva, il capitolo 1 descrive alcune nozioni di base sulla meccanica quantistica e sulla teoria dell'informazione quantistica.

La seconda sezione è interamente focalizzata sullo studio della generazione di numeri casuali privati e sicuri, sfruttando risorse quantistiche. In particolare, sono stati studiati i protocolli Semi-Device-Independent, in quanto forniscono un alto livello di sicurezza senza sacrificare le prestazioni.

Il capitolo 2 descrive il framework generale della generazione quantistica di numeri casuali, i diversi tipi di generatori di numeri casuali quantistici, confrontando i loro pro e contro. Poi vengono brevemente introdotti i diversi tipi di entropie che saranno considerate nella tesi. Infine, viene descritta la procedura per analizzare la sicurezza di qualsiasi protocollo quantistico di generazione di numeri casuali.

Il capitolo 3 descrive un nuovo protocollo Source-Device-Independent (Soruce-DI) per la generazione quantistica di numeri casuali. Il protocollo sfrutta le quadrature del campo elettromagnetico e la struttura del POVM implementato dalla misura eterodina per generare numeri casuali privati e sicuri. Nella prima sezione è descritto il principio di funzionamento teorico e la sicurezza è dimostrata contro gli attacchi generali. Quindi l'effettiva implementazione sperimentale della fibra viene descritta insieme alla procedura di post-elaborazione. Nella sezione 3, i risultati sono presentati, dimostrando che con questo protocollo è possibile raggiungere un rate di generazione sicura fino a 17,4 Gbps, il record per questo tipo di generatori. Infine, vengono infine discussi alcuni lavori in corso relativi al funzionamento in real-time e alla miniaturizzazione del prototipo.

In questo lavoro ho contribuito alla progettazione sia del protocollo che dell'esperimento. Ho contribuito all'implementazione sperimentale, all'analisi dei dati, alla prova di sicurezza e alla scrittura del manoscritto [1]

Il capitolo 4 descrive un nuovo strumento numerico per l'analisi della sicurezza dei QRNG "trusted" e Source-DI. Lo strumento sfrutta una nuova formulazione della quantum conditional min-entropy per sistemi con stati sconosciuti ma misure caratterizate. Questa nuova formulazione è espressa come un problema di ottimizzazione semi-definita positiva e sia la forma primaria che la duale sono derivate analiticamente. Infine, i risultati di questo nuovo metodo vengono prima confrontati con gli scenari in cui è noto un limite "tight" e quindi con gli scenari in cui sono noti solo limiti non ottimali. Nel primo caso si ottengono risultati compatibili, mentre nel secondo caso il nuovo metodo è in grado di ottenere rate significativamente più elevati.

In questo lavoro ho contribuito allo sviluppo della formulazione SDP alternativa per la min-entropy. Ho scritto il software che esegue l'ottimizzazione e ho eseguito tutte le simulazioni. Ho contribuito alla scrittura del manoscritto, che sarà inviato presto a un server di e-print.

Il capitolo 5 descrive un nuovo protocollo per certificare, in modo Source-DI, una quantità illimitata di casualità dai sistemi quantistici a dimensione finita. In particolare, la prima sezione descrive i vantaggi offerti da POVM rispetto alle misurazioni proiettive per la certificazione della casualità. Quindi viene impiegato lo strumento descritto in nel capitolo 4 per ricavare limiti inferiori sul tasso di generazione sicura, per POVM con diverse strutture. Quindi, grazie ai risultati numerici, viene derivato un limite analitico (che coincide con quello numerico) per alcuni POVM simmetrici. Infine, l'ultima sezione, descrive l'implementazione sperimentale del protocollo con una sorgente a singolo fotone "heralded" e POVM simmetrici con 3,4 e 6 uscite. In tutti i casi i risultati sono compatibili con la teoria e mostrano l'esatto trend in funzione del numero di elementi POVM, dimostrando che nel limite di infiniti elementi, è possibile una generazione di casualità illimitata.

Il capitolo 6 descrive una nuova implementazione di un protocollo QRNG Semi-DI. Il protocollo non fa alcuna assunzione sulla sorgente o sul dispositivo di misura, ma presuppone un limite inferiore sulla sovrapposizione tra gli stati emessi. Nella prima sezione viene

descritto il protocollo generale e viene discussa una nuova implementazione con misura eterodina. Il vantaggio principale di tale implementazione è che rilassa il requisito di una stabilizzazione di fase attiva, che può essere compensata nella fase di post-elaborazione. La seconda sezione analizza la sicurezza e le prestazioni attese per questa configurazione, mentre la sezione successiva descrive l'implementazione sperimentale con componenti in fibra ottica. Nell'ultima sezione vengono presentati i risultati, dimostrando che, nonostante vi sia una quantità non nulla di rumore e un'efficienza non perfetta dei rivelatori, la casualità può essere estratta e i risultati sono compatibili con un modello che tiene conto delle inefficienze.

Poi la terza e ultima sezione si concentra sull'implementazione sperimentale dei protocolli di comunicazione quantistica, in particolare la distribuzione delle chiavi quantistiche.

Il capitolo 8 descrive la progettazione e l'implementazione sperimentale di un prototipo completo per la QKD in spazio libero che utilizza fotoni a 1550nm. Il prototipo, sviluppato in collaborazione con l'Agenzia Spaziale Italiana (ASI), è stato testato con due trasmettitori: uno basato su componenti in fibra e realizzato con solo componenti commerciali e un secondo, sviluppato in collaborazione con Scuola Sant'Anna di Pisa, che sfrutta la tecnologia della fotonica integrata in silicio. Il prototipo dispone anche di un sistema di iniezione in fibra a singolo modo e di rilevatori di singoli fotoni superconduttori. È stato testato in un collegamento in spazio libero lungo 145 metri nell'area urbana di Padova, dimostrando per entrambe le sorgenti, un risultato positivo. Questo prototipo è il primo passo verso lo sviluppo di un sistema QKD completo per applicazioni satellitari.

Il Capitolo 9 descrive un nuovo trasmettitore per QKD capace di modulare la polarizzazione dei singoli fotoni. Il trasmettitore è caratterizzato da un interferometro di Sagnac che migliora notevolmente la stabilità del modulatore e riduce la potenza richiesta per la modulazione. La prima sezione descrive il principio di funzionamento del trasmettitore e quindi viene presentata l'implementazione sperimentale con luce a 800nm. I risultati sperimentali mostrano un'elevata stabilità e un basso errore intrinseco.

Il capitolo 10 descrive un nuovo metodo di sincronizzazione per QKD che non richiede alcun riferimento temporale ausiliario. Il metodo funziona inviando una sequenza di qubit pubblica e condivisa a tempi prestabiliti. Inoltre, la sequenza di qubit pubblici può essere utilizzata anche per compensare le fluttuazioni del canale e allineare in tempo reale i sistemi di riferimento della polarizzazione dei due utenti. Dopo aver descritto la configurazione, basata sul trasmettitore POGNAC, viene spiegato il principio di funzionamento dell'autosincronizzazione e viene discussa la sua resilienza al rumore. Quindi, l'ultima sezione descrive i risultati sperimentali, mostrando un QBER intrinseco da record per il trasmettitore POGNAC e un'elevata robustezza del metodo di autosincronizzazione rispetto alle perdite.

Infine, il capitolo 11 descrive l'implementazione di un test di Bell basato sull'entanglement in time-bin, non influenzato dal post-selection loophole. La prima sezione descrive un'analisi teorica degli schemi di entanglement time-bin e la loro descrizione con il linguaggio degli operatori POVM. Quindi viene presentata l'implementazione sperimentale, basata su switch

ottici veloci controllati da un sistema di feedback PID. Infine, i risultati mostrano che il metodo presentato è in grado di ottenere una violazione Bell che non è influenzato dal post-selection loophole.

Contents

Part I

Introduction

CHAPTER 1

Introduction to Quantum Information

In this chapter we will present some introductory notions about Quantum Mechanics and Quantum Information, that will be used in the thesis.

The content of the following chapter is based on standard textbooks covering Quantum Mechanics, Quantum Information, Quantum Optics and Classical Information Theory [7–13].

1.1 Postulates of Quantum Mechanics

Quantum Mechanics has proven to be an incredibly powerful theory for predicting the behavior of particles in their microscopic world. Like any other physical theory, it provides a mathematical framework to represent mathematically physical objects, the laws that these objects obey, and a set of rule for computing the probabilities of certain events. The entire framework is based upon some fundamental postulates, developed mostly by Dirac and von Neumann, that provide a deep link between fundamental physical entities and their mathematical formulation. Since they cannot be derived by other principles, these postulates have been formulated from experimental observations.

The postulates of quantum mechanics can be expressed as:

1. **States**: The set of states of an isolated physical system is in one-to-one correspondence to the projective space of a Hilbert $\mathscr{H} \simeq \mathbb{C}^d$ space of dimension d. In particular, any physical state can be represented by a normalized ray vector $|\psi\rangle \in \mathscr{H}$, using the Dirac notation. Thus all the vectors $e^{i\phi}|\psi\rangle$ differing from $|\psi\rangle$ by a phase factor are mapped to the same physical state. It's worth noting that, being $\mathscr{H}$ a vector space, linear combinations of vectors are also states, allowing the phenomenon of *superposition*.

2. **Evolution**: The evolution of an isolated physical system with state space $\mathscr{H}$ is described by an unitary transformation $\hat{U}$. For any fixed time interval $[t_0, t_1]$ there exists

a unitary $U(t_0, t_1)$, unique up to a phase factor, describing the mapping of states $|\psi(t_0)\rangle$ at time t_0 to

$$|\psi(t_1)\rangle = \hat{U}(t_0, t_1)\,|\psi(t_0)\rangle \tag{1.1}$$

at time t_1.

3. **Observables:**: Any physical property of a system that can be measured is an observable and all observables are represented by self-adjoint linear operators acting on the state space $\mathscr{H}$. Each eigenvalue x of an observable $\hat{O}$ corresponds to a possible value of the observable. Since $\hat{O}$ is self-adjoint, it takes the form

$$O = \sum_x x\hat{\Pi}_x \tag{1.2}$$

where Π_x is a projector operator ($\hat{\Pi}_x^2 = \hat{\Pi}_x$) onto the subspace with eigenvalue x.

4. **Measurements**: The measurement of an observable $\hat{O}$ yields an eigenvalue x of its spectrum. If the system is in state $|\psi\rangle$ just before the measurement, then the probability of observing outcome x is given by the Born rule

$$P_X(x) = \mathrm{Tr}\left[\hat{\Pi}_x\,|\psi\rangle\,\langle\psi|\right] \tag{1.3}$$

where $\langle\psi|$ is the dual of $|\psi\rangle$. The state just after the measurement, conditioned on the result x of the measurement is given by:

$$\left|\psi^{'}\right\rangle = \sqrt{\frac{1}{P_X(x)}}\hat{\Pi}_x\,|\psi\rangle \tag{1.4}$$

5. **Composite systems**: The composite state space $\mathscr{H}$ of n systems with state space $\mathscr{H}_i$ is isomorphic to the tensor product

$$\mathscr{H} = \bigotimes_{i=1}^{n} \mathscr{H}_i \tag{1.5}$$

If the single systems are in a state $|\psi_i\rangle \in \mathscr{H}_\rangle$ the joint state is:

$$|\Psi\rangle = \bigotimes_{i=1}^{n} |\psi_i\rangle \in \mathscr{H} \tag{1.6}$$

1.2 Quantum Information's basic block: the Qubit

In information theory and in computer science the basic building block is the bit. This is a mathematical construct, a Boolean variable, that can assume only one of two possible values and can be implemented in any physical two-state system. For example, can be implemented in the position of a mechanical or electronic switch, in two different voltage levels, in the intensity, wavelength or polarization of light, two directions of magnetization of a ferromagnetic material and a numerous of others incredible ways.

All the modern world is based on the bit: electronic, computation, digital communication are just an example of the applications that rely on the concept of bits. The main characteristic of the bit is the mutual exclusivity of the values it can assume: in any moment the value of the bit is either 1 or 0.
When one is dealing with quantum mechanical system, however, a way richer phenomenology is possible.
In fact is possible to build the quantum version of bit, the qubit, using a two level quantum mechanical system. Unlike the bit, quantum mechanics tell us is that the qubit can be in a linear *superposition* of $|0\rangle$ and $|1\rangle$, the two possible outcomes of a measure. Thus the most general state the system can assume can be written as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{1.7}$$

The state of a qubit is a vector in a two-dimensional complex vector space. The special states $|0\rangle$ and $|1\rangle$ are known as computational basis states and form an orthonormal basis for this vector space. However, like the bit, the outcomes of a measurement performed on the qubit can be only one of the two states of the computational basis and this, in the case of a state in the form given by Eq 1.7, happens with probability α^2 for $|0\rangle$ and β^2 for $|1\rangle$. The normalization condition for probabilities implies that $|\alpha|^2 + |\beta|^2 = 1$, and so $|\psi\rangle$ is a vector of unitary length. With the above condition, Equation 1.7 can be written as:

$$|\psi\rangle = e^{i\eta}\left(\cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\right) \tag{1.8}$$

$$\theta \in [0,\pi] \quad \phi \in [0,2\pi] \tag{1.9}$$

where η is a global phase, carrying no information about the state, since physical states are described by ray vectors on a Hilbert space. This reformulation is useful because permits to express the state of a qubit in function of two angles, θ and ϕ representing a point on the surface of a three dimensional sphere called the Bloch sphere. This graphical representation is handy when one is working with qubit.

This representation is useful to catch a fundamental difference between the bit and the qubit. While the bit can assume only two different and discrete values, the qubit can represent an infinite continuous set of states, spanning all over the surface of the sphere: this means that infinite information can be represented by the qubit. However, whenever we try to access to the information, by measuring it, we change the state of the qubit, making its state to collapse into one of the eigenstates. How can we use the qubit as a resource if we destroy its fundamental property at the moment we are reading it?
The answer is that, even if we cannot access the qubit, we can perform unitary operations on it preserving *all* the information it contains. This is the power of quantum computation. Moreover, the qubit is a quantum mechanical system and must obey to the laws of quantum mechanics that, as we are going to see, forbids or provides an advantage on some tasks performed on the qubit, respect the classical predictions. But how we can realize a qubit in practice?
As already said any quantum two level system could be used as a qubit: the states of an electron in an atom, the nuclear spin in a uniform magnetic field, the polarization of a photon are just few examples of the physical realizations of a qubit system. One of the most

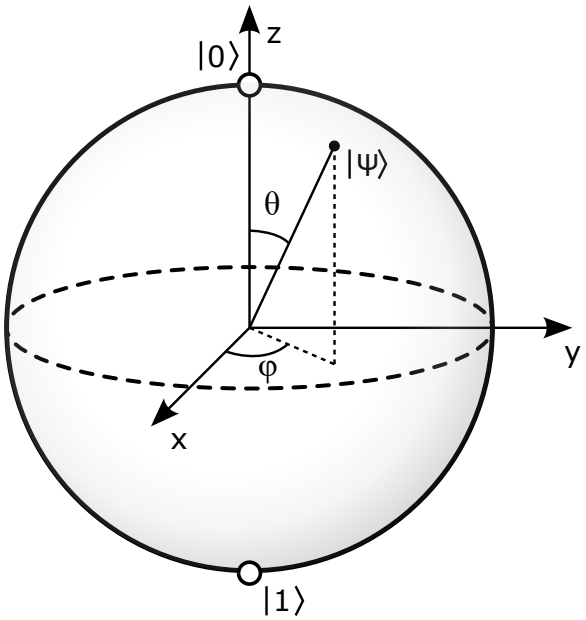


Figure 1.1: *Representation of the Bloch sphere*

widely used implementation is trough single photon's polarization: here $|0\rangle$ and $|1\rangle$ can be the horizontal and vertical polarization of the photon.

1.3 No-cloning theorem

Quantum mechanics, from the beginning, caused a sort of shock and surprise, mining the fundamental conception of how nature was believed to work. Many predictions were in contrast with the common sense, so used to the macroscopic world ruled by the laws of classical physics. One of these strange effects predicted by quantum mechanics, that is of absolute importance in quantum information theory and cryptography, is linked to the action of copy. Copy of information is performed every day: fax, photocopiers, scanners but also copies on CD, DVD or USB-keys. All of these actions are so normal in our classical world that the hypothesis that copy is forbidden in the quantum world seems absurd. Quantum mechanics, however, states that it is impossible to create a perfect quantum cloning machine and the formalization of this idea is enclosed in the No-cloning theorem [14].
Suppose to have a quantum system A in a pure state $|\psi\rangle_A$ that belongs to a generic Hilbert space $\mathscr{H}$. Now if we want to copy that state, what we need is another system B described by a pure state $|e\rangle_B$ that belongs to the same Hilbert space $\mathscr{H}$. The initial state of this composite system can be described by

$$|\psi\rangle_A \otimes |e\rangle_B \tag{1.10}$$

The operation of copy can be represented by a unitary operator U such that:

$$U(|\psi\rangle_A \otimes |e\rangle_B) = |\psi\rangle_A \otimes |\psi\rangle_B \ \ \forall\psi \tag{1.11}$$

Since it must be valid for all ψ we can require that:

$$\begin{aligned} U(|\psi\rangle_A \otimes |e\rangle_B) &= |\psi\rangle_A \otimes |\psi\rangle_B \\ U(|\phi\rangle_A \otimes |e\rangle_B) &= |\phi\rangle_A \otimes |\phi\rangle_B \end{aligned} \tag{1.12}$$

Taking the inner product of the two equations and remembering that U must preserve the inner product we have:

$$\langle\phi|\psi|\phi|\psi\rangle = |\langle\phi|\psi|\phi|\psi\rangle|^2 \tag{1.13}$$

which is satisfied only in the case $|\psi\rangle = |\phi\rangle$ or for $|\psi\rangle$ orthogonal to $|\phi\rangle$.
These few lines are describing a stunning and central feature of quantum systems: a quantum cloning machine that can clone an unknown arbitrary quantum system can't be built. However if we relax the requests and we admit also imperfect copies, an universal quantum machine is possible and can reach a fidelity $\mathcal{F} = 5/6$ [15]. This is the key point that assures security in many quantum cryptography protocols: if information is encoded in a single quantum system, and this system is transmitted, this cannot be copied without introducing errors, thus revealing the presence of a possible eavesdropper.

1.4 Density matrix formalism

The formalism introduced until now has only dealt with vectors in the state space $\mathcal{H}$ and unitary evolution. These vectors, called *pure states*, represents a physical system whose state is completely known. However, if the system under consideration is not isolated and interacts with an unknown system, or, more generally, if the state is not perfectly known, we deal with *mixed states*, that are a statistical mixture of pure states. More precisely, if the state of the system under consideration can be in the state $|\psi_i\rangle$ with probability p_i we can describe it as:

$$\hat{\rho} = \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{1.14}$$

where $\hat{\rho}$ now is a linear operator, usually called *density matrix*. Any *convex* combination of two density matrix $\hat{\rho}, \hat{\sigma}$, $\hat{\tau} = (\lambda\hat{\rho} + (1-\lambda\hat{\sigma}))$, with $\lambda \in [0,1]$ is also a density matrix.

This formulation is equivalent to the state vector formulation but usually is handier when dealing with mixed states. Moreover it also removes the asymmetry between states, that were represented as vector, and operators that were represented as matrices. From another perspective, a linear operator $\hat{\rho}$ is a density matrix if it fulfills the following conditions

- Unit trace: $\mathrm{Tr}[\hat{\rho}] = 1$
- Semidefinite positive: $\mathrm{Tr}[\hat{\rho}|\psi\rangle\langle\psi|] \geq 0 \ \ \forall |\psi\rangle \in \mathcal{H}$

Moreover, the associated state is pure if its *rank* is 1. Equivalently,

$$\mathrm{Tr}\left[\hat{\rho}^2\right] = 1 \tag{1.15}$$

The previously defined postulates of Quantum Mechanic can be also reformulated in the density matrix formalism. In fact if the evolution of the state vector is defined by Eq. 1.1

then:

$$\hat{\rho}(t_1) = \sum_i p_i |\psi_i(t_1)\rangle \langle\psi_i(t_1)| = \sum_i p_i |\psi_i(t_0)\rangle \hat{U}(t_0,t_1) \langle\psi_i(t_0)| \hat{U}^\dagger(t_0,t_1) \tag{1.16}$$

$$= \hat{U}(t_0,t_1)\hat{\rho}(t_0,t_1)\hat{U}^\dagger(t_0,t_1) \tag{1.17}$$

Similarly, for measurements the Born rule 1.3 becomes:

$$P_X(x) = \mathrm{Tr}\left[\hat{\Pi}_x \hat{\rho}\right] \tag{1.18}$$

and the state after measuring with outcome x is given by:

$$\hat{\rho}_x = \frac{\hat{\Pi}_x \hat{\rho} \hat{\Pi}_x}{P_X(x)} \tag{1.19}$$

This new formulation comes helpful to describe the state of the system after a measurement if the outcome is unknown. In this case the system could be in any of the post-measurement states $\hat{\rho}_x$ with probability $P_X(x)$

$$\hat{\rho}_{PM} = \sum_x P_X(x)\hat{\rho}_x = \hat{\Pi}_x \hat{\rho} \hat{\Pi}_x \tag{1.20}$$

Pure states, being an element of a vector space $\mathscr{H}$, can be found in a coherent superposition, which is a purely quantum phenomenon. This peculiar property is often at the basis of the advantage of many quantum protocols and algorithm respect their classical counterpart. However, the formalism of QM should be able to describe also "classical" states. Consider a classical random variable Z distributed according to P_Z, this can be represented by the state:

$$\hat{\rho}_c = \sum_Z P_Z |z\rangle \langle z| \tag{1.21}$$

with $\{|z\rangle\}$ an orthonormal basis in $\mathscr{H}_Z$. Since all the $|i\rangle$ are orthogonal to each other, these are the only states the system can be found in, and they behave like the usual classical states.

An hybrid class of states, which is extremely important for the analysis of the security of Quantum Protocols is given by the *Classical-Quantum states*:

$$\hat{\rho}_{ZE} = \sum_z P_Z |z\rangle \langle z| \otimes \hat{\rho}_z^E \tag{1.22}$$

where $\{|z\rangle\}$ an orthonormal basis in $\mathscr{H}_Z$ and $\hat{\rho}_z^E$ are density operator in $\mathscr{H}_E$. Usually, these states arise when a joint state $\hat{\rho}_{AE} \in \mathscr{H}_A \otimes \mathscr{H}_E$ is locally measured in the system A, but the outcome is unknown. In this case the reduced quantum state $\hat{\rho}_z^E$ contains information about the quantum correlation between the two systems A and E.

1.5 Local realism, Entanglement and Bell inequalities

In the previous sections, we saw how Quantum Mechanics describes effects that are in contrast with our common sense and our expectation. But quantum mechanics attacked even

deeper aspects that were thought to belong to nature: reality and locality.
Reality states that the physical properties of objects exist in a defined state independently on the observation. This is clearly true for classical physics, but it can't be said for QM since QM gives us the probability to measure a certain state and moreover predicts that the value of two non-commuting operators cannot be simultaneously determined. Locality, on the other end, states that two space-like separated events must be independent. Again QM predicts that a system of entangled particles can share correlations that are non-local, apparently violating the principle of locality. Historically these two principles were thought so fundamental that was a common opinion believe that law of physics had to at both: any complete physical theory must be consistent with local realism. For sure this was the opinion of Einstein, Podolsky and Rosen which in 1935 published a ground-breaking article [16], where they showed that, if both reality and locality principles are assumed, quantum mechanics must be incomplete and that some "hidden variables" must be included in the theory in order to make it complete.
But is this hidden-variable model just another reformulation of quantum mechanics or it can be tested in some way? The answer to this question was given in 1964 by John Bell in [17]. In his remarkable work, he showed that any local hidden variable theory has a bound on the correlation experienced on space-like separated particles, and this bound can be calculated and tested experimentally. This limitation can be express in the form of an inequality: the expectation value of some observables of the two particles must be below a certain threshold in the case of a local hidden variable theory. If experiments are performed, and value higher of this bound are obtained, this means that nature cannot be described by such set of theories.
After few years experiments started to tests Bell's predictions, starting with the one by Freedman in 1972 [18], and then by Aspect in 1981,1982 [19] [20]. The reported results were well beyond the bound predicted by local hidden variable theories and in good agreement with the one predicted by quantum mechanics. The conclusion was that nature is not-local or not-realistic, or both. Unfortunately, experiments performed suffered problems of experimental design or set-up that affect the validity of the experimental finding. These problems are often referred to as "loopholes".
Despite being an old problem, is really challenging to design and realize a loophole-free Bell test and only in 2015 3 teams managed to perform such experiment [21–23] (plus one in 2016[24]) closing simultaneously many critical loopholes.

1.5.1 CHSH Inequality

The original inequality derived by Bell was hard to test experimentally since it required perfect (anti)correlated particles. A generalization of that inequality was derived in 1974 by Clauser, Horne, Shimony, and Holt [25] where the authors proposed the experiment needed to test their inequality. Suppose to have two space-like separated parties Alice and Bob, each of them receives a particle, and on this particle they can measure a property. The outcome $A(x), B(y)$ on Alice's and Bob's side respectively, depends on the settings they used and we assume, without loss of generality, that the outcomes can only be ± 1. One practical example could be the polarization of photons; if Alice and Bob receive one photon each, they can measure polarization of the photons and the setting, in this case, is the base they use to

perform the measurement. Limiting to the case where only 2 settings are employed we have $x = \{a, a'\}$ and $y = \{b, b'\}$.
If we now assume that there is a local hidden variable λ that describes the system, then A and B must be function of this hidden variable yielding $A(x,\lambda)$, $B(y,\lambda)$. Finally, if the theory is local, since Alice and Bob are space-like separated, $A(x,\lambda)$ must be independent from $B(y,\lambda)$. Thus we can write the correlations between the two measurements as:

$$C_{AB}(x,y) = \int_\Lambda A(x,\lambda)B(y,\lambda)\rho(\lambda)d\lambda \tag{1.23}$$

where $\rho(\lambda)$ is the probability density function associated to the hidden variable λ. Considering another setting for Bob and using the fact that the measures take only ± 1 values:

$$\begin{aligned}\left|C_{AB}(a,b) - C_{AB}(a,b')\right| &= \left|\int_\Lambda \big(A(a,\lambda)B(b,\lambda) - A(a,\lambda)B(b',\lambda)\big)\rho(\lambda)d\lambda\right| \\ &\leq 1 - \int_\Lambda \big(B(b',\lambda)B(b,\lambda)\big)\rho(\lambda)d\lambda\end{aligned} \tag{1.24}$$

We can choose now another setting a' such that

$$C_{AB}(a',b') = 1-\delta \qquad \text{with } \ 0 \leq \delta \leq 1 \tag{1.25}$$

This parameter is introduced to relax the condition of perfect correlation in the original paper by Bell.
Now we can divide Λ into two regions

$$\Lambda^{\pm} = \{\lambda | A(a,\lambda) = \pm B(b,\lambda)\} \tag{1.26}$$

Using 1.25 we can write:

$$\int_\Lambda A(a',\lambda)B(b,\lambda)\rho(\lambda)d\lambda = \int_{\Lambda^+} A(a',\lambda)B(b,\lambda)\rho(\lambda)d\lambda + \int_{\Lambda^-} A(a',\lambda)B(b,\lambda)\rho(\lambda)d\lambda \tag{1.27}$$

$$= 1-\delta \tag{1.28}$$

then using 1.26

$$\int_{\Lambda^+} A(a',\lambda)^2\rho(\lambda)d\lambda - \int_{\Lambda^-} A(a',\lambda)^2\rho(\lambda)d\lambda = 1-\delta \tag{1.29}$$

Using that $A(x,\lambda) = \pm 1$ and the normalization on $\rho(\lambda)$ we have:

$$1 - 2\int_{\Lambda^-} \rho(\lambda)d\lambda = 1-\delta \tag{1.30}$$

$$\int_{\Lambda^-} \rho(\lambda)d\lambda = \frac{1}{2}\delta \tag{1.31}$$

We can now rearrange the second term in Eq 1.24:

$$\int_\Lambda \big(B(b',\lambda)B(b,\lambda)\big)\rho(\lambda)d\lambda = \int_{\Lambda^+} A(a',\lambda)B(b,\lambda)\rho(\lambda)d\lambda - \int_{\Lambda^-} A(a',\lambda)B(b,\lambda)\rho(\lambda)d\lambda \tag{1.32}$$

$$\geq \int_{\Lambda^+} A(a',\lambda)B(b,\lambda)\rho(\lambda)d\lambda - 2\int_{\Lambda^-} |A(a',\lambda)B(b,\lambda)|\rho(\lambda)d\lambda \tag{1.33}$$

$$= C_{AB}(a',b) - \delta \tag{1.34}$$

Substituting into the original equation we have:

$$\big|C_{AB}(a,b) - C_{AB}(a,b')\big| = 1 - C_{AB}(a',b) + \delta = 2 - C_{AB}(a',b) - (1-\delta) \tag{1.35}$$

$$= 2 - C_{AB}(a',b) - C_{AB}(a',b') \tag{1.36}$$

and finally obtaining

$$\big|C_{AB}(a,b) + C_{AB}(a,b') + C_{AB}(a',b) - C_{AB}(a',b')\big| \leq 2 \tag{1.37}$$

which is the usual form for the CHSH inequality. We can see that for the CHSH inequality the bound for LHV theories is 2: any measured value above 2 (compatible with errors) would be a proof that the two particles testes are experiencing correlations not explainable by an LHV theory, and so, in contrast with local realism.

1.5.2 Quantum mechanics predictions

In Eq 1.37 we saw that the bound in the CHSH inequality for local hidden variable theories is 2, but what are the predictions of quantum mechanics? In the case of quantum mechanics, we don't assume to have hidden variables, so the correlations $C_{AB}(a,b) = \langle A(a)B(b)|A(a)B(b)\rangle$ are given by the expectation values of the measure operators on the wavefunction describing the two particles state. Thus we ca rewrite the CHSH inequality in the form:

$$\big|\langle A(a)B(b)|A(a)B(b)\rangle + \big\langle A(a')B(b)\big|A(a')B(b)\big\rangle + \big\langle A(a)B(b')\big|A(a)B(b')\big\rangle \tag{1.38}$$

$$- \big\langle A(a')B(b')\big|A(a')B(b')\big\rangle\big| \leq B_{QM} \tag{1.39}$$

In the case Alice and Bob shares a maximally entangled state , for example $|\psi\rangle = \frac{1}{2}(|1\rangle|-1\rangle - |-1\rangle|1\rangle)$, where $|\pm 1\rangle$ are the eigenstates of σ_x, they can choose their settings such that

$$A(a) = \sigma_x \otimes I \tag{1.40}$$

$$A(a') = \sigma_z \otimes I$$

$$B(b) = I \otimes -\frac{\sigma_x + \sigma_z}{\sqrt{2}}$$

$$B(b') = I \otimes \frac{\sigma_x - \sigma_z}{\sqrt{2}} \tag{1.41}$$

For these value of the settings is follows that

$$C_{AB}(ab) = C_{AB}(a'b) = C_{AB}(ab') = -C_{AB}(a'b') = \cos\left(\frac{\pi}{4}\right) \tag{1.42}$$

Leading to $B_{QM} = 2\sqrt{2}$, which is the upper bound for the CHSH inequality for quantum mechanics. The proof of this proposition is called Tsirelson's bound [26]. This higher bound means that quantum mechanics violates the CHSH bound for local hidden variable theory and so is not compatible with the principle of local realism. For the sake of completeness is notable that a general theory subject only to the no-signaling condition has an upper bound of 4.

Anyway there is still a way to reconcile QM and LHV theories via the so-called superdeterminism. Superdeteminism attacks directly one of the assumptions of Bell's theorem: the free will. Bell's theorem assumes that the types of measurements performed at each detector can be chosen independently of each other and of the hidden variable being measured. In other words, is the experimenter "free will" that chooses the settings for each round of the experiment. Superdeterminism instead states that there is no randomness in nature and everything is just evolving in time, following the law of a deterministic physics. In this sense also the choice of the settings of the experimenter are already determined before they happen, in fact, there is not even a choice, the settings used are just the ones that had to be used. Since the chosen measurements can be determined in advance, the results at one detector can be affected by the type of measurement done at the other without any need for information to travel faster than the speed of light.

Part II

Secure Quantum Random Number Generators

CHAPTER 2

Quantum Random Number Generators

In the following chapter, we will introduce the concept of a Quantum Random Number Generator, the possible applications of such device, the different existing types and basic notions needed for the analysis of its security. A more detailed discussion can be found in [27, 28].

2.1 The need for true randomness.

Randomness is an invaluable resource for many different applications such as cryptography [29], scientific simulations[30, 31], gambling and fundamental physics tests[21–23]. Especially in cryptography, random numbers are a basic building block for almost any protocol, and if their privacy is compromised, the security of the entire protocol can be broken. For this reason, Random Number Generators (RNG) have always been a target for attackers, and in many occasions their successful exploit led to important security breaches[32, 33]. Additionally, in 2013 leaks of NSA classified documents revealed that the DUAL EC DBRG random number generator, proposed as a NIST standard [34], contained a backdoor that could give access to the whole random sequence. [34, 35]. This backdoor had been successfully exploited in at least one documented attack: the Juniper network attack (CVE7755).

But, backdoors can be a problem even for hardware devices. There have been demonstrations of manufacturers or attackers that inserted malicious modifications at the hardware level in real world RNGs, for example changing the dopants level in the circuit [36].

Today's the most common type of RNG are Pseudo Random Number Generators (PRNG) and are directly implemented in software or hardware. An algorithm starts with an initial value, called *seed*, and generates a sequence of numbers whose statistics are close to a uniform distribution. The unpredictability of their outcomes relies on some assumptions on the algorithm and the computational infeasibility of brute-forcing all the initial states. The advantages of such type of generators are given by their cost, speed, and availability. How-

ever, despite their common use, in this type of generators, there is no space for randomness. Their working principle is entirely deterministic, and the randomness in the outcomes is only apparent since it is only related to the observer's ignorance about the internal state of the algorithm. Due to their algorithmic nature, this type of generators will eventually repeat their outcome after a *period* and they can also exhibit pattern in their output [37]. Randomness testing suite [38–40] were developed in order to test PRNG for biases, pattern, and correlations in their output. Unfortunately, there is no way to test the quality of a random number generator from a finite sampling of its output. To get an intuition on that, consider a perfect random number generator that outputs a binary string of n random bits. Since the samples come from a uniform distribution, the probability of getting a particular string, included those with all 0 or all 1, is the same as every other combination. So, there are no methods that *a posteriori* can certify the quality of RNG.

Since deterministic algorithms cannot provide a true source of randomness, people started to look at classical physical processes as a tool to generate genuine randomness. Some processes, such as the flip of a coin, the thermal noise on a resistance [41] or metastability of specially designed electronic circuits [42], are intrinsically hard to predict due to their chaotic nature. These type of generators, usually called True RNG (TRNG), can indeed solve some of the problems typical of PRNG since they don't have a periodic output in their outcomes and they are typically free of patterns (although they can still exhibit some type of correlations). However, from a fundamental point of view, the search for genuine randomness still comes to a dead end. Classical mechanics is a fully deterministic theory and, given the initial conditions of the system, the laws of motion permit to predict with absolute precision the state of the system at any instant in the future or in the past. In the Newtonian perspective, the evolution of the entire Universe was already written since the beginning of time. Again, the randomness in these processes is only apparent and is only related to the ignorance of the observer, who hasn't access to all the initial conditions with enough precision. From a more practical point of view, the lack of randomness in the classical process means that is not possible to bound the entropy of the system *a priori*, and the quality of the TRNG can only be evaluated using the statistical test suites. Moreover, TRNG are physical objects build with real devices that are subject to unavoidable non-idealities that can compromise the quality of the output. Clock, temperature and voltage drifts are just some examples of practical issues that can bias the output of these generators. In order to solve the problem *unbiasing* techniques are usually employed [43–46].

The impossibility of generating *genuine* randomness from both algorithm and classical processes motivated the research and development of Quantum Random Number Generators (QRNG). One of the peculiar features of Quantum Mechanics, in fact, is the probabilistic nature of its laws. The outcome of some processes, such as the measure of the spin of a particle in basis complementary to the prepared one, are inherently random. From both the fundamental and practical point of view, this is a complete shift of paradigm. In contrast to the previous cases, here the randomness is *genuine* and not apparent: even having access to position and momentum of all the particles in the Universe, there is no way to predict the outcome of such measurement. From a practical point of view, this fundamental unpredictability is an assurance for privacy. If the random number cannot be predicted, it's impossible for an attacker to have access to them. Moreover, since the physical process itself is not deterministic and has to obey to the laws of Quantum Mechanics, it is possible to lower-

bound *a priori* the minimum amount of randomness (or entropy) that can be extracted. This is a guarantee on the quality of the source that is not subject to the flaws of statistical test suites. Unfortunately QRNG, similarly to TRNG, are built with real devices and are also subject to imperfections and non-idealities. These imperfections, if not correctly taken into account, can leak information to the outside and can be used to predict the numbers. Then one has to be careful to analyze how these imperfections can affect the security of their generator and the amount of trust that he is confident to make on his devices.

The level of trust, or equivalently the type of assumptions, that one has to put on a real QRNG can be used to classify the QRNG in different categories.

2.2 Types of QRNG

The first Quantum Random Number Generators were built measuring the time difference between subsequent decay of a radioactive source a [47, 48]. In fact, while the decay rate of a radioactive source can be precisely calculated, nothing can be said about when a specific nucleus will decay. Since then, other processes have been employed in order to realize smaller, more practical, and faster devices. In the last twenty years the development of QRNG has focused mostly on optical implementations, thanks to the advances of quantum optics and the commercial availability of many components, from the sources (Laser, LED, Quantum Dots) to the detectors (Single Photon Detectors, Photodiodes, Balanced Detectors). In this section, we will review some of the optical implementations, highlighting the differences and the security level offered by each implementation.

Rather than classifying the QRNG respect their source or underlying measured process, we will classify them respect the level of trust that is associated to their implementation. How critical is my application? What is the performance that is required? Can I trust the manufacturer? These are the typical questions that one has to answer when selects an RNG for a particular application. As we will see the price to pay for an increased security level is lower performances.

Quantum Random Number Generators can be divided in three main categories: Trusted, Device-Independent (DI) and Semi-Device-Independent (Semi-DI). Figure 2.1 visually represents the tradeoff between security and performance among the different class of QRNG.

2.2.1 Trusted QRNG

Typically a QRNG is composed by a source that prepares a well defined quantum state and a measurement station that measures the state. Trusted QRNG, as the name suggests, assume a perfect characterization of all its internal components, meaning that at every round of the protocol the state emitted by the source is assumed to be known and the measurement station is assumed to behave as expected. Such strong assumptions on the devices are usually not particularly suited in adversarial scenarios, where an attacker tries to force the QRNG; however, they permit to develop simple protocols that can reach high generation speed. As an example, in this category, we can find the first optical scheme based on a beamsplitter, a weak coherent source, and two single photon detectors, proposed in 1994 by Rarity[49]. In the proposal, a single photon is sent to a balanced beamsplitter, and single photon detectors

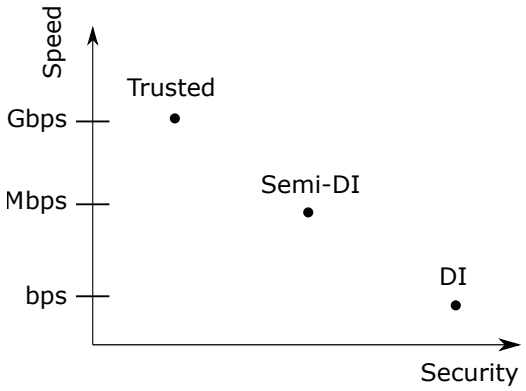


Figure 2.1: *The figure represent the tradeoff between security and performances offered by the different categories of QRNG:*

(SPD) are placed in the transmitted and reflected arms. Depending on which detector clicks a 0 or 1 is generated, providing a simple but practical quantum random number generator. After this, other types of trusted QRNG have been proposed that exploited a polarization beam splitter and diagonally polarized photons, the time of arrival of photons on a single photon detector [50–53], the spatial mode of single photons detected by SDP arrays[54, 55] and photon number detection [54, 56–58]. Moreover, in[59] it was shown that also continuous variable systems and standard photodiodes could be used to build a QRNG. In particular, homodyne detection can be used to sample the random fluctuations of the vacuum of the EM field or amplified spontaneous emission [60]. Additionally, also laser phase noise can be used as a source, with a delayed self-heterodyning detection for both pulsed [61] and CW sources[62]. Remarkably, these last types of generators can achieve the astonishing speed of 68Gbps [62]. It's also worth noting that all the commercial devices fall into this category [63–66].

However, it is important to stress out that these type of QRNG are not particularly suited for security applications. In all the cases the entropy is evaluated just looking at the probability distribution of the classical outcomes, while biases due to imperfections are removed using unbiasing techniques. This methodology is the same as the one used for TRNG and carries the same drawbacks. If the assumptions on the trusted devices are not fulfilled, because of non-idealities of the devices, drifts, malfunctions or attacks, then the quantum "origin" of randomness can be lost, rising no alerts to the user, which would keep using the device. In this case the randomness of the output would be again apparent and insecure.

2.2.2 Device-Independent QRNG

On the opposite side of the chart, we have Device-Independent (DI) protocols, which offer the highest level of security since they do not assume anything about the inner working of their devices, which can be even fully controlled by the attacker. This implies that contrarily to "trusted" QRNG, the privacy of the random number is calculated taking into account that the adversary can also share quantum correlations with the devices.

Introduced in[67], they exploit non-locality and the violation of a Bell Inequality to certify the randomness and the privacy of the generated numbers, only from the experimental data. A loophole-free violation of a Bell inequality, in fact, certifies that the generated output cannot be generated by a deterministic strategy, and hence are random.

The first protocols[68, 69] and realizations[70] were based on *randomness expansion*: in this protocol a perfect source of randomness providing a seed of $\mathcal{O}(\sqrt{n}\log n)$ bits is expanded quadratically using the Bell test. Clearly, the requirement of perfect randomness is a big limitation for this protocol. Luckily, a new protocol called *randomness amplification* was proposed in [71] where partially random bits can be *amplified* in a DI way, in order to obtain arbitrarily perfect random bits. Remarkably in [72], using the Entropy Accumulation Theorem [73], the authors were able to show that DI randomness amplification can be obtained with the current experimental technology.

Unfortunately, from the experimental point of view, the realization of a DI-QRNG is extraordinarily complex and challenging. Recently, the experimental results presented in [74, 75], showed DI *randomness expansion* closing both the locality and the detection loophole. Unfortunately, due to the small Bell violation, the maximal secure rate was 180bps, which is far too slow for any practical application.

2.2.3 Semi-Device Independent QRNG

Recently, Semi-Device Independent (Semi-DI) QRNG protocols have been proposed, trying to bridge the gap between "trusted" and DI QRNG. They work in the same adversarial scenario as DI QRNG, but they make some assumption on the devices used. In particular, the assumptions can be related to the dimension of the underlying Hilbert space [76, 77], the measurement device [78–82] or the source [83], for example the mean photon number [84] or the maximum energy of the emitted states [84–87]. However, even though some assumptions on the devices are made, the evaluation of the security is similar to the DI case, where the adversary is assumed to share not only classical but also quantum correlations with the devices. Hence, the achievable randomness must be minimized respect all the possible attacker's strategies compatible with the measured data. This security estimation offers a guarantee on the quantum "origin" of the extracted randomness.

The advantage of working in the Semi-DI framework is that no entanglement is strictly needed and the protocols can be implemented in a prepare&measure way. This greatly simplifies the experimental implementation and permits to achieve higher generation rates, if compared to DI QRNG. Still, due to the higher complexity, their generation rate cannot compete with "trusted" QRNG and only recently a Semi-DI QRNG [79] could break the Gbps barrier.

In this thesis, we will focus on this type of protocol since they provide a good trade-off between security and performance, making them suitable for secure practical applications.

2.3 Entropies

A fundamental quantity in the analysis of the security of QRNG as QKD is entropy. In this section, we will introduce the notion of entropy in both Classical Information Theory and Quantum Information Theory.

The starting point in the zoo of entropies (Figure 2.2 visually explains this concept) is undoubtedly the Shannon Entropy. In its pioneering work of 1948 [88] Shannon considering a random variable X distributed according to the probability distribution $P_X(x)$ defined the quantity:

$$S(X) = \sum_x -P_x(X)\log\left(P_X(x)\right) \tag{2.1}$$

as entropy. This quantity characterizes quantitatively the amount of our uncertainty respect to the random variable X. The quantity $-\log\left(P_X(x)\right)$, called *surprisal* characterizes the information content of a particular event. Clearly, deterministic event shouldn't carry any information, since when they happen we don't learn anything. On the other hand rare events should be characterized by a high content of information.

In the asymptotic limit of many Independent Identically Distributed (IID) repetitions of a protocol, the Shannon Entropy quantify the average amount of randomness that can be extracted by the random variable X.

The quantum analogous of the Shannon Entropy is the Von Neumann Entropy of a quantum state ρ:

$$H(\hat{\rho}) = -\mathrm{Tr}\left[\hat{\rho}\log\left(\hat{\rho}\right)\right] = -\sum_x \lambda_x \log\left(\lambda_X\right) \tag{2.2}$$

where λ_x are the eigenvalues of $\hat{\rho}$.

Another useful quantity is the conditional entropy:

$$S(X|Z) = -\sum_x P_{X|Z=z}(x)\log\left(P_{X|Z=z}(x)\right) \tag{2.3}$$

and its quantum version

$$H(\hat{\rho}_x|\hat{\rho}_z) = H(\hat{\rho}_{xz}) - H(\hat{\rho}_z) \tag{2.4}$$

where $\hat{\rho}_{xz}$ is a joint state in $\mathscr{H}_x \otimes \mathscr{H}_z$ and $\rho_z = \mathrm{Tr}_X[\hat{\rho}_{x,z}]$ The conditional entropy quantify the average uncertainty, in the asymptotic IID limit of about the random variable X given the information that $Z = z$ for some other random variable Z.

The conditional entropy plays a central role in the evaluation of the security of both QRNG and QKD since the legitimate user is interested to bound the private amount of randomness generated given the information that a possible attacker could have gained during the entire execution of the protocol.

Shannon and Von Neumann entropies can be seen as a particular realization of a broader set of entropies called Rényi entropies of order α and defined as:

$$H_\alpha(X) = \frac{1}{1-\alpha}\log\left(\sum_x P_X(x)^\alpha\right) \tag{2.5}$$

for $\alpha \in [0, \infty]$, where the points $0, 1$ and ∞ are considered under the limit.

The usual Shannon entropy is recovered in the limit $\alpha \to 1$, while values of $0 \leq \alpha < 1$ give more weight to events with higher probability and values of $1 \geq \alpha > \infty$ give more weight to events with lower probability. Consequently, they are monotonically decreasing respect to α. In a similar manner to what has been done before one can also define relative Rényi entropies and their quantum version.

Among all the Rényi entropies, those associated with the values $\alpha = \infty$ play a unique role, especially in the non-asymptotic regime. The $S_\infty(X)$ is also called min-entropy and is linked to the probability of correctly guessing the value of X in a single-shot:

$$S_\infty(X) = S_{min}(X) = -\log_2(p_{guess}(X)) \tag{2.6}$$
$$p_{guess}(X) = \max_x P_X(x) \tag{2.7}$$

For an attacker interested in guessing the outcome of X in a single shot, the optimal strategy is to bet on the most probable outcome of $P_X(x)$. Its conditional version is given by:

$$S_\infty(X|E) = S_{min}(X|E) = -\log_2(p_{guess}(X|E)) \tag{2.8}$$
$$p_{guess}(X|E) = \max_x P_X(x|E) \tag{2.9}$$

We can also define its quantum conditional version [89, 90], already written in its Semidefinite Positive (SDP) (see Section A for more details) optimization from. This is the formulation that will be mainly used later on.

$$H_{min}(X|Y) = -\log\left(\min_{\hat{\sigma}_Y} \mathrm{Tr}[\sigma_Y]\right) \tag{2.10}$$
$$\text{s.t } \hat{\rho}_{XY} \leq \mathbb{1}_X \otimes \sigma_Y \tag{2.11}$$
$$\sigma_Y \geq 0 \tag{2.12}$$

where $\hat{\rho}_{XY}$ is the joint state in $\mathscr{H}_X \otimes \mathscr{H}_Y$.

The quantum conditional min-entropy is related by a duality relation to another quantity called the max-entropy (which is the Rényi entropy of order $\frac{1}{2}$)[89]. Consider $\rho_{XYZ} \in \mathscr{H}_X \otimes \mathscr{H}_y \otimes \mathscr{H}_Z$ to be pure. Then:

$$H_{min}(X|Y) = -H_{max}(X|Z) \tag{2.13}$$

Like in the classical case, the quantum conditional min and max entropies are connected to the guessing probability in the single-shot scenario, in case side-information is present. In particular, these quantum versions are able to take into account the case where also quantum side information is accessible to the adversary. Consider for example a *classical-quantum* state, introduced in 1.22, in the form:

$$\hat{\rho}_{XE} = \sum_x P_X(x) |x\rangle\langle x| \otimes \hat{\rho}_x^E \tag{2.14}$$

This is the joint post measurement state when a generic state $\rho_A E$ is measured in the subsystem A, but the outcome of the measurements $|z\rangle$ are not known. In this case the quantum conditional min-entropy simplifies in:

$$H_{min}(X|E) = -\min_{\hat{E}_x} \log_2\left(\sum_x P_X(x)\,\mathrm{Tr}\left[\hat{E}_x \rho_x^E\right]\right) \tag{2.15}$$

with $\hat{E}_x$ some POVM acting on $\mathscr{H}_E$. In this case, $H_{min}(X|E)$ quantifies the amount of randomness that is present in the outcome X given that an attacker could have access to the quantum side information E. The optimal strategy for an attacker is to find a set of POVM $\hat{E}_x$ that maximize the overlap with the conditional states ρ_x^E for each possible outcome x. Then, if a particular $\hat{E}_x$ clicks, in that round, he can bet on x.

Unfortunately, the quantum conditional min and max entropies are very sensitive to small changes in the probability distribution, and a slight modification of the system's state might have a tremendous impact on its entropy [91]. Moreover, while they quantify the right amount of randomness in the single-shot regime, they don't converge asymptotically to the von Neumann entropy. In fact using their additivity [91]:

$$H_{min}\left(\rho_{AB}\otimes\rho_{A'B'}|\sigma_B\otimes\sigma_{B'}\right)=H_{min}(\rho_{AB}|\sigma_B)+H_{min}(\rho_{A'B'}|\sigma_{B'}) \tag{2.16}$$

one can see that in the IID limit:

$$\lim_{n\to\infty}\frac{1}{n}\left(H_{min}(\rho_{AB}^{\otimes n}|\sigma_B^{\otimes n})\right)=H_{min}(\rho_{AB}|\sigma_B) \tag{2.17}$$

which is $\neq H(\rho_{AB}|\sigma_B)$ in general. Both problems can be solved using their *smoothed* versions:

$$H_{min}^{\epsilon}(\rho_{AB}|\sigma_B)=\sup_{\tilde{\rho}_{AB}\in\mathscr{B}_{\epsilon}(\rho_{AB})}H_{min}^{\epsilon}(\tilde{\rho}_{AB}|\sigma_B) \tag{2.18}$$

where $\mathscr{B}_{\epsilon}(\rho_{AB})$ is a ball centered in ρ_{AB} (using the *Trace distance* as a measure) with radius ϵ, which is called the smoothing parameters. For this quantity the asymptotic limits are correctly recovered:

$$\lim_{\epsilon\to 0}\lim_{n\to\infty}H_{min}^{\epsilon}(\rho_{AB}^{\otimes n}|\sigma_B^{\otimes n})=H(\rho_{AB}|\sigma_B) \tag{2.19}$$

2.4 The security analysis of a Semi-DI QRNG

In this section, we will briefly describe the main steps required for the analysis of the security of a Semi-DI QRNG, following the framework presented in [93]. We will often compare it to the case were trusted QRNG are considered, in order to highlight the differences.

2.4.1 True randomness

The analysis of the security of a QRNG aims to estimate the *true amount of randomness* in the generator's output that is private to the user, so that is unpredictable to anyone else. The concept of *true randomness* can be formally defined if one assumes a causal space-time structure. Then a random variable X is defined *ϵ-truly random* if its probability distribution is ϵ-close (w.r.t the trace distance) to the uniform and if it is uncorrelated to any other variables which are not in the future light-cone of X. If we define $P_{\tilde{X}}(x)=\frac{1}{|X|}$ the uniform distribution, $\mathscr{C}$ the set of variables correlated with X but not in its future light cone (also called *Side-Information*) and $P_{X\mathscr{C}}$ the joint distribution of X and $\mathscr{C}$, we can formally express the previous sentence as

$$D(P_{X\mathscr{C}},P_{\tilde{X}}\times P_{\mathscr{C}})\leq\epsilon \tag{2.20}$$

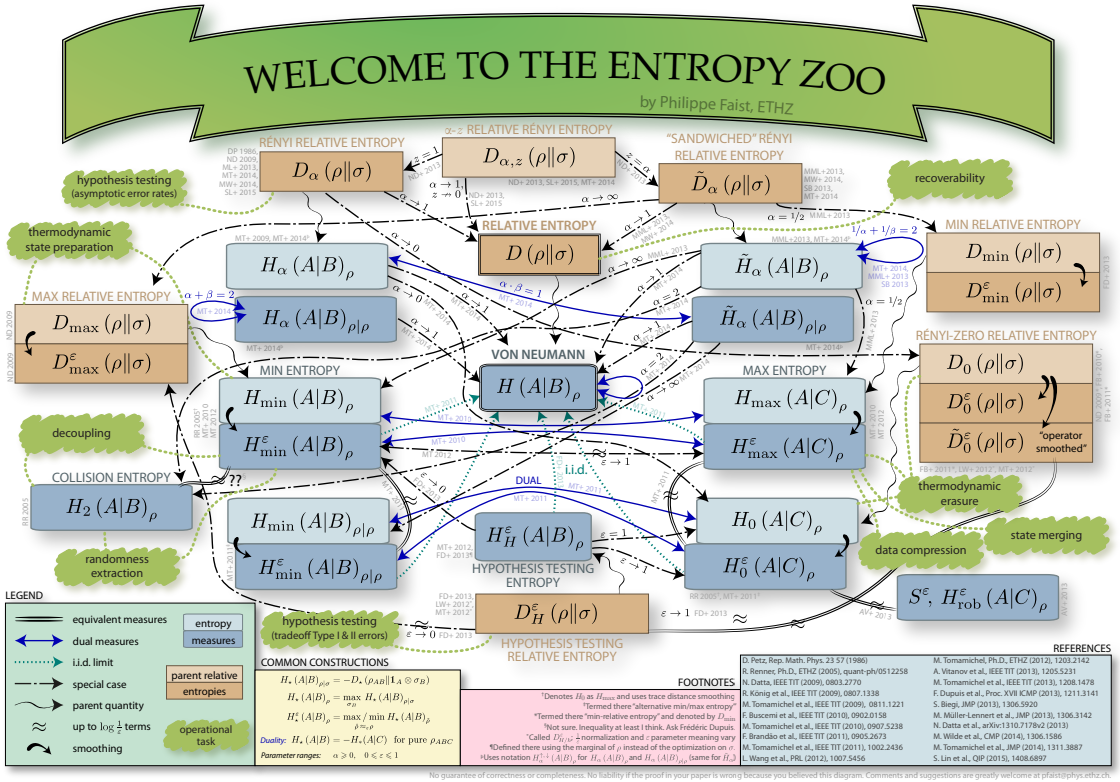


Figure 2.2: *A "non-exhaustive" graph of entropies and their relations. Taken from[92]*

where D is the Trace distance between the the two probability distribution

$$D(P_X, Q_X) = \frac{1}{2}||P_X - Q_X||_1 = \frac{1}{2}\sum_x |P_X(x) - Q_X(x)| \tag{2.21}$$

So the distribution of P_X conditioned on $\mathscr{C}$ should be almost indistinguishable (except for a probability up to ϵ) to an uniform distribution. The case of perfect randomness is recovered in the limit $\epsilon \to 0$.

2.4.2 Randomness estimation

In general, a QRNG can be decomposed in a *source*, that prepares a fixed state and *measurement* station that measures the incoming states and record the output. In the ideal case where the state produces is always *fixed* and *pure* and the measurements are projective, the output is truly random.

The typical example is a photon source that prepares a polarization qubit in the $|+\rangle$ state and measures it, my means of a Polarization Beam Splitter (PBS), in the $|H\rangle, |V\rangle$ basis with the two projectors $\Pi_H = |H\rangle\langle H|, \Pi_V = |V\rangle\langle V|$. In this case the two outputs H, V are uniformly distributed, and if the system is uncorrelated with any other objects, the output is *truly random*.

However, practical QRNG are subject to imperfections, non-idealities and deviations, hence their outcomes are inevitably mixed with classical (and predictable) noise. We define the output of this imperfect generator *raw randomness*. In the previous example, this could happen if the source does not perfectly prepares a balanced superposition of $|0\rangle$ and $|1\rangle$: then in such case the output will be biased with $P_H \neq P_V \neq 0.5$. Other common imperfections are related to the detection stage and include: the non-unity efficiency of detectors, dark counts and afterpulsing.

In this case, if we trust that no Side-information is present, the content of true randomness in the raw randomness generated is given by the classical min-entropy 2.6. If an attacker has no information about the generator, except for its output statistics P_H, P_V, its optimal strategy is to always bet on the most probable result and amount of extractable randomness is

$$H_{min}(X) = -\log_2(\max P_X(x)) = -\log_2(\max(p, 1-p)) \tag{2.22}$$

which achieves its maximum in the ideal case $p = 0.5$.

However, we have made a strong assumption: we assumed that the attacker shares no correlation with the QRNG. If Side-Information is present the quantity 2.6 doesn't represents anymore the amount of *true randomness*. Let's supposes that the attacker knows the working principle of the QRNG. If he is able to intercept the flying qubit before this reaches the PBS, he can substitute it with one forged by himself. In this case, he can choose to send half of the times the state $|H\rangle$ and half of the times the state $|V\rangle$. To the measurement station, the incoming state $\hat{\rho} = \frac{1}{2}|H\rangle + \frac{1}{2}|V\rangle$ would reproduce the same statistics of $|+\rangle$. The *true randomness* estimate given by $H_{min}(X)$ would still be 1; however the attacker would know the outcome with probability 1 each time.

If one wants to include the classical side information into account the right quantity is given by the classical conditional min-entropy $H_{min}(X|C)$, presented in Eq. 2.8. In this case $P(H|H) = P(V|V) = 1$ and

$$H_{min}(X|C) = -\log_2(1) = 0 \tag{2.23}$$

The amount of *true randomness* in this case is correctly estimated.

However, the attacker can also share quantum correlation with the generator. This is the most general type of Side-Information available to the attacker. In this case, also the classical conditional min-entropy $H_min(X|C)$ fails to correctly estimate the true amount of randomness. Going back to the previous example, if the attacker has access to the source, he could prepare a pair of qubit in a maximally entangled state:

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|H\rangle_A \otimes |H\rangle_E + |V\rangle_A \otimes |V\rangle_E) \tag{2.24}$$

and send one photon to the PBS while keeping the other one. In this case the state seen by the PBS is still $\hat{\rho} = \frac{1}{2}|H\rangle\langle H| + \frac{1}{2}|V\rangle\langle V|$ and $P(H) = P(V) = 1$. Unfortunately, after the measurement, the joint state $\left|\Phi^+\right\rangle$ gets projected to either $\rho_{HH} = |H\rangle_A \otimes |H\rangle_E$ or $\rho_{VV} = |V\rangle_A \otimes |V\rangle_E$, and the attacker is able to predict the outcomes again with perfect precision.

Also, in this critical case the right amount of randomness can be estimated. The right quantity is now the conditional quantum min-entropy $H_{min}(X|E)$ of Eq. 2.15. In this case the conditional states ρ_x^E are $\rho_H^E = \frac{1}{2}|H\rangle\langle H|, \rho_V^E = \frac{1}{2}|V\rangle\langle V|$.

The two POVM $\hat{E}_H, \hat{E}_V$ that maximize the overlap with ρ_H^E, ρ_V^E are then just the projectors $\hat{\Pi}_H, \hat{\Pi}_V$.

Then $H_{min}(X|E)$ becomes:

$$H_{min}(X|E) = -\log_2\left(\mathrm{Tr}\left(\hat{\Pi}_H \rho_H^E\right) + \mathrm{Tr}\left(\hat{\Pi}_V \rho_V^E\right)\right) = 0 \tag{2.25}$$

From this analysis, we quickly understood that the presence of Side information can completely undermine the privacy of the generated numbers, that would still seem random to the user but would be completely predictable by an attacker. The most general quantity that never underestimate the content of *true randomness* even in the presence of Side information is given by the quantum conditional min-entropy $H_{min}(X|E)$. Unfortunately, this quantity is the hardest to estimate or bound. In order to compute it one has to know the global joint state ρ_{AE} and optimize over all the possible strategies of the attacker $\left\{\hat{E}_x\right\}$. Moreover, most of the QRNG protocols, like the one described above, would not be able to generate any randomness in this scenario. This is the reason why Trusted QRNG need to trust the inner working of their devices: by trusting them they can assume the state of the source or the shape of their measurement, making *de facto* the side information *trivial*. Then they can simply use the classical min-entropy $H_{min}(X)$ (that is easy to compute since it depends only on the output statistic $P_X(x)$), to estimate the randomness. However, if the assumptions are not respected their security can be compromised. On the other hand, DI QRNG, since they don't assume anything on their devices, need to bound $H_{min}(X|E)$. As we have seen they exploit non-locality and the violation of a Bell inequality to do so, with all the complexity that this requires.

Semi-DI QRNG, instead, try to combine the good points of both approaches. They work in a paranoid scenario similar to the one of DI QRNG, and so they bound $H_{min}(X|E)$; however they do make some assumption on some part of their devices. This is required in order to avoid a test of non-locality. For example Source-DI protocols, assume trusted measurements but do not trust the source. In this case they work with a Prepare'n'Measure implementation, but in order to estimate $H_{min}(X|E)$ they consider the scenario where the attacker holds a *purification* of the state they receive (which is the one that gives him the most information) and then they optimize over all the possible strategies $\left\{\hat{E}_x\right\}_x$ in order to pick the one giving the most conservative estimate. More details about this procedure will be given in Chapter 4.

2.4.3 Randomness extraction

The next step in the analysis of the security of a QRNG is the *randomness extraction*. Given a practical QRNG, its output will in general not be *truly random*. If we consider a string Z of n bits of the outputs of the generator part of it will be known by an attacker with some Quantum Side Information E and only $H_{min}(Z|E)$ bits of Z can be considered *truly random*. Then, informally, a *randomness extractor* is a procedure that is able to generate a substring $\tilde{Z}$ of $\approx H_{min}(Z|E)$ bits from Z, of truly random numbers.

There are many different techniques for the randomness extraction, where only a few works against quantum adversaries [94–96]. In this thesis, we will focus only on the method, called Leftover hashing, presented in [96], since it can be implemented in a simple and efficient way also for high generation rates.

