Università degli Studi di Padova

Department of Information Engineering

---

Ph.D. School in Information Engineering

Information Science and Technology

XXVII Class

# Improving Quantum Key Distribution and Quantum Random Number Generation in presence of Noise

*Ph.D. Candidate:*
Davide Giacomo Marangon

*Supervisor:*
Prof. Paolo Villoresi

*Course coordinator*:
Prof. Carlo Ferrari

*Ph.D. School Director*:
Prof. Matteo Bertocco

---

Academic Year 2014 - 2015

# Abstract

L'argomento di questa tesi puó essere riassunto nella frase *utilizzare il rumore classico per generare un migliore rumore quantistico*. In particolare questa tesi riguarda da una parte la possibilitá di sfruttare il rumore classico per trasmettere in modo efficace informazione quantistica, e dall'altra la misurazione del rumore classico per generare una migliore casualitá quantistica. Nel primo caso ci si riferisce all'inviare bit quantistici attraverso l'atmosfera per creare trasmissioni allo scopo di distribuire chiavi crittografiche in modo quantistico (QKD) e questo sará oggetto di **Capitolo 1** e **Capitolo 2**. Nel quadro delle comunicazioni quantistiche, la QKD  caratterizzata da notevoli difficoltá sperimentali. Infatti, in linea di principio la QKD offre sicurezza incondizionata ma le sue realizzazioni pratiche devono affrontare tutti i limiti del mondo reale. Uno dei limiti principali sono le perdite introdotte dai canali di trasmissione. Le perdite causano errori e gli errori rendono il protocollo meno sicuro perch un avversario potrebbe camuffare la sua attivitá di intercettazione utilizzando le perdite. Quando questo problema viene affrontato da un punto di vista teorico, si cerca di modellare l'effetto delle perdite mediante trasformazioni unitarie che trasformano i qubits in media secondo un livello fisso di attenuazione del canale. Tuttavia questo approccio é in qualche modo limitante, perch se si ha ha un elevato livello di rumore di fondo e le perdite si assumono costanti in media, potrebbe accadere che il protocollo possa abortire o peggio ancora, non iniziare, essendo il quantum bit error rate (QBER) oltre il limite (11%) per la distribuzione sicura. Tuttavia, studiando e caratterizzando un canale ottico libero, si trova che il livello di perdite é tutt'altro che stabile e che la turbolenza induce variazioni di trasmissivitá che seguono una statistica log-normale. Il punto pertanto é sfruttare questo rumore classico per generare chiave anche quando *normalmente* non sarebbe possibile. Per far ció abbiamo ideato uno schema adattativo per la selezione in tempo reale (ARTS) degli istanti a basse perdite in cui vengono istantaneamente rilevati picchi di alta trasmissivitá. A tal scopo, si utilizza un fascio laser classico ausiliario co-propagantesi con i qubit ma convenientemente inframezzato nel tempo. In questo modo la scintillazione viene monitorata in tempo reale e vengono selezionati gli intervalli di tempo che daranno luogo ad un QBER praticabile per una generazione di chiavi. Verrá quindi presentato un criterio utile per la preselezione dell'intervallo di QBER basso in cui un treno di impulsi intensi si propaga nello stesso percorso dei qubits, con i parametri scelti in modo tale che la sua oscillazione

nel tempo riproduce quello della comunicazione quantistica. Nel **Capitolo 2** presentiamo quindi una dimostrazione ed i risultati di tale protocollo che é stato implementato presso l'arcipelago delle Canarie, tra l'isola di La Palma e quella di Tenerife: tali isole essendo separate da 143 km, costituiscono un ottimo teatro per testare la validitá del protocollo in quanto le condizioni di distanza sono paragonabili a quelle satellitari e la gamma di scintillazione corrisponde quella che si avrebbe in ambiente con moderato maltempo in uno scenario di tipo urbano.

Per quanto riguarda il contenuto del **Capitolo 3** descriveremo un metodo innovativo per la generazione fisica di numeri casuali che si basa sulla constatazione che un fascio di luce coerente, attraversando un lungo percorso con turbolenza atmosferica dá luogo ad immagini casuali e rapidamente variabili. Tale fenomeno é stato riscontrato a partire dai diversi esperimenti di comunicazione quantistica effettuati alle Isole Canarie, dove il fascio laser classico utilizzato per puntare i terminali, in fase di ricezione presentava un fronte d'onda completamente distorto rispetto al tipico profilo gaussiano. In particolare ció che si osserva é un insieme di macchie chiare e scure che si evolvono geometricamente in modo casuale, il cosiddetto profilo dinamico a speckle. La fonte di tale entropia é quindi la turbolenza atmosferica. Infatti, per un canale di tale lunghezza, una soluzione delle equazioni di Navier-Stokes per il flusso atmosferico in cui si propaga il fascio é completamente fuori portata, sia analiticamente che per mezzo di metodi computazionali. Infatti i vari modelli di dinamica atmosferica sono basati sulla teoria statistica Kolmogorov, che parametrizza la ripartizione dell'energia cinetica come l'interazione di vortici d'aria di dimensioni decrescenti. Tuttavia, tali modelli forniscono solo una descrizione statistica per lo spot del fascio e delle sue eventuali deviazioni ma mai una previsione istantanea per la distribuzione dell' irraggiamento. Per tale motivo, quando un raggio laser viene inviato attraverso l'atmosfera, quest'ultima puó essere considerato come un diffusore volumetrico dinamico che distorce il fronte d'onda del fascio. All'interno del Capitolo verranno presentati i dati sperimentali che assicurano che le immagini del fascio presentano le caratteristiche di impredicibilitá tali per cui sia possibile numeri casuali genuini. Inoltre, verrá presentato anche il metodo per l'estrazione della casualitá basato sull'analisi combinatoria ed ottimale nel contesto della Teoria dell'Informazione.

In **Capitolo 5** presenteremo un nuovo approccio per quanto riguarda la generazione di bit casuali dai processi fisici quantistici. La Meccanica quantistica é stata sempre considerata come la migliore fonte di casualitá, a causa della sua intrinseca natura probabilistica. Tuttavia il paradigma tipico impiegato per estrarre numeri casuali da un sistema quantistico assume che lo stato di detto sistema sia puro. Tale assunzione, in principio comporta una generazione in cui il risultato delle misure é complemente impredicibile secondo la legge di Born. Il problema principale tuttavia é che nelle implementazioni re-

ali, come in un laboratorio o in qualche dispositivo commerciale, difficilmente é possibile creare uno stato quantico puro. Generalmente ció che si ottiene é uno stato quantistico *misto*. Uno stato misto tuttavia potrebbe essere in qualche modo correlato con un altro sistema quantistico in possesso, eventualmente, di un avversario. Nel caso estremo di uno stato completamente misto, un generatore quantistico praticamente é equivalente ad un generatore che impiega un processo di fisica classica, che in principio é predicibile. Nel Capitolo, si mostrerá quindi come sia necessario passare da un estimatore di casualitá classico, come l' *entropia minima classica* $H_{min}(Z)$ di una variabile casuale $Z$ ad un estimatore che tenga conto di una informazione marginale $E$ di tipo quantistico, ovvero l'*entropia minima condizionata* $H_{min}(Z|E)$. La entropia minima condizionata é una quantitá fondamentale perché consente di derivare quale sia il minimo contenuto di bit casuali estraibili dal sistema, in presenza di uno stato non puro. Abbiamo ideato un protocollo efficace basato sul *principio di indeterminazione entropica* per la stima dell'entropia min-condizionale. In generale, il principio di indeterminazione entropico consente di prendere in considerazione le informazioni che sono condivise tra piú parti in possesso di un sistema quantistico tri-partitico e, soprattutto, consente di stimare il limite all'informazione che un partito ha sullo stato del sistema, dopo che é stato misurato. Abbiamo adattato tale principio al caso bipartito in cui un utente Alice, $A$, é dotato di un sistema quantistico che nel caso in studio ipotizziamo essere preparato dall'avversario stesso, Eve $E$, e che quindi potrebbe essere con esso correlato. Quindi, teoricamente Eve potrebbe essere in grado di prevedere tutti i risultati delle misurazioni che Alice esegue sulla sua parte di sistema, cioé potrebbe avere una conoscenza massima della variabile casuale $Z$ in cui si registrano i risultati delle misure nella base $\mathcal{Z}$. Tuttavia mostreremo che se Alice casualmente misura il sistema in una base $\mathcal{X}$ massimamente complementare a $\mathcal{Z}$, Alice puó inferire un limite inferiore l'entropia per $H_{min}(Z|E)$. In questo modo per Alice, utilizzando tecniche della crittografia classeica, é possibile espandere un piccolo seme iniziale di casualitá utilizzato per la scelta delle basi di misura, in una quantitá molto maggiore di numeri sicuri. Presenteremo i risultati di una dimostrazione sperimentale del protocollo in cui sono stati prodotti numeri casuali che passano i piú rigorosi test per la valutazione della casualitá.

Nel **Capitolo 6**, verrá illustrato un sistema di generazione ultraveloce di numeri casuali per mezzo di variabili continue(CV) QRNG. Siccome numeri casuali genuini sono una preziosa risorsa sia per l'Information Technology classica che quella quantistica, é chiaro che per sostenere i flussi sempre crescenti di dati per la crittografia, é necessario mettere a punto generatori in grado di produrre streaming con rate da Gigabit o Terabit al secondo. In Letteratura sono riportati alcuni esempi di protocolli QRNG che potrebbero raggiungere tali limiti. In genere, questi si basano sulla misura dele quadrature del campo elettromagnetico che puó essere considerato come un infinito

sistema quantistico bosonico. Le quadrature del campo possono essere misurate con il cosiddetto sistema di rivelazione a omodina che, in linea di principio, puó estrarre un segnale di rumore a banda infinita. Di conseguenza, la banda del segnale casuale viene ad essere limitata solo dalla banda passante dei dispositivi utilizzati per misurare. Siccome, rilevatori a fotodiodi lavorano comunemente nella banda delle decine dei GHz, se il segnale é campionato con un ADC sufficientemente veloce e con un elevato numero di bit di digitalizzazione, rate da Gigabit o Terabit sono facilmente raggiungibili. Tuttavia, come nel caso dei QRNG a variabili discrete, i protocolli che si hanno in Letteratura, non considerano adeguatamente la purezza dello stato quantistico da misurare. Nel L'idea é di estendere il protocollo a variabile discreta del capitolo precedente, al caso continuo. Mostreremo come nell'ambito CV, non solo sia abbia il problema della purezza dello stato ma anche il problema relativo alla *precisione* delle misure utilizzate su di esso. Proporremo e daremo i risultati sperimentali per un nuovo protocollo in grado di estrarre numeri casuali ad alto rate e con un elevato grado di sicurezza.

# Abstract

The argument of this thesis might be summed up as *the exploitation of the noise to generate better noise*. More specifically this work is about the possibility of exploiting classic noise to effectively transmit quantum information and measuring quantum noise to generate better quantum randomness. What do i mean by exploiting classical noise to transmit effectively quantum information? In this case I refer to the task of sending quantum bits through the atmosphere in order set up transmissions of quantum key distribution (QKD) and this will be the subject of **Chapter 1** and **Chapter 2**. In the Quantum Communications framework, QKD represents a topic with challenging problems both theoretical and experimental. In principle QKD offers unconditional security, however practical realizations of it must face all the limitations of the real world. One of the main limitation are the losses introduced by real transmission channels. Losses cause errors and errors make the protocol less secure because an eavesdropper could try to hide his activity behind the losses. When this problem is addressed under a full theoretical point of view, one tries to model the effect of losses by means of unitary transforms which affect the qubits in average according a fixed level of link attenuation. However this approach is somehow limiting because if one has a high level of background noise and the losses are assumed in average constant, it could happen that the protocol might abort or not even start, being the predicted QBER to high. To address this problem and generate key when *normally* it would not be possible, we have proposed an adaptive real time selection (ARTS) scheme where transmissivity peaks are instantaneously detected. In fact, an additional resource may be introduced to estimate the link transmissivity in its intrinsic time scale with the use of an auxiliary classical laser beam co-propagating with the qubits but conveniently interleaved in time. In this way the link scintillation is monitored in real time and the selection of the time intervals of high channel transmissivity corresponding to a viable QBER for a positive key generation is made available. In **Chapter 2** we present a demonstration of this protocol in conditions of losses equivalent to long distance and satellite links, and with a range of scintillation corresponding to moderate to severe weather. A useful criterion for the preselection of the low QBER interval is presented that employs a train of intense pulses propagating in the same path as the qubits, with parameters chosen such that its fluctuation in time reproduces that of the quantum communication.

For what concern the content of **Chapter 3** we describe a novel principle for *true random number generator* (TRNG) which is based on the observation that a coherent beam of light crossing a very long path with atmospheric turbulence may generate random and rapidly varying images. To implement our method in a proof of concept demonstrator, we have chosen a very long free space channel used in the last years for experiments in Quantum Communications at the Canary Islands. Here, after a propagation of 143 km at an altitude of the terminals of about 2400 m, the turbulence in the path is converted into a dynamical speckle at the receiver. The source of entropy is then the atmospheric turbulence. Indeed, for such a long path, a solution of the Navier-Stokes equations for the atmospheric flow in which the beam propagates is out of reach. Several models are based on the Kolmogorov statistical theory, which parametrizes the repartition of kinetic energy as the interaction of decreasing size *eddies*. However, such models only provide a statistical description for the spot of the beam and its wandering and never an instantaneous prediction for the irradiance distribution. These are mainly ruled by temperature variations and by the wind and cause fluctuations in the air refractive index. For such reason, when a laser beam is sent across the atmosphere, this latter may be considered as a dynamic volumetric scatterer which distorts the beam wavefront. We will evaluate the experimental data to ensure that the images are uniform and independent. Moreover, we will assess that our method for the randomness extraction based on the combinatorial analysis is optimal in the context of Information Theory.

In **Chapter 5** we will present a new approach for what concerns the generation of random bits from quantum physical processes. Quantum Mechanics has been always regarded as a possible and valuable source of randomness, because of its intrinsic probabilistic Nature. However the typical paradigm is employed to extract random number from a quantum system it commonly assumes that the state of said system is pure. Such assumption, only in theory would lead to full and unpredictable randomness. The main issue however it is that in real implementations, such as in a laboratory or in some commercial device, it is hardly possible to forge a pure quantum state. One has then to deal with quantum state featuring some degree of *mixedness*. A mixed state however might be somehow correlated with some other system which is hold by an adversary, a quantum eavesdropper. In the extreme case of a full mixed state, practically one it is like if he is extracting random numbers from a classical state. In order to do that we will show how it is important to shift from a classical randomness estimator, such as the *min-classical entropy* $H_{min}(Z)$ of a random variable $Z$ to quantum ones such as the *min-entropy conditioned* on quantum side information $E$.

We have devised an effective protocol based on the entropic uncertainty principle for the estimation of the min-conditional entropy. The entropic uncertainty principle lets one to take in account the information which is shared

between multiple parties holding a multipartite quantum system and, more importantly, lets one to bound the information a party has on the system state after that it has been measured. We adapted such principle to the bipartite case where an user Alice, $A$, is supplied with a quantum system prepared by the provider Eve, $E$, who could be maliciously correlated to it. In principle then Eve might be able to predict all the outcomes of the measurements Alice performs on the basis $\mathcal{Z}$ in order to extract random numbers from the system. However we will show that if Alice randomly switches from the measurement basis to a basis $\mathcal{X}$ mutually unbiased to $\mathcal{Z}$, she can lower bound the min entropy conditioned to the side information of Eve. In this way for Alice is possible to expand a small initial random seed in a much larger amount of trusted numbers. We present the results of an experimental demonstration of the protocol where random numbers passing the most rigorous classical tests of randomness were produced.

In **Chapter 6**, we will provide a secure generation scheme for a continuos variable (CV) QRNG. Since random true random numbers are an invaluable resource for both the classical Information Technology and the uprising Quantum one, it is clear that to sustain the present and future even growing fluxes of data to encrypt it is necessary to devise quantum random number generators able to generate numbers in the rate of Gigabit or Terabit per second. In the Literature are given several examples of QRNG protocols which in theory could reach such limits. Typically, these are based on the exploitation of the quadratures of the electro-magnetic field, regarded as an infinite bosonic quantum system. The quadratures of the field can be measured with a well known measurement scheme, the so called homodyne detection scheme which, in principle, can yield an infinite band noise. Consequently the band of the random signal is limited only by the passband of the devices used to measure it. Photodiodes detectors work commonly in the GHz band, so if one sample the signal with an ADC enough fast, the Gigabit or Terabit rates can be easily reached. However, as in the case of discrete variable QRNG, the protocols that one can find in the Literature, do not properly consider the purity of the quantum state being measured. The idea has been to extend the discrete variable protocol of the previous Chapter, to the Continuous case. We will show how in the CV framework, not only the problem of the state purity is given but also the problem related to the *precision* of the measurements used to extract the randomness.

# Contents

# Chapter 1

# Introduction

Quantum Cryptography represents the first tangible application of Quantum Information. At present time indeed Quantum Communication Networks implementing protocols of quantum key distribution (QKD) can be found also outside the academic laboratories. This result follows an almost twenty years long theoretical and experimental effort, which involved major Quantum Information and Optics groups. This research boosted and made it evolve the seminal idea of Charles Bennett and Gilles Brassard of securing the exchange of cryptographic keys by means of Quantum Mechanics.

## 1.1 The BB84 protocol

At the present time Quantum Cryptography is a real and working solution that Quantum Mechanics offers to a problem that appears to be still far in the future. Interestingly, this problem is also caused by Quantum Mechanics: it is the possibility to break current cryptographic protocols by means of a Quantum Computer. The security of the current cryptographic protocols, e.g. RSA or AES, is based on the *factual* difficulty in solving hard computational problems as the factorization of the product of two large prime numbers on which modern cryptographic protocols are based. In particular this problem would take an exponential time on a classic computer. On a quantum computer however it runs on polynomial time as P. Shor found in 1994 [1].

The only protocol which has been proven to offer unconditional security is the *one time pad* as demonstrated by C. Shannon, cfr.[2]: given a binary string of length $L$ corresponding to the binary version of the message $m$ to encrypt, the so-called *plaintext*, the encrypted message $e$, the *ciphertext*, is obtained taking the bitwise exclusive-or (XOR), between $m$ and another string $k$ of the same length which is formed by *randomly* chosen bits. This string corresponds to the *key*, and is combined with $m$ in the following way

$$e = m \oplus k, \tag{1.1}$$

where every bit of $m$ is xored with the corresponding bit at the same position of $k$. The one time pad is the most effective way to encrypt information since the only way an eavesdropper has to decrypt the message, it is to get the key and to perform the inverse

operation $m = e \oplus k$: assuming that the eavesdropper has the encrypted message, he can try a *brute force attack*, that is to apply all the $2^L$ keys, corresponding to all the possible combinations of $L$ bits, but the only result he will get is a set of *plausible* messages. Naturally, the longer the length of the string message, the smaller the set would be, but at this point the computational resources needed would make the attack infeasible.

If two users Alice and Bob aim to use the one-time-pad protocol to communicate without being eavesdropped, they need to share the same key for the encryption of the plain text and then the decryption of the cyphertext. The security of the protocol is then guaranteed if the key is used just once and if the no information is leaked about the key. This last point represents an issue because if Alice and Bob do not have any mean to exchange directly the key, e.g. because their locations are distant, the whole protocol can not be reliably applied. Indeed if Alice and Bob need to encrypt their communications it is because they can not trust the channel they are using, e.g. they assume an eavesdropper in between, the so called Eve, is wiretapping the channel itself. If it is so, then the key cannot be exchanged on that same channel because Eve could intercept it too. Alice and Bob then should meet directly and pre-share a key as the messages they hypothesize to exchange in the future. All these difficulties make the one-time-pad not practical, and this is the reason why asymmetric encryption protocol were preferred.

The BB84 protocol, from the name of its inventors C. Bennet and G. Brassards who published the work in 1984 [3], is a communication procedure which lets Alice and Bob to obtain a shared secure key to be used for symmetric one time pad encryption, also if they cannot meet directly.

The protocol indeed gives to Alice and Bob the power to detect an attack of Eve while they are exchanging the key. The BB84 protocol involves the use of a *quantum channel* in connection with a *classical* channel. Alice and Bob exchange qubits through the quantum channel, i.e. bits encoded in some degree of freedom of a quantum system. In the following example we are going to use the photon as the quantum system, and its polarization as degree of freedom.