The technique exploits special hash functions, called two-universal hash function,[97] defined as the family $\mathscr{F}$ of functions from an alphabet χ to $\{0,1\}^l$ such that, if $f(z)$ is chosen uniformly in $\mathscr{F}$:

$$Pr(f(x)=f(x^{'}))\leq\frac{1}{2^l} \tag{2.26}$$

for any $x\neq x^{'}\in\chi$.

Then if ρ_{ZE} is a classical-quantum state and $\mathscr{F}$ is a family of two-universal family of hash functions then:

$$\frac{1}{2}||\rho_{F(Z)EF}-\mathbb{1}\otimes\rho_{EF}||_1\leq\epsilon_{hash} \tag{2.27}$$

$$\epsilon_{hash}=2^{-\frac{1}{2}(H_{min}(Z|E)-l)} \tag{2.28}$$

where $||\cdot||_1$ is the Trace norm and

$$\rho_{F(Z)EF}=\sum_{f\in\mathscr{F}}\frac{1}{|\mathscr{F}|}\rho_{f(Z)E}\otimes|f\rangle\langle f| \tag{2.29}$$

So if $f\in\mathscr{F}$ is uniformly chosen such that the output length l is $< H_{min}(Z|E)$, the output string $f(Z)$ will be uniform and independent from E, except with probability $\epsilon_{hash}<1$. This probability ϵ_{hash} decreases exponentially as a function of the difference between l and $H_{min}(Z|E)$.

Then practically, given $H_{min}(Z|E)$ and chosen an appropriate ϵ_{hash} (commonly $\epsilon_{hash}\leq 10^{-10}$), one randomly selects a 2-universal hash function $f\in\mathscr{F}$ with output l such that:

$$l\leq H_{min}(Z|E)+2\log_2(\epsilon_{hash}) \tag{2.30}$$

A similar relation holds also for the smooth conditional quantum min-entropy defined in Eq. 2.18 [96].

These 2-universal hash function can be efficiently constructed using Toeplitz matrices that requires only $n+l-1$ coefficients instead of nl. The vector-matrix multiplication can be efficiently computed using the Fast Fourier Transform with a $\mathscr{O}(n\log(n))$ complexity [98]. Finally they can also be implemented in hardware, for example on Field Programmable Gate Array (FPGA), reaching speeds as high as 8 Gbps[99].

Summing up, uniformity is not the only important parameter for the evaluation of randomness but correlations play a fundamental role. Side-Information, if not taken into account correctly, can completely undermine the privacy of the generated numbers and different entropies quantify the true content of randomness for different types of Side Information. The correct estimation of the min-entropy, is fundamental in order to guarantee a correct extraction of uniform and uncorrelated bits, using the Leftover Hashing Lemma and 2-universal hash functions.

CHAPTER 3

A Source-Device-Independent Ultrafast Heterodyne QRNG

Semi-device-independent (Semi-DI) QRNG [28], are a promising approach to enhance the security with respect to a standard "fully trusted" QRNG, achieving fast generation rate, dramatically larger than DI-QRNG. These require some weaker assumptions to bound the side information. Such assumptions can be related to the dimension of the underlying Hilbert space [76, 77], the measurement device [78–82] or the source [83], for example the mean photon number [84] or the maximum energy of the emitted states [84–87].However, due to the weaker assumptions, their experimental implementation is usually more complex than trusted QRNG and, in general, less practical. For example, their generation rate is usually limited to tens of Mbps (except for [79]), and it requires an active switch of either the source or the measurements.

In this chapter, we introduce a new QRNG belonging to the family of the Source-device independent (Source-DI), by exploiting continuous variable (CV) observables of the electromagnetic (EM) field. In previously realized CV-QRNGs [59, 79],random numbers were generated by using a homodyne detector that measures a quadrature of the EM field. We propose and demonstrate a CV-QRNG based on heterodyne detection in the Source-DI framework: we bound analytically the eavesdropper quantum side information (i.e., the conditional min-entropy), and we achieve, to our knowledge, the fastest generation rate in the Semi-DI framework.

The advantages of heterodyne measurement over homodyne are multiple: beside offering better tomography accuracy than homodyne [100, 101], heterodyne measurement offers an increased generation rate since it allows a "simultaneous measurement" of both quadratures. In addition, the experimental setup is simplified with respect to the protocol based on homodyne introduced in [79], since there is no need for an active switch to measure the two quadratures. Finally, it is possible to derive a constant lower bound on the conditional quantum min-entropy that doesn't change during the experiment.

Our Source-DI protocol assumes a trusted detector, but it does not make any assumption

on the source: an eavesdropper may fully control it, manipulating it in order to maximize her ability to predict the outcomes of the generator. Such approach is very effective in taking into account any imperfect state preparation. Although these are the typical assumptions that hold for QRNGs in the Semi-DI framework, this protocol features a critical difference. Previous protocols counteract the eavesdropper via an active measurement strategy on the state, which implies the need for additional randomness to certify the numbers. Instead here the removal of the active basis switch has a profound impact on the type of protocol implemented: in this scheme no initial external randomness is required, making it a randomness generation protocol and not a randomness expansion protocol, unlike previous Semi-DI and DI realizations. Moreover, we realize a practical implementation of the protocol with a compact fiber optical setup that employs only standard telecom components.

Some contents of this chapter are part of our work [1].

3.1 Theory

3.1.1 A heterodyne QRNG

CV-QRNGs are characterized by high generation rates due to the use of fast photodiodes instead of (slow) single photon detectors: continuous spectrum of the observables typically assures more than one bit of entropy per measurement, and the use of photodiodes with high bandwidth allow to sample the quadratures at GSample/s.

In this QRNG, we implement a heterodyne detection scheme, presented in Fig 3.1, where two "noisy quadrature observables" are measured simultaneously [102, 103].

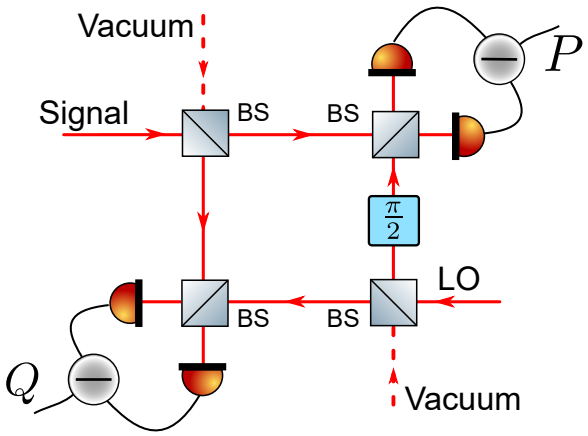


Figure 3.1: *Schematic representation of the optical Heterodyne (or Double Homodyne) measurement. This image (and many others in the thesis) uses elements from the ComponentLibrary by Alexander Franzen [104], licensed under CC BY-NC 3.0*

As suggested by Arthurs and Kelly in 1965 [102], the two EM quadratures $\hat{Q}, \hat{P}$ can be measured simultaneously even if the two operators do not commute $[\hat{Q}, \hat{P}] \neq 0$, paying the price of an added noise in the measurement. In fact, what is measured are actually two

operators $\hat{q}$ and $\hat{p}$

$$\hat{q} = \hat{Q} + \hat{A} \qquad \hat{p} = \hat{P} + \hat{B} \tag{3.1}$$

where $\hat{A}$ and $\hat{B}$ describe the quantum noise necessary to have $[\hat{q}, \hat{p}] = 0$. This relation on $\hat{q}, \hat{p}$ implies $\langle [\hat{A}, \hat{B}]^2 \rangle \leq -1$ and eventually $\Delta\hat{q}\Delta\hat{p} \geq \hbar$. This means that when the two quadratures are measured simultaneously, the minimum uncertainty on the measurement is double respect the Heisenberg limit [13].

The heterodyne measurement can be also represented with the following Positive Operator Value Measurement (POVM) $\left\{\hat{\Pi}_\alpha\right\}_{\alpha\in\mathbb{C}}$ where

$$\hat{\Pi}_\alpha = \frac{1}{\pi} |\alpha\rangle \langle\alpha| \,, \tag{3.2}$$

and $|\alpha\rangle$ is the coherent state with complex amplitude α. If we define ρ_{A} the density matrix of the EM field, the output of the heterodyne measurement is represented by the random variable X

$$X = \{q, p\}\,, \qquad q = \mathrm{Re\{e\}}(\alpha)\,,\ p = \mathrm{Im\{m\}}(\alpha)\,, \tag{3.3}$$

distributed according to the following probability density function known as Husimi function:

$$\mathrm{Q}_{\rho_{\mathrm{A}}}(\alpha) = \mathrm{Tr}\left[\hat{\Pi}_\alpha \rho_{\mathrm{A}}\right] = \frac{1}{\pi} \langle\alpha| \rho_{\mathrm{A}} |\alpha\rangle \,. \tag{3.4}$$

In an ideal scenario where the QRNG user (Alice) can trust the source of random states, such scheme has the immediate advantage of doubling the generation rate with respect to an homodyne receiver. Since the “raw" random numbers X are typically not uniformly distributed, it is essential to process them with a randomness extractor [105]. A randomness extractor (for more details see Sec. 2.4.3) compresses the input string of raw numbers, such that the shorter output string is composed by i.i.d. random bits.

However, the continuous POVM of Eq.3.3 can never be implemented in a real setup: practically, any heterodyne measurement is discretized. This means that the possible outcomes X_δ of the measure are discrete with a resolution given by δ_q and δ_p for the two “quadratures”. The discretized version of the POVM element $\hat{\Pi}_\alpha$ is then given by

$$\hat{\Pi}^\delta_{m,n} = \int_{m\delta_q}^{(m+1)\delta_q} dq \int_{n\delta_p}^{(n+1)\delta_p} dp\ \hat{\Pi}_{q+ip} \tag{3.5}$$

and the possible outputs are distributed according to a discretized version of the Husimi function:

$$\mathrm{Q}^\delta_{\rho_{\mathrm{A}}}(\mathrm{m,n}) = \mathrm{Tr}\left[\hat{\Pi}^\delta_{\mathrm{m,n}} \rho_{\mathrm{A}}\right] = \int_{\mathrm{m}\delta_{\mathrm{q}}}^{(\mathrm{m}+1)\delta_{\mathrm{q}}} \mathrm{dq} \int_{\mathrm{n}\delta_{\mathrm{p}}}^{(\mathrm{n}+1)\delta_{\mathrm{p}}} \mathrm{dp} \mathrm{Q}_{\rho_{\mathrm{A}}}(\mathrm{q}+\mathrm{ip})\,. \tag{3.6}$$

In a fully-trusted QRNG, when the source is trusted and the input state is pure (such as for the vacuum) or the privacy of the generated numbers is not a concern, the number of random bits that can be extracted per sample is given by the so-called classical min-entropy of X_δ

$$H_{\min}(X_\delta) = -\log_2[\max_{m,n} \mathrm{Q}^\delta_{\rho_{\mathrm{A}}}(\mathrm{m,n})]\,. \tag{3.7}$$

However, ultrafast generation is worthless for cryptographic applications if the numbers are not secure and private. As discussed in Sec. 2.4.2, if security is important, quantum side information must be also taken into account and the conditional quantum min-entropy $H_{\min}(X|\mathscr{E})$ [89, 91, 106, 107] must be evaluated. We recall that in the Source-DI framework, an eavesdropper may have full control of the source and then may have some prior information on the generated numbers. We will show that with a heterodyne scheme, it is possible to generate unpredictable and secure numbers also when the source of quantum states is controlled by the eavesdropper.

3.1.2 A Secure POVM-based QRNG

In the Source-DI framework, the legitimate user, Alice, does not make any assumption on ρ_{A}, such as its dimension or purity: the source may be even controlled by a malicious QRNG manufacturer, Eve. This framework is well suited to deal with imperfect sources of quantum states [78]. On the contrary, Alice carefully characterizes her local measurement apparatus and trusts it.

In this scenario, Eve is assumed to prepare the state ρ_{A} to be measured. In particular, Eve will prepare ρ_{A} in order to maximize her guessing probability P_{guess} of the outcomes of Alice heterodyne measurement. If the state ρ_{A} is not pure, it can be prepared by Eve as a incoherent superposition of states τ_β^{A} with probabilities $p(\beta)$, such as

$$\rho_{\mathrm{A}} = \int p(\beta)\tau_\beta^{\mathrm{A}} d\beta \tag{3.8}$$

As shown below, for quantum state ρ_{A} with positive Glauber-Sudarshan representation [13], Eve optimizes her strategy by using τ_β^{A} that are coherent states.

When Eve generates the state τ_β^{A}, the best option for her is to bet on the heterodyne outcome with higher probability, namely

$$\max_{m,n} \mathrm{Tr}\left[\hat{\Pi}_{m,n}^{\delta}\tau_\beta^{\mathrm{A}}\right] \tag{3.9}$$

On average, Eve's probability of guessing correctly the output of the heterodyne measurement can be written as:

$$P_{\text{guess}}(X_\delta|\mathscr{E}) = \int p(\beta) \max_{m,n} \mathrm{Tr}\left[\hat{\Pi}_{m,n}^{\delta}\tau_\beta^{\mathrm{A}}\right] d\beta. \tag{3.10}$$

Having full control of the source, given the state ρ_{A}, Eve chooses the decomposition $\{p(\beta), \tau_\beta^{\mathrm{A}}\}$ that maximizes P_{guess}. We note that the states $\hat{\tau}_k$ are, in general, not orthogonal. In such scenario, quantum correlations between Alice and Eve are modeled by a shared pure bipartite state ρ_{AE}. The states τ_{k} are related to the optimal measurement that Eve should perform on ρ_{AE} in order to maximize her guessing probability.

According to the Leftover Hash Lemma (LHL) [91, 96], the extractable randomness in the presence of side information is quantified by the quantum conditional min-entropy

$$H_{\min}(X_\delta|\mathscr{E}) = -\log_2 P_{\text{guess}}(X_\delta|\mathscr{E}), \tag{3.11}$$

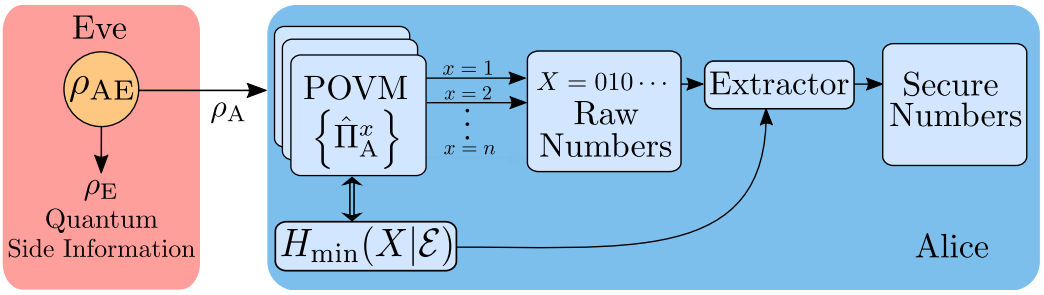


Figure 3.2: Structure of the Source-DI protocol. *In the general Source-DI scenario, Eve prepares the state ρ_A that she sends to Alice such that her purification gives her the maximal guessing probability on Alice's outcome. The structure of the POVM chosen by Alice to measure ρ_A already impose a lower bound on $H_{min}(X|\mathcal{E})$, independently from the input state or the output of her measurement (see Proposition 1). This bound is used to calibrate an extractor that returns, at each round of the protocol, secure random bits when applied to Alice's outcome.*

where $P_{guess}(X_\delta|\mathcal{E})$ is maximum probability of guessing X_δ conditioned on the quantum side information $\mathcal{E}$

$$P_{guess}(X_\delta|\mathcal{E}) = \max_{\{p(\beta),\tau^A_\beta\}} \int p(\beta) \max_{m,n} \mathrm{Tr}\left[\hat{\Pi}^\delta_{m,n}\tau^A_\beta\right] d\beta\,. \tag{3.12}$$

The maximization in (3.12) is performed over all possible decomposition $\{p(\beta),\tau^A_\beta\}$ that satisfy $\rho_A = \int p(\beta)\tau^A_\beta d\beta$. The above considerations are valid not only for the heterodyne measurement but are correct for any POVM measurement (also with Hilbert spaces of finite dimensions).

Fig. 3.2 represents a general protocol within this framework.

In the case of infinite precision $\delta_p, \delta_q \to 0$ (i.e. the continuum limit) it is possible to define the "differential quantum min-entropy"[107] as

$$h_{min}(X|\mathcal{E}) = \lim_{\delta_p,\delta_q\to 0} [H_{min}(X_\delta|\mathcal{E}) + \log_2 \delta_p\delta_q] \tag{3.13}$$

and a corresponding $p_{guess}(X|\mathcal{E}) = 2^{-h_{min}(X|\mathcal{E})}$.

In this case p_{guess} is a probability density and not a proper probability such as P_{guess}. By exploiting the properties of POVMs, we derive a lower bound on $H_{min}(X_\delta|\mathcal{E})$ (and thus an upper bound on $P_{guess}(X_\delta|\mathcal{E})$).

Proposition 1. *For any POVM $\{\hat{\Pi}_x\}_{x\in X}$ the quantum conditional min-entropy $H_{min}(X|\mathcal{E})$ is lower-bounded by*

$$H_{low} = -\max_{\{x\in X,\tau_A\in\mathcal{H}_A\}} \log_2\left(\mathrm{Tr}\left[\hat{\Pi}_x\tau_A\right]\right). \tag{3.14}$$

Proof. Given a set of POVM $\{\hat{\Pi}_x\}$, the maximum over x in (3.12) is bounded by $\max_x \mathrm{Tr}\left[\hat{\Pi}_x\tau^A_\beta\right] \leq \max_{x,\tau_A} \mathrm{Tr}\left[\hat{\Pi}_x\tau_A\right]$. Then Eq. (3.12) is upper bounded by:

$$\begin{aligned} P_{guess}(X|\mathcal{E})_{min} &\leq \max_{\{x,\tau_A\}} \mathrm{Tr}\left[\hat{\Pi}_x\tau_A\right] \max_{\{p(\beta),\tau_B\}} \int p(\beta)d\beta \\ &= \max_{\{x,\tau_A\in\mathcal{H}_A\}} \mathrm{Tr}\left[\hat{\Pi}_x\tau_A\right] \end{aligned} \tag{3.15}$$

from which the bound on the min-entropy follows by using (3.11). □

If the POVM reduce to projective measurements, the above bound is trivial, since it always possible to find a state τ_{A} such that $\mathrm{Tr}\left[\hat{\Pi}_x \tau_{\mathrm{A}}\right]=1$: in this case,no randomness can be extracted. However, for an overcomplete set of POVM we may have $\max_{\{x,\tau_{\mathrm{A}}\}} \mathrm{Tr}\left[\hat{\Pi}_x \tau_{\mathrm{A}}\right]<1$ and therefore randomness can always be extracted. We now exploit the above proposition for the specific case of heterodyne measurement.

Corollary 1.1. *For the heterodyne measurement the quantum conditional min-entropy is lower-bounded by*

$$H_{min}(X_\delta|\mathscr{E}) \geq -[\max_{\{m,n,\tau_{\mathrm{A}}\}} \log_2(\mathrm{Tr}\left[\hat{\Pi}^\delta_{m,n}\tau_{\mathrm{A}}\right])] = \log_2 \frac{\pi}{\delta_q \delta_p}. \tag{3.16}$$

Proof. It is well known that the Husimi function $\mathrm{Q}_{\rho_{\mathrm{A}}}(\mathrm{q}+\mathrm{ip})$ is upper bounded by $\frac{1}{\pi}$. Then, $\forall \tau_{\mathrm{A}}$, the following inequality holds:

$$\mathrm{Tr}\left[\hat{\Pi}^\delta_{m,n}\tau_{\mathrm{A}}\right] = \int_{m\delta_q}^{(m+1)\delta_q} dq \int_{n\delta_p}^{(n+1)\delta_p} dp \mathrm{Q}_{\rho_{\mathrm{A}}}(\mathrm{q}+\mathrm{ip}) \tag{3.17}$$

$$\leq \int_{m\delta_q}^{(m+1)\delta_q} dq \int_{n\delta_p}^{(n+1)\delta_p} dp \frac{1}{\pi} \leq \frac{\delta_q \delta_p}{\pi} \tag{3.18}$$

By Proposition 1, it follows that $H_{\min}(X_\delta|\mathscr{E}) \geq \log_2 \frac{\pi}{\delta_q \delta_p}$. □

By the definition of differential quantum min-entropy it follows that $h_{\min}(X|\mathscr{E}) \geq \log_2 \pi$. The bounds are tight, i.e. $h_{\min}(X|\mathscr{E}) = \log_2 \pi$ and $H_{\min}(X_\delta|\mathscr{E}) = \log_2 \frac{\pi}{\delta_q \delta_p} + O(\delta)$, for quantum state with positive Glauber-Sudarshan $\mathscr{P}(\alpha)$ representation.

To show the tightness, we note that any matrix ρ_{A} can be written as

$$\rho_{\mathrm{A}} = \int \mathscr{P}(\alpha) |\alpha\rangle \langle\alpha| d^2\alpha \tag{3.19}$$

where $\mathscr{P}(\alpha)$ is the Glauber-Sudarshan P-function. If $\mathscr{P}(\alpha)$ is positive it can be interpreted as a probability density and the state ρ_{A} can be seen as an incoherent superposition of coherent states.

For small $\delta_{p,q}$ the guessing probability of Eq. (3.12) becomes

$$P_{\mathrm{guess}}(X_\delta|\mathscr{E}) = \delta_q \delta_p \max_{\{p(\beta),\tau^{\mathrm{A}}_\beta\}} \int p(\beta) \max_\alpha \mathrm{Q}_{\tau^{\mathrm{A}}_\beta}(\alpha) + \mathrm{O}(\delta^3). \tag{3.20}$$

Since coherent states maximize the value of the Husimi function $\mathrm{Q}_{\tau^{\mathrm{A}}_\beta}(\alpha)$, then the optimal decomposition in (3.20) is precisely $\{\mathscr{P}(\alpha), |\alpha\rangle\langle\alpha|\}$ such that $P_{\mathrm{guess}}(X_\delta|\mathscr{E}) = \frac{\delta_q \delta_p}{\pi} + O(\delta^3)$ and $H_{\min}(X_\delta|\mathscr{E}) = \log_2 \frac{\pi}{\delta_q \delta_p} + O(\delta)$.

By using a heterodyne measurement scheme, a quantum tomography of the input state is also obtained [13]: while Alice generates the raw random numbers, she also reconstructs the

state ρ_A. Then it is possible to evaluate numerically the quantum conditional min-entropy by using (3.11) and (3.12). Although for a qubit system, this problem was elegantly addressed by [108], it is not of easy solution in the CV case. On the other hand, Corollary 1 gives an easy lower bound on $H_{\min}(X_\delta|\mathscr{E})$. Alice knows that even if Eve forges a state with an optimal $\mathscr{E}$, such side information will not let Eve guess the heterodyne outcome with a probability larger than $\frac{\delta_q\delta_p}{\pi}$.

In the presence on an imperfect source of quantum states, this is the most conservative strategy to adopt, but ensures the generation of completely secure random numbers while avoiding a complex numerical maximization.

It is worth to note that the min-entropy of the random numbers is bounded by a function that depends on the measurement resolution only. The measurement, in this scenario, is under control of the user: Alice can readily obtain the min-entropy (3.16) by measuring δ_p and δ_q of her well characterized apparatus. The min-entropy is constant, and Alice does not need to worry updating its value, as long as she trusts the apparatus. In the case of imperfect heterodyne measurement Proposition 1 can be still used: the characterization of the measurement apparatus allows to define what are the actual POVM $\widetilde{\Pi}^{\delta}_{m,n}$ corresponding to such measurement. In eq. (3.16) the ideal POVM $\hat{\Pi}^{\delta}_{m,n}$ should replaced by the operators $\widetilde{\Pi}^{\delta}_{m,n}$. The bound $\log_2 \frac{\pi}{\delta_q\delta_p}$ should be modified accordingly and its explicit value depends on the actual form of the operators $\widetilde{\Pi}^{\delta}_{m,n}$.

Finally, we point out that in many cases such lower bound is (almost) tight: indeed, coherent and thermal states have positive Glauber-Sudarshan $\mathscr{P}(\alpha)$ function and for those states the bound $\log_2 \pi$ on the differential min-entropy is tight (the bound of the min-entropy is almost tight due to discretization). Moreover, in contrast to other Semi-DI QRNG where the min-entropy needs to be estimated in real-time to provide security [76, 79, 85], in this protocol it depends on the structure of the heterodyne POVM, and it is always constant. Hence, Alice can apply on X_δ a randomness extractor calibrated on $\log_2 \frac{\pi}{\delta_q\delta_p}$ and erase any guessing advantage of Eve.

3.1.3 Security against general attacks

Until now we estimated the quantum conditional min-entropy $H^{(1)}_{\min}(X|\mathscr{E})$ for a single run of the protocol. Usually, this corresponds to consider security against only individual attacks. In this scenario, Eve is allowed to interact only with the $\hat{\rho}_A$ that is exchanged during one round of the protocol and, while she can store its ancilla in a quantum memory, she is allowed to measure it independently respect the previous and future ancillas. The most general scenario is given by coherent (or general) attacks, where Eve can interact with a global interaction $\hat{U}_c$ with all the n states $\hat{\rho}^i_A$ exchanged during the protocol, and she can also apply a global measurement $\hat{\Pi}_n$, to all her ancillas.
However, since we calculate the min-entropy on the worst state $\tau^{(1)}$ that is allowed by physics, this result holds also for coherent attacks.

In this section we will show it explicitly, by bounding the min-entropy for n runs of the protocol $H^{(n)}_{\min}(X|\mathscr{E})$ in terms of the min-entropy for a single run of the protocol $H^{(1)}_{\min}(X|\mathscr{E})$.

When Eve performs a coherent attack, she can prepare a general n—partite state $\hat{\tau}^{(n)}$ to

maximize her probability of guessing the n outcomes of Alice measurements, that can be written as

$$\hat{\Pi}_{\mathbf{x}} \equiv \hat{\Pi}_{x_1} \otimes \hat{\Pi}_{x_2} \otimes \cdots \otimes \hat{\Pi}_{x_n} . \tag{3.21}$$

The guessing probability of Eve for n runs of the protocol $P^{(n)}_{\text{guess}}(X|\mathscr{E})$ can be written as

$$P^{(n)}_{\text{guess}}(X|\mathscr{E}) = \max_{\{x_i\}} \left[\max_{\tau^{(n)}} \text{Tr}\left[\left(\hat{\Pi}_{x_1} \otimes \cdots \otimes \hat{\Pi}_{x_n} \right) \tau^{(n)} \right] \right] \tag{3.22}$$

$$= \max_{\{x_i\}} \left[\max_{\tau_1} \text{Tr}\left[\hat{\Pi}_{x_1} \hat{\tau}_1 \right] \cdots \max_{\tau_n} \text{Tr}\left[\hat{\Pi}_{x_n} \hat{\tau}_n \right] \right] \tag{3.23}$$

$$= \prod_{i=1}^{n} \left(\max_{x_i, \tau_i} \text{Tr}\left[\hat{\Pi}_{x_i} \tau_i \right] \right) \tag{3.24}$$

$$= \left[P^{(1)}_{\text{guess}}(X|\mathscr{E}) \right]^n \tag{3.25}$$

where $P^{(1)}_{\text{guess}}(X|\mathscr{E})$ is the guessing probability for one run of the protocol. In the above equations the state $\tau^{(n)}$ is a generic n-partite state, while τ_i are generic single-party states. The crucial step is going from Eq. (3.22) to Eq. (3.23). The argument of the outer maximization in Eq. (3.22) is given by $\max_{\tau^{(n)}} \text{Tr}[\hat{\Pi}_{\mathbf{x}} \tau^{(n)}]$ and corresponds to the maximum eigenvalue of the operator $\hat{\Pi}_{\mathbf{x}}$. Since $\hat{\Pi}_{\mathbf{x}}$ is the product of Hermitian operators with non-negative eigenvalues, its maximum eigenvalue is equal to the product of their maximum eigenvalues, namely $\max_{\tau_1} \text{Tr}\left[\hat{\Pi}_{x_1} \hat{\tau}_1 \right] \cdots \max_{\tau_n} \text{Tr}\left[\hat{\Pi}_{x_n} \hat{\tau}_n \right]$. This means that Eve's optimal strategy is to generate a n-mode separable state $\tau^{(n)} = \tau_1 \otimes \tau_2 \otimes ... \otimes \tau_n$.

Therefore, the min-entropy for n runs of the protocol $H^{(n)}_{\text{min}}(X|\mathscr{E})$ can be written as:

$$H^{(n)}_{\text{min}}(X|\mathscr{E}) = -\log_2 P^{(n)}_{\text{guess}}(X|\mathscr{E}) \tag{3.26}$$

$$= -\log_2 [(P^{(1)}_{\text{guess}}(X|\mathscr{E}))^n] = n H^{(1)}_{\text{min}}(X|\mathscr{E}) .$$

Hence, the bound on the min-entropy is valid not only in the single-shot regime, but also for n repetitions of the protocol and coherent attacks.

3.2 Experimental Implementation

3.2.1 Design

The proposed new protocol has been implemented with an all-fiber setup at telecom wavelength with the scheme in Fig. 3.3; in this way is possible to exploit the availability of fast off-the-shelf components for classical telecommunication while keeping the setup compact.

The heart of the experiment lies in the heterodyne detection of the vacuum state that samples the Q function with the help of a coherent field $|\alpha\rangle$ of a strong Local Oscillator (LO). This has been experimentally implemented using a commercial 90° optical hybrid, commonly used for coherent communications. The pairs of optical output then were recorded by a couple of InGaS Balanced photoreceivers.

The signal port of the 90° optical hybrid was closed, so that no photon would enter from there and the vacuum $|0\rangle$ was than measured. Since we work in the Source-DI scenario,

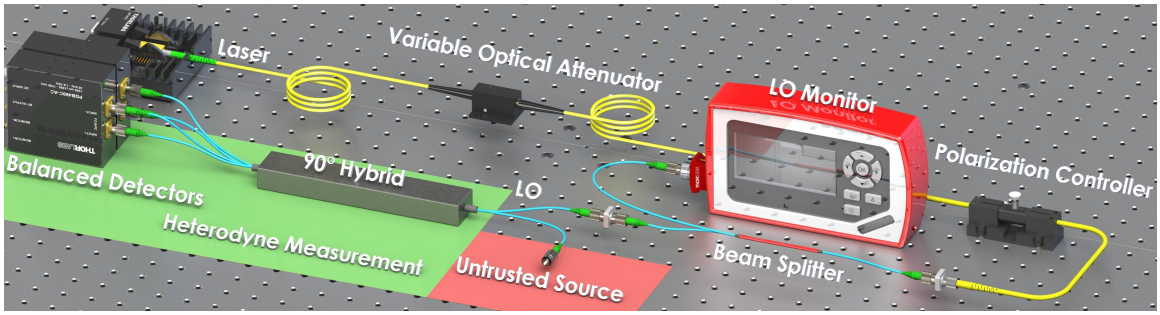


Figure 3.3: Schematic representation of the experimental setup. *The setup consists of a* 1550nm *laser used as a LO, measured in real time. The heterodyne detection is performed by a* 90° *optical hybrid and a pair of balanced InGaS detectors. The VOA is used during the calibration phase. Only commercial off-the-shelf devices were used.*

from the point of view of security, the quantum state measured can be anything, since is considered to be fully controlled by Eve.

After the heterodyne detection, a 10-bit Oscilloscope has been used as analog-to-digital converter (ADC) to digitize the two analog signals, each one proportional to one of the quadrature (q, p).

These signals directly sample the Q-function in the phase space, as shown in Fig. 3.9.

However, from the oscilloscopes we record only voltages. In order to map them into phase space (or shot-noise) units we need to calibrate the detectors and estimate the content of electronic noise. This calibration is done sweeping the power of the LO by means of a computer-controlled Variable Optical Attenuator (VOA). Then, the resolution of the ADC can be directly converted to the equivalent resolution in the phase space, thanks to the calibration function and a bound on the min entropy $H_{\min}(X|\mathscr{E})$ is computed.

The raw data are then digitally filtered, taking only a 1.25 GHz window in the central part of the spectrum obtained by the detectors. In such a way the classical noise that is coupled with the detector is filtered, increasing the Signal to Noise ratio (SNR). Then, the data are downsampled at 1.25 GSample/s, matching the bandwidth of the signal and removing any correlation introduced by the oversampling. Finally, a random Toeplitz matrix implementing 2-universal hash function calibrated on $H_{\min}(X|\mathscr{E})$ is constructed and used to extract the secure numbers.

3.2.2 Components

The local oscillator's laser

The laser employed for the strong Local Oscillator is a Thorlabs SFL1550P packed in a Butterfly 14-pin Packaging. This is an External Cavity Laser (ECL) centered at 1550nm featuring a narrow linewidth, typically smaller than 50kHz. The laser internally provides an optical isolator to prevent damages in case of back reflections. In order to ensure a stable power output and single mode operation, the laser is controlled both in current and in temperature by a Thorlabs ITC4001 Benchtop Laser Diode/TEC Controller. In fact, the SFL1550P is not unconditionally single-frequency for all the range of currents and

temperatures, but a side mode suppression ratio (SMSR) $\geq 40dB$ is guaranteed only for specific combinations, reported in the datasheet.

The laser was operated at a fixed current of 298 mA and the while the temperature was kept fixed to 24° by a PID controller, integrated into the ITC4001's TEC.

In this case, the parameters of the PID had a substantial impact on the SMSR and had to be finely tuned every time the environmental conditions changed.

The motorized Variable Optical Attenuator

During the calibration procedure is necessary to perform a sweep of the LO power from 0 mW to its maximum power. Experimentally this has been done introducing a Variable Optical Attenuator (VOA) just after the laser. An external attenuation is preferred respect to sweeping the current applied to the laser diode since it doesn't modify any optical property of the laser beam, spectra and mode included.

The VOA employed is a dual band Thorlabs VOA50-APC, working in the windows around 1310 and 1550 nm, with an adjustable attenuation range between $1-50$dB. The attenuator collimates the fiber guided beam through a tiltable window before coupling the beam back in the fiber. The attenuation is adjusted with a mechanical screw that tilts a window, varying the coupling efficiency.

After the attenuator, a 90:10 single mode optical coupler (Thorlabs TW1550R2A2) sends 10% of the optical power to an optical powermeter Thorlabs PMD100D, connected to the computer via USB.

In order to fully automatize the QRNG acquisition, we modified the VOA such that it was possible to control it with a computer. In particular, a stepper motor 28BYJ-48 was mechanically connected to the adjustment screw. The stepper motor is controlled by a control board based on the ULN2003A Darlington NPN array, driving it in a half-step mode with 4076 steps per rotation. The control board is then connected to an Arduino Uno which implements the serial communication with the computer and drives the ULN2003A through the DIO pins.

Finally, a python software on the computer reads the current power of the power meter and controls the stepper motor in order to reach the desired power. The size of the steps is adaptive and is based on an experimentally fitted model for the attenuator.

The 90° Optical Hybrid

The single polarization 90° Optical Hybrid is a Kylia COH-24, typically used as for coherent receivers in classical optical communications. The optical diagram is reported in Fig. 3.4

The hybrid is implemented using micro-optical components in order to ensure high mechanical and temperature stability. The device features a low insertion loss ≤ 1.5dB in addition to the theoretical 6dB.

The balanced detectors

The two pairs of optical signals coming from the 90° Optical Hybrid are revealed by a couple of Thorlabs PDB480C-AC balanced detectors. These detectors are composed of two InGaS

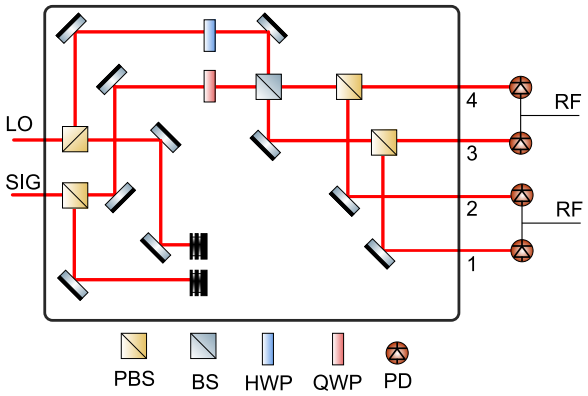


Figure 3.4: *Optical diagram of the Kylia COH24. Adapted from the datasheet [109]*

PIN photodiodes, reversely biased and connected in series as shown in Figure 3.5 With this configuration is possible to access to the single detector photocurrent via the Monitor port and to the differential signal via the Rf port.

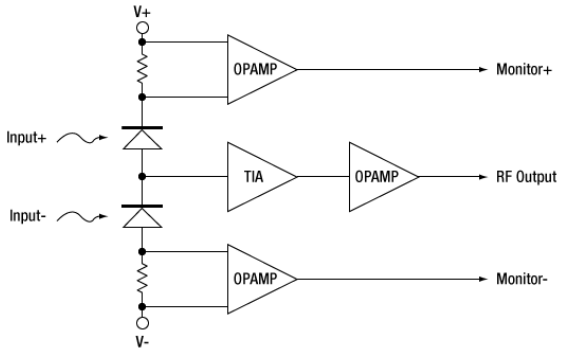


Figure 3.5: *Electrical schematics of the balanced detectors*

The PIN detectors feature a Responsivity of $\approx 0.95 AW^{-1}$ at 1550 nm and a 3dB bandwidth from 300kHz to 1.6GHz.

Due to the high gain and high speed of the transimpedance amplifier in the RF path, a DC blocker is needed, and the RF signal is only AC-coupled.

The Common Mode Rejection Ratio (CMRR), which quantifies the ability of the detector to suppress signal that appear simultaneously and in-phase on both inputs, is higher than 35dB for the entire frequency range. However, in order to obtain such high CMRR levels, manual fine-tuning of the optical power reaching the detectors is fundamental. This was done before each round of the protocol, using the Monitor ports as reference.

Finally, in order to improve the stability of the system over time, an external temperature stabilization system has been realized in order to keep the temperature of the detector fixed. A Peltier cell has been connected to the enclosure of the detector, together with two NTC 10kΩ thermistor. The seconds were directly connected to two ADC of an Arduino Uno, while the Peltier was connected to an H-Bridge Arduino Shield (Infineon BTN8982TA) originally intended as a motor control shield. Finally, a standalone PID controller was implemented on

the Arduino to control the Peltier current based on the temperature read by the thermistors. The typical stability of $0.1°C$ was sufficient for our need.

The Oscilloscope

The Oscilloscope employed was a Lecroy HDO9004 featuring 10-bits of vertical resolution, 4 GHz of analog bandwidth and up to 40 GSps of sampling rate.

The oscilloscope was connected to the computer via Ethernet and controlled via a python script using the VISA protocol. The raw data from the oscilloscope was streamed and stored on the computer using a binary encoding to save bandwidth and reduce latency.

3.2.3 Detector's calibration

In the SDI framework, we assume a trusted and characterized measurement device. In order to enforce that, before every run of the experiment we perform a calibration of the detection stage. This procedure is necessary for the evaluation of security, because it links the voltage output of the detectors to the relative quantities in the phase space, enabling us to calculate δ_q, δ_p.

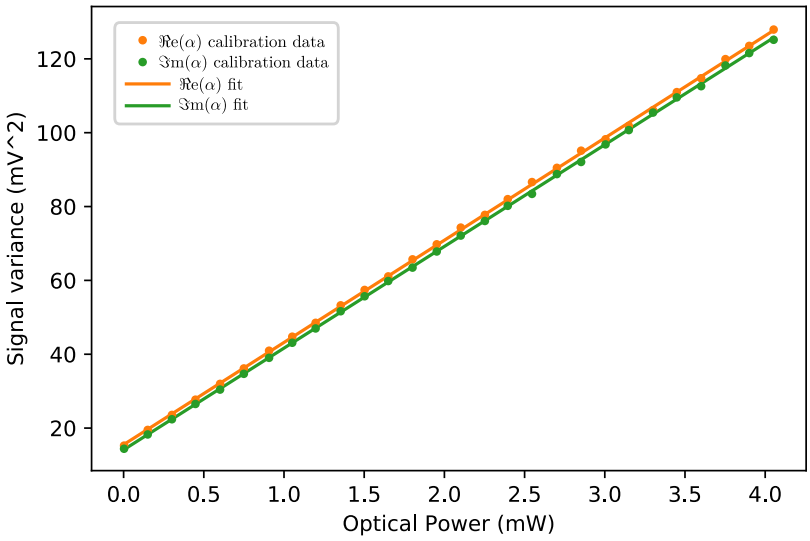


Figure 3.6: *The graph shows the linear dependence of the signal quadrature σ_V^2 as a function of the LO power.*

Theoretically, if no electronic noise is present in the system, the two quantities are related by the relation:

$$\sigma_q^2 = \frac{\sigma_V^2}{kP_{\mathrm{LO}}} \tag{3.27}$$

where k is a constant to be determined. In the above equation σ_q^2 is the variance in shot-noise units, σ_V^2 is the variance in physical units and P_{LO} the power of the local oscillator.

The constant k is related to the properties of the detectors and the noise of the electronic system and can be expressed as:

$$k = R^2 G^2 B h f \tag{3.28}$$

where R is the responsivity of the detectors in $\mathrm{A\,W^{-1}}$, G is the gain of the transimpedance amplifier in $\mathrm{V\,A^{-1}}$, B is the electronic bandwidth in Hz, h is the Plank constant and f the optical frequency. However, instead of relying on a model, it is possible to measure directly k through a calibration procedure: the vacuum is injected in the signal port of the Heterodyne while the power of the LO, P_{LO}, is raised from 0 mW to the working power. During this process, we record the variance of the electronic signal for each quadrature $\sigma^2_{V_q}$ and $\sigma^2_{V_p}$. From a linear fit we have:

$$\sigma^2_{V_{q,p}} = m_{q,p} P_{\mathrm{LO}} + c_{q,p} \tag{3.29}$$

In an ideal condition (no electronic noise) the constants $c_{q,p}$ should be 0, however in any real experiment their value never vanish. In this convention, the theoretical quadrature variances in shot-noise units for the vacuum are given $\sigma^2_{q,p} = \frac{1}{2}$, the constant k is obtained as $k_{q,p} = 2m_{q,p}$

Since we are not including the $c_{q,p}$ in the conversion factor $k_{q,p}$, we are considering the most conservative scenario, in which all classical noise is not trusted.

Indeed, for a vacuum input state $|0\rangle$ and a given value of P_{LO}, the measured variances in shot-noise units are then given by

$$\sigma^2_{q,p} = \frac{\sigma_V^2}{k P_{\mathrm{LO}}} = \frac{m_{q,p} P_{\mathrm{LO}} + c_{q,p}}{2 m_{q,p} P_{\mathrm{LO}}} = \frac{1}{2} + \frac{c_{q,p}}{2 m_{q,p} P_{\mathrm{LO}}} \tag{3.30}$$

which are always larger than $\frac{1}{2}$ for non-vanishing $c_{q,p}$. In this way the electronic noise (related to $c_{q,p}$) is regarded as noise on the source: it leads to an increase of the variances $\sigma_{q,p}$, thus lowering the min-entropy.

Figure 3.9 clearly shows this effect: the reconstructed Q function is larger than the one expected for the vacuum because of this noise.

The calibration is performed automatically by the python software that controls the QRNG: by varying the Variable Optical Attenuator (VOA), the power of the LO is changed from 0.01mW to 4.05mW, when measured with the monitor photodiode. For each power, the signal of the balanced detector is recorded, and the variance σ_V^2 is estimated. As we can see in Figure 3.6 the relation is linear for all the tested powers (i.e. we never reached the saturation of the detector's amplifiers).

From the fit, $m_1 = (2.783 \pm 0.005) \cdot 10^{-2} \mathrm{V^2/W}$ and $q_1 = (1.526 \pm 0.005) \cdot 10^{-5} \mathrm{V^2}$ for the slope and intercept of the first detector and $m_2 = (2.748 \pm 0.004) \cdot 10^{-2} \mathrm{V^2/W}$ and $q_2 = (1.419 \pm 0.004) \cdot 10^{-5} \mathrm{V^2}$ for the second one. The errors are propagated in the estimation of the $H_{\min}(X|E)$ and the most conservative value in the 1 standard deviation confidence interval is used as a lower bound. Using a more conservative 3 standard deviation confidence interval, the bound on the min-entropy is reduced from 13.949 to 13.930 bits, for an equivalent secure generation rate of 17.41 Gbps.

In the experiment this calibration procedure is performed every time we adjust the polarization controller in the LO path. The entire setup is placed in a thermally isolated container in order to improve the stability of the system and the calibration procedure is typically needed only once a day.

3.2.4 Noise Filtering and autocorrelation test

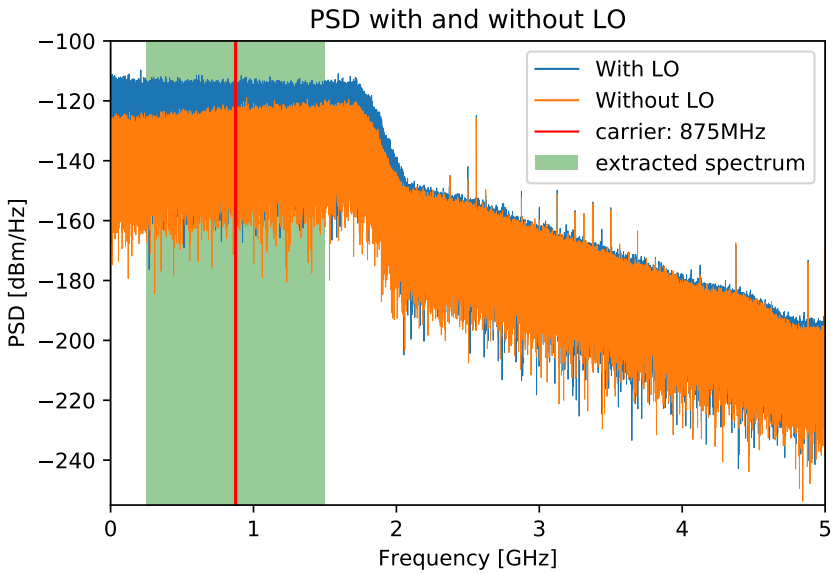


Figure 3.7: *Spectrum obtained from the detectors with or without the LO active. In green is highlighted the portion kept after the digital filtering and used for the generation. The peaks present after the* 3dB *point of the detectors are introduced by the oscilloscope at harmonics of the sampling frequency and are not present if the spectrum is obtained with an analog spectrum analyzer (HP 8561B).*

To further reduce the classical noise from the detectors (at the expense of a reduced generation rate) we perform a filtering of the signal.

Figure 3.7 shows the power spectral density of the signal produced by the detectors when the LO is turned on and when the LO is off. Although, the response seems uniform along the entire bandwidth of the detectors (1.6GHz), the initial part of the spectrum ($DC - 1$MHz) is affected by technical noise. In order to filter out this noise and enhance the signal-to-noise ratio, we have considered for the random generation only a window large 1.25GHz centered around 875MHz. With this selection, the gap is never lower than 9.6dB.

The filtering has been implemented digitally. First, the raw signal, oversampled at 10Gsps, is multiplied with a sinusoidal signal (the carrier) at 875MHz. Then the mixed signal is Fourier Transformed using the FFT algorithm, implemented in the FFTW library. After the mixing, the symmetric Fourier transform of the real signal is shifted by 875MHz respect to the 0, making it not anymore symmetrical. Now we perform a low-pass filtering with a 3-dB cutting off frequency of 625MHz. Different types of filters were employed (Butterworth, Chebyshev Bessel); however we found out that a Brick-wall filter was giving

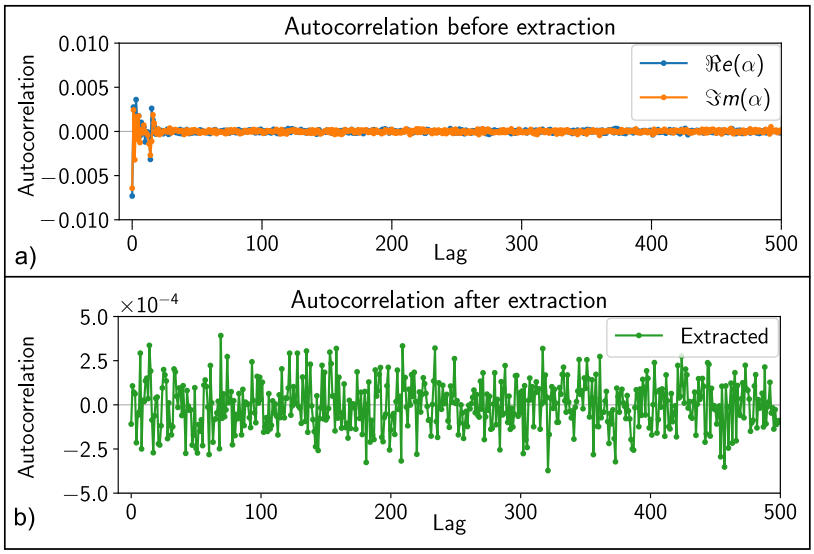


Figure 3.8: *Panel a) shows the autocorrelation measured for a sample of* $5 \cdot 10^7$ *raw numbers before the extraction while panel b) shows the autocorrelation of the extracted numbers. The spikes present in the first lags before the extraction are due to the noise introduced by the sampling equipment. The extraction procedure completely removes the correlations and is clearly visible a flat response.*

the best results. After the low pass filter, the output is inversely transformed using the inverse FFT.

However, employing a Brick-wall filter in the frequency domain inevitably induces correlation in the time-domain of the signal: indeed we observe a "sinc" dependence in the autocorrelation, as expected from the Wiener-Khinchin[110, 111] theorem. The correlation is removed by downsampling the signal in such a way to match the first zero of the autocorrelation function. Figure 3.8 shows the residual autocorrelation after the downsampling, before and after the randomness extraction for a run of $5 \cdot 10^7$ samples. The results, even before the extraction, are good, with values always below $7.5 \cdot 10^{-3}$ and typically below $1 \cdot 10^{-4}$, except for the first lags. The value of the first lag is due to noise introduced by the oscilloscope at harmonics of its sampling rate frequency.

In Figure 3.7, these distortions are clearly visible at high frequencies, where there is no contribution from the signal. However, after the extractor, all the classical noise is eliminated and the autocorrelation is completely flat, also for the initial lags.

3.2.5 Sampling and randomness extraction

The analog electric signals coming from the detector are digitized by the HDO9004 oscilloscope, in order to be further post-processed. The oscilloscope doesn't work in real-time but in burst mode, meaning that the signals are sampled at 10 GSps until the entire memory is completely filled. Then, the data are streamed to the computer via an Ethernet connection. Then, the filters discussed in Section 3.2.4 are applied off-line. Finally, always offline, the randomness extraction is applied to the filtered data. We implemented the fast computable two-universal hash function introduced in [93]; then we used it to extract the final numbers

from the filtered samples. We calibrated the extractor with the value obtained bounding $H_{\min}(X|\mathscr{E})$.

The secure parameter ϵ_{hash} was set to 10^{-12} for matrices of the size 4096×2844. The size of the matrix was optimized in order to get a fast extraction without filling the RAM of the PC.

We extracted, using a PC, $\approx 5.18 \cdot 10^{10}$ random numbers from an initial set of $7.5 \cdot 10^{10}$ raw numbers.

In this protocol, the conditional quantum min-entropy $H_{\min}(X|\mathscr{E})$, which characterizes the one-shot private randomness, is not estimated from a finite sample of data but is bounded a priori using the information from the calibration and the POVM structure. For this reason, the estimation is not affected by finite-size effects, which can have a big impact on real-time applications.

3.3 Results

Here we present the results obtained with the setup and protocol described in the previous sections.

Before the actual run of the QRNG, we perform the calibration procedure described in Sec 3.2.3. Thanks to the calibration function it was possible to obtain the following resolution parameters in phase space units: $\sigma_q^2 = 0.55135 \pm 0.00001$ and $\sigma_p^2 = 0.56732 \pm 0.00001$. These parameters represent the discretization of the POVM in the phase space induced by the hardware, without taking into account the electronic noise.

Then, we acquired $6 \cdot 10^{10}$ measurements of both the q and p quadrature, at an equivalent sampling speed of 10 GSps.

After filtering and conversion in phase space units, it is possible to plot the distribution of the data, that directly sample the Husimi Q-function. As can be seen from Fig. 3.9, the measured Q-function is slightly larger than the one expected for a pure vacuum state, where both variances are expected to be equal to 1/2.

The increase of the variances is due to classical noise of the detectors: in this approach, such noise is regarded as a "spreading" of the Q-function. Then, the effect of the electronic noise in reducing the generation rate is already included in the analysis for the quantum min-entropy.

The classical min-entropy $H_{\min}(X_\delta)$ corresponds to the larger probability of output and it is given by

$$H_{\min}(X_\delta) = 14.100 \tag{3.31}$$

However, the quantum min-entropy can be lower bounded by Eq. (3.16). With the quadrature resolutions used for the experiment, we obtain

$$H_{\min}(X_\delta|\mathscr{E}) \geq -\log_2\left(\frac{\pi}{\sigma_Q \sigma_P}\right) \geq 13.949 \tag{3.32}$$

This minimal reduction of the generation rate, from 14.10 to 13.949 bits per sample, drastically increases the security guaranteed by the entire protocol.

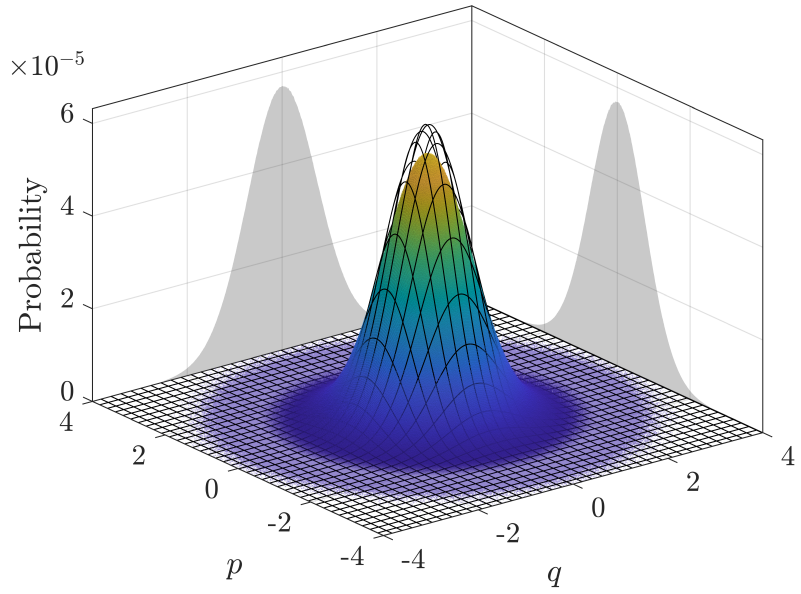


Figure 3.9: Experimental state tomography. *The plot shows the Husimi function for the vacuum (meshed curve) and the measured state (colored histogram). The projections refer to the experimental data. The measured variance is slightly larger than the one expected for the vacuum due to the electronic noise that widens the distribution.*

Finally, since after the downsampling the effective sampling rate S_r of the system is 1.25GSps, the final secure generation rate that can be obtained from this system is $S_r \cdot H_{\min}(X_\delta|\mathscr{E}) = 17.42$ Gbit/s.

The generation rate can be further improved using an ADC with a resolution larger than 10 bits. We have simulated the performance of our generator for different resolutions of the ADC, and the results are presented in Fig. 3.10. The min-entropy scales linearly as a function of the number of bits in the ADC and this could be an useful resource to further increase the total generation rate.

It is important to stress that these rates are not calculated in the asymptotic regime, i.e., in the limit of infinite repetitions of the protocol, but are valid for single-shot measurements. In fact, the conditional min-entropy $H_{\min}(X_\delta|\mathscr{E})$ is not estimated from the data, but it's bounded considering the structure of the POVM and the optimal strategy for the attacker: since no parameter estimations are involved (except the ones from the calibration), the rates are not affected by finite-size statistics, unike all previous Semi-DI protocols.

Finally, in order to check for problems in the implementation, we performed some statistical test on the generated numbers. We tested them with the NIST [38] and "dieharder" suite [39]: in both cases all the tests were passed, as we can see in Table B.1,B.2. Passing these tests doesn't certify the randomness, but only shows that some patterns are not present in the analyzed data. However, since the QRNG is supposed to pass all of them, is a way to

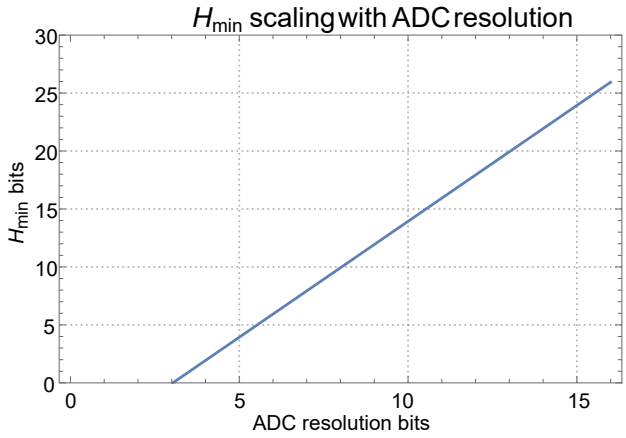


Figure 3.10: *The generation rate per measurement scales linearly as a function of the number of bits in the ADC's resolution*

double-check that the setup is working as expected.

3.4 Ongoing and future work

The proof of principle demonstration, described in the previous section, showed that high rates and high standards of security can be obtained with this protocol. However, this experiment aimed to show only the feasibility of the protocol, and some key steps are needed for a practical implementation that is able to work in real scenarios.

3.4.1 Real-time operation

The first one is the need for dedicated sampling hardware. In this demonstration, the analog RF signal coming from the balanced photodiodes is sampled by an oscilloscope with a high sampling rate (10Gsps) but small buffer memory (128 Mpts). This implies that between each acquisition of max 128 Mpts, we need to wait for the oscilloscope to write into the slow disk memory before being ready to acquire again. Moreover, an oscilloscope is an expensive and bulky instrument that adds complexity to the implementation. Hence, a dedicated ADC capable of directly sampling the RF signal at high bandwidth (at least 1.25GHz) is needed, with the capacity to stream the data to another processing device. This processing device is related to the second problem: the randomness extraction. The raw data at the output of the balanced photodiode is biased, since it is Gaussian distributed, and can, in theory, be partially correlated with the attacker. Hence, the randomness extraction routine cannot be avoided. In this demonstration, the randomness extraction was done via software on a PC, after the acquisition. However, usually the random numbers are needed in real-time by the application and this implementation is not suitable in this scenario. A device capable of processing the raw data in real-time is needed, capable of supporting the high data rate.

Aware of these limitations, we are currently developing a solution based on a fast ADC

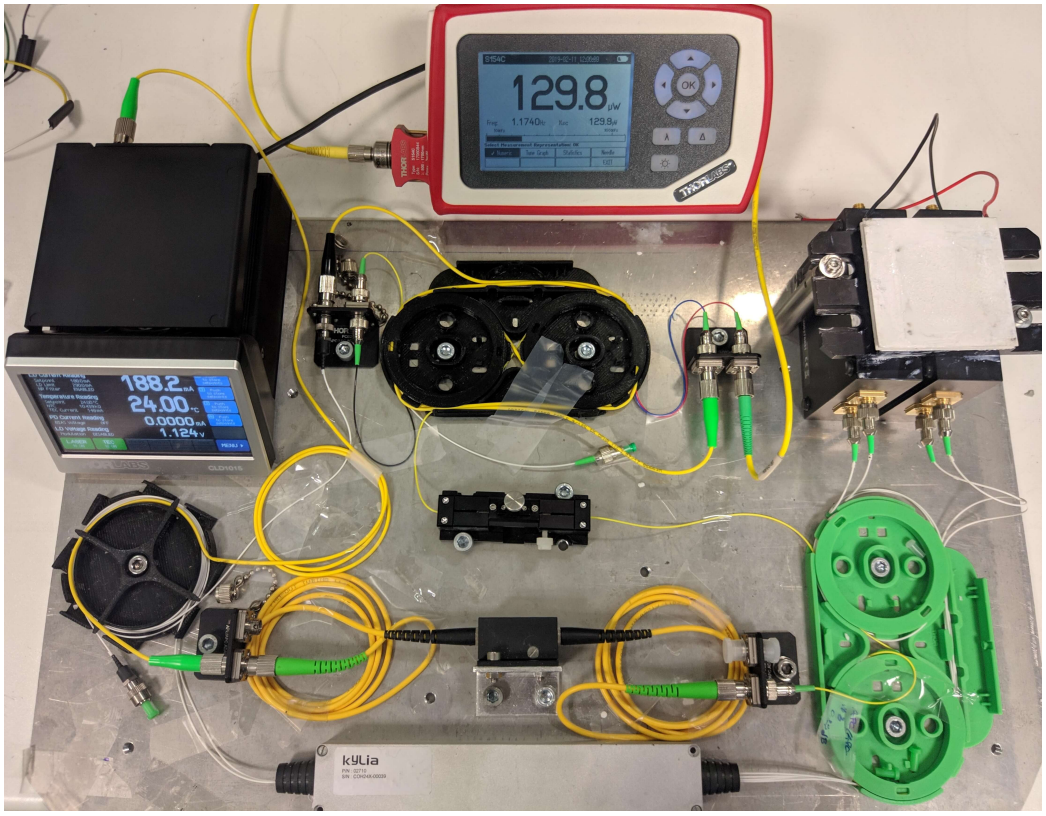


Figure 3.11: *Photo of the actual setup. On the top left we can see the controller of the laser with the laser source used for the LO. In the center is possible to see, starting from the bottom, the 90 degree hybrid in its metallic enclosure, the variable optical attenuator, the polarization controller, the fiber beamsplitter and the power meter used to monitor the power of the LO. Finally, on the top right are visible the two balanced detectors.*

connected to an FPGA. In particular, a fast ADC (such as the AD9680 by Analog Devices) is able to sample the signal up to 1250 MSps with 14-bits of resolution and transfer them continuously to the FPGA via the JESD204B protocol. In this way, the bottleneck caused by the memory is avoided. On the FPGA, the receiver data is rapidly parallelized and processed in real-time in hardware, exploiting the huge bandwidth and processing power offered by the FPGA. Finally the processed number can be streamed to the user's interface using multi-gigabit transceiver connected to the FPGA.

Similar solutions already showed the possibility to achieve up to 8 GBps of random numbers extracted in real-time [99].

3.4.2 Photonic integrated QRNG

Another significant limitation is given by the size of the setup. This is an issue for satellite applications, but it's relevant also for practical applications, where RNG is usually required to be portable. Moreover, in order to incentivize a wide adoption of such QRNG, the cost of the setup should be lowered to the minimum possible.

A possible solution to these problems is given by Integrated Optics, which offers the possibility to integrate many optical components in small-scale devices with costs that are massively reduced in case of large batch productions. So, in collaboration with ASI and Scuola Sant'Anna di Pisa, we have realized prototypes in Silicon Photonics of a complete QRNG based on heterodyne detection. All the components, except for the laser, are integrated in the chip an offer high bandwidth and stability in a centimeter-scale device.

At the time of writing the devices have been fabricated, and the first prototypes are being characterized.

3.5 Conclusions

In this chapter, we have described a new secure and practical Source-DI QRNG based on heterodyne detection. The newly developed protocol exploits the properties of the POVM implemented by the heterodyne measurement in order to obtain a direct lower bound to the conditional min-entropy, and hence on its security. This bound, also valid in the non-asymptotic regime, enables the user to erase all the side information related to an imperfect or malicious source of quantum states. Compared to previous Source-DI QRNGs [28, 78, 79] this security is obtained without affecting the generation rate: in the previous protocols, part of the generated numbers were consumed to estimate and update the bound to the conditional min-entropy. In the protocol introduced here, the bound is constant, since it is determined by the resolution of the trusted measurement apparatus only. Hence, all the secure numbers are available to the user. Such simplification has many advantages for any practical implementation of the protocol. In particular, our protocol does not rely on external randomness to work, making it a standalone random number generator, while previous Semi-DI QRNG were based on randomness expansion protocols, that require either an initial seed or an external source of randomness to work.

Our approach allows us to merge the speed of heterodyne measurements and the security of semi-device-independent protocols. Indeed, we realized the protocol with off-the-shelf components achieving with an off-line post-processing, an equivalent rate of 17.42 Gbit/s.

CHAPTER 4

A numerical approach to unstructured QRNG

4.1 A Numerical Unstructured approach to entropy estimation

We have seen that the estimation of conditional quantum entropy, which is the critical parameter in a QKD or QRNG security proof, is an hard problem.

Recently, Coles et al. [112] proposed a novel numerical tool for the calculation of the secure rates of any QKD protocol. This is motivated by the fact that secure rates are known only for a small class of QKD protocols: in general is very hard to provide (tight) rates for protocols without symmetries or that take into account imperfections of the practical implementation. Their approach instead, directly attacks the general entropic formulation of the secret rate, performing a numerical optimization over all the adversary strategies compatible with the data measured by Alice and Bob. Moreover, by exploiting the duality of the convex formulation of the problem they can greatly reduce the computational cost of this optimization. Finally, the dual problem involves a maximization instead of a minimization, and so the output will be a lower bound instead of an upper bound, which is returned by the primal. Therefore, if the solver doesn't reach the global optimum it will underestimate the rate, without threat to the security.

We sketch now the core idea of their approach, in order to provide a notation for the discussion about the QRNG. Further details can be found in the original article.

The scenario considered is the usual entanglement-based QKD, with two users; however the method is also valid for prepare and measure protocols, applying the source replacement trick.
In the case of one-way direct reconciliation the secure rate is given by the Devetak–Winter formula [113]:

$$K_{\text{sec}} = H(Z_A|E) - H(Z_A|Z_B) \tag{4.1}$$

where $Z_{A,B}$ are the POVM used by Alice and Bob for the generation of the key and $H(X|Y) :=$

$H(\rho_{XY})-H(\rho_Y)$ is the conditional von Neumann entropy with

$$\rho_{Z_A Z_B}=\sum_{j,k}\mathrm{Tr}\Big[(Z_A^j\otimes Z_B^k)\rho_{AB}\Big]|j\rangle\langle j|\otimes|k\rangle\langle k|\,, \tag{4.2}$$

$$\rho_{Z_A E}=\sum_j|j\rangle\langle j|\otimes\mathrm{Tr}_A[(Z_A^j\otimes\mathbb{1})\rho_{AE}]. \tag{4.3}$$

where the state ρ_{AB} shared by Alice and Bob is unknown and can, in general, be correlated with the eavesdropper whose system E purifies ρ_{AB}. Since they don't know ρ_{AB} and how much side-information has been leaked to Eve, they perform a set of local measurements $\{\Gamma_i\}$ an they estimate the expectation values $\gamma_i=\mathrm{Tr}[\Gamma_i\rho_{AB}]$. With these information they can constrain the form of ρ_{AB}, which must be contained in the set

$$\mathscr{C}=\{\rho_{AB}\,|\,\mathrm{Tr}[\Gamma_i\rho_{AB}]=\gamma_i\} \tag{4.4}$$

to reproduce the experimental observation. Since, in general, they don't perform a full quantum tomography the set $\mathscr{C}$ includes many density operators, and they pick the worst case scenario, given by:

$$K_{\mathrm{sec}}=\min_{\rho_{AB}\in\mathscr{C}}(H(Z_A|E))-H(Z_A|Z_B) \tag{4.5}$$

where $H(Z_A|Z_B)$ is pulled out from the optimization since it can be estimated from the experimental data.
However this optimization, which they refer as the primal problem, can be computationally very expensive, since the number of parameter grows as $d_A^2d_B^2$, where d_i is the dimension of the Hilbert space for the system i.

In contrast, the dual form of the problem needs to optimize over only d_C parameters, where d_C is the number of experimental constraints γ_i. Strong duality assures that the optimal objective is the same for both the primal and the dual.

In order to obtain the dual formulation we first consider the system E in Eq. 4.5 to be be a purifying system of ρ_{AB}: in this case the state pure state ρ_{ABE} is the one that maximizes Eve's information. Then, using the result for tripartite pure states that links the conditional entropy to the relative entropy [114] we ca rewrite Eq. 4.5 as:

$$K_{\mathrm{sec}}=\min_{\rho_{AB}\in\mathscr{C}}\left[D\left(\rho_{AB}\middle\|\sum_j Z_A^j\rho_{AB}Z_A^j\right)\right]-H(Z_A|Z_B) \tag{4.6}$$

where $D(x\|y)=\mathrm{Tr}\big[x\log_2(x)\big]-\mathrm{Tr}\big[x\log_2(y)\big]$ is the relative entropy.
Then is transformed to the dual:

$$K_{\mathrm{sec}}=\max_{\vec{\lambda}}\min_{\rho_{AB}\in\mathscr{P}}\left[D\left(\rho_{AB}\middle\|\sum_j Z_A^j\rho_{AB}Z_A^j\right)+\sum_i\lambda_i(\mathrm{Tr}[\rho_{AB}\Gamma_i]-\gamma_i)\right]-H(Z_A|Z_B) \tag{4.7}$$

where now the minimization is over all the semidefinite positive operators in $\mathscr{H}_{d_Ad_b}$, and the maximization is unconstrained over the multipliers λ_i.

This can be further simplified using the results of [115], where they solve analytically the minimization problem leading to:

$$K_{\text{sec}} \geq \frac{\theta}{\ln 2} - H(Z_A|Z_B) \tag{4.8}$$

$$\theta = \max_{\vec{\lambda}} \left(-\left\| \sum_j Z_A^j e^{(\mathbb{1}-\vec{\lambda}\cdot\vec{\Gamma})} Z_A^j \right\| - \vec{\lambda}\cdot\vec{\gamma} \right) \tag{4.9}$$

$$\tag{4.10}$$

where $\|\cdot\|$ is the supremum norm.
Another advantage respect to the direct solution of the primal problem, is that the dual solution always yields a lower bound instead of an upper bound. So, even if the solver doesn't find the global optimum the returned secure rate is physically possible, although not optimal. For the primal instead, only the global minimum gives a physically realizable rate, while in all the other cases it's always overestimated. For the same reason, the dual is more robust respect the finite-precision of the solvers that can be implemented in a PC.

However, this mathematical tool is helpful only if one is interested in the conditional von Neumann entropy. In the QRNG setting instead one is interested in the quantum conditional *min-entropy*, that characterizes the randomness in the single shot scenario. In the next section a new tool for the estimation of this quantity in a numerical and unstructured way will be presented.

4.2 An alternate formulation of min-entropy in the Source-DI

The usual setting considered in QKD and QRNG is the one in which the user (Alice) of the protocol measures a quantum state and is interested to evaluate the entropy of the measured (and so classical) random variable given that it can be correlated with a quantum system, that can be held by an adversary (Eve). In this scenario the state that we have to consider for the calculation of the $H_{min}(Z_A|E)$is a classical-quantum state:

$$\rho_{XE} = \sum_x p_x |x\rangle \otimes \hat{\rho}_x^E \tag{4.11}$$

where $|x\rangle$ are the possible outcomes of Alice POVM Π_x and p_x are the probabilities of the measurements, while ρ_x^E are the projected states on the adversary system after Alice's measurement. In particular we can restrict to the case where the state shared by Alice and Eve before Alice measurement is pure $|\psi_{AE}\rangle$, since this maximizes Eve's side information. In this context the classical-quantum state in Eq. 4.11, is just the post-measurement state:

$$\rho_{XE} = \sum_x |x\rangle\langle x|_A \otimes (\hat{\Pi}_x \otimes \hat{\mathbb{1}}_E) |\psi_{AE}\rangle\langle\psi_{AE}| (\hat{\Pi}_x \otimes \hat{\mathbb{1}}_E) \tag{4.12}$$

Then in this case the $H_{min}(Z_A|E)$can be written in terms of the guessing probability

$p_{guess}(X|E)$ [89] :

$$\begin{aligned} H_{min}(X|E) &= -\log_2(p_{guess}(X|E)) \\ p_{guess}(X|E) &= \max_{\hat{E}_x^E} \sum_x^d P_X(x)\,\mathrm{Tr}\left[\hat{E}_x^E \hat{\rho}_x^E\right] \end{aligned} \tag{4.13}$$

In this formulation the idea is that if an adversary has some side-information E encoded in the quantum state $\hat{\rho}_x^E$ for each x outcome of A, the maximum probability for him to guess x is obtained by maximizing over all the possible measurements he can perform $\hat{E}_x^E$, weighted by the probability of the x outcome on Alice's side. This strategy will find a set of $\hat{E}_x^E$ which will be the optimal measurements for Eve.

The calculation of this quantity can be quite hard in practice, because the set of measurements over which we have to optimize is infinite.

As seen in Section 2.3, if ρ_x^E is known there is an explicit SDP formulation for the problem of Eq 4.13, which can be efficiently solved.

However, this is no longer an SDP if $\hat{\rho}_x^E$ is unknown, since one would need to optimize over both $\hat{\rho}_x^E$ and $\vec{E_x^E}$.

Now we want to shot that the same optimization can be cast as an equivalent SDP even if $\hat{\rho}_x^E$ is unknown, of the form:

$$p_{guess}(Z_A|E) = \max_{\{\delta_x \in \mathscr{G}\}} \sum_x^d \mathrm{Tr}_{AB}\left[\left(\hat{\Pi}_x^A \otimes \hat{\mathbb{1}}^B\right)\delta_x\right] \tag{4.14}$$

which can be written as:

$$\begin{aligned} \underset{\delta_x}{\text{maximize}} \quad & \sum_x^d \mathrm{Tr}_{AB}\left[\left(\hat{\Pi}_x^A \otimes \hat{\mathbb{1}}^B\right)\delta_x\right] \\ \text{subject to} \quad & \delta_x \geq 0 \,\forall x, \\ & \mathrm{Tr}\left[\sum_x \delta_x\right] = 1, \\ & \mathrm{Tr}\left[\left(\Gamma_i^A \otimes \Gamma_j^B\right)\sum_x \delta_x\right] = \gamma_{ij} \end{aligned} \tag{4.15}$$

where δ_x can be thought as the sub-normailzed states that Eve can send to Alice and Bob, $\hat{\Pi}_x^A$ are the POVM used by Alice to generate the key and Γ_i^A, Γ_j^B are POVM that Alice and Bob use to check the incoming states while γ_{ij} are the experimental expectation values of those measurements.

Before proving this equivalence let's stop and gain a bit of intuition on why the problem can be written as in Eq 4.14.

The intuition comes from the interpretation of the min-entropy in the source-device independent scenario for QRNG presented in [1]. In that case the adversary Eve had full knowledge of the quantum state in input and she could also choose which one to send to Alice. Alice on her could measure using $\hat{\Pi}_X^A$ giving x with probability $P_X(x)$, and we are interested, again in Eve's guessing probability. In this case is natural to define it as:

$$p_{guess} = \max_{\{\delta_x \in \mathscr{G}\}} \sum_x^d \mathrm{Tr}_{AB}\left[\left(\hat{\Pi}_x^A \otimes \hat{\mathbb{1}}^B\right)\delta_x\right] \tag{4.16}$$

where τ_x^A are the states that Eve sends to Alice with probability p_x and $\hat{\Pi}_x^A$ are the measurement performed by Alice.

In this case is clear the physical meaning of this expression, since the best guessing probability for Eve is given by the state τ_x^A with the maximum overlap with Alice's measurement $\hat{\Pi}_x^A$, weighted by the occurrence of the result x.

Here we formally prove the equivalence for the two expressions 4.13 and 4.16.

Proposition 2. *Expression 4.13 and 4.16 are equivalent*

Proof. We start from the definition in 4.13

$$p_{guess} = \max_{\rho_{ABE}\in\mathscr{C}} \max_{\hat{E}_x^E} \sum_x^d P_X(x)\,\mathrm{Tr}\left[\hat{E}_x^E \hat{\rho}_x^E\right] \tag{4.17}$$

where

$$\rho_{XE} = \sum_x P_X(x)\,|x\rangle\langle x|_A \otimes \rho_X^E \tag{4.18}$$

$$\rho_X^E = \frac{\mathrm{Tr}_{AB}\left[(\hat{\Pi}_x^A \otimes \hat{\mathbb{1}}^B \otimes \hat{\mathbb{1}}_E)\rho_{ABE}\right]}{P_X(x)} \tag{4.19}$$

$$P_X(x) = \mathrm{Tr}_{ABE}\left[(\hat{\Pi}_x^A \otimes \hat{\mathbb{1}}^B \otimes \hat{\mathbb{1}}_E)\rho_{ABE}\right] \tag{4.20}$$

that can be rewritten as:

$$p_{guess} = \max_{\rho_{ABE}\in\mathscr{C}} \max_{\hat{E}_x^E} \sum_x^d P_X(x)\,\mathrm{Tr}_{BE}\left[\frac{\left(\hat{\mathbb{1}}^B \otimes \hat{E}_x^E\right)\mathrm{Tr}_A\left[(\hat{\Pi}_x^A \otimes \hat{\mathbb{1}}^B \otimes \hat{\mathbb{1}}_E)\rho_{ABE}\right]}{P_X(x)}\right] \tag{4.21}$$

$$p_{guess} = \max_{\rho_{ABE}\in\mathscr{C}} \max_{\hat{E}_x^E} \sum_x^d \mathrm{Tr}_{ABE}\left[(\hat{\Pi}_x^A \otimes \hat{\mathbb{1}}^B \otimes \hat{E}_x^E)\rho_{ABE}\right] \tag{4.22}$$

The idea is that for any POVM element of Alice, Eve should measure ρ_{ABE} in such a way to maximize her information gain. From the point of view of Alice, she will receive some states τ_x from Eve. So

$$p_{guess} = \max_{\rho_{ABE}\in\mathscr{C}} \max_{\{\hat{E}_x^E\}} \sum_x^d \mathrm{Tr}_{AB}\left[\left(\hat{\Pi}_x^A \otimes \hat{\mathbb{1}}^B\right)\underbrace{\mathrm{Tr}_E\left[(\hat{\mathbb{1}}^A \otimes \hat{\mathbb{1}}^B \otimes \hat{E}_x^E)\rho_{ABE}\right]}_{\tilde{p}_x\tau_x=\delta_x}\right] \tag{4.23}$$

$$p_{guess} = \max_{\{\delta_x\in\tilde{\mathscr{C}}\}} \sum_x^d \mathrm{Tr}_{AB}\left[\left(\hat{\Pi}_x^A \otimes \hat{\mathbb{1}}^B\right)\delta_x\right] \tag{4.24}$$

$$\tag{4.25}$$

where δ_x are sub-normalized states ad the optimization is constrained over the set $\tilde{\mathscr{C}}$ that is compatible with the experimental observations. □

This optimization is equivalent to the SDP in Eq. 4.15. In the QRNG scenario that expression can be further simplified since Bob's system $\mathscr{H}_B$ is trivial:

$$\begin{aligned} \underset{\delta_x}{\text{maximize}} \quad & \sum_x^d \text{Tr}_A\left[\hat{\Pi}_x^A \delta_x\right] \\ \text{subject to} \quad & \delta_x \geq 0 \,\forall x, \\ & \text{Tr}\left[\sum_x \delta_x\right] = 1, \\ & \text{Tr}\left[\Gamma_i^A \sum_x \delta_x\right] = \gamma_i \end{aligned} \tag{4.26}$$

This SDP however doesn't include finite size effects in the parameter estimation. In fact here we assume to have an infinite statistic and to measure γ_{ij} with infinite precision. Unfortunately this is never possible experimentally, since the acquisitions can only run for a finite amount of time. In this case the experimental expectation values γ_{ij} will be inevitably be affected by a statistical uncertainty and their estimate will be associated to a confidence interval $[\gamma_{ij} - \zeta(n,\epsilon), \gamma_{ij} + \zeta(n,\epsilon)]$ (we are assuming symmetric intervals but the works also for asymmetric intervals.) Since we are worried about the security the optimization over which the states $\rho_A BE$ are constrained needs to be performed for all the values in these confidence intervals, picking the most conservative one.

Luckily the finite size corrections can be easily included in the optimization relaxing the last constraint:

$$\begin{aligned} \underset{\delta_x}{\text{maximize}} \quad & \sum_x^d \text{Tr}_{AB}\left[\left(\hat{\Pi}_x^A \otimes \hat{\mathbb{1}}^B\right) \delta_x\right] \\ \text{subject to} \quad & \delta_x \geq 0 \,\forall x, \\ & \text{Tr}\left[\sum_x \delta_x\right] = 1, \\ & |\,\text{Tr}\left[\left(\Gamma_i^A \otimes \Gamma_j^B\right) \sum_x \delta_x\right] - \gamma_{ij}| \leq \zeta(n) \end{aligned} \tag{4.27}$$

where $\zeta(n,\epsilon)$ is usually given by a tail inequality such as the Chernoff-Hoeffding [116] or the Azuma [117].

4.2.1 Duality

The SDP proposed can efficiently estimate the guessing probability from the data statistics providing an optimal key rate. In this formulation it represents a maximization problem on the guessing probability, that is a minimization on the min-entropy. We will call this problem the primal problem. Similarly to the primal problem presented in Section 4.1, if the optimal solution is not reached (due to finite precision of the machine, or other problems) the solution would underestimate the guessing probability and so, overestimate the secure rate. This is clearly not acceptable for security applications. Moreover, every time new γ_{ij} are calculated a new SDP has to be run, reducing the speed in a real-time operation. Luckily all

these problems can be solved using the dual formulation of the SDP. This dual optimization problem provides an upper bound on the solution of the primal. In this way the guessing probability is never underestimated, giving always conservative bounds on key secret key rate. Additionally, the dual objective function is a linear function of the γ_{ij}, making it possible to compute a (sub-optimal) bound when new γ_{ij} are given, without having to re run the SDP. We will now derive the dual formulation of the general form for the SDP given by Eq 4.27, since the other special cases can be retrieved in the limits $\zeta \to 0$.

Proposition 3. *The dual SDP of 4.27 is given by*

$$\begin{aligned} \underset{b,c_{ij},e_{ij},f_{ij}}{\text{minimize}} \quad & -b + \sum_{ij} \gamma_{ij}\left(e_{ij} - f_{ij}\right) + \zeta(n)\left(e_{ij} + f_{ij}\right) \\ \text{subject to} \quad & \left(\left(\hat{\Pi}_x^A \otimes \mathbb{1}^B\right) + b\mathbb{1} + \sum_{ij}\left(f_{ij} - e_{ij}\right)\left(\hat{\Gamma}_i^A \otimes \hat{\Gamma}_j^B\right)\right) \leq 0 \;\forall x, \\ & e_{ij} \geq 0 \;\forall i,j, \\ & f_{ij} \geq 0 \;\forall i,j \end{aligned} \tag{4.28}$$

The objective function is indeed linear in the experimental data γ_{ij}

Proof. Our primal SDP is given by:

$$\begin{aligned} \underset{\delta_x}{\text{maximize}} \quad & \sum_x^d \text{Tr}_{AB}\left[\left(\hat{\Pi}_x^A \otimes \hat{\mathbb{1}}^B\right)\delta_x\right] \\ \text{subject to} \quad & \delta_x \geq 0 \;\forall x, \\ & \text{Tr}\left[\sum_x \delta_x\right] = 1, \\ & \left|\text{Tr}\left[\left(\Gamma_i^A \otimes \Gamma_j^B\right)\sum_x \delta_x\right] - \gamma_{ij}\right| \leq \zeta(n) \end{aligned} \tag{4.29}$$

but we rewrite the last constraint using slack variable in order to have only equality constraint except for the positive semidefinite condition.

$$\begin{aligned} \underset{\delta_x}{\text{maximize}} \quad & \sum_x^d \text{Tr}_{AB}\left[\left(\hat{\Pi}_x^A \otimes \hat{\mathbb{1}}^B\right)\delta_x\right] \\ \text{subject to} \quad & \delta_x \geq 0 \;\forall x, \\ & \text{Tr}\left[\sum_x \delta_x\right] = 1, \\ & \text{Tr}\left[\left(\Gamma_i^A \otimes \Gamma_j^B\right)\sum_x \delta_x\right] - \gamma_{ij} + s_{ij} = \zeta(n), \\ & -\text{Tr}\left[\left(\Gamma_i^A \otimes \Gamma_j^B\right)\sum_x \delta_x\right] + \gamma_{ij} + t_{ij} = \zeta(n), \\ & s_{ij} \geq 0, \\ & t_{ij} \geq 0 \end{aligned} \tag{4.30}$$

We first write the associated Lagrangian:

$$\begin{aligned}\mathscr{L} = &\mathrm{Tr}\left[\sum_x \left(\hat{\Pi}_x^A \otimes \mathbb{1}^B\right)\delta_x\right] + \sum_x \mathrm{Tr}\left[G_x \delta_X\right] + b\left(\mathrm{Tr}\left[\sum \delta_x\right] - 1\right) \\ &+ \sum_{ij} c_{ij}\left(\mathrm{Tr}\left[\left(\hat{\Gamma}_i^A \otimes \hat{\Gamma}_j^B\right)\sum_x \delta_x\right] - \gamma_{ij} + s_{ij} - \zeta(n)\right) \\ &+ \sum_{ij} d_{ij}\left(-\mathrm{Tr}\left[\left(\hat{\Gamma}_i^A \otimes \hat{\Gamma}_j^B\right)\sum_x \delta_x\right] + \gamma_{ij} + t_{ij} - \zeta(n)\right) \\ &+ \sum_{ij} e_{ij} s_{ij} + \sum_{ij} f_{ij} t_{ij}\end{aligned} \tag{4.31}$$

where G_x, b, c_{ij}, d_{ij}, e_{ij} and f_{ij} are the Lagrange multipliers. Then we group all the operators that multiply δ_x

$$\begin{aligned}\mathscr{L} = &\sum_x \left(\mathrm{Tr}\left[\delta_x\left(\left(\hat{\Pi}_x^A \otimes \mathbb{1}^B\right) + G_x + b\mathbb{1} + \sum_{ij} c_{ij}\left(\hat{\Gamma}_i^A \otimes \hat{\Gamma}_j^B\right) - \sum_{ij} d_{ij}\left(\hat{\Gamma}_i^A \otimes \hat{\Gamma}_j^B\right)\right)\right]\right) \\ &- b + \sum_{ij}\left[c_{ij}\left(-\gamma_{ij} + s_{ij} - \zeta(n)\right) + d_{ij}\left(\gamma_{ij} + t_{ij} - \zeta(n)\right) + s_{ij} e_{ij} + f_{ij} t_{ij}\right]\end{aligned} \tag{4.32}$$

$$\begin{aligned}\mathscr{L} = &\sum_x \left(\mathrm{Tr}\left[\delta_x \underbrace{\left(\left(\hat{\Pi}_x^A \otimes \mathbb{1}^B\right) + G_x + b\mathbb{1} + \sum_{ij}\left(c_{ij} - d_{ij}\right)\left(\hat{\Gamma}_i^A \otimes \hat{\Gamma}_j^B\right)\right)}_{K_x}\right]\right) \\ &\underbrace{-b + \sum_{ij}\left[c_{ij}\left(-\gamma_{ij} + s_{ij} - \zeta(n)\right) + d_{ij}\left(\gamma_{ij} + t_{ij} - \zeta(n)\right) + s_{ij} e_{ij} + f_{ij} t_{ij}\right]}_{\Delta}\end{aligned} \tag{4.33}$$

$$\mathscr{L} = \sum_x \mathrm{Tr}\left[\delta_x K_x\right] + \Delta \tag{4.34}$$

Then we find the conditions for the optimum:

$$\frac{\partial \mathscr{L}}{\partial \delta_x} = 0 \rightarrow K_x = 0 \tag{4.35}$$

$$\frac{\partial \mathscr{L}}{\partial s_{ij}} = 0 \rightarrow \left(c_{ij} + e_{ij}\right) = 0 \tag{4.36}$$

$$\frac{\partial \mathscr{L}}{\partial t_{ij}} = 0 \rightarrow \left(d_{ij} + f_{ij}\right) = 0 \tag{4.37}$$

So at the optimal point the following conditions must be met:

$$c_{ij} = -e_{ij} \tag{4.38}$$
$$d_{ij} = -f_{ij} \tag{4.39}$$
$$\Delta^* = -b + \sum_{ij} \gamma_{ij}\left(e_{ij} - f_{ij}\right) + \zeta(n)\left(e_{ij} + f_{ij}\right) \tag{4.40}$$
$$K_x^* = \left(\left(\hat{\Pi}_x^A \otimes \mathbb{1}^B\right) + b\mathbb{1} + \sum_{ij} \left(f_{ij} - e_{ij}\right)\left(\hat{\Gamma}_i^A \otimes \hat{\Gamma}_j^B\right) \right) \leq 0 \tag{4.41}$$

In the constraint on K_x we dropped G_x since they always need to be semidefinite positive and replaced the equality with the inequality.

Finally the problem can be written in its dual form:

$$\begin{aligned} \underset{b, e_{ij}, f_{ij}}{\text{minimize}} \quad & \Delta^* \\ \text{subject to} \quad & K_x^* \leq 0 \, \forall x, \\ & e_{ij} \geq 0 \, \forall i, j, \\ & f_{ij} \geq 0 \, \forall i, j \end{aligned} \tag{4.42}$$

or explicitly:

$$\begin{aligned} \underset{b, e_{ij}, f_{ij}}{\text{minimize}} \quad & -b + \sum_{ij} \gamma_{ij}\left(e_{ij} - f_{ij}\right) + \zeta(n)\left(e_{ij} + f_{ij}\right) \\ \text{subject to} \quad & \left(\left(\hat{\Pi}_x^A \otimes \mathbb{1}^B\right) + b\mathbb{1} + \sum_{ij} \left(f_{ij} - e_{ij}\right)\left(\hat{\Gamma}_i^A \otimes \hat{\Gamma}_j^B\right) \right) \leq 0 \, \forall x, \\ & e_{ij} \geq 0 \, \forall i, j, \\ & f_{ij} \geq 0 \, \forall i, j \end{aligned} \tag{4.43}$$

□

The asymptotic dual form is recovered in the limit $\zeta(n) \to 0$:

$$\begin{aligned} \underset{b, c_{ij}}{\text{minimize}} \quad & -b - \sum_{ij} c_{ij}\gamma_{ij} \\ \text{subject to} \quad & \left(\hat{\Pi}_x^A \otimes \mathbb{1}^B\right) + b\mathbb{1} + \sum_{ij} c_{ij}\left(\hat{\Gamma}_i^A \otimes \hat{\Gamma}_j^B\right) \leq 0 \, \forall x \end{aligned} \tag{4.44}$$

As anticipated this dual formulation has several advantages. The fact that always returns a lower-bound is fundamental for protocols that rely on security. For practical applications, the linearity of the objective function is game-changer point. In practical protocols the min-entropy has to be evaluated for every block of keys or random numbers. Although the SDP can reach the global optimum efficiently on modern PC, that still requires second or even minutes for large problems. Clearly this is not acceptable if a real-time operation is necessary. Moreover, randomness extraction and privacy amplification are usually performed directly

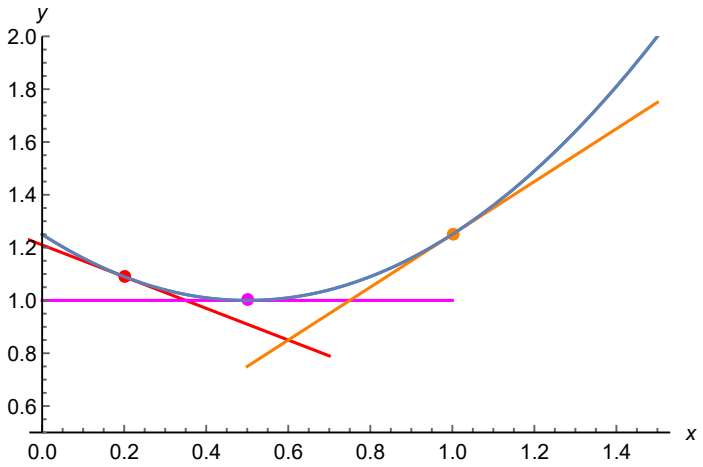


Figure 4.1: *Linerization of a convex function in any point will provide a strictly lower bound of the function.*

in hardware (such FPGA), in order to speed up the processing and achieve high bandwidth. For this platforms SDP solvers are still lacking. However, since the the dual formulation is linear in the γ_{ij}, given a set of parameters b^*, e^*_{ij}, f^*_{ij} that are optimal for certain values of $\tilde{\gamma}_{ij}$, if the function δ is then evaluated with the same parameters, but different γ_{ij} it will always provide strictly lower bound. The situation is graphically explained in Figure 4.1 Then is possible to compute in advance the full dual SDP for some parameters γ_{ij} and store it in a Look Up Table on the FPGA. When the experiments will output a particular set og γ_{ij} the FPGA will pick the closer parameters and only evaluate the linear function δ instead of the full SDP. This will slightly reduce the number of bits in the outcome but can be implemented at much higher speeds.

4.3 Comparison with the Entropic Uncertainty Principle and Quantum State Tomography

Before applying this new method to scenarios where we don't have optimal tool for the evaluation of the min-entropy, we want to test it respect known solutions, in order to check it's consistency.

In the Source-DI QRNG scenario there are few way to obtain tight bounds for the quantum-conditional min-entropy in specific scenarios.

The first one has been proposed by *Fiorentino et al.* in [108] but is only valid for qubits and requires a set of tomographyically complete measurements.

Consider a unknown qubit state represented by the density matrix ρ_A. This can be parameterized as a function of the Stokes parameters

$$\rho_A(S_1,S_2,S_3)=\begin{bmatrix} 1+S_3 & S_1-i\cdot S_2 \\ S_1+i\cdot S_2 & 1-S_3 \end{bmatrix} \tag{4.45}$$

If a set of tomographyically complete measurements, $\hat{P}^{\pm}_x, \hat{P}^{\pm}_y, \hat{P}^{\pm}_z$ is used, the parameters

S_1, S_2, S_3 can be retrieved from the measurements and ρ_A is fully reconstructed. In [108] the authors prove that if the generation of random number is performed registering the outputs measured in the Z basis $|0\rangle, |1\rangle$ then:

$$H_{min}(Z|E) \geq -\log_2\left(\frac{1+\sqrt{1-|(S_1 - i\cdot S_2)|^2)}}{2}\right) \tag{4.46}$$

The relation is in line with our intuition: the closer ρ_A is to a pure state and the further it is from the Z projector, the higher is the min-entropy. Their solutions exploits the geometry of the Bloch sphere and provides a tight bound.

In order to test the new SDP tool we considered the same scenario: we neglected the finite size effect in the dual SDP and considered the QRNG scenario where Bob's system is trivial:

$$\begin{aligned} \underset{b, c_i}{\text{minimize}} \quad & -b - \sum_i c_i \gamma_i \\ \text{subject to} \quad & \hat{\Pi}_x^A + b\mathbb{1} + \sum_{ij} c_i \hat{\Gamma}_i^A \leq 0 \; \forall x \end{aligned} \tag{4.47}$$

where key generating POVM
$\hat{\Pi}_x^A = \{|0\rangle\langle 0|, |1\rangle\langle 1|$ and the control POVM $\Gamma_i^A = \{|0\rangle\langle 0|, |1\rangle\langle 1|, |+\rangle\langle +|, |-\rangle\langle -|, |L\rangle\langle L|, |R\rangle\langle R|\}$

Then we generated 10000 random matrices covering the entire Bloch sphere and we evaluated the differences between the analytic value of Eq 4.46 and the SDP output. The SDP has been implemented in Python 2.7 using the PICOS library [118] for the modeling of the problem and the python interface to the MOSEK solver [119]. The software internally uses functions from the QuTip module [120].

The results are presented in Fig. 4.2

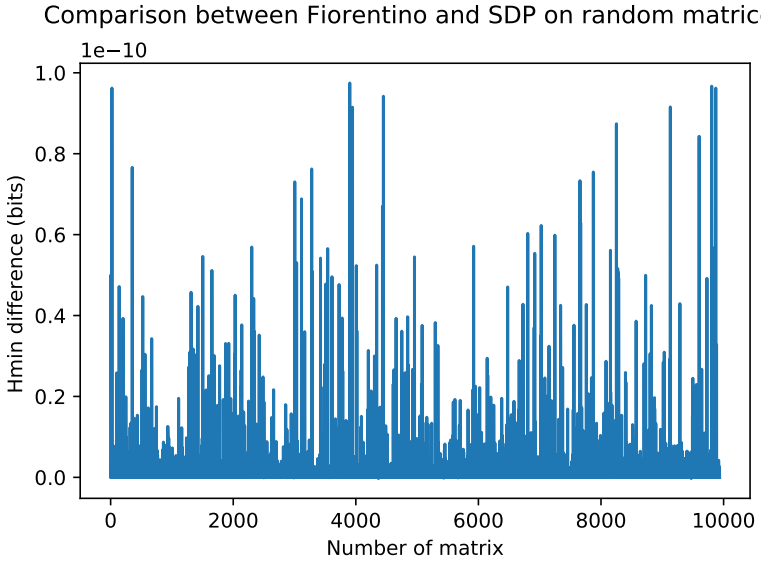


Figure 4.2: *Comparison between the analytical results of [108] and the numerics from the SDP for a qubit measured with a set of tomographically complete measurements. The tolerance of the solver is* $10^{-}8$.

As we can see the results agree, up to a factor 10^{-10}, smaller than the tolerance of the solver 10^{-8} and, more importantly, they never overestimate the min-entropy.

Another method that is able to give tight bounds in some scenario, was first proposed by *Vallone et al.* in [78] and relies on the Entropic Uncertainty Principle.

In this protocol (valid not only for qubits), the random state ρ_A is measured in two conjugate bases: $M_Z = |0\rangle\langle 0|, |1\rangle\langle 1|$ called the generation base and $N_X = |+\rangle\langle +|, |-\rangle\langle -|$ called the check base.

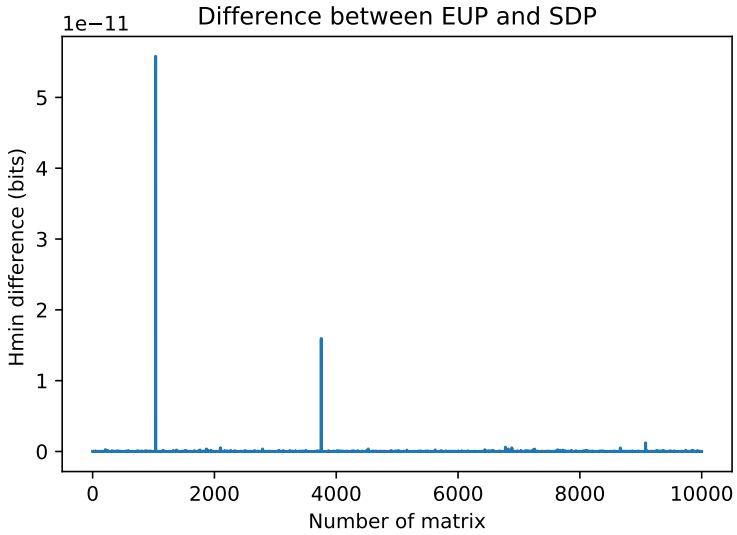


Figure 4.3: *Comparison between the analytical results of [78] and the numerics from the SDP for a qubit mesured with a set of conjugate measurements. The tolerance of the solver is* $10^{-}8$.

Then for a generic tripartite state $\rho_A EB$ that purifiesρ_A the EUP can be written as:

$$H_{min}(Z|E)_{\rho_{AEB}} + H_{max}(X|B)_{\rho_{AEB}} \geq q_{MU} \tag{4.48}$$

$$q_{MU} = \log_2\left(\frac{1}{c_{max}}\right) \tag{4.49}$$

$$c_{max} = \max_{j,k} |\langle x_j | z_k \rangle|^2 \tag{4.50}$$

where q_{MU} is the Maassen-Uffink compatibility factor. In the QRNG case the system B is trivial and we have:

$$H_{min}(Z|E)_{\rho_{AE}} \geq q_{MU} - H_{max}(X) \tag{4.51}$$

If M_Z and N_X are measurements corresponding to Mutually Unbiased Basis in dimension d, $q_{MU} = \log_2(d)$, and the EUP is tight.

Then we will have for qubits:

$$H_{min}(Z|E)_{\rho_{AE}} \geq \log_2(2) - H_{max}(X) \tag{4.52}$$

Since $H_{max}(X)$ now is not conditioned on anything, it can be easily estimated from the

data [78]:

$$H_{max}(X)=2\log_2(\sum_{x=0}^{d-1}P_x(x)) \tag{4.53}$$

where $P_x(x)$ are the probabilities of the outcomes in the N_X basis.

We employed the same approach as before in order to compare the two estimates, where now the $\hat{\Pi}_x^A=\{|0\rangle\langle 0|,|1\rangle\langle 1|$ and the control POVM $\Gamma_i^A=\{|0\rangle\langle 0|,|1\rangle\langle 1|,|+\rangle\langle +|,|-\rangle\langle -|\}$

The results are presented in Fig 4.3 and as we can see we get the same results up to a factor $\leq 10^{-10}$ which is smaller than the tolerance of the solver used.

The ultimate limit in the estimation is given by the number of bits employed for the representation of float numbers on the PC and tolerance of the solver used. The problem can be solved using arbitrary precision math libraries [121] and arbitrary precision SDP solvers such as SDPA-GMP[122]. However, this is usually not required for our applications and we will work with the tolerances presented above.

4.4 Tighter bound than the EUP

The EUP presented in Eq. 4.50 is known to be tight only for projective measurements that represents MUB, and it can be quite loose for other projective measurements and POVM in general.

In [123] the authors propose few bounds on the EUP that are tighter than the common Maassen-Uffink state independent bound. The tightest presented can only be evaluated numerically: we will call it EUP_{tight} and can be computed as:

$$H(Z|E)_{min}+H(X|B)_{max}>q_t^* \tag{4.54}$$

$$q_t^*=\max_{0\leq p\leq 1}\lambda_{min}[\Delta(p)] \tag{4.55}$$

$$\Delta(p)=p\Delta_{XZ}+(1-p)\Delta_{ZX} \tag{4.56}$$

$$\delta(X,Z)=\sum_x a_x(X,Z)\cdot X_x \tag{4.57}$$

$$a_x(X,Z)=-\log_2(||\sum_z Z_z X_x Z_z||_\infty) \tag{4.58}$$

$$\tag{4.59}$$

where $||\cdot||$ is the sup norm.

Here we want to first reproduce the results of their paper and then compare it with our SDP method in scenarios where the EUP is not tight to see if we can get tighter bounds.

In [123] the author consider the following situation: they fix the dimension of the Hilbert space $d=dim(\mathscr{H}_A)=3$ and they introduce the following measurements $Z=\{|0\rangle,|1\rangle,|2\rangle\}$,$X=\{U|0\rangle,U|1\rangle,U|2\rangle\}$ with

$$U=\begin{bmatrix}\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}}\\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{6}} & -\frac{2}{\sqrt{3}} & \frac{1}{\sqrt{6}}\end{bmatrix} \tag{4.60}$$

and they expect: $q_{MU}=0.58$, $q_t=0.64$ In this case we get: $q_t:0.64$ and the right dependence of $q_t(p)$ from the parameter p (see [123]).

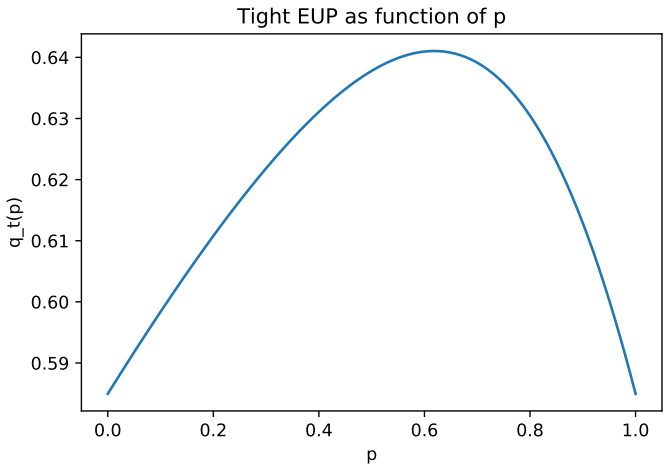


Figure 4.4: *Dependence of the $q_t(p)$ factor from the parameter p*

Then we consider a simple qubit scenario, similar to the one presented in [78], but instead of having two MUB measurements, we consider what happen when the "check" measurements N_x is rotated by an angle θ respect to the "generation" measurement M_z. If we send a state $\rho_A = |+\rangle\langle+|$ it should saturate the bound of $log_2(d) = 1$). In Figure 4.5 the comparison between the tight EUP and the SDP are presented.

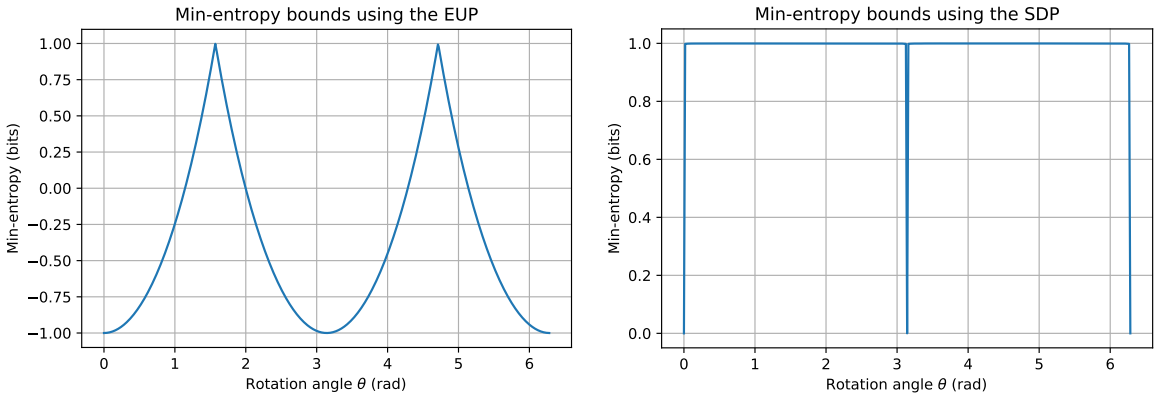


Figure 4.5: *Comparison between the estimation of $H_{min}(Z|E)$ for qubits when the check basis is rotated by θ respect the generation basis. The left panel shows the estimation using the EUP while the right panel shows the SDP results.*

The difference between the two estimation is quite remarkable. As expected the EUP can saturate the bound only for $\theta = \frac{\pi}{2}$, which is the case of MUB considered before. However until $\theta \approx 65°$ no randomness can be certified. On the contrary, the SDP saturates the bound $\log_2(d)$ for any measurement N_X which is rotated by ϵ (up to numeric precision) respect to M_Z. Intuitively this is the expected behavior: in the limit of infinite statistics the any rotated basis with $\theta \neq 0, \pi$ provides different expectation values between a pure state and a mixed

state, and so is able to correctly bound the purity of the incoming state.

4.5 Analysis of the discrete POVM QRNG

Another interesting scenario to consider is the one where only one set of measurement is used for both generation and estimation of the randomness.

We have seen that if projective measurements are used, it is not possible to bound the purity of a state with only one set of measurements, but at least two are needed. However, the situation changes if general POVM are used, as in the case of 3.1.2.

Can we get tight results with the Entropic uncertainty principle and what about the SDP?

We consider a qubit scenario where the generation is done with the following POVM:

$$\hat{\Pi}_1 = \frac{2}{3} |1\rangle \langle 1| = \frac{2}{3} |\psi_1\rangle \langle \psi_1| \tag{4.61}$$

$$\hat{\Pi}_2 = \frac{2}{3} \left(\frac{\sqrt{3}}{2} |0\rangle - \frac{1}{2} |1\rangle \right) \left(\frac{\sqrt{3}}{2} \langle 0| - \frac{1}{2} \langle 1| \right) = \frac{2}{3} |\psi_2\rangle \langle \psi_2| \tag{4.62}$$

$$\hat{\Pi}_3 = \frac{2}{3} \left(\frac{\sqrt{3}}{2} |0\rangle - \frac{1}{2} |1\rangle \right) \left(\frac{\sqrt{3}}{2} \langle 0| - \frac{1}{2} \langle 1| \right) = \frac{2}{3} |\psi_3\rangle \langle \psi_3| \tag{4.63}$$

Instead of considering only this particular case, we analyze a more general scenario where the generation is done with $\{\hat{\Pi}_1, \hat{\Pi}_2, \hat{\Pi}_3\}$ and the check is done with the same POVM rotated by θ. Given the shape of the POVM, we evaluate the min-entropy for the state $\rho_A = |0\rangle$, which is supposed to saturate the bound. We compared two versions of the EUP, the Maassen-Uffink and the tight one, against the SDP. The special case of generation and check with a single set of measurements is retrieve for $\theta = 0$.

The results are presented in Fig 4.6

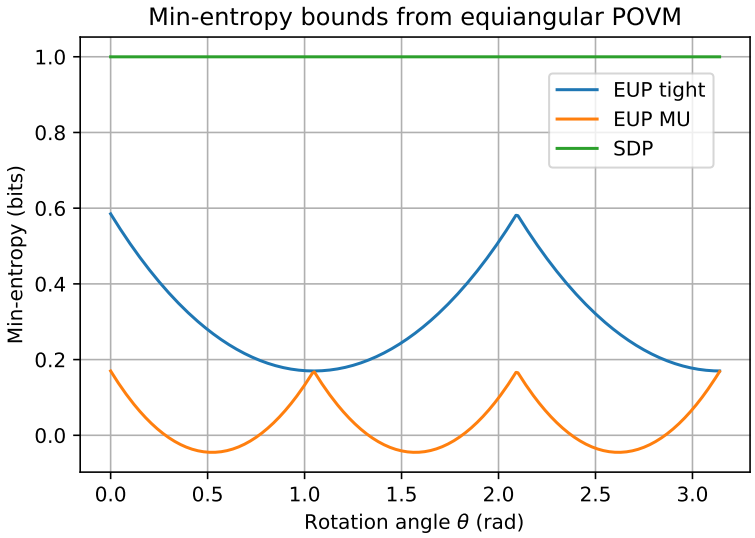


Figure 4.6: *Dependance of the $q_t(p)$ factor from the parameter p*

From the results we can see that the tight bound of the EUP always outperforms the Maassen-Uffink and the maximum of $H_{min}(Z|E) \approx 0.585$ is reached for $\theta = 0$, so in the one POVM condition. The SDP instead is always able to certify 1 bit of entropy (which is the maximum extractable in this case) for every value of θ, including when only one POVM is used.

These numerical findings have motivated the development of a new Source-DI QRNG protocol based on single POVM measurements, presented in Chap. 5. The numerical results obtained from the SDP have been used at the beginning, to validate our intuition and then helped in analyzing the attacker's strategy for developing an analytic solution.

4.6 Conclusions

In this Chapter we have presented a new tool for the estimation of the quantum conditional min-entropy $H_{min}(X|E)$ when the key generation measurements and the control check POVM are known. The method can take into account finite-size effects and, more importantly, can be expressed in terms of SDP that enable an efficient implementation on modern PC and are assured to converge to the global optimum. Moreover, the linearity of the objective function in the dual formulation makes it practical for applications where high-speed computation of the $H_{min}(X|E)$ is required.

With this new tool we computed the expected $H_{min}(X|E)$ for the protocols described in [108] and [78] where tight results were already known. In both cases the SDP was able to reproduce the results up to a precision limited by the tolerance of the solver ($10^{-}8$). Then we compared the results of our method and the EUP is scenarios where the EUP is known to provide non-tight results (ie. for non-MUB projective measurements and POVM). Our method always outperformed the EUP in every scenario.

Finally, we have applied it for the estimation of randomness in a newly developed Source-DI QRNG protocol presented in Chap 5.

The method showed a great flexibility and high performance, making it a new useful tool for the evaluation of security of unstructured QRNG and QKD protocols.

CHAPTER 5

Unbounded Randomness in finite dimensions: A POVM approach

Almost all the DI and SDI protocol for QRNG employ projective measurements, thus limiting the maximal certification to 1 bit per measurement for qubits. The possibility to increase the generation rate using general measurement has been discussed for entangled system in the device-independent scenario [82, 124, 125]. While projective measurements can only certify up to one bit of randomness for every pair of entangled qubits, POVM can saturate the optimal bound of 2 bit. Additionally, unbounded generation is possible if repeated non-demolition measurements are performed on one of the qubits [126]. However, all these scenarios require entanglement as a resource.

Here we try to address a different problem: is it possible to have an unbounded randomness generation from a qubit using am SDI prepare and measure scheme, where coherence is the resource? The answer is yes. Using generalized POVM measurement, it is possible to increase both the number of random bits that can be certified per measurement and the security, in a Source-Device-Independent (Source-DI) way, since the certification is done without any assumption on the source. The amount of randomness, for a fixed dimension of the POVM, scales $\propto log_2(N)$ with N the number of POVM outcomes, so that an unbounded amount of random bits can be certified for any dimension of the measured quantum system. In order to validate these findings, an optical setup implementing a 3,4 and 6 outcomes POVM has been realized, using heralded qubits from a Sagnac entangled source.

5.1 Theory

In the prepare and measure scenario a QRNG is composed of two systems: a source, that emits a quantum state $\hat{\rho}_A$ and a measurement station that performs a set of measurements $\{\hat{M}_i\}$ on the received state. At each round, the measurement device produces an outcome X with some probability P_X. In the trusted scenario both $\hat{\rho}_A$ and $\hat{M}_i$ are known and characterized: in this case the number of random bit that can be extracted is given by the classical min-entropy $H_{min}(X) = -\max_X \left(\log_2(P_X)\right)$. In the Source-DI scenario, no assumptions are

made on the source and an attacker, Eve, could also share quantum correlation with the unknown received $\hat{\rho}_A$ state. In this case, the amount of **private** randomness that can be extracted is correctly quantified by the quantum conditional min-entropy $H_{min}(X|E)$, where Alice's output is conditioned on Eve's (quantum) side information E. Bounding $H_{min}(X|E)$ is harder than $H_{min}(X)$, since requires to optimize over all Eve's strategies compatible with the measured data.

As discussed in Section 3.1.2, if the received state $\hat{\rho}_A$ is pure, Eve does not have access to any quantum side information, since a joint Alice-Eve state must be separable $\hat{\rho}_{AE} = \hat{\rho}_A \otimes \hat{\rho}_E$. On the contrary, if $\hat{\rho}_A$ is mixed, there always exists a purification $\hat{\rho}_{AE}$ of $\hat{\rho}_A$, such that the systems A and E are correlated. Bounding the $H_{min}(X|E)$ is then profoundly linked with the problem of bounding the purity of the unknown state $\hat{\rho}_A$.

For qubits, an analytic solution has been proposed in [108], where a set of tomographically complete measurements is used to reconstruct $\hat{\rho}_A$ and hence bound the $H_{min}(X|E)$ as a function of only the Stokes parameters:

$$f(\hat{\rho}) = -\log_2\left(\frac{1+\sqrt{1-|S_1 - iS_2|^2}}{2}\right) \geq H_{min}(\rho) \tag{5.1}$$

Unfortunately, the method is only valid for qubits and requires the full tomography of the incoming stated $\hat{\rho}_A$, which can be expensive to perform, especially for higher dimensional states.

Another solution exploits the Entropic Uncertainty Principle, where measurements in two conjugate bases M_Z, N_X allow to bound the quantum conditional min-entropy thanks to the following relation:

$$H_{min}(Z|E)_{\rho_{AE}} \geq q - H_{max}(X) = q - 2\log_2\left(\sum_{x=0}^{d-1} P_x(x)\right) \tag{5.2}$$

where q is the compatibility factor, already discussed in Chap 4. However, we have seen in Sec 4.3 that the EUP is not tight when POVMs are used.

We are interested in deriving a tight bound for the $H_{min}(X|E)$ when a POVM is used in a qubit protocol. In this case, Eve sends unknown qubit states $\hat{\rho}_A$ and Alice uses a POVM for both the generation and the check stage. At first sight, one could argue that the protocol is not really Source-DI, since we are assuming that $\hat{\rho}_A$ is a qubit. However, if the POVMs used by Alice, are spanning only a two dimensional space (i.e., they measure along linear combination of $|0\rangle$ and $|1\rangle$), Eve has no advantage to send a higher dimensional system and we can consider, without loss of generality, the incoming $\hat{\rho}_A$ as a qubit. This intuitive idea can be formalized, introducing a squashing model for the measurement [80].

In this section, we will fist use the numerical tool described in Chapter 4 to get reliable and tight bounds on the $H_{min}(X|E)$. Then we will use the information obtained from the optimal points retrieved by the SDP to study and gain an intuition of the optimal strategy for the attacker. Finally, taking into account this information, we will derive an analytical bound (similar to 5.1) for some particular shapes of the POVM.

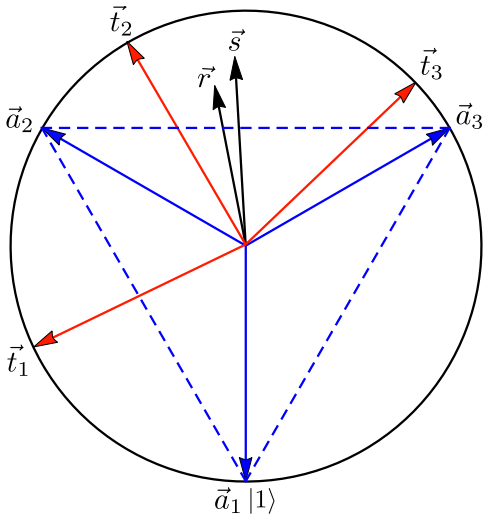


Figure 5.1: *The blue vectors represents the measurements of the POVM in the XZ plane of the Bloch sphere. The red vectors represent a possible strategy for Eve.*

5.1.1 The Three-State POVM: Numerical results

Let's consider the simple case of a three equiangular POVM on the equator of the Bloch sphere depicted in Fig 5.1

The POVM are:

$$\hat{\Pi}_1 = \frac{2}{3} |1\rangle \langle 1| = \frac{2}{3} |\psi_1\rangle \langle \psi_1| \tag{5.3}$$

$$\hat{\Pi}_2 = \frac{2}{3} \left(\frac{\sqrt{3}}{2} |0\rangle + \frac{1}{2} |1\rangle \right) \left(\frac{\sqrt{3}}{2} \langle 0| + \frac{1}{2} \langle 1| \right) = \frac{2}{3} |\psi_2\rangle \langle \psi_2| \tag{5.4}$$

$$\hat{\Pi}_3 = \frac{2}{3} \left(\frac{\sqrt{3}}{2} |0\rangle - \frac{1}{2} |1\rangle \right) \left(\frac{\sqrt{3}}{2} \langle 0| - \frac{1}{2} \langle 1| \right) = \frac{2}{3} |\psi_3\rangle \langle \psi_3| \tag{5.5}$$

but we can write them in a more compact form as:

$$\hat{\Pi}_x = \frac{1}{3} (\mathbb{1} + \vec{a}_x \cdot \vec{\sigma}) \tag{5.6}$$

$$\vec{a}_1 = (0, 0, -1) \quad \vec{a}_2 = (\frac{\sqrt{3}}{2}, 0, \frac{1}{2}) \quad \vec{a}_3 = (\frac{\sqrt{3}}{2}, 0, \frac{1}{2}) \tag{5.7}$$

where $\vec{\sigma} = \{\sigma_x, \sigma_y, \sigma_z\}$ is the vector of the Pauli matrices.

To get reliable numerical lower-bounds on the achievable $H_{min}(X|E)$ we can use a simplified version of the dual formulation of the SDP introduced in Eq. 4.47

$$\begin{aligned} \underset{b, c_i}{\text{minimize}} \quad & -b - \sum_i c_i \gamma_i \\ \text{subject to} \quad & \hat{\Pi}_x^A + b\mathbb{1} + \sum_{ij} c_i \hat{\Gamma}_i^A \leq 0 \quad \forall x \end{aligned} \tag{5.8}$$

where Bob's system is considered trivial, and the rates are calculated in the asymptotic regime $n \to \infty$.

In this specific case the POVM $\{\hat{\Pi}_1, \hat{\Pi}_2, \hat{\Pi}_3\}$ is used both for the random number generation and for the check of the purity of $\hat{\rho}_A$. So in the above optimization, we will have:

$$\hat{\Pi}_i^A = \hat{\Pi}_i \quad \forall i \tag{5.9}$$

$$\hat{\Gamma}_i^A = \hat{\Pi}_i \quad \forall i \tag{5.10}$$

Then, we need to provide the experimental expectation values γ_i. In order to do that, $\hat{\rho}_A$ are generated such that they sample all the Bloch sphere and then $\gamma_i = \mathrm{Tr}\{\hat{\rho}_A \hat{\Pi}_i\}$.

The results, for the XZ plane of the Bloch sphere, are presented in the contour plot in Fig 5.2

It is possible to distinguish two different areas: the one inside the lines that connect the three $\vec{a}_i$ of the POVM, and the one outside. Inside this region, the $H_{min}(X|E)$ is minimal and constant with $H_{min}(X|E) = \log_2(3/2)$. This result is interesting and in contrast with projective measurements, where a single projective measurement is never able to achieve $H_{min}(X|E) > 0$. In fact, it is always necessary to switch between two different projective measurements in order to bound the min-entropy.Outside this region, the $H_{min}(X|E)$ monotonically increases and reaches its maximum of $H_{min}(X|E) = 1$ for three pure states, that lie in between the $\vec{a}_i$.

The reason can be intuitively understood: consider the state orthogonal to $\hat{\Pi}_1$, if that state is sent $\hat{\Pi}_1$ never clicks and this measurement alone certifies the purity of ρ_A. On the other hand, the other two outcomes relative to $\hat{\Pi}_2, \hat{\Pi}_3$ happen with equal probability of 0.5. So, in this case, it behaves like an unbiased coin, and the maximum achievable randomness is 1 bit per measurement.

Additionally, this numerical tool can also be useful to get a more precise understanding of Eve's optimal strategy and the physics behind the attack. If we consider the primal formulation of the SDP:

$$\begin{aligned} \underset{\delta_x}{\text{maximize}} \quad & \sum_x^d \mathrm{Tr}_A\left[\hat{\Pi}_x^A \delta_x\right] \\ \text{subject to} \quad & \delta_x \geq 0 \, \forall x, \\ & \mathrm{Tr}\left[\sum_x \delta_x\right] = 1, \\ & \mathrm{Tr}\left[\left(\Gamma_i^A\right) \sum_x \delta_x\right] = \gamma_i \end{aligned} \tag{5.11}$$

after the optimization we obtain not only the maximum of the objective function p^*_{guess} but also the optimal states $\{\delta_x^*\}_{x=1,2,3}$ that Eve has to send in order to maximize her p_{guess}. These states that are subnormalized and are already multiplied for the probability of being sent, completely define Eve's strategy. The evolution of these states as a function of $\hat{\rho}_A$ can be studied to reconstruct Eve's strategy in different conditions.

Together with the software that performs the SDP optimization, an interactive visualization tool has been developed, in order to easily visualize Eve's strategy.

Figure 5.2 provides an example of such a tool for a section of the XZ plane. With the two sliders on the top, the user can manipulate $\hat{\rho}_A$ (that in this case is bounded to be in the

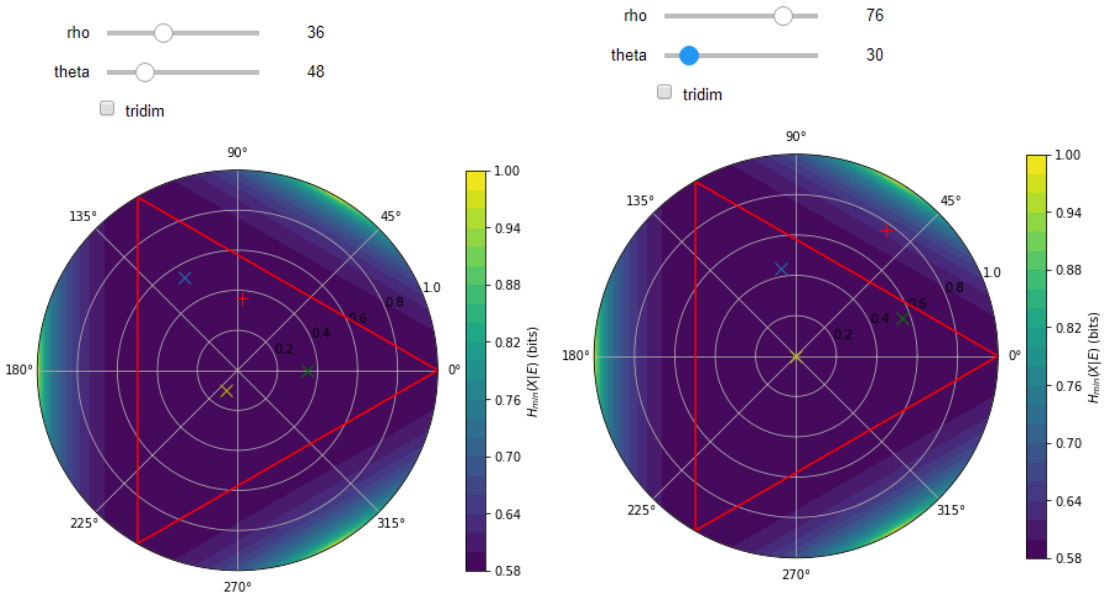


Figure 5.2: *Contour plot of the $H_{min}(X|E)$ calculated with the SDP for $\hat{\rho}_A$ on the XZ plane of the Bloch sphere. The angle 0 is aligned with the state $|V\rangle$. Additionally, 4 marker are superimposed. The red + represents a specific $\hat{\rho}_A$, selected with the interactive sliders. The other 3 crosses represent the optimal δ_x^* states relative to that $\hat{\rho}_A$. On the left we can see the strategy for a state that lies inside the triangle connecting the POVM elements and on the right the strategy for a state outside the region. They are associated to two different strategies.*

XZ plane), which is then represented on the plot as with the red + symbol. The green, blue and yellow crosses represent the three δ_x^*

On the left side of the figure, it's possible to see that when $\hat{\rho}_A$ is inside the triangle, the three δ_x^* are all non-zero and aligned with $\vec{a}_x$. In this case, all the single outcomes can be predicted with the maximal probability of 2/3. On the right, we can see that when $\hat{\rho}_A$ lies outside the triangle, Eve employs only two δ_x^*, while the third one is never sent.

Moreover, from the contour plot, we can see that outside the triangular region, all the points with the same distance from the boundary of the region (i.e. from one of the three red lines) lead to the same $H_{min}(X|E)$. This behavior could be explained if the two states sent by Eve are fixed once the distance from the boundary is fixed and what changes is the probability that one or the other state is sent.