In the protocol Alice and Bob agree to encode the values of the bits, which will compose the key, in non-orthogonal states belonging to mutually unbiased basis e.g. the horizontal/vertical $\{|H\rangle, |V\rangle\}$ and the diagonal $\{|\nearrow\rangle, |\nwarrow\rangle\}$, according the following predetermined rules

| Polarization basis | Bit value 0 | Bit 1 |
|---|---|---|
| $\{\|H\rangle, \|V\rangle\}$ | $\|H\rangle$ | $\|V\rangle$ |
| $\{\|\nearrow\rangle, \|\nwarrow\rangle\}$ | $\|\nearrow\rangle$ | $\|\nwarrow\rangle$ |

Once that Alice and Bob authenticated their identities to each other, they can start the BB84 protocol, consisting then of four steps:

1. Alice uses a source of single photons: she prepares every photon in one of all the four states swapping randomly between the four polarizations and she sends them to Bob. Alice has then a string of random bits corresponding to the states she sent to Bob;

2. Bob measures the single photons swapping randomly between the two bases: Bob obtains then a string of random bits according to the results of the measurements;

3. on a classical channel Alice and Bob disclose which *bases* they used to prepare and measure the qubits respectively. Since the states are non-orthogonal, when the two bases do not match, the bit value obtained by Bob is uncorrelated with the one of Alice. Being the bases of Bob chosen randomly, only the 50% of the bits is in average correct. Therefore they discard from their strings the bit corresponding to unmatched bases. Besides, Alice discards also those bits which correspond to photons which she sent but Bob did not receive. At the end of this process, the so called *sifting*, Alice and Bob have two *raw keys*;

4. Alice and Bob then extract random sub-samples of the raw keys and check for the presence of errors. In absence of errors the two keys are equal and can be safely used to encrypt and decrypt messages. However, let's suppose an eavesdropper, Eve, tries to get the keys and then she measures the photons. Since she does not know the preparation basis, she has to adopt the same strategy of Bob, i.e. to choose between the two bases. Since the measurement destroys the photon, she has to prepare the state as she measured it, and then to send it to Bob. If she guesses correctly the basis, she resends the correct photon, however half of the times, being the states non-orthogonal, she sends to Bob the wrong photon. The joint probabilities of a wrong basis choice for Eve and Bob, cause Alice to find the 25% of bits wrong after the sifting, when they compare random sub-samples of the raw keys. This enables to spot the action of the eavesdropper, Alice and Bob discard the whole key and a new transmission is started. In the more general case when the rate of errors is below the critical limit, post-processing techniques, the so-called *information reconciliation and privacy amplification* cfr.[4], are applied on the sifted keys to correct the errors and eliminate the possible information acquired by Eve.

In the last 30 year the simple and effective idea of Bennett and Brassard evolved under the theoretical and experimental effort which made it possible to evolution of this idea into what could become the second quantum revolution after the first one of the electronics based on semiconductor.

## 1.2 The need of long range optical communications

In 2008 a benchmark for the QKD level of maturity was given the experiment denominated SECOQC, *SEcure COmmunication based on Quantum Cryptography* [5]. This experiment was the result of an inter-European collaboration lasted four years with the aim to demonstrate an operative integrated network. This network was set up in Vienna and it was constituted by six *trusted nodes*. A peculiarity of QKD systems is indeed that the communication can be established *point-to-point*, i.e. transmitter and receiver are connected directly. In order then to connect two distant parties that cannot be

linked directly, the SECOQC network enforced the *hop-by-hop* protocol: a classical key is bounced from a node to next one being encrypted at every *hop* with another key established via QKD between the two nodes.

The important point about the SECOQC network is that the six nodes were linked with eight different quantum cryptographic systems which featured almost all the existing physical paradigms, in which QKD protocols were implemented up to the 2008: i.e. plug and play systems [6], phase coding systems[7], continuous variable systems[8], discrete variable systems, cfr.[4]. Another interesting fact that is that out of eight systems, only the system implemented by the group of the University Ludwig Maximillians (LMU) of Muenchen, exchanged qubits in free space with a BB84 + decoy protocol (see below). The remaining seven used protocols with the quantum channel realized with an optical fiber. The maximum and minimum distances linked by the fiber systems were of 85 km (with a Coherent One Way protocol [1] and 6 km (with a Continuous Variable protocol[2]) respectively. The LMU system was used to connect the last node from the rest of the network: the distance was of 80 meters.

Conversely to the conclusions which might be drawn from this example, in the commonly accepted future picture of Quantum Communications the largest distances will be reached by free space optical links. What motivates this prediction is the fact that optical fibers cannot be used for an extension over 400 km. At present time the length record is of 250 km [9], for the Swiss link Geneva-Neuchatel. The main reason is due to the non null attenuation, ranging typically from 0.2 to 0.35 dB/km: the longer the channel, the higher the number of photons absorbed per packet and consequently the higher the number of errors at the receiver. Additional limiting reasons are polarization errors and mode dispersion, cfr. [10] and [4].

As the SECOQC example shows, an alternative to the fibers is to exchange the photons in free space. Indeed QKD protocols can be effectively implemented with photons because their polarization is not affected during the propagation in the air and interestingly, the wavelength dependent attenuation of the atmosphere is low for that range of wavelengths where the quantum efficiency of single photon detectors is higher, i.e. approximately 0.1 dB/km for $\lambda$s between 750 and 850 nm.

It is worth stressing that to connect distant parties with the paradigm hop-by-hop can somehow work only if the networks are small and the nodes are realized by a limited amount of known parties, as in the case of demonstrative SECOQC network or the more recent eight nodes Tokyo network [11]. For the security of the protocol it is necessary that all the intermediate nodes, which encrypt and repeat the classical key, are indeed *trusted*. Any given Alice and Bob in the network, who aim to securely share a key, should control directly the repeaters in order to exclude any third party to have access to them. For urban, regional, etc. networks with chains of intermediate nodes this task becomes clearly not feasible.

An alternative way are *quantum repeaters*: these devices are based on quantum entanglement and quantum swapping to directly propagate. This technology however is

[1] developed by the University of Geneva)

[2] developed by the consortium Univ. Libre de Bruxelles, CNRS and Thales

still at the early stages of development cfr.[12].

In order to cover long distances to connected together small trusted networks, a remaining solution, would be to employ direct optical links. However there are two main drawbacks represented by

- the curvature of the Earth surface
- the likely presence of line of sights obstacles
- atmospheric induced losses

For example the line of sight from a 100 m tall building is roughly of 35 km[1] before being obstructed by the Earth surface itself. Naturally this is valid, in case of clear visibility and in absence of other obstacles, conditions difficult to met in urban areas densely populated and polluted. In addition, a very important point is that the closer an horizontal path is to the ground, the higher are losses due to atmospheric turbulence as consequence of the convective air flows.

With the current unavailability of quantum repeaters, the solution which has been reputed the most viable to reach long distances is to use *satellites*. Besides, the large field of view, a neat advantage of using satellites lies in the fact that for a vertical path, the layer of atmosphere to cross is just about a tens of kilometers, so the impact of the atmospheric losses is significantly less, roughly 30 - 40 db, with respect to horizontal paths (e.g. 60 dB cfr. [13]).

Effective ways to employ satellites have been matter of study of several investigations [13]. Among the many configuration, a simple and effective scheme involves satellites in low Earth orbits (LEO), between 200 and 2000 km above the Earth, as transmitting terminals towards receiving ground stations. Indeed the quantum beam signal results less affected by the atmospheric losses if the atmosphere is crossed in the terminal phase of its propagation, rather than at the beginning.

A satellite then can be regarded as a trusted node in the sky [14] and a key between Alice and Bob, on two distant ground stations, can be shared in the following way: the satellite establishes a quantum connection with Alice and they generate a first key; the satellite then generates a second key with Bob and it encrypts the first key pre-shared with Alice with this latter. The encrypted key of Alice is then sent on a classic channel to Bob that decrypts it with the second key exchanged before. Naturally also in this case there is the issue of trusting the satellite but the fact that the node is orbiting at an average distance of 1000 km above the Earth, with speeds around 10000 km/s lowers the possibility of manumission.

At the present time, the field of Quantum Communications is experiencing the so-called *Quantum Race to the Space* [15] with the main research groups worldwide rushing to set the milestone of the first QKD implementation between Earth and Space. On this regard, in 2008 the first exchange of single photons from a LEO satellite was realized by Villoresi et al. [16]. The experiment was performed by using the optical system of a laser

[1] assuming $r = 6378$ km the Earth radius, and $h = 100$ m the height of the building, the horizon falls at a distance $d = r \tan\left(\sec^{-1}\left(1 + \frac{h}{r}\right)\right)$

ranging ground station (in Matera, Italy) to shine satellites carrying retro-reflectors. The transmission was performed by suitably setting the repetition rate and the intensity of the laser to match the atmospherical losses such that on the retro-reflector, there was in average a single photon per pulse. The single photons were then back reflected and detected by the same transmitting station. Another step towards the space frontier was achieved again at the Matera laser ranging facility by Vallone et al. [17] with the retro-reflection transmission of polarized single photons.

Long range quantum communications were and are still thoroughly tested also on the terrestrial links because one can study and devise solutions to the issues which will likely affect the protocols once that they will be implemented with satellites. In the following Chapter, we will illustrate an experiment performed on a 143 km long free space channel where we tested a transmission protocol which will enable communications with satellites also in regimes of strong attenuations.

# Chapter 2

# QKD: Adaptive Real Time Selection

In this Chapter, an experiment will be presented which had the aim of testing a new transmission protocol in free space for Quantum Key Distribution. This experiment belongs to that research branch of Quantum Information and Quantum Communications devoted to study and develop the tools necessary to build a worldwide quantum network, for the secure exchange of cryptographic keys by means of QKD. The innovative element of this protocol is the exploitation of the atmospherical turbulence, which is the main limiting factor in a optical communication, to improve the key distribution itself.

## 2.1 Introduction

In order to understand the contribute of this work in the context of QKD, it is necessary to present the main factors common to experimental realizations of QKD protocols which can be detrimental to the security of the protocol itself. Indeed it is worth to stress that although the ideal Quantum Cryptography is strong (= unconditionally secure) under the theoretical point of view, practical implementations are challenging. On this regard, most of the theoretical works are indeed about proof of security for protocols under different set of non ideal conditions, e.g. finite keys, channel induced decoherence, high losses, etc.

In the following we will introduce the two main experiment which were performed on the same link we used to test our protocol.

For what concerns free space communications, experiments on terrestrial free space optical (FSO) links represent a benchmark for the future protocols with satellites. A link that in the last ten years served for different experiments is 143 km long between the islands of La Palma and Tenerife at the Canary Islands (Spain), see Section 2.3. The effectiveness of testing on the ground techniques that should work in the Space, lies in the fact that the layer of atmosphere to cross is much longer than the vertical layer (roughly 10 km) for a transmission with a satellite [13]. The paradigm is then that if *something works with the worst conditions, it has to work also in better conditions.*

In 2006 two seminal experiments at the Canary FSO paved the way to satellite quantum communications being the first free space implementation of QKD protocols on a distance of over 100 km, and overpassing by a factor of 6 the length of the previous record of 23.4 km by Kurtsiefer et al. [18]. These two experiments were tested a decoy-state BB84 protocol by T. Schmitt-Manderbach et al. [19] and an entanglement based QKD protocol by R. Ursin et. al [20].

The main difference between the two protocols lies in the source of photons: in the experiment of Ursin et al., photons in an entangled state of polarization were used to encode the qubits in order to enforce the protocol Ekert 91 (E91) [21]. In this protocol Alice and Bob achieve a perfectly secret key by measuring respectively one part of a binary quantum system in an entangled state of some degree of freedom, e.g. photons entangled in polarization. Being the system entangled Alice and Bob get a list of outcomes, i.e. the key, which are perfectly correlated (or anti- depending on the state).

According to the protocol, the quantum system is distributed by a third party and the check that none is eavesdropping the channel can be verified by estimating test of non-locality with the measured outcomes, e.g. by observing the violation of Bell inequality. The E91 protocol has two main advantages: it does not need a quantum random number generator for the choice of the bases because the outcomes of the reduced party are random by definition. Besides, a source of entangled photons (with a low probability of double pair emission) is a the ideal single photon source required by the theory and which offers the highest level of security.

The critical importance of the photon source for the protocol security, can be illustrated with the experiment of Schmitt-Manderbach et al., which employed faint laser pulses. Given that single photon sources are yet not ready for QKD [12], protocols such has BB84 or the B92 are implemented by means of weak coherent pulses (WCP) obtained by strongly attenuating laser coherent radiation. A WCP has to feature an average number of photon per pulse, $\mu$, very low, typically $\mu \approx 0.1$. The reason of this constraint is due to the fact that the photon emission of a coherent light source is characterized by a Poissonian probability distribution, therefore one has a non null probability to find more than one photon per pulse. This possibility represents a security issue because an eavesdropper, Eve, monitoring the channel could intercept and store the extra photon in a quantum memory, without being detected: when Alice announces the bases, Eve measures correctly the photon discovering bits of the key. This attack, the so called *photon number splitting* (PNS) represents the most powerful of the possible Eve's strategies [4]. The use of WCP then makes the secure key rate to scale as $t^2$ being $t$ the transmissivity of the channel, whereas by using an ideal single photon sources the rate would scale linearly with $t$. The discovery of the PNS strategy caused a kind of stall at the beginning of 2000, because quadratic dependence of the rate on the link transmissivity shortened the achievable distances. The situation was unblocked in the first half of the 2000s, with the introduction of variations on the BB84 protocols, namely the SARG04 [22] and the *decoy protocol* [23], which fixed the dependence of the key rate to $t^{3/2}$ and $t$ respectively. Briefly, in a decoy protocol *decoy* signals with different $\mu_{\text{decoy}}$s

are randomly interleaved to the key signal: because Eve does know the attenuation for the different decoys, she can not subtract photons adapting the attack for the different attenuation, resulting in detectable modification of the photon statistics.

The effectiveness of this protocol can be understood by considering that without decoy states, in the BB84 experiment a secure rate of key could not be achievable due to the 30 dB of losses registered: with the used setup, losses at maximum of 20 dB were tolerable to generate key. Indeed, the qubit error ratio (QBER), i.e. the ratio between the erroneous sifted bits and the total number of sifted bits, allows to generate secure keys only when is lower than the 11%. Since the photons scattered are not registered, one has that the relative error increases in presence of strong losses, because the spurious detections due to unfiltered stray light, afterpulses, thermal excitations, etc. [24], are not compensated by correct detections. Losses and dark counts represent then the second critical limiting factor in QKD experiments. The main drawback is that the larger the QBER the lower the rate of secure bits generated. In the experiment of 2006 the source was implemented by modulating at 10 MHz four diodes for the four polarizations, firing randomly together two diodes for the decoy states. With losses for roughly 34 dB and a QBER = 6.48%, the final bit rate was of 12.8 bit/s.

At present time, for the future of Quantum Communications, fast WCP sources seem to be more easy to achieve rather than fast and low noise detectors [12]. For example, by employing vertical-cavity surface emitting lasers (VCSEL) modulation frequencies up to 1.5 GHz have been reported [25]. Besides, high rates can be achieved also *indirectly* by using only a single CW laser whose output is coupled with polarization modulators as in [26]. For what concerns single photon detectors, instead it is necessary to find trade-off between efficiency, dark counts and dead-time. The latter is indeed the main factor which limits the count rate. Detection rates up to the GHz were achieved with InGaAs photodiodes (better efficiency for $\lambda \sim 1550$) [27, 4]. However Si-APD (silicon avalanche photo diodes) are preferred because they feature lower dark count rates in the range $750\text{nm} < \lambda < 850\text{nm}$) [25, 24].

The point worth to underline is that the possibility to success in sharing a secret key between Alice and Bob depends on the interplay between an optimized setup and the losses which characterize the free space optical channel. In an optimized setup, the possible causes of dark counts can be attenuated for example by cooling the detectors, or by using very narrow filters to reduce the stray light. However for a given level of optimization, the second factor which raises the QBER are losses during the propagation of the beam in atmosphere: one can divide the losses in two classes: *geometric* and *atmospherical*.

### 2.1.1 Geometric Losses

To this class refer the losses caused by the optical setup. The main source of loss is the *beam divergence* due to the aperture diffraction of the transmitting telescope. In particular, the lower the ratio between the beam area at the receiver and its telescope aperture, the smaller is the loss. In order then to improve the SNR, it is necessary to design the telescopes to maximize the power coupling, i.e. the divergent beam at a

given distance has to match at the best the aperture of the receiving telescope, cfr. [28] (it has to be considered, that when the transmission is done in atmosphere, the beam experiences additional divergence due to the turbulence, see below).

In this sense, also errors due to the *pointing* of the telescopes can be regarded as losses: for a transmission involving one or both parties moving, this problem is of main relevance. Tracking systems and telescopes collocated on gimbal mounts are then necessary to keep the coupling between the parties. On this regard, notable examples are given by the first ground-to-aircraft QKD protocol realized by Nauerth et al. [29] and the already cited ground-to-satellite exchange of single photons. In the former case, Nauerth et al. implemented a BB84 protocol between a receiving optical ground station and a transmitting aircraft flying on round orbits such that the average distance was of 20 km. In the second case, the experiments with the photons retro-reflected by satellites were made possible by the enhanced precision of the spatial and temporal tracking systems of the Matera laser ranging ground station. Satellites on LEO and MEO orbits indeed have an average altitude of over 500 km and move with a velocity of over 7000 km/s. Consequently, on the ground very fast tracking systems with very limited pointing errors are necessary, e.g. less than $\mu$rad, in order to minimize the losses due to wrong aiming. Although we are dealing with geometric losses, it is worth to point out that also temporal accuracy is required. Synchronization mechanisms, usually achieved with temporal signals from GPS, are necessary in order to anticipate the motion of the satellites and to compensate the trip time of the pulses. This should avoid to miss the satellite in case of transmission from ground towards the space, and it should avoid to anticipate or retard the acquisition in the opposite case [**?**].

As we will show, however, also with not moving parties is necessary to implement tracking systems because atmosphere induces heavy drifts of the movement on the laser beams.

### 2.1.2 Atmospheric Losses

Fundamentally when a coherent beam of light propagates in atmosphere, it undergoes a process of attenuation and distortion. The addition of these two effects causes the losses in the transmission of weak coherent pulses. In order to understand how these distortions arise from the turbulent atmosphere we are going to briefly introduce a common physical model for the atmosphere.

Atmosphere is a physical system whose dynamic is described by Fluid Mechanics. As a fluid, also the atmospheric wind flow is characterized by laminar and turbulent motion. When a fluid enters in a turbulent regime, its dynamics becomes unfeasible to be described analytically, i.e. by resolving the Navier-Stokes equations which describe the motion of a fluid. The problem of characterizing the fluctuations of the wind flow physical parameters at two separate spatial coordinates, can be addressed by adopting a statistical approach. An effective statistical model is the one introduced by A. Kolmogorov [30] in 1941. The model considers that in a turbulent atmospheric regime originating by the heating of the air close to the terrestrial surface, the air masses moving with the wind speed can break into *eddies* of scale $L$, the so-called *outer scale* (the outer scale

depends strictly on the environmental conditions, however typically it can range from 1 to 100 m). The eddies continue further to break into smaller eddies transferring the initial kinetic energy, until the damping *inner scale* scale $l_0$ is reached, (up to 1 mm). For scales $r << l_0$ the remaining energy is dissipated as heat and the eddies disappear. Further, the model assumes that on spatial scales $r$ such that $l_0 << r << L$, the *inertial subrange*, turbulence can be considered homogenous and isotropic. The effectiveness of the Kolmogorov model lies in the fact that it allows to statistically quantify the spatial correlation of fluctuating parameters, such as the wind speed $v(\mathbf{r})$ or the air refractive index $n(\mathbf{r})$. In particular, these correlations can be expressed by means of the so-called *structure functions*, e.g. $D(v(\mathbf{r}_1), v(\mathbf{r}_2))$: one can show that within the inertial subrange, correlations depend only on the module of the vectors $|\mathbf{r}_1 - \mathbf{r}_2|$ connecting the two points but not on its direction.

The Kolmogorov model is a powerful tool to analyze statistically the dynamic of atmosphere but a deep analysis would require much more space and it would go also beyond the interest of this experiment. Indeed most of the results which can be derived applying the model to the optical propagation, are valid in a situation of *weak turbulence*, cfr. [31]. On this regard it is worth stressing that the length of the optical link considered for this experiment is such that we are in a regime of strong turbulence, as we will show in Chapter 2, Section 3.2.

The eddies model turns out to be useful to give a qualitative idea of the losses caused by beam distortions. These latter are caused by local non homogeneities of the air refractive index which varies randomly in time. In particular the effects which contribute mainly to the losses are:

- beam wandering: at the receiver side, the beam spot wanders around the ideal optical axis of propagation. The cause of this movement can be ascribed to the the motion of eddies whose scale is larger then the beam diameter. If $w$ is the diameter of the beam, and $v_t$ the transverse velocity of the wind flow with respect to the optical axis, one has that the time scale of the this jitter is roughly given by $d/v_t$, cfr.[32]. To mitigate this effect closed loop feedback control system are devised in order to automatically correct the wander of the beam and a method is presented in Section 2.3.

- beam spreading: one observes a beam divergence which is larger than the divergence one would observe after propagation in vacuum caused by the diffraction at the transmitting telescope aperture. The cause of this broadening is are the eddies with a scale smaller than the beam diameter. The detrimental effect of the spreading is an enhanced power decoupling with the receiving telescope. In the experiment of Manderbach et al. almost half of the whole losses were ascribed to beam spreading.

  The losses can be mitigated by using a large aperture receiver telescope in order to collect the largest fraction possible of signal, e.g. the telescope used as receiver in the Canary experiments has the aperture diameter of 1 meter (see Section 2.3). In addition the design of the transmitting telescope aperture must be tailored in

order to take in account also the additional atmospheric spreading.

The combined geometrical effects of wandering and spreading, summed to the varying attenuation in time of the beam intensity due to the random inhomogeneities of the air refractive index, give then rise to the so-called *scintillation*. More specifically scintillation is the random variation of the irradiance of the beam which can be compared to the twinkling of star light in the sky. In next Section we will show how it can be exploited to generate secure key in a regime of high losses.

## 2.2 The ARTS method

In this work, we present a method that exploits strong atmospheric turbulence for secret key generation, in conditions in which the long-time average QBER is too high for secure communication.

This approach is made possible by the fact that the temporal profile of the transmissivity in a long and strongly turbulent channel has characteristic peaks lasting few milliseconds, and following a lognormal distribution [33]. On these grounds, we will introduce and demonstrate an *adaptive real time selection* (ARTS) scheme based on the ideas introduced in [33]. The scheme is based on the estimation of the link transmissivity over its intrinsic time scale by an auxiliary classical laser beam, the so called *probe*, co-propagating with the qubits, but conveniently interleaved in time. In this way, the link scintillation is monitored in real time and only the high channel transmissivity intervals corresponding to a viable QBER for a positive key generation rate, can be selected because the transmissivity peaks are instantaneously detected.