5.1.2 The Three-State POVM: An analytic bound

Thanks to the numerics described in the previous section, we were able to get precious insights into the physics behind the system we are considering. In this section, we will use this information to develop an analytic bound on the $H_{min}(X|E)$, that always coincides with our numerics.

As already said, the attacker in the Source-DI framework is allowed to send any state $\hat{\rho}_A$; however, in this case, pure states always provide higher guessing probabilities. Consider the qubit case with $\hat{\rho}_M$ mixed and guessing probability $P_m = \max_x \mathrm{Tr}\left[\hat{\Pi}_x \hat{\rho}_M\right]$, then is always possible to decompose $\hat{\rho}_M$ with two pure states $|\psi_1\rangle, |\psi_2\rangle$ such that $\hat{\rho}_M = \lambda |\psi_1\rangle\langle\psi_1| + (1-\lambda)|\psi_2\rangle\langle\psi_2|$ but then:

$$P_m = \max_x \left(\mathrm{Tr}\left[\hat{\Pi}_x \left(\lambda |\psi_1\rangle\langle\psi_1| + (1-\lambda)|\psi_1\rangle\langle\psi_1|\right)\right]\right) \tag{5.12}$$

$$\leq \lambda \left(\max_x \mathrm{Tr}\left[\hat{\Pi}_x |\psi_1\rangle\langle\psi_1|\right]\right) + (1-\lambda)\left(\max_x \mathrm{Tr}\left[\hat{\Pi}_x |\psi_2\rangle\langle\psi_2|\right]\right) \tag{5.13}$$

Then, for the three outcome POVM Eve's optimal strategy is to send instead of $\hat{\rho}_A = \frac{1}{2}(\mathbb{1} + \vec{r}\cdot\vec{\sigma})$ three pure states $\hat{\tau}_k = \frac{1}{2}\left(\mathbb{1} + \vec{t}_k \cdot \vec{\sigma}\right)$ such that:

$$p_1\vec{t}_1 + p_2\vec{t}_2 + p_3\vec{t}_3 = \vec{r} \tag{5.14}$$

In this way the guessing probability:

$$P_{guess} = \max_{\vec{t}_k} \sum_k p_k \,\mathrm{Tr}\left[\hat{\Pi}_k \hat{\tau}_k\right] \tag{5.15}$$

$$= \frac{1}{3} + \frac{1}{3}\sum_k p_k \vec{t}_k \cdot \vec{a}_k \tag{5.16}$$

is maximized.

Now, if $\vec{r}$ projection in the plane of the POVM is inside the dashed triangle of Figure 5.1, delimited by the lines connecting the three $\vec{a}_k$, then the guessing probability is always saturated for:

$$\vec{t}_k = \vec{a}_k \tag{5.17}$$

Eve's best strategy is to send three pure states exactly aligned with the POVM elements. In this case

$$P_{guess} = \frac{1}{3} + \frac{1}{3}\sum_k p_k = \frac{2}{3} \tag{5.18}$$

However, if the projection of $\vec{r}$ lies outside the dashed triangle, this is no longer the optimal strategy for Eve. In this case, we can parametrize $\vec{r}$ as :

$$\vec{r} = q\vec{t}_1 + (1-q)\left[\lambda\vec{t}_2 + (1-\lambda)\vec{t}_3\right] \tag{5.19}$$
$$= q\vec{t}_1 + \vec{s}(1-q) \tag{5.20}$$
$$P_{guess} = \frac{1}{3} + \frac{q}{1}\vec{t}_1\cdot\vec{a}_1 + \frac{1-q}{3}\left[\lambda\vec{t}_2\cdot\vec{a}_2 + (1-\lambda)\vec{t}_3\cdot\vec{a}_3\right] \tag{5.21}$$
$$= \frac{1}{3} + \frac{q}{3}\vec{t}_1\cdot\vec{a}_1 + \frac{1-q}{3}\left[\vec{s}\cdot\vec{a}_3 + \lambda\vec{t}_2\cdot(\vec{a}_2-\vec{a}_3)\right] \tag{5.22}$$
$$\tag{5.23}$$

with $\lambda, q \in [0,1]$ and

$$\vec{s} = \left[\lambda\vec{t}_2 + (1-\lambda)\vec{t}_3\right] \tag{5.24}$$

First of all we fix $\vec{t}_1$ (and thus q) and try to find the best choice for $\vec{t}_2, \vec{t}_3$ and λ. We can consider $\vec{t}_2$ as variable, while $\vec{t}_3$ and λ should be derived from Eq 5.24. Indeed, we can find λ by squaring the relation $(1-\lambda)\vec{t}_3 = \vec{s} - \lambda\vec{t}_2$ and by remembering that $|\vec{t}_k| = 1$. Then we get:

$$\lambda = \frac{1-s^2}{2(1-\vec{s}\cdot\vec{t}_2)} \tag{5.25}$$

Then since $\vec{a}_2 - \vec{a}_3 = \sqrt{3}\hat{x}$ with $\hat{x}$ versor of the x axis, Eve should maximize the last term in the P_{guess}:

$$F = \lambda\vec{t}_2\cdot(\vec{a}_2-\vec{a}_3) = \lambda\vec{t}_2\cdot\sqrt{3}\hat{x} \tag{5.26}$$

By substituting the expression 5.25 for λ we can rewrite:

$$F = \frac{1-s^2}{2(1-\vec{s}\cdot\vec{t}_2)}\vec{t}_2\cdot\hat{x} \tag{5.27}$$

If we define: $\vec{s} = s(\cos(\theta), \sin(\theta)), \vec{t}_2 = (\cos(\phi), \sin(\phi))$ we get:

$$F = (1-s^2)\frac{\cos(\phi)}{2(1-s\cos(\phi-\theta))} \tag{5.28}$$

This expression is maximized for $\cos(\phi) = s\cos\theta = s_x$.

Geometrically this implies that $\vec{t}_2$ and $\vec{t}_3$ have the same angle respect $\vec{a}_2$ and $\vec{a}_3$ as shown in Figure 5.3:

In this case $\vec{a}_2\cdot\vec{t}_2 = \vec{a}_3\cdot\vec{t}_3$ and the P_{guess} can be written as:

$$P_{guess} = \frac{1}{3} + \frac{q}{3}\vec{t}_1\cdot\vec{a}_1 + \frac{1-q}{3}\vec{t}_2\cdot\vec{a}_2 \tag{5.29}$$
$$= \frac{1}{3} + \frac{q}{3}\vec{t}_1\cdot\vec{a}_1 + \frac{1-q}{3}\left(s_x a_{2x} + \sqrt{1-s_x^2}a_{2z}\right) \tag{5.30}$$
$$= \frac{1}{3} + \frac{q}{3}t_{1z} + \frac{1-q}{3}\left(s_z a_{2z} + \sqrt{1-s_z^2}a_{2x}\right) \tag{5.31}$$

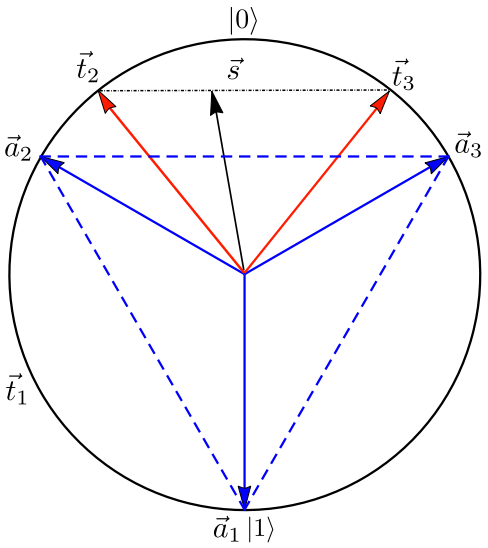


Figure 5.3: *Eve's optimal strategy*

Now it is necessary to find the optimal state for $\vec{t}_1$ and we can parametrize q as:

$$q = \frac{s_z - r_z}{s_z - t_{1z}} \tag{5.32}$$

so that the P_{guess} becomes a function of s_z and t_{1z}. The maximum is achieved for:

$$\frac{\partial P_{guess}}{\partial s_z} = \frac{\partial P_{guess}}{\partial t_{1z}} = 0 \tag{5.33}$$

with the constraint $t_{1z} \leq 0$ and $s_z \geq r_z$, as it can seen in the figure. In this case, the only solution is obtained for

$$s_z = r_z \rightarrow q = 0 \tag{5.34}$$

So for Eve is not beneficial to use a third state, but a statistical mixture of two pure states always yields higher guessing probabilities.

Finally we write an analytical (tight) bound on the P_{guess} as a function of the estimated s_z:

$$P_{guess} = \frac{1}{3}\left(1 + \vec{t}_2 \cdot \vec{a}_2\right) = \frac{1}{3}\left(1 + \frac{s_z}{2} + \frac{\sqrt{(1 - s_z^2)}}{2}\right) \tag{5.35}$$

for $s_z \geq \frac{1}{2}$.

5.1.3 Extension to N equispaced POVM on the plane

The same argument can be extended for POVM with an arbitrary number N of elements, equally spaced along a plane on the Bloch sphere.

Here only the analytic derivation will be discussed since the SDP extension is trivial.

An equiangular POVM with N outcomes can be written as

$$\hat{\Pi}_k = \frac{1}{N}(\mathbb{1} + \vec{a}_k \cdot \vec{\sigma}) \tag{5.36}$$

$$\vec{a}_k = (\cos 2k\alpha, 0, \sin 2k\alpha) \tag{5.37}$$

$$\alpha = \frac{\pi}{N} \tag{5.38}$$

The vectors orthogonal to the edge of the polytope are:

$$\vec{w}_k = \frac{\vec{a}_k + \vec{a}_{k+1}}{2} = \cos\alpha \hat{u}_k \tag{5.39}$$

$$\hat{u}_k = (\cos(2k+1)\alpha, 0, \sin(2k+1)\alpha) \tag{5.40}$$

Suppose that the measurement outcomes are compatible with the state $\rho = \frac{1}{2}(\mathbb{1} + \vec{r} \cdot \vec{\sigma})$. Again, Eve has two different strategies, depending if the state $\vec{r}$ is inside the polytope, which happens if:

$$\vec{r} \cdot \vec{u}_k \leq \cos\alpha \forall k \tag{5.41}$$

so if the projection of $\vec{r}$ on u_k is lower than $|\vec{w}_k|$.

In this case Eve's optimal strategy is to send N pure states $\hat{\rho}_k$ with probability p_k such that:

$$\vec{t}_k = \vec{a}_k \tag{5.42}$$

$$\sum p_k \hat{\rho}_k = \hat{\rho} \tag{5.43}$$

$$\tag{5.44}$$

and the guessing probability:

$$P_{guess} = \frac{1}{N} + \frac{1}{N}\vec{t}_k \cdot \vec{a}_k = \frac{2}{N} \tag{5.45}$$

In contrast, if the state ρ lies outside the polytope, there is one $k = k^*$ such that if $\vec{r} \cdot \vec{u}_k^* \geq \cos\alpha$. Then Eve chooses only two pure states $\vec{t}_{k^*}, \vec{t}_{k^*+1}$ in between $\vec{a}_{k^*}, \vec{a}_{k^*+1}$, such that $\vec{t}_{k^*} \cdot \vec{a}_{k^*} = \vec{t}_{k^*+1} \cdot \vec{a}_{k^*+1}$.

Since $\vec{t}_{k^*} \cdot \vec{u}_{k^*} = \vec{r} \cdot \vec{u}_{k^*}$ we have

$$\vec{t}_{k^*} \cdot \vec{a}_{k^*} = \vec{r} \cdot \vec{u}_{k^*} \cos\alpha + \sqrt{1 - (\vec{r} \cdot \vec{u}_{k^*})^2} \sin\alpha \tag{5.46}$$

Then the P_{guess} can be written as:

$$P_{guess} = \frac{1}{N} + \frac{1}{N}\vec{t}_{k^*} \cdot \vec{a}_{k^*} \tag{5.47}$$

$$= \frac{1}{N}\left(1 + \vec{r} \cdot \vec{u}_{k^*} \cos\frac{\pi}{N} + \sqrt{1 - (\vec{r} \cdot \vec{u}_{k^*})^2} \sin\frac{\pi}{N}\right) \tag{5.48}$$

Finally, we can obtain an analytic formula for the P_{guess} that takes into account both strategies, introducing the Heavside function $\theta(x)$:

$$P_{guess} = \frac{2}{N} + \frac{1}{N}\sum_k \left(\vec{r} \cdot \vec{u}_k \cos\frac{\pi}{N} + \sqrt{1 - (\vec{r} \cdot \vec{u}_k)^2} \sin\frac{\pi}{N} - 1\right)\theta\left(\vec{r} \cdot \vec{u}_k - \cos\frac{\pi}{N}\right) \tag{5.49}$$

5.1.4 Results

Both the SDP and the analytical method have been tested for N up to 100. The results were calculated respect the statistics reproduced by $\hat{\rho}_A$ sampled from the entire Bloch sphere. The SDP and the analytical method always agreed, up to a factor smaller than the tolerance set for the SDP optimizer.

In Figure 5.4, it is possible to see the contour plots for $\hat{\rho}_A$ on the XZ plane of the Bloch sphere and $N = 3, 4, 5, 6$.

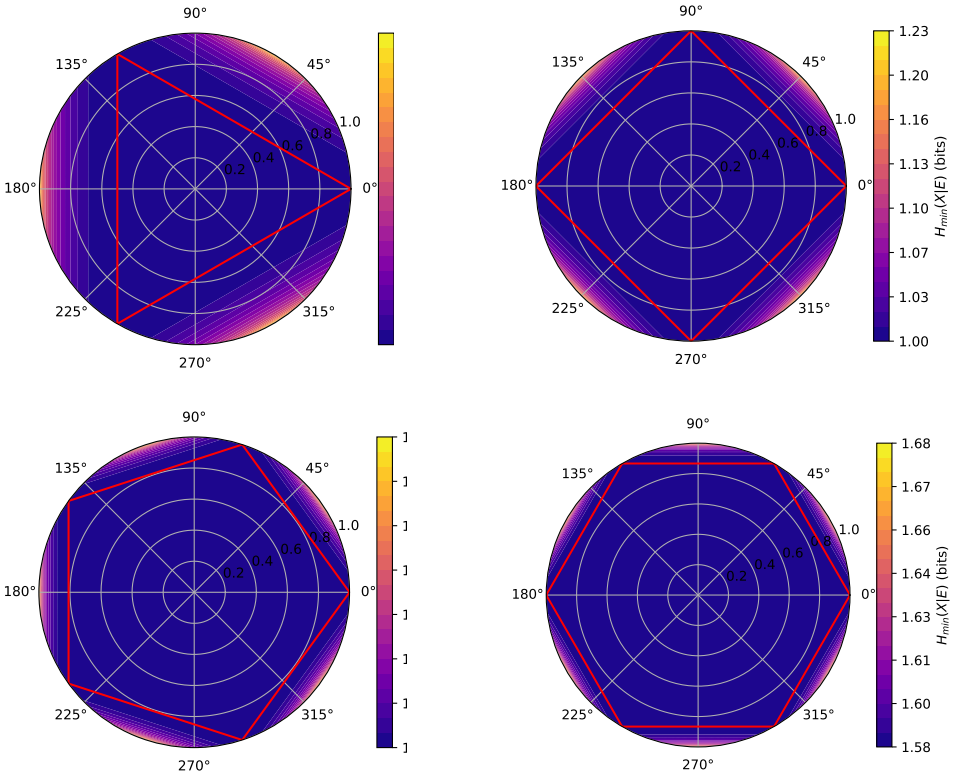


Figure 5.4: *Contour plot of $H_{min}(X|E)$ for $\hat{\rho}_A$ in the XZ plane. The POVM considered have 3, 4, 5, 6 equispaced elements in the same plane of $\hat{\rho}_A$*

By increasing the number of outcomes both the lowest and the highest $H_{min}(X|E)$ increase, in fact from the analytic formula we have:

$$\max_{\vec{r}}\left(H_{min}(X|E)\right) = \log_2(N) - \log_2\left(1+\cos\frac{\pi}{N}\right) \tag{5.50}$$

$$\min_{\vec{r}}\left(H_{min}(X|E)\right) = \log_2(N) - 1 \tag{5.51}$$

This scaling as a function of N for a qubit system and equiangular POVM on a plane is reported in Fig 5.5.

The difference between $\max_{\vec{r}}\left(H_{min}(X|E)\right)$ and $\min_{\vec{r}}\left(H_{min}(X|E)\right)$:

$$\max_{\vec{r}}\left(H_{min}(X|E)\right) - \min_{\vec{r}}\left(H_{min}(X|E)\right) = 1 - \log_2\left(1+\cos\frac{\pi}{N}\right) \approx \frac{\pi^2}{2N^2\ln 2} \tag{5.52}$$

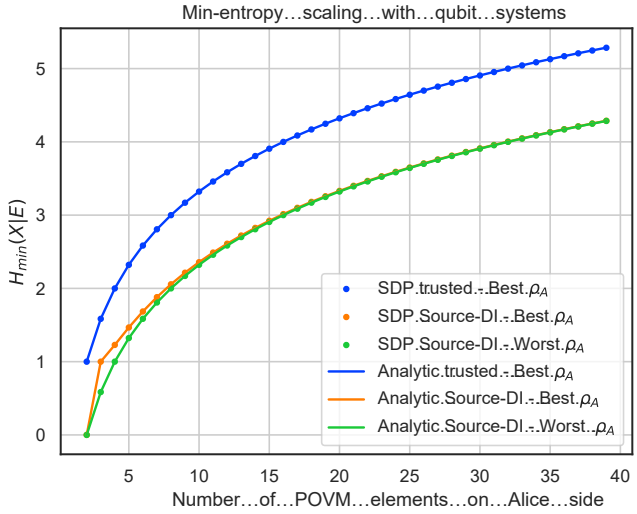


Figure 5.5: *Scaling of $H_{min}(X|E)$ as a function of N. Numerical and analytic results agree up to tolerance of the SDP solver. In the Source-DI scenario, both the max and the min $H_{min}(X|E)$ for each N are showed. A comparison with the trusted model is also reported.*

on the other hand gets smaller, since the distance between the POVM's elements also gets smaller. Moreover, in Fig 5.5 we can see a comparison between the extractable randomness in the trusted and in the Source-DI scenarios. The price to pay for the increased security of the Source-DI estimation is constant for all N and is 1 bit per measurement.

Finally, the results show that in the limit $N \to \infty$ we would have $H_{min}(X|E) \to \infty$, meaning that unbounded randomness can be certified even from quantum systems with finite dimension d, including qubits.

5.2 An experimental implementation using heralded single photons

In order to validate the theoretical predictions described in the previous paragraphs, we realized a simple optical setup to perform a proof-of-principle demonstration with a heralded single photon source. The preparation and measurement exploit the polarization degree of freedom of single photons. A schematic representation of the setup is shown in Figure 5.6.

A brief description of the setup will now be given.

5.2.1 The heralded source

A continuous wave (CW) laser at 404.5nm (160MHz FWHM linewidth) optically pumps a 30mm long Periodically Poled Potassium Titanyl Phosphate (PPKTP) crystal placed in a Sagnac interferometer. The polarization of the pump is adjusted with an HWP placed before the PBS that starts the Sagnac loop. The two polarization components, travel clockwise and

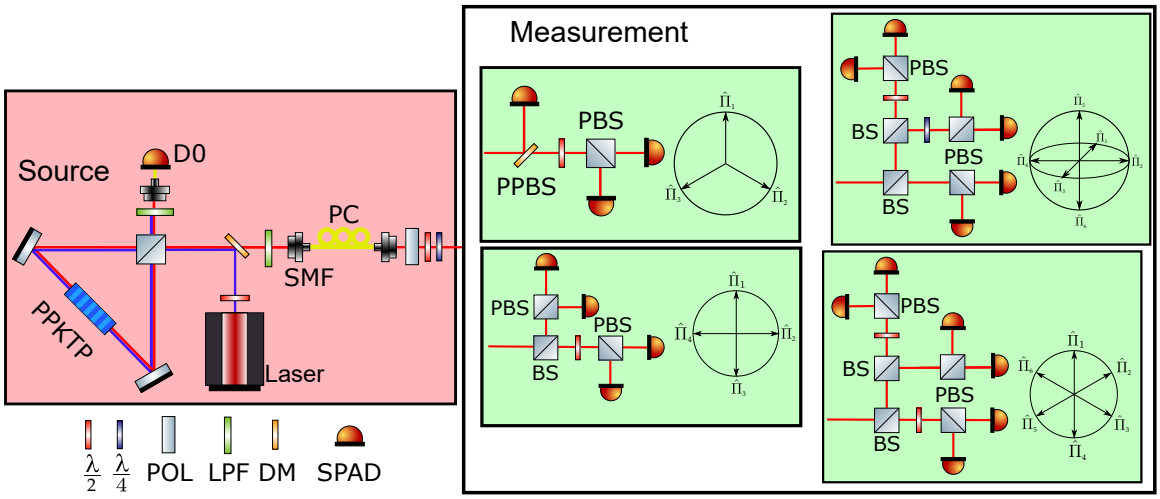


Figure 5.6: *A Sagnac-type source generates correlated photon pairs at 809 nm. The signal photon is detected by a SPAD and provides a time signal to gate the other detectors. The idler photon is first prepared in the desired polarization state and then sent to the measurement station. Four different POVM have been realized with* 3, 4 *and* 6 *outcomes.*

anti-clockwise in the loop and excite the PPKTP crystal placed in the middle. The crystal has a poling period $\Lambda = 10\mu$m and emits correlated photon pairs at $809nm$, with 0.2nm FWHM, generated through a quasi-phase-matched Spontaneous Parametric Downconversion (SDPC) process. The SPDC is a collinear type-II, so the photon pairs are generated with orthogonal polarization. At the exit of the Sagnac loop, the photons pass through the PBS that separates the two photons into two different paths. Finally, the photons pass through a Long Pass Filter (LPF) that blocks the pump and are then collected by single mode fibers.

When the pump light is diagonally polarized (and an HWP is placed after the reflection path of the PBS) this type of source can be used to generate entangled photon pairs [127].

However, in this experiment, we don't require entanglement but only heralded single photons. The polarization of the pump is set to horizontal, so that the pump travels only counter-clockwise in the Saganc and the downconverted photons form a fully separable state $|\psi\rangle = |H\rangle_s \otimes |V\rangle_i$. These are then deterministically separated by the PBS and the $|H\rangle_s$ is directly revealed by a Silicon Single Photon Avalanche Detector (SPAD) (Excelitas SPCM-NIR), with $\approx$65% of quantum efficiency at 810nm, $\approx$800ps FWHM of temporal jitter and 21 ns of dead time. A click in this detector "certifies" the presence of the idler photon since the downconverted photons are generated at the same time. This signal can be used as gate for the detection of the idler photon, reducing the noise coming from the SPAD's dark counts.

Finally, the idler photon $|V\rangle_i$ is collected by a single mode fiber and sent to the preparation stage. Here a polarizer, an HWP, and a QWP are used to prepare the photon in any required polarization. The photon then is sent to Alice's measurement station.

Taking into account filtering and finite SPAD efficiency, we obtain a heralded photon generation rate of $\approx$10kHz.

We stress again that we work in the Source-DI scenario, where the source is untrusted, and no information about the preparation is used to estimate the private randomness that can be extracted by Alice.

5.2.2 The measurement setup

The POVM $\{\Pi_i\}$ used by Alice are N-output measurement in the two dimensional Hilbert space of photon polarization. The implementation of such POVM can be done using interferometric setups (as in [128]); however they do not offer long term stability. For this reason, we decided to follow the approach presented in [129], where only passive linear optical components are used, and different outcomes are mapped into different optical paths.

Let's first consider the 3 outcome equiangular POVM.

In this case, the photon first passes through a Partial Polarizing Beam Splitter that reflects with probability 2/3 $|V\rangle$, while fully transmits $|H\rangle$. Thus, detecting the reflected photons directly implements the first POVM element $\hat{\Pi}_1 = \frac{2}{3}|V\rangle\langle V|$. On the other hand, if we write parametrize the input state as $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$ the state at the output of the transmitted port can be written as: $|\psi\rangle = \alpha|H\rangle + \frac{1}{\sqrt{3}}\beta|V\rangle$. After the PPBS the HWP at $\frac{\pi}{8}$ rotates the state to:

$$|\psi\rangle = \alpha|-\rangle + \frac{1}{\sqrt{3}}\beta|+\rangle = \frac{1}{\sqrt{2}}\left(\alpha + \frac{1}{\sqrt{3}}\beta\right)|H\rangle + \frac{1}{\sqrt{2}}\left(\alpha - \frac{1}{\sqrt{3}}\beta\right)|V\rangle \tag{5.53}$$

Then, after the regular PBS the detectors in the transmitted and reflected port click with probability $\frac{1}{2}|\alpha + \frac{1}{\sqrt{3}}\beta|^2$ and $\frac{1}{2}|\alpha - \frac{1}{\sqrt{3}}\beta|^2$ respectively, implementing the POVM elements $\hat{\Pi}_2, \hat{\Pi}_3$.

A photo of the setup is presented in Fig 5.7

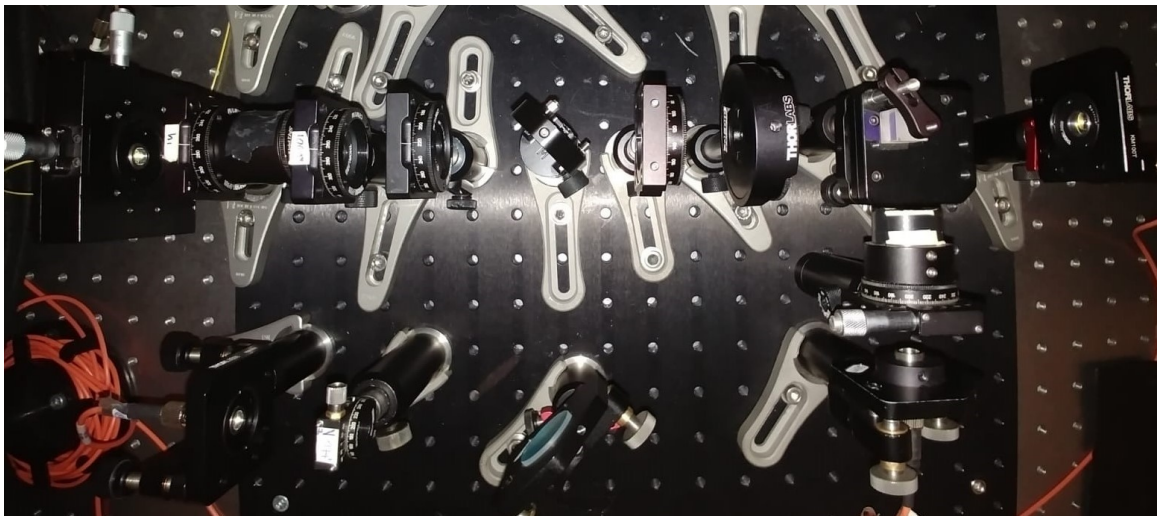


Figure 5.7: *Photo of the actual implementation of the three-outcome POVM*

The POVM with 4 and 6 outcomes can be implemented in a similar way, and they don't require any non-standard component such as the PPBS.

The 4 outcome POVM is realized in the following way: a 50:50 BS reflects and transmits the photons with equal probability, then in the reflected path a PBS performs a measurement in the $\mathbb{Z}$ basis, while in the transmitted path the HWP at $\frac{\pi}{8}$ followed by the PBS, performs a measurement in the $\mathbb{X}$ basis. In this way, the four POVM elements $\hat{\Pi}_{\{1,2,3,4\}} = \{\frac{1}{4}|H\rangle\langle H|, \frac{1}{4}|+\rangle\langle +|, \frac{1}{4}|V\rangle\langle V|, \frac{1}{4}|-\rangle\langle -|\}$ are realized. In a similar way, a BS with transmissivity $\frac{1}{3}$ followed by a BS with transmissivity $\frac{1}{2}$ in the reflected path creates three

different optical paths where the probability *o detect the photon is $\frac{1}{3}$. Then one path is directly measured along the $\mathscr{Z}$ basis with a simple PBS, implementing the elements $\hat{\Pi}_{1,4} = \frac{1}{6}|H\rangle\langle H|, \frac{1}{6}|V\rangle\langle V|$. In the second arm an HWP at $\frac{\pi}{12}$ before the PBS implements the elements $\hat{\Pi}_{2,5} = \frac{1}{6}(\frac{\sqrt{3}}{2}|H\rangle + \frac{1}{2}|V\rangle)(\frac{\sqrt{3}}{2}\langle H| + \frac{1}{2}\langle V|), \frac{1}{6}(\frac{1}{2}|H\rangle - \frac{\sqrt{3}}{2}|V\rangle)(\frac{1}{2}\langle H| - \frac{\sqrt{3}}{2}\langle V|)$. Similarly, in the third arm an HWP at $\frac{\pi}{6}$ before the PBS implements the elements: $\hat{\Pi}_{3,6} = \frac{1}{6}(\frac{1}{2}|H\rangle + \frac{\sqrt{3}}{2}|V\rangle)(\frac{1}{2}\langle H| + \frac{\sqrt{3}}{2}\langle V|), \frac{1}{6}(\frac{\sqrt{3}}{2}|H\rangle - \frac{1}{2}|V\rangle)(\frac{\sqrt{3}}{2}\langle H| - \frac{1}{2}\langle V|)$.

Finally, we also implemented an Informationally Complete POVM [130] with 6 outcomes. The implementation is similar to the previous one with the change that an HWP is now rotated at $\frac{\pi}{8}$ and the other HWP is substituted with a QWP at $\frac{\pi}{4}$. In this way each arm measures along one of the $\mathbb{X}, \mathbb{Y}, \mathbb{Z}$ bases, implementing the following POVM elements $\hat{\Pi}_{\{1,2,3,4,5,6\}} = \{\frac{1}{6}|H\rangle\langle H|, \frac{1}{6}|+\rangle\langle +|, \frac{1}{6}|L\rangle\langle L|, \frac{1}{6}|V\rangle\langle V|, \frac{1}{6}|-\rangle\langle -|, \frac{1}{6}|R\rangle\langle R|\}$.

After the polarization measurements, the photons are collected by multimode fibers and revealed by Silicon SPAD, with performance similar to the one used for the heralding measurement.

This implementation, however, suffers from a severe limitation: the number of optical elements required to implement the POVM scales with the number N of outcomes. This is also valid for the number of SPAD, which are complex and expensive instruments. An alternative implementation, that requires an active modulation, has been introduced in [131], where the polarization measurement is not mapped to a different path but to a different time-slot. With this implementation, the number of optical elements and detector is constant for every N; however the price to pay is a reduced maximum repetition rate, due to the temporal multiplexing.

5.2.3 Coincidence logic and software

The single photons are detected by commercial SPAD with $\approx 800ps$ of temporal jitter. The TTL signal generated by the SPAD is then recorded by a QuTau Timetagger that digitizes the time of arrival of the electrical pulse with a resolution of 81ps and streams it to a PC via the USB2 interface. The advantage of working with a heralded source is the possibility to filter out most of the noise coming from the SPAD by looking only at the coincidences between the heralding detector (called D0) and the other detectors. In order to do so a python software on the PC, retrieves the timetags and calculates in real-time the coincidences between D0 and any other detector, keeping the tag only if the delay between the two events is inside the user defined coincidence window, set at 1ns in this experiment. The values are plotted in real-time, greatly simplifying the alignment and preparation of the state.

5.2.4 Data analysis and results

As described in the previous section, we only keep the detection events that happen within a coincidence window of 1ns respect the signal coming from D0. For each successful event, we record the number of the detector that clicked. For a typical run of the experiment, we acquire a total number of N_{tot} of 10^7 coincidence events.

Then we evaluate the $H_{min}(X|E)$ both in the asymptotic limit ($H_{min}(X|E)_a$) and taking into account the finite-size contribution ($H_{min}(X|E)_f$). While the second estimation is the

important one if the random numbers are used in a real implementation, the first estimate can give valuable information about the non-idealities present in the experiment, such as the effect of a non-perfect state preparation and noise contribution.

Let's start with $H_{min}(X|E)_a$. In this case the total number of events per detector N_{Π_i} is directly converted to a probability $p_{\Pi_i} = \frac{N_{\Pi_i}}{\sum_i N_{\Pi_i}}$ of the occurrence of a particular POVM element $\hat{\Pi}_i$. These p_{Π_i} can be directly inserted in the SDP (they are exactly the γ_i since $\hat{\Gamma}_i = \hat{\Pi}_i$) or in the estimation of $\vec{r}$. However, since they are calculated from a finite sample size and $\hat{\rho}_A$ is usually pure (and hence at the boundary of the physically allowed region), they can lead to non-physical states, similarly to what happens for Quantum State Tomography algorithms that directly invert the measured data [132]. To solve the problem, we use the constrained maximum-likelihood estimation technique presented in [133] to retrieve a physical state $\tilde{\rho}_A$ compatible with the measured statistics p_{Π_i}. The asymptotic min-entropy $H_{min}(X|E)_a$ is then calculated for the reconstructed state $\tilde{\rho}_A$.

For what regards $H_{min}(X|E)_f$, this procedure has never been necessary in our case. When finite-size effects are taken into account, the error on the estimation of the p_{Π_i} is upper an lower bounded with the Chernoff-Hoeffding inequality [116] and we associate to each p_{Π_i} a confidence interval

$$[p_{\Pi_i} - \zeta(n,\epsilon), p_{\Pi_i} + \zeta(n,\epsilon)] \tag{5.54}$$

with

$$\zeta(n,\epsilon) = \sqrt{\frac{-\log_2(\epsilon)}{2n}} \tag{5.55}$$

Then $H_{min}(X|E)_f$ is calculated, minimizing $H_{min}(X|E)$ respect all the possible $\gamma_i \in [p_{\Pi_i} - \zeta(n,\epsilon), p_{\Pi_i} + \zeta(n,\epsilon)]$. For the typical values of $N_{tot} = 10^7$ and $\epsilon = 10^{-10}$, we always got optimal states in the physical allowed region.

Let's discuss the results for the 3 outcome POVM, presented in Tab 5.1.

State	$H_{min}(X\|E)_f$	$H_{min}(X\|E)_a$	$H_{min}(X\|E)_t$	MLE fitted $\tilde{\rho}_A$
$\|H\rangle$	0.933	0.969	1.000	$\begin{bmatrix} 9.996\cdot10^{-1} & -0.01 \\ -0.01 & 4\cdot10^{-3} \end{bmatrix}$
$\|V\rangle$	0.585	0.585	0.585	$\begin{bmatrix} 0.005 & -0.005 \\ -0.005 & 0.995 \end{bmatrix}$
$\|+\rangle$	0.676	0.687	0.685	$\begin{bmatrix} 0.460 & 0.477 \\ 0.477 & 0.540 \end{bmatrix}$
$\|L\rangle$	0.585	0.585	0.585	$\begin{bmatrix} 0.483 & -0.008 \\ -0.008 & 0.517 \end{bmatrix}$

Table 5.1: *Results for the 3 outcome POVM. $H_{min}(X|E)_t$ is the theoretical value expected for the state, $H_{min}(X|E)_a$ is the asymptotic value calculated on the reconstructed state $\tilde{\rho}_A$, while $H_{min}(X|E)_f$ takes into account the finite-size effects.*

In this case we repeated the experiment preparing four different states $|H\rangle, |V\rangle, |+\rangle, |L\rangle$. The first state $|H\rangle$ is the one that permits to maximize $H_{min}(X|E)$ and is expected to reach

a theoretical value $H_{min}(X|E)_t = 1$. In practice, we can only obtain an asymptotic value of $H_{min}(X|E)_a = 0.969$ per measurement, due to the limited extinction ratio of the filtering PBS in the preparation stage and unavoidable dark counts in $\hat{\Pi}_1$ due to accidentals. As expected when finite-size effects are taken into account, the extractable entropy decreases, since the optimization is performed over a larger set of states compatible with the measurements . The state $|V\rangle$ and $|L\rangle$, are able to reach the theoretical lower bound of ≈ 0.585 bits per measurement even in the asymptotic regime. The reason, however, is different: $|V\rangle$ is aligned with one of the POVM elements $\hat{\Pi}_1$ and so maximizes the overlap $\mathrm{Tr}\{\hat{\Pi}_1\hat{\rho}_A\}$, maximizing Eve's guessing probability. On the other hand, since the POVM measure only on the XZ plane, the statistics generated by $|L\rangle$ is also reproduced by the maximally mixed state $\frac{1}{2}\mathbb{1}_2$. This state, however can always be decomposed as an incoherent superposition of the three states aligned with the $\hat{\Pi}_i$, saturating the lower bound of the $H_{min}(X|E)$. Finally, the asymptotic value for $|+\rangle$ is slightly higher than the expected because the prepared (and estimated) state is not exactly $|+\rangle$ but slightly tilted. Similar considerations are valid for the 4 and 6 outcome POVM aligned on the plane, whose results are presented in Tab 5.2 and 5.3. The results for the informationally complete (IC) 6 outcomes POVM are presented in Tab 5.4 and require some additional comments.

State	$H_{min}(X\|E)_f$	$H_{min}(X\|E)_a$	$H_{min}(X\|E)_t$	MLE fitted $\hat{\rho}_A$
$\|H\rangle$	1.000	1.000	1.000	$\begin{bmatrix} 0.998 & 0.001 \\ 0.001 & 0.002 \end{bmatrix}$
$\|+\rangle$	1.000	1.000	1.000	$\begin{bmatrix} 0.502 & -0.499 \\ -0.499 & 0.498 \end{bmatrix}$
$\|L\rangle$	1.000	1.000	1.000	$\begin{bmatrix} 0.499 & -0.005 \\ -0.005 & 0.501 \end{bmatrix}$
$\left\|\frac{\pi}{8}\right\rangle$	1.158	1.178	1.228	$\begin{bmatrix} 0.852 & -0.352 \\ -0.352 & 0.148 \end{bmatrix}$

Table 5.2: *Results for the 4 outcome POVM. The state $\left|\frac{\pi}{8}\right\rangle$ is rotated by $\frac{\pi}{8}$ in the XZ plane respect to $|H\rangle$. $H_{min}(X|E)_t$ is the theoretical value expected for the state, $H_{min}(X|E)_a$ is the asymptotic value calculated on the reconstructed state $\tilde{\rho}_A$, while $H_{min}(X|E)_f$ takes into account the finite-size effects.*

Since the POVM is topographically complete, all the reconstructed states are pure up to experimental imperfections (purity is always $\geq 99\%$). The $H_{min}(X|E)$ for the optimal state $|int\rangle$ is higher respect the 6 outcome POVM on the plane, since the distance between $|int\rangle$ and any of the $\hat{\Pi}_i$ is higher than in the other case.

5.3 Conclusions

In this Chapter, we have described a new Source-DI protocol for secure QRNG, that can achieve unbounded randomness generation from finite-dimensional quantum systems. The protocol extends the concept introduced in [78] using non-projective measurement permitting to avoid the active basis switching and at the same time increasing the generation rate

State	$H_{min}(X\|E)_f$	$H_{min}(X\|E)_a$	$H_{min}(X\|E)_t$	MLE fitted $\hat{\rho}_A$
$\|H\rangle$	1.585	1.585	1.585	$\begin{bmatrix} 0.997 & 0 \\ 0 & 0.003 \end{bmatrix}$
$\left\|\frac{\pi}{6}\right\rangle$	1.585	1.585	1.585	$\begin{bmatrix} 0.747 & 0.425 \\ 0.425 & 0.253 \end{bmatrix}$
$\|L\rangle$	1.585	1.585	1.585	$\begin{bmatrix} 0.505 & -0.006 \\ -0.006 & 0.495 \end{bmatrix}$
$\left\|\frac{\pi}{12}\right\rangle$	1.620	1.644	1.685	$\begin{bmatrix} 0.928 & 0.251 \\ 0.251 & 0.072 \end{bmatrix}$

Table 5.3: *Results for the 6 outcome POVM on the plane. The states $\left|\frac{\pi}{6}\right\rangle, \left|\frac{\pi}{12}\right\rangle$ are rotated by the respective angles in the XZ plane respect to respect to $|H\rangle$.$H_{min}(X|E)_t$ is the theoretical value expected for the state, $H_{min}(X|E)_a$ is the asymptotic value calculated on the reconstructed state $\tilde{\rho}_A$, while $H_{min}(X|E)_f$ takes into account the finite-size effects.*

State	$H_{min}(X\|E)_f$	$H_{min}(X\|E)_a$	$H_{min}(X\|E)_t$	MLE fitted $\hat{\rho}_A$
$\|H\rangle$	1.585	1.585	1.585	$\begin{bmatrix} 0.997 & 0.006-0.005j \\ 0.006+0.005j & 0.003 \end{bmatrix}$
$\|+\rangle$	1.585	1.585	1.585	$\begin{bmatrix} 0.502 & 0.494+0.002j \\ 0.494-0.002j & 0.498 \end{bmatrix}$
$\|L\rangle$	1.585	1.585	1.585	$\begin{bmatrix} 0.503+0.j & 0.003+0.494j \\ 0.003-0.494j & 0.497-0.j \end{bmatrix}$
$\|int\rangle$	1.874	1.923	1.924	$\begin{bmatrix} 0.788 & -0.287-0.291j \\ -0.287+0.291j & 0.212 \end{bmatrix}$

Table 5.4: *Results for the IC 6 outcome POVM. The state $|int\rangle$ is in between the three states $|H\rangle, |+\rangle, |L\rangle$. $H_{min}(X|E)_t$ is the theoretical value expected for the state, $H_{min}(X|E)_a$ is the asymptotic value calculated on the reconstructed state $\tilde{\rho}_A$, while $H_{min}(X|E)_f$ takes into account the finite-size effects.*

per measurement. The security analysis has been performed using the newly developed numerical tool described in Sec. 4, taking into account finite-size effects. Additionally, exploiting the numerical results, we were able to characterize the attacker's strategy, and we obtained analytical bound on the $H_{min}(X|E)$ for some symmetric configurations of the POVM. Finally, we tested experimentally our theoretical predictions with a simple optical setup implementing $3, 4$ and 6 outcomes-POVM that measured the polarisation degree of freedom of single photons. For every run, the experimental results matched the theoretical predictions and showed an advantage of POVM measurements over projective ones.

This new protocol features a reduced experimental complexity and increased performances, if compared to other discrete-variable semi-DI QRNG, making it an interesting resource for practical applications.

CHAPTER 6

A Semi-Device-Independent QRNG based on an overlap assumption and heterodyne detection

In the previous chapters we mainly focused on Source-DI QRNG, however the zoology of Semi-DI QRNG is far more rich. The trust (and the assumptions) can be moved from the measurement to the source, hence realizing a Measurement-DI QRNG [83, 134, 135].

Alternatively, it's possible to avoid trusting specifically the measurement or the source device and an assumption is made on the channel capacity. [76, 84–87, 136]

These types of QRNG are usually called in the literature semi-self-testing or (with a slight abuse of notation) Semi-DI.

In this chapter a new type of Semi-DI QRNG based on an energy bound and heterodyne detection will be presented. The advantage over similar solutions that exploit discrete variable or homodyne detection, is an increased speed an increased resilience respect phase fluctuations. In particular the system does not require an active phase stabilization and the phase tracking is done via software, greatly simplifying the experimental implementation. Moreover, it can be easily scaled to more than two input and two outputs.

The results presented here, however, are only preliminary and a better security analysis and an improved experimental setup are under test at the time of writing.

6.1 Semi-DI QRNG based on a bound on the channel capacity

In this section we will describe informally the typical working scenario of a Semi-DI QRNG (for a formal and detailed discussion see [84, 87]). Then we will briefly discuss different protocols (with different assumptions) and different experimental implementations.

In general, Semi-DI QRNG are formulated in the prepare and measure scenario described in Fig 6.1, where both Alice and Bob's devices are considered as black boxes.

Alice box can accept different inputs $\{x_j\}_{j=1,n}$ that lead to the generation of different quantum states ρ_{x_j}. Bob's station also accepts different inputs $\{y_j\}_{j=1,m}$ that can be used to

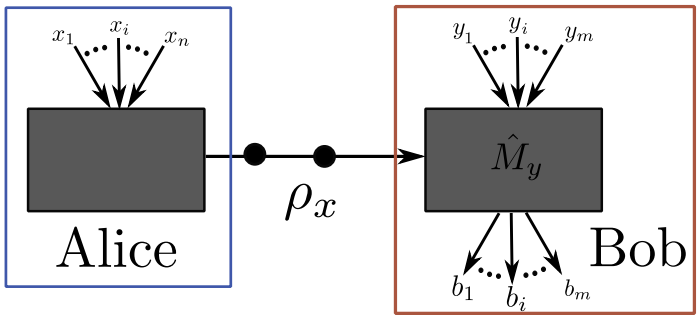


Figure 6.1: *General scenario for a Semi-DI QRNG*

select an unknown measurement $\hat{M}_{y_j}$, that leads to an output $b_{x,y}$. If no further restrictions are imposed in principle any conditional probability $p(b|xy)$ can be observed. However if the channel capacity is limited, for example with a bound on the max dimension of the Hilbert space of ρ_x or a bound on the maximal energy that can be transmitted, the space of possible probabilities $p(b|xy)$ is restricted. In this case, there exist a set $\mathcal{Q}$ of probabilities that can be achieved with quantum strategies but cannot be reproduced with only classical resources. This quantum "advantage" can be used to certify if quantum resources were used from the experimental data $p(b|xy)$ only, similarly to what happens for nonlocality with a Bell test [137]. Moreover, in analogy to what happens for DI QRNG [138], certain subset of $\mathcal{Q}$ can certify genuine and private quantum randomness, meaning that output b of Bob's measurement cannot be perfectly predicted, whatever is the side-information E available to an attacker.

In the experiment presented in this Chapter we will consider a prepare&measure scenario where an upper bound is assumed on the overlap on the states $\hat{\rho}_x$. This protocol has been proposed and experimentally realized in [85] using single photon detectors. Such bound can be translated into a bound on the maximum energy between the states ρ_x, however this link is never explicitly considered in [85]. Independently, in [84, 87] a more general framework based on the energy bound has been developed. The protocol proposed in these works have been experimentally realized in [86] with single photon detectors and in [139] with homodyne detection.

We decided to implement the analysis in [85] because was similar to the SDP described in Chap. 4 but we are currently working to implement also the analysis described in [87].

6.2 Semi-DI QRNG based on the overlap assumption

In the protocol described in [85] for the single time bin implementation, Alice's box has two inputs $x=\{0,1\}$ and can send two different and unknown quantum states $|\psi_0\rangle, |\psi_1\rangle$. Bob instead has a single measurement with 2 elements $\hat{\Pi}_0, \hat{\Pi}_1$ with two respective outcomes $b=\{0,1\}$.

The main assumption of the protocol is that the overlap between the two states $|\langle\psi_0|\psi_1\rangle|$ is lower bounded by some value δ:

$$|\langle\psi_0|\psi_1\rangle| \geq \delta \tag{6.1}$$

If $\delta \in (0,1)$, the two states are not orthogonal and they cannot be deterministically distinguished. This also implies that there is no way for the Eavesdropper to perfectly predicts the outcome of the measurement. In fact, even if Eve performs an optimal unambiguous state discrimination (USD), some of the measurement will be inconclusive, leading to a non-null randomness generation.

After some run of the protocol Alice and Bob can use the obtained data to calculate the conditional probabilities $p(b|x)$ that they will use to bound Eve's side information E. In fact, in order to get secure and private random numbers, they need to bound the quantum conditional min-entropy $H_{min}(b|E)$ as a function of δ and their experimental data $p(b|x)$ only.

As usual we can write the guessing probability $p_{guess}(b|E)$ of guessing b given E as in Renner's formulation of Eq. 4.13. In this case we consider an attacker with complete knowledge of the input states, the details of the measurement and the inner workings of the devices, which can vary at each run. The measurement strategies are then labelled by λ. Then the guessing probability,averaged over inputs and measurement strategies, occurring with probabilities $p(x)$ and $p(\lambda)$, can be written as:

$$p_{guess}(b|E) = \max_{q_\lambda, \Pi_1^\lambda} \sum_x p(x) \sum_\lambda q_\lambda \max\{\mathrm{Tr}\left[\rho_x \hat{\Pi}_0^\lambda\right], \mathrm{Tr}\left[\rho_x \hat{\Pi}_1^\lambda\right]\}, \tag{6.2}$$

where $\rho_x = |\psi_x\rangle\langle\psi_x|$ and $q_\lambda = p(\lambda)$. The maximization is performed over all possible measurement strategies which are consistent with the observed experimental data, ie. with the constraint:

$$\sum_\lambda q_\lambda \mathrm{Tr}\left[\rho_x \hat{\Pi}_b^\lambda\right] = p(b|x) \tag{6.3}$$

As the authors in [85] point out, at first look it would seem that the p_{guess} explicitly depends on the states ρ_x. However, since there are only two states the problem can be restricted to a 2-dimensional Hilbert space without loss of generality. Thus, the two state can be written as $|\psi_0\rangle = |0\rangle$ and $|\psi_1\rangle = \delta|0\rangle + \sqrt{1-\delta}|1\rangle$ in some basis $\{|0\rangle, |1\rangle\}$. With this formulation the maximum depends only on δ and the observed data $p(b|x)$.

Another problem for the optimization is that the number of measurement strategies seems unbounded. Luckily the result in [140] shows that we can group together all strategies for which the inner maximization occurs for the same term. Then four strategies are left, depending if the max occurs in for the first or the second term for each x. These strategies are labeled by (λ_0, λ_1) where λ_x determines which term is maximal for the input x. With this formulation the inner maximization can also be removed.

Then the POVM cam be written as: $\hat{\Pi}_b^{\lambda_0,\lambda_1}$ and the p_{guess} can be written as:

$$p_{guess} = \max_{q_{\lambda_0,\lambda_1}, \Pi_b^{\lambda_0,\lambda_1}} \sum_{x=0}^{1} p(x) \sum_{\lambda_0,\lambda_1=0}^{1} q_{\lambda_0,\lambda_1} \mathrm{Tr}\left[\rho_x \hat{\Pi}_{\lambda_x}^{\lambda_0,\lambda_1}\right]. \tag{6.4}$$

The weights q_{λ_0,λ_1} can be absorbed into the POVM elements that become

$$\hat{M}_b^{\lambda_0,\lambda_1} = q_{\lambda_0,\lambda_1} \hat{\Pi}_b^{\lambda_0,\lambda_1} \tag{6.5}$$

In this form the p_{guess} optimization can be rewritten as an SDP:

$$\begin{aligned}
\underset{M_b^{\lambda_0,\lambda_1}}{\text{maximize}} \quad & \sum_{x=0}^{1} p(x) \sum_{\lambda_0,\lambda_1=0}^{1} \mathrm{Tr}\left[\rho_x \hat{M}_{\lambda_x}^{\lambda_0,\lambda_1}\right] \\
\text{subject to} \quad & M_b^{\lambda_0,\lambda_1} = \left(M_b^{\lambda_0,\lambda_1}\right)^{\dagger}, \\
& M_b^{\lambda_0,\lambda_1} \geqslant 0, \\
& \sum_b M_b^{\lambda_0,\lambda_1} = \frac{1}{2}\,\mathrm{Tr}\left[\sum_b M_b^{\lambda_0,\lambda_1}\right]\mathbb{1}, \\
& \sum_{\lambda_0,\lambda_1} \mathrm{Tr}\left[\rho_x M_b^{\lambda_0,\lambda_1}\right] = p(b|x)
\end{aligned} \tag{6.6}$$

where the constraints impose to the operators $M_b^{\lambda_0,\lambda_1}$ to be Hermitian, positive semidefinite, sum to the identity and that are compatible with the data $p(b|x)$ measured experimentally.

With a procedure similar to the one outlined in Sec. 4.2.1, the primal SDP of Eq. 6.6 can be written in its dual formulation which exhibits all the advantages discussed in Chap 4:

$$\begin{aligned}
\underset{H^{\lambda_0,\lambda_1},\, \nu_{bx}}{\text{minimize}} \quad & \sum_{bx} \nu_{xb} p(b|x) \\
\text{subject to} \quad & H^{\lambda_0,\lambda_1} = \left(H^{\lambda_0,\lambda_1}\right)^{\dagger}, \\
& \left[\sum_x \rho_x \left(\frac{1}{2}\delta_{\lambda_x,0}\delta_{b,0} + \frac{1}{2}\delta_{\lambda_x,1}(1-\delta_{b,0}) \right.\right. \\
& \left.\left. + \nu_{bx}\right)\right] + H^{\lambda_0,\lambda_1} - \frac{1}{2}\mathrm{Tr}\left[H^{\lambda_0,\lambda_1}\right]\mathbb{1} \leqslant 0
\end{aligned} \tag{6.7}$$

where H^{λ_0,λ_1}, ν_{bx} are the Lagrangian multipliers.

Also in this case the dual SDP is linear in the experimental data $p(b|x)$, meaning that for a practical implementation a valid (but suboptimal) bound for p_{guess} can be rapidly obtained just by plugging new $p(b|x)$ in the objective function for some already calculated ν_{xb}. Moreover, also finite-size effects can be easily taken into account adding the finite size correction directly in the objective function:

$$p_{guess} = \sum_{bx} \nu_{xb} p(b|x) + \sum_{bx} |\nu_{xb}|\, t(n_{bx}, \epsilon) \tag{6.8}$$

where $t(x)$ is a tail inequality such as the Chernoff-Hoeffding, n_{bx} are the experimental counts and ϵ is a security parameter.

In the next section we will see how this analysis is applied to our experimental implementation and what are the theoretical bounds we can expect on the $H_{min}(b|E)$.

6.2.1 Heterodyne detection

In our implementation of the protocol, Alice's box can send two coherent states $|\psi_0\rangle = |\alpha\rangle, |\psi_1\rangle = -|\alpha\rangle$ and Bob can measure the states with the Heterodyne detection which effec-

tively implements the POVM:

$$\hat{\Pi}_\beta = \frac{1}{\pi} |\beta\rangle \langle\beta| \tag{6.9}$$

The POVM with a continuous set of elements $\hat{\Pi}_\beta$ is then discretized grouping all the elements with a positive real part $Re(\beta)>0$ into $\hat{\Pi}_0$ and the others into $\hat{\Pi}_1$. Formally:

$$\hat{\Pi}_0 = \int_{-\infty}^{+\infty} dIm\beta \int_0^{\infty} dRe\beta \frac{1}{\pi} |\beta\rangle \langle\beta| \tag{6.10}$$

$$\hat{\Pi}_1 = \int_{-\infty}^{+\infty} dIm\beta \int_{-\infty}^{0} dRe\beta \frac{1}{\pi} |\beta\rangle \langle\beta| \tag{6.11}$$

A phase space representation is shown in Figure 6.2 If we assume that the Heterodyne

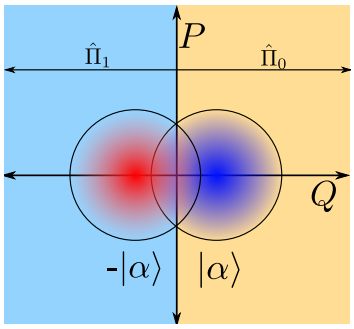


Figure 6.2: *Phase space representation of Alice's states and Bob's POVM*

detection is always phase-aligned with the two states as in Figure 6.2 we can calculate the expected δ and $p(b|x)$ as function of α for an honest implementation:

$$\delta = e^{-2|\alpha|^2} \tag{6.12}$$

$$p(0|0) = p(1|1) = \frac{1}{2}(1 + erf(Re(\alpha))) \tag{6.13}$$

$$p(1|0) = p(0|1) = \frac{1}{2}(1 - erf(Re(\alpha))) \tag{6.14}$$

Then we can plug these probabilities and δ in the SDP derived in Eq 6.7 in order to obtain a bound on the maximal $H_{min}(b|E)$ that can be achieved by this setup in ideal conditions and without actions by the Eavesdropper. The results are shown in Fig.6.3. As expected, when α is 0, Alice is sending only one state, the vacuum $|0\rangle$, and no randomness can be certified since no correlation is present between the input x and the output b. As soon as α is greater than 0, randomness can be certified with a maximum of 0.23 bits per measurement for $Re(\alpha)=0.27$. At higher α the $H_{min}(b|E)$ decreases, since the two states can be distinguished better and better.

It's important to point out that these results are calculated for an ideal and honest implementation of the scheme: if non-idealities are present or Eve performs an attack on the device the outcome probabilities $p(b|E)$ would be different and the respective $H_{min}(b|E)$ lower.

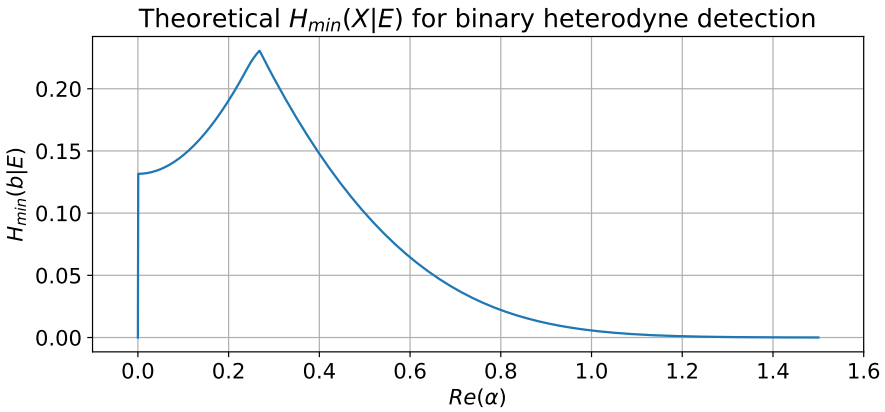


Figure 6.3: *Extractable randomness from the discretized heterodyne measurement as a function of α.*

6.3 Experimental implementation

The idealized protocol described in the previous section has been experimentally implemented with an all-fiber setup, shown in Fig. 6.4, which employs only COTS components.

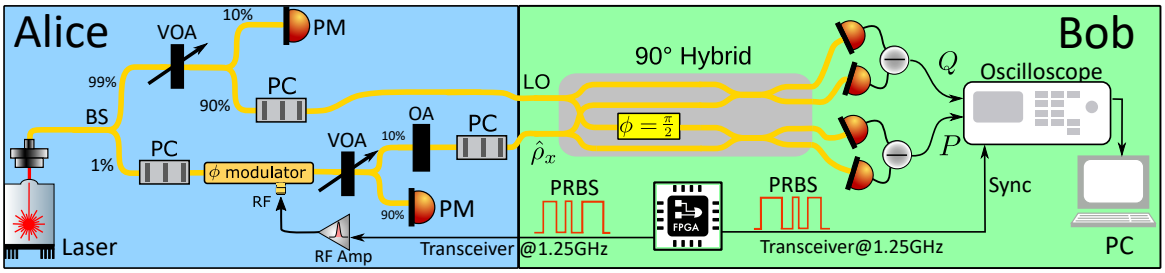


Figure 6.4: *Schematic representation of the experimental setup.*

6.3.1 The optical setup

A bright laser with max optical power of 100mW emits in continuous mode at 1550nm. Then light is splitted by a 99:1 fiber BS in two fibers. The one with 99% of the power is used for the LO and is sent first to an automatic Variable Optical Attenuator (VOA) and then is splitted again with a 90:10 BS: 10% of the power is sent to a powermeter (PM) for logging purposed and 90% of the light is first sent to a fiber Polarization Controller (PC) and then to the LO port of the 90° optical hybrid. The VOA plus PM is used to calibrate the detectors in with the same procedure described in Chap. 3. However, since in this case we do not trust our detectors, the calibration is not necessary and does not affect the security of the protocol. The PC before the LO port is necessary in order to maximize the optical power transferred to the 90° optical hybrid, since this element features a polarizer at it's input.

The arm with 1% of the laser light is used to prepare the states $|\psi_i\rangle$. The light is sent first to a PC and then to fiber $LiNbO_3$ phase modulator (MPZ-LN-20 by iXblue) with 20GHz of bandwidth. The phase modulator is used to add a π phase shift to the light travelling in it when an RF signal is received, thus preparing the $-|\tilde{\alpha}\rangle$ state. The PC is used to align the polarization of the incoming light to the extraordinary mode of the $LiNbO_3$ crystal, in order to maximize the modulation efficiency. The modulated light is then sent to a mechanical VOA, used to change the magnitude of α before being splitted by a 90:10 BS. 90% of the light is sent to a PM , while 10% is sent to a fixed optical attenuator. With this configuration, after calibrating the attenuation introduced by the OA, we can have a one-to-one mapping between the power read on the PM and the optical power in sent to Bob. Finally the light after the OA is sent to a PC used to control the polarization before sending the light into the signal port of the 90° optical hybrid. The two pairs of in-phase and out-phase optical signals are sent to two InGaS Balanced Photoreceiver (PDB480C-AC) with 1.6GHz of bandwidth.

This setup can be further improved using all polarization maintaining fiber components, removing the need of 3 polarization controller for polarization stabilization and greatly enhancing the entire stability.

6.3.2 The electronic setup

The balanced photoreceivers in the receiver's setup have a bandwidth of 1.6GHz (3db point). In order to exploit all the bandwith for the protocol, a fast RF signal with a similar frequency has to be sent to the phase modulator that switches between $|\alpha\rangle$ and $-|\alpha\rangle$.

In our lab the only instrument able to produce square pulses at similar speeds is an FPGA. The specific FPGA used for this experiment is equipped with several SerDes (Serializer-Deserializer) that drive high speed transceivers, able to operate up to 12.5GBps. We implemented on the FPGA a pseudo random number generator (PRNG) based on linear feedback shift registers characterized by the following polynomial:

$$x^{31} + x^{28} + 1 \tag{6.15}$$

This PRNG is commonly called PRBS31 and is used in classical communication for Bit Error Rate Tests (BERT). Sequences of 10bits generated by the PRNG are then sent to the SerDes using the global clock at 125MHz. The SerDes takes the data from a 10 bit parallel interface and sends the serialized data to an high speed transceiver. Here, using a dedicated programmable clock at 625MHz, a random sequence at $1.25 Gbps$ is obtained at the output of the SMA connector relative the transceiver. A screenshot of the electrical signal is shown in Fig 6.5

Unfortunately, the limited voltage swing of the signal and the limited current provided by the FPGA, cannot directly drive the phase modulator. Then the signal is sent to a 20 GHz RF amplifier by iXblue, before entering the phase modulator. The phase shift applied by the phase modulator is then adjusted by adjusting the gain of the amplifier, which changes the amplitude of the generated RF signal.

At the receiver side, the RF signal generated by the balanced phtotodetectors are sampled and digitized by Tektronix DPO70004 Oscilloscope with 4GHz of analog bandwidth, 25GSps per channel of sampling rate and 8 bit of vertical resolution. Since the Oscilloscope runs a full version of Windows 10, the data are acquired in bursts in the memory of the oscilloscope

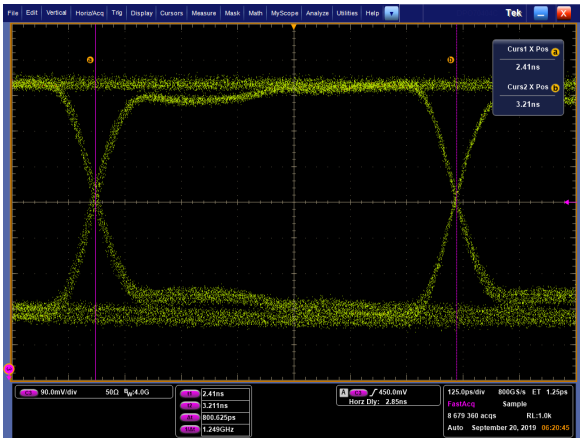


Figure 6.5: *Eye of the PRBS31 signal emitted from the FPGA*

and directly processed on board via a python script. We also sample a copy of the RF signal sent to the phase modulator for synchronization purposes.