We will present a demonstration of this protocol on the same optical link of Canary Island, in loss conditions that are equivalent to satellite links, and with scintillation range corresponding to moderate to severe weather.

## 2.3 Experimental setup

The free space optical link was set between the islands of La Palma and Tenerife at the Canary Islands. On the island of La Palma and Tenerife, at an altitude of 2400 m are indeed available the observatories of the Astrophysical Institute of the Canary (IAC) and of the European Space Agency (ESA). These facilities were set there because of the atmospherical and meteorological conditions which make those spots particularly suitable for astronomical observations. The fact that the two islands are separated by 143 km, that the FSO features clear visibility and stable conditions, and that the large telescope of the ESA Optical Ground Station (OGS) on Tenerife can be pointed horizontally, made in the past this link the preferred testbench for many experiments of Quantum Communications.

The overall link setup is reported in Figure 2.1. On the island of La Palma, Alice sent on the same optical channel both a classical signal the atmospheric probe and the quantum signal. On the island of Tenerife, Bob received both the signals: thanks to the

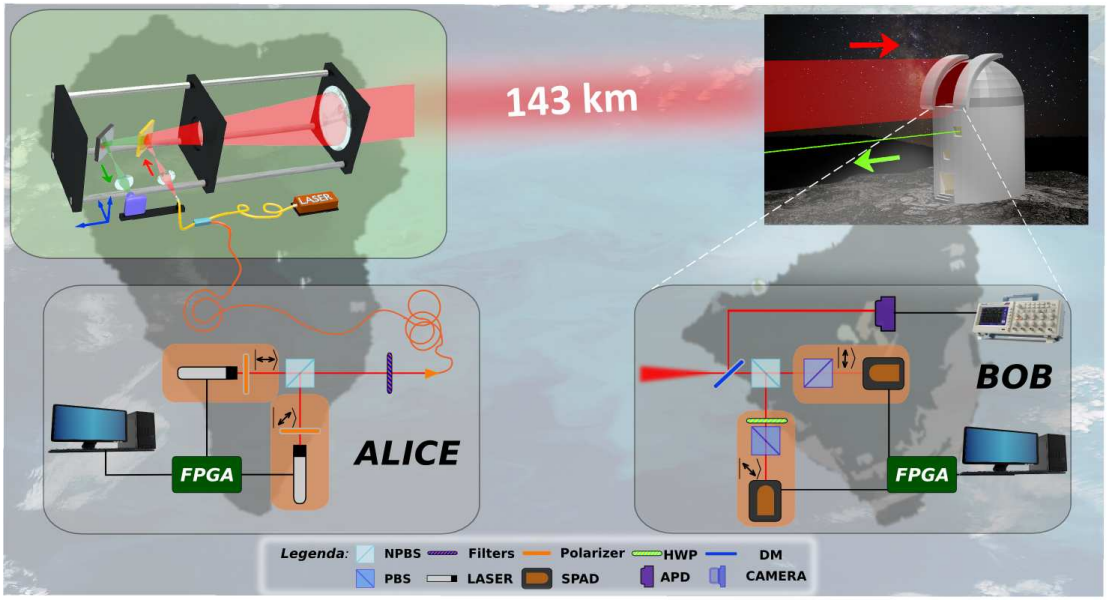


Figure 2.1: Experimental setup: Alice, located at JKT observatory in La Palma, sends qubits by using two 850 nm FPGA-controlled attenuated lasers with different polarization. Qubit photons are combined with an atmospheric probe laser (30mW @ 808 nm) and transmitted through a suitably designed telescope. The Alice telescope is also used to collect the beacon laser sent by Bob, located at the Optical Ground Station in Tenerife, and required for tracking the pointing of the transmitter. Bob receives both the signals through the OGS telescope (see Appendix): the probe is monitored by an APD and the qubits are detected with two SPADs. FPGA: Field Programmable Gate Arrays; HWP: half-wave plate; NPBS: non-polarizing beam splitters; PBS, polarizing beam splitter; SPAD, single-photon avalanche photodiode; DM: dichroic mirror.

probe he could discriminate the enhanced transmissivity peaks of the channel and then acquire keys correspondingly.

In the following subsections, a detailed analysis of the apparatus will be given.

### 2.3.1 Alice

The transmitter telescope (Alice) was located on the roof top of the Jacobus Keptein Telescope (JKT) observatory in the island of La Palma, at an altitude of 2360 m. The telescope is an open structure of iron rods hold together by three steel flanges, see Figure 2.2. The first flange is mounted on a large xyz stage for a coarse pointing of the telescope. The second flange is suspended above the ground by the rods and it carries all the optical components. In the third last flange, a lens is encapsulated. This telescope was designed in order to mitigate at the best the atmospherical abberations without using adaptive optics. The first peculiarity is the lens which is a custom hand-made plano convex singlet with a diameter of 230 mm. With such an aperture it is possible to achieve, after 143 km, a beam spot comparable to the dimensions of the primary mirror of the receiving telescope in order to maximize the power transfer between the two parties (cfr. [34] [35]). The second peculiarity of the telescope is the tracking system which enables to compensate the beam wandering. The telescope does not only transmit the quantum and the classical probe signal but also receives a beacon laser $\lambda = 532$ nm which is sent by Bob. The beacon enters the telescope and it counter propagates along the same optical path of the other two signals. The beam is then focused on the sensor of a camera which periodically reads the position of the wandering spot. This information is used in a feedback loop to correct accordingly the point source on the focal plane.

The system can be appreciated more in detail in Figure **??**. The second flange is collocated in a position close to the focal planes of the lens which, being chromatic, has $f = 2202$ for $\lambda = 810$ nm and $f = 2202$ for $\lambda = 532$ nm. The flange has an aperture at the center, where an optical cage system is fixed with

- a dichroic mirror which back reflects the quantum + probe signal (red dashed line) towards the telescope aperture and transmits the beacon signal (red dashed line). The position of the dichroic mirror was properly set in order to not have the clipping of the beams.

- a mirror which directs the beacon signal toward the camera (green dashed line).

A XYZ movable platform is mounted on a breadboard attached at the basis of the flange. This platform carries both the signal fiber and the CMOS camera such that the movement of the platform affects both the systems. The platform is realized by mounting on a stepped motor stage for the Z movement, a XY support controlled by another pair of stepped motors.

On this support we have a cage system with the optics for the beacon and the quantum + probe signal. For what concerns the latter, at the fiber output a $f = 8$ mm IR coated lens collimates the beam, which is then refocused by another $f = 18$ mm. It is worth noting that, having the quantum signal and the probe two different wavelengths,

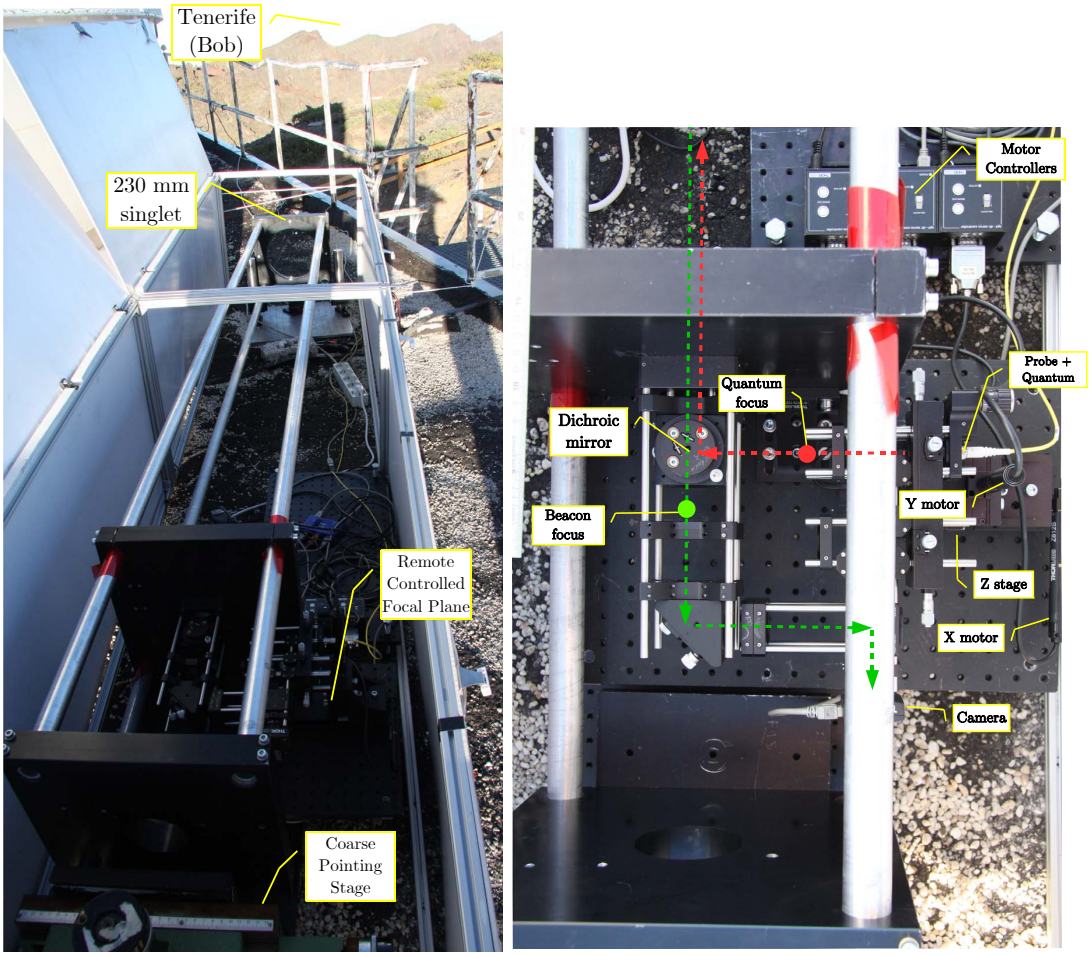


Figure 2.2: On the left the whole Alice telescope. On the right a detail of the focal plane with the main components.

$\lambda = 850$ and $\lambda = 808$ respectively, they do not share the same focal plane. However, the probe signal is classical and can sustain higher losses, instead the quantum signal has to match the focal plane of the singlet in order to maximize it at the receiver side. For this reason, once that the IR signal was properly aligned on the same path of the beacon[1], the point of focus was searched by firing the non attenuated 850 nm lasers and by finely moving the Z stage according to the power readings from Bob. Once that the optimal position was found, the position of the camera and of the beacon focusing doublet where manually adjusted by moving directly the cage plates. In particular it was necessary to obtain a beacon image enough small to appreciate the beam drifts on the sensor.

Every time, before starting the transmission protocol, the same procedure adopted

[1]this was done by setting the probe laser at maximum power and by moving the beam in order to have the green and IR signal aligned as well in near as in the far field

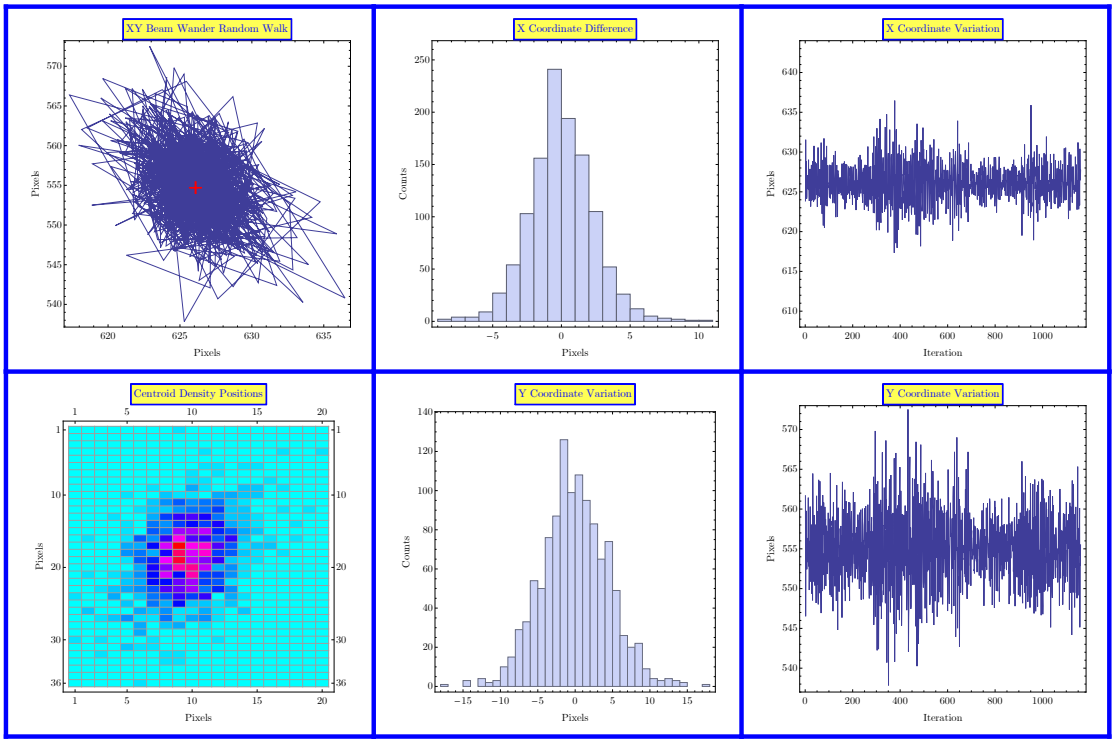


Figure 2.3: We report different statistical plot regarding the centroid distribution of the beacon laser on the camera for the feedback control of the focal plane.

for the Z axis were repeated for the X and Y directions: once the position with the highest power readings was found, the corresponding coordinates were saved in the system as *reference position*. At this point the feedback procedure is started: the camera grabs frames and a Matlab routine evaluates the deviations of the beacon centroid with respect to the reference position, sending then corrections to the motor controllers. In Figure 2.3 the 1161 corrections data referring to almost four hours of acquisition are presented. On the first column of the grid, top, a sort of random walk is reported which shows the series of consecutive deviations from the reference position. Every point represents an estimation of the centroid performed in average every 12 s: this parameter was optimized according the observed stability of the link. Once that the instructions are sent to the controllers, the stepping motors take in average 0.24 seconds to re-center the focal plane. From the bottom density plot, one can see that the beam wander tends to visit positions close to the center, being the centroid accumulated around the reference. This behavior indicates that the link was sufficiently stable over the acquisition. However, this stability was not symmetrical: if one considers the central column, the histograms of the difference between centroids coordinates and the reference, show clearly that the drifts in the Y direction were larger than those in X. More specifically, we had that within five pixels from the center, there were the 96% of the X corrections, while the 74% for Y. The cause

of this asymmetry could be addressed to the large eddies flowing with more intensity in a direction rather the other one. This is also confirmed by the third column were the absolute coordinates of the centroids are plotted for X and Y as function of the iteration. Besides the larger values for Y, one can notice also an increase in the turbulence activity starting approximately from the interaction 300: these deviations correspond to the peripheral points in the plots of the first column. However this behavior did not represent a problem because the system was designed to promptly correct even larger drifts.

#### Quantum and probe signals

The Alice module and the classic probe signal, as the computer operating the software for the telescope correction where housed inside the observatory. The optical Alice module was implemented on a breadboard, with two 850 nm attenuated lasers providing the quantum signal. The polarization of the 850 nm lasers was set to the two different bases by means of half wave plates and quarter wave plates. The encoding of the quantum signal was then obtained by controlling the lasers with an FPGA. For what concerns the transmitted qubits, in order to measure the QBER of the channel, we used the same data structure of a recent free-space QKD implementation based on the B92 protocol [**?**, **?**]. A raw key is composed into N packets of 2880 bits each, sent at the rate of 2.5 MHz; as regards the payload slots, Alice sends two qubits separated by 200 ns. Due to communication with the FPGA, each packets is sent every 20 ms resulting in an average sending rate of 150 kHz.

For the atmospheric probe for the estimation of the link transmissivity, a **Thorlabs LP808-SF30** fiber coupled diode laser $\lambda = 808$ nm laser was used. This laser was controlled by a temperature and current driver **Thorlabs ITC-4001**, which provided also the modulation of the signal. Classical and quantum lasers were coupled into single mode fibers and injected into a fiber beam splitter. One of the two beam splitter output was delivered toward to the telescope, cfr. Figure 2.2.

### 2.3.2 Bob

At the receiver part (Bob), in Tenerife, we used the 1 m aperture telescope of the ESA Optical Ground Station to receive the signals. This telescope has the peculiarity that it can be pointed horizontally. After the Coudé path, the collimated classical and quantum beams were divided by a dichroic mirror.

The qubits were measured in two bases, using PBS and waveplates (cfr. Figure 2.1). The counts detected by the two single-photon avalanche photodiodes, **Excelitas SPCM-AQRH**, were stored on a FPGA. The probe beam was detected by an high-bandwidth APD (avalanche photodetector) and the voltage amplitude signal stored by an oscilloscope.

The two FPGAs are synchronized every second by a pulse-per-second (pps) signal equipped by two GPS receivers located in the two islands.

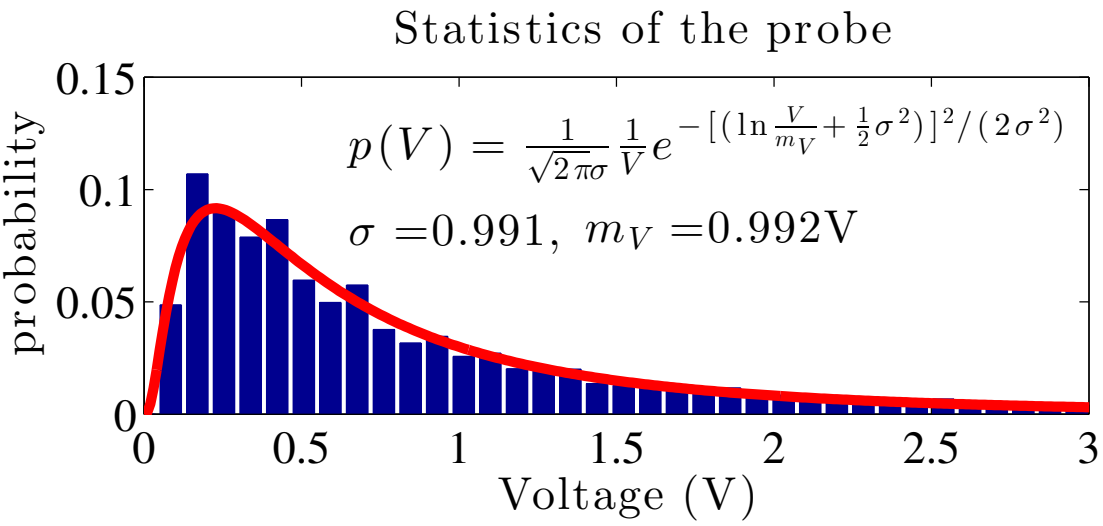


Figure 2.4: Experimental occurrences of probe intensities (measured by photodiode voltages) and lognormal fit.

### 2.3.3 The Log-normal distribution of the scintillation

Here we show the distribution of the measured voltages of the data used in Figure 2.5. According to the theory [61, 59], they follow a log-normal distribution. In Figure 2.4 we show the experimental probabilities of occurrence of different photodiode voltages corresponding to different probe intensities. We also show the corresponding log-normal curve that fits the experimental data. In the figure we report the log-normal parameters obtained in the fit.

## 2.4 Preliminary analysis

In order to test the ability of estimating the link transmissivity, we first sent on the same free-space channel, two signals: the classical probe, detected with a fast photodiode at the receiver, and a single strongly attenuated laser. The classical signal featured pulses of 100 $\mu$s duration at 1 kHz repetition rate, while the attenuated laser at 850 nm was a continuous beam. At the receiver, the quantum signal was detected by a Single Photon Avalanche Photodiode (SPAD) and acquired in packets with duration of 1 ms.

We would like to test the correspondence between the intensity of the received classical beam and the photons received on the quantum channel. In Figure 2.5 we show, for 11 s of acquisition time, the photon counts detected in each packet, compared to the voltage registered by the fast photodiode. As it can be seen in the inset, there is a strong correspondence between the two signals.

To demonstrate the correlation we performed the ARTS method, consisting in the following procedure. Given a set of $L$ packets (each of $1ms$ length), we let $V_i$ be the probe signal amplitude and $S_i$ the number of detected photons in the quantum signal

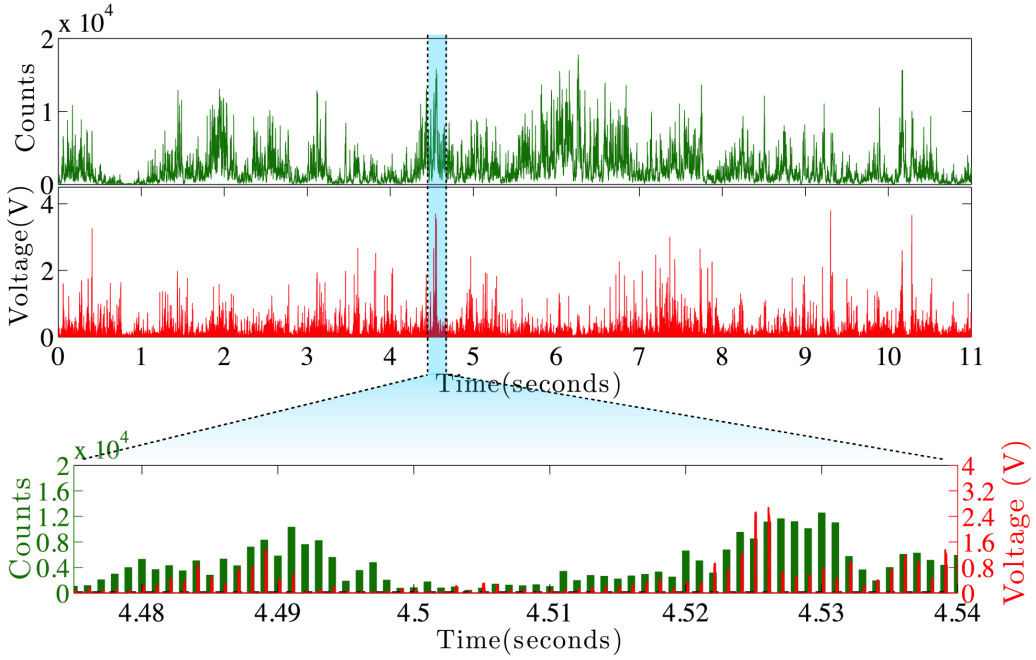


Figure 2.5: Comparison between the counts detected by the SPAD (green line) and the voltage measured by the fast photodiode at the receiver (red line). In the inset we show a zoomed detail of the acquisition in order to better appreciate the correlation between the quantum and classical signal.

for the $i$-th packet, respectively. We set a threshold value $V_{\mathrm{T}}$ for the probe voltage and post-select only those packets such that $V_i > V_{\mathrm{T}}$; in particular, we denote by $\mathcal{I}(V_{\mathrm{T}}) = \{i \in [1, L] : V_i > V_{\mathrm{T}}\}$ the indexes of the packets for which the above condition holds and by $N_{\mathrm{P}}(V_{\mathrm{T}})$ the corresponding number of packets, that is, $N_{\mathrm{P}}(V_{\mathrm{T}}) = |\{\mathcal{I}(V_{\mathrm{T}})\}|$. Furthermore, we define the following quantities:

$$S(V_{\mathrm{T}}) = \sum_{i \in \mathcal{I}(V_{\mathrm{T}})} S_i, \quad \overline{\mathcal{S}}(V_{\mathrm{T}}) = \frac{S(V_{\mathrm{T}})}{N_{\mathrm{P}}(V_{\mathrm{T}})} \tag{2.1}$$

with $S(V_{\mathrm{T}})$ representing the total number of detected bits and $\overline{\mathcal{S}}(V_{\mathrm{T}})$ the mean number of detection per packets after the post-selection performed with threshold $V_{\mathrm{T}}$.

The effect of the ARTS procedure can be clearly appreciated in Fig. 2.6, where $\overline{\mathcal{S}}(V_{\mathrm{T}})$ (normalized to the mean counts obtained without thresholding) is plotted (green line) as a function of the threshold: a higher threshold value corresponds to a larger mean number of counts per packet. This demonstrates that the probe and quantum signals are strongly correlated and one can significantly improve the signal-to-noise ratio (SNR) by thresholding[1]. As side effect, we have that the pre-selection also decreases the overall

[1]Here we define the SNR as the ratio between the overall signal (true signal plus background) and the background

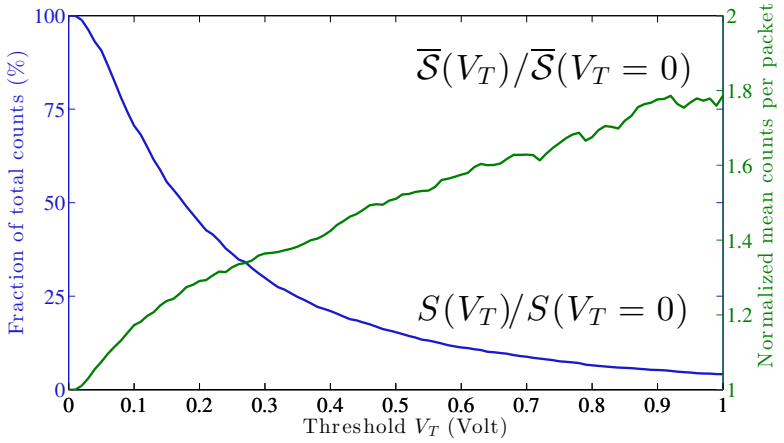


Figure 2.6: Mean counts per packet $\overline{\mathcal{S}}(V_\mathrm{T})$ (normalized to the mean counts obtained without thresholding) and fraction of total count $S(V_\mathrm{T})/S(V_\mathrm{T}=0)$ in function of the probe threshold.

number of detections in the transmission $S(V_\mathrm{T})$ as can be noticed by considering the ratio $S(V_\mathrm{T})/S(V_\mathrm{T}=0)$ (blue line).

## 2.5 Application of ARTS method to QKD

We then apply the results previously described to a QKD experiment. In particular, we will show that, increasing the SNR by thresholding gives, in some cases, benefits in terms of the secret key length, even if the total number of sifted bits will decrease. In fact, when the QBER is above 11%, the maximum QBER tolerable for standard QKD, ARTS will reduce the QBER below this limit, allowing secure key generation. We point out that at the receiver the beam has a mean photon number per pulse below 1, namely it is the single photon level. However, at the transmitter side, due to the 30 dB average attenuation of the channel we are not working in the single photon regime because the pulses contain in average more than one photon. However, our aim was to simulate a possible realistic scenario where one would employ fast (hundreds of MHz to GHz) free-space QKD systems which are nowadays commonly available. Since our system has a transmission rate of 2.5 MHz, the detected rate is comparable to the rate observable with a transmitter emitting true single photon pulses with a repetition rate of about 1 GHz, considering fixed the amount of optical and atmospheric attenuation.

First, given the number of errors $E_i$ in the $i$-th packet, we define the overall number of errors $E(V_\mathrm{T})$ and the quantum bit error rate $Q(V_\mathrm{T})$ in the post-selected packets as

$$E(V_\mathrm{T}) = \sum_{i\in\mathcal{I}(V_\mathrm{T})} E_i\,, \quad Q(V_\mathrm{T}) = \frac{E(V_\mathrm{T})}{S(V_\mathrm{T})}. \tag{2.2}$$

For evaluating the actual impact of the ARTS on the performance of a quantum key

distribution system, it is then important to study how the two complementary effects of thresholding: the increase of mean detected bits per packet $\overline{\mathcal{S}}(V_{\mathrm{T}})$ and the decrease of total detections $S(V_{\mathrm{T}})$ influence the achievable secret key rate of the system, and the optimal trade-off should be found.

Being the length of the output secret key dependent on the number of available sifted bits and on their bit error rate, as a first step we need to derive an expression for both of these quantities. As demonstrated in [59], the statistics of the transmission of a long free-space channel follows a log-normal distribution. The measured probe voltage at the receiver, being constant the transmitted intensity, follows the same distribution, given by $p(V; m_V, \sigma^2) = \frac{1}{\sqrt{2\pi}\sigma}\frac{1}{V}e^{-[(\ln\frac{V}{m_V}+\frac{1}{2}\sigma^2)]^2/(2\sigma^2)}$. In the previous expression $\sigma^2$ is defined as functions of the mean $m_V$ and of the variance $v_V$ of the probe intensities distribution, that is, $\sigma^2 = \ln\left(1+\frac{v_V}{m_V^2}\right)$. As an example, we show in Appendix, the distribution of the measured voltages of the data used in Figure 2.5, that, according to the theory [61, 59], follows a log-normal distribution.

In the following analysis, we assume that the number of detected photons and the probe intensity have completely correlated log-normal distributions [59]. This hypothesis implies that both distributions have the same parameter $\sigma^2$. Then, we can predict the number of packets above threshold $N_{\mathrm{P}}(V_{\mathrm{T}})$ and the number of sifted bits surviving the thresholding $S(V_{\mathrm{T}})$ in case of null background by $S(V_{\mathrm{T}})/S(0) = \int_{V_{\mathrm{T}}}^{+\infty}\frac{V}{m_V}p(V; m_V, \sigma)dV$ and $N_{\mathrm{P}}(V_{\mathrm{T}})/N_{\mathrm{P}}(0) = \int_{V_{\mathrm{T}}}^{+\infty}p(V; m_V, \sigma)dV$. By taking into account the background clicks we get:

$$\begin{aligned} N_{\mathrm{P}}(V_{\mathrm{T}}) &= N_{\mathrm{P}}(0)\frac{1}{2}\left[1-\mathrm{erf}\left(\frac{\ln\frac{V_{\mathrm{T}}}{m_V}+\frac{1}{2}\sigma^2}{\sqrt{2\sigma^2}}\right)\right]. \\ S(V_{\mathrm{T}}) &= n_b N_P(V_{\mathrm{T}}) + \frac{1}{2}[S(0) - n_b N_P(0)]\left[1-\mathrm{erf}\left(\frac{\ln\frac{V_{\mathrm{T}}}{m_V}-\frac{1}{2}\sigma^2}{\sqrt{2\sigma^2}}\right)\right], \end{aligned} \tag{2.3}$$

where $n_b$ is the average background count per packet. In fact, the assumption of complete correlation between the quantum and the probe signal, is not strictly verified in our experiments and eq. (2.3) turns out to be an approximation of the experimental values. Still, it allows to derive an effective post-selection threshold, as will be seen in the following (e.g., in figure 2.7).

We now define a further predictive model for estimating the bit error rate on the quantum channel as a function of the probe threshold. Let us assume that the average bit error rate on the quantum channel is $m_Q$ and that the number of counts per packet due to background noise is $n_b$. Now, since background counts output a random result, the corresponding bit error rate is 1/2, and we can write the predicted quantum bit error rate $Q_{th}$ as a function of the threshold $V_{\mathrm{T}}$, namely,

$$Q_{th}(V_{\mathrm{T}}) = m_Q\left(1-\frac{n_b}{\overline{\mathcal{S}}(V_{\mathrm{T}})}\right)+\frac{1}{2}\frac{n_b}{\overline{\mathcal{S}}(V_{\mathrm{T}})} \tag{2.4}$$

where the predicted value for $\overline{\mathcal{S}}(V_{\mathrm{T}}) = \frac{S(V_{\mathrm{T}})}{N_{\mathrm{P}}(V_{\mathrm{T}})}$ is obtained by using equation (2.3). Given these quantities, the asymptotic key rate of a QKD system based on the BB84

protocol[62] and the ARTS procedure (namely the probe thresholding mechanism) reads as follows:

$$R(V_{\mathrm{T}}) = \frac{S(V_{\mathrm{T}})}{S(0)} \left[1 - 2h_2\left(Q(V_{\mathrm{T}})\right)\right] \tag{2.5}$$

It is worth noting that to take into account the asymptotic rate instead of the finite-length one [63, 64], may be considered a restrictive approach, especially because the post-selection further reduces the number of available sifted bits. However, it is sufficient to choose the size of the blocks to be fed as input to the key distillation procedure (i.e., information reconciliation and privacy amplification) such that, without loss of generality, the asymptotic bound provides a reasonable approximation of the actual rate. It is worth to stress that the B92 protocol for a depolarizing channel has a higher QBER with respect to the one of BB84 protocol. We used this approach however to compare our results with other protocols being this experiment the first proof of principle of this method. We are aware that this mismatch might imply a slight discrepancy with respect a strong security analysis.

In Figure 2.7, we finally compare the theoretical (solid blue line) and the experimental values (blue crosses) for the measured QBER and the asymptotic key rate as a function of the probe intensity threshold in a data acquisition. The curves for the theoretical QBER and for the key rate were obtained by substituting maximum likelihood estimates for the log-normal parameters $m_V$ and $\sigma^2$ in eq. (2.4) and in eq. (2.5). The other two parameters, $S(0)$ and $N_{\mathrm{P}}(0)$, needed for predicting $S(T)$ and $N_{\mathrm{P}}(T)$, are directly measured (they correspond to the total sifted bits and the total number of packets received respectively).

The experimental data refer to an acquisition of $5 \cdot 10^5$ sifted bits in condition of high background, simulated by a thermal light source turned on in the receiver laboratory. The intensity of the background was chosen in order to obtain a mean QBER larger than 11%. In particular, we measured an average value of $n_b = 35.17$ for the background clicks per packet and we assume $m_Q = 5.6 \cdot 10^{-2}$. As clearly shown in the figure, eq. (2.4) provides a good approximation of the experimental curve.

As one can appreciate from the same Figure, we have a remarkable correspondence between the shape of the theoretical rate, $R_{th}$, and the measured rate, $R_{exp}$. The fact that the experimental points do not fit the expected curve can be ascribed to the discrepancy in the empirical joint distribution of probe intensities and counts with respect to the model; in particular, we measured the following fitting parameters for the normalized log-normal distributions: $\sigma_V^2 = 0.967$ for the probe intensities and $\sigma_S^2 = 0.716$. However, the derivation of the optimal threshold for maximizing the secret key length (magenta dashed line) from the probe distribution yields the optimal $V_{\mathrm{T}}$ also for the experimental data. In particular, the optimal threshold inferred from the probe distribution is $V_{T,\mathrm{opt}}^{(\mathrm{th})} = 375$ mV, and coincide with the one resulting from optimization on the experimental data, yielding a rate of $R(V_{T,\mathrm{opt}}^{(\mathrm{th})}) = 5.55 \cdot 10^{-2}$.
Also, we observe that for $V_{\mathrm{T}} < 70$ mV no key can be extracted, being the QBER higher than the theoretical maximum (i.e., $Q = 11\%$), whereas by increasing the threshold value a non-zero secret key rate is achievable. With the optimal threshold value, the measured

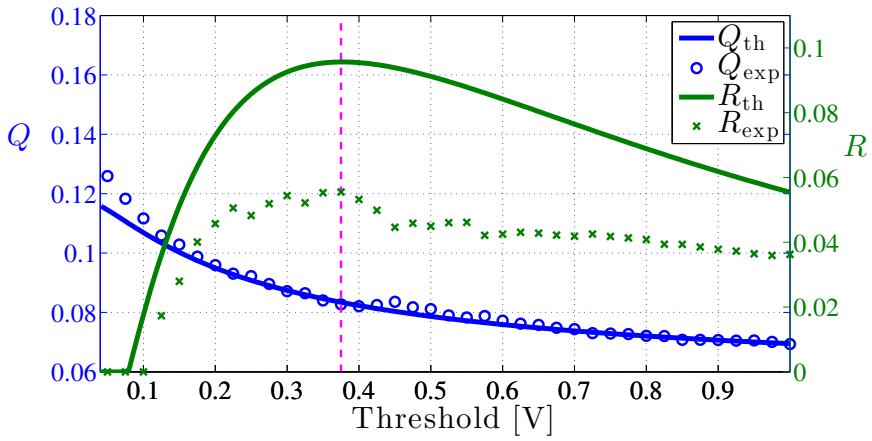


Figure 2.7: Experimental QBER ($Q_{\mathrm{exp}}$) and secure key rate ($R_{\mathrm{exp}}$) in function of the probe threshold (measured by the photodiode voltage). With solid lines with show the corresponding theoretical predictions ($Q_{\mathrm{th}}$ and $R_{\mathrm{th}}$).

QBER is $Q(V_{T,\mathrm{opt}}^{(\mathrm{th})}) = 8.38 \cdot 10^{-2}$; a significant gain with respect to the initial value, $Q(0) = 13.14 \cdot 10^{-2}$ is therefore achieved. Finally, we observe that for increasing values of $V_{\mathrm{T}} > V_{T,\mathrm{opt}}^{(\mathrm{th})}$ the QBER still decreases, but so does the rate, since the reduction in the residual number of sifted bits does not compensate the advantage obtained from the lower QBER. This result is of absolute practical relevance, as it shows that leveraging the probe intensity information is an enabling factor for quantum key distribution, allowing to distill a secret key.

As for the security of this post-selection approach as applied to a QKD system, we conjecture that no advantage is delivered to a potential attacker in the true single photon regime, being the thresholding nothing but a further sifting step on the received bits [56, 57]. If the attacker tried to force Alice and Bob to post-select a particular bit, in fact, she would alter the probe signal *before* the disclosure of the preparation bases on the public channel, and, therefore, before she could actually know if her measured bit is correct. On the other hand, altering the probe statistics or interrupting the probe transmission would not yield any advantage to the attacker, as it would just break the correlation between the quantum and the classical signal and would thus result in a denial of service attack. The security analysis gets more involved if we allow *photon number splitting* (PNS) attacks. In that case, the attacker may force Bob to receive just the qubits for which the PNS attack was successful, i.e., only those pulses with multiple photons. A decoy state protocol may counteract this strategy, but its effectiveness with a turbulent free-space link has to be investigated.

### 2.5.1 Comparison with other methods

The advantage of the ARTS with respect to other techniques, lies in the fact that it is a real time and self-adapting procedure. On this regard, one can consider the CAD1 and CAD2 distillation schemes discussed in [56]. These schemes represent a generalization of Maurer's advantage distillation technique [58]. They collect sequences of correct (possibly non consecutive) sifted bits, and distill one single secure bit out of each sequence. The length of each sequence should be chosen according to a tradeoff. In fact, longer sequences allow to distill keys with higher channel QBERs, but provide a lower key rate in the case of low QBERs. However, in a turbulent, rapidly time-varying channel, its effectiveness would be limited by the difficulty of choosing the suitable parameters of the distillation strategy according to the varying QBER.

Another generalization of the advantage distillation in [58] is proposed in [57], where parities for many pairs of bits are shared between Alice and Bob along the public channel and those pairs with non matching parities are discarded, while the remaining ones (over which the QBER is lower) are syndrome decoded. However, the above presented distillation methods do not take advantage of the intrinsic QBER variability of the channels, rather they rely on the assumption that the channel maintains its QBER stable for long so that parameters can be optimized.

More similar to ARTS is the method introduced in [55]: it relies on detecting transmissivity peaks in the channel by observing variations of the sifted bit rate and can hence be quite effective in dealing with turbulent channels. More precisely, a post-selection is performed when the number of received sifted bits is above a given threshold, determined by the mean QBER of the channel. The post-selection is effective only when the threshold is set in order to get at least several bits for coherence time of the channel (typically of the order of few milliseconds): in fact, only in this condition it is possible to post-select the correct instants of high transmissivity. In the case of very turbulent channel and extreme environmental conditions (say mist or high humidity), the number of received bits per coherence time of the channel can be lower (or of the order) than 10: in this case, the post-selection cannot be implemented and only the ARTS method becomes effective.

We performed a simulation to compare the two techniques by assuming that the probe and the signal statistic are perfectly correlated. The rate achievable in the two cases are shown in Figure 2.8, demonstrating that the ARTS methods outperform the post-selection on the received sifted bits when the number of mean sifted bits received per coherence time of the channel are below $\sim 10$ and the SNR is below 20.

## 2.6 Conclusions

We have presented a proof of principle demonstration of a method exploiting the atmospheric turbulence as a resource for QKD. The turbulence will implies a fluctuating transmissivity of the channel used for quantum communication. The ARTS method, easily integrable in current QKD systems, is based on the sampling of a classical beam

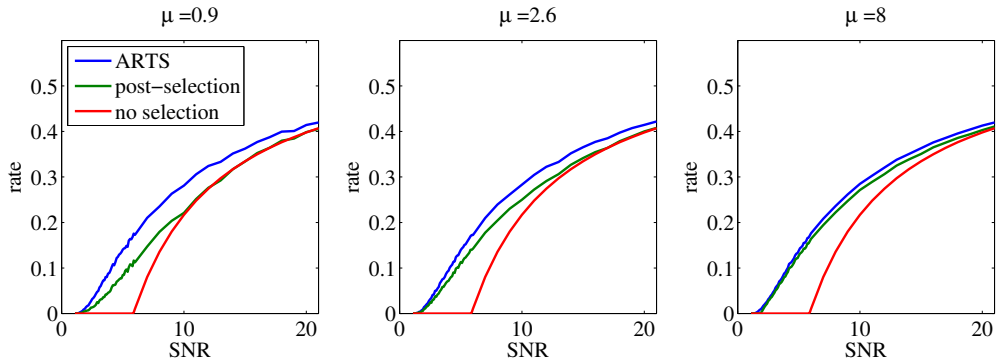


Figure 2.8: Comparison between the rates achievable by the ARTS, the post-selection and the standard QKD technique (no selection). We assumed that the channel QBER is 3% and the lognormal parameter is $\sigma = 1$, similar to the parameter we measured in the tested free-space channel. The parameter $\mu$ is the mean sifted bits per coherence time of the channel.

(probe signal) sent on the same channel of the quantum bits. By measuring the intensity of the probe at the receiver, it is possible to select in real time the best time slots of high channel transmissivity. We demonstrated that with the ARTS method we were able to decrease the measured QBER; moreover, this method allows to extract secret key in extreme conditions, namely when the initial average QBER is above the security threshold of 11%.

# Chapter 3

# A true random number generator based on the optical turbulence.

What in the previous Chapter represented the *noise*, in this Chapter will be the *the signal*. We will describe a novel principle for a *true random number generators* TRNG based on the observation that a coherent beam of light crossing a long path with atmospheric turbulence may generate random and rapidly varying images. To implement our method in a proof of concept demonstrator, we used the same free space optical link employed for the QKD experiment at the Canary Islands. Here, after a propagation of 143 km at an altitude of the terminals of about 2400 m, the turbulence in the path is converted into a dynamical speckle at the receiver. In Section 3.1 we will present why it has been hypothesize that atmospheric turbulence can be a suitable source of entropy. Section 3.2 is divided in two parts: in the first one we will give a characterization of the optical link in order to individuate the optimal setting for the sampling of the turbulent physical noise, in the second one we will present evidences that indeed the obtained samples (the spatial coordinates of the speckles) are independent in time and uniformly distributed. In Section 3.3 we will present the algorithm based on the combinatorial analysis to extract randomness from the images and we will show that is optimal in the context of Information Theory. Section 3.4 will be devoted to the presentation of statistical tests for randomness assessment while, in Section 3.5 the results will be discussed.