6.3.3 Postprocessing software and analysis

Since the signal and LO travel in different fibers and no active phase stabilization is present, the relative phase between the two pulses is subject to drifts over time. From the point of view of the retrieved data, this means that the two gaussian distributions relative to $|\alpha\rangle$ and $-||\alpha\rangle\rangle$ will start to rotate around the center of the phase space, keeping fixed their overlap and their distance from the center. This effect is compensated by the analysis software that performs a sort of phase tracking algorithm and adapts the discretization of the heterodyne measurement (shown in Eq. 6.11) to the recovered relative phase.

The entire acquisition is divided in "chunks" of n samples, for each chunk we calculate the centroid of each distribution. Then we calculate the line that connects the two centroid and the line normal to this which passes through the middle point. These last two lines are used as a new reference frame for Q and P respectively and the heterodyne POVM is discretized respect this new reference frame. A picture of the recovered frame is shown in Fig. 6.6

Then we calculate the number of events n_{xb} for each of the $p(b|x)$. After repeating the procedure for all the "chunks" we sum all the n_{xb} and calculate the $p(b|x)$. We keep track of the direction of the phase rotation in order to assign the events to the correct class.

6.4 Results

With the setup described in the previous sections we performed the experiment for different values of $\mu = |\alpha|^2$. The value of μ was estimated for each run using the conversion from the measured optical power obtained by the calibrated PM in the signal arm. The μ was adjusted using the VOA positioned before the BS and the PM.

With the value of μ we could estimate δ and insert it into the SDP. The $p(b|x)$ were calculated using the method described in Sec.6.3.3.

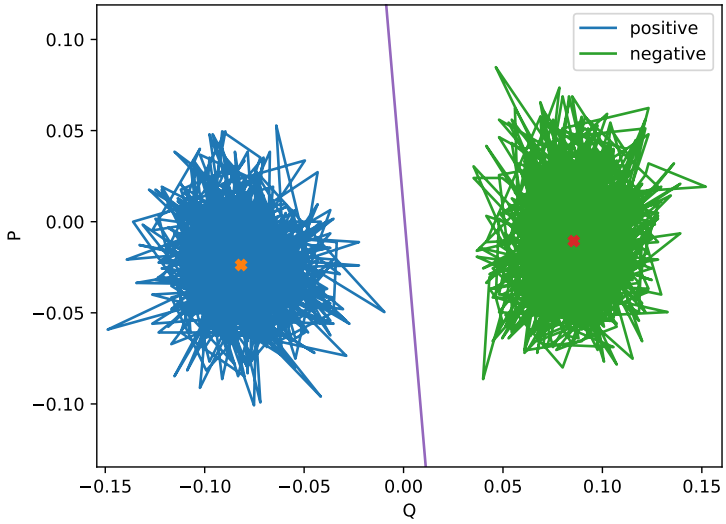


Figure 6.6: *Results obtained from the phase tracking software*

The obtained results are shown in Figure 6.7

In the upper panel we show the theoretical and experimental value for $p(0|0)$ as a function of μ while in the lower panel we show the results of the SDP. In both cases the experimental values are well below the ones predicted by theory. In particular the maximum theoretical $H_{min}(X|E)$ is 0.23 bits per measurement, while experimentally we could only reach 0.078 bits per measurement. However this is an expected result. The theoretical value are calculated for an optimal receiver which is not affected by any loss, noise and whose detectors are 100% efficient. In a real implementation unfortunately all these effects are unavoidable and contribute to a worse discrimination of the incoming states. This reduces the value of $p(0|0)$, which in turn reduces the certifiable $H_{min}(b|E)$.

In order to understand what is the magnitude of these non-idealities we fitted the experimental probabilities to a model where noiseless but inefficient detectors (with efficiency η) are used for the heterodyne detection. The MLE fit returned a value of $\eta = 0.171 \pm 0.002$. With this value inserted in our theoretical model we run again the SDP and we see that experimental data and theoretical predictions perfectly agree.

6.5 Conclusions

In this chapter we have presented a new implementation of the Semi-DI QRNG protocol based on the overlap assumption described in [85]. The novelty of this implementation is the heterodyne detection, which offers some key advantages if compared to experiments employing single photon detectors [85, 86] or homodyne detection[139]. When compared to the first one it shows higher rate and lower cost, since commercial SPD are more expensive than PIN photodetectors and cannot sustain detection rates over 10 MHz. Instead, fast balanced detectors used for the heterodyne setup, are commonly used up to 100 GHz in

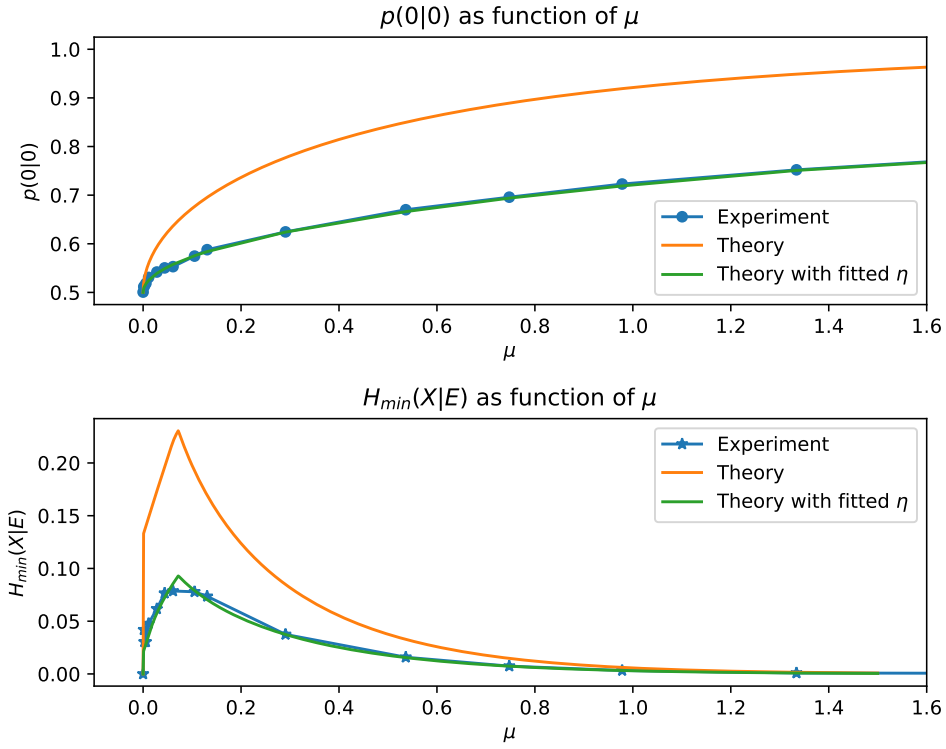


Figure 6.7: *Results obtained from the phase tracking software*

classical communications [141]. If compared to homodyne detection, it solves a critical problem related to phase stabilization. Since homodyne can measure only one quadrature, it is necessary to implement a fast and active phase stabilization system that constantly locks the phase between the two states $|\alpha\rangle, -|\alpha\rangle$ and the strong LO. Otherwise, the distinguishability of the projection of the two states on the quadrature sampled by the homodyne will decrease, up to the limit case when they are 90° shifted, and the two projection completely overlap. This problem is naturally avoided by the heterodyne, since the measurement directly samples both quadratures and the state's discrimination can be done in post-processing using a software-based phase tracking.

In order to show the practical advantages of heterodyne detection, we have implemented experimentally tested the protocol with an all-fiber setup working at 1.25GHz of repetition rate.

The results show that unavoidable losses and excess noise have an impact on the achievable randomness certification, which is almost 3 times lower than what is expected from theory. Still, the system is able to correctly work at high speed without the need of an active phase stabilization, making it a practical solution for Semi-DI QRNG.

Part III

Quantum Communication and Quantum Key Distribution

CHAPTER 7

Introduction to Quantum Key Distribution

The capability of safely transmitting information over untrusted channels is of fundamental importance for any security application. Nowadays, both symmetric and asymmetric encryption schemes are commonly used, but unfortunately they cannot guarantee an *unconditional* security. Their security, in fact, is based on assumptions on the maximal computational power that an attacker could have. However, new theoretical discoveries or new technological developments, could suddenly make this methods insecure. From this point of view, a big threat for most of the classical cryptography is represented by quantum computers. Many quantum algorithms, such as the prime factorization discovered by Shor [142], can exponentially reduce the time needed to crack actual systems seriously threatening all the security framework that is used daily in our society.

Quantum Key Distribution (QKD), together with one-time-pad, can provide a definitive solution to this problem. In this case, the laws of quantum mechanics permit to bound the information that a possible attacker has gained during the key transmission, certifying the security of the distributed keys. In this case the security is unconditional and is not affected by the attacker's computational power, nor it will be in the future.

QKD, proposed by Bennet and Brassard in 1984 [143], is probably one of the first application of quantum information theory and undoubtedly gave an impulse to the entire field. Nowadays, it reached an high maturity and is commercial technology [144].

In this Chapter we will briefly introduce the basic concepts of QKD and describe the BB84 protocol. A more detailed description can be found in the reviews [145–147]. For what concerns the security analysis of QKD, a modern and comprehensive description can be found in [91] for the asymptotic case while in [96] a discussion on finite-size effect can be found.

7.1 Unconditional security: The one time pad and the key exchange problem

While most of the cryptographic methods that are commonly used nowadays only provide computational security, there is a classical (and old) encryption scheme that has proven to be secure against any attacker. This is the Vernam cipher or one-time pad (OTP),invented in 1882 by Frank Miller but patented in 1919 by Gilbert Vernam. In this cipher, the original message is represented as binary string m. Then the ciphertext c is obtained by performing a bitwise XOR operation between m and random key k with the same number of bits of the original message:

$$c = m \oplus k \tag{7.1}$$

where the $\oplus$ is the bitwise XOR operation. The decryption of the ciphertext is as simple as the encryption: is necessary to XOR c again with the key k since:

$$c \oplus k = m \oplus k \oplus k = m \oplus (k \oplus k) = m \tag{7.2}$$

Despite its simplicity, the OTP was proven to be unconditionally secure by the father of modern information theory, Claude Shannon in 1948 [148]. Intuitively, if an attacker tries to bruteforce the ciphertext c, he will obtain as recovered message an possible bitstring with the same length of c, an so we will not be able to discriminate the legitimate message m from the other strings.

However it is mandatory for the security of the protocol that the key k is completely random, never reused and kept secret, otherwise information about k is leaked and can be used to decrypt the messages. Then keys as long as the message are required to be shared between the users in advance, kept secret and destroyed as soon as their are not required anymore.

Thus, while the OTP gives a perfect method to encrypt a message, it only shift the problem to the key distribution, making it extremely unpractical.

7.2 A quantum solution to key distribution problem

Quantum Key Distribution exploits the peculiar laws of quantum mechanics to provide a solution to the key distribution problem, allowing two parties, typically called Alice and Bob, to share a random and secure string of bits through an insecure quantum channel and an authenticated classical channel.

The first idea of Quantum Cryptography was proposed by Stephen Wiesner in 1970 and then published in 1983 [149]. However, the first protocol for a secure quantum communication was proposed by Charles H. Bennett and Gilles Brassard in 1984 [150] and since then is known as BB84. The BB84 exploits the exchange of single quantum particles between Alice and Bob for the exchange of the secret key. The security in this case,is guaranteed by the properties of quantum mechanics, and thus is conditioned only on fundamental laws of physics on being correct. These types of protocols where Alice encodes the key in a quantum

system and sends it to Bob are typically called prepare and measure. However, in 1991 A. Ekert showed that also the entanglement between two particles could be used to share a key[151]. In this case an entangled source is placed between Alice and Bob that receive and measure one particle of the entangled pair each. For these types of protocols, called entanglement-based, security is assured by the violation of a Bell inequality and can be implemented in a Device-Independent way [152].

In the next section we will take the BB84 as an example to describe the various steps of a typical prepare and measure QKD protocol

7.2.1 The BB84 protocol

The two users that want to share a secret key, Alice and Bob, need to have access to an untrusted public quantum channel and an authenticated classic channel.

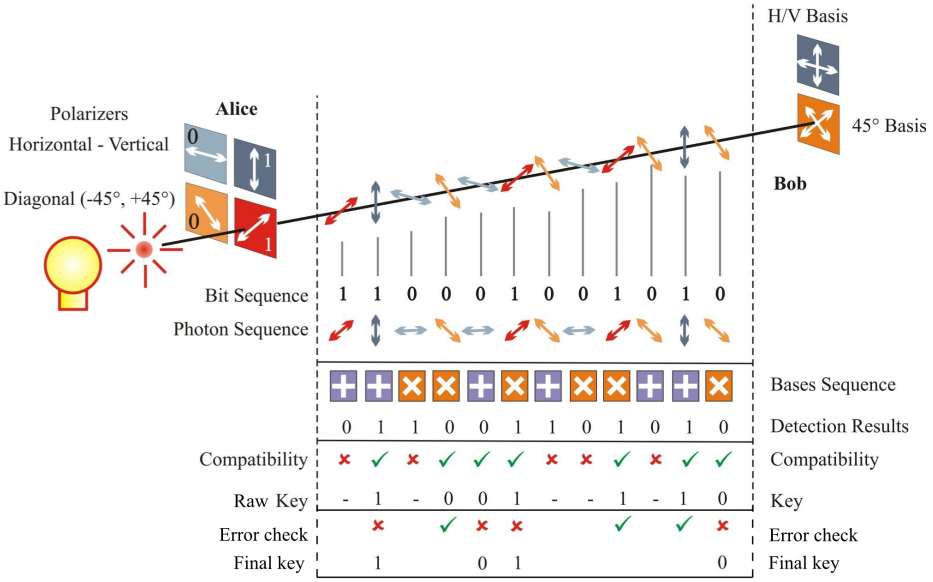


Figure 7.1: *Graphical representation of the polarization implementation of the BB84 protocol. Adapted from [153]*

The first step is the **quantum transmission**. During this step Alice encodes a random sequence of bits in a qubit, using randomly one of two mutually unbiased bases, $\mathbb{Z}$ and $\mathbb{X}$. In the original BB84 the encoding is done with equal probability, but this probability can be biased [154] in order to increase the efficiency. The prepared qubits are sent to Bob via the quantum channel and Bob randomly measures the qubits in $\mathbb{Z}$ or $\mathbb{X}$ (if he uses the efficient BB84[154] also the measurement probability is biased).

Then they perform the **sifting**: Bob publicly announces the bases used for the measurement and Alice will tell for which bits they used different bases and they have to discard. They are left with the sifted bits.

After that they perform the **parameter estimation**: they publicly announce a subset of the sifted bits and they calculate the Quantum Bit Error Rate (QBER), that is used to

estimate the amount of information leaked to Eve during the quantum transmission phase. If this quantity is above a threshold value, they cannot certify the security of the key and the protocol is aborted. Otherwise, they proceed to the error correction.

During the **error correction** they interactively share a small portion of their strings in order to correct any mismatch between the two strings. At the end of this procedure they are left, except for a probability ϵ_c, with two identical strings.

Finally they perform **privacy amplification**. This procedure is equivalent to the randomness extraction discussed in Sec 2.4.3. By measuring the quantum states and sniffing the communication during the previous steps, the attacker could have partial knowledge about the key. Luckily this information can be bounded and erased using a strong randomness extractor. Then, after estimating the smooth min-entopy $H_{min}(X|E)$ of their string conditioned on the attacker's information, Alice and Bob apply the same a strong extractor to their string. The resulting (shorter) strings are now, up to some security and correctness parameter ϵ_s, ϵ_c, secure and identical.

7.3 Security

Informally, the security of the BB84 can be related to three facts:

- Alice sends a set of non-orthogonal states
- The no-cloning theorem
- Information gains implies perturbation in quantum mechanics

Intuitively, if Alice encodes the key in non-orthogonal states, for the no-cloning theorem, Eve can't perfectly copy the quantum state of the transmitted qubit and, if she tries to do it, the state she obtains necessary contains errors. Instead, if she tries to measure the quantum state, she needs to interact with it, introducing errors which can be revealed by Alice and Bob.

This short discussion, however, is far from a formal and rigorous mathematical proof of security.

The first security proof for the BB84 under arbitrary attacks was presented in [155] and then refined by Shor and Preskill in [156] using the properties of CSS codes. Here the authors show that the achievable secure key rate in the asymptotic limit can be expressed as:

$$r_{sec} = 1 - 2h(Q) \tag{7.3}$$

where $h(x)$ is the binary entropy and Q is the QBER. This means that the BB84 is robust and can distill a secure key for QBER up to 11%.

Later, in 2005 Devetak and Winter derived a general asymptotic bound for protocols with one-way direct reconciliation for the classical post-processing:

$$r = H(A|E) - H(A|B) \tag{7.4}$$

where $H(X|Y)$ is the conditional von Neumann entropy. This formulation gives a profound insight to the physics of the problem: the first term $H(A|E)$ is the conditional entropy of

Alice's string conditioned on Eve's side information E and represents the ignorance of Eve about Alice string. The second term $H(A|B)$ instead represents the ignorance of Bob about Alice's string. Then, the infinite key rate can be understood as the information that is left after privacy amplification (that depends on $H(A|E)$) minus the information that we have to disclose in order to correct the mismatch between Alice and Bob's string (that depends on $H(A|B)$).

In the same period, Renner developed a complete security framework for QKD based on the concept of composable security and derived for the first time a finite-key security proof [91]. After that tighter bound in the finite regime were derived, which exploited the EUP [157].

7.4 Assumptions and attacks

We have stressed that QKD is able to guarantee an unconditional security against any attacker constrained by the laws of physics. However,*unconditional security* should not be confused with *absolute security*, which can never be obtained [158].

The security of QKD holds under a set of assumptions[158]:

- Eve cannot intrude into Alice's and Bob's devices to access either the emerging key or their choices of settings
- Alice and Bob must trust the random number generators that select the state to be sent or the measurement to be performed.
- The classical channel is authenticated with unconditionally secure protocols, which exist [97]
- Eve is limited by the laws of physics. In particular, has to obey the whole of quantum physics
- The theoretical model and the experimental implementation of the devices has to match. In a certain sense, this require to trust the devices used in the protocol (a condition similar to the one discussed in Chap 2)

If one of these assumptions is not respected, the security of the entire protocol cannot be guaranteed. This last assumption in particular is extremely hard to enforce in any practical scenario, since any real device will inevitably slightly deviate from any theoretical model.

In the years, these imperfections have been successfully used to compromise real QKD systems. These attacks usually exploit the imperfections of Alice preparation stage, or flaws in of Bob's detectors.

One of the common attacks is called **Photon Number Splitting (PNS)** . Despite the efforts to develop on-demand true single photon sources, such sources are still not commercially available and weak coherent pulses (WCP) from a laser source are typically used. Unfortunately, their Poissonian statistics always yields a non-zero probability multi-photon emission. These multi photon events can compromise the security since, Eve can simply block all the single photon events, while in the other case she forwards one photon to Bob and she can measures the others, without disturbing Bob's system [159]. Luckily, new protocols based

on the decoy technique, are not affected by this issue [154, 160]. Another common attack is the **Trojan horse** attack. Here Eve sends bright pulses in the trasmitter or receiver setup and, by looking at the reflections, she can learn the modulation they used and their settings [161]. In this case the assumption of no information leakage from the lab is not respected. Probably the most successful attack is the **Detector's blinding** attack. This type of attack has been used to break also also commercial QKD systems [162]. Here the attacker shines a continuous bright laser in the SPAD modules at the receiver, bringing them from the Geiger mode to the linear mode. In this regime, Bob's detectors are not single photon detector anymore: they click only if another bright pulse is shot at it, regardless of the quantum properties of that pulse. In this way Eve has the full control of Bob's detector and can make it click when she wants, compromising the protocol. This attack can be mitigated, for example, by randomly changing the efficiency of the detectors [163] or employing new protocols, such as Measurement Device-Independent [164, 165], which are not affected by this issue.

Thus, also if QKD is unconditionally secure, the security of real implementations can be severely compromised. In order to mitigate the problem few solutions can be developed. First, is possible to improve security proofs in order to include imperfections of the devices relaxing the assumptions. This path however, requires to consider all the imperfections, also the ones still unknown, making it quite impractical. From a technological point of view, an option could be to develop devices with smaller imperfections respect the ideal one.
Finally, a third solution is to push toward the theoretical and experimental development of Device-Independent protocols, whose security does not relies on the devices used.

CHAPTER 8

QCosOne: A daylight free-space QKD prototype for future satellite terminals

Space-based quantum key distribution would allow, in the near future, secure communications between parties over continental distances, complementing short-range fiber-based quantum networks. A major challenge in the implementation of a global network is to render space-to-ground quantum links compatible with such fiber-based networks, which require, for example, effective daytime operation. Moving the operating wavelength of space quantum communication to the telecom C band allows to fulfill these requirements, but further demonstrations and systems are still necessary.

In this chapter I'll describe the QCosOne project, realized in collaboration with the Italian Space Agency (ASI) and Scuola Sant'Anna di Pisa, were we have developed a full prototype for daylight quantum key distribution. The prototype, based on polarization encoding and operating at the wavelength of 1550 nm, has been realized exploiting both fiber-based modulator and integrated silicon photonics for the transmitter architecture.

The system has been tested over a 145m-long free-space channel in Padua, during severals sunny days and the performance of both transmitters have been compared. In particular, the integrated transmitter showed a lower intrinsic QBER and higher stability making it possible to reach a secret key rate exceeding 30 kbps in daylight when taking into account finite-size effect.

The clear superiority of integrated photonics versus the discrete-components counterpart, opens the way for designing compact and efficient optical payloads for satellite QKD systems, compatible with today's telecom infrastructure.

Some contents of this chapter are part of our work [2].

8.1 Towards daylight satellite QKD systems

QKD systems in the last few decades have rapidly moved from proof-of-principle demonstrations to mature commercial products, capable of working without interruptions over hundreds of kilometers. Recently, thanks to new technological developments, fiber-based QKD has been demonstrated at distances of over 420km[166]. Moreover, new protocols such as Twin-Field introduced in [167], have been showed to overcome the PLOB bound [168] that limits the achievable rate of point-to-point quantum communications in absence of quantum repeters. The first proof-of-principle implementations of such protocols[169–171] showed that distances of more than 550km can be achieved with today's technology.

The implementation of QKD over longer fiber distances, however, would necessarily require quantum repeaters, whose experimental realization is still complex and challenging[172].

With today's technology a more practical solution is represented by Satellite QKD. In fact, in satellite-ground links the major effect on losses and turbulence is only caused by the effective thickness of the atmosphere of about 10km, making it able to reach distances much longer than what is possible with optical fiber.

Despite the recent demonstrations also realized in satellite-to-ground links [173–176], free-space QKD-technology is currently limited and cannot compete with its fiber-based counterpart [166, 177–179], both in terms of performance and reliability of the link. Hence, in the vision of a continental-scale quantum network (or quantum internet) [180–183]) where both types of link are required to jointly operate, certain key requirements for free-space QC can be formulated, as i) full-day functionality, ii) compatibility with standard fiber-based technology at telecom wavelength, and iii) the achievement of stable coupling of the free-space signal into a single-mode fiber (SMF).

Regarding i), the background noise due to sunlight poses a serious limitation on the achievable performance of day-time free-space QC, limiting most of the demonstrations obtained so far to night-time. For this reason, various studies have focused on the feasibility of *daylight* QKD [184–189]. Most of them exploited light in the 700-900 nm band which allows for for a good atmospheric transmission, and to exploit commercial low noise silicon-based single-photon avalanche diodes (SPADs). To reduce the background noise due to Sun and to maintain, at the same time, a good efficiency in the atmospheric transmission, the choice to use light signals in the telecom C-band (around 1550 nm) has only very recently started to be investigated [188, 189].

Moving the operating wavelength to the telecom band comes with (at least) two advantages. Firstly, it is the standard choice in fiber-based optical (classical and) QC, hence fulfilling the requirement ii). Secondly, it is compatible with integrated photonics [3, 190–192], which represents a promising choice for designing light, compact, scalable and low power-consuming devices suitable for portable QKD transmitter and to design satellite optical payloads [193, 194].

Furthermore, to match the requirement iii) it is necessary to actively compensate for the optical aberrations (at least the beam wander and angle-of-arrival fluctuation) introduced by atmospheric turbulence, which is experimentally challenging. However, a stable coupling of the light signal into a SMF has the advantage of allowing the use of commercially available superconductive nanowire single-photon detectors (SNSPDs), which represents the standard

for fiber-based state-of-the-art QKD demonstrations [166, 178, 195].

Taking into account the previous points, we can see the QCosOne project as a ground demonstration aimed to evaluate problems and performances of future daylight satellite links.

8.2 The big picture

The realization of a complete free-space QKD system, requires the development of many different components that are interfaced to each other and need to work together during the key exchange. In order to reduce the total complexity, we decided to take a modular approach ad divide the prototype design in different logic units. Each unit is responsible of a specific task and includes the interfaces necessary to correctly communicate with the other units. This approach has two fundamental advantages: first, after the units and the interfaces are defined, each unit can be developed in parallel. Secondly, if at any time one of the units needs to be replaced or upgraded, there won't be compatibility issues as long as the interfaces are correctly implemented. In QCosOne we have 5 fundamental units that are schematically represented in Fig 8.1: QKD source, QKD receiver, PAT (Pointing, Acquisition, Tracking), Syncronization and Telecom (or classical channel)

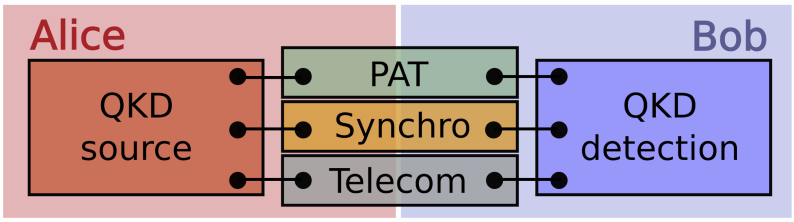


Figure 8.1: *Schematic representation of the different units in the QCosOne project*

In the next sections each unit will be discussed in detail.

8.3 QKD source

8.3.1 Protocol and implementation

We chose to realize the 3-state 1-decoy version of the efficient BB84 protocol proposed by Rusca *et al.* [196]. This protocol has been chosen mainly for two reasons: first, for the typical parameters of our experiment, this protocol yields an higher Secret Key Rate (SKR) in finite-size regime respect the 2 decoy analysis presented in [197]. Additionally, the generating only two intensity levels and three polarization states drastically reduces the complexity of the experimental implementation. In fact, both for the bulk and the integrated QKD source, only a digital signal is required for the intensity and for the polarization modulation. The generation of 2 decoy and 4 states of polarization would have required an high-speed DAC, increasing the complexity of the electronic driving system.

The protocol works in the following way: Alice randomly encodes a weak coherent pulse either in the $\mathbb{Z}=\{|0\rangle,|1\rangle\}$ basis, with probability $p_A^{\mathbb{Z}}$, or in the $\mathbb{X}=\{|+\rangle,|-\rangle\}$ basis,

with probability $p_A^{\mathbb{X}} = 1 - p_A^{\mathbb{Z}}$. The basis $\mathbb{X}$ is Mutually Unbiased with respect to $\mathbb{Z}$, namely $|\langle 0|\pm\rangle|^2 = |\langle 1|\pm\rangle|^2 = 1/2$. In our implementation, we have chosen $|0\rangle := |L\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$, $|1\rangle := |R\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$ and $|\pm\rangle := (|H\rangle \pm |V\rangle)/\sqrt{2}$. Alice needs to generate only three polarization states, $|0\rangle$ and $|1\rangle$ with uniform probability for the $\mathbb{Z}$ basis, and $|+\rangle$ for the $\mathbb{X}$ one. The intensity level of the pulse is randomly chosen between two values, μ_1 and μ_2, with probabilities p_{μ_1} and $p_{\mu_2} = 1 - p_{\mu_1}$, respectively. The two values can differ between pulses prepared in $\mathbb{X}$ and $\mathbb{Z}$ ($\mu_1^{\mathbb{X}} \neq \mu_1^{\mathbb{Z}}$, $\mu_2^{\mathbb{X}} \neq \mu_2^{\mathbb{Z}}$), because we carry out the yield analysis separately in the two bases [198]. This procedure allows to detect a possible photon-number-splitting attack [199].

Bob, at his site, measures the incoming photons in the two bases $\mathbb{Z}$ and $\mathbb{X}$, with probability $p_B^{\mathbb{Z}}$ and $p_B^{\mathbb{X}} = 1 - p_B^{\mathbb{Z}}$, respectively. After the photons exchange, Alice and Bob announce, for each detected event, their basis choices. Then, $n_{\mathbb{Z}}$ raw sifted bits are obtained by comparing the detections in the $\mathbb{Z}$ basis, while the ones from the $\mathbb{X}$ basis are used to estimate the information leakage toward a potential eavesdropper.

After generating a raw key, Alice and Bob proceed with the error correction (EC) and the privacy amplification (PA) steps, ultimately obtaining, for each PA block, a secure secret key of l bits, which is bounded by [196]:

$$\begin{aligned} l \leq\, & s_{\mathbb{Z},0} + s_{\mathbb{Z},1}(1 - h(\phi_{\mathbb{Z}})) - \lambda_{\mathrm{EC}} \\ & - 6\log_2(19/\epsilon_{\mathrm{sec}}) - \log_2(2/\epsilon_{\mathrm{cor}}) \,, \end{aligned} \tag{8.1}$$

where $s_{\mathbb{Z},0}$ and $s_{\mathbb{Z},1}$ are the lower bounds on the number of vacuum and single-photon detections in the $\mathbb{Z}$ basis, $\phi_{\mathbb{Z}}$ is the upper bound on the phase error rate corresponding to single photon pulses, $h(\cdot)$ is the binary entropy, $\lambda_{\mathrm{EC}} = f_{\mathrm{EC}} n_{\mathbb{Z}} h(Q_{\mathbb{Z}})$ is the total number of bits revealed during the EC step — which depends on the reconciliation efficiency of the EC algorithm (Cascade, in our case $f_{\mathrm{EC}} \approx 1.06$), the number of raw key bits $n_{\mathbb{Z}}$, and on the QBER $Q_{\mathbb{Z}}$ — and $\epsilon_{\mathrm{sec}} = 10^{-10}$, $\epsilon_{\mathrm{cor}} = 10^{-12}$ are the secrecy and the correctness parameters, respectively [196].

The classical postprocessing, that includes the classical communication between Alice and Bob, the error correction and the privacy amplification, is handheld by the telecom unit and is performed by a software based on the AIT QKD R10 software suite by the Austrian Institute of Technology (AIT)[200], .

8.3.2 Bulk source

The design goals of the QKD source were: portability and long-term stability. Since we were planning to move the QKD transmitter outside the lab environment, we looked to transmitter design that showed an high stability with respect to external perturbations. Moreover, the ultimate goal was to develop a QKD transmitter for a future satellite payload, where space and tuning are severely limited. The final design is presented in Fig 8.2.

The laser

The laser used for the experiment is a distributed feedback (DFB) laser module by Gooch&Housego, with maximum optical power of 10mW, center wavelength of 1550nm and nominal FWHM linewidth of 1MHz. The module integrates a TEC controller for temperature stabilization.

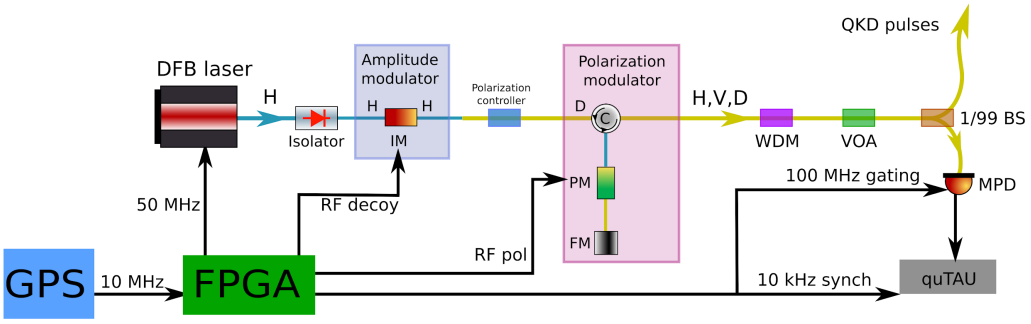
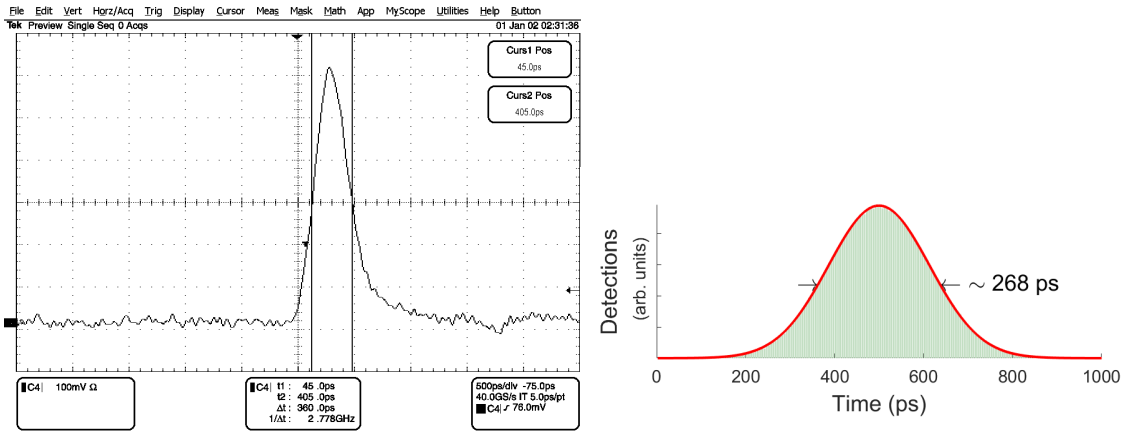


Figure 8.2: *Schematic representation of the working principle of the bulk QKD source*

The module also integrates a bias-tee which can be used to directly modulate the laser current via an RF signal. The maximum modulation bandwidth is 12GHz (3db point).

The laser is normally biased under threshold so that no stimulated emission occurs. When an optical pulse is needed a short electrical pulse ($\approx 350ps$ FWHM), generated by a Xilinx $XC7Z020$ FPGA, and amplified by a wideband Monolithic InGaP HBT MMIC Amplifier (6GHz BW) by Minicircuits, is sent to the RF port, directly modulating the current above threshold. In this way the laser is gain-switched and short phase-randomized optical pulses are obtained.



(a) **(b)**

Figure 8.3: *a) RF pulse used for the direct modulation of the DFB laser, b) temporal histogram of the produced optical pulses*

The bias voltage, the temperature of the laser and the shape of the RF pulse affect the dynamics of the laser changing the spectrum and the chirp of the emitted optical pulse. In order to find the best parameters for the experiment, recorded the emitted spectrum with an Optical Spectrum Analyzer while scanning the above mentioned parameters. In order to reduce the spectral broadening and the chirp, before measuring the spectrum with the OSA we filtered the light with a 100GHz commercial DWDM centered around channel 34 (1550.12nm). The results, showed in Fig.8.4 , are compatible with the description given in

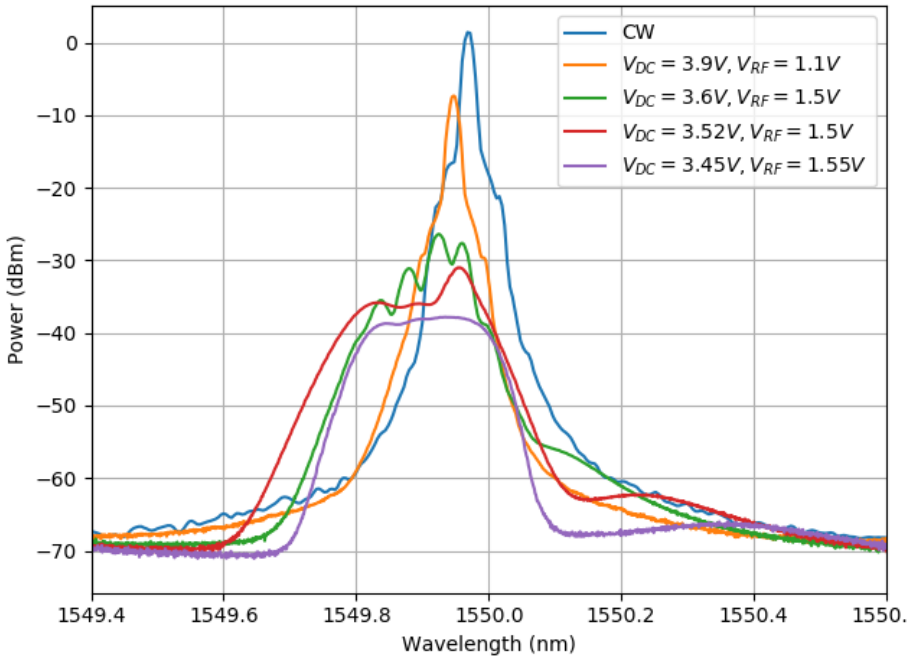


Figure 8.4: *Spectrum of the filtered light as a function of the modulation parameters (the mismatch of the wavelength respect the nominal channel of the WDM is due to a calibration offset of the OSA)*

[201].

Finally, with the selected parameters we generate a stream of phase-randomized pulses at 50MHz with ∼270 ps of FWHM.

Intensity modulator for decoy

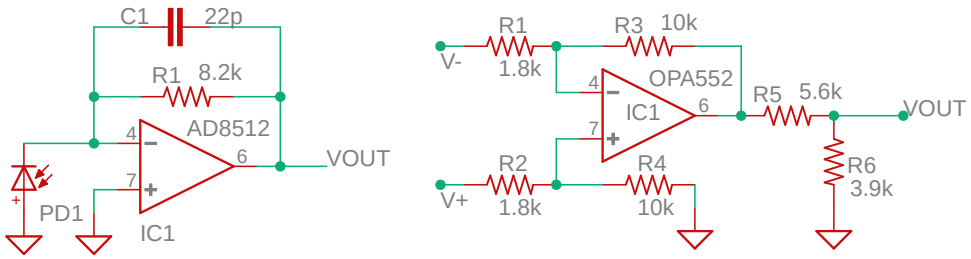
The intensity modulation required for the decoy procedure is realized by a LN81S zero-chirp intensity modulator (IM) by Thorlabs with an RF bandwidth of 10 GHz. The modulator is made by an X-Cut Titanium Indiffused $LiNbO_3$ crystal and integrates a polarizer, making it able to support only the H polarization. The device features an RF port, a DC bias control port and a monitor photodiode port. The RF port is used to modulate the light with time-changing signals. The device has a typical V_π at 1GHz is $5.6V$ for an input impedance of $Z_i = 50\Omega$. In order to be able to drive the modulator with signals coming from the FPGA, the $LVDS$ signals are amplified by a wideband InGaP amplifier by Mini-Circuits with a gain of 25dB and P1dB of 21dbm.

Unfortunately, $LiNbO_3$ modulators are very sensitive to temperature, mechanical and RF power drifts, which directly reflect in a unpredictable drift of the transmitted optical power. While X-Cut crystals are far less sensitive than Z-Cut crystals, the effect is visible also in our device. For this specific reason the device is equipped with an integrated monitor photodiode, that measures part of the transmitted light and a DC bias port, which is able to slowly change the relative phase, in order to compensate for the drifts in the output power.

In order to guarantee stability over time, we have developed a digital feedback loop based

on a modified PID algoritm on a ESP32 micro-controller. The control system constantly read the power of the monitor photoiode and control the DC bias voltage in order to compensate any intensity drift.

The ESP32 microcrontroller, is mounted on a Adafruit HUZZAH32 board that features 18 12-bit Successive Approximation Register (SAR) ADC and 2 $\Delta - \Sigma$ 8-bit DAC. Unfortunately, these analog interfaces cannot directly sample the monitor photodiode and drive the bias port. The small photocurrent generated by the photodiode needs to be first amplified by a transimpedance amplifier before being sampled by the ADC (which has a range of 0-1.1V). The DAC on the other hand can only supply few mA and voltages from 0 to 3.3V, which are not sufficient to drive the bias port (-8 to +8V). In order to provide the necessary analog signals we have realized a transimpedance amplifier (TIA) and a differential amplifier (DA), whose schematics are reported in Fig 8.5



(a) **(b)**

Figure 8.5: *Circuit schematics of: a) the transimpendace amplifier used to amplify the photocurrent of the monitor photodiode, b) the differential amplifier used to drive the bias port of the IM*

The TIA employs an AD8512 precision and low noise op-amp, specifically designed for photodiode receivers. Since we do not require high bandwidth, we don't apply a reverse bias to the photodiode, making it working in photovoltaic mode, reducing the photocurrent noise. The feedback resistance is selected such that the output voltage matches the ADC range. The feedback capacity of 22pF is necessary in order to avoid oscillations and ringing. The DA employs an OPA552 high-voltage, high-current op amp for driving the bias port. Since the OPA552 is stable only for gain ≥ 5 (which is higher than the required value of ±8V), the output is attenuated with a resistive voltage divider. Since we require a bipolar output, but the ESP's DAC can only provide unipolar output from 0 to 3.3V, we drive both inputs of the DA with an independent DAC channel. When a positive output is required the non-inverting input is driven and the inverting input is set to 0V, while when negative outputs are required we do the opposite.

The PID algorithm is implemented directly in the ESP32, which is programmed with the Arduino environment.

The results of the feedback control are presented in Fig 8.6

On the top panel we can see the typical time response of the PID, which is around 8s. This value is limited by the chosen PID parameters and not by the electronics (which is able to work up to hundreds of kHz). In the lower panel we can see the comparison between the output power with and without the PID. When the PID is on, a constant optical power is

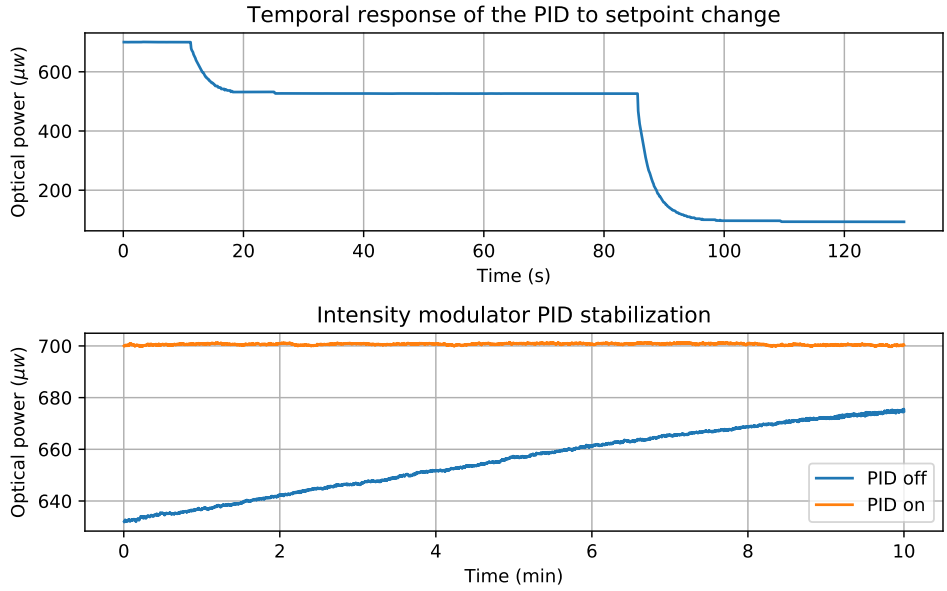


Figure 8.6: *In the top figure we can see time response of the PID to a setpoint change. In the lower figure we can see the drift in output power of the IM with and without the PID.*

maintained with fluctuations with 0.3%.

An alternative solution that is able to self-compensate the drifts thanks to its Saganc configuration has been presented in [202]. Unfortunately, at the time, we were not aware of this interesting and simple configuration.

In any case, after a proper mechanical and thermal insulation, we haven't experienced significant intensity drifts during the realization of the free-space QKD links and no active feedback was necessary.

The polarization modulator

A common solution for the fast modulation of polarization in fiber is given the so called "inline" phase-modulator configuration [203, 204].

In this configuration, diagonally polarized light is sent to a Z-Cut Titanium Diffused $LiNbO_3$ phase modulator. These phase modulators can support light travelling both in the TE and TM mode of the waveguide, however the strength of the electro-optical effect is different for the two modes (the effect in one axis is usually 3 time larger than the other). So when an RF pulse (with voltage V_{RF}) is applied to the incoming state $|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ the output state $|\psi\rangle = \frac{e^{i\phi_g(V_{RF})}}{\sqrt{2}}\left(|H\rangle + e^{i\phi_r(V_{RF})}|V\rangle\right)$ acquires both a global phase $e^{i\phi_g(V_{RF})}$ and a relative phase $e^{i\phi_r(V_{RF})}$ between the two polarization components. By properly tuning V_{RF} all the polarization states in the XY plane of the Poincarè sphere can be generated. In particular it is possible to generate $|+\rangle, |L\rangle, |-\rangle, |R\rangle$ which are the states required for the BB84 protocol.

Unfortunately, Z-Cut $LiNbO_3$ modulator are even more sensitive to thermal and me-

chanical fluctuations than X-Cut modulators and an active stabilization (similar to the one presented in the previous section) would have been necessary.

Instead, we decided to implement the double pass configuration with a Faraday mirror (FM) described in [205] and schematically represented in Fig.8.2. In this configuration the "inline" polarization modulator described previously is placed between the second port of a circulator and a Faraday mirror. Since the FM "exchanges" $|H\rangle$ with $|V\rangle$ any phase fluctuation that occurs when the light travels from the circulator to the FM is exactly canceled out on his way back from the FM to the circulator (for a formal discussion see [205]). Thanks to this self-compensation, a long-term stability in the output polarization is ensured.

But this configuration provides another key advantage. The creation of three states of polarization can be obtained by modulating only the optical pulse after this is reflected by the FM by sending three different voltages V_0,$V_{\pi/2}$ and V_π (or $V_{-\pi/2}$) to the Phase Modulator. This would require a fast DAC connected to the FPGA, increasing the cost and the complexity of the electronic fronted. However, the same modulation can be obtained with a single digital signal. If we modulate the pulse before it gets reflected by the FM the final state will acquire a negative phase shift ϕ_e, while if we modulate the state after the FM reflection it will acquire a positive phase shift ϕ_l, and the final state will be $|\psi\rangle = |H\rangle + e^{i(\phi_l - \phi_e)}|V\rangle$. The if we choose $V_{RF} = V_{\pi/2}$, we obtain $|L\rangle = |H\rangle - i|V\rangle$ if the reflected pulse is modulated,$|R\rangle = |H\rangle + i|V\rangle$ if the pulse before reflection is modulated, $|D\rangle$ if none of the pulses (or both) are modulated.

Clearly, this reduced complexity on the amplitude modulation of the electrical pulses comes at the price of an higher accuracy required on the timing.

In our implementation we employed, a circulator followed by a Lithium Niobate phase-modulator by iXblue Photonics, in which the input polarization-maintaining fiber is aligned at 45° with respect to the fast-optical axis of the modulator followed by a Faraday mirror by OzOptics. The RF pulses are generated by the FPGA and then are amplified by a wideband InGaP amplifier by Mini-Circuits with a gain of 25dB and P1dB of 21dbm.

Each polarization state is characterized by an extinction ratio (ER) , that is the ratio between optical power in two orthogonal polarization states, of at least 17 dB.

The limited ER (as discussed in [205]) is caused by the Polarization Mode Dispersion induced by the crystal and the PM fiber of the Phase modulator connected to the circulator.

The stability of the polarization modulator has been tested and the results, presented in Fig 8.7, show than an ER of up to 15db is maintained for ≈10min. The drift is mainly caused by the fluctuation of the input polarization, caused by the temperature drift of the circulator's SM fiber. A circulator with PM fiber would solve the issue, at the expense of a lower ER. A solution could be to connect the circulator's PM fiber and the Phase modulator PM fiber rotated by 90°, so that part of the PMD is compensated.

Most of the drawbacks of this polarization modulator can be solved using the POGNAC, described in Chapter 9. Unfortunately, at the time we did not came up with that idea yet.

The decoy estimation

The last section of the QKD transmitter is dedicated to the attenuation and check of the mean photon number.

The optical pulses pass through a dense wavelength-division-multiplexer (dWDM) matched with the one at the receiver for spectrally cleaning the signal wavelength. Then we have a

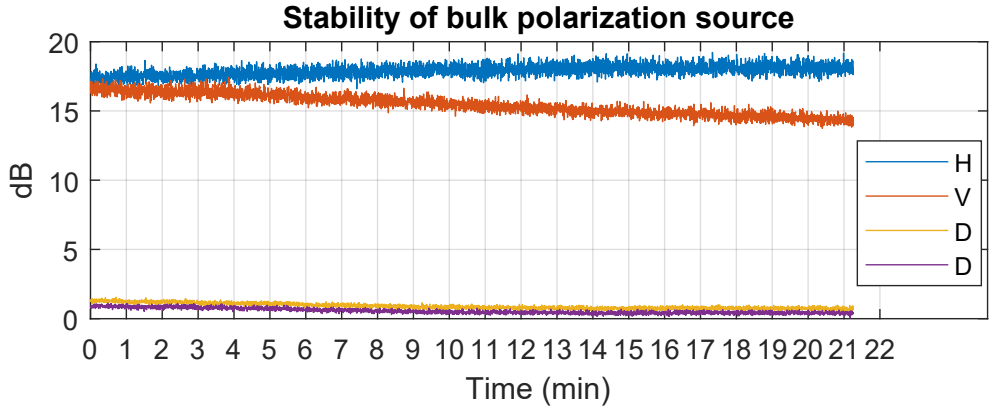


Figure 8.7: *Stability of the bulk polarization modulator.*

variable optical attenuator (VOA), and a 99/1 fiber beam splitter (BS). The 1% output is directed to an InGaAs/InP SPAD by Micro Photon Devices [206], while the 99% goes to the transmitting telescope. The SPAD is gated with a 100 MHz clock generated by the FPGA and synchronized with the 50MHz signal that drives the laser. The NIM signal generated by the SPAD are converted with a NIM-TTL card and then recorded by a quTAU timetagger by quTools. Since the quTAU cannot be clocked, we also acquire a decimated version of the 100MHz gating signal for synchronization.

Having calibrated the losses in the transmitter and in the transmitter telescope, the timetags from the SPAD can be used to have a realtime estimation of the decoy levels $\mu_{1,2}^{\mathbb{X},Z}$.

This information is used both as as a check for the intensity drifts of the IM and for setting the right parameters in the privacy amplification.

Finally, Fig 8.8 shows a photo of the portable QKD source during the first tests.

8.3.3 Silicon photonics quantum state encoder

Fiber modulators based on $LiNbO_3$ crystals are an effective commercial resource for the realization of a portable QKD transmitter. However, their price is rather expensive and in the previous section we have seen that the performance they can offer, if not actively stabilized, are rather limited for what regards both the stability and the extinction ratio. Moreover, their spatial footprint cannot be further reduced without increasing the RF power required to drive them.

All these points play an important role not only in satellite applications, where space, power and tunability are limited, but also for a wider adoption of QKD that requires an higher scalability and lower costs.

In the last few years, the huge development of Silicon Photonics[207, 208], mainly driven by the datacenter industry, made it possible to realize stable, compact and low cost photonic transceiver capable of working up to 30GHz, [209]. These capabilites, easily accessible through MPW runs[210], motivated the development and demonstration of Photonic Integrated Circuit (PIC) for quantum communications, both in discrete and continuous variable [191, 192, 211].

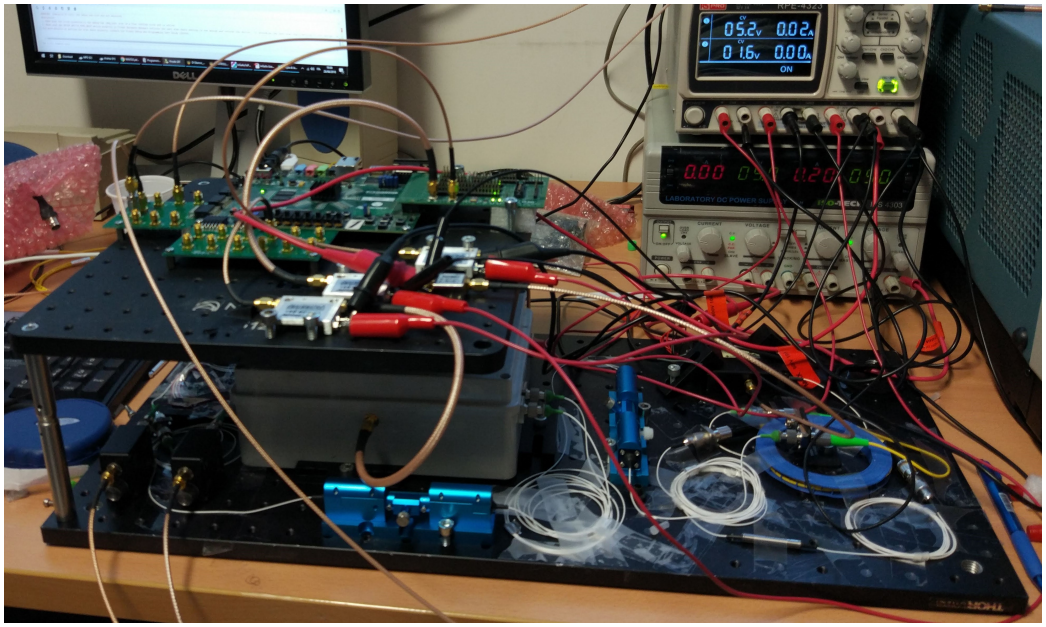


Figure 8.8: *Photo of the bulk QKD transmitter*

The long-term stability and possibility to shrink down the size of the QKD transmitter down to such a small volume represented an attractive choice for designing portable transmitters and payloads for satellite QC. Hence, we decided to develop, in collaboration with ASI and Scuola Superiore Sant'Anna di Pisa, a compact Silicon PIC capable of performing both the intensity and polarization modulation required for the implementation of the protocol described in Sec 8.3.1. The PIC was designed in-house and realized exploiting the Europractice IC Service [210] offered by the IMEC foundry.

Now we will describe the design and working principle of the integrated QKD source, presented in Fig. 8.9

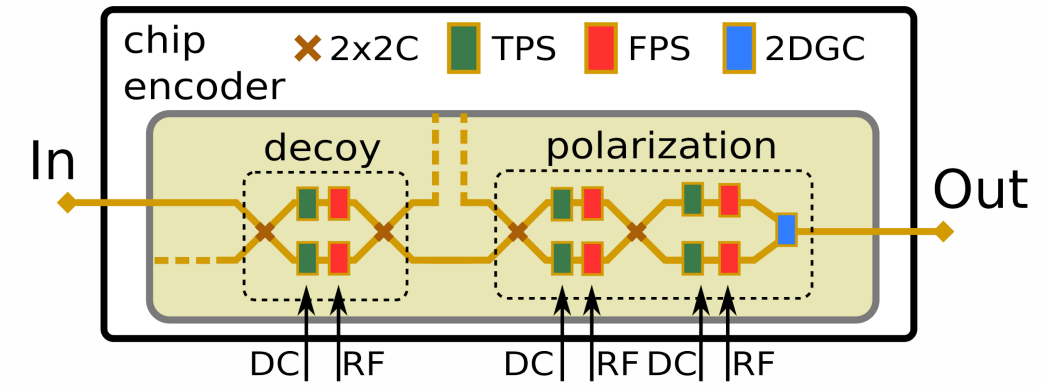


Figure 8.9: *Schematic representation of the integrated source with optical In/Out fiber connections and required DC and RF signals. The components used are 2x2 MMI couplers (2x2C), Thermal Phase Shifters (TPS), Fast carrier-depletion Phase Shifers (FPS), 2d-Grating Coupler (2DGC).*

PIC's building blocks technology

The PIC comprises several interferometric structures exploiting standard building blocks provided by the foundry, e.g. multi-mode interference (MMI) devices acting as 50/50 beam splitters, slow thermo-optics modulators (TOMs, ∼kHz of bandwidth, DC modulation) and fast carrier-depletion modulators (CDMs, ∼10 GHz of bandwidth, RF modulation).These two types of phase modulators are the key elements that enable both polarization and intensity modulation on the PIC. The TOM exploits the thermal dependence of the silicon's refractive index to change the phase of light travelling in the waveguide. In the PIC is realized by depositing a metal close to the waveguide. The magnitude of the phase shift can be tuned by changing the heat dissipated by the metal structure, which is controlled by an external voltage source. Since the effect is driven by the thermal diffusion in the material, the 3db bandwidth for the TOM is quite low, approx 10kHz. However, they show relatively low $V_\pi = 4V$ and they do not introduce modulation-dependent losses. The CDM instead exploits a different physical mechanism to provide the phase-shift. The silicon waveguide is doped with a P-type and N-type region,as shown in Fig 8.10: The doping creates a PN junction

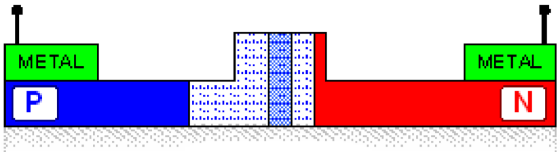


Figure 8.10: *Cross section of a doped carrier depletion modulator*

across the waveguide, that behaves like a diode. When the junction is reverse biased, the carrier concentration in the intrinsic region changes (gets depleted), changing the refractive index of the waveguide. The maximum bandwidth achievable for this type of modulators, mainly depends on the carrier mobility and can be higher than tens of GHz[212]. The V_π depends on the length of the modulators and is usually $\approx 14\text{V}\,\text{mm}^{-1}$. However, the change of the carrier concentration in the waveguide changes also the absorption of the waveguide and CDM exhibits modulation-dependent losses, which can be a problem in the realization of a QKD source.

More details on the working principle of the components of the PIC and on the fabrication process can be found in Refs. [191, 213, 214].

PIC design and working principle

Light is coupled from a standard SMF28e single mode fiber into the PIC via an 8-channel SMF-array glued to the PIC's grating couplers (GCs). Then an interferometric structure realizes a Mach-Zehnder interferometer (MZI), and one of the output is sent to the next structure on the PIC, while the second output is coupled out for monitoring purposes. In this way we implement the amplitude modulation of the pulses, according to QKD protocol (described in 8.3.1), which requires preparing pulses with two different intensities μ_1 and μ_2, with $\mu_1 > \mu_2$. Each arm of the MZI contains a slow TOM and a fast CDM for the phase modulation. A DC-bias voltage is applied to to one of the TOM, fixing the working point of

the MZI at the lowest intensity level μ_2. When μ_1 is required an RF signal is sent to one of the CDM that rapidly changes the relative phase and the intensity at the output of the MZI.

Then the light is sent to a second structure that allows to realize the polarization modulation. The structure has another MZI, similar to the one just described, then both outputs of the MZI are followed by a TOM and ad CDM each before being combined in a 2-dimensional grating coupler (GC2d).The GC2d launches the light coming from the two arms into orthogonal porlazation modes, thus converting the path-encoded information used within the PIC into the polarization-encoded information at the output of the GC2d. Referring to the Bloch sphere, the colatitude θ of the produced polarization state $|\psi\rangle = \cos(\theta/2)|H\rangle + e^{i\varphi}\sin(\theta/2)|V\rangle$ is controlled by acting on the internal MZI, whereas the longitude φ is set by acting on the external phase modulators. Therefore, by voltage biasing the TOMs of the inner MZI the balanced superposition of horizontal and vertical polarization $|+\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ is created. If no RF signal is applied, the output state remains $|+\rangle$, whereas, by applying an RF signal on the external CDMs, a $\pi/2$ phase shift can imposed to either arm, respectively creating the states $|L\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$ or $|R\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$. In this way, we obt eneration basis $\mathbb{Z} = \{|0\rangle, |1\rangle\}$, $-\rangle\}$, with $|\pm\rangle := (|H\rangle \pm |V\rangle)/\sqrt{}$ sented in Fig 8.11

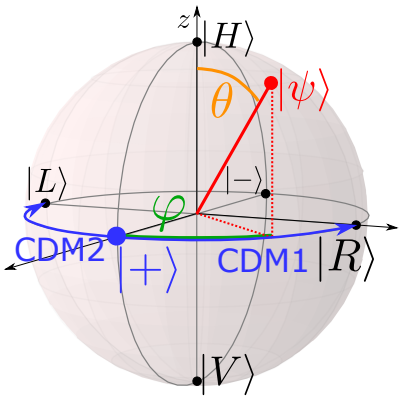


Figure 8.11: *States generated by the PIC source. If no control signal is sent the pivotal $|+\rangle$ state is generated. If the upper CDM is activated, a $\pi/2$ shift is applied to ϕ and $|R\rangle$ is generated. If the lower CDM is activated a $'\pi/2$ shift is applied and $|L\rangle$ is generated.*

Another possible encoding would have required the use of only the internal MZI: if the internal TOM are biased in a way to generate $|+\rangle$ without RF modulation, then by applying a $\pi/2$ modulation to the internal CDMs one can generate $|H\rangle$ and $|V\rangle$. Unfortunately, our PIC were affected by a fabrication issue that limited the 2x2 MMI extinction ratio and prevented us to use this encoding.

The light at the output of GC2d is coupled into one of the 8-channel of the SMF-array and then sent over a standard SMF28 single mode fiber.
The size of the PIC is about 5 mm × 5 mm, while the complete package is compact within a total volume of 1.2 cm × 1.5 cm × 1.2 cm. A picture of the packaged PIC soldered to

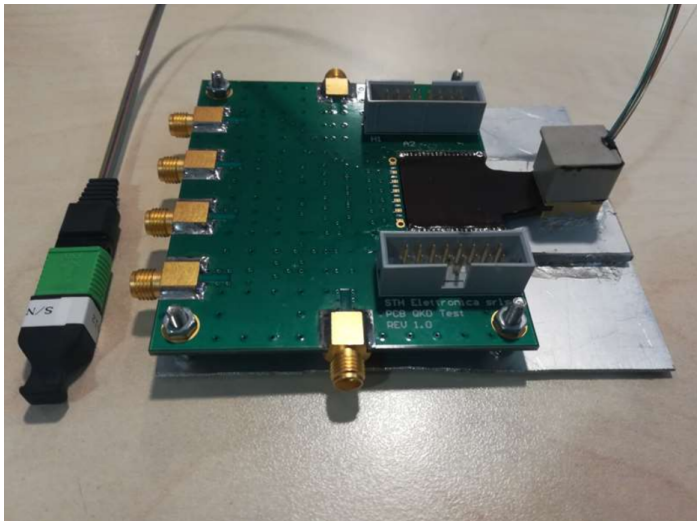


Figure 8.12: *Photo of the PIC assembled on the connectorized RF PBC.*

a standard 7 cm × 8 cm control board is presented in Fig. 8.12. The package has been designed, developed and assembled to the purpose in-house (featuring 20 DC and 6 RF ports), so as to make it rugged, portable and easily usable in field experiments.