## 3.1 Introduction

This work was based on the observation that a laser beam propagating across a free space optical channel, in addition to the beam wandering and beam spreading already presented in the previous Chapter, at the end of the link features a *speckled* intensity wavefront in presence of strong atmospheric turbulence. Practically, at the receiver side one does not observe a gaussian intensity profile but collection of light and dark spots varying in number, shape and position randomly, according the atmospheric turbulent flow.

Under an abstract point of view aimed then to investigate whether the observed

phenomenon could be a source of entropy and in the affirmative case the possibility of extracting uniform and independently distributed random variables from it. Under a more practical point of view we were interested to proof the feasibility of a TRNG based on a macroscopic physical process to be in case employed in protocols of optical secure communications.

The working principle of a TRNG consists of sampling a natural random process and then to output an uniformly distributed random variable. The sources of entropy mainly exploited are all *microscopic* and they include the amplification of electronic noise [65], phase noise of semiconductor lasers [66], unstable free running oscillators [67] and chaotic maps [68]. There are at least two issues with TRNGs. The first one is theoretical and is about the fact that a chaotic physical system has a deterministic evolution in time. More specifically, one has that the dynamic of a classical physical system is written by its equations of the motion and the initial conditions of its degrees of freedom: once that both are known, the future (as the past) states of the system can be predicted. In general, the impossibility to know precisely the initial conditions of a system leads to the unpredictability about its evolution (naturally there are different degrees of unpredictability, according the system considered). In particular, a chaotic system features an evolution which is sensitive to the initial conditions: although it *appears random*, the dynamic is still deterministic and so, in principle, predictable.

An analysis of the physical system used to generate the numbers is then fundamental for selecting those conditions which will not lead the system to some periodical, completely predictable trajectory [69, 70]. This selection can be performed by means of a robust statistical model for the physical system. On this regard can be interesting to cite the work of P. Diaconis et al. [71], where the authors were able to individuate a set of initial conditions for an experimental device which flipped coins, such that the coin landed showing always the same face.

The second problem deals with the unavoidable hardware non-idealities which spoil the entropy of the source, e.g. temperature drifts modify the thresholds levels, or the amplifier stages make spurious technical noise to leak inside the random signal. Most of the TRNGs are then forced to include a final post-processing stage with the purpose of increasing the entropy of the emitted bits.

In our case, we individuated the source of entropy in the atmospheric turbulence. Atmospheric turbulence is characterized by a chaotic dynamic. These are mainly ruled by temperature variations and by the wind, and cause inhomogeneities in the air refractive index. Consequently, when a laser beam is sent across the atmosphere, this latter may be considered as a dynamic macroscopic volumetric scatterer of different scales. These scatterers, which are in motion according the turbulent flow of the air masses, affect both the amplitude and the phase of the propagating field: basically one has that the resultant field $\mathbf{E}(x, y, t)$ at a given space and time at the receiver, can be written in the complex phase-space as a sum

$$\mathbf{E}(x, y, t) = e^{i\omega_0 t} \sum_n E_n(x, y, t) e^{i\phi_(x,y,t)} \tag{3.1}$$

where the amplitudes $E_n(x, y, t)$ and phases $\phi_(x, y, t)$ depends on the single scatterer.

Practically, the field undergoes a random walk in complex space: the observed speckle pattern given by the square of the field depends on how the different random contributions add together, in particular they can add constructively or destructively according the distribution of the relative phase and amplitude of the components.

The point is then that the observed optical noise is the product of a field which along its 143 km path interacted with a number of moving scatterer *very* unfeasible to determine and whose chaotic motion is *very* unfeasible to predict. Indeed the present time models for atmospheric dynamic only provide a statistical description for the spot of the beam and its wandering [72, 28, 73] and never an instantaneous prediction for the irradiance distribution (which could be calculated by the Laplace demon only).

A beam of coherent light propagating along a random scatterer was studied in the context of the random walk. Indeed, the complex field undergoes subsequent diffusion process which according to the type of medium may be either described as a normal random walk or as a Lévy flight [74], giving rise to a random distribution of the intensity as consequence of the interference effects [75]. Static speckle patterns obtained by passing a laser beam through volumetric scatterers [76, 77] have been already exploited for the purpose of random number generation and as key element of physical un-clonable functions [78]. However, these approaches are based on still scattering medium and cannot be used for real time random number generation.

## 3.2 Characterization and sampling of the physical noise

We established a free space optical (FSO) link 143 $km$ long by sending a $\lambda = 810\,nm$ laser beam between the *Jacobus Kaptein Telescope* (JKT) in the Island of La Palma, to the ESA *Optical Ground Station* (OGS) in the Island of Tenerife (see Figure 3.1 for details) channel already employed in several experiments of Quantum Communications[20, 79, 80, **?**]. The intensity of the laser was adjusted in order to conveniently exploit the camera dynamic range to properly acquire the typical effects of beam propagation in strong turbulence, including wandering, beam spreading and scintillation [72]. As seen in the previous Chapter, the motion of eddies larger than the beam cross section, bends it and causes a random walk of the beam center on the receiver plane. Whereas, small scale inhomogeneities diffract and refract different parts of the beam which then constructively and destructively interfere giving rise to a speckle pattern on the telescope pupil. Both the previous factors spread the beam beyond the inherent geometrical limit. Furthermore, it is possible to observe scintillation, namely fluctuations in the irradiance of the signal.

In free-space optical propagation, the speckle pattern formation can be addressed to interplay between the degree of atmospheric turbulence and the optical beam propagation length. The strength of the turbulence is quantified by the structure constant $C_n^2$ (dimensions $[L]^{-\frac{2}{3}}$) which expresses the spatial fluctuation of the air refractive index [72]. Typically, values for *weak turbulence* are in the order of $10^{-16}\ m^{-2/3} \sim 10^{-18}\ m^{-2/3}$ whilst, for strong turbulence, $C_n^2 = 10^{-13}\ m^{-2/3} \sim 10^{-14}\ m^{-2/3}$. To estimate the turbulence effects on a laser beam, it is necessary to evaluate the *Rytov variance*, defined

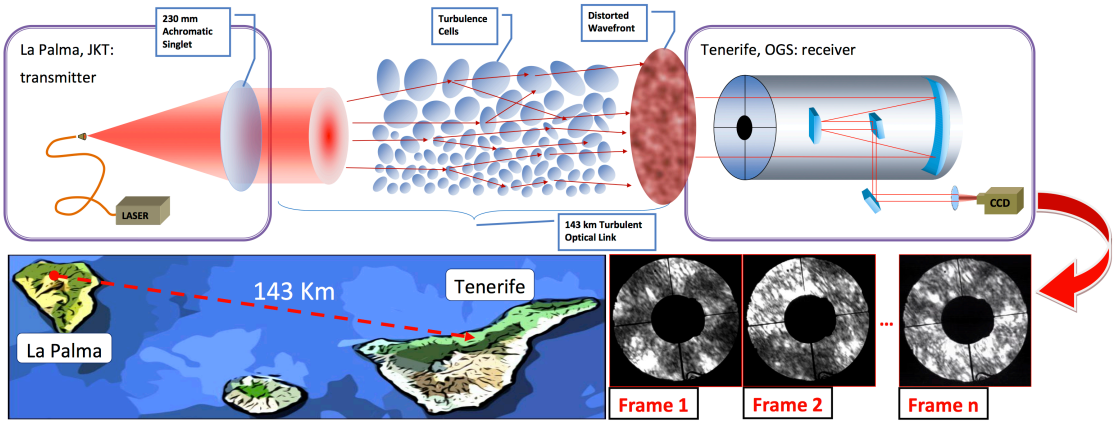


Figure 3.1: Experimental setup. At the transmitter side in La Palma, a $\lambda = 810\,nm$ laser beam is collimated with a $230\,mm$ achromatic singlet, explicitly realized to limit geometrical distortions, and then sent through a $143\,km$ free space optical channel. At the receiver side, at the OGS observatory in Tenerife, the pupil of the Ritchey-Chrétien telescope (diameter of $1016\,mm$) is illuminated by the distorted wave-front and imaged on a high resolution CCD camera. This figure was produced by the authors.

as

$$\sigma_R^2 = 1.23 k^{7/6} C_n^2 L^{11/6} \tag{3.2}$$

where $k$ is the modulus of the wave-vector and $L$ the length of the path. Indicatively, one has strong or weak effects for $\sigma_R^2 > 1$ or $\sigma_R^2 < 1$ respectively [81]. In particular, significant beam wandering and intensity speckles are observed at the receiver when $\sigma_R^2$ overtakes unity: the weaker is the level of turbulence, the longer has to be the link in order to get a random optical dynamic. For the link between La Palma and Tenerife we estimated a night-time average structure constant $C_n^2 \approx 3 \cdot 10^{-17}\ m^{-2/3}$: this value is consistent with the values obtained in other studies, i.e. [82]. Recently, in [32] a $C_n^2$ oscillating between $\approx 5 \cdot 10^{-16}\ m^{-2/3}$ and $\approx 4 \cdot 10^{-17}\ m^{-2/3}$ has been reported. With the estimated $C_n^2$ and $L = 143$ km, we had $\sigma_R^2 \approx 11$ such that the condition for the speckle pattern formation was always satisfied. This can be appreciated from Figure 3.2 where $\sigma_R^2$ is plotted as function of $L$ for different values of the structure constant, ranging from weak turbulence $C_n^2 = 10^{-17}\ m^{-2/3}$ to strong $C_n^2 = 10^{-13}\ m^{-2/3}$. Practically, although the Canary Island link is characterized by a weak - middle level of turbulence during the night (green shaded area in the plot), thanks to the length of the channel we were constantly working in a condition of large, i.e. $> 1$, Rytov variance. Moreover, from the plot it is interesting to notice that speckles on shorter scales, could be observed only if the strength of the turbulence would sufficiently high according the trends.

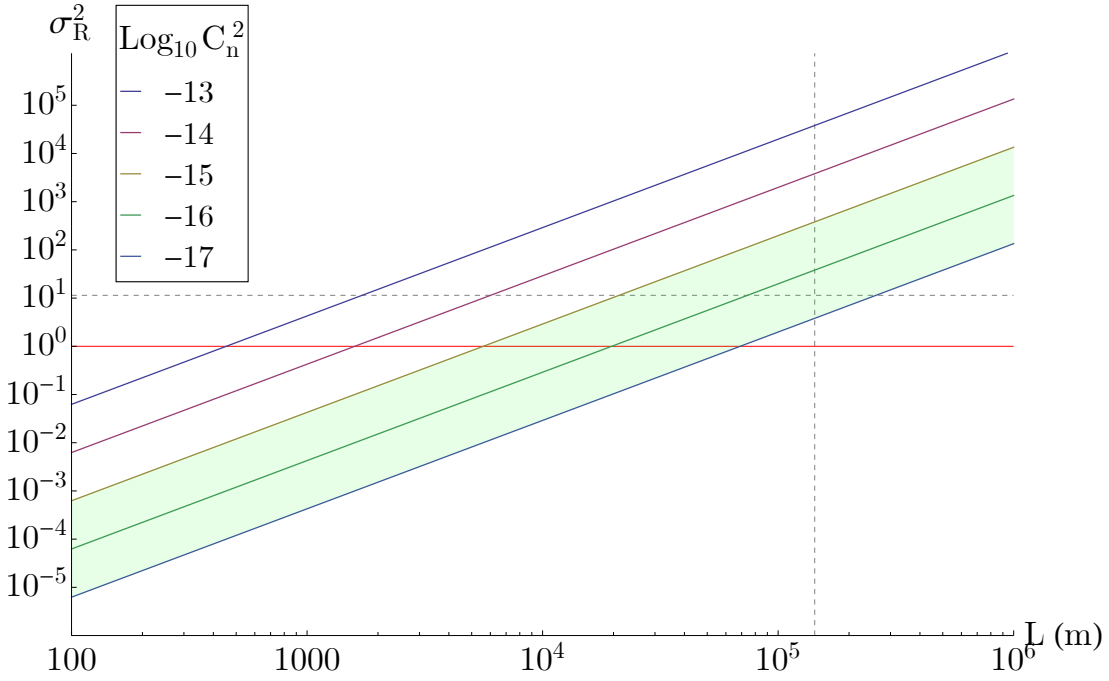


Figure 3.2: Rytov parameter is plotted in function of the length, for different levels of turbulence as measured by the structure constant. It is then possible to observe that by increasing the length of propagation, the Rytov parameter reaches the level of strong optical turbulence also in regimes of weak turbulence. In particular the shaded area refers to the degree of turbulence we registered in the Canary Islands: for a path length of 143 km we got a Rytov variance $\sigma_R^2 \approx 11$, value which allowed us to observe the speckle pattern.

### 3.2.1 Physical characterization of the link

As consequence of the turbulence and of the link length, at the pupil of the receiver ESA telescope, we observed the continuous random speckle pattern moving according the unpredictable flow of the atmosphere. Images where then acquired with a *Thorlabs DCC-1545* CMOS camera featuring a resolution of 1280 x 1024 pixels. A typical frame is reported in Figure **??**: since we were interested in evidencing the complex spatial distribution of the speckle intensity, it was necessary to properly set the frame rate and the acquisition in order to not smooth out the pattern and/or register correlated frames. This can be the case if the sampling rate is too high with respect to the proper time scale of the phenomenon (which we can relate to the time scale of the scintillation, see below).

Setting an exposure times of 3 ms and a sampling rate of 12 and 25 fps was the optimal choice in order to achieve a level of light sufficient to reveal the complexity of

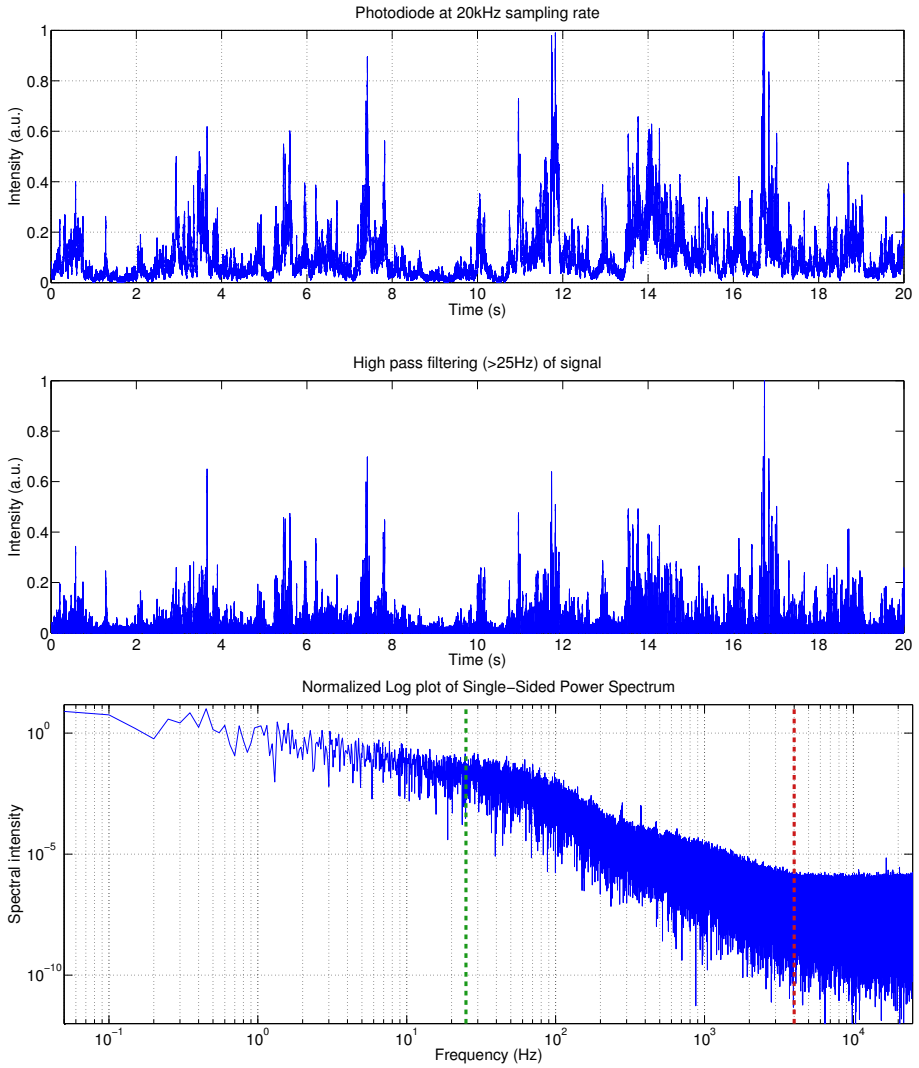


Figure 3.3: (top graph) Full intensity received by the telescope acquired with a photodiode with sampling rate of 20kHz. (middle graph) Intensity pattern with all the frequencies below 25Hz (frame rate of the camera) filtered. (bottom graph) Frequency spectrum of the intensity. Green dashed line represents the maximum frame rate of the camera (25Hz), while red dashed line represents the frequency (4kHz) above which the noise becomes dominant (flat spectrum).

the intensity pattern while not blurring its structure. Moreover, the interval between consecutive frames was set to be longer than 10 ms, which is the typical time scale of the scintillation induced by the atmosphere. With such frame rates it was possible to generate independent and uncorrelated speckle distributions.

More in detail, this can be understood considering the intensity of the received signal integrated over all the telescope aperture and acquired with a photodiode at a sampling rate of 20 kHz, as reported in Figure 3.3 (top). The signal is characterized by a sequence of intense peaks spanning well above the average value, which is a common behavior for beams along strong turbulence. Its dynamics extends in frequency well above our maximum frame rate, as is shown in Fig. 3.3 (middle), in which the signal is filtered leaving the components greater than 25 Hz: the relevant structure of the peaks is actually preserved.

Equivalently, the spectral content of the scintillating signal that is shown in Fig. 3.3 (bottom), clearly attest that the 25 fps frame rate is not oversampling the scintillation process. Indeed, if the integrated intensity is characterized by such dynamics, spatial pattern of the intensity will present at least the same dynamics. Therefore consecutive frames will freeze completely different realizations of the beam profile.

In Fig. 3.4 a plot is reported obtained by mapping the correlations in intensity between the same pixels but on different frames. More precisely, for each pixel of the sensor, we evaluated the serial correlation coefficient $C_i = \frac{n\sum_f I_f^i I_{f+1}^i - \left(\sum_f I_f\right)^2}{n\sum_f I_f^2 - \left(\sum_f I_f\right)^2}$ with $i \in [1, \ldots, 1280 \times 1024]$ between the intensity values $I_f^i$ cycling on the frames $f$, and we assigned the evaluated coefficients to respective pixels. The $C_i$s are expected to be null, if the intensity values are uncorrelated, otherwise 1 or -1 for strong correlation or anti-correlation respectively. The area of the telescope pupil was not completely available due to the optical structure holding the secondary mirror: by observing Fig. 3.4 one can notice that the regions of full correlation are those ones which are were reached by the light. On the contrary, for the pupil active area we have an average correlation of $C_{av} = 0.16$. Moreover, the analysis of the correlation was relevant also to exclude from the active area those pixels constantly yielding the same intensity values, because they were defective or because of additional optical obstructions.

### 3.2.2 Stability of the link

The optical link used for the experiment has been deeply studied and characterized for the experiments of Quantum Communications of the last decade. In good weather conditions, we measured an average attenuation of about 30 dB over 90 minutes of acquisition. As one can observe from Fig. 3.5 the link transmission is stable for the whole acquisition time. This feature has been observed also for longer time interval: naturally in case of cloud activity, the link would suffer deep additional losses, which in the worst case obstacle completely the channel.

### 3.2.3 Centroids: the center of mass of the speckles

Considering the logic scheme of a TRNG, once that the random noise is sampled, one has to set a rule in order to extract the i.i.d random variable. In our case, the random noise was the bi-dimensional nonhomogeneous, i.e. not gaussian, distribution of the laser beam intensity. The samples were the images. However, before setting a rule we needed

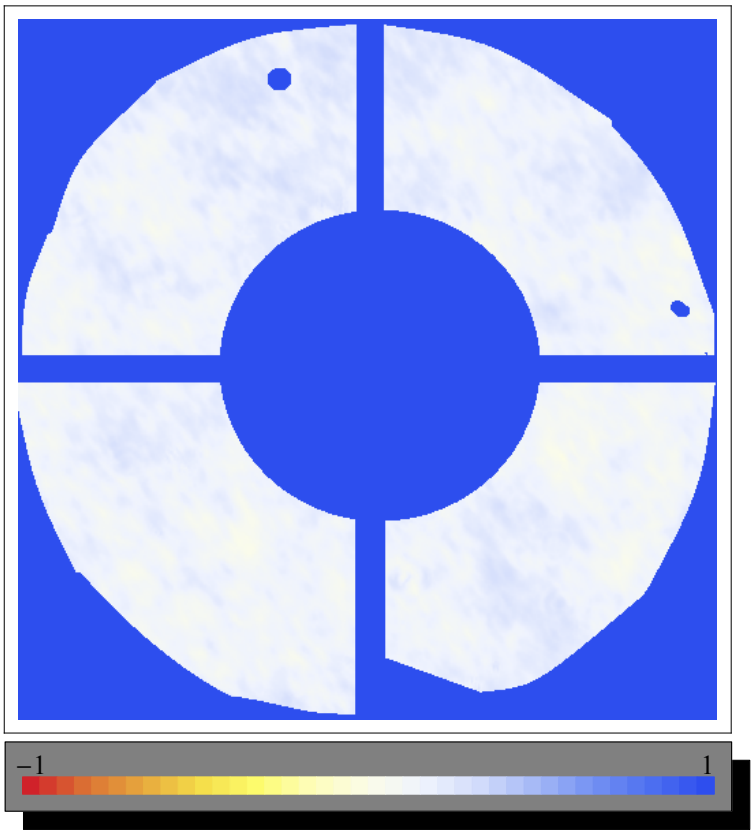


Figure 3.4: In this plot the intensity correlation between pixels belonging to 336 consecutive frames is reported.

to associate a random variable to the sampled noise. For this purpose we processed the frames in order to extract the coordinates of the different intensity spots.

Typical algorithms for image analysis which allow to compute several so-called digital *moments* were employed. More precisely, given $E$ the number of bits used by the acquisition software to encode the intensity (color) levels of monochromatic light on the active area $m \cdot n$ of the sensor, we can consider the recorded image as a two variables function $I(x, y)$ where $x \in \{0, \ldots, m\}$, $y \in \{0, \ldots, n\}$ and $I(x, y) \in \{0, \ldots, 2^E\}$. The $(j, k)^{th}$ moment of an image is then defined as

$$M^{jk} = \sum_{x=1}^{m} \sum_{y=1}^{n} I(x, y) x^j y^k \quad . \tag{3.3}$$

The *center of gravity* $C$, the so-called *centroid*, of an image is then located at position $(\widehat{x}, \widehat{y})$ where the coordinates are accordingly given by

$$\widehat{x} = \frac{M^{10}}{M^{00}}, \qquad \widehat{y} = \frac{M^{01}}{M^{00}} \tag{3.4}$$

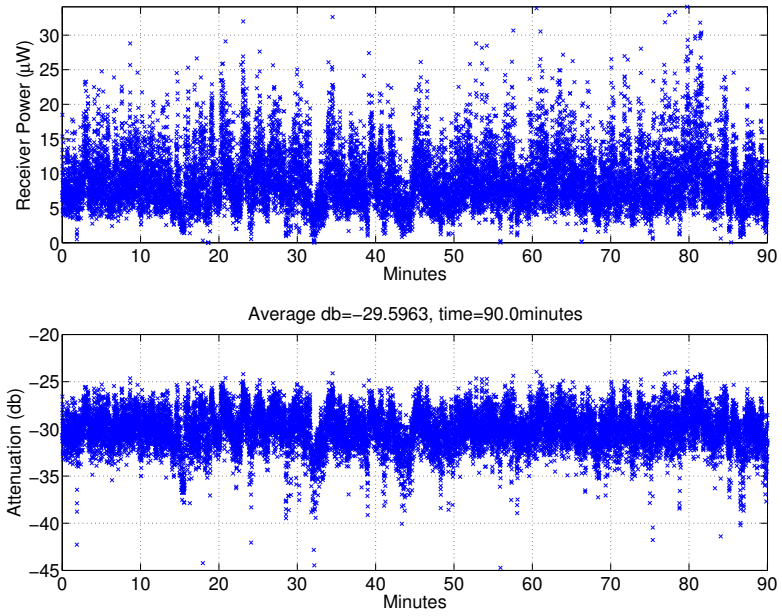


Figure 3.5: Power intensity received and the corresponding attenuation, measured across the 143 kilometers long optical link: the average measured attenuation is 30 dB.

We applied then a technique for instance used in Biology to count the number of cells in biological samples. Indeed in images composed by distinguishable components (as coloured cells on a uniform background), it is possible to *locally* calculate the centroids $C_i$ of those components, by binarizing the intensity level, i.e. by setting $E = 1$, and then evaluating the moments on the closed subsets $S_i = \{(x, y)|I(x, y) = 1\}$, that is

$$M_{jk}(S_i) = \sum_{(x,y)\in S_i} I(x, y)x^j y^k \tag{3.5}$$

where the index $i$ runs on the different elements of the image.

To extract more randomness from the geometrical pool of entropy, the intensity profile of the frames has been partitioned into eight different sub-levels. We treated separately every different intensity level, $L$, as a source of *spots*; more specifically then we generated sets $S_{L,i}$ out of the $L \in \{1, \ldots, 8\}$ levels. For a given $L$ and a spot $i$ the coordinates of a centroids are then

$$\widehat{x}_{L,i} = \frac{1}{A_{i,L}} \sum_{x\in S_{i,L}} x \qquad \widehat{y}_{L,i} = \frac{1}{A_{i,L}} \sum_{y\in S_{i,L}} y \tag{3.6}$$

where $A_{i,L}$ simply the area of the spot, that is the total number of pixels which compose that spot. In order to remove edge effects due to the shape irregularities of the pupil, pixels close to irregular edges were removed.

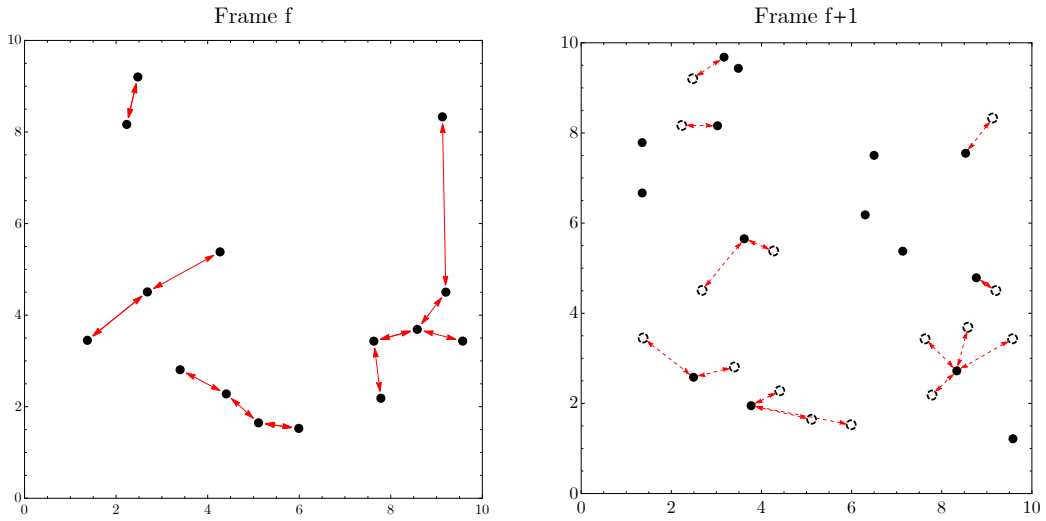


Figure 3.6: On the left, the distances $d^f_{intra}$ between closest neighboring centroids are evaluated inside the same frame $f$. On the right, the centroids of the frame $f$ are brought to next frame $f+1$ (dashed circles) and then the distances $d^{f-f+1}_{inter}$ between the time-shifted closest neighbouring centroids are evaluated.

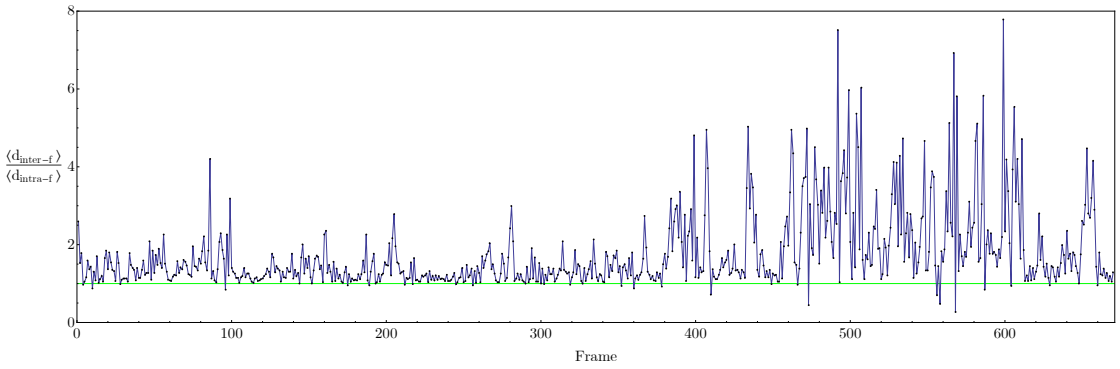


Figure 3.7: Distribution of the experimental ratios $\frac{\langle d^{f-f+1}_{inter}\rangle}{\langle d^f_{intra}\rangle}$.

The analysis follows with some techniques we applied in order to evaluate the temporal independence of the centroids position, and their identical distribution on the active area of the sensor.

In order to quantify the topological correlation between centroids of consecutive frames, we applied the following procedure. Given a frame $f$, we evaluated the distances $d^f_{intra}$ between closest neighboring centroids, and its average $\langle d^f_{intra}\rangle$. Then by transferring the centroid coordinates of this frame to the next one, $f+1$, we evalu-

ated the average distance $\langle d_{inter}^{f-f+1} \rangle$ between the centroids of the frame $f$ and the closest neighboring centroids belonging to the frame $f+1$, see Figure 3.6.

The ratio $\frac{\langle d_{inter}^{f-f+1} \rangle}{d_{intra}^{f} \rangle}$ is then plotted in Figure 3.7: considering the tri-dimensional distribution, i.e. sensor area on more frames, one has that the ratios would be null, if the centroid positions did not evolve in time. Moreover, if consecutive frames were highly correlated, their coordinates would not feature a significant difference from to frame. In other words, in presence of strong correlation the movement of each centroid is lower than the typical distance between centroids and the ratios $\frac{\langle d_{inter}^{f-f+1} \rangle}{d_{intra}^{f} \rangle}$ would attain a value close to zero.

On the contrary, one can notice that the ratios are of the order of 1 or higher, and when the number of centroids decreases in a transition $f \to f+1$, the ratio becomes greater than 1: this means that the relative positions between centroids changes from frame to frame. The number of centroids varies as well: the increasing (decreasing) trends in the plotted ratios, indicates that the spatial distribution becomes sparser (denser), i.e. also the number of centroids fluctuates following the scintillation.

For what concerns the spatial uniformity, in Figure 3.8 a stacked plot of the centroid distribution on the sensor active area is given, acquired at 12 fps. As one can notice, the centroids spread homogeneously without avoiding any region of the detector (the white removed areas are optical obstacles of the telescope pupil, where centroids do not fall in).

## 3.3 Extraction rule: the lexicographic index

With the random variables corresponding to the centroids coordinate of every frame, eventually we could implement the third stage in the logic scheme of a generator, i.e. apply a *rule* to extract random numbers.

The CCD relevant pixels are labelled sequentially with an index $s$, $s \in \{1, \dots, N\}$ and the $n_f$ speckle centroids of the frame $f$ are elaborated (for details on the centroid extraction see Methods, subsection A). By considering then the pixels where a centroid fall in, an ordered sequence $S_f = \{s_1, s_2, \dots, s_{n_f}\}$ with $s_1 < s_2 < \cdots < s_{n_f}$, can be formed. In this way the pixel grid can be regarded as the classical collection of urns - the pixel array - where the turbulence randomly throws in balls - the speckle centroids: a given frame $f$ "freezes" one $S_f$ out of the

$$T_f = \frac{N!}{(N-n_f)!n_f!} \tag{3.7}$$

possible and equally likely sequences of $n_f$ centroids. Among all of them, a given $S_f$ can be univocally identified with its lexicographic index $I(S_f)$

$$I(S_f) = \sum_{k=1}^{n_f} \binom{N - s_k}{n_f - k + 1} \tag{3.8}$$

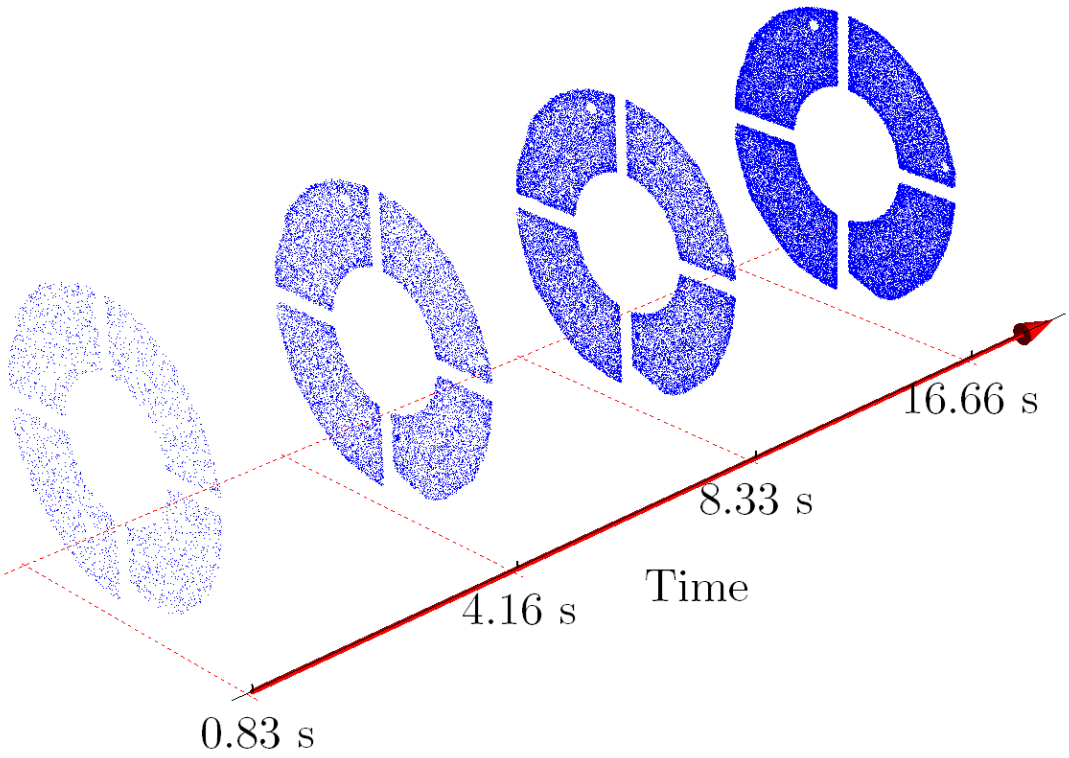


Figure 3.8: As the time flows, the speckle centroids fill homogeneously the sensor active area. Blank areas correspond to optical obstacles in pupil of the telescope, which prevent the light to be detected by the detector.

with $0 \leq I(S_f) \leq T_f - 1$. Basically, (3.8) enumerates all the possible arrangements which *succeed* a given centroids configuration and the TRNG distillates randomness by realizing the correspondence $S_f \iff I(S_f)$. Indeed, as an uniform RNG is supposed to yield numbers *identically and independently distributed* (i.i.d.) in a range $[X, Y]$, as this method generates a random integer in the range $[0, T_f - 1]$. In order to obtain formula (3.8) we need to enumerate the combination of $n_f$ balls contained in $N$ urns. The positions of the ball are identified with the integers $s_1 < s_2 < \cdots < s_{n_f}$. The number of possible combinations is $T_f = \binom{N}{n_f}$.

Let's first calculate the number of combinations that precede the given combination. This can be obtained by summing all the possible combinations in which the first ball falls in the positions $s_1'$ with $s_1' < s_1$, namely $\sum_{m=1}^{s_1-1} \binom{N-m}{n_f-1}$, plus all the combination in which the first ball is in $s_1$ and the second ball is in $s_2'$ with $s_1 < s_2' < s_2$, namely $\sum_{m=s_1+1}^{s_2-1} \binom{N-m-1}{n_f-2}$, plus all the combination in which the first ball is in $s_1$, the second

in $s_2$ and the third ball is in $s_3'$ with $s_2 < s_3' < s_3$ and so on. This number is given by

$$p(S_f) = \sum_{k=0}^{n_f-1} \sum_{m=s_k+1}^{s_{k+1}-1} \binom{N-m}{n_f-k-1} \tag{3.9}$$

where we defined $s_0 = 0$. From $\sum_{k=0}^{n} \binom{k}{j} = \binom{n+1}{j+1}$, it can be shown that $\sum_{m=s_k+1}^{s_{k+1}-1} \binom{N-m}{n_f-k-1} = \binom{N-n_k}{n_f-k} - \binom{N-n_{k+1}+1}{n_f-k}$ so that $p(S_f) = \binom{N}{n_f} - \sum_{k=1}^{n_f} \binom{N-s_k}{n_f-k+1} - 1$. The number of combination that succeed $S_f$ can be easily computed by

$$I(S_f) = \binom{N}{n_f} - 1 - p(S_f) = \sum_{k=1}^{n_f} \binom{N-s_k}{n_f-k+1} \tag{3.10}$$

where $0 \leq I(S_f) < T_f$. The number $T_f - 1$ represents then the upper bound to the uniform distribution of arrangement indexes which can be obtained by all the possible arrangements of $n_f$ centroids: the largest index, that is $I(S_f) = T_f - 1$, is obtained when all the centroids occupy the first urns of the grid.

To be conveniently handled, a binary representation $b_{I_f}$ of the random integers $I(S_f)$ must be given. The simpler choice is to transform the integer $I(S_f)$ in binary base, obtaining a sequence with $L_{T_f} = \lfloor \log_2 T_f \rfloor$ bits. However, only if $T_f \bmod 2^i = 0$ for $i \in \mathfrak{N}$, every frame $f$ would theoretically provide strings $L_{T_f}$ bits long. In general this is not the case and hence, all the frames with $\log_2 I(S_f) \geq L_{T_f}$ should be accordingly discarded to avoid the so-called *modulo bias*. This issue, which clearly limits the rate of generation, can be solved by adopting the encoding function $E : b_{I_f} \to E\left[b_{I_f}\right] \equiv b'_{I_f}$ developed by P. Elias [83]. With this approach, a string longer than $L_{T_f}$ is mapped into a set of shorter sub-strings with equal probability of appearance. To convert the integer $I(S_f)$, uniformly distributed in the interval $[0, T_f - 1]$, into an unbiased sequence of bits, we may first consider the binary expansion of $T_f$

$$T_f = 2^L + \alpha_{L-1} \cdot 2^{L-1} + \cdots + \alpha_0 \cdot 2^0 \tag{3.11}$$

where $L = \lfloor \log_2 T_f \rfloor$ and $\alpha_k = 0, 1$. Random bit strings are associated to $I(S_f)$ according to the following rule: find the greatest $m$ such that

$$I(S_f) < \sum_{k=m}^{L} \alpha_k 2^k \tag{3.12}$$

and extract the first $m$ bits of the binary expansion of $I(S_f)$. By this rule, when $I(S_f) < 2^L$, $L$ bits can be extracted; when $2^L \leq I(S_f) < 2^L + \alpha_{L-1} 2^{L-1}$, $L - 1$ bits can be extracted and so on; when $I(S_f) = T_f - 1$ and $\alpha_0 = 1$ (namely when $m = 0$) no string is assigned. It can be easily checked that this method, illustrated in Figure 3.9, produces unbiased sequences of bits from integers uniformly distributed in the interval $[0, T_f - 1]$.

This approach is optimal: the positions of $n_f$ centroids in $N$ pixels can be seen as a biased sequence of $N$ bits, with $n_f$ ones and $N - n_f$ zeros. The content of randomness

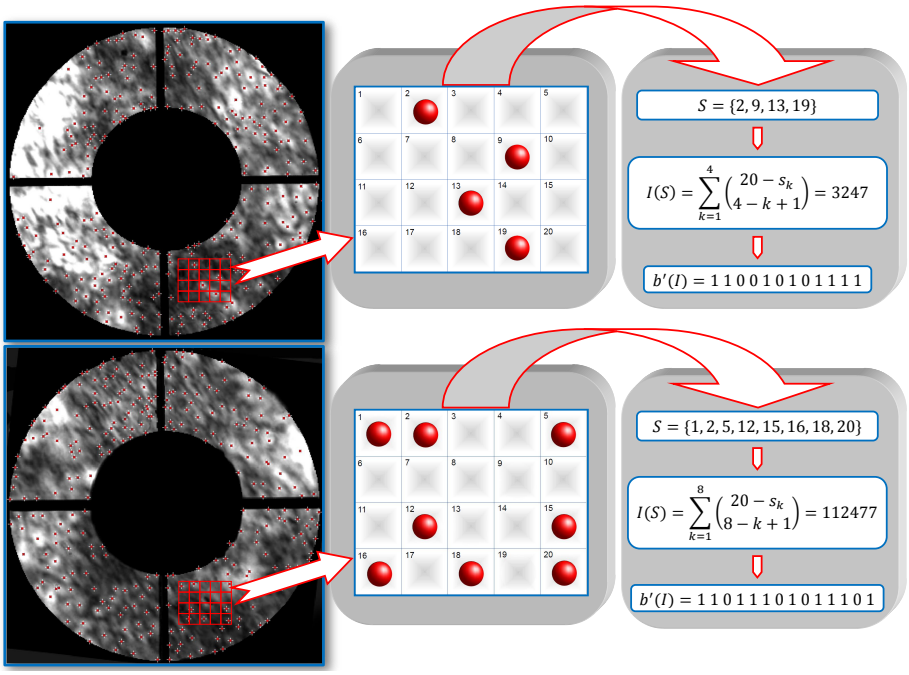


Figure 3.9: We report two sample frames, with the centroids of the brightest speckles evaluated. It is worth to stress that for illustrative purposes the image has been simplified: in the real implementation centroids are evaluated on different intensity levels and every cell corresponds to a pixel. To illustrate the method, let's consider 20 urns (the pixels) and 4 balls (the centroids) as in top figure. The total number of combinations is $T = \binom{20}{4} = 4845$ with $L = \lfloor \log_2 T \rfloor = 12$. The ball positions are defined by the sequence $S \equiv \{s_1, s_2, s_3, s_4\} = \{2, 9, 13, 19\}$ that corresponds to the lexicographic index $I(S) = 3247$. Since $I(S) < 2^L$ it can be expressed with $L = 12$ bits, i.e. the binary expansion of $I(S)$ "110010101111", can be extracted from $S$. A similar procedure is used for the bottom figure with 8 balls in 20 urns giving $I(S) = 112477$. We have $L = 16$ and $I(S) \geq 2^L$: in this case less than 16 bits can be extracted. The method explained in the main text allows to extract the sequence $b'(I) = 11011101011101$.

of this biased sequence is $h_2(q) = -q \log_2 q - (1 - q) \log_2(1 - q)$ with $q = \frac{n_f}{N}$. By the Elias method it is possible to unbias the sequence in an optimal way: it can be shown that the efficiency $\eta = \frac{\langle L_{b'} \rangle}{N}$, the ratio between the average length of $b'_{I_f}$ and $N$, reaches the binary entropy $h_2(q)$ in the limit of large $N$, $\lim_{N \to \infty} \eta = h_2(q)$. In this way it has been possible to preserve the i.i.d. hypothesis for the set $[0, 1]$ maximizing the rate of the extraction.