Characterization of the PIC

The intensity modulation capability of the PIC has been characterized sending bright laser light into the chip and recording the intensity of the output light with a fast biased photodiode. The CDM in the first MZI were driven by a PRBS generator sending Non Return to Zero (NRZ) modulation at 10 Gbit/s in push-pull mode (i.e. sending the signal in one arm and the negated in the other). The signal of the photodiode has been then recorded by a fast oscilloscope. The results, presented in Fig 8.13, showed an extinction ratio of 10dB at 10Gbps.

We also characterized the modulation at the typical frequencies used in the experiment. The voltage used for the biasing of the TOM was 6.69V, while RF pulses at 100MHz with 2.53V of amplitude and 2ns of width were sent to the CDM. With this configuration we obtain a ratio $\mu_1/\mu_2 = 5.2$ which is often the optimal one for the experimental parameters of our channel.

As anticipated, our PIC were affected by a fabrication issue that limited the 2x2 MMI extinction to 14.7dB. This issue has a big effect on the polarization modulation stage since in this way not all the states on the Bloch sphere can be generated. By sweeping the voltage of the internal and external TOM in the polarization modulation stage and analyzing the output with a polarimeter, it's possible to sample the states on the Bloch sphere. The results, presented in Fig 8.14 clearly show two "holes" in the Bloch sphere

For this reason we were forced to employ the encoding where $|+\rangle, |L\rangle$ and $|R\rangle$ are generated.

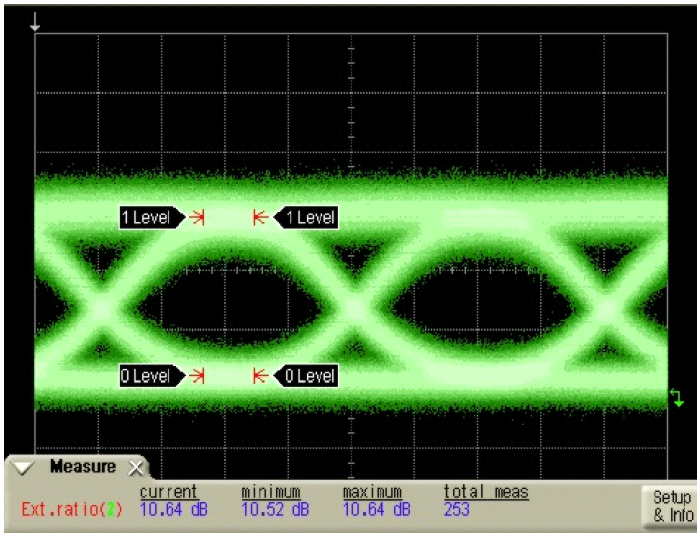


Figure 8.13: *The eye diagram shows an ER of 10dB in the output's optical intensity when the IM is driven with 10Gbps signal*

Finally, we connected the PIC with the laser source described in Sec 8.3.2 and the quantum state analyzer (which measures the polarization of the generated states with a set of SNSPD), in order to evaluate the stability and extinction ratio of the polarization state. The internal TOM was driven with a DC voltage of $2.19V$, while the external CDM were driven with square pulses 5ns wide at 50MHz of repetition rate, with an amplitude of 10.64V and 9.8V .

The results show an extinction ratio up to 25db (or a QBER below 0.3%) and long-term stability of over an hour. The reported QBER is presented in Fig 8.15

8.4 Beacon and PAT

The Pointing, Acquisition and Tracking (PAT) unit consists of the transmitter and receiver telescopes and their respective optical setups. The main goal of the PAT unit is to provide a stable optical link over a turbulent free-space channel.

8.4.1 Optical setup

At the transmitter telescope (Alice), the quantum signal at $1550nm$, a *'power'* beacon at $1545nm$ and a *'pointing'* beacon at $1064nm$ are coupled to a SMF28 single-mode optical fiber via two wavelength-division-multiplexers (WDM). The three beams are collimated at the output of the fiber and magnified to a beam diameter of $120mm$ via a $F_{\#}=7.5$ Galileian telescope. A $635nm$ beacon is also coupled to the beam before magnification via a dichroic mirror (DM), to serve as the coarse-alignment transmitter beacon.

The free-space link is realized over $145m$ in the urban area of the city of Padova in Italy, at a height of about $10m$ above ground. We realized a continuous operation of the QKD

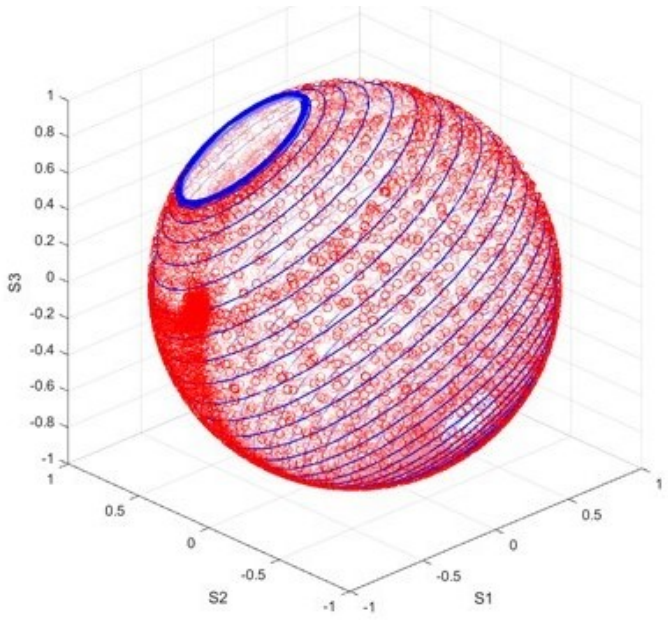


Figure 8.14: *The limited ER of the 2x2 MMI prevents the generation of states close to* $|H\rangle$,$|V\rangle$

system throughout the day (from 11am to 8pm) over several days in the month of April 2019. The coarse geometric alignment over the channel is maintained by a forward loop with the 635nm transmitter beacon and receiver camera, and a backward loop with a 850nm receiver beacon and transmitter camera. An automatic system corrects for low frequency pointing drifts acting on the transmitter telescope mount.

The receiver (Bob), is a 315mm $F_{\#}=15$ Dall-Kirkham telescope. As the receiver is larger than the incoming transmitter beam, the light is coupled off-axis to avoid losses due to the central obstruction. The beam is collimated via an achromatic doublet lens $f_{coll}=75mm$. A fast-steering mirror (FSM - Smaract STT25.4) is placed on the image plane of the entrance pupil which is generated after the collimating lens at a distance approximately equal to f_{coll}. A DM separates the *'pointing'* beacon from the *'power'* beacon and quantum signal. The 1064nm beam is focused by a $f_{PSD}=250mm$ plano-convex lens onto a silicon lateral-effect position-sensitive detector (PSD - On-Trak Photonics 2L4SP) which has an active area of $4mm \times 4mm$ and a resolution of 61nm. The *'power'* beacon and quantum signal pass through a 12nm band-pass filter centered at 1550nm (50% transmission), are coupled to a SMF28 single mode optical fiber, and are eventually separated by a WDM. The quantum signal is sent to the quantum state analyser stage, while the 1545nm beacon power is measured with a photodiode to monitor the fiber-coupling efficiency.

An automatic system manages automatically the alignment and power optimization between the two telescopes. In particular, the software installed both at the receiver and transmitter are able to communicate over Internet and the transmitter's mount is automatically moved with the objective to maximize the optical power received by Bob.

Figure 8.17 shows a photo of the setup during a preliminary field trial.

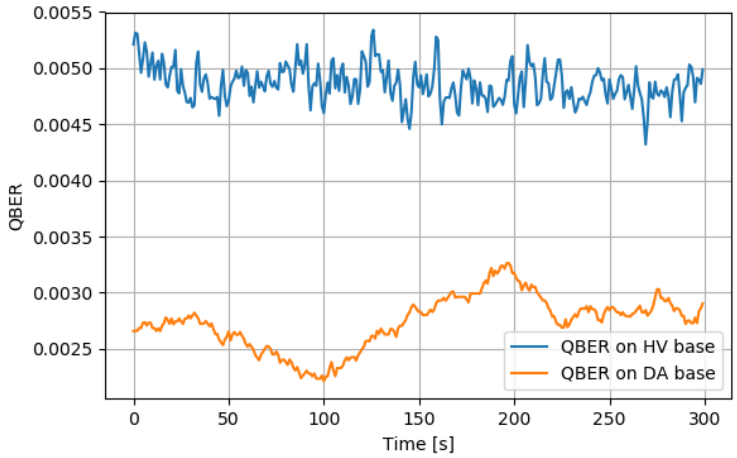


Figure 8.15: *Experimental QBER of the states produced by the PIC source at 50Mhz*

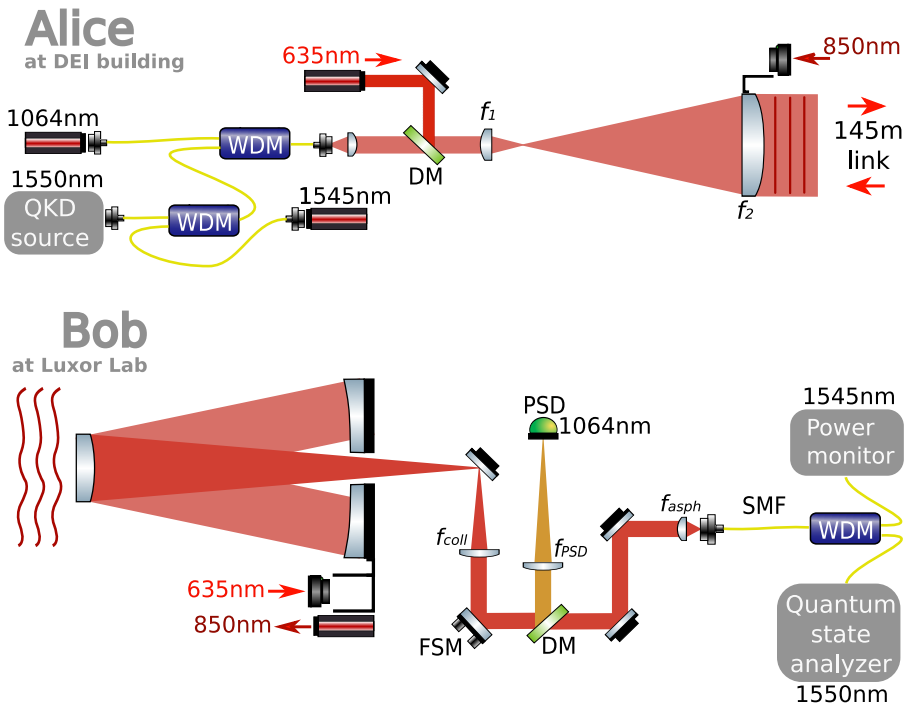


Figure 8.16: *Experimental setup of Alice and Bob terminals.*

8.4.2 Angle-of-Arrival correction system.

The closed-loop Angle-of-Arrival (AoA) correction system is a two-dimensional proportional-integral-derivative (PID) control based on sensing the tip and tilt fluctuations via the X and Y displacement of the centroid of the *'pointing'* beacon on the focal plane at the PSD, and applying a correction with the two-axis FSM.

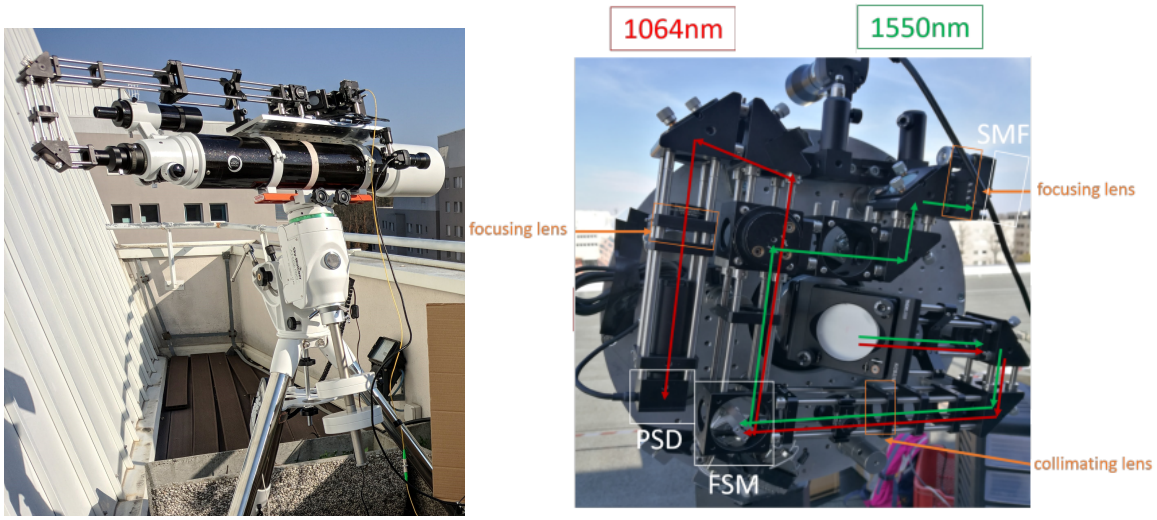


Figure 8.17: *On the left a photo of the transmitter telescope, on the right the optical setup of the receiver telescope*

The current output of the PSD is converted by a trans-impedance amplifier (On-Trak Photonics OT301) and fed to an auto-aligner module (Thorlabs KPA101) which performs a digital PID control on the position error signal. The parameters of the PID were adjusted via software to optimize the stability and minimize the residual error. The $\pm 10V$ analog output of the KPA101 is given to the FSM controller (Smaract AVC) which generates the $100V$ direction and speed driving signals for the piezo-electric actuators of the mirror.

8.4.3 Characterization of the free-space link

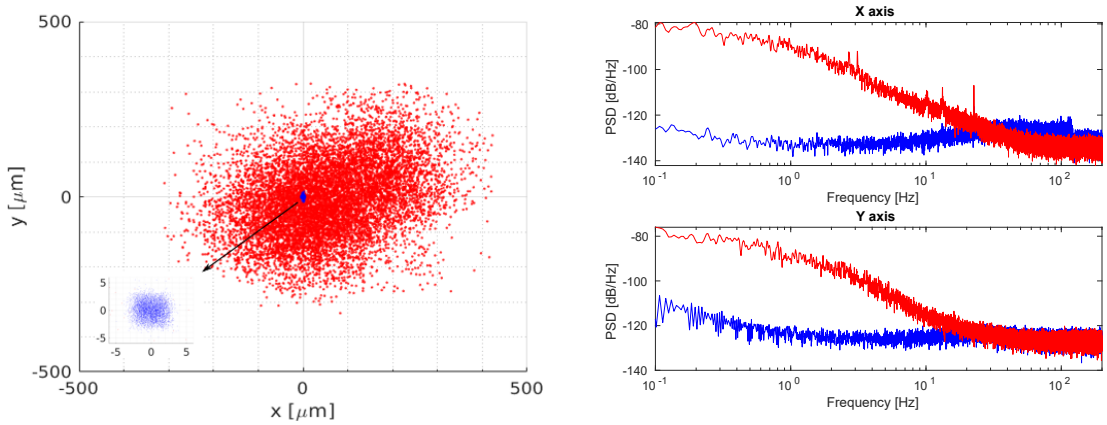


Figure 8.18: *Centroid fluctuation on the PSD (left) and its power spectral density (right). Red, control 'off'. Blue, control 'on'.*

We realised an optical model of the receiver telescope in order to assess the performance

of the feedback system. As shown in Fig.8.18 (left), the RMS of the centroid fluctuation on the PSD without tip/tilt correction is $\mathrm{RMS}_{off} = 150\mu m$, which corresponds to an average AoA fluctuation caused by turbulence of $\alpha_{off} = 10\mu rad$. After activating the feedback, the RMS of the centroid is reduced to $\mathrm{RMS}_{on} < 5\mu m$, which translates into a residual AoA fluctuation of $\alpha_{on} < 0.4\mu rad$. The closed loop bandwidth of the feedback system, $\sim 25Hz$, is enough for compensating most of the spectrum of AoA fluctuations, as shown in Fig.8.18 (right).

In terms of SMF coupling efficiency, the maximum achievable efficiency for our system, excluding turbulence effects, is $\rho_0 = 33.43\%$. From Fig.8.19, we can see that the SMF coupling is robust to AoA fluctuations up to $1\mu rad$. Specifically, we find that without control the coupling efficiency drops to $\rho_{off} = 13.57\%$. While the expected efficiency with active control is instead $\rho_{on} = 33.37\%$, proving the effectiveness of our tip/tilt correction system.

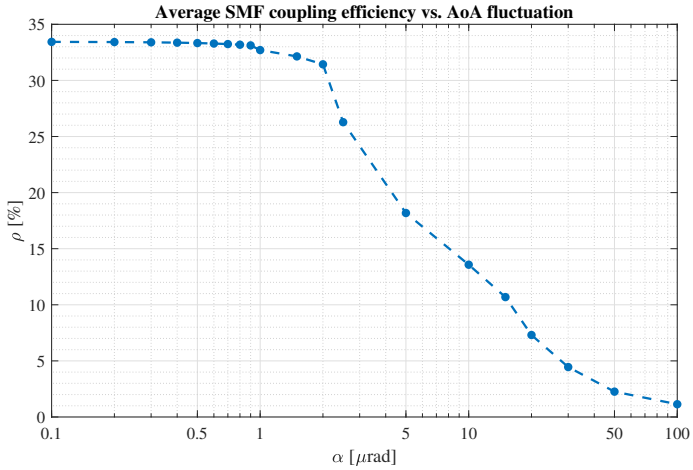


Figure 8.19: *SMF coupling efficiency as a function of the AoA.*

This model only takes into account the effect of the first two orders of turbulence, namely tip and tilt fluctuations. The coupling efficiency observed in the experiment can be fitted to a more advanced model that takes into account the higher order contributions.
The effects of the active control on the coupling efficiency is evident when looking at the coupling efficiency histograms of the *'power'* beacon, as shown in Fig. 8.20, with the mean coupling efficiency increasing from 2.9% with control *'off'* to 9.5% with control *'on'*.

We applied the statistical model described in [215] to analyse the effect of higher order contributions on the coupling efficiency. In particular, we used the probability density function (PDF) of the normalized coupling efficiency (equation (28) of [215]) to fit the histogram of the data taken with the control *'on'*, assuming a Kolmogorov spectrum of the turbulence [216] and setting to zero the statistical variances of Zernike modes associated to tip/tilt fluctuations. We used as fit parameters the Fried coherence length r_0 and the instantaneous coupling efficiency in absence of turbulence ρ_0, that takes into account the static aberrations of the optical system. The choice of fitting the data with control *'on'* is due to the fact that the statistics of data with control *'off'* results from the combined effect of

atmospheric turbulence and mechanical vibrations of the telescopes, which are not included in the model.

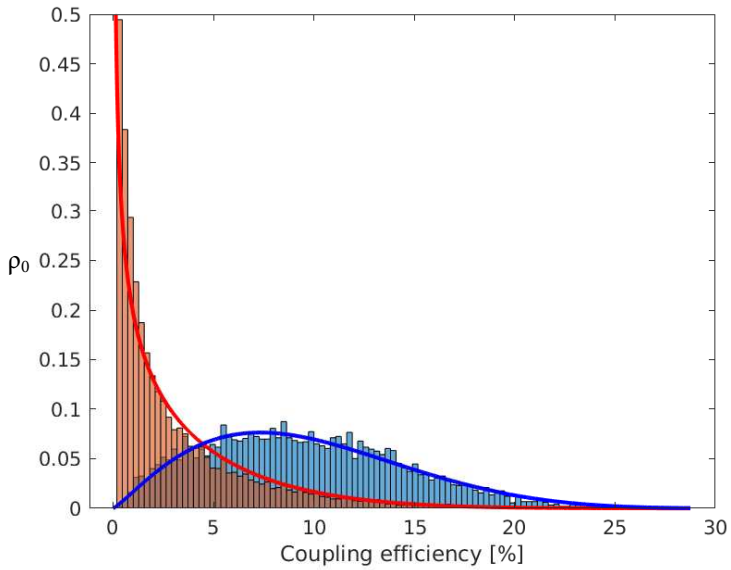


Figure 8.20: *Coupling efficiency histogram with fitting distributions. Red, control 'off'. Blue, control 'on'.*

Fig. 8.20 shows, in blue, the fitting distribution of the data with control *'on'*, characterized by $r_0 = 8.9cm$ and $\rho_0 = 34.3\%$, and, in red, the normalized coupling efficiency without removing tip/tilt fluctuations and using the same parameters r_0 and ρ_0. The value of the parameter ρ_0 is in line with the one calculated from the optical model of the telescope.

This model proved useful also for the characterization of the channel during the operation of the QKD system. However, since the filtering of the *'power'* beacon was not sufficiently strong, it had to be switched off during the key exchange phase to avoid injecting noise into the QKD detection system. Therefore, we applied the model directly to the quantum signal.

We sliced the QKD acquisition into intervals of 1 minute, calculating the coupling efficiency histogram for every interval and fitting it using the same method described above, finding the results shown in Fig. 8.21.

The Fried coherence length r_0 remains stable at about $10cm$ from 14:00 to 17:00, rising to $\sim 30cm$ in the late afternoon, in line with what observed in similar link and climate configurations [217]. The value of ρ_0, on the other hand, is slightly lower than expected. This is probably due to an underestimation of the fixed attenuation term of the quantum channel, taken to be around $10dB$. Further investigations of this aspect will allow a better evaluation of the different losses of the system, proving useful for an overall evaluation of its performance.

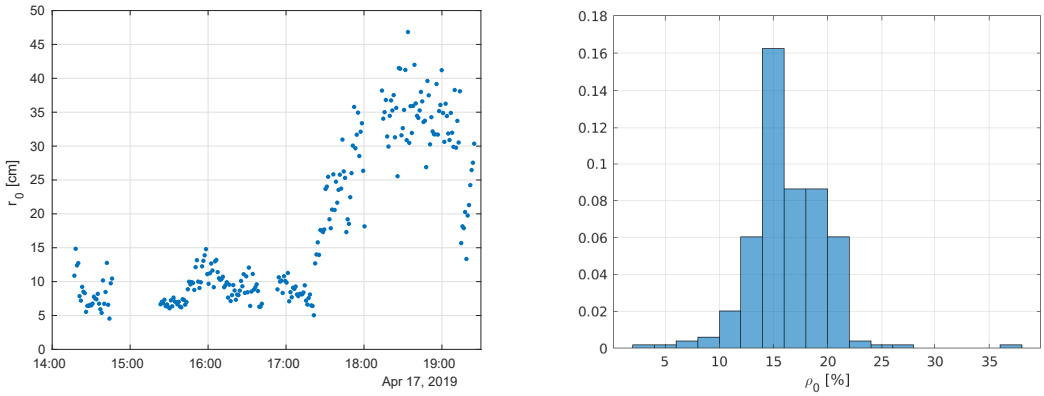


Figure 8.21: *Fitted value of the Fried coherence length r_0 through a day of continuous QKD operation (left) and histogram of the corresponding fitted ρ_0 values (right). The mean value of ρ_0 is* 16.3%.

8.5 The state analyzer

The receiver telescope couples both the 1545nm bright beacon laser and the quantum signal at 1550nm in the same SMF28 fiber. Hence, before measuring the quantum states we need to separate the signal and compensate the unitary rotation of the polarization induced by the single mode fibers, in order to align Alice and Bob polarization reference frames. These tasks, together with the detection and timetagging, are accomplished by the state analyzer, presented in Fig 8.22. The input fiber, carrying the 1545nm beacon (dWDM

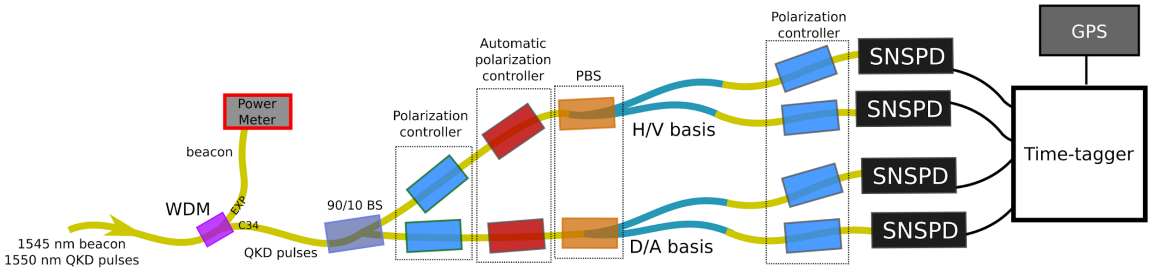


Figure 8.22: *Schematic representation of the passive state analyzer*

channel 40) and the 1550nm quantum signal (dWDM channel 34) are sent to dWDM that reflects input light in a 100GHz window centered around channel 34 in the CH34 port, while transmitting the remaining portion of the spectrum in the EXT port. The dWDM has an extinction ratio of over 100dB for signals that are more than 200GHz apart. The EXP port, that contains the 1545nm beacon is connected to a power meter, in order to check the coupling efficiency of the telescope, while the C34 port of the dWDM is connected to the polarization analyzer. The latter comprises a 10/90 beam splitter (an almost optimal value for the implementation of the efficient-BB84 of Sec. 8.3.1) from which two equal SM fiber-path emerge. Each arm comprises a manual polarization controller (PC), an automatic polarization controller (APC) by General Photonics, and a PBS to perform the projective

polarization measurement. The PC and APC are used to align one arm in the $\mathbb{Z}$ basis and the other in the $\mathbb{X}$ basis. At each output port of the two PBSs is connected a Superconducting Nanowire Single Photon Detector (SNSPD). The SNSPD system is the ID281 made by IdQuantique and is characterized by 4 MoSi SNSPD enclosed in a cryostat, working at 0.8K. The SNSPDs have a free-running dark count rate of $\approx$100Hz, a temporal jitter of $\approx$33ps and a nominal quantum efficiency of 91%, 84%, 83% and 35% for the four channels. Since the quantum efficiency of the SNSPD is maximized for horizontal polarization, a manual polarization controller is needed before each SNSPD. Each photodetection event recorded by the SNSPDs produces a fast electric pulse of ≈ -20mV of amplitude. This is amplified to LVTTL levels by an wideband low-noise inverting RF amplifier and sent to a timetagger (quTAU by quTOOLS) with 81ps of timing resolution. Since the quTAU's clock cannot be externally clocked and does not have a start signal, we tag the PPS signal and a decimated copy of the 10MHz generated by Bob's GPS-disciplined clock, for synchronization purpose.

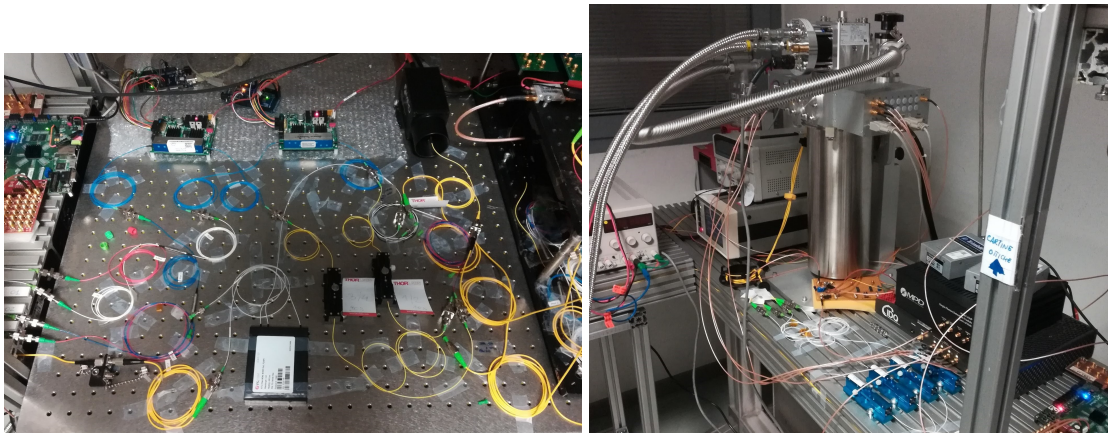


Figure 8.23: *Photo of the actual state analyzer and detector unit*

8.5.1 Alignment software

In order to reduce the efforts needed to align Alice and Bob's polarization reference frames, we have developed a small Python utility to automatically perform the basis alignment. The software's GUI is showed in Fig 8.24

When the alignment procedure is started, the QKD transmitter sends the fixed sequence of qubits $|0\rangle, |1\rangle, |+\rangle, |+\rangle$. On the receiver the timetags from the detectors are acquired for a fixed exposure time and the histograms of the four peaks are showed for each detector. The software identifies the polarization state relative to each peak and calculates the relative extinction ratio. Then the user can select to align the two pairs of detectors Det1,Det2 and Det3,Det4 along the $\mathbb{Z}$ or $\mathbb{X}$ basis. In the case of the first one the software tries to maximize the ER of the $|0\rangle, |1\rangle$ states and balance the ER for the $|+\rangle$, while for $\mathbb{X}$ it does the opposite.

The alignment of the basis is physically done by the automatic polarization controller (APC), located in each measurement arm. The APC features 4 piezoelectric actuators rotated by 45°to each other (see Fig 8.25), that can squeeze the fiber, inducing a localized birefringence that acts as variable waveplate.

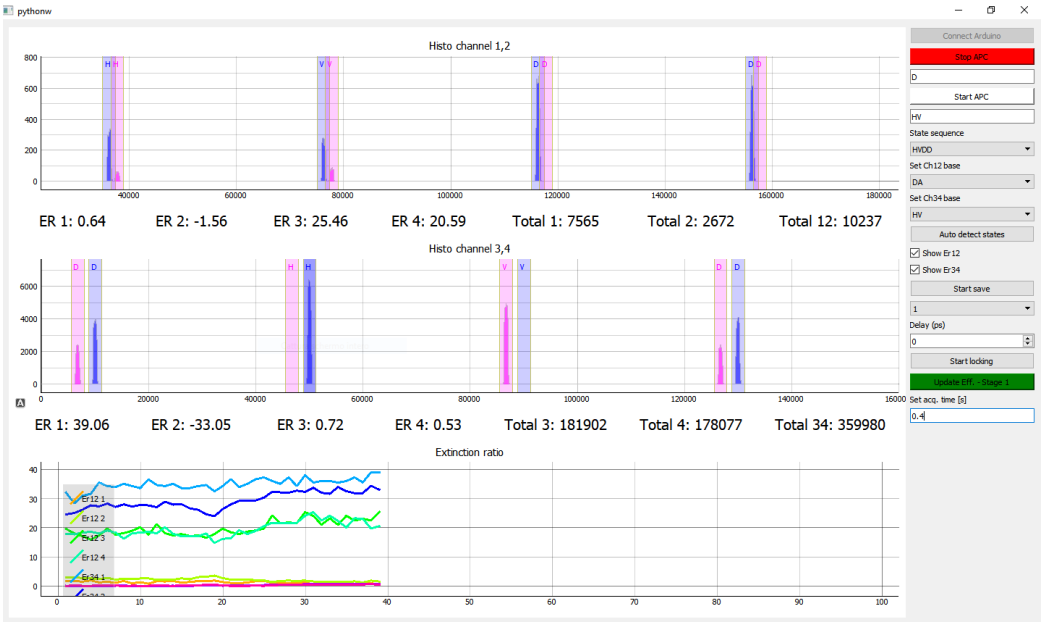


Figure 8.24: *GUI of the alignment software*

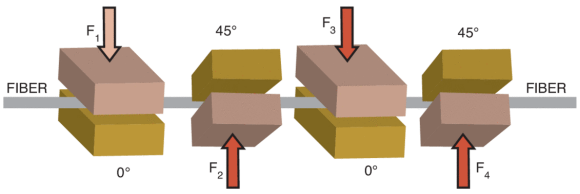


Figure 8.25: *Working principle of the APC [218].*

The amount of squeezing, and so the polarization rotation, can be controlled by a parallel digital interface. In our case, each APC is connected to an independent Arduino via the parallel interface, while the Arduino is connected to the computer where the python program runs via the USB interface.

Each time a new value for the ER is available, the python program sends the value to the Arduino, together with the information regarding which basis should be aligned. The algorithm in the Arduino performs in loop an Hill-Climbing optimization[219]. The APCs in our setup have 4 different piezoelectric 1-D actuators that stress and strain the optical fiber, changing the polarization of the light that traverses the fiber. Our optimization algorithm cycles the 4 actuators sequentially. At each round, the position of an actuator is changed with a step size proportional to the measured QBER. If such change caused a reduction in the measured QBER, our algorithm keeps changing the position of the same actuator in the same direction, always with a step size proportional to the measured QBER. Instead, if an increased QBER is measured, then the algorithm reverses the direction of motion for the actuator. Only one reversal is permitted per round, after which the next actuator is selected and a new round begins.

for a single actuator, moving to the next actuator if no improvement is registered. The

size of the steps for each iteration is adaptively selected, depending on the difference between the actual value and the target value for the objective function.

The loop is interrupted when a target ER (usually 25dB) is obtained.

The same principle can be used to actively align the reference frame while the QKD is running, using the information gained from the parameter estimation and error correction routines. Another option is to use a pre-shared and publicly disclosed string for the enconding of the qubits, interleaved with the normal QKD run. This solution is described in Chap. 10

8.6 GPS Syncronization and FPGA control system

The QKD source and the QKD receiver need to be finely synchronized in order to be able to correctly correlate the string encoded and sent by Alice with Bob's measured data. In our setup a rough synchronization is obtained using two Thunderbolt E-GPS Disciplined Clock by Trimble, one at Alice's side and one in Bob's setup. This device contains an Oven-Controlled Crystal Oscillator (OCXO) disciplined by a GPS in order compensate long term drifts of the oscillator. The device outputs a 10 MHz clock and a Pulse Per Second (PPS) signal. In our tests, the absolute difference between the receiver time and the UTC time from the GPS always remained below 300 ns. The 10MHz signal in Alice's setup is feeded into the FPGA that controls the QKD source (a Xilinx C7Z020FPG) and is used to derive the master clock. In this way any signal coming from the FPGA is synchronized with the GPS. These signals are the laser trigger, the decoy RF modulation, the polarization RF modulation and the gating signal for the MPD SPAD. Also the PPS is recorded by the FPGA and is used as a "start" signal for the entire protocol.

On Bob's side, since the quTAU used cannot be externally clocked and doesn't feature a start signal, we tag the PPS and a decimated copy of the 10MHz signal. This temporal information is used to "re-align" the received tags in post-processing.

An finer synchronization is performed via software and is described in Sec 8.7.1

8.7 Postprocessing

For the real-time implementation of the QKD protocol a classical and authenticated channel between Alice and Bob is needed for the post-processing analysis. We have chosen to develop a dedicated software for the authentication and all the post-processing steps that employs the transmission-control-protocol (TCP) and the internet-protocol (IP) network stack offered by the Linux operating system. In this way the application is agnostic over the physical implementation, that can be a radio bridge, a dedicated optical link or simply a connection to internet. In particular, the software manages the following steps of classical post-processing: control of the sending of the key, reception of the optical signal, synchronization between transmitted and received messages, basis reconciliation, error correction, correction confirmation, parameter estimation and privacy amplification. The output of this pipeline is a secure and identical key shared between the two parties.

Our software is developed from the open-source QKD project from AIT(see [200]), which is released under the GPL and LGPL license. We have chosen to use this as a starting point

because of few key factors:

- Open source
- The software has been already used in many field-tests
- It implements the entire network and interprocess stack
- The code is flexible and modular

The last point is fundamental, since it gives us the possibility to develop and modify only a small portion of the code, the one that needs to be adapted to our protocol, while keeping untouched the core, reducing the development time and the chances of bugs. A graphical representation of the pipeline is showed in Fig. 8.26:

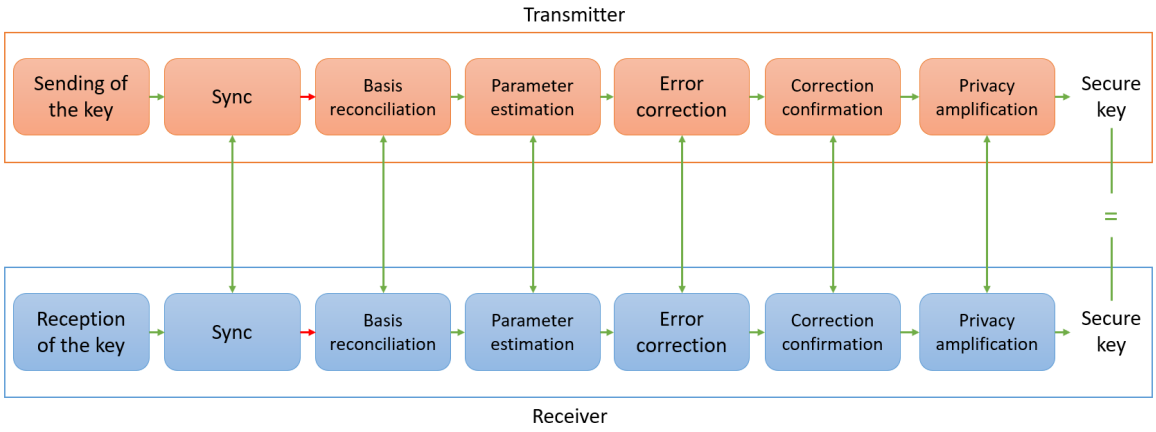


Figure 8.26: *Pipeline of the postprocessing software*

Two instances of this stack run simultaneously, one at the transmitter (Alice) and one at the receiver (Bob), and perform classical communication via internet. The input is the raw key, a binary encoding of the sent or received quantum states, the output is the secret key, which is the same at both sides and completely unknown to eavesdroppers. Parameter estimation is based on the protocol described in 8.3.1, while the error correction is performed by the CASCADE module already present in the AIT libraries.

8.7.1 Fine software synchronization

As discussed in the previous sections, Alice and Bob's terminal are synchronized using GPS-disciplined OCXO. This method can guarantee a difference between the two clocks below 300ns. However, in the analysis of the tags realized by the software at Bob's side, a finer temporal alignment is performed.

The algorithm receives as input the times of all the detected photons and estimates the frequency difference between Alice' and Bob's clocks. In particular, the variation in time of the difference between the measured and expected time of arrival is related to the different clock frequencies. Based on this, the expected times of arrival are recalculated simulating a clock with the same frequency as the one of Alice. As a result, the selected events produce

at Bob' side a string that is correlated to the one of Alice. In order for Bob and Alice to know which detection corresponds to the first photon sent by Alice a cross-correlation is performed between parts of Alice and Bob's strings. Specifically, Bob sends a part of its string to Alice, which perform the cross-correlation. Since the absolute difference between Alice and Bob's clocks is below 300 ns, the mismatch between the two string is at most 30 bits (with repetition rate of 100 MHz), making the cross-correlation not computationally hard.

In Chapter 10 an extended version of this method is described, which allows to "self-synchronize" Alice and Bob without the need of a GPS signal.

8.8 Results of the field trial

Exploiting the setup described in the previous sections, we performed multiple QKD runs during February and April 2019, on several days of clear sky condition. Both the bulk and the integrated QKD source have been tested.

8.8.1 Setting up the experiment

The QKD source and detection units, at Alice's and Bob's side respectively, are linked by a free-space channel established between the Department of Information Engineering (DEI) and the LUXOR Laboratory (LUXOR) (see Fig 8.27). Alice's transmitter telescope is placed at DEI building while Bob's receiving telescope was mounted on a fixed support located at LUXOR.

Figure 8.27: *Aerial view of the link*

After aligning the two telescopes, and reaching a good SMF coupling efficiency, we aligned the two measurement bases using the alignment procedure described in Sec 8.5.1.

Then we adjusted the parameters on Alice's FPGA in order to generate the polarization pulses with basis-probability $p_A^{\mathbb{Z}}=0.9$ and $p_A^{\mathbb{X}}=0.1$ and intensities $\mu_1^{\mathbb{Z}}=0.56$, $\mu_2^{\mathbb{Z}}=0.27$, $\mu_1^{\mathbb{X}}=0.69$, and $\mu_2^{\mathbb{X}}=0.33$ at the aperture of the transmitting telescope, with decoy-probability $p_{\mu_1}=0.7$ and $p_{\mu_2}=0.3$. At the receiver the basis detection ratio is determined by the splitting ratio of the BS: we have $p_B^{\mathbb{Z}}=0.9$ and $p_B^{\mathbb{X}}=0.1$. These working parameters are close to optimal for a total attenuation ranging from 20 to 30 dB, a QBER of the order of 1% and a number of sifted bits $n_{\mathbb{Z}}\gtrsim 10^8$, as we expected in our experiment according to our simulations and Ref. [196]. The random bits used for running the protocol are obtained from the Source-Device-Independent QRNG based on the heterodyne measurement described in Chap. 3.

It is worth noting that the possibility of using different intensity levels for the two bases without losing security (as discussed in Ref. [198]) is particularly interesting for the PIC source, since non ideal CDMs typically incur phase-dependent losses translating into polarization-dependent amplitude levels of the QKD pulses.

8.8.2 Results for the bulk source

We performed various QKD in the first half of March 2019 and here we discuss the four QKD runs performed on March 15th, 2019.

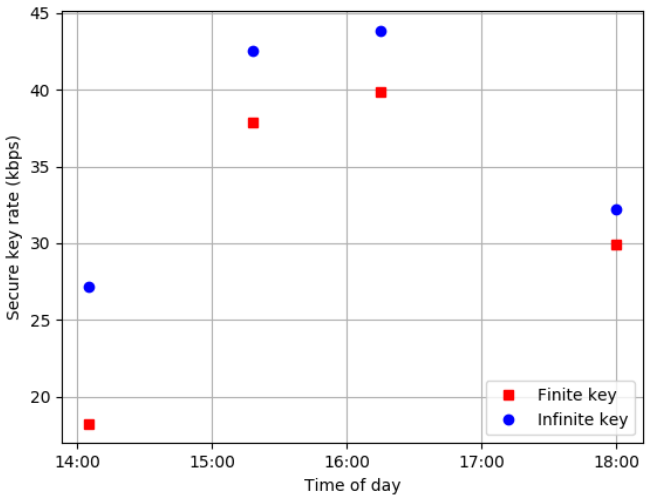


Figure 8.28: *Secret key rates obtained in daylight.*

The mean total detection rate (within a 1 ns detection window around the expected arrival time of the pulses), when renormalized for taking into account the different quantum efficiencies of the SNSPDs, is about 120 kHz. In daylight the background counts due to environmental light vary, ranging from 30 and 230 Hz, and being about 150 Hz on average. Hence, the SNR is about 800, while the total losses are about 22 dB (4 dB due to the free-space channel, 13 dB due to the SMF coupling efficiency and 5 dB of fixed attenuation in the state analyzer). The measured losses are compatible with the losses expected in such a

link, ranging from 20 to 30 dB.

On average in the four QKD runs, each lasting for about 1 hour from 2:00 to 6:00 p.m., we obtained a quantum-bit-error-rate of about 2.2% and 0.8% in the Z and X basis, respectively. By applying the finite-key analysis to raw-key bit blocks of mean size $n_Z^{\mathrm{EC}} = 10^8$, we finally obtained a mean secret generation rate of 33.8 kbps, with two runs exceeding 37 kbps. This mean value becomes 37.5 kbps if we neglect finite-key corrections. The final results for the different QKD runs are presented in Fig. 8.28.

It is worth noticing that the presented results are the best we obtained in one afternoon of data acquisition, where we optimized the losses in the state analyzer. However, we managed to obtain a secret key rate of about 1 kbps also around noon and earlier in the mornings of previous days, demonstrating that daylight QKD at 1550 nm is feasible with our QCosone prototype. Unfortunately, data acquisition on 15th march failed from 10:00 a.m. to 1 p.m. due to a temporary overheating of the SNSPDS.

8.8.3 Results for the PIC source

On April 18th we managed to perform the QKD experiment continuously for eight hours of daylight, as shown in Fig. 8.29.

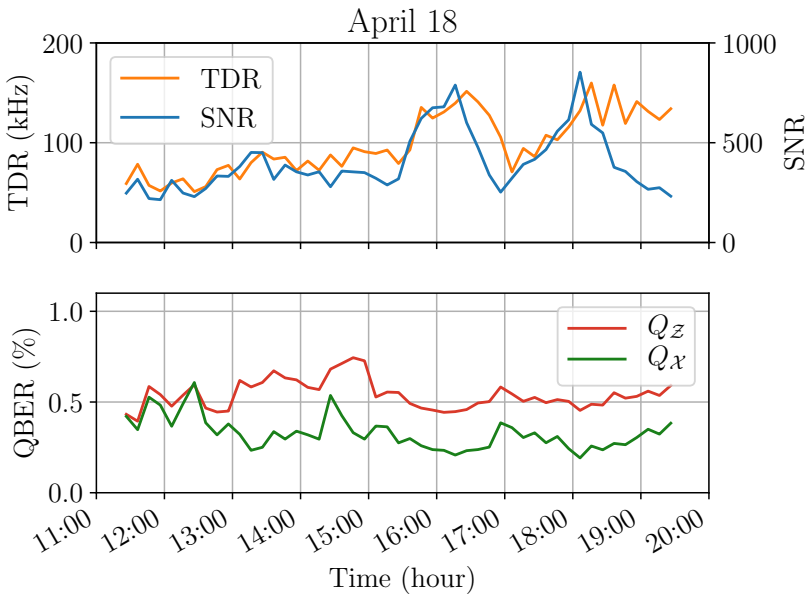


Figure 8.29: *TDR, SNR and QBER obtained on April 18th, 2019.*

The total detection rate (TDR, orange line) within a 1ns-wide detection window around the expected arrival time of the pulses (when renormalized taking into account the different quantum efficiencies of the SNSPDs) ranges from 60 to 130 kHz, being around 100 kHz on average. As expected, in our experiment the SMF coupling efficiency and hence the TDR increased approaching the late afternoon, thanks to the reduced turbulence due to the weaker temperature gradient. In daylight, the background rate within the detection window

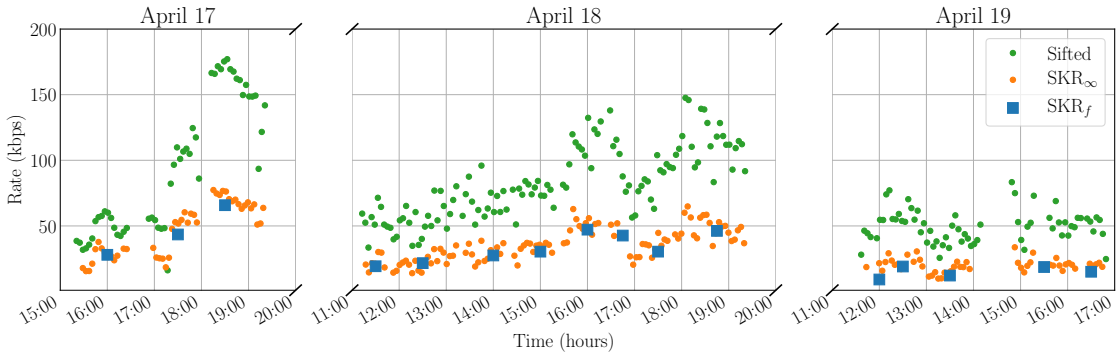


Figure 8.30: *Results obtained in daylight during three consecutive days of QKD runs. The maximum Sun elevation was about 55° at 13:00; sunset was around 20:00.*

due to environmental light varies, ranging from 200 to 400 Hz and being about 240 Hz on average. Hence, the signal-to-noise ratio (SNR, blue line) is about 400, while the total losses are around 24 dB on average (5 dB of fixed attenuation due to the optics of the receiver, 5 dB of fixed attenuation in the state analyzer and 14 dB due to the mean SMF coupling efficiency). The drop of the SNR after 18:30 is due to the fact that the receiving telescope was facing toward the sunset, hence increasing the background rate.

We notice that, by narrowing the detection window, the SNR increases (at the expense of a lower sifted rate). In our case, by reducing the detection window to 500 ps, the detection rate decreases by 25%, while the noise is reduced by 50%. For low SNR values, the above strategy may result in a higher key rate [220]. With the reduced detection window, the simulation of the post-processing procedure provides that our setup would be able to produce a secret key even with 14 dB of additional losses (if only beam-diffraction is considered such losses would correspond to a link distance of about 50 km).

The measured QBER is less than 0.75% for all of the eight hours without the use of any active polarization stabilization system, reaching a value as low as $Q_{\mathbb{Z}} \approx 0.45\%$ in the $\mathbb{Z}$ basis and $Q_{\mathbb{X}} \approx 0.25\%$ in the $\mathbb{X}$ basis.

In Fig. 8.30 we report the results of the different QKD runs performed over three consecutive days. The weather conditions were good on all of the three days, with a clear and sunny sky. The Sun reached its maximum elevation (55°) around 13:00 and the sunset was around 20:00. Each QKD run lasted for the time needed to guarantee that the requirement $n_{\mathbb{Z}} \gtrsim 10^8$ was fulfilled. As we showed in Fig. 8.29, the TDR increased during the day, thus making the effective duration of the QKD runs vary, typically from 15 to 55 minutes.

Each graph in Fig. 8.30 shows the rate of the sifted bits $n_{\mathbb{Z}}$ (green dots), the asymptotic (infinite-size) SKR (SKR$_\infty$, orange dots) and the finite-size SKR (SKR$_f$, blue squares) as a function of the hour of the day. Each dot is obtained by an average over four minutes of data acquisition by merging all the runs, while each SKR$_f$ point is obtained with a single QKD run. The obtained results are comparable over the three days. The sifted bit rate ranges from 50 to 150 kbps, depending essentially on the TDR, hence showing an improvement while approaching the late afternoon. The same trend characterizes also the SKR$_\infty$, which ranges from 20 to 70 kbps. We manged to obtain a SKR$_f$ of several tens of kbps for all days,

reaching a maximum of 65.8 kbps in the last acquisition of April 17th. Remarkably, each QKD run performed on April 18th lasted for about 50 minutes, allowing to obtain a mean SKR_f about 33 kbps, hence outperforming the results obtained with comparable free-space QKD system at 1550 nm by two orders of magnitude [188, 189].

It is worth noticing that a complete QKD experiment in free-space has never before been performed with the Sun at its maximum elevation. Indeed, Gong *et al.* in [189] tried to perform QKD for the whole daytime in a 8km-long link in Shanghai, but the impracticable turbulence conditions and the sunlight background did not allow them to extract a key at around noon. We demonstrated that performing daylight QKD in the middle of the day (around 13:00 in our case) is possible, obtaining a SKR of tens of kbps even in such a condition in two different days.

This is the best result to date for a free-space QKD system operating in daylight [184–189], with performances comparable to fiber-based systems [177, 179]. This result demonstrates that the developed chip encoder is characterized by an excellent polarization stability over time. This feature makes silicon-photonics PICs very attractive in the context of polarization-based satellite QC.

8.9 Conclusions

In this chapter we have presented a complete prototype for polarization-based daylight free-space QKD at 1550nm. We have realized two different QKD transmitters based on commercial fiber-optic components and integrated photonics in silicon. Then we have developed a fast fiber injection system, capable of maintaining the coupling of the signal from the receiver telescope to a single mode fiber, in turbulent conditions. Thanks to the single mode coupling we could exploit efficient, fast and low-noise SNSPD for the detection of the quantum signal.

We performed several QKD runs with both sources, obtaining an extremely low QBER ($\sim$0.5%) and a SKR of several tens of kbps, also with the Sun at its maximum elevation. We overcame the strong background noise coming from the Sun light by exploiting temporal (i.e., synchronization), spatial (i.e., single mode fibers) and wavelength (i.e, dense WDM) filters. To our knowledge, this is the first time that intensity and polarization modulations are realized in a single chip used as qubit encoder for decoy-state QKD, as well the first time that such integrated technology is used in a real free-space QKD-trial in an urban area, thanks to the dedicated packaging designed and realized to the purpose.

In particular, the PIC offered an higher stability and lower QBER if compared to the fiber solution, making it very attractive for the design and development of optical payloads to be placed in portable terminals or satellites dedicated to QC, given the low resources needed in terms of power, weight and space.

Further improvements to our prototype can be achieved by increasing the system clock rate, for example up to 1 GHz (as in Refs. [166, 179, 191, 192]), and exploiting adaptive optics to increase the SMF coupling efficiency [221] and thus the tolerable losses and achievable link distance. However, the obtained results show that daylight QKD technology is mature enough to foresee the real application of a global scale QC-network in the next future [182, 183]. It will likely comprise free-space, satellite and fiber-based channels

exploiting quantum technologies to accomplish tasks such as QKD, realizable also in the device- or measurement-device independent framework [222, 223], entanglement distribution [224], quantum teleportation [225] and quantum time distribution [226], as envisaged by the Italian Quantum Backbone [227], a fiber-based infrastructure connecting the National Institute of Metrological Research in Turin with the ASI Space Center in Matera.

CHAPTER 9

POGNAC: A self-compensating polarization-based QKD transmitter

Widespread effort have been made to simplify the requirements of QKD systems and to enhance the stability of the practical implementations. Recently, for example, a 3 state and 1 decoy state version of the BB84 protocol [150] has been proposed [204], and demonstrated to be secure [228, 229], notably simplifying the requirements of the quantum state encoder and increasing the performances in the finite-key regime. Likewise, a stable intensity modulator for decoy-state preparation [202], as well as a stable phase modulator for time-bin encoding [230] have been demonstrated at repetition rates above GHz, both based on Sagnac interferometric configurations.

Despite polarization encoding being the predilected choice for free-space and satellite-based QKD experiments, few steps have been made to develop a simple and stable polarization state encoder. The use of inline Lithium Niobate ($LiNbO_3$) modulators has been an adopted solution [203, 204], where the birefringence of the crystal is controlled by an external RF field. The applied voltage changes the index of refraction of both polarization modes differently, introducing a relative phase between each polarization, thereby modulating the polarization state. However, high $\widetilde{V}_\pi$ voltage are needed to introduce a relative π shift between orthogonal polarizations, usually a factor 1.5 higher when compared to V_π of standard phase modulators. Moreover, the stability of this inline configuration is critical, as the temperature variations caused by the environment or by the heating due to the RF internal power induce drift in the resulting polarization state.

To address this problem, a double-pass self-compensating configuration with a Faraday Mirror has been proposed in [205], which significantly improved long term stability. However, this approach has important drawbacks such as the use of non standard products (the polarization maintaining (PM) fiber has to be oriented at 45° with respect to the optical axis of the $LiNbO_3$ crystal), high $\widetilde{V}_\pi$ voltages, the required use of high birefringence fibers to compensate for polarization mode dispersion and the need of Titanium-Diffused $LiNbO_3$ modulators able to guide two orthogonal polarizations that are hardly available at wavelength outside the C band. Moreover, any misalignment of the PM fiber with respect to the optical axis of the $LiNbO_3$ crystal will impact the possibility to generate orthogonal states.

Another approach is the use of four independent lasers which are then combined with polarization beamsplitters (PBSs), polarization controllers (PCs) and a beamsplitter (BS) [173, 188, 231, 232]. This approach, surely simplifies the electronic control of the QKD transmitter, but is expensive and power inefficient since it requires four times as many lasers, laser current drivers and temperature controllers. Furthermore, the use of independent lasers could could open side-channels that undermine the security of the implementation in the presence of an eavesdropper. In fact, differences in the temporal shapes and frequency spectrum of the independent laser pulses could be exploited to infer the polarization state without requiring a direct measurement [203].

In this chapter we describe the POGNAC, a polarization modulator based on a $LiNbO_3$ phase modulator inside a Sagnac interferometer. We implement and test it by using standard off-the-shelf telecommunication components. Our polarization modulator exhibits high degree of simplicity and stability, low intrinsic quantum bit error rate (QBER), and can be implemented for operation on both the 800 nm band and the 1550 nm band, rendering it compatible with free-space, optical fiber and satellite-based QKD.

Some contents of this chapter are part of our work [3].

9.1 Working principle

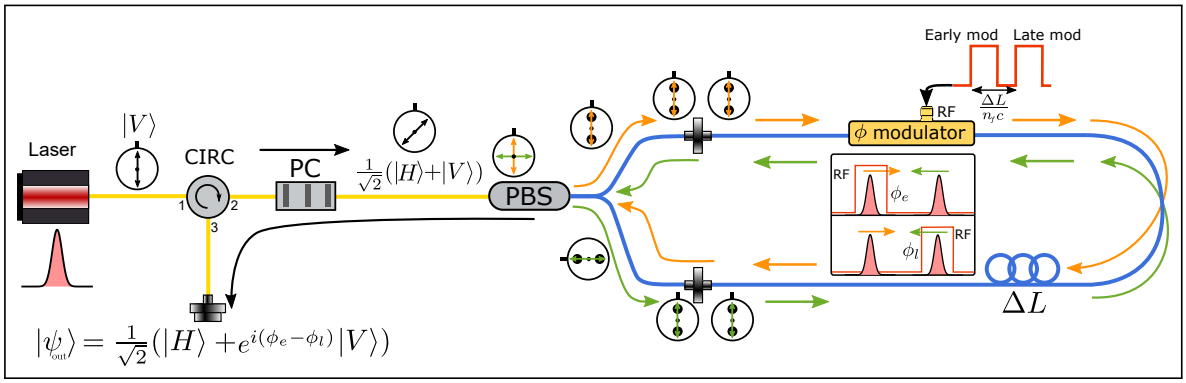


Figure 9.1: *Schematic representation of the working principle of the POGNAC. SM fibers are drawn in yellow while PM fibers in blue.*

Our proposed polarization modulator based on a Sagnac interferometer (POGNAC) can be seen in Fig. 9.1. A linearly polarized laser pulse enters the optical circulator (CIRC) in port 1 and exits in port 2. A PC is then encountered which transforms the polarization state into $|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i\varphi_0}|V\rangle)$, a balanced superposition of horizontal and vertical polarization with arbitrary relative phase, i.e. any state on the equator of the Bloch sphere with $|H\rangle$ ($|V\rangle$) at the north (south) pole. The light is split into orthogonal linear polarizations by a fiber PBS. It is important to note that each of the polarized beams exiting from the PBS is aligned to the slow axis of a PM fiber. This effectively maps the polarization degree of freedom onto the optical path of the photons, with the polarized light traveling only along the slow axis

of the PM fibers of both PBS exit ports. This is the standard behavior of COTS fiber-based PBSs.

This PBS marks the beginning of the Sagnac interferometer, fully implemented with PM fibers. The vertically polarized component travels in the clockwise direction (CW) while the horizontally polarized component travels in the counter-clockwise direction (CCW). In the CW direction a $LiNbO_3$ phase modulator is first encountered introducing a phase ϕ_e to the light pulse. A PM fiber delay line is then encountered, after which the CW light pulse impinges once again on the PBS. The CW propagating light exits the Sagnac interferometer with horizontal polarization. In the reverse direction, the CCW first encounters the PM fiber delay line. Then, the $LiNbO_3$ phase modulator which introduces a phase ϕ_ℓ to the CCW propagating light pulse. Lastly, the CCW light pulse impinges once again on the PBS, exiting the Sagnac interferometer with vertical polarization.

Since inside the PM fiber Sagnac interferometer, both the CW and CCW travel along the fast axis of the PM fiber, no polarization mode dispersion is observed and a single polarization mode propagates in the phase modulator. This ensures that both CW and CCW pulses exit the Sagnac interferometer at the same time, perfectly recombining the two orthogonal polarization states after the PBS. The emerging polarization state is thus given by

$$\left|\psi_{\text{out}}^{\phi_e,\phi_\ell}\right\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{i(\phi_e-\phi_\ell-\varphi_0)}\,|V\rangle\right). \tag{9.1}$$

Since the polarization state depends only on the phase difference $\phi_e - \phi_\ell$, any phase drift that introduces a common phase to both counter-propagating pulses is self-compensated, making the design immune to thermal and bias drifts.

Considering that the CW pulse anticipates the arrival of the CCW pulse on the $LiNbO_3$ crystal by a factor $\frac{\Delta L}{n_f c}$ (where n_f is the index of refraction of the PM fibre and c the velocity of light), by carefully timing the applied voltage on the phase modulator, the polarization state $|\psi_{\text{out}}\rangle$ can be modulated. For sake of simplicity, lets suppose that $\varphi_0 = 0$. If no voltage (or equal voltage) is applied to the CW and CCW pulses, the polarization state remains unchanged, i.e.

$$\left|\psi_{\text{out}}^{0,0}\right\rangle = |D\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right). \tag{9.2}$$

Instead, if $V_{\pi/2}$ voltage is applied to the CW pulse and no voltage is applied to the CCW pulse, the output state becomes

$$\left|\psi_{\text{out}}^{\frac{\pi}{2},0}\right\rangle = |L\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + i\,|V\rangle\right). \tag{9.3}$$

Alternatively, if no voltage is applied to the CW pulse and $V_{\pi/2}$ voltage is applied to the CCW pulse

$$\left|\psi_{\text{out}}^{0,\frac{\pi}{2}}\right\rangle = |R\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - i\,|V\rangle\right). \tag{9.4}$$

Finally, if V_π is applied to the CW (or CCW pulse), and no voltage is applied to the other, the output state becomes

$$\left|\psi_{\text{out}}^{\pi,0}\right\rangle = |A\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - |V\rangle\right). \tag{9.5}$$

The modulated light pulses then exit through port 3 of the CIRC.

By noting that $\{|D\rangle, |A\rangle\}$ and $\{|L\rangle, |R\rangle\}$ form two mutually unbiased basis (MUBs), we can conclude that our proposed polarization modulator can generate the necessary polarization states to perform the standard BB84 QKD protocol [150]. We note that when $\varphi_0 \neq 0$ the same scheme allows the generation of two MUBs lying on the equator of the Bloch sphere. Furthermore, by choosing $\{|L\rangle, |R\rangle\}$ as the key generation states and $|D\rangle$ as the control state, the simplified 3 polarization state version of BB84 [204] can be implemented requiring only two voltage levels, i.e 0 and $V_{\pi/2}$, and fine positioning of the RF electrical pulse which can be done using digital outputs of a Field Programmable Gate Array (FPGA). It can be useful to note that the four polarization states can also be generating by applying 4 different voltage levels, i. e. zero, $V_{\pi/2}$, V_{π} and $V_{3\pi/2}$, only to the CW or CCW pulse, always applying zero voltage to the other.

9.2 Experimental implementations

We used a World Star Tech laser diode emitting light at 850 nm and an Hewlett-Packard 8013B pulse generator (PG) to generate laser pulses with 1.2ns FWHM duration and 100 kHz repetition rate due to laser source limitation. The light pulses first traversed a Glan-Thompson Polarizer, and was then coupled into a single mode (SM) fiber. In our implementation, the CIRC was replaced with a 50:50 BS. This replacement introduced additional 6dB of losses which did not represent a problem since the light pulses were attenuated to the single photon level after the polarization modulator. A PC then transformed the polarization state into $|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i\varphi_0}|V\rangle)$. The light pulses then impinged a fiber based PBS. A $\Delta L = 1$m PM fiber was used as the delay line inside the Sagnac interferometer. The RF signal used to drive the $LiNbO_3$ phase modulator were generated by an Avnet Zedboard FPGA board which was triggered by the PG. The FPGA generated squared pulses with 3ns duration that could be arbitrarily delayed with respect to the trigger pulses with approximately 100ps precision. This allowed us to send an electrical pulse that modulated either the CW propagating or the CCW propagating pulse, or not to send any electrical pulse according to a previously established pseudorandom sequence. The electrical pulses were then amplified to $V_{\pi/2}$ by an RF amplifier and then sent to the phase modulator. In this manner we simulated the polarization state transmission required by the simplified version of BB84 [204]. To test the generation of the $|A\rangle$ state, we replaced the FPGA with the Agilent 33521A arbitrary function generator that produced electrical pulses with 20ns duration, allowing us to generate a $|D\rangle$, $|A\rangle$ sequence. This replacement was necessary to reach V_{π} necessary to obtain the $|A\rangle$ state.

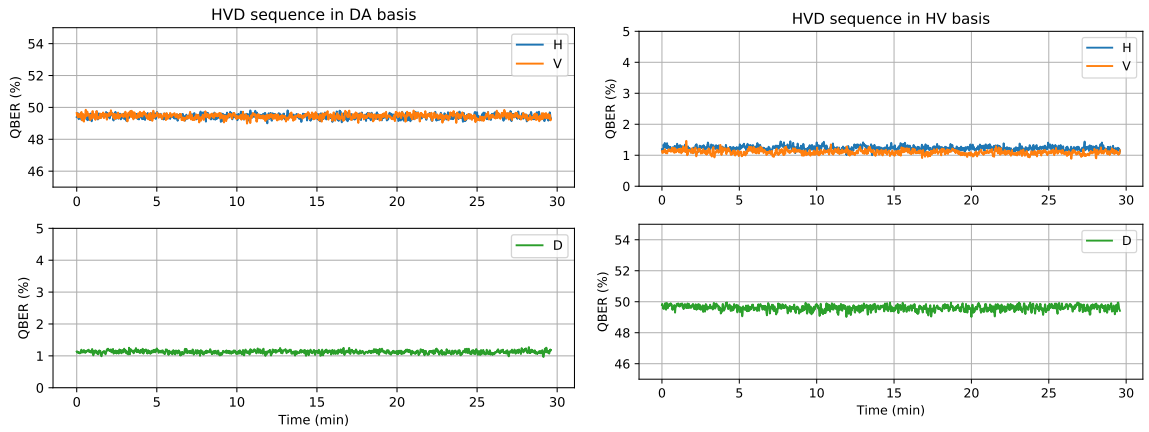
The light exited the polarization modulator through the 50:50 BS and then encountered an Optical Attenuator (OA) that attenuated to the single photon level. Then, anoter PC (not shown in Fig. 9.1) compensated the unitary transformation due to the SM fibers outside the POGNAC and transformed the generated states into $|H\rangle$, $|V\rangle$, $|D\rangle$ and $|A\rangle$. The light pulses were then launched into free-space using a fiber collimator. A free-space polarization analyzer was then used to evaluate the performances of the polarization modulator. The analyzer was composed by a half-wave plate (HWP) and a PBS. This allowed us to measure in the $\{|H\rangle, |V\rangle\}$ or in the $\{|D\rangle, |A\rangle\}$ basis by simply rotating the HWP. The single photon detection was performed using Excelitas SPCM-AQRH single-photon avalanche diode and

the quTAU timetagger. A computer was then used to analyze the results.

9.3 Results

The pseudorandom $\{|H\rangle, |V\rangle, |D\rangle\}$ sequence was continuously sent by our polarization encoder and measured by the free-space polarization analyzer in the $\{|H\rangle, |V\rangle\}$ basis. Every three seconds, the QBER was calculated. The results can be seen in the left panel of Figure 9.2. An average QBER of $1.23 \pm 0.07\%$ was measured for $|H\rangle$ and $1.10 \pm 0.07\%$ for $|V\rangle$. Instead, for $|D\rangle$ a $49.6 \pm 0.2\%$ QBER was measured, as expected for a MUB state.

After approximately 30 minutes, the HWP of the free-space polarization analyzer was rotated to measure in the $\{|D\rangle, |A\rangle\}$ basis, without modifying the polarization encoder. As before, every three seconds, the QBER was calculated. The results can be seen in the right panel of Figure 9.2. An average QBER of $1.12 \pm 0.04\%$ was measured for $|D\rangle$. Instead, for $|H\rangle$ and $|V\rangle$ a $49.4 \pm 0.1\%$ QBER was measured, as expected for MUB states.



(a) **(b)**

Figure 9.2: *QBER as a function of time for the pseudorandom* $\{|H\rangle, |V\rangle, |D\rangle\}$ *sequence* ($V_{\pi/2}$ *modulation) measured in: a) the* $\{|D\rangle, |A\rangle\}$ *basis, b) the* $\{|H\rangle, |V\rangle\}$ *basis*

Similarly, to test the generation of the $|A\rangle$ state, a $\{|D\rangle, |A\rangle\}$ sequence was sent and the HWP of the free-space polarization analyzer was rotated to measure in the $\{|D\rangle, |A\rangle\}$ basis. As before, every three seconds, the QBER was calculated. The results can be seen in figure 9.3. An average QBER of $0.20 \pm 0.02\%$ was measured for $|A\rangle$ and $0.13 \pm 0.01\%$ for $|D\rangle$.The lower QBER in this configuration can be attributed to the cleaner electrical RF pulses generated by the function generator respect to the ones generated by the FPGA.

Since no active polarization compensation was present in any case, the results shown in Fig. 9.2 - 9.3 demonstrate the high stability of the POGNAC and the low intrinsic QBER.

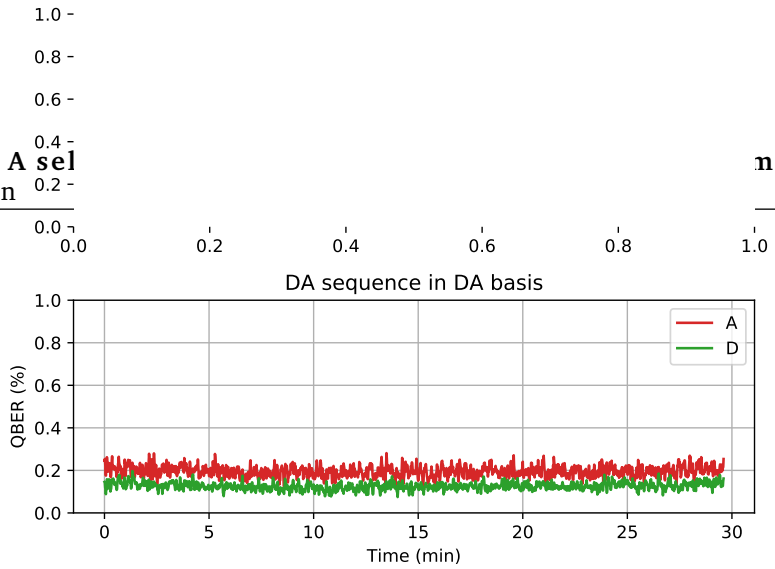


Figure 9.3: *QBER as a function of time for the* $\{|D\rangle, |A\rangle\}$ *sequence (*V_π *modulation) measured in the* $\{|D\rangle, |A\rangle\}$ *basis.*

9.4 Conclusion

In this Chapter we have proposed and experimentally tested the POGNAC, a novel polarization encoder system for free-space, fiber and satellite QKD. Compared to the previously proposed solutions our approach offers several key advantages. The self-compensating Sagnac-loop design greatly improves long-term stability over inline implementations [203–205], making it insensible to temperature fluctuations and DC drifts.

Compared to the previously proposed autocompensating solution in [205] the POGNAC doesn't need custom phase modulator. In fact in the Sagnac loop only one polarization is guided and standard Proton-Exchange Phase Modulators (PE-PM) can be used. The Faraday Mirror solution instead requires Titanium-diffused phase modulators (TD-PM) that are able to support both polarizations. TD-PM are commercially available from few manufacturers, while PE-PM are standard telecom devices available at different wavelength, included the 800 nm band, relevant for free space QKD.

Moreover, the modulation voltages required by our solution are considerably lower than previous proposals. In the POGNAC the phase modulation is directly converted in a polarization modulation. Instead in [203–205] the applied voltage changes the index of refraction of both polarization modes differently, introducing a relative phase between each polarization, thereby modulating the polarization state. Usually, these implementation require a V_π 1.5 times higher than our proposal.

Our experimental results show that low QBER can be obtained stably overtime without the need of an additional feedback system, greatly simplifying the design of a polarization QKD source. Such simplicity renders our source suitable for CubeSat missions, where a small footprint and low energy consumption are of critical importance [233]. Furthermore, the temporal stability of the source attests the compatibility with QKD links with satellites even in Middle Earth Orbit [234], or part of a Global Navigation Satellite Systems [235], where visibility times between the ground station and satellite can exceed the hour.

Lastly, the configuration based on a Sagnac interferometer could allow for high repetition rates, up to few GHz, as recently demonstrated with an intensity modulator for decoy-state preparation [202], as well as a stable phase modulator for time-bin encoding [230].

CHAPTER 10

Self-synchronized and self-compensated QKD with a POGNAC state encoder

A critical aspect that needs to be taken into account in a QKD system is the distribution of a temporal reference between the transmitter (Alice) and the receiver (Bob). This is crucial for at least two reasons: first, it allows to discriminate between the quantum signal and the noise introduced by either the quantum channel or detector defects. Secondly, it allows to correlate the qubit sequence transmitted by Alice with the detection events recorded by Bob. This correlation then enables the distillation of the quantum secure cryptographic key. The transmission of the temporal reference is usually achieved by optically sending a decimated version of Alice's clock. This requires the use of a secondary fibre channel [236], or complex time or wavelength multiplexing schemes to separate the quantum information from the classical light pulses [173]. Also, as shown in Sec. 8.6, Global Navigation Satellite Systems (GNSS) can be used to synchronize Alice and Bob since these systems can give precise temporal references [2, 220]. All these approaches, however, add complexity to the QKD implementations.

Another aspect to take into account when the polarization encoding is used in fiber optical links is the natural birefringence of fiber, which causes the polarization state of transmitted photons to change continuously and in an unpredictable fashion [237]. Several approaches have been conceived to counteract these random polarization drifts, most of them requiring auxiliary laser pulses and complex time or wavelength multiplexing schemes [238], which add unwanted complexity to the QKD setups. A different approach was introduced by Ding *et al.* that used the reveled sifted key [239], produced during the error correction and privacy amplification procedures, to detect and compensate the polarization drifts of the fiber link.

In this chapter we describe a new method to perform temporal synchronization without the need of auxiliary time reference, by sending a shared public qubit sequence at pre-established times.The shared sequences are also exploited to monitor and compensate the polarization drift introduced by the of optical fiber link, with an approach somewhat similar

to the work of Ding *et al.* [239]

These methods have been tested using a simple setup that exploits polarization encoding over a 26 km fiber-optical link, using the simplified three-state and 1-decoy protocol described in Sec 8.3.1. The QKD source employs the POGNAC polarization modulator described in Chap 9, which exhibits high stability and a low intrinsic Quantum Bit Error Rate (QBER) [3]. The reduced complexity of both the transmitter and the receiver, as well as the robustness and stability demonstrated by our implementation, represents and important step towards technological mature and commercial-ready QKD systems.

Some contents of this chapter are part of our work [4, 5].

10.1 Setup

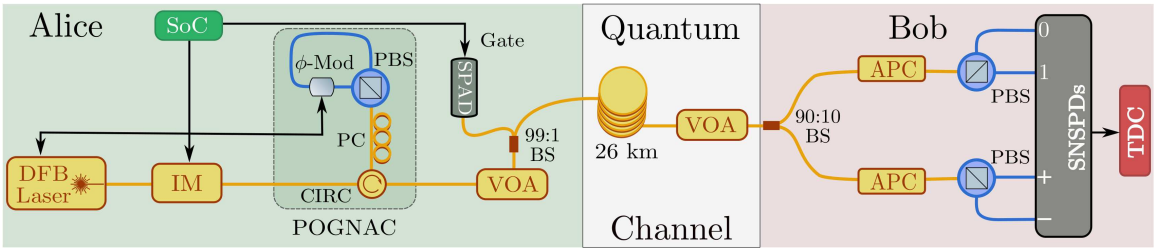


Figure 10.1: *Experimental Setup. Single Mode fibers are indicated in yellow while Polarization Maintaining fibers in blue.*

A gain-switched distributed feedback (DFB) laser source outputs a 50 MHz stream of phase-randomized pulses (with 270 of full-width-at-half-maximum, FWHM) at 1550nm wavelength. The light pulses first pass through a Lithium Niobate intensity modulator (IM) used to set the intensity levels required by the decoy-state method. The pulses then enter the POGNAC polarization modulator (described in Chap. 9) realized using only standard commercial off-the-shelf (COTS) fiber components.

The photons emerge from the POGNAC with a polarization state given by

$$\left|\psi_{\text{out}}^{\phi_e,\phi_\ell}\right\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{i(\phi_e-\phi_\ell)}|V\rangle\right), \tag{10.1}$$

where the phases ϕ_e and ϕ_ℓ can be set by carefully timing the applied voltage on a Lithium Niobate phase modulator (ϕ-Mod). This was achieved with the Zynq-7000 ARM/FPGA System-on-a-Chip (SoC, manufactured by Xilinx), which in our implementation overlooks the operation of the QKD source.

If no voltages are applied by the SoC, the polarization state remains unchanged, i.e. $\left|\psi_{\text{out}}^{0,0}\right\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$. Instead, if ϕ_e is set to $\frac{\pi}{2}$ while ϕ_ℓ remains zero, the output state becomes $\left|\psi_{\text{out}}^{\frac{\pi}{2},0}\right\rangle = |L\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle)$. Alternatively, if ϕ_e remains zero while ϕ_ℓ is set to $\frac{\pi}{2}$, the output state becomes $\left|\psi_{\text{out}}^{0,\frac{\pi}{2}}\right\rangle = |R\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle)$. In this way we generate the three states required by the simplified 3 polarization state version of BB84 [204], with the key-generation basis $\mathbb{Z} = \{|0\rangle, |1\rangle\}$ where $|0\rangle := |L\rangle$, $|1\rangle := |R\rangle$, and the control state $|+\rangle$ of the $\mathbb{X} = \{|+\rangle, |-\rangle\}$ basis.

The optical pulses then encounter a variable optical attenuator (VOA) which weakens the light to the single photon level. A 99:1 beam splitter (BS) is used to estimate the intensity level of the pulses: the 1% output port is directed to a gated InGaAs/InP Single Photon Avalanche Diode (SPAD, manufactured by Micro Photon Device Srl [206]), while the other output port is directed to Quantum Channel (QC). In our implementation the QC is formed by a 26 km spool of G.655 dispersion-shifted fiber with 0.35dB/km of loss followed by a VOA. This VOA allows us to introduce further channel loss in order to test our system's resilience.

Alice sends key-generation states with probability $p_A^{\mathbb{Z}}=0.9$ ($p_A^{\mathbb{X}}=0.1$), while the two intensity levels are $\mu_1\approx 0.80$ and $\mu_2\approx 0.28$, which are sent with probabilities $p_{\mu_1}=0.7$ and $p_{\mu_2}=0.3$. These parameters are close to optimal according to our simulations and Ref [196]. The random bits used to run the protocol are obtained from the Source-Device-Independent quantum random generator based on optical heterodyne measurement described in Chap. 3

The fiber receiving setup consists of a 90:10 fiber BS setting the detection probabilities of the two measurement bases to $p_B^{\mathbb{Z}}=0.9$ and $p_B^{\mathbb{X}}=0.1$. Each output arm of the BS is connected to an automatic polarization controller (APC) and a polarizing beam splitter (PBS). The four outputs are sent to four superconductive nanowire single-photon detectors (SNSPDs, manufactured by ID Quantique SA) cooled to 0.8 K. The detection efficiencies are around 85% for the detectors in the $\mathbb{Z}$ basis, whereas it is 90% and 30% for the $|+\rangle$ and $|-\rangle$ detectors, respectively. As discussed in [2, 240], some events are randomly discarded in post-processing to balance the different efficiencies. All the detectors are affected by about 200 Hz of free-running intrinsic dark count rate. The SNSPD detections are recorded by the quTAG time-to-digital converter (TDC, manufactured by qutools GmbH) with 1 ps of temporal resolution and jitter of 10 ps.

10.2 Self-synchronization theory

In this section an informal description of the self-synchronization protocol will be given, while a formal and detailed explanation can be found in [4].

In a typical QKD protocol, Alice transmits a qubit string (the raw key) encoded in the state of a train of attenuated optical pulses. The time between two consecutive qubits, τ^A, is set by Alice's clock. On the other side, Bob receives only some of the qubits (due to losses), analyzes their state and uses his clock to measure their time of arrival. We consider the case in which Alice and Bob's clocks may have a time bias as well as a relative drift in time of their frequencies. This implies that Bob may measure a different time τ^B between subsequent qubits.

The goal of Bob is to determine the position of the detected qubits in Alice's raw key: this operation is needed to correctly generate the sifted key, perform the parameter estimation and the subsequent post-processing. The above problem can be reformulated as follows: Bob needs to determine the expected time of arrival (measured by his clock) of the qubits sent by Alice, namely he needs to solve two tasks:

i) *Period recovery*: to recover the period τ^B from the obtained detections.

ii) *Time-offset recovery*: to determine the time delay t_0^A between the measured and sent sequence.

Step i) is needed to correctly reconstruct the separations in the raw key between consecutive detections. Step ii) is needed to associate each detection to the corresponding bits in Alice's raw string.

For the period recovery Bob takes the times t_i^B returned by his clock when he registered a click in the detector and performs an FFT. For computational efficiency this FFT is calculated only on a subsample N_s of the total detection N_t acquired for a defined exposure time (usually 1s). The highest peak of FFT returns a first estimate τ_0^B, i.e. Alice's sending frequency measured with Bob's clock. Then, in order to refine the estimation of τ_0^B at longer time scales, Bob calculates $\mod_{\tau_0^B}(t_i)$ for the first N_s t_i^B and fits the value with a linear model. The returned slope is equal to $\frac{\tilde{\tau}^B - \tau_0^B}{\tilde{\tau}^B}$ where $\tilde{\tau}_B$ is the new improved estimate. This fitting procedure is repeated iteratively, doubling each time the size of N_s until $N_s = N_t$. The last estimate of $\tilde{\tau}_B$ provides the optimal recovered period.

However, even if Bob can recover the right τ_B, with high probability he will not be able to detect the first pulse, due to losses in the channel. Moreover, the presence of background makes it not straightforward to distinguish the detection of Alice's qubit from noise. To precisely determine t_0^A, our approach is to to calculate the correlation between the signal received by Bob with a binary synchronization string s^A that has length L. The string s^A, which is also known to Bob, is transmitted before the QKD signals and is encoded in the $\mathbb{Z}$ basis. At the receiver Bob performs a cross-correlation between the string he recovers from the tags in the $\mathbb{Z}$ basis and the pre-shared string s^A. The lag at which the maximum of the cross-correlation occurs is the best estimate of t_0^A.

10.2.1 Robustness to noise

Before using the synchronization method described before in a real QKD run, we decided to characterize its robustness against the noise that could arise in the channel.

For the test we used the same transmission and detection probabilities of the QKD. So, since the synchronization string, s^A, sent by Alice is entirely encoded in the $\mathbb{Z}$ basis, only 90% of it will be decoded in the right basis (sifted). For the purpose of the synchronization algorithm, just the number of sifted bits at Bob side matters. Hence, we will talk about overall transmittance η as the ratio between the number of sifted bits at Bob side and the number of pulses sent by Alice.

The string sent by Alice is composed by a synchronization string, followed by random bits obtained from the quantum random number generator. We choose a number of states in the synchronization string s^A of $L = 10^6$. If η is the overall transmittance, the number of synchronization states received by Bob is $L\eta$. Therefore, assuming zero QBER and background noise, the maximum correlation value will be $\simeq \eta$, while the standard deviation of the correlation for other lags will be $\simeq \sqrt{\eta/L}$. The distinguishability, Δ, of the maximum correlation peak among the others is given by the ratio of the former and the latter $\Delta \simeq \sqrt{L\eta}$. We set a threshold on the distinguishability of $\Delta \geq 10$, as successful detection of the maximum correlation. Hence, for our choice of L, the algorithm can cope with overall losses up

to 40 dB. In practice, the presence of background and misalignment between the transmitter and the receiver lowers the maximum losses that the algorithm can handle.

We tested the robustness of the offset analysis by tuning the QBER and the number of bits of s^B. We used strings generated from several QKD runs as well as simulations of the experiment. In particular, the simulation takes into account the losses and misalignment of the setup but not the presence of the background and dark counts. In Fig. 10.2, the result of the simulation is highlighted by the blue region, corresponding to the values of QBER and bits in s^B in which the algorithm is expected to work. As regards the strings generated by the QKD setup, the orange dots show when the analysis was successful.

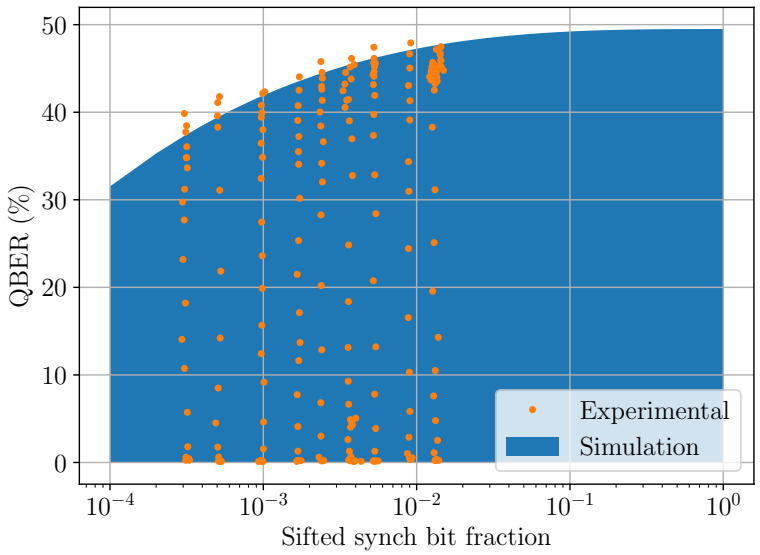


Figure 10.2: *Successful synchronization for different values of QBER and detected bits. The blue region shows where the synchronization have been established using simulated data. Orange dots correspond to successful synchronization with data generated by our setup.*

As expected, the simulation shows a good outcome of the analysis up to 10^{-4} sifted synchronization bit fraction. This is no longer true for high value of the QBER. Over 30% of QBER the algorithm needs more bits in s^B to contrast the reduction of the maximum correlation due to the bits flip. The background detection comes into play in the experimental runs, reducing the amount of losses the algorithm can tolerate. In our case, the analysis fails below a sifted synchronization bits ratio of $3 \cdot 10^{-4}$, with 200 Hz of free-running background detection rate. The robustness to the QBER is comparable to what obtained with the simulated strings. The comparison is limited to a ratio of about $3 \cdot 10^{-2}$ due to the maximum event rate our TDC can process. It is interesting to note the very high robustness to the QBER, well above the threshold to establish a secure channel. In fact, a very rough alignment between transmitter and receiver is sufficient for the synchronization to take place. This implies that the precise alignment of the receiver and transmitter may be realized after the synchronization phase, maybe using the same states sent by Alice and without the use of external reference, requiring additional lasers and detectors.

10.2.2 Polarization compensation scheme

The natural birefringence of fiber optics causes a transformation of the polarization state of the photons that travel through the fiber. This transformation is troublesome for QKD since it causes Alice and Bob to effectively have different polarization reference frames. As a consequence of this mismatch QBER increases, lowering the Secret Key Rate (SKR) up to the point where no quantum secure key can be established. To prevent this a polarization compensation system must be utilized.

Here we propose a polarization compensation scheme that exploits a shared public sting, which is not necessarily related to the synchronization string. Every second, the shared string of 10^6 states is transmitted by Alice encoded using weak coherent pulses in the $\mathbb{Z}$ basis and with μ_1 intensity. Bob detects the sequence, and after performing the temporal synchronization routine, he estimates the QBER of his recorded sequence. Bob still has to estimate the QBER in the $\mathbb{X}$ basis. For this purpose, at the end of each interval Alice reveals the basis used to encode the QKD qubits that follow the public string. This process is actually the standard reconciliation procedure of QKD. Since in the protocol we implement only one state is transmitted in the control $\mathbb{X}$ basis, Bob can immediately estimate the QBER.

The estimated QBER values are then fed into an optimization algorithm which controls the APCs of Bob's setup (described in Sec. 8.5.1).

Compared to the approach of Ding *et al.* [239], our approach has the advantage that only the reconciliation step is required to obtain sufficient information to run the polarization compensation algorithm. This allows for a greater tracking speed which is necessary to stabilize links with polarization drift of few Hz bandwidth. Also, the length of the shared string and its transmission frequency can be changed to best match the requirements of the fiber optical link. Furthermore, the public string can be transmitted in an interleaved fashion together with the QKD qubits at predetermined times.

10.3 Results

10.3.1 POGNAC intrinsic stability and low QBER

In Fig. 10.3, the intrinsic stability of our QKD polarization source is reported.

This measurement was performed by sending a pseudo-random qubit sequence of $\{|0\rangle, |1\rangle, |+\rangle\}$ states and measuring the QBER of the sifted string recovered by Bob. To remove all fluctuations not attributable to the source, the fiber channel was bypassed. Furthermore, the 90:10 BS was replaced with a 50:50 BS in order to have comparable statistics for both measurement bases. Every second the QBER was estimated for both the $\mathbb{Z}$ key-generation basis and the $\mathbb{X}$ control basis. In 45 minutes an average QBER of $Q_{\mathbb{Z}} = 0.07 \pm 0.02\%$ was measured for the $\mathbb{Z}$ basis while the average QBER for the $\mathbb{X}$ was $Q_{\mathbb{X}} = 0.02 \pm 0.01\%$. These measurements corroborate the results of Chap. 9 and demonstrate intrinsic stability of the POGNAC polarization modulator. Furthermore, with over 30 dB of extinction ratio between orthogonal states, the average QBER here reported is the lowest for any active QKD source fully implemented using exclusively COTS components, to the best of our knowledge.

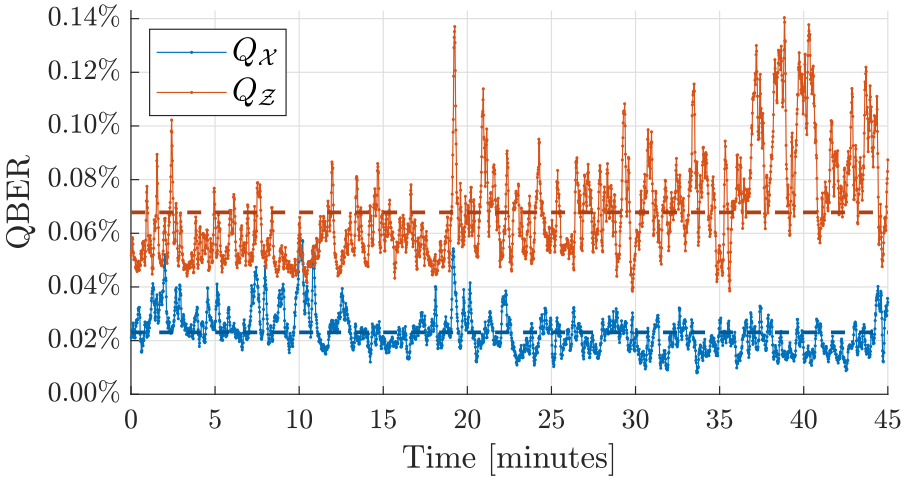


Figure 10.3: *Intrinsic Stability of the POGNAC source at 50 MHz repetition rate. The average QBER measured for the key-generation basis was* $Q_{\mathbb{Z}} = 0.07 \pm 0.02\%$ *(dashed orange line) while an average* $Q_{\mathbb{X}} = 0.02 \pm 0.01\%$ *(dashed blue line) was measured for the control basis.*

10.3.2 Polarization drift compensation with 26 km of optical fiber

To test our polarization drift compensation algorithm we performed a 6 hour long run with the QC including both a 26 km optical fiber spool and ≈10 dB of additional attenuation set by the VOA.

On average, the detected bits of the shared polarization compensation string in the $\mathbb{Z}$ basis were $\approx 8 \times 10^3$ while the sifted bits from the control basis were $\approx 3 \times 10^3$. This allowed to correct the polarization drift with an average QBER measured for the key-generation basis of $Q_{\mathbb{Z}} = 0.3 \pm 0.1\%$ while an average $Q_{\mathbb{X}} = 0.2 \pm 0.1\%$ for the control basis, for six hours of continuous operation. The results are reported in Fig. 10.4. After the experimental run, we noted a lower detection efficiency of 45% for the detectors of the $\mathbb{Z}$ basis. This was due to a non-optimal polarization rotation of the photons entering the SNSPD detectors, which are polarization sensitive. This reduced detection efficiency did not hamper the polarization drift compensation algorithm demonstrating its robustness even in non-optimal conditions.

10.3.3 QKD secure key rate for different channel losses

To test the performances of our simple QKD system with self-synchronization and self-compensating polarization encoder, as well as its resistance to channel losses, several runs were executed each with increased losses. The losses were added increasing the attenuation of the VOA after the 26 km of fiber. As before, a pseudo-random qubit sequence of $\{|0\rangle, |1\rangle, |+\rangle\}$ was transmitted at a repetition rate of 50 MHz, where the first L qubits of the sequence formed the publicly known synchronization string. For each run the SKR was calculated in the asymptotic limit: $SKR_{\infty} = s_{\mathbb{Z},0}/t + s_{\mathbb{Z},1}(1 - h(Q_{\mathbb{X}}))/t - f \cdot h(Q_{\mathbb{Z}})$, where t is the duration of each acquisition, $h(\cdot)$ is the binary entropy, $f = 1.06$ is the Shannon inefficiency of typical error correction algorithms, while $s_{\mathbb{Z},0}$ and $s_{\mathbb{Z},1}$ are the lower bounds on the number of vacuum and single-photon detections in the $\mathbb{Z}$ basis, calculated as in [196]

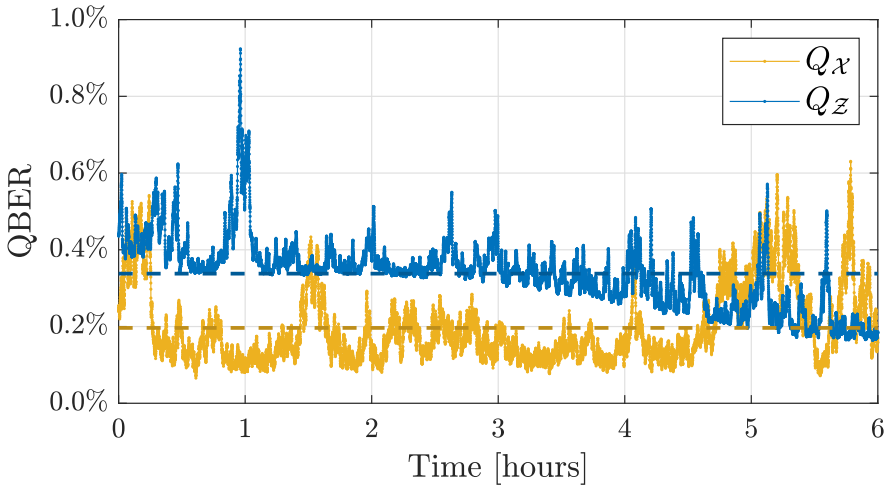


Figure 10.4: *QBER Measurement for a 6 hour long acquisition along a 26 km optical fiber channel. The average QBER measured for the key-generation basis was* $Q_{\mathbb{Z}} = 0.3 \pm 0.1\%$ *(dashed yellow line) while an average* $Q_{\mathbb{X}} = 0.2 \pm 0.1\%$ *(dashed purple line) was measured for the control basis.*

but without finite-key corrections. The results are presented in Fig. 10.5.

As shown in [4], if the background and dark counts are not considered, the synchronization can be established up to 40 dB of total channel losses with $L = 10^6$. A longer string, with $L = 10^7$, could be used to synchronize up to 50 dB of losses. In our experiment, the presence of dark counts lowers the bounds by about 6 dB. Indeed, using a synchronization string of length $L = 10^6$, we performed several QKD runs with losses up to 34 dB. With $L = 10^7$, we successfully ran QKD protocols up to the channel loss at which the key rate drops to zero. In the QKD run with highest losses, we achieved a secure key rate of 80 bits per second at 43 dB total channel losses, corresponding to about 215 km of SMF28 fibre (0.2 dB/km) or 253 km of ultralow-loss fiber (0.17 dB/km). It is important to note that our QKD implementation withstands up to 44 dB of total channel loss, as reported in the SKR_∞ simulation of Fig. 10.5. Our results prove that the self-synchronization method properly works even at the highest losses tolerated by our QKD implementation.

10.4 Conclusions

In this chapter we have presented a simple polarization encoded QKD implementation with self-synchronization and a self-compensating polarization modulator. Its simple design reduces the complexity for both the QKD transmitter and receiver. In fact, the same optical setup is used for three different tasks, i.e. synchronization, polarization compensation and QKD, without requiring any changes of the working parameters of the setup or any additional hardware. The QKD transmitter shows high intrinsic stability and the lowest average QBER ever reported for an active polarization source developed using only COTS components. The SKR in the asymptotic limit was assessed for a 26 km fiber channel with additional channel losses resulting in 80 secure bits per second at 43 dB of total channel

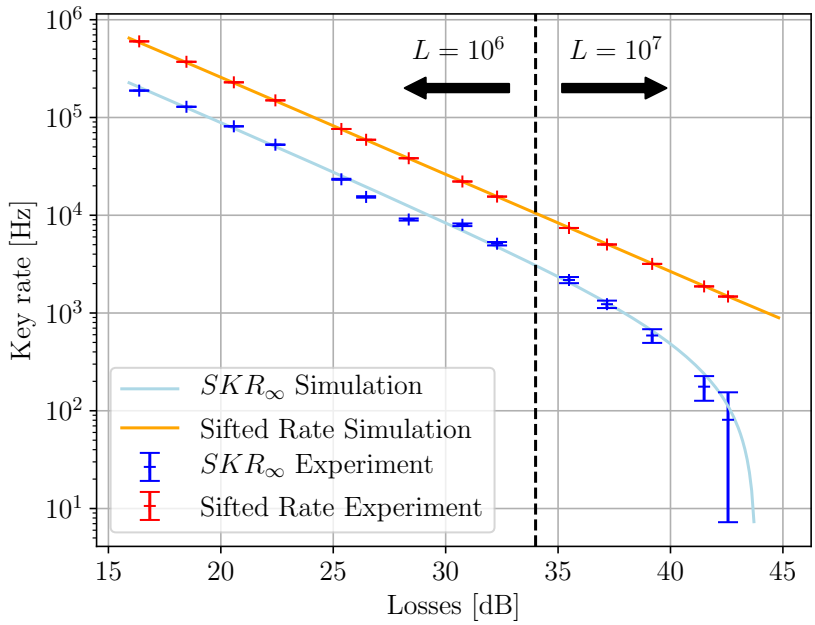


Figure 10.5: *Sifted and secure key rate as a function of total channel losses. The crosses represent the experimental runs performed with the self-synchronization method, while the lines show the results of our simulation based on the physical parameters of our experiment. Error bars are standard deviations, obtained by simulating 1000 repetitions of the experiment.*

losses, demonstrating resilience to high channel losses for both our QKD implementation and the self-synchronization algorithm. The simplicity of our QKD implementation renders it compatible with many different scenarios, ranging from urban QKD fiber links [192] to free-space satellite QKD links via CubeSats [233], where a small footprint and low energy consumption are of critical importance. Our implementation is particularly promising for free-space QKD [2, 173, 188] since polarization is not significantly affected by atmospheric propagation [241].

CHAPTER 11

Post-selection loophole-free genuine time bin

In 1989 Franson conceived a simple interferometric setup to highlight the counter-intuitive implications of quantum mechanics [242]. He proposed to send a pair of entangled photons to two equal measurement stations (Alice and Bob), each composed of an unbalanced interferometer. By exploiting the quantum interference expected in the detection events recorded at the output ports of the interferometers, it should be possible to rule out local realistic models [17] by violating a Bell-CHSH inequality [243]. Franson's idea was first implemented by exploiting *energy-time* entanglement, which can be easily created by pumping a non-linear crystal with a continuous-wave (CW) laser [244–246]. In fact, the two emitted photons are generated at the same instant, but the emission time is uncertain within the coherence time of the source, thus leading to indistinguishability in the alternative paths the photons will take in the measurement stations. Extending Franson's idea, *time-bin* (TB) entanglement was introduced by Brendel *et al.* in 1999 [247]: the CW laser is replaced by a pulsed laser which shines the non-linear crystal after passing through an unbalanced "pump" interferometer. Now, the pair of photons can be emitted at two possible times, depending on the path taken by the pump-pulse in the first interferometer (see Fig. 11.1a). Both energy-time and time-bin entanglement have been widely used to distribute entanglement over long distances [248–252], and to realize fiber-based cryptographic systems [145, 253], aiming for device-independent security [159, 222, 254], which requires the loophole-free violation of a Bell inequality, as reported in [21–24].

However, Aerts *et al.* noted that Franson's Bell-test is intrinsically affected by the so-called *post-selection loophole* (PSL) [255], which is present independently to the other common loopholes (eg., locality and detection) that could affect local-realistic tests [256]. In fact, in Franson's configuration, Alice and Bob should post-select only the indistinguishable events occurring within a coincidence window $\Delta\tau_c$, discarding those photons arriving at different times. When performing such post-selection, there exists a local-hidden-variable (LHV) model which reproduces the quantum predictions [255, 257]. The reason for this is that a LHV model admits the local delays to depend on the local parameter (φ_A or φ_B), but Alice and Bob need to compare these delays to perform the post-selection. Therefore, even though

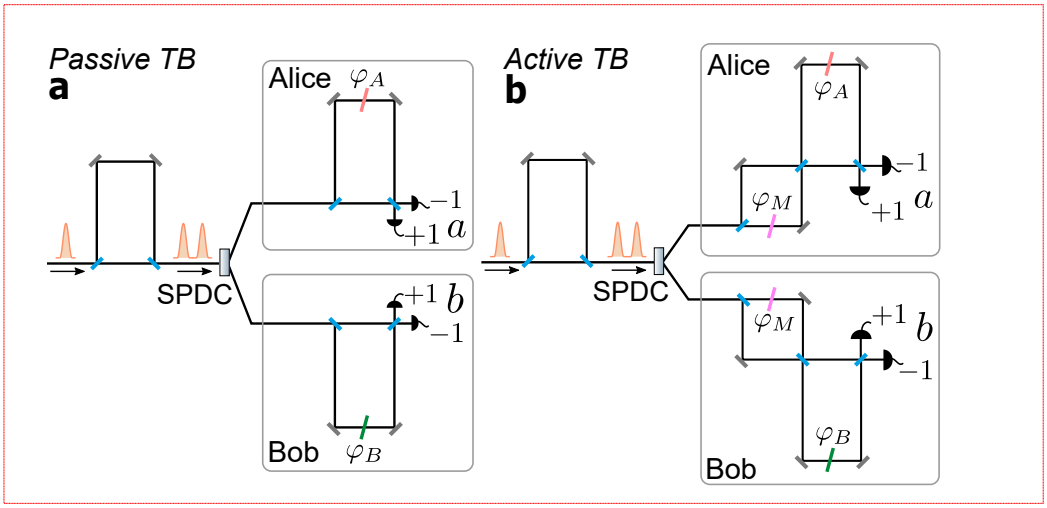


Figure 11.1: *Time-bin schemes to realize a Bell-test à la Franson.* **a** *In the passive TB, by post-selecting the events detected in coincidence only in the central time-slot, Alice and Bob can violate the Bell's inequality, but the scheme is affected by an intrinsic PSL.* **b** *In the active TB, the passive beam splitter is replaced by a balanced MZI acting as an optical switch. By exploiting a fast phase modulator φ_M in one arm of the balanced MZI, Alice and Bob can violate the Bell-CHSH inequality without discarding any data, i.e. this scheme is free of the PSL.*

the physical system is completely local, the measurement-process post-selection invalidates the locality assumption required to derive the Bell's inequality. The same loophole affects the time-bin entanglement scheme shown in Fig. 11.1a, invalidating Bell's inequality as test of local realism and enabling the hacking of Franson' scheme when used for cryptographic purposes [258]. In this case, the Bell-test gives false evidence, since the apparent violation would tell users the setup is device-independently secure, while it is in fact insecure because of the PSL.

Many modifications to Franson's original scheme have been proposed to address the PSL, with both energy-time and time-bin entanglement. Regarding the former, a proposal by Cabello *et al.* modified the geometry of the interferometers by interlocking them in a *hug configuration*, and introduced a *local* post-selection, which does not require communication between Alice and Bob [259]. In this way, *genuine* energy-time entanglement can be generated, i.e. not affected by the PSL. Soon after this proposal had been conceived, table-top experiments were realized [260, 261] and a few years later the distribution of genuine energy-time entanglement through 1 km of optical fibers [262] and its implementation in an optical fiber-network was reported [263]. However, the hug configuration requires to stabilize two long interferometers whose extension is determined by the distance between Alice and Bob: the larger the separation is, the more demanding the stabilization becomes. In the case of time-bin entanglement, the original proposal mentioned the use of *active* switches [247], such as movable mirrors synchronized with the source, instead of passive beam splitters (Fig. 11.1a), to prevent discarding any data. This solution can also be exploited to overcome the PSL [257], but no such scheme has been realized so far.

Here we propose and implement, for the first time, a genuine time-bin entanglement scheme allowing the violation of a Bell's inequality free of the PSL. In our scheme, the active switches are realized by replacing the first beam splitter, in each unbalanced interferometer

of the measurement stations, with another balanced interferometer with a fast phase-shifter in one arm, as sketched in Fig. 11.1b. By actively synchronizing the phase-shifter with the pump pulses, it is possible to use the full detection statistics, overcoming the PSL. The independence between Alice' and Bob's terminals, the relaxed stabilization requirements, as well as the compliance with off-the-shelves components open the possibility to exploit such scheme over long distances, paving the way to a conclusive loophole-free Bell-test [21–24] with time-bin entanglement.

In the following Chapter, we will analyze the passive and active time-bin schemes by making use of the *Positive Operator Valued Measure* (POVM) formalism [45], after which we will present the experiment and the obtained Bell-CHSH inequality violation attesting the faithfulness of our scheme.

Some contents of this chapter are part of our work [6].

11.1 Conceptual analysis of time-bin entanglement schemes

In the passive time-bin scheme, a pump Mach-Zehnder interferometer (MZI) with a temporal imbalance equal to Δt is used to split a short light pulse into two, as sketched in Fig. 11.1a. This light is focused into a non-linear crystal producing photon pairs via a spontaneous parametric down conversion (SPDC) process. By optimizing the pump energy, the generation of double photon-pairs is suppressed, and the Bell state $\left|\Phi^+\right\rangle = (|S\rangle_A|S\rangle_B + |L\rangle_A|L\rangle_B)/\sqrt{2}$ is produced, where the indexes A and B represent the generated photons that are sent to Alice' and Bob's measurement stations. Each of these is composed by an unbalanced MZI that has the same imbalance Δt of the pump-interferometer and can introduce a further phase shift φ_A (φ_B). The output ports of each interferometer are followed by two single-photon detectors, and the possible outcomes are labeled $a = \pm 1$ and $b = \pm 1$ for Alice and Bob respectively, depending on which detector clicks.

In the passive TB scheme, each photon of the pair can be detected only at three possible distinct times $(t_0 - \Delta t, t_0, t_0 + \Delta t)$, due to the pump- and measurement-MZIs. By post-selecting the detection events that occur in the central time-slot only, Alice's measurement station realizes the projection $\{\hat{P}_a\}_{a=\pm 1}$ defined by $\hat{P}_a = |\psi_a\rangle\langle\psi_a|$ where

$$|\psi_a\rangle = \left(|S\rangle + a\ \mathrm{e}^{\mathrm{i}\varphi_A}|L\rangle\right)/\sqrt{2} \tag{11.1}$$

and similar relations hold for Bob's measurement station (with a replaced by b and A by B). Since the delay is local, one could think that this should allow the violation of the Bell's inequality. There is simply no physical mechanism for the remote phase shift to influence the local delay. However, for a coincidence to occur, Bob's delay needs to coincide with Alice's one, and Bob's delay is controlled by Bob's phase shift, remotely from the point of view of Alice. This constitutes a coincidence loophole for the Bell inequality [264], somewhat similar to a detection loophole with 50% detection efficiency, but much worse since it is present even when using loss-free equipment, therefore introducing an unavoidable intrinsic loophole in the setup.

Quantum mechanics provides the probabilities $\mathscr{P}_{a,b}$ for photon detections that occur within a coincidence window $\Delta\tau_c < \Delta t$ around the central time-slot for each pair of detectors a, b. The probabilities $\mathscr{P}_{a,b}$ depend on the initial state $\left|\Phi^+\right\rangle$ and on the local phase shifts φ_A,

φ_B introduced by the measurement stations and are given by

$$\mathscr{P}_{a,b}(\varphi_A,\varphi_B)=\frac{1}{4}\left[1+ab\mathscr{V}\cos(\varphi_A+\varphi_B)\right] \tag{11.2}$$

where $\mathscr{V}$ is the visibility of two-photon interference.

Disregarding the PSL, the interference in the post-selected events will seem to violate the Bell-CHSH inequality, which provides an upper limit for a combination of four correlation functions $E(\varphi_A,\varphi_B)$ with different phases φ_A,φ_B, when assuming the existence of a LHV model [243]. The correlation function is given by

$$E(\varphi_A,\varphi_B)=\sum_{a,b}ab\mathscr{P}_{a,b}(\varphi_A,\varphi_B) \tag{11.3}$$

and the Bell-CHSH inequality $S\leq 2$ is given in terms of the S-parameter

$$S\equiv E(\varphi_A,\varphi_B)+E(\varphi'_A,\varphi_B)+E(\varphi_A,\varphi'_B)-E(\varphi'_A,\varphi'_B) \tag{11.4}$$

where φ_A,φ'_A and φ_B,φ'_B denote the values of the phase-shifts introduced by Alice and Bob respectively [243]. Quantum mechanics predicts the correlation function

$$E^{\mathrm{QM}}(\varphi_A,\varphi_B)=\mathscr{V}\cos(\varphi_A+\varphi_B) \tag{11.5}$$

which leads to a maximum value for the S-parameter equal to $S_{\max}=2\sqrt{2}\mathscr{V}$ for the settings $\varphi_A=-\pi/4$, $\varphi'_A=\pi/4$ and $\varphi_B=0$, $\varphi'_B=\pi/2$. Hence, the Bell-CHSH inequality will seem to be violated only if $\mathscr{V}>1/\sqrt{2}\approx 0.71$.

It is worth noticing that if no post-selection is applied in the passive TB scheme, then the Bell-CHSH inequality does hold, and could in principle be violated. However, in this case Alice's measurement station implements the POVM given by $\{\hat{\Gamma}_a\}_{a=\pm1}$ with $\hat{\Gamma}_a=(1/4)\mathbb{1}+(1/2)\hat{P}_a$, where $\mathbb{1}=|S\rangle\langle S|+|L\rangle\langle L|$ (and similar relations hold for Bob). Thus, with no post-selection, the quantum probabilities $\mathscr{P}_{a,b}$ for photon detections at the two stations lead to a maximum value for the S-parameter that can be written as $S_{\max}=2\sqrt{2}\mathscr{V}'$, with the overall three-peak visibility $\mathscr{V}'=\mathscr{V}/4$ and the Bell-CHSH inequality cannot be violated even with perfect visibility $\mathscr{V}=1$.

On the other hand, a proper violation can be achieved in the active TB scheme here proposed (see Fig. 11.1b). We replace the passive beam-splitter with an additional balanced MZI acting as a fast optical switch, which allows the measurement MZI to recombine the $|S\rangle$ and $|L\rangle$ pulses, making them indistinguishable. In this way, contrary to the passive TB scheme which recombines the two temporal modes in a probabilistic manner, our scheme deterministically compensates for the delay Δt and no detections are discarded. Indeed, by imposing the phases φ_S and $\varphi_L=\varphi_S-\pi$ on the $|S\rangle$ and $|L\rangle$ pulses respectively, the balanced MZI determines the path they will take in the measurement MZI, as sketched in Fig. 11.2a.

At each detector, we expect a detection pattern that depends on the value of φ_S, as shown in Fig. 11.2a. From a formal point of view, in our TB scheme Alice's measurement station implements the POVM $\{\hat{\Pi}_a\}_{a=\pm1}$, where $\hat{\Pi}_a=\frac{1}{2}\left(\cos^2\frac{\varphi_S}{2}|S\rangle\langle S|+\sin^2\frac{\varphi_L}{2}|L\rangle\langle L|\right)+|\chi_a\rangle\langle\chi_a|$ with $|\chi_a\rangle=(\mathrm{i}e^{-\mathrm{i}\frac{\varphi_S}{2}}\sin\frac{\varphi_S}{2}|S\rangle+ae^{\mathrm{i}(\varphi_A-\frac{\varphi_L}{2})}\cos\frac{\varphi_L}{2}|L\rangle)/\sqrt{2}$ (the phase difference between the transmitted and reflected mode by a beam splitter is $e^{\mathrm{i}\pi/2}=\mathrm{i}$). If $\varphi_L=\varphi_S-\pi$, the POVM reduces to

$$\hat{\Pi}_a=\frac{1}{2}\cos^2\left(\frac{\varphi_S}{2}\right)\mathbb{1}+\sin^2\left(\frac{\varphi_S}{2}\right)\hat{P}_a\ . \tag{11.6}$$

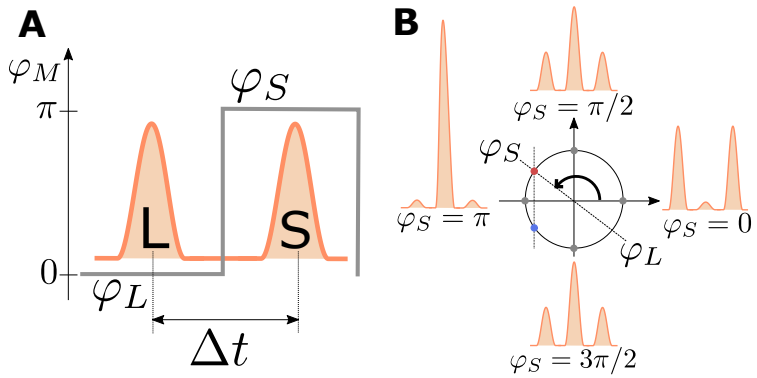


Figure 11.2: *Functioning of the active TB scheme.* **a** *In a balanced MZI, the relative phase φ_M sensed by a traveling pulse determines the output port it will exit at with probabilities $\cos^2(\varphi_M/2)$ and $\sin^2(\varphi_M/2)$. By using a fast modulator, it is possible to impose the different phase-shifts φ_S and φ_L to the the $|S\rangle$ and $|L\rangle$ photons while they are traveling along the balanced MZI. By fixing $\varphi_S = \pi$ and $\varphi_L = 0$, it is possible to temporally recombine $|S\rangle$ and $|L\rangle$ pulses, making them indistinguishable.* **b** *The detection pattern at the output ports depends on the values φ_S and $\varphi_L = \varphi_S - \pi$. If $\varphi_S = \pi$, all detection events occur in the central time-slot, whereas if $\varphi_S = 0$ they are present only in the lateral time-slots. Any other detection histogram can be obtained with two different φ_S values, one with $\varphi_S < \pi$ (red dot) and the other with $\varphi_S > \pi$ (blue dot). For example, $\varphi_S = \pi/2$ and $\varphi_S = 3\pi/2$ have the same click distribution.*

If Alice sets the phase $\varphi_S = \pi$ (and thus $\varphi_L = 0$), $\hat{\Pi}_a$ reduces to $\hat{P}_a$ and her station actually projects onto the state $|\psi_a\rangle$, with no post-selection procedure. Indeed, in the detection pattern the lateral peaks "disappear", as shown in Fig. 11.2b and it is not necessary to discard any data. Hence, the violation of Bell-CHSH inequality expected from our scheme is free of the PSL.

11.2 Description of the experiment

We implemented the active TB scheme proposed above by using the experimental setup sketched in Fig. 11.3. A mode-locking laser produced a pulse train with wavelength centered around 808 nm, 76 MHz of repetition rate and ∼150 fs of pulse duration. This beam is used to pump a second-harmonic-generation (SHG) crystal which generates coherent pulses of light up-converted to 404 nm. Each of the obtained pulse passes through a free-space unbalanced Michelson interferometer (that is the pump-interferometer) which produces a coherent state in two temporal modes. The imbalance $\Delta l = L - S$ between the two arms is about 90 cm, corresponding to a temporal imbalance $\Delta t = \Delta l/c \approx 3$ ns (with c the speed of light in vacuum), much greater than the coherence time of the pulses. Then, the pulses pump a 2-mm long Beta-Barium Borate (BBO) crystal to produce the entangled photon state via type II SPDC [265] at 808 nm.

The two photons are sent to Alice' and Bob's terminals after being spectrally filtered (3 nm bandwidth) and collected by two single-mode optical fibers. Each station is composed of two MZIs, a balanced one and an unbalanced one. The balanced MZI is composed by a 50:50 fiber coupler which defines the two arms of the interferometer. To guarantee the zero

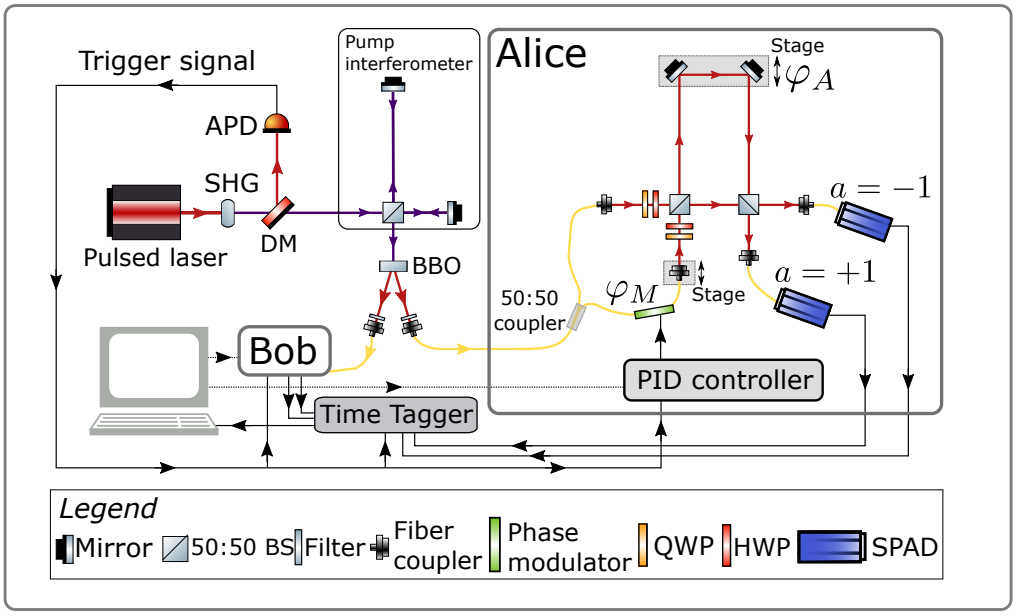


Figure 11.3: *Experimental setup to implement the active TB scheme. Bob's measurement station is analogue to Alice's one. APD: analog-photo-detector; DM: dichroic mirror.*

imbalance of this MZI, a nanometric stage is placed in one of the two arms.

The balanced MZI works as a fast optical switch, since there is a fast (∼GHz bandwidth) phase-modulator in one of its arms. The modulation voltage is set to V_π such that $\varphi_S - \varphi_L = \pi$, while the DC bias of the phase-modulator is driven by an external proportional-integral-derivative (PID) controller, that is responsible of locking the phase φ_S to π. The complete operating principle of the PID controller is detailed in the Methods.

The two arms of the balanced MZI are recombined at a 50:50 free-space beam splitter (BS) after been optimized for polarization rotations. This BS begins the unbalanced MZI whose imbalance is equal to that of the pump-interferometer (within the coherence time ∼200 μs of the photons). The two mirrors of the long arm of the unbalanced MZI are placed on a nanometric piezoelectric stage to both guarantee the required imbalance Δt and introduce the local phase shift φ_A and φ_B to realize the Bell-test. At the two output ports of the measurement stations we used two avalanche single photon detectors (SPADs, ∼50% detection efficiency), labeled as $a = \pm 1$ and $b = \pm 1$. The detection events are then time-tagged by a time-to-digital converter (Time Tagger) with 81 ps resolution and the data are stored in a PC.

11.2.1 Operating principle of the PID controller

In our experiment we drive the phase φ_M introduced by the phase-modulator (PM) in the balanced MZI to make the photons take a precise path in the subsequent MZI. To realize this, we implemented the PID controller that is sketched in Fig. 11.4.

First, we synchronize the phase transition with the pump-pulses that produce the photon pair. This is performed by a fast analog-photo-diode (APD) that collects the 808 nm pulsed beam (after being separated with a dichroic mirror (DM) from the 404 nm pulse train produced by the SHG stage, see Fig. 11.3) and produces an electric signal synchronized with

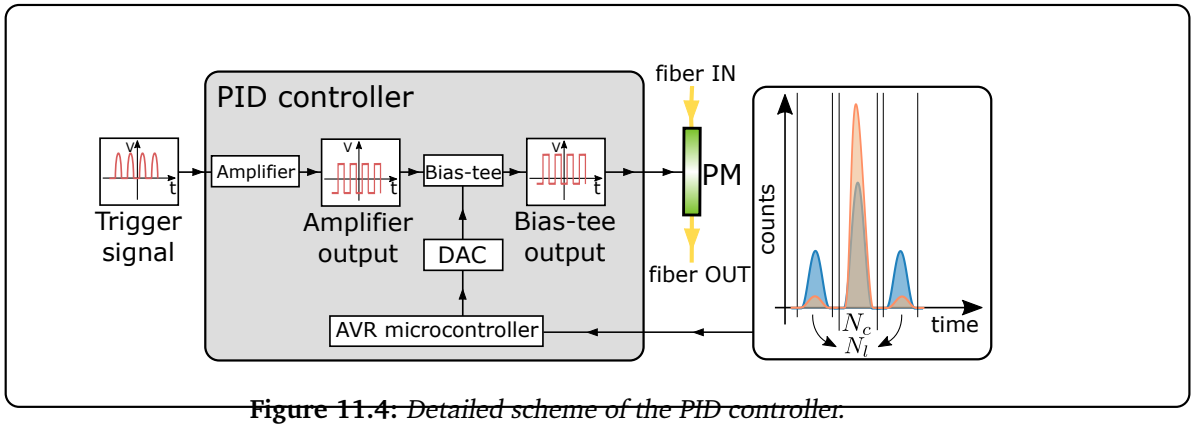


Figure 11.4: *Detailed scheme of the PID controller.*

the optical pulses. This signal is spit in two: one is then collected by the time-tagger for timing purposes and the other one is sent to the PID controller.

The first stage of the PID controller is an amplifier (iXblue) which produces a square wave with fixed amplitude centered around 0 V. The amplitude V_π of this wave set the strength $\Delta\varphi = \varphi_S - \varphi_L = \pi$ of the transition introduced by the phase-modulator. The raise time of the square wave is less than 2.5 ns to guarantee that the π-transition occurs within the short-long temporal separation Δt.

The absolute value of the phase φ_S of the balanced MZI is perturbed by temperature fluctuations and vibrations due to the environment. In order to correctly implement our scheme, we have to compensate this phase fluctuation (which occurs in the order of tens of seconds), by locking the value of φ_S to π.

To perform this locking, the second stage of the PID controller is given by a bias-tee (MiniCircuits) which compensates the intrinsic phase shift of the balanced MZI by changing the offset voltage V_{bias} of the square wave produced by the amplifier. This is obtained by the combined action of an AVR micro-controller (Arduino) and a digital-to-analog converter (DAC) by maximizing the extinction ratio R between the central and the lateral peaks $R = (N_c - N_l)/(N_c + N_l)$, where N_c are the counts associated to the central peak and N_l are all the counts in the lateral ones recorded by one of the two detectors of the measurement station. All the counts in each detector can be estimated in real-time by looking at the raw data collected by the time-tagger (QuTools), and they produce the detection histogram sketched in the inset of Fig. 11.4, which corresponds to the real detection histograms presented in Fig. 11.5.

To successfully lock φ_S to π the PID controller has to first evaluate its real-time value by observing the detection histogram and computing R. Unfortunately, there is no one-to-one correspondence between the extinction ratio and the phase φ_S. Indeed, for each possible value of R there exist two possible values for φ_S that reproduce the observed histograms (with the exception of 0 and π), as shown in Fig. 11.2b. Therefore, we must include an additional information that allows us to distinguish between the two possible phase values. This information is given by the derivative of the extinction ratio. If an increase of the phase value causes an increase of the ratio, we choose the phase $0 < \varphi_S < \pi$ (requiring further increase to reach π). Otherwise, we choose the phase $\pi < \varphi_S < 2\pi$ (requiring a decrease to reach π). Since the PID requires an error function that is equal to zero when the objective is reached, we choose the function $E_{\varphi_S} = \text{sgn}\left(\frac{dR}{d\varphi_S}\right)\frac{N_l}{N_c}$, which guarantees that the PID's objective

is both to lock the value of φ_S to π and to identify correctly the value of the phase, since the symmetry between the two possible phase values is broken by the sign of the derivative of the extinction ratio.

11.3 Results of the Bell-test

With the setup shown in Fig. 11.3, we performed the time-bin Bell-test with three different schemes: I) the *passive TB with post-selection*, II) the *passive TB with no post-selection*, III) the *active TB with no post-selection* proposed above. To realize I), we bypassed the balanced MZI in each of the measurement stations, hence obtaining the passive TB configuration of Fig. 11.1a. By choosing a coincidence window $\Delta\tau_c \approx 2.4$ ns and by post-selecting the coincident events that occurred only in the central time-slot, Alice (Bob) implemented the projective measurement given by $\hat{P}_a$ ($\hat{P}_b$) and the expected Bell-CHSH violation is affected by the PSL. To realize II), we used the same configuration as in I), but we did not discard any data by choosing a coincidence window $\Delta\tau_c \approx 8.1$ ns, which corresponds to the total width of the three peak-profile in the detections (see Fig. 11.5). In this case, Alice (Bob) implemented the POVM given by $\hat{\Gamma}_a$ ($\hat{\Gamma}_b$) and no Bell-CHSH violation is expected.

To implement III), we exploited the balanced MZI in each station and we used the PID controller to lock the phase φ_S and φ_L to π and 0 respectively, independently at each terminal. We did not discard any data by choosing a large coincidence window as in II), but, in this case, the Bell-CHSH inequality is directly applicable, since Alice (and Bob) implemented the POVM given in Eq. (11.6) with $\varphi_S = \pi$. The expected Bell-CHSH violation is free of the post-selection loophole and this represents the main result of our work.

We show in Fig. 11.5 a typical detection histogram obtained with one of the four detectors during the data acquisition (the results are similar for all the detectors). In the case of TB schemes I) and II), since the balanced MZI is bypassed, we obtained the expected three-peak profile (blue histogram). On the other hand, in our active TB scheme III), the PID controller makes the lateral peaks disappear, as shown by the orange detections histogram. This guarantees the correct functioning of the PID controller, whose details are described in the Methods. It is worth noticing that the whole three-peak profile is within the chosen coincidence window $\Delta\tau_c = 8.1$ ns, thus guaranteeing that no data is discarded.