The combinatorial approach here introduced allows a general approach compared to other techniques used to convert into random numbers the pixel coordinates of a detector. For example, in [76], bi-dimensional random number arrays are obtained by converting in bits the position of those active pixels whose thresholds were adjusted in

order to get the desired bivariate random distribution when illuminated with an uniform speckle pattern (i.e. to get an uniform distribution would be necessary to have half of the pixels over threshold and half below). With respect to the direct conversion approach, our method is more resilient, because by extracting the maximal entropy for a given frame, we do not need to constantly adjust the detector thresholds in function of the speckle pattern to get an uniform distribution of 0s and 1s.

By implementing the technique of the previous Section with different configurations of masks and centroids, we were able to reach a maximum average rate of 17 $kbit/frame$ (with a grid of 891000 urns and an average of 1600 centroids per frame). Theoretically, having used a frame rate of 25 $frame/s$ this method could provide a rate of 420 $kbit/s$ using a similar camera and it could further increase by using a larger sensor. It is worth to stress that, for the present proof of principle, the distillation of random bits has been done off-line so one should consider the possibility of providing the image grabbing setup with a dedicated hardware, e.g. FPGA, to extract the lexicographic index and apply the Elias coding. Another point worth remarking is that the extraction speed is in any case limited by the acquisition rate that has not to overcome the physical time scale of the phenomenon, cfr. Section 3.2 in order to not introduce correlation between the images.

## 3.4 Analysis of the extracted bits

The analysis that has been done so far had a double purpose: on one hand we had the necessity to study whether the physical process was suitable to generate randomness; on the other hand, verified said suitability, it was necessary to find a method to handle the random variables without *spoiling* the randomness, e.g. to fix opportunely the frame rate or to not introduce digital bias. In the field of physical randomness generation, these are the two methodological stages which attains to the *a priori* characterization the source of entropy and the sampling of the source. More precisely, they define the so called statistical model of the generator, i.e. the set of experimental and technical conditions which should guarantee the generation of identically and independently distributed bits.

The last stage of the analysis consists then in checking whether the generated bits are random or not. This is a sort of *a posteriori* characterization which is important to detect deviations from the condition of i.i.d. bits. Typically, if the experimental conditions required by the statistical model are matched during the generation, deviations can be caused by the fact that the statistical model itself is wrong or incomplete, or they are caused by hardware defects or software errors. In particular the latter cause is common for TRNG exploiting e.g. electronic noise and the signal must be processed by several devices.

Analysis is performed by applying the theory of hypothesis testing. We will briefly introduce here, the rationale behind statistical test of randomness. Fundamentally, a test studies a given property of a bit string and it evaluates if this property is compatible with the hypothesis that the analyzed string is random. More precisely, by applying a test on a set of random variable, e.g. bits, another random variable $\mathcal{T}$ with outcome $\tau$, the so-called *test statistic* is obtained.

According to a given test, $\mathcal{T}$ follows a given probability distribution. For example, if one wants to check whether the 0s and 1s are identically distributed in a $n$ bit long string, i.e. $P(b_i = 0) = P(b_i = 1)$ with $i = 1, \ldots, n$, a *frequency* test can be applied: let's define $\tau_{freq} = \frac{(n_0 - n_1)^2}{n}$, then $\mathcal{T}_{freq}$ is distributed according the $\chi^2$ distribution with one degree of freedom. Consequently, the outcome of a test of randomness is not a yes/no response but a probability value, the so called *p-value* $\mathcal{P}$. Namely, the $\mathcal{P}$ is the probability to obtain a test statistic $\tau'$ equal or worse, i.e. more extreme, with respect to the one observed $\tau$, given the i.i.d. hypothesis holding true.

More formally, if we consider the frequency test $\mathcal{P}_{freq} = P(\mathcal{T}_{freq} = \tau'_{freq} \geq \tau_{freq})$: for example $\tau_{freq} = 3.481$ then one obtains $\mathcal{P}_{freq} = P(\tau'_{freq} \geq 3.841) = 0.05$. If the i.i.d holds true, then one is expected to have a $\tau_{freq} < 3.841$ for the 95% of the tested strings. The lower the p-value, the lower the probability that an ideal RNG yields the same or a worse result: so for a given string, the i.i.d. hypothesis is rejected if it is very unlikely to get the same result if the bits are i.i.d.. For what concerns RNG tests, unlike results are typically considered those ones yielding $\mathcal{P} < 0.01$ or $\mathcal{P} < 0.001$, i.e. for $\mathcal{P} \geq 0.01$ and $\mathcal{P} \geq 0.001$ the i.i.d. hypothesis is not rejected with a confidence level of 99% and 99.9% respectively. However because there are probabilities of $\alpha = 0.01$ and $\alpha = 0.001$ respectively of an erroneous rejection of the hypothesis (the so called error of type 1)[1] for a correct application of a test one should apply it on an enough large set of string, e.g. for a significance level $\alpha = 0.01$ one is expected to obtain a test statistic with $\mathcal{P} < 0.01$ roughly once every 100 strings tested. In the following analysis, for a given level of confidence, we will say that a test is *passed* if the i.i.d. hypothesis is not rejected, otherwise we will say that the test is not passed.

It is worth specifying that do not exist tests for all the possible deviation from the condition of i.i.d.: for example a 2000 bit string having the first 1000 bits equals to 0s and the remaining bits equal to 1s, would pass a frequency test but it would not pass e.g. a 4 bit serial test, which check the uniform distribution of all the words with four bits.

The common procedure to test a generator, it is then to carry out several tests in order to check different features. We applied this method to the numbers generated by joining strings obtained from the frames. The test strategy was then to use software suites of statistical tests which cover many possible issues random numbers can have. However before employing the large suites, in order to have a first feedback on the quality of the numbers we run on the strings some tests which are generally failed by TRNG, as consequence of hardware defects or wrong coding. Indeed for a TRNG it is more likely to fail those tests regarding low-level bit problem as frequency tests or the autocorrelation test, rather than those tests regarding the non uniformity in multidimensional spaces, typical issues of PRNGs. The theory of these tests is reviewed in Appendix C. In the following they will be briefly introduced in order to illustrate the preliminary results.

As first result of the statistical analysis, we present the outcomes of two tests, the *frequency* and the *autocorrelation* test respectively [84]. While, the frequency test checks

[1] it is worth notice that when a the limits for the p-values are very low, there are chances to accept the hypothesis also for strings that are not i.i.d.

the uniformity of the single bit words, the autocorrelation test is of particular importance in order to verify whether the bits features some dependencies from the neighboring bits up to 64 positions.

The results of both the tests are reported in the first two rows of Table 3.1. From the frames we extracted and analysed 1483 strings 20 000 bits long (this string size has been selected for two main reasons: the first one in order to have a string sample large enough to comply the significance level both $\alpha = 0.01$ (at least 100 elements) and $\alpha = 0.001$ (at least 1 000). The second reason is because this string size is commonly used in standard tests suits such as FIPS-140-1 and AIS31, cfr. **??**, such that by passing or failing the above tests helps to understand the odds to pass also deeper statistical tests). The total number of test statistics obtained is reported in the second column of Table 3.1, while in the third and in the fourth columns there is the number of tests statistics which not passed with confidence level of 99% and 99.9% respectively. For a given level of confidence the value between parenthesis is the critical tolerable number of failure: as one can see the number of strings which not passed the tests are inside the critical limits, confirming the uniformity and the absence of correlations of the numbers.

The second type of tests we applied are the so-called *serial tests*: the feature checked is the uniform distribution of multi-bits words, i.e. 2-bits, 2-bits overlapped and three 3-bits words. The aim of these tests is to verify whether the generator is distributing with the same probability not only the single bits but also the different patterns e.g. 00, 000, 01, etc.. Practically the strings are the divided into groups of two or three bits and the relative frequencies are evaluated. In particular the 2-bits overlapped test check also the uniform distribution of the possible choices: e.g. given the pair $b_i b_{i+1}01$, is evaluated the probability to get $b_{i+1}b_{i+2} = 10$ or $b_{i+1}b_{i+2} = 11$. The results are reported in the last three rows of Table 3.1 and also in this case the number of failures is inside the limits.

| | **Test Statistics** | $\mathcal{P} < 0.01$ | $\mathcal{P} < 0.001$ |
|---|---|---|---|
| **Autocorrelation Test** | 94912 | 921 (1042) | 80 (124) |
| **Frequency test** | 1483 | 20 (26) | 1 (5) |
| **Serial 2 bits** | 1483 | 18 (26) | 1 (5) |
| **Serial 2 bits over.** | 1483 | 17 (26) | 1 (5) |
| **Serial 3 bits** | 1483 | 17 (26) | 1 (5) |

Table 3.1: In table, for every test (first column) the overall number of tests statistics (second column) obtained from videos recorded in different conditions are reported. The number of failures are listed in the third and fourth columns. These numbers can be compared with the theoretical number of failures (inside the parentheses) which are expected when the i.i.d. hypothesis hold true. As it can be seen for all the tests the failures are inside the limits both for the 99% and 99.9% confidence levels.

It is interesting to consider the results of the 8-bits serial test, i.e. the test which evaluates the uniform distribution of bytes. A visual evidence that an overall uniformity is preserved during the whole acquisition time, it is given in Figure 3.10 where the distribution of $1.4 \cdot 10^6$ bytes obtained from a 671 frames video sample is plotted. If

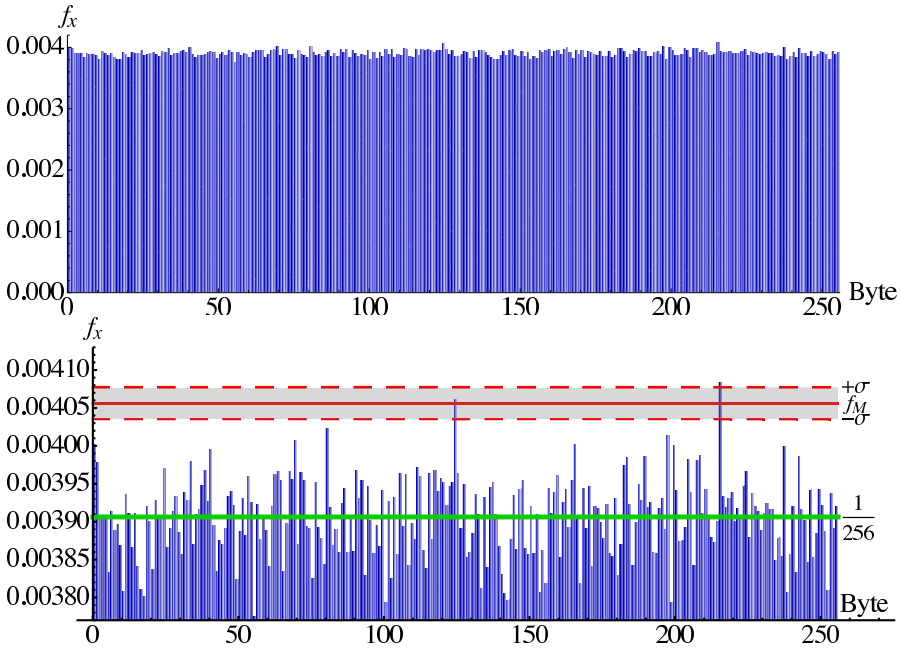


Figure 3.10: (**Left**) The histogram represents the relative frequencies of byte occurrences, obtained from $1.4 \cdot 10^6$ bytes corresponding to 671 fraes. The distribution is uniform, as demonstrated by the chi-square test on the frequency giving a $\mathcal{P}$-val $= 0.77$. (**Right**) Zoom of the histogram: the frequencies randomly distribute at the sides of the expected mean value (green line). Furthermore, the maximal byte frequency (corresponding to the byte 216) it is fully compatible with its expected value $f_M$ (red solid line) and the $\pm\sigma$ limits (red dashed lines).

the bytes were used for cryptographic purposes, it is meaningful to consider the binary *min-entropy* $h_{min} = \max_i[-\log_2(p_i)]$ where $p_i$ is the measured appearance probability of the byte $i \in [0, 255]$. A value of $h'_{min} = 7.936$ bits per byte has been measured and this is compatible with the expected min-entropy for a sample of that size, that is $H_{min} = 7.946 \pm 0.007$. This experimental value is thus in agreement with the expected value from the theoretical prediction on uniform distribution, assessing an eavesdropper has no advantage with respect to random guessing (see Appendix A for a derivation of the expected min-entropy $H_{min}$).

The numbers were tested to cover other possible issue with three state-of-the-art batteries of tests which are presented in Appendix B. The suites were selected because the tests that implement are a particularly suited to detect defective in physical TRNG. The results on the bit strings are presented in Table C.1. The parameters of the tests were tailored for the bit length of the strings in order to make the tests effective. Problems were not detected being all the results outside the critical limits of $\mathcal{P}$-val $\leq 10^{-3}$ or $\mathcal{P}$-val $\geq 0.990$. From this analysis, where the more stringent and effective tests were applied and passed, the i.i.d. hypothesis resulted confirmed and strengthened.

## 3.5 Conclusions

As pointed out above, we are here addressing the two issues of introducing a method to extract good random numbers from random images and of generating these images from light propagating through the atmosphere. In particular, we exploited the propagation of the light over 143km of turbulent atmosphere, giving rise to random speckle patterns at the receiver. The advantages of the method above presented in comparison with other TRNG resides in exploiting a good entropy source and in an efficient method to convert this entropy in a string of random bits. Indeed, when the conditions for strong optical turbulence are met, the scintillation images are resulting from a process that cannot be predicted, providing to a significant amount of entropy that may be extracted. In particular, the analytical models that are presently known to describe the dynamic of a turbulent fluid are not able to provide the evolution of the instantaneous intensity distribution. Moreover, if such models will be conceived, it is very presumable that they would require an extreme computational power to model the outcome of the propagation and still, according to the principle of the underlying nonlinear dynamics, maintaining the peculiar sensitivity on the initial conditions.

Other types of generators rely on small scale chaotic processes, such as sampling of laser intensity noise, but they must be carefully tuned in order to avoid the physical system to end in periodic trajectories and predictable outputs during the operation [88]. In particular, we can compare our method with the one proposed in [89] and realized in [90] where random numbers are obtained by sampling a detector illuminated with speckles produced by passing a laser beam between two rotating diffusers: such an approach however, as stressed by the authors themselves, could lead to periodicity due to the possibility that the same pattern repeats itself. Our TRNG is more resilient because we can safely exclude any periodicity of the speckle pattern.

A further advantage in exploiting optical beam propagation in turbulence is the fact that the physical process and the hardware are less prone to be influenced and controlled by an attacker, as is the case of generators which operate at the noise level limit. For example, generators based on measuring low amplitude voltage fluctuations in a resistor caused by the electronic thermal noise, can be easily influenced by modifying the environmental temperature [91].

We now give two examples of application of our method. Our method could be directly applied in situations involving similar optical links, such as long range quantum communication experiments that require the generation of random numbers [19, 92]. The second case is to apply the method by reducing the scale of the generator. The problem is then to individuate physical processes which can give rise to a speckle pattern randomly evolving in time. Different techniques, such as the dynamic light scattering, exploit speckle pattern analysis to infer a characterization of the diffusers, typically ranging from turbid media to organic tissues [93, 94]. Such diffusers could be valid candidates for the purpose of continuous random number generation. By illuminating a colloidal suspension with a coherent light, random numbers could be extracted from the randomly evolving speckle pattern caused by the Brownian motions of the particles [95].

Concerning our extraction technique, the algorithm here devised can be applied to any image from which it is possible to distill a spatial distribution of points. For example the lexicographic algorithm could be easily embedded in device which have a camera as mobile phones [96] (cleary it would be necessary to investigate the possibility of finding a suitable kind of images to be taken with the phone camera from which i.i.d. random variables can be obtained). As last point we want to stress that the data obtained passed the most sensitive tests for TRNGs. The fact that here the randomness is generated without the need of any post-processing technique demonstrates the effectiveness of the present method.

# Chapter 4

# State of the art about true quantum randomness

In the following a brief introduction to the field of quantum random number generator (QRNG) will be given. The purpose of this introduction is to present the state of the art in order to understand the contribute brought by this work.

Quantum Mechanics has been always regarded as the ultimate source of true randomness because of its intrinsic *probabilistic nature*. A random number generator based on Classic Physics indeed could be intended as a *deterministic generator* where the algorithm corresponds to the equations of motion and the seed corresponds to the initial conditions of the degrees of freedom. Fundamentally, when Newtonian Physics is involved, variables associated to the physical processes appear "random" because of the ignorance about the system. This point can be illustrated by citing the words of P.S. Laplace while describing in 1814 what would be later called *Laplace's Demon*:

> "We may regard the present state of the universe as the effect of its past and the cause of its future. An intellect which at a certain moment would know all the forces that set nature in motion, and all positions of all items of which nature is composed, if this intellect were also vast enough to submit these data to analysis, it would embrace in a single formula the movements of the greatest bodies of the universe and those of the tiniest atom; for such an intellect nothing would be uncertain and the future just like the past would be present before its eyes."

(op. cit. P.S. Laplace, A Philosophical Essay on Probabilities, [97]).

The fact that quantum physical processes could have been a resource for the generation of random numbers has been clear since the 70s with the first concepts and prototypes typically based on radioactive processes[98] [99] [100]. This kind of generator never found a widespread use considered the difficulties in handling radioactive elements. With the evolution of microelectronics, the interest shifted more towards noise of chaotic origin, being easily embeddable in digital devices.

## 4.1 Optical QRNGs

A true academic interest for QRNG started with the advent of the experimental QKD implementations in the mid 1990s, when increased the need of true sources of randomness for the choice of the polarization bases. The first theoretical work dates back to 1994, where Rarity et al. [101] presented possibel designs of optical QRNGs. However only in the year 2000, arrived the first experimental prototypes with the work of Jennewein et al. [102] and Stefanov et al. [103], (see below). It was the beginning of what can be defined the era of the optical QRNG, which we are going to briefly review.

In the last fifteen years quantum optical randomness was exploited in several paradigms. Two main categories can be individuated both chronologically and physically. The first prototypes to be introduced were based on *discrete variables* (DV-QRNG), i.e. they process pulses corresponding to single photon detection. To the second category belong *continuous variables* generators (CV-QRNG): introduced towards the end of 2000s, they process fluctuating analog signals obtained by employing photodiodes rather then single photon detector. This is a relevant point because photodiodes with respect to single photon detectors which are affected by dead time, feature larger bandwidth which enables to reach generation rate of the order of Gbit/s compared to the Mbit/s of the discrete variable QRNG.

### 4.1.1 Discrete Variables QRNG

This class of generator can be further divided into two sub-categories: the *welcher-weg* (which way) generators and the *time-interval* generators.

Welcher-Weg QRNG. To this category belong those generators which exploit two characteristic features of the quantum world: the indivisibility of the single quanta and the outcome unpredictability of a pure state projected onto a non orthogonal subspace with respect of the preparation one. The first two QRNGs already mentioned, [103] and [102] were based on a scheme of [101]: the value 0 or 1 is associated to a bit according to *which way* a photon takes after interacting with a beam splitter. At the two outputs of the beam splitter are indeed placed single photon detectors whose clicks are electronically processed to generate random strings.

The paradigm was implemented both with unpolarized photons in front of a 50:50 beam-splitter, and with diagonal polarized photons and a polarizing beam splitter, separating horizontal and vertical polarizations. In these two examples, photons were generated by attenuated light emitting diodes. In 2004 with the work of Hai-Qiang et al. [104] single photons were generated by employing a parametric down conversion source, with a photon of the entangled pair measured by a beamsplitter and the other heralding the emission. Another generator based the photon polarization is the one presented by Fiorentino et al. [105] which will be analyzed in the next Chapter.

Time-Interval QRNG: to this class of generator belong those devices which extract random numbers on the time of arrival of photons. With respect to the previous class, they usually employ just a single photon counter which simplifies the setup avoiding the problem of unbalanced beam splitter or unbalanced detector with different efficiencies.