To realize each of the Bell-tests described above, we first calibrated the shifts to be introduced by the nanometric stages in Alice' and Bob's unbalanced MZIs. This is obtained by scanning the coincidence rate for a pair of detector by moving Bob' stage while Alice's one is fixed. From the sinusoidal pattern obtained in such a way, we estimated the experimental visibility $\mathscr{V}_{\text{exp}}$ for each scheme. Then, we imposed the shifts (φ_A, φ_B) needed to obtain the maximal violation of the Bell inequality (as described above) and acquired the data for sufficient time to achieve significant statistics.

The results obtained for each of the three schemes described above are represented in Table 11.1. As expected, violation of the Bell-CHSH inequality was obtained with the first and the third scheme with clear statistical evidence, but only the third one is not affected by the PSL. The minor violation obtained in III) is due to imperfection in the balanced MZI alignment and in the locking procedure occurring during data acquisitions needed to experimentally estimate the S-parameter S_{exp}. It is worth stressing that any imperfection in

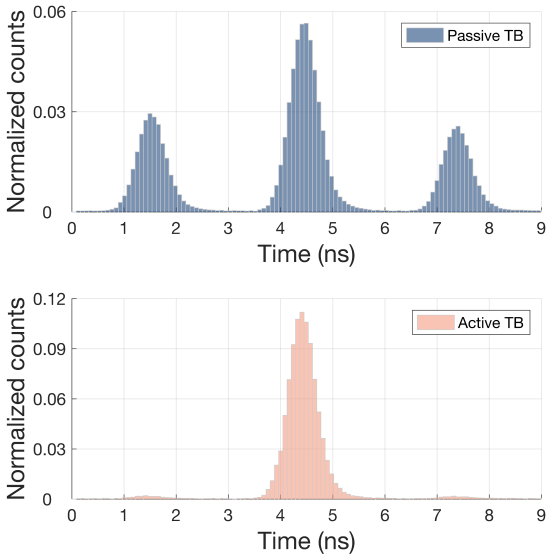


Figure 11.5: *Typical detection histograms obtained during data acquisition. The two histograms represent all the raw detections collected by one of the four detectors during the data acquisition. The blue histogram shows a typical detection pattern obtained with the passive TB scheme, in which the three-peak profile is observed. The orange histogram shows the detection pattern obtained with the active TB scheme: the PID controller is able to lock φ_S to π and φ_L to 0, thus making the lateral peak disappear, allowing us to realize a time-bin Bell-test free of the PSL. The counts are normalized to fairly compare the two histograms.*

the locking mechanism setting $\varphi_S = \pi$ corresponds to an effective lower visibility, but it does not introduce any loophole in the Bell inequality.

11.4 Conclusions and outlooks

Time-bin encoding [247] is a valid resource for both performing fundamental tests of quantum mechanics [266–268] and distributing entanglement over long distances [252]. However, all the time-bin entanglement realizations performed so far were affected by the post-selection loophole, which makes this technique unsuitable for quantum information protocols. A possible way to overcome this problem requires to violate the so-called "chained" Bell-inequalities [269], but the needed visibility ($\gtrsim 0.94$ [258]) is considerably higher than the one of the Bell-CHSH inequality ($\gtrsim 0.71$). Even if such a high visibility is achievable

Scheme	$\Delta\tau_c$	PSL	$\mathcal{V}_{\text{exp}}$	S_{exp}	SD
I) passive TB	2.4 ns	Yes	0.95 ± 0.05	2.58 ± 0.03	18.3
II) passive TB	8.1 ns	No	0.23 ± 0.02	0.67 ± 0.02	—
III) active TB	8.1 ns	No	0.89 ± 0.03	2.30 ± 0.03	9.3

Table 11.1: *Main results. SD refers to Standard Deviation of the Bell-CHSH violation.*

with time-bin entanglement, as shown in [270], our scheme clearly relaxes this requirement, since the Bell-CHSH inequality is directly applicable.

In this chapter we have presented the first implementation of genuine time-bin entanglement, which represents a crucial step towards its exploitation for fundamental tests of physics and the realization of the quantum Internet [182]. In fact, our scheme can be realized using only commercial off-the-shelves fiber components and, since its stability does not depend on the distance between Alice and Bob, it is easier to be implemented with respect to the hug configuration [259]. Furthermore, as long as both the π-phase transition imposed by the modulator and the detectors jitter are shorter than the imbalance Δt, it is possible to shorten it, rendering it compatible with today's photonic integrated technologies [191, 271]. Finally, our work makes time-bin entanglement a viable technique to obtain a loophole-free Bell violation, that is the enabling ingredient of any device-independent protocol [159, 222, 254, 272].

CHAPTER 12

Conclusions

Quantum Random Number Generation and Quantum Key Distribution have made huge steps forward in the last few decades and nowadays are mature and commercial technologies.

However, QRNG used in practical applications still require a high level of trust on the internal devices and on the manufacturer. The main motivation for this is that more secure alternatives, such as Semi-DI QRNG, cannot match the simplicity the cost and the performances of "trusted" QRNG. In the first part of this thesis we have demonstrated that Semi-DI, and in particular Source-DI, protocols can be implemented with simple optical setups and are able to offer performances perfectly comparable with "trusted" QRNG, making them a preferable solution, due to their increased security. In particular in Chapter 3 we have presented a simple Source-DI protocol based on heterodyne detection that is able to generate more than 17 Gbps of secure and private random numbers, breaking the previous record for this category of QRNG by more than an order of magnitude. Then, in Chapter 4 we have developed a new tool for the security analysis of "trusted" and Source-DI QRNG, and in Chapter 5 we employed this new tool to demonstrate that unbounded randomness generation, in a Source-DI scenario, is possible with finite-dimensional quantum systems. Finally in Chapter 6, we proposed a new implementation for a continuous-variable Semi-DI QRNG that doesn't require active phase stabilization, greatly simplifying the experimental realization.

In the second part of the thesis, we have focused on some critical problems of practical QKD implementations. The first problem, analyzed in Chapter 8, was related to the feasibility of daylight QKD at telecom wavelength in satellite applications. For this reason, we have developed, in collaboration with the Italian Space Agency (ASI), a complete e prototype for daylight free-space QKD at 1550 nm. The prototype has been tested with two transmitters: a fiber-based one, realized with only commercial components and a second one, developed in collaboration with Scuola Sant'Anna di Pisa, exploiting the Silicon Photonics technology. The prototype featured a single mode fiber injection system and superconducting nanowire

single photon detectors. We have tested it in a 145m long free space link in the urban area of Padova, from morning till evening. In both cases we have been able to obtain a secret key rate in the order of tens of kbps, showing that daylight QKD technology is mature enough to foresee the real application in satellite quantum communications. In Chapter 9, we have addressed the problem of stability in current transmitters for polarization encoded QKD. To solve the problem we have proposed and realized a new transmitter, called POGNAC and based on a Sagnac interferometer, that self-compensate external fluctuations and guarantees long-term stability and a low intrinsic error. Then in Chapter 10, we have studied the problem of time synchronization without any auxiliary time reference. To solve the problem we have developed a synchronization method that can be implemented directly in the quantum channel with a particular encoding and publicly announcing the initial stream of the qubits. We have implemented the protocol, employing the POGNAC, showing at the same time a record-low intrinsic QBER and the high robustness of the synchronization method with respect to losses. Finally, in Chapter 11 we have studied the problem of the post-selection loophole in setups employing time-bin entanglement, which poses severe limitations for the adoption of this scheme in DI-QKD. We have solved the problem developing a fast-switching optical scheme and a phase-locking mechanism that allowed us to violate the CHSH inequality without post-selection.

Appendices

APPENDIX A

SDP

This section on SDP is based on Watrous's Lecture Notes [273]- and all proofs can be found there.

A Semi-Definite Program] (SDP) is a triple $\{A, B, \Psi\}$, where $A \in \text{Herm}(\mathscr{H}_A), B \in \text{Herm}(\mathscr{H}_B)$ are Hermitian operators and Ψ is Hermiticy-preserving map from $\text{Herm}(\mathscr{H}_A)$ to $\text{Herm}(\mathscr{H}_B)$.

Then is possible to associate to the SDP the following two optimization problems:

$$\begin{array}{rll} & \underline{\text{primal problem}} & \underline{\text{dual problem}} \\ \texttt{minimize:} & \text{Tr}[AX] & \texttt{maximize:} \quad \text{Tr}[BY] \\ \texttt{subject to:} & \Psi[X] \geq B & \texttt{subject to:} \quad \Psi^\dagger[Y] \leq A \\ & X \geq 0 & \qquad\qquad\quad Y \geq 0 \end{array} \tag{A.1}$$

The primal problem is said to be *feasible* if exists a $X > 0$ that satisfies the constraint $\Psi[X] \geq B$. Similarly, the dual problem is *feasible* if exists a $Y > 0$ such that $\Psi^\dagger[Y] \leq A$. In such case the the optimal solution for the primal α and the dual β can be written as:

$$\alpha = \inf\{\langle A, X\rangle \text{st} X \geq 0,\ \Psi[X] \geq B\} \tag{A.2}$$

$$\beta = \sup\{\langle B, Y\rangle \text{st} Y \geq 0,\ \Psi^\dagger[Y] \leq A\} \tag{A.3}$$

with the convention that if the primal is infeasible $\alpha = -\infty$ while $\beta = \infty$ if the dual is infeasible.

Moreover, if $\Psi[X] - B \geq 0$ or $A - \Psi^\dagger[Y] \geq 0$, the respective formulation is said to be *strictly feasible*.

The two formulations are related to each other by a duality relation. In general we only have **weak duality**:

Theorem 1. *For any SDP, we have* $\alpha \geq \beta$

This implies that every dual problem provides a lower bound while the primal provides an upper bound.

For many interesting problems, however, a stronger relation holds called **strong duality**

Theorem 2. *If the primal and the dual are in the form of Eq A.3 and Slater's conditions holds then* $\alpha = \beta$

where the Slater's conditions are

- if the primal problem is feasible and the dual is strictly feasible, then strong duality holds and there exists a valid choice X for the primal problem with $\mathrm{Tr}[AX] = \alpha$
- if the dual problem is feasible and the primal is strictly feasible, then strong duality holds and there exists a valid choice Y for the dual problem with $\mathrm{Tr}[BY] = \beta$
- f both problems are strictly feasible, then strong duality holds and there exist valid choices of X and Y with $\alpha = \beta = \mathrm{Tr}[AX] = \mathrm{Tr}[BY]$

The advantage of SDP is that these optimization problems can be efficiently solved numerically and are guararantee to converge to the global optimum.

APPENDIX B

Results of statistical tests

The following table present the results of the statistical test suite for the Soruce-DI heterodyne QRNG presented in Chap 3

Test's name	P-value	Result
diehard birthdays	0.398	PASSED
diehard operm5	0.391	PASSED
diehard rank 32x32	0.414	PASSED
diehard rank 6x8	0.767	PASSED
diehard bitstream	0.529	PASSED
diehard opso	0.655	PASSED
diehard oqso	0.758	PASSED
diehard dna	0.731	PASSED
diehard count 1s str	0.482	PASSED
diehard count 1s byt	0.361	PASSED
diehard parking lot	0.515	PASSED
diehard 2dsphere	0.484	PASSED
diehard 3dsphere	0.739	PASSED
diehard squeeze	0.580	PASSED
diehard sums	0.140	PASSED
diehard runs	0.478	PASSED
diehard runs	0.316	PASSED
diehard craps	0.348	PASSED
diehard craps	0.937	PASSED
marsaglia tsang gcd	0.504	PASSED
marsaglia tsang gcd	0.444	PASSED
sts monobit	0.204	PASSED
sts runs	0.716	PASSED
sts serial	0.151	PASSED
rgb bitdist	0.056	PASSED
rgb minimum distance	0.043	PASSED
rgb permutations	0.068	PASSED
rgb lagged sum	0.019	PASSED

Table B.1: *Result of Dieharder test suite on the extracted random numbers. In the case of multiple tests in a category, the smallest have been reported.*

Test's name	P-value	Result
Frequency	0.980	PASSED
BlockFrequency	0.323	PASSED
CumulativeSums	0.819	PASSED
CumulativeSums	0.265	PASSED
Runs	0.187	PASSED
LongestRun	0.864	PASSED
Rank	0.372	PASSED
DFT	0.341	PASSED
NonOverlapping	0.016	PASSED
Overlapping	0.748	PASSED
Universal	0.381	PASSED
ApproximateEntropy	0.509	PASSED
RandomExcursions(RE)	0.315	PASSED
RE Variant	0.047	PASSED
Serial	0.318	PASSED
LinearComplexity	0.373	PASSED

Table B.2: *Result of NIST test suite on the extracted random numbers. In the case of multiple tests in a category, the smallest have been reported.*

Ringraziamenti

Vorrei innanzitutto ringraziare il mio supervisore prof. Giuseppe Vallone, o semplicemente Pino, per il suo supporto, per la sua guida costante e per la passione incontenibile che in questi anni mi ha trasmesso. Un grazie al prof. Paolo Villoresi per avermi dato la possibilità di lavorare in questo incredibile gruppo, per la sua instancabile dedizione e per avermi insegnato che, se lo si vuole, alla fine una soluzione la si trova sempre.

Un ringraziamento speciale va poi a tutti i compagni di laboratorio che in questi anni hanno contribuito a rendere il Luxor una seconda casa: un grazie a Davide Giacomo che mi ha insegnato tutto, a Matteo anche se provava ad hackerarmi il PC, a Tommasin per l'elettronica alternativa, ad Albertone per la sua enrgia inesauribile e all'ASI expert anche se non mi ha ancora portato sulle mini-moto. Un grazie a Cesco, ormai un fratello, che senza di lui avrei chiuso baracca subito (semi-cit). Un grazie ad Andrea ed al suo idraulico, a Costa e a tutte le sue viti che non sono mai riuscito a svitare, a Luca che mi fa vergognare per quanto sono brutti i miei codici, all'Alessia che per fortuna ci tiene tutti in riga, a Giulio che ha scelto il *Secret Hitler*. A thank to Mujtaba for the endless discussions about any possible physical phenomena and Hamid for having listened to all my *random* theories. Un grazie a Mirko, il miglior boy-scout che si può avere in Candada. Un grazie anche al buon Davide Bacco: *C*arismatico, *U*nico, *E*legante ed *A*tletico. Un grazie poi agli altri abitanti del Luxor: Tex per le perle di saggezza, Donazzan che ci comprava i gelati e l'Alessandra che porta sempre l'allegria (anche troppa).

Come non ringraziare tutte le varie missioni, **LA** Matera in particolare, in cui alla fine ci siamo sempre divertiti un casino.

Un grazie agli amici di Verona, che ancora mi sopportano quelle poche volte che torno: un grazie all' l'Ander che alla fine mi ha stampato in 3D mezzi esperimenti, a Ippo la Giò e il piccolo Lori che ci sfamano a cena, al Piga per i discorsi sul C++ dopo le birre, al Charlie che ha sempre una serie nuova, alla Sara e al Simo che devo ancora andare a trovare, alla Zaffa che ci mette sempre casa, alla Chiara che prima o poi finirà il dottorato anche per te, al Sap quando esce, ad Elia che non so come fa a piacerti l'Americano.

Un grazie ai Tonnorandi (ormai Tonnorati), Rave Carlo e Marco, per tutti gli scozzini multi-country e per le risposte ad ogni dubbio accademico ed esistenziale.

Un grazie a Giacomino (e alle sue camicie blu), che mi deve ancora portare a pescare, a Luca, la Vale ed il Baz, per le birrette agli Amici.

Un grazie alle mie ex coinquiline, ma tuttora onnipresenti, Giulia e Chiara, per tutte le risate e per riuscire a non farci parlare sempre e solo di fisica.

Un grazie speciale ad Olimpia (e Lou), per tutto il tempo che questo dottorato le ha tolto ma per essere stata al mio fianco, sempre.

Infine voglio ringraziare la mia famiglia ed i miei genitori, Luciana e Gabriele, che mi hanno sempre sostenuto in tutto.

Bibliography

[1] M. Avesani et al., "Source-device-independent heterodyne-based quantum random number generator at 17 Gbps", Nature Communications **9**, 5365 (2018) (cit. on pp. 2, 6, 38, 61).

[2] M. Avesani et al., "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics", arXiv e-prints **1907**, 10039 (2019) (cit. on pp. 3, 109, 146, 148, 154).

[3] C. Agnesi et al., "All-fiber self-compensating polarization encoder for quantum key distribution", Optics Letters **44**, 2398 (2019) (cit. on pp. 3, 110, 141, 147).

[4] L. Calderaro et al., "Fast and simple qubit-based synchronization for quantum key distribution", ArXiv e-prints **1909**, 12050 (2019) (cit. on pp. 4, 147, 148, 153).

[5] C. Agnesi et al., "Simple Quantum Key Distribution with qubit-based synchronization and a self-compensating polarization encoder", ArXiv e-prints **1909**, 12703 (2019) (cit. on pp. 4, 147).

[6] F. Vedovato et al., "Postselection-loophole-free Bell violation with genuine time-bin entanglement", Physical Review Letters **121**, 190401 (2018) (cit. on pp. 4, 157).

[7] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Vol. 52, 6 (Cambridge University Press, Cambridge, Nov. 2010), pp. 604–605 (cit. on p. 14).

[8] A. Weinmann et al., "Quantum Mechanics (Non-Relativistic Theory)", The Mathematical Gazette **43**, 305 (1959) (cit. on p. 14).

[9] A. Peres and L. E. Ballentine, "Quantum Theory: Concepts and Methods", American Journal of Physics **63**, 285–286 (1995) (cit. on p. 14).

[10] R. Renner, *Quantum Information Theory*, tech. rep. (2013) (cit. on p. 14).

[11] J. M. Renes, *Quantum Information Theory*, tech. rep. (2015) (cit. on p. 14).

[12] B. Hans-A, T. C. Ralph, and E. Edition, *A Guide to Experiments in Quantum Optics*, edited by H. Bachor and T. C. Ralph (Wiley, Jan. 2004) (cit. on p. 14).

[13] U. Leonhardt, *Measuring the quantum state of light*, Vol. 22 (Cambridge university press, 1997) (cit. on pp. 14, 39, 40, 42).

[14] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned", Nature **299**, 802 (1982) (cit. on p. 17).

[15] V. Bu žek and M. Hillery, "Quantum copying: beyond the no-cloning theorem", Phys. Rev. A **54**, 1844–1852 (1996) (cit. on p. 18).

[16] A. Einstein, B. Podolsky, and N. Rosen, "Can Quantum-Mechanical Description of Reality Be Considered Complete?", Physical Review **47**, 2–5 (1935) (cit. on p. 20).

[17] J. S. Bell, "On the Einstein Podolsky Rosen paradox", Physics Physique Fizika **1**, 195–200 (1964) (cit. on pp. 20, 155).

[18] S. J. Freedman and J. F. Clauser, "Experimental Test of Local Hidden-Variable Theories", Physical Review Letters **28**, 938–941 (1972) (cit. on p. 20).

[19] A. Aspect, P. Grangier, and G. Roger, "Experimental Tests of Realistic Local Theories via Bell's Theorem", Physical Review Letters **47**, 460–463 (1981) (cit. on p. 20).

[20] A. Aspect, J. Dalibard, and G. Roger, "Experimental Test of Bell's Inequalities Using Time- Varying Analyzers", Physical Review Letters **49**, 1804–1807 (1982) (cit. on p. 20).

[21] B. Hensen et al., "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres", Nature **526**, 682–686 (2015) (cit. on pp. 20, 25, 155, 157).

[22] M. Giustina et al., "Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons", Physical Review Letters **115**, 250401 (2015) (cit. on pp. 20, 25, 155, 157).

[23] L. K. Shalm et al., "Strong Loophole-Free Test of Local Realism", Physical Review Letters **115**, 250402 (2015) (cit. on pp. 20, 25, 155, 157).

[24] W. Rosenfeld et al., "Event-Ready Bell Test Using Entangled Atoms Simultaneously Closing Detection and Locality Loopholes", Physical Review Letters (2017) 10.1103/PhysRevLett.119.010402 (cit. on pp. 20, 155, 157).

[25] J. F. Clauser and M. a. Horne, "Experimental consequences of objective local theories", Physical Review D **10**, 526–535 (1974) (cit. on p. 20).

[26] B. Cirel'son, "Quantum generalizations of bell's inequality", English, Letters in Mathematical Physics **4**, 93–100 (1980) (cit. on p. 23).

[27] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators", Reviews of Modern Physics **89**, 15004 (2017) (cit. on p. 25).

[28] X. Ma et al., "Quantum random number generation", npj Quantum Information **2**, 16021 (2016) (cit. on pp. 25, 37, 56).

[29] D. Eastlake, J. Schiller, and S. Crocker, *Randomness Requirements for Security*, tech. rep. (June 2005) (cit. on p. 25).

[30] T. H. Click, A. Liu, and G. A. Kaminski, "Quality of random number generators significantly affects results of Monte Carlo simulations for organic and biological systems", Journal of Computational Chemistry (2011) 10.1002/jcc.21638 (cit. on p. 25).

[31] A. M. Ferrenberg, D. P. Landau, and Y. J. Wong, "Monte Carlo simulations: Hidden errors from good random number generators", Physical Review Letters (1992) 10.1103/PhysRevLett.69.3382 (cit. on p. 25).

[32] I. Goldberg and D. Wagner, "Randomness and the netscape browser", Dr Dobb's Journal-Software Tools for the Professional Programmer **21**, 66–71 (1996) (cit. on p. 25).

[33] N. Heninger et al., "Mining your Ps and Qs: detection of widespread weak keys in network devices", USENIX Security Symposium (2012) (cit. on p. 25).

[34] E. B. Barker and J. M. Kelsey, *Recommendation for random number generation using deterministic random bit generators*, tech. rep. (National Institute of Standards and Technology, Gaithersburg, MD, 2012) (cit. on p. 25).

[35] D. J. Bernstein, T. Lange, and R. Niederhagen, "Dual ec: a standardized back door", in *The new codebreakers* (Springer, 2016), pp. 256–281 (cit. on p. 25).

[36] G. T. Becker et al., "Stealthy dopant-level hardware Trojans: Extended version", Journal of Cryptographic Engineering **4**, 19–31 (2014) (cit. on p. 25).

[37] P. Hellekalek, "Good random number generators are (not so) easy to find", Mathematics and Computers in Simulation (1998) 10.1016/s0378-4754(98)00078-0 (cit. on p. 26).

[38] L. E. Bassham et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications", (2010) 10.6028/NIST.SP.800-22r1a (cit. on pp. 26, 53).

[39] R. Brown, D. Eddelbuettel, and D. Bauer, *Dieharder: A random number test suite* (2011) (cit. on pp. 26, 53).

[40] P. L'Ecuyer and R. Simard, "TestU01", ACM Transactions on Mathematical Software (2007) 10.1145/1268776.1268777 (cit. on p. 26).

[41] Z. Huang and H. Chen, "A truly random number generator based on thermal noise", in International conference on asic, proceedings (2001), pp. 862–864 (cit. on p. 26).

[42] M. Majzoobi, F. Koushanfar, and S. Devadas, "FPGA-based true random number generation using circuit metastability with adaptive feedback control", in Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics) (2011) (cit. on p. 26).

[43] J. von Neumann, "Various techniques used in connection with random digits", in *Monte carlo method*, Vol. 12, edited by A. S. Householder, G. E. Forsythe, and H. H. Germond, National Bureau of Standards Applied Mathematics Series (US Government Printing Office, Washington, DC, 1951) Chap. 13, pp. 36–38 (cit. on p. 26).

[44] M. Blum, "Independent unbiased coin flips from a correlated biased source-A finite state markov chain", Combinatorica (1986) 10.1007/BF02579167 (cit. on p. 26).

[45] Y. Peres, “Iterating Von Neumann’s Procedure for Extracting Random Bits”, The Annals of Statistics (2007) 10.1214/aos/1176348543 (cit. on pp. 26, 157).

[46] H. Zhou and J. Bruck, “Efficient generation of random bits from finite state Markov chains”, IEEE Transactions on Information Theory (2012) 10.1109/TIT.2011.2175698 (cit. on p. 26).

[47] M. Isida and H. Ikeda, “Random number generator”, Annals of the Institute of Statistical Mathematics **8**, 119–126 (1956) (cit. on p. 27).

[48] C. H. Vincent, “The generation of truly random binary numbers”, Journal of Physics E: Scientific Instruments (1970) 10.1088/0022-3735/3/8/303 (cit. on p. 27).

[49] J. G. Rarity, P. C. Owens, and P. R. Tapster, “Quantum random-number generation and key sharing”, Journal of Modern Optics **41**, 2435–2444 (1994) (cit. on p. 27).

[50] M. Stipčević and B. M. Rogina, “Quantum random number generator based on photonic emission in semiconductors”, Review of Scientific Instruments (2007) 10.1063/1.2720728 (cit. on p. 28).

[51] J. F. Dynes et al., “A high speed, postprocessing free, quantum random number generator”, Applied Physics Letters (2008) 10.1063/1.2961000 (cit. on p. 28).

[52] M. Fürst et al., “High speed optical quantum random number generation”, Optics Express (2010) 10.1364/oe.18.013029 (cit. on p. 28).

[53] M. Wahl et al., “An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements”, Applied Physics Letters (2011) 10.1063/1.3578456 (cit. on p. 28).

[54] Q. Yan et al., “Multi-bit quantum random number generation by measuring positions of arrival photons”, Review of Scientific Instruments (2014) 10.1063/1.4897485 (cit. on p. 28).

[55] D. G. Marangon et al., “Enhanced security for multi-detector quantum random number generators”, Quantum Science and Technology **1** (2016) 10.1088/2058-9565/1/1/015005 (cit. on p. 28).

[56] M. Ren et al., “Quantum random-number generator based on a photon-number-resolving detector”, Physical Review A - Atomic, Molecular, and Optical Physics (2011) 10.1103/PhysRevA.83.023820 (cit. on p. 28).

[57] B. Sanguinetti et al., “Quantum random number generation on a mobile phone”, Physical Review X (2014) 10.1103/PhysRevX.4.031056 (cit. on p. 28).

[58] M. J. Applegate et al., “Efficient and robust quantum random number generation by photon number detection”, Applied Physics Letters (2015) 10.1063/1.4928732 (cit. on p. 28).

[59] C. Gabriel et al., “A generator for unique quantum random numbers based on vacuum states”, Nature Photonics **4**, 711–715 (2010) (cit. on pp. 28, 37).

[60] B. Qi et al., “High-speed quantum random number generation by measuring phase noise of a single-mode laser”, Optics Letters (2010) 10.1364/ol.35.000312 (cit. on p. 28).

[61] C. Abellán et al., "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode", Optics Express **22**, 1645 (2014) (cit. on p. 28).

[62] Y. Q. Nie et al., "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations", Review of Scientific Instruments **86**, 063105 (2015) (cit. on p. 28).

[63] ID Quantique, *Random Number Generation using Quantum Physics*, 2010 (cit. on p. 28).

[64] *Quantum Random Number*, http://www.micro-photon-devices.com/Products/Instrumentation/Quantum-Random-Number (cit. on p. 28).

[65] *qStream Quantum Random Number Generator*, https://www.quintessencelabs.com/products/qstream-quantum-true-random-number-generator/ (cit. on p. 28).

[66] *PQRNG 150*, https://www.picoquant.com/scientific/product-studies/pqrng-150-product-study (cit. on p. 28).

[67] R. Colbeck, "Quantum And Relativistic Protocols For Secure Multi-Party Computation", ArXiv e-prints **0911**, 3814 (2009) (cit. on p. 29).

[68] R. Colbeck and A. Kent, "Private randomness expansion with untrusted devices", Journal of Physics A: Mathematical and Theoretical **44**, 095305 (2011) (cit. on p. 29).

[69] S. Pironio and S. Massar, "Security of practical private randomness generation", Physical Review A - Atomic, Molecular, and Optical Physics (2013) 10.1103/PhysRevA.87.012336 (cit. on p. 29).

[70] S. Pironio et al., "Random numbers certified by Bellĝs theorem", Nature (2010) 10.1038/nature09008 (cit. on p. 29).

[71] R. Colbeck and R. Renner, "Free randomness can be amplified", Nature Physics **8**, 450–453 (2012) (cit. on p. 29).

[72] M. Kessler and R. Arnon-Friedman, "Device-independent Randomness Amplification and Privatization", ArXiv e-prints **1705**, 04148 (2017) (cit. on p. 29).

[73] F. Dupuis, O. Fawzi, and R. Renner, "Entropy accumulation", arXiv:1607.01796 [quant-ph] (2016) (cit. on p. 29).

[74] Y. Liu et al., "Device-independent quantum random-number generation", Nature **562**, 548–551 (2018) (cit. on p. 29).

[75] P. Bierhorst et al., "Experimentally generated randomness certified by the impossibility of superluminal signals", Nature (2018) 10.1038/s41586-018-0019-0 (cit. on p. 29).

[76] T. Lunghi et al., "Self-Testing Quantum Random Number Generator", Physical Review Letters **114**, 150501 (2015) (cit. on pp. 29, 37, 43, 92).

[77] G. Cañas et al., "Experimental quantum randomness generation invulnerable to the detection loophole", ArXiv e-prints, 1–6 (2014) (cit. on pp. 29, 37).

[78] G. Vallone et al., "Quantum randomness certified by the uncertainty principle", Physical Review A - Atomic, Molecular, and Optical Physics **90**, 052327 (2014) (cit. on pp. 29, 37, 40, 56, 69–71, 73, 89).

[79] D. G. Marangon, G. Vallone, and P. Villoresi, "Source-Device-Independent Ultrafast Quantum Random Number Generation", Physical Review Letters **118**, 060503 (2017) (cit. on pp. 29, 37, 43, 56).

[80] Z. Cao et al., "Source-independent quantum random number generation", Physical Review X **6**, 11020 (2016) (cit. on pp. 29, 37, 75).

[81] F. Xu, J. H. Shapiro, and F. N. C. Wong, "Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring", Optica **3**, 1266 (2016) (cit. on pp. 29, 37).

[82] S. Gómez et al., "Experimental nonlocality-based randomness generation with nonprojective measurements", Physical Review A **97** (2018) 10.1103/PhysRevA.97.040102 (cit. on pp. 29, 37, 74).

[83] Z. Cao, H. Zhou, and X. Ma, "Loss-tolerant measurement-device-independent quantum random number generation", New Journal of Physics **17** (2015) 10.1088/1367-2630/17/12/125011 (cit. on pp. 29, 37, 92).

[84] T. V. Himbeeck et al., "Semi-device-independent framework based on natural physical assumptions", Quantum **1**, 33 (2017) (cit. on pp. 29, 37, 92, 93).

[85] J. B. Brask et al., "Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination", Physical Review Applied **7**, 054018 (2017) (cit. on pp. 29, 37, 43, 92–94, 100).

[86] D. Rusca et al., "Practical self-testing quantum random number generator based on an energy bound", ArXiv e-prints **1904**, 04819 (2019) (cit. on pp. 29, 37, 92, 93, 100).

[87] T. Van Himbeeck and S. Pironio, "Correlations and randomness generation based on energy constraints", ArXiv e-prints **1905**, 09117 (2019) (cit. on pp. 29, 37, 92, 93).

[88] C. E. Shannon, "Communication Theory of Secrecy Systems", Bell System Technical Journal **28**, 656–715 (1949) (cit. on p. 30).

[89] R. König, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy", IEEE Transactions on Information Theory **55**, 4337–4347 (2009) (cit. on pp. 31, 40, 61).

[90] A. Vitanov et al., "Chain rules for smooth min-and max-entropies", IEEE Transactions on Information Theory (2013) 10.1109/TIT.2013.2238656 (cit. on p. 31).

[91] R. Renner, "Security of Quantum Key Distribution", IEEE Access **4**, 724–749 (2005) (cit. on pp. 32, 40, 103, 107).

[92] P. Faist, "Quantum coarse-graining: an information-theoretic approach to thermodynamics", arXiv preprint arXiv:1607.03104 (2016) (cit. on p. 33).

[93] D. Frauchiger, R. Renner, and M. Troyer, "True randomness from realistic quantum devices", ArXiv e-prints (2013) (cit. on pp. 32, 51).

[94] L. Trevisan, "Extractors and pseudorandom generators", Journal of the ACM **48**, 860–879 (2001) (cit. on p. 35).

[95] A. De and T. Vidick, "Near-optimal extractors against quantum storage", in Proceedings of the 42nd acm symposium on theory of computing - stoc '10 (2010), p. 161 (cit. on p. 35).

[96] M. Tomamichel et al., "Leftover Hashing Against Quantum Side Information", IEEE Transactions on Information Theory **57**, 5524–5535 (2011) (cit. on pp. 35, 36, 40, 103).

[97] J. L. Carter and M. N. Wegman, "Universal classes of hash functions", Journal of Computer and System Sciences (1979) 10.1016/0022-0000(79)90044-8 (cit. on pp. 36, 107).

[98] N. Lord, G. H. Golub, and C. F. V. Loan, "Matrix Computations", The Mathematical Gazette (2007) 10.2307/3621013 (cit. on p. 36).

[99] T. Gehring et al., "8 GBit/s real-time quantum random number generator with non-iid samples", ArXiv e-prints 1812.05377 (2018) (cit. on pp. 36, 56).

[100] J. Řeháček et al., "Surmounting intrinsic quantum-measurement uncertainties in Gaussian-state tomography with quadrature squeezing", Scientific Reports **5**, 12289 (2015) (cit. on p. 37).

[101] C. R. Müller et al., "Evading Vacuum Noise: Wigner Projections or Husimi Samples?", Physical Review Letters **117**, 70801 (2016) (cit. on p. 37).

[102] E. Arthurs and J. L. Kelly, "On the Simultaneous Measurement of a Pair of Conjugate Observables", Bell System Technical Journal **44**, 725–729 (1965) (cit. on p. 38).

[103] N. G. Walker, "Quantum theory of multiport optical homodyning", Journal of Modern Optics **34**, 15–60 (1987) (cit. on p. 38).

[104] A. Franzen, "ComponentLibrary", SVG library (2006) (cit. on p. 38).

[105] X. Ma et al., "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction", Physical Review A - Atomic, Molecular, and Optical Physics **87**, 62327 (2013) (cit. on p. 39).

[106] F. Furrer et al., "Min- and Max-Entropy in Infinite Dimensions", Communications in Mathematical Physics **306**, 165–186 (2011) (cit. on p. 40).

[107] F. Furrer et al., "Position-momentum uncertainty relations in the presence of quantum memory", Journal of Mathematical Physics **55**, 122205 (2014) (cit. on pp. 40, 41).

[108] M. Fiorentino et al., "Secure self-calibrating quantum random-bit generator", Physical Review A **75**, 032334 (2007) (cit. on pp. 43, 67, 68, 73, 75).

[109] *Coh24 coherent receiver*, http://kylia.com/kylia/wp-content/uploads/2015/02/datasheet-COH-V1.2.pdf (cit. on p. 47).

[110] N. Wiener et al., "Generalized harmonic analysis", Acta mathematica **55**, 117–258 (1930) (cit. on p. 51).

[111] A. Khintchine, "Korrelationstheorie der stationären stochastischen prozesse", Mathematische Annalen **109**, 604–615 (1934) (cit. on p. 51).

[112] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, "Numerical approach for unstructured quantum key distribution", Nature Communications **7**, 11712 (2016) (cit. on p. 58).

[113] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states", Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **461**, 207–235 (2005) (cit. on p. 58).

[114] P. J. Coles, "Unification of different views of decoherence and discord", Physical Review A - Atomic, Molecular, and Optical Physics **85** (2012) 10.1103/PhysRevA.85.042103 (cit. on p. 59).

[115] M. Zorzi, F. Ticozzi, and A. Ferrante, "Minimum Relative Entropy for Quantum Estimation: Feasibility and General Solution", IEEE Transactions on Information Theory **60**, 357–367 (2014) (cit. on p. 60).

[116] W. Hoeffding, "Probability Inequalities for Sums of Bounded Random Variables", Journal of the American Statistical Association **58**, 13–30 (1963) (cit. on pp. 63, 88).

[117] K. Azuma, "Weighted sums of certain dependent random variables", Tohoku Mathematical Journal (1967) 10.2748/tmj/1178243286 (cit. on p. 63).

[118] G. Sagnol et al., "Picos, a python interface to conic optimization solvers", in Proceedings of the in 21st international symposium on mathematical programming (2012) (cit. on p. 68).

[119] A. Mosek, "The mosek optimization software", Online at http://www. mosek. com **54**, 5 (cit. on p. 68).

[120] J. R. Johansson, P. D. Nation, and F. Nori, "QuTiP 2: A Python framework for the dynamics of open quantum systems", Computer Physics Communications (2013) 10.1016/j.cpc.2012.11.019 (cit. on p. 68).

[121] F. Johansson et al., *Mpmath: a Python library for arbitrary-precision floating-point arithmetic (version 0.18)*, http://mpmath.org/ (Dec. 2013) (cit. on p. 70).

[122] M. Nakata, "A numerical evaluation of highly accurate multiple-precision arithmetic version of semidefinite programming solver: sdpa-gmp,-qd and-dd.", in 2010 ieee international symposium on computer-aided control system design (IEEE, 2010), pp. 29–34 (cit. on p. 70).

[123] P. J. Coles and M. Piani, "Improved entropic uncertainty relations and information exclusion relations", Physical Review A - Atomic, Molecular, and Optical Physics **89**, 1–11 (2014) (cit. on p. 70).

[124] A. Acín et al., "Optimal randomness certification from one entangled bit", Physical Review A **93** (2016) 10.1103/PhysRevA.93.040102 (cit. on p. 74).

[125] O. Andersson et al., "Device-independent certification of two bits of randomness from one entangled bit and Gisin's elegant Bell inequality", Physical Review A **97** (2018) 10.1103/PhysRevA.97.012314 (cit. on p. 74).

[126] F. J. Curchod et al., “Unbounded randomness certification using sequences of measurements”, Physical Review A **95**, 020102 (2017) (cit. on p. 74).

[127] T. Kim, M. Fiorentino, and F. N. C. Wong, “Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer”, Physical Review A **73**, 012316 (2006) (cit. on p. 85).

[128] R. B. Clarke et al., “Experimental realization of optimal detection strategies for overcomplete states”, Physical Review A. Atomic, Molecular, and Optical Physics **64**, 123031–1230313 (2001) (cit. on p. 86).

[129] M. Schiavon, G. Vallone, and P. Villoresi, “Experimental realization of equiangular three-state quantum key distribution”, Scientific Reports **6** (2016) 10.1038/srep30089 (cit. on p. 86).

[130] J. M. Renes et al., “Symmetric informationally complete quantum measurements”, Journal of Mathematical Physics **45**, 2171–2180 (2004) (cit. on p. 87).

[131] N. Dalla Pozza and M. G. Paris, “Naimark extension for the single-photon canonical phase measurement”, Physical Review A **100**, 1–7 (2019) (cit. on p. 87).

[132] Z. Hradil, “Quantum-state estimation”, Physical Review A - Atomic, Molecular, and Optical Physics **55**, R1561–R1564 (1997) (cit. on p. 88).

[133] P. Faist and R. Renner, “Practical and Reliable Error Bars in Quantum Tomography”, Physical Review Letters **117** (2016) 10.1103/PhysRevLett.117.010404 (cit. on p. 88).

[134] Y. Q. Nie et al., “Experimental measurement-device-independent quantum random-number generation”, Physical Review A **94** (2016) 10.1103/PhysRevA.94.060301 (cit. on p. 92).

[135] F. Bischof, H. Kampermann, and D. Bruß, “Measurement-device-independent randomness generation with arbitrary quantum states”, Physical Review A **95**, 062305 (2017) (cit. on p. 92).

[136] M. Avesani, “Security of quantum protocols certified by the dimension of the hilbert space”, (2015) (cit. on p. 92).

[137] N. Brunner et al., “Dimension of physical systems, information processing, and thermodynamics”, New Journal of Physics **16** (2014) 10.1088/1367-2630/16/12/123050 (cit. on p. 93).

[138] O. Nieto-Silleras, S. Pironio, and J. Silman, “Using complete measurement statistics for optimal device-independent randomness evaluation”, New Journal of Physics (2014) 10.1088/1367-2630/16/1/013035 (cit. on p. 93).

[139] D. Rusca et al., “Fast and practical implementation of self-testing qrng based on an energy bound”, in *Qcrypt 2019, montreal, canada* (2019) (cit. on pp. 93, 100).

[140] J. D. Bancal, L. Sheridan, and V. Scarani, “More randomness from the same data”, New Journal of Physics (2014) 10.1088/1367-2630/16/3/033011 (cit. on p. 94).

[141] finisar, *100 GHz balanced detector*, https://www.finisar.com/communication-components/bpdv412xr (cit. on p. 101).

[142] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", in Proceedings 35th annual symposium on foundations of computer science (), pp. 124–134 (cit. on p. 103).

[143] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing", in *Proc. of ieee int. conf. on comp., syst. and signal proc., bangalore, india, dec. 10-12, 1984* (1984) (cit. on p. 103).

[144] IdQuantique, *Quantum Safe Security* (cit. on p. 103).

[145] N. Gisin et al., "Quantum Cryptography", Review of Modern Physics", Reviews of Modern Physics **74**, 145–195 (2002) (cit. on pp. 103, 155).

[146] V. Scarani and R. Renner, "Security bounds for quantum cryptography with finite resources", in Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), Vol. 5106 LNCS, 20 (May 2008), pp. 83–95 (cit. on p. 103).

[147] S. Pirandola et al., "Advances in Quantum Cryptography", ArXiv e-prints **1906**, 01645 (2019) (cit. on p. 103).

[148] C. E. Shannon, "A Mathematical Theory of Communication", Bell System Technical Journal (1948) 10.1002/j.1538-7305.1948.tb01338.x (cit. on p. 104).

[149] S. Wiesner, "Conjugate coding", ACM SIGACT News **15**, 78–88 (1983) (cit. on p. 104).

[150] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing", Theoretical Computer Science **560, Part 1**, Theoretical Aspects of Quantum Cryptography – celebrating 30 years of {BB84}, 7–11 (2014) (cit. on pp. 104, 140, 143).

[151] A. K. Ekert, "Quantum cryptography based on Bell's theorem", Physical Review Letters **67**, 661–663 (1991) (cit. on p. 105).

[152] U. Vazirani and T. Vidick, "Fully device-independent quantum key distribution", Phys. Rev. Lett. **113**, 140501 (2014) (cit. on p. 105).

[153] Swissquantum, *BB84 protocol* (cit. on p. 105).

[154] H. K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution", Physical Review Letters (2005) 10.1103/PhysRevLett.94.230504 (cit. on pp. 105, 108).

[155] D. Mayers, "Quantum key distribution and string oblivious transfer in noisy channels", in Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics) (1996) (cit. on p. 106).

[156] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol", Physical Review Letters **85**, 441–444 (2000) (cit. on p. 106).

[157] M. Tomamichel et al., "Tight finite-key analysis for quantum cryptography", Nature Communications **3**, 634 (2012) (cit. on p. 107).

[158] V. Scarani et al., "The security of practical quantum key distribution", Reviews of Modern Physics **81**, 1301–1350 (2009) (cit. on p. 107).

[159] A. Acín, N. Gisin, and L. Masanes, "From Bell's theorem to secure quantum key distribution", Physical Review Letters **97**, 120405 (2006) (cit. on pp. 107, 155, 164).

[160] X. Ma et al., "Practical Decoy State for Quantum Key Distribution", Physical Review A **72**, 1–15 (2005) (cit. on p. 108).

[161] N. Gisin et al., "Trojan-horse attacks on quantum-key-distribution systems", Physical Review A **73**, 022320 (2006) (cit. on p. 108).

[162] L. Lydersen et al., "Hacking commercial quantum cryptography systems by tailored bright illumination", Nature Photon **4**, 5 (2010) (cit. on p. 108).

[163] C. C. W. Lim et al., "Random variation of detector efficiency: A countermeasure against detector blinding attacks for quantum key distribution", IEEE Journal on Selected Topics in Quantum Electronics **21** (2015) 10.1109/JSTQE.2015.2389528 (cit. on p. 108).

[164] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution", Physical Review Letters **108** (2012) 10.1103/PhysRevLett.108.130502 (cit. on p. 108).

[165] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution", Phys. Rev. Lett. **108**, 130503 (2012) (cit. on p. 108).

[166] A. Boaron et al., "Secure Quantum Key Distribution over 421 km of Optical Fiber", Phys. Rev. Lett. **121**, 190502 (2018) (cit. on pp. 110, 111, 138).

[167] M. Lucamarini et al., "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters", Nature **557**, 400–403 (2018) (cit. on p. 110).

[168] S. Pirandola et al., "Fundamental limits of repeaterless quantum communications", Nature Communications **8** (2017) 10.1038/ncomms15043 (cit. on p. 110).

[169] M. Minder et al., "Experimental quantum key distribution beyond the repeaterless secret key capacity", Nature Photonics **13**, 334–338 (2019) (cit. on p. 110).

[170] Y. Liu et al., "Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending", Physical Review Letters **123**, 100505 (2019) (cit. on p. 110).

[171] X. Zhong et al., "Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution", Physical Review Letters **123**, 100506 (2019) (cit. on p. 110).

[172] N. Sangouard et al., "Quantum repeaters based on atomic ensembles and linear optics", Reviews of Modern Physics **83**, 33–80 (2011) (cit. on p. 110).

[173] S.-K. Liao et al., "Satellite-to-ground quantum key distribution", Nature **549**, 43–47 (2017) (cit. on pp. 110, 141, 146, 154).

[174] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution", npj Quantum Inf. **3**, 30 (2017) (cit. on p. 110).

[175] C. Agnesi et al., "Exploring the boundaries of quantum mechanics: advances in satellite quantum communications", Philos. Trans. Royal Soc. A **376**, 20170461 (2018) (cit. on p. 110).

[176] I. Khan et al., “Satellite-Based QKD”, Opt. Photon. News **29**, 26 (2018) (cit. on p. 110).

[177] K.-I. Yoshino et al., “Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days”, Opt. Express **21**, 31395 (2013) (cit. on pp. 110, 138).

[178] N. T. Islam et al., “Provably secure and high-rate quantum key distribution with time-bin qudits”, Science Advances **3**, e1701491 (2017) (cit. on pp. 110, 111).

[179] Z. Yuan et al., “10-Mb/s Quantum Key Distribution”, J. Light. Technol. **36**, 3427–3433 (2018) (cit. on pp. 110, 138).

[180] M. Peev et al., “The SECOQC quantum key distribution network in Vienna”, New Journal of Physics **11**, 75001 (2009) (cit. on p. 110).

[181] M. Sasaki et al., “Field test of quantum key distribution in the Tokyo QKD Network”, Opt. Express **19**, 10387–10409 (2011) (cit. on p. 110).

[182] H. J. Kimble, “The quantum internet”, Nature **453**, 1023–1030 (2008) (cit. on pp. 110, 138, 164).

[183] S. Wehner, D. Elkouss, and R. Hanson, “Quantum internet: A vision for the road ahead”, Science **362**, eaam9288 (2018) (cit. on pp. 110, 138).

[184] W. T. Buttler et al., “Daylight Quantum Key Distribution over 1.6 km”, Phys. Rev. Lett. **84**, 5652–5655 (2000) (cit. on pp. 110, 138).

[185] R. J. Hughes et al., “Practical free-space quantum key distribution over 10 km in daylight and at night”, New J. Phys. **4**, 43 (2002) (cit. on pp. 110, 138).

[186] M. P. Peloso et al., “Daylight operation of a free space, entanglement-based quantum key distribution system”, New J. Phys. **11**, 45007 (2009) (cit. on pp. 110, 138).

[187] H. Ko et al., “Experimental filtering effect on the daylight operation of a free-space quantum key distribution”, Sci. Rep. **8**, 15315 (2018) (cit. on pp. 110, 138).

[188] S.-K. K. Liao et al., “Long-distance free-space quantum key distribution in daylight towards inter-satellite communication”, Nature Photonics **11**, 509–513 (2017) (cit. on pp. 110, 138, 141, 154).

[189] Y.-H. Gong et al., “Free-space quantum key distribution in urban daylight with the SPGD algorithm control of a deformable mirror”, Opt. Express **26**, 18897 (2018) (cit. on pp. 110, 138).

[190] C. Ma et al., “Silicon photonic transmitter for polarization-encoded quantum key distribution”, Optica **3**, 1274–1278 (2016) (cit. on p. 110).

[191] P. Sibson et al., “Integrated silicon photonics for high-speed quantum key distribution”, Optica (2017) 10.1364/optica.4.000172 (cit. on pp. 110, 118, 120, 138, 164).

[192] D. Bunandar et al., “Metropolitan Quantum Key Distribution with Silicon Photonics”, Phys. Rev. X **8**, 21009 (2018) (cit. on pp. 110, 118, 138, 154).

[193] M. A. Krainak et al., “Integrated photonics for NASA applications”, in Components and packaging for laser systems {v}, Vol. 10899 (2019), p. 14 (cit. on p. 110).

[194] J. Anzalchi, P. Inigo, and B. Roy, "Application of photonics in next generation telecommunication satellites payloads", in International conference on space optics 2014, Vol. 10563 (2017) (cit. on p. 110).

[195] Y. Liu et al., "Experimental Twin-Field Quantum Key Distribution Through Sending-or-Not-Sending", arXiv e-prints, arXiv:1902.06268 (2019) (cit. on p. 111).

[196] D. Rusca et al., "Supplementary Material to Finite-key analysis for the 1-decoy state QKD protocol", Applied Physics Letters **112**, 1–4 (2018) (cit. on pp. 111, 112, 135, 148, 152).

[197] C. C. W. Lim et al., "Concise security bounds for practical decoy-state quantum key distribution", Physical Review A - Atomic, Molecular, and Optical Physics **89** (2014) 10.1103/PhysRevA.89.022307 (cit. on p. 111).

[198] Z.-W. W. Yu, Y.-H. H. Zhou, and X.-B. B. Wang, "Reexamination of decoy-state quantum key distribution with biased bases", Phys. Rev. A **93**, 32307 (2016) (cit. on pp. 112, 135).

[199] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution", Phys. Rev. A **61**, 52304 (2000) (cit. on p. 112).

[200] *AIT QKD R10 Software* (cit. on pp. 112, 132).

[201] M. Nakazawa, K. Suzuki, and Y. Kimura, "Transform-limited pulse generation in the gigahertz region from a gain-switched distributed-feedback laser diode using spectral windowing.", Optics letters **15**, 715–717 (1990) (cit. on p. 114).

[202] G. L. Roberts et al., "Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution", Optics Letters **43**, 5110 (2018) (cit. on pp. 116, 140, 145).

[203] M. Jofre et al., "100 MHz Amplitude and Polarization Modulated Optical Source for Free-Space Quantum Key Distribution at 850 nm", Journal of Lightwave Technology **28**, 2572–2578 (2010) (cit. on pp. 116, 140, 141, 145).

[204] F. Grünenfelder et al., "Simple and high-speed polarization-based QKD", Applied Physics Letters **112** (2018) 10.1063/1.5016931 (cit. on pp. 116, 140, 143, 145, 147).

[205] Lucio-Martinez et al., "Proof-of-concept of real-world quantum key distribution with quantum frames", New Journal of Physics **11**, 95001 (2009) (cit. on pp. 117, 140, 145).

[206] A. Tosi et al., "Fully programmable single-photon detection module for InGaAs/InP single-photon avalanche diodes with clean and sub-nanosecond gating transitions", Review of Scientific Instruments **83**, 013104 (2012) (cit. on pp. 118, 148).

[207] R. Soref, "The past, present, and future of silicon photonics", IEEE Journal on Selected Topics in Quantum Electronics (2006) 10.1109/JSTQE.2006.883151 (cit. on p. 118).

[208] D. Thomson et al., "Roadmap on silicon photonics", Journal of Optics (United Kingdom) (2016) 10.1088/2040-8978/18/7/073003 (cit. on p. 118).

[209] A. Novack et al., “A 30 GHz silicon photonic platform”, in Ieee international conference on group iv photonics gfp (2013), pp. 7–8 (cit. on p. 118).

[210] *No Title* (cit. on pp. 118, 119).

[211] G. Zhang et al., “An integrated silicon photonic chip platform for continuous-variable quantum key distribution”, Nature Photonics (2019) 10.1038/s41566-019-0504-5 (cit. on p. 118).

[212] J. Witzens, “High-Speed Silicon Photonics Modulators”, Proceedings of the IEEE (2018) 10.1109/JPROC.2018.2877636 (cit. on p. 120).

[213] P. Velha et al., “Wide-band polarization controller for Si photonic integrated circuits”, Opt. Lett. **41**, 5656–5659 (2016) (cit. on p. 120).

[214] P. P. Absil et al., “Imec iSiPP25G silicon photonics: a robust CMOS-based photonics technology platform”, in Silicon photonics x, Vol. 9367 (2015), p. 93670V (cit. on p. 120).

[215] L. Canuet et al., “Statistical properties of single-mode fiber coupling of satellite-to-ground laser links partially corrected by adaptive optics”, Journal of the Optical Society of America A (2018) 10.1364/josaa.35.000148 (cit. on p. 127).

[216] R. J. Noll, “Zernike Polynomials and Atmospheric Turbulence.”, J Opt Soc Am **66**, 207–211 (1976) (cit. on p. 127).

[217] N. Tikhonov, M. A. Vorontsov, and G. Carhart, “Characterization of optical turbulence (Cn2) data measured at the ARL A_LOT facility”, Information Sciences (2005) (cit. on p. 128).

[218] N. Corporation, “Polarization in fiber optics”, Report (cit. on p. 131).

[219] T. Fukuchi and T. Shiina, *Industrial applications of laser remote sensing* (Bentham Science, 2012), p. 194 (cit. on p. 131).

[220] G. Vallone et al., “Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels”, Phys. Rev. A **91**, 42320 (2015) (cit. on pp. 137, 146).

[221] M. Chen, C. Liu, and H. Xian, “Experimental demonstration of single-mode fiber coupling over relatively strong turbulence with adaptive optics”, Applied Optics (2015) 10.1364/ao.54.008722 (cit. on p. 138).

[222] A. Ac\’\in et al., “Device-Independent Security of Quantum Cryptography against Collective Attacks”, Phys. Rev. Lett. **98**, 230501 (2007) (cit. on pp. 139, 155, 164).

[223] H. Liu et al., “Experimental Demonstration of High-Rate Measurement-Device-Independent Quantum Key Distribution over Asymmetric Channels”, Phys. Rev. Lett. **122**, 160501 (2019) (cit. on p. 139).

[224] J. Yin et al., “Satellite-based entanglement distribution over 1200 kilometers”, Science **356**, 1140–1144 (2017) (cit. on p. 139).

[225] J.-G. Ren et al., “Ground-to-satellite quantum teleportation”, Nature **549**, 70–73 (2017) (cit. on p. 139).

[226] P. Kómár et al., “A quantum network of clocks”, Nature Physics **10**, 582 (2014) (cit. on p. 139).

[227] D. Calonico, “A fibre backbone in Italy for precise time and quantum key distribution”, 4th ETSI/IQC Workshop on Quantum-Safe Cryptography, Toronto 19-21 Sep 2016 (cit. on p. 139).

[228] D. Rusca et al., “Finite-key analysis for the 1-decoy state QKD protocol”, Applied Physics Letters **112**, 171104 (2018) (cit. on p. 140).

[229] D. Rusca et al., “Security proof for a simplified Bennett-Brassard 1984 quantum-key-distribution protocol”, Physical Review A **98**, 1–6 (2018) (cit. on p. 140).

[230] S. Wang et al., “Practical gigahertz quantum key distribution robust against channel disturbance”, Optics Letters **43**, 2030 (2018) (cit. on pp. 140, 145).

[231] D. Bacco et al., “Experimental quantum key distribution with finite-key security analysis for noisy channels”, Nature Communications **4**, 1–8 (2013) (cit. on p. 141).

[232] G. Vest et al., “Design and Evaluation of a Handheld Quantum Key Distribution Sender module”, IEEE Journal of Selected Topics in Quantum Electronics **21**, 131–137 (2015) (cit. on p. 141).

[233] D. K. L. Oi et al., “CubeSat quantum communications mission”, EPJ Quantum Technology **4**, 6 (2017) (cit. on pp. 145, 154).

[234] D. Dequal et al., “Experimental single-photon exchange along a space link of 7000 km”, Phys. Rev. A **93**, 10301 (2016) (cit. on p. 145).

[235] L. Calderaro et al., “Towards quantum communication from global navigation satellite system”, Quantum Science and Technology **4**, 15012 (2019) (cit. on p. 145).

[236] Y. Liu et al., “Decoy-state quantum key distribution with polarized photons over 200 km”, Opt. Express **18**, 8587–8594 (2010) (cit. on p. 146).

[237] Y. Ding et al., “High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits”, npj Quantum Inf. **3**, 25 (2017) (cit. on p. 146).

[238] G. B. Xavier et al., “Full polarization control for fiber optical quantum communication systems using polarization encoding”, Opt. Express **16**, 1867–1873 (2008) (cit. on p. 146).

[239] Y.-Y. Ding et al., “Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits”, Opt. Lett. **42**, 1023–1026 (2017) (cit. on pp. 146, 147, 151).

[240] M. K. Bochkov and A. S. Trushechkin, “Security of quantum key distribution with detection-efficiency mismatch in the single-photon case: Tight bounds”, Phys. Rev. A **99**, 32308 (2019) (cit. on p. 148).

[241] C. Bonato et al., “Influence of satellite motion on polarization qubits in a Space-Earth quantum communication link”, Opt. Express **14**, 10050–10059 (2006) (cit. on p. 154).

[242] J. D. Franson, "Bell inequality for position and time", Physical Review Letters (1989) 10.1103/PhysRevLett.62.2205 (cit. on p. 155).

[243] J. F. Clauser et al., "Proposed experiment to test local hidden-variable theories", Physical Review Letters (1969) 10.1103/PhysRevLett.23.880 (cit. on pp. 155, 158).

[244] Z. Y. Ou et al., "Observation of nonlocal interference in separated photon channels", Physical Review Letters (1990) 10.1103/PhysRevLett.65.321 (cit. on p. 155).

[245] J. Brendel, E. Mohler, and W. Martienssen, "Experimental Test of Bell's Inequality for Energy and Time", Europhysics Letters (EPL) **20**, 575–580 (1992) (cit. on p. 155).

[246] P. G. Kwiat, A. M. Steinberg, and R. Y. Chiao, "High-visibility interference in a Bell-inequality experiment for energy and time", Physical Review A (1993) 10.1103/PhysRevA.47.R2472 (cit. on p. 155).

[247] J. Brendel et al., "Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication", Physical Review Letters **82**, 2594–2597 (1999) (cit. on pp. 155, 156, 163).

[248] P. R. Tapster, J. G. Rarity, and P. C. M. Owens, "Violation of bell's inequality over 4 km of optical fiber", Physical Review Letters (1994) 10.1103/PhysRevLett.73.1923 (cit. on p. 155).

[249] W. Tittel et al., "Violation of bell inequalities by photons more than 10 km apart", Physical Review Letters (1998) 10.1103/PhysRevLett.81.3563 (cit. on p. 155).

[250] W. Tittel et al., "Long-distance Bell-type tests using energy-time entangled photons", Physical Review A - Atomic, Molecular, and Optical Physics (1999) 10.1103/PhysRevA.59.4150 (cit. on p. 155).

[251] I. Marcikic et al., "Distribution of time-bin entangled qubits over 50 km of optical fiber", Physical Review Letters (2004) 10.1103/PhysRevLett.93.180502 (cit. on p. 155).

[252] T. Inagaki et al., "Entanglement distribution over 300 km of fiber", Optics Express (2013) 10.1364/oe.21.023241 (cit. on pp. 155, 163).

[253] W. Tittel et al., "Quantum cryptography using entangled photons in energy-time bell states", Physical Review Letters (2000) 10.1103/PhysRevLett.84.4737 (cit. on p. 155).

[254] R. Arnon-Friedman et al., "Practical device-independent quantum cryptography via entropy accumulation", Nature Communications **9**, 459 (2018) (cit. on pp. 155, 164).

[255] S. Aerts et al., "Two-Photon Franson-Type Experiments and Local Realism", Physical Review Letters **83**, 2872–2875 (1999) (cit. on p. 155).

[256] J.-Å. Larsson, "Loopholes in Bell inequality tests of local realism", Journal of Physics A: Mathematical and Theoretical **47**, 424003 (2014) (cit. on p. 155).

[257] J. Jogenfors and J.-Å. Larsson, "Energy-time entanglement, elements of reality, and local realism", Journal of Physics A: Mathematical and Theoretical **47**, 424032 (2014) (cit. on pp. 155, 156).

[258] J. Jogenfors et al., "Hacking the Bell test using classical light in energy-time entanglement-based quantum key distribution", Science Advances (2015) 10.1126/sciadv.1500793 (cit. on pp. 156, 163).

[259] A. Cabello et al., "Proposed bell experiment with genuine energy-time entanglement", Physical Review Letters (2009) 10.1103/PhysRevLett.102.040401 (cit. on pp. 156, 164).

[260] G. Lima et al., "Experimental Bell-inequality violation without the postselection loophole", Physical Review A - Atomic, Molecular, and Optical Physics (2010) 10.1103/PhysRevA.81.040101 (cit. on p. 156).

[261] G. Vallone et al., "Testing Hardy's nonlocality proof with genuine energy-time entanglement", Physical Review A - Atomic, Molecular, and Optical Physics (2011) 10.1103/PhysRevA.83.042105 (cit. on p. 156).

[262] A. Cuevas et al., "Long-distance distribution of genuine energy-time entanglement", Nature Communications (2013) 10.1038/ncomms3871 (cit. on p. 156).

[263] G. Carvacho et al., "Postselection-Loophole-Free Bell Test over an Installed Optical Fiber Network", Physical Review Letters (2015) 10.1103/PhysRevLett.115.030503 (cit. on p. 156).

[264] J. A. Larsson and R. D. Gill, "Bell's inequality and the coincidence-time loophole", Europhysics Letters (2004) 10.1209/epl/i2004-10124-7 (cit. on p. 157).

[265] P. G. Kwiat et al., "New high-intensity source of polarization-entangled photon pairs", Physical Review Letters (1995) 10.1103/PhysRevLett.75.4337 (cit. on p. 159).

[266] I. Marcikic et al., "Long-distance teleportation of qubits at telecommunication wavelengths", Nature (2003) 10.1038/nature01376 (cit. on p. 163).

[267] G. Vallone et al., "Interference at the Single Photon Level Along Satellite-Ground Channels", Phys. Rev. Lett. **116**, 253601 (2016) (cit. on p. 163).

[268] F. Vedovato et al., "Extending Wheeler's delayed-choice experiment to space", Science Advances (2017) 10.1126/sciadv.1701180 (cit. on p. 163).

[269] S. L. Braunstein and C. M. Caves, "Wringing out better Bell inequalities", Nuclear Physics B (Proceedings Supplements) (1989) 10.1016/0920-5632(89)90441-6 (cit. on p. 163).

[270] M. Tomasin et al., "High-visibility time-bin entanglement for testing chained Bell inequalities", Physical Review A (2017) 10.1103/PhysRevA.95.032107 (cit. on p. 164).

[271] V. Sorianello et al., "Graphene-silicon phase modulators with gigahertz bandwidth", Nature Photonics (2018) 10.1038/s41566-017-0071-6 (cit. on p. 164).

[272] A. Acín and L. Masanes, "Certified randomness in quantum physics", Nature **540**, 213–219 (2016) (cit. on p. 164).

[273] J. Watrous, "CS 766 Theory of Quantum Information", Lecture Notes (2011) (cit. on p. 168).