An example is the one presented by Stipcevic et al. [106] where a Light Emitting Diode (LED) sends photons directly on a single photon detector, then the time between consecutive detections is measured. The way to do it consists in counting the number of periodic pulses of an high speed quartz oscillator whose frequency is higher than the rate of photon detections. In correspondence of every event the clock is stopped and then restarted: a comparison rule is applied on adjacent intervals, so if the first interval contains a number of clock pulses higher than the next one, a 0 is extracted, otherwise a 1. In this way every three detections, a bit can be produced, with a rate of 1 Mbit/s. A faster generator, 50 Mbit/s, is the one introduced in 2010 by Furst et al. [107]: the source of randomness is again a LED which shines a single photon detector. The LED is strongly attenuated in order to obtain Poissonian photon detection distribution. The generator then continuously counts how many photons are detected in a fixed time interval: if the number of detection is even, a bit 0 is emitted otherwise, for an odd number, the output is a bit 1. Remarkably the generator does not feature any post-processing stage. An even faster generator is the one of Wahl et al. [108]. The working principle of this generator is based also on the time statistical properties of photon detections. In particular, the Poissonian probability distribution of the photon detection process is characterized by an exponential distribution of the time intervals between the detection events. Random bits are then obtained by converting in binary digits the intervals registered between consecutive events. According the data sheet this QRNG has a nominal rate of 150 Mbit/s. A post-processing stage is necessary in order to remove bias inevitably introduced by the dead time of the the detectors.

### 4.1.2 Continuous Variables QRNG

Also this class of generators can be sub-divided into two sub-categories: the *quadrature* generators and the *optical noise* generators. These generators are based on the sampling of field gaussian state quadratures detected by with homodyne scheme: in 2010 was realized the first QRNG based on this paradigm by Gabriel et al. [109]. The working principle of these generators will be presented in Chapter 6. It is worth to stress that the name *continuous variable QRNG* usually refers just to this kind of generator.

Optical Noise Generators: a wide set of generators belongs to this class which where developed in the last recent years. To this class belong also the record for the fastest generation rates (theoretical and real)[1]. We included these generator in the continuous variable class because, as for the quadrature generators, random numbers are generated by sampling a current signal produced, in this case, by one or more photodiodes illuminated by an intensity varying laser signal. We are going to introduce some of the most relevant examples, starting with the generators which employ the laser phase noise. In 2010 Guo et al. [110] introduced a generator to generate the numbers by sampling the intensity fluctuations of a VCSEL laser beam which passes through a kind of Mach-Zender interferometer (MZI). In this configuration called, self-delayed homodine,

[1]Most of the time the analog to digital converter used to sample the signal have a limited amount of memory, so the number must be extracted offline from a sampled and stored signal. The theoretical rate is then the maximal rate achievable if it would be possible to run the generator continuously.

the delay line of the interferometer is set in order to make the laser to interfere with itself as consequence field phase fluctuations of quantum origin due to the spontaneous emission of the photons. This generator was the first of this kind featured a generation rate of 20 Mbit/s. Contemporarily, also Qi et al. [111] proposed a generator based on an interferometric scheme, which was later improved in the 2012 by the same group [112], with a phase noise from a distributed feedback laser (DFB). This generator has a rate of 6 Gbit/s and notably, it features a sound analysis of the physical process. Besides this generator feature a dedicated work by Ma et al. [113] featuring the correct post-processing of the numbers. Another pair of works about the same generator, worth to mention are by Jofre et al. [114] of 2011 and Abellan et al. [115] of 2014, where phase fluctuations were obtained by interfering pulses with random phases from a high rate a DFB laser. This QRNG features a remarkable rate of 43 Gb/s.

It is worth to stress that contemporarily to the presented prototypes, many setups were proposed based on laser relaxation oscillations, e.g. [88][116][66][117]. However these generators are commonly regarded as *classical* because the dynamic of the relaxations is chaotic, cfr. [115].

## 4.2 Device Independent Randomness protocols

The important point worth to stress is that typically in the QRNG of the previous Section, randomness is handled classically, e.g. in [118]. Indeed, the raw random bits generated after the direct measurement of a quantum process, more or less characterized, are analyzed and post-processed as if the bits were extracted from a classical random number generator. More specifically, the approach is to apply statistical tests of randomness and then, in case of failure, treat the bits with classical post-processing algorithms until the tests were passed. Such post-processing techniques are aimed to remove bit bias and correlations generally caused by a measuring hardware not properly calibrated for the process (e.g. dead time of the detectors, too high sampling rate etc.). In some cases, also for commercial quantum random number generators the employed technique was still the one introduced by John Von Neumann at the dawn of Monte Carlo methods. Besides that, it is worth specifying that *does not exist* any *a posteriori* test of randomness which can establish the independent and identical distribution of the bits. Indeed, for any test which assesses the uniformity of a given statistical feature, another test can be conceived which can discover the lack of uniformity for another feature.

The drawback of this paradigm lies in the fact that if the purity of the state cannot be enforced or if the post-processing techniques are not properly chosen, the quantumness and its intrinsic unpredictability are lost and a QRNG could become comparable to a classical random number generator, e.g. a dice or a coin.

A complete shift in the paradigm arrived with the work of R. Colbeck [119] which introduced the basis for the development of *devices independent* randomness. In this context, Quantum Theory itself is *questioned*, in the sense that one accounts for the possibility of Quantum Mechanics to be a deterministic theory, numbers are certified to be random only if one is able to rule out the Local Hidden Variables theories.

In the early years of Quantum Mechanics, doubts were cast about its probabilistic description of the Nature. More specifically, it was hypothesized that there could've been some unknown parameter which, once discovered, could've explained the *apparently* intrinsic randomness. Otherwise stated, Quantum Mechanics is a deterministic theory which is explained in terms of probabilities only because there is lack of knowledge about some *hidden* parameter. Theories which could provide a deterministic interpretation of Quantum Mechanics are called *local hidden variables* theories. The existence of such theories was questioned by John Bell who, in 1964, provided a tool to rule out hidden variables from Quantum Mechanics. Indeed Bell proved that given a local causal structure of the space time, if hidden variables theories exist, then the correlations between events separated by space-like intervals should satisfy a set of inequalities. However, when two parties of a bipartite quantum system (e.g. two photons or two electrons) in an entangled state of some degree of freedom (e.g. polarization or spin) are suitably measured, the outcomes of such measurements feature non-local correlations which violate these inequalities. The violation then can be experimentally observed in presence of quantum non-locality but it cannot be reproduced by hidden variable theories.

The theoretical framework comprehends a pair of black boxes that can receive two inputs and emits two outputs: according within the DI framework, no assumption is made on the internal working of the boxes and therefore one checks whether correlations between input/output variable distributions can be explained in terms of *non-locality*.

In 2010 with a seminal experiment of Pironio et al. [120], numbers were certified to be true after being generated in a setup where Bell inequality in the CHSH form was violated by using trapped ions. In this experiment roughly 6000 raw random bits were generated in a month. With a protocol based on the resolution of semi-definite programming, which relates the amount of CHSH violation to the probability of guessing correctly the output of the generator, the authors were able to distil 42 bits *true*, i.e. non-deterministic, random bits.

This experiment paved the way to a series of theoretical works which were produced in the following years. Indeed in this first experiment, a protocol of *randomness expansion* was realized: to violate properly the Bell inequality, the inputs of the black boxes must be select with a private *seed* of perfect random bits[1]. The generation rate is positive because the seed is *expanded* quadratically and part of the new bits can be used to determine the next choices for the inputs. However the protocol has the drawback that in order to achieve Bell certified expansion, initial perfect randomness is needed[2].

The turning point arrived in 2012 with the work of R. Colbeck and R. Renner [121] who introduced a protocol for *randomness amplification*. The authors demonstrated that by using chained Bell inequalities, true randomness can be obtained also if the seed is not perfect in a given measure. Although amplification has not yet been proved experimentally, this work represented a milestone having deep implications for what

[1] I the experiment was assumed also that the two black boxes were not interacting (although they were not separated by a space-like interval)

[2] In the experiment, the seed was obtained by mixing together physical and pseudo-random numbers, both deterministic sources

concerns the problem of the *free choice*: for the first time a method was available the generation of random variables that cannot be the result of any pre-determined scheme. More specifically, numbers obtained applying this protocol would not be random only if the *whole Universe* could be explained in terms of a super-deterministic theory.

In 2013 the amplification protocol was extended by Gallego et al. [122] in order to make it possible to amplify any seed with an arbitrarily small, but not null, content of randomness.

The argument of randomness expansion and amplification in the last two years gave rise to many other works of the main theoretical groups not only of Quantum Information Theory but also of Computer Science. However, the main issue with these protocols lies in the fact that the experimental conditions and setups are extremely demanding. For example, randomness amplification requires several black-boxes enforcing loophole free Bell violations. But at present time none has been yet be able to violate Bell inequalities with all the loophole closed. It is worth to mention that in 2013, the expansion protocol was implemented again with super-efficient detector which made it possible to improve by several orders of magnitude the generation rate [123].

## 4.3 New protocols to certify only quantum randomness

The benefit caused by these works, was that they brought attention to the problem of randomness characterization under a quantum and post-quantum perspective, and the possible degrees of ability an adversarial system can have in guessing correctly the generator outcomes. In the last year, there has been a growing interest in finding methods to certify randomness in a framework where Quantum Mechanics is assumed to hold. Therefore no-locality experiments are not necessary and QRNG setup can be greatly simplified. However, conversely to the first QRNGs, these protocols shield the generation not only from classical noise but also from quantum side information.

In these new frameworks, true quantum randomness can be distilled if the QRNG user is able to carefully quantify the percentage of bits which can be guessed by an eavesdropper carrying out the best guessing strategy based on quantum side information, i.e. the eavesdropper holds a quantum system correlated with the QRNG.

In the next Chapters we are going to present the protocols and the experimental realization of QRNG where we exploited a quantum informational tool of recent discovery, the entropic uncertainty principle in presence of quantum memories, to estimate the amount of true quantum random bits extractable from a quantum process.

# Chapter 5

# Secure quantum random bits from the uncertainty principle

As explained in the previous Chapter, the typical issue with generators employing quantum physical processes as source of randomness is that the question whether the numbers are truly quantum unpredictable or not, is poorly addressed. In particular one has that if the system is not prepared in a pure state or it has undergone a process of decoherence, it could be correlated with some other system, i.e. there could be some side information available for the eavesdropping of the generator. More generally, if the state of the system is mixed, one would get only unpredictable randomness in the quantum sense, in the measure that system is pure. The remaining fraction of randomness can be regarded as *classical*. In this Chapter then we will introduce a protocol of randomness generation which distills only bits of quantum origin and secure against any classical or quantum side information, and we will present also the results of an experiment where we tested our protocol. In Section 5.1 the definition of true randomness, inherited by the protocols of randomness amplification, will be introduced. Besides, we will show that the correct randomness quantifier in presence of quantum side information is the conditional min-entropy. In Section 5.2 the Quantum Informational tool that we used for the estimation of conditional min-entropy, the entropic uncertainty principle, will be presented. Examples of the application of the principle for randomness generation will be given in in Section 5.3. The experiment we performed to test the validity of the new method will be presented in Section 5.4 with the respective results. The final conclusions will be given in Section 5.5.

## 5.1 Introduction

In a mathematical context, random numbers are associated to a variable $X$ which is independently and identically distributed. The requirement that $X$ has to feature an identical distribution catches the idea the outcomes $x$ must have the same probability of appearance. The requirement of independence is instead related to the idea of unpredictability of a given $x$.

## 5. SECURE QUANTUM RANDOM BITS FROM THE UNCERTAINTY PRINCIPLE

Out of the works abut device independent randomness, a whole set of useful tools can be exploited in order to define a formal consistent framework where to present our results. Device independent protocols relate the certification of randomness with the violation of Bell inequalities. A fundamental prerequisite is to assume the validity of the *no-signalling* principle. Basically the no-signalling principle states that information can not be transferred instantaneously and then this requirement set a local causal structure for the evolution of the system one is considering. So, if non-local correlations are (truly) observed but signalling is assumed, this implies a deterministic structure of reality. This is the case of the Bohm theory where non-local correlations can be explained within a full deterministic theory which does not admit randomness.

So, in this work

- we assume a local causal structure arising from relativistic space-time or even more generally a causal structure where information cannot travel with an infinite speed;
- because non-local correlations are not involved, we assume the results of quantum events not to be deterministically explained in terms of a Local Hidden Variable theory.

The first requisite is necessary in order to give a definition of *true randomness*, the second requisite is functional to the first one because no-signalling without non-locality does not rule out LHV theories.

True Randomness. Given a causal space-time structure, the concept of true randomness is linked to the one of causality by considering that a random variable $X$ is generated in a spatio-temporal frame of reference such that it is possible to associate to $X$ a space coordinate to its generation place and a time coordinate to its generation instant. In this framework, a variable $X$ is perfectly true random if it is *uniformly distributed conditioned on any other variable which does not belong to the future light-cone of* $X$. In other words, one requires the variable $X$ to be uncorrelated with any other variable $E$ which does not belong to the future of $X$. This can be formally expressed by introducing the trace distance between two probability distribution $P_Y$ and $Q_Y$ of a random variable $Y$ is defined as

$$D(P_Y, Q_Y) = \frac{1}{2}\sum_y |P_Y(y) - Q_Y(y)| = \frac{1}{2}||P_Y - Q_Y||_1 \tag{5.1}$$

two probability distribution for $Y$ are then indistinguishable if $D(P_Y, Q_Y) = 0$. By considering the set $\mathfrak{E}$ of the random variables inside the same causal structure of $X$ but outside its future light cone, and $P_{\bar{X}}(x) = \frac{1}{|X|}$ the uniform distribution on $X$, the requirement for perfect randomness can be restated as

$$D(P_{X|\mathfrak{E}=E}, P_{\bar{X}}) = 0\,. \tag{5.2}$$

Practically the probability distribution of $X$ conditioned on some variable $E$ must be indistinguishable from $P_{\bar{X}}$: this is the case when the $X$ and $E$ are independent such that

the joint distribution $P_{X\mathfrak{E}=E}$ can be expressed just as product of the side distributions, i.e.

$$D(P_{X|\mathfrak{E}=E}, P_{\bar{X}}) = \frac{1}{2}||P_{X\mathfrak{E}=E} - P_{\mathfrak{E}=E} \times P_X||_1 = 0\,. \tag{5.3}$$

If the requirement of perfect true randomness is relaxed, one can introduce the concept of $\epsilon$-true randomness that is $P_{X|\mathfrak{E}=E}$ and $P_{\bar{X}}$ are indistinguishable to a small factor $\epsilon$

$$D(P_{X|\mathfrak{E}=E}, P_{\bar{X}}) = \frac{1}{2}||P_{X\mathfrak{E}=E} - P_{\mathfrak{E}=E} \times P_X||_1 = \epsilon\,. \tag{5.4}$$

This last case is of relevance because usually there is just the condition to obtain an $\epsilon-$true random variable from a generator and then one aims to reduce the distance, i.e. to reduce $\epsilon$ to $\epsilon'$ with $\epsilon' < \epsilon$.

Quantum Random Number Generator Assumed the absence of LHV theories, a generator of true random numbers can be realized in the following way: given a $d$-level quantum system $A$ prepared in a *pure* state $\rho_A$, the random variable $Z$ is obtained by measuring the state $\rho_A$ with a $d$ outcome measurement $\mathbb{Z}$: each outcome $z$ is obtained with a given probability $P_Z(z)$, where $P_Z(z) = \mathrm{Tr}[\mathbb{Z}\rho_A]$ is given by the Born rule. A classical example is a qubit, a $d = 2$ system, prepared in the state $\rho_A = |+\rangle\langle+|$ and measured with $\sigma_Z$, then one has that $P_Z(0) = P_Z(1) = \frac{1}{2}$. To the outcome of $Z$ then can be associated a classical binary variable, a bit. The extractable randomness from the process of measuring a given quantum system can be quantified in terms of *entropy*. In particular, a relevant quantity is the *minimal* amount of true random bits that can be extracted per measurement, which correspond to the *classical min-entropy*

$$H_\infty(Z) = -\max_z[\log_2 P_Z(z)] \tag{5.5}$$

and practically it quantifies the minimal degree of uncertainty that one can have about the outcome of a measurement. For the previous example, when $H_\infty(Z)$ is evaluated on the classical post-measurement state $\rho_Z \equiv \sum_z P_Z(z)|z\rangle\langle z|$ (where $z$ has been encoded in an orthonormal basis $\{|z\rangle\}$), one has $H_\infty(Z) = 1$ bit of uncertainty which corresponds to the maximal amount possible for a binary quantum system. Under an operational point of view, it turns out to be useful to introduce also the *guessing probability* defined as

$$p_{guess}(Z) = 2^{-H_\infty(Z)} \tag{5.6}$$

which restates the idea of the uncertainty in terms of the probability to correctly guess the outcome of a quantum state measurement. Again for the previous example one has that the probability to guess $Z$ is given by $p_{guess}(Z) = \frac{1}{2}$. The guessing probability gives also a reason of the "max" in the min-entropy definition: an eavesdropper willing to predict the outcome does need to devise any elaborate plan because to bet on the most probable event the best guessing strategy.

In a realistic scenario however $H_\infty(Z)$ does not represent an appropriate quantity to measure the content of true random bits can be extracted from a quantum process. As first example we think about a scenario where an user Alice uses a QRNG of the kind

presented before, to generate cryptographic keys and an eavesdropper Eve aims to knows them. In order to get the keys, Eve exploits some classical side information $W$. Eve could have been correlated with the QRNG in the past: she stole it from Alice, she analyzed it and discovered that the photon source emits a fixed amount of qubits polarized in $\{|H\rangle, |V\rangle\}$ basis instead of $\{|+\rangle, |-\rangle\}$. Eve could be correlated in the present: she stole it from Alice and she embedded on it a device to change remotely in the $\{|H\rangle, |V\rangle\}$ the photon polarization. In this last case Eve balances perfectly the fraction of vertical and horizontal polarized photons, i.e. she provides a state $\rho_A = \frac{1}{2}(|H\rangle\langle H| + |V\rangle\langle V|)$. Alice is unaware of the presence of Eve, so when measures the min-classical entropy she gets $H_\infty(Z) = 1$ and she is induced to believe that her QRNG is fully unpredictable. However, this result for Alice is completely misleading because thanks to the side information $W$, for Eve $p_{guess} = 1$. A proper measure of entropy must take in account for the side information and indeed this is the case of the min entropy of $Z$ conditioned on $W$

$$H_\infty(Z|W) = -\log_2 \left( \sum_w P_W(w) \max_z [P_{Z|W=w}(z|w)] \right) . \tag{5.7}$$

In the example, when Eve prepares the state in the $H$ ($V$) polarization, Alice measures it with certainty: $P_{Z|W=w}(0|0) = 1$ ($P_{Z|W=w}(1|1) = 1$); moreover Eve prepares the two state with the same probability $P_W(w) = \frac{1}{2}$: one easily derives that indeed $H_\infty(Z|W) = 0$.

In the just introduced scenario we were dealing with $W$ classical side information. However it results convenient to consider the more general case of quantum side information. One can consider the case where Eve provides to Alice a QRNG with a quantum backdoor: we suppose that Eve holds two entangled photons in the state $|\Phi\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$ and sends to Alice one of the two photons as the system she uses for the randomness extraction. If Alice measures in the $\{|H\rangle, |V\rangle\}$ basis she obtains a perfect random bit from the point of view of the classical min-entropy, since the two outcomes, $|H\rangle$ and $|V\rangle$, are equally probable. However, due to the correlations in the $|\Phi\rangle$ state, Eve knows perfectly the outputs of Alice's measurements: the "random" bit held by Alice can be predicted with certainty by Eve. Again, what prevents Alice to extract true random bits is the fact that the variable $Z$ is not independent from the variable $E$ outside its future light cone originated at the spatio-temporal coordinate of the measurement.

In this work, the issue of how to extract the numbers in such a user unfavourable framework is addressed. However, it is worth stressing that thanks to this scenario we can provide a solution also for a problem much more common and, at the same time, fundamentally relevant. This problem is the practical inability to produce (or to keep) *pure* quantum states in a QRNG. Indeed in the previous example, by tracing out Eve, Alice holds a *completely mixed* state, i.e. a state that being just an incoherent sum of pure states corresponds to a classical state. However a general case can account for a partial degree of purity. Typically, the quantum system $A$ may have a quantum correlation with a generic system $E$, which may, or may not, be possessed by an adversary. In particular, we can regard to the system $E$ as a *purification* of $A$ which encompasses all

the side information. This is relevant because in most of the cases, when the presence of an eavesdropper can be ruled out, $E$ can be identified with the purifying system "environment".

Generally, when a state has not rank 1, i.e. it is mixed, only $\epsilon-$true random bits can be generated. The bit remaining fraction features just an *accidental randomness*, i.e. randomness due to the ignorance about some side degrees of freedom, as in a classical framework. If Alice had access to the purification of her mixed state, she would not experience any accidental randomness. In principle then, if an eavesdropper is able to retrieve this side information from a system correlated (in a quantum or classical way) with the generator, then he would be able to predict the remaining fraction of bits. In the worst scenario, this purification is already hold by the Eve as in the example of before.

If we admit the presence of quantum side information, we need to consider the *classical-quantum state* Alice gets after the measurement. In detail, given $E$ a generic system quantum correlated with the system $A$ and given $Z$ a random variable which takes values $z$ with probabilities $P_Z(z)$, let $\rho_E^z$ the density operator on $\mathcal{H}_E$ conditioned to $Z = z$. The post-measurement state is then given by

$$\rho_{ZE} \equiv \sum_z |z\rangle\langle z| \otimes \rho_E^z \,. \tag{5.8}$$

Analogously to the classical case, on the state $\rho_{ZE}$ one can evaluate the conditional min-entropy $H_{\min}(Z|E)$, which corresponds (a formal definition will be given later) the probability of guessing $Z$ having access to the quantum system $E$

$$p_{guess}(Z|E) = 2^{-H_{\min}(Z|E)} \,. \tag{5.9}$$

For instance, in the previous example with the entangled state $|\Phi\rangle$, $p_{guess}(Z|E) = 1$: the system of Alice does not allow the generation of true random numbers. In general then, $p_{guess}$ depends on the degree of purity and the ability to find an optimal strategy to exploit $E$. It becomes then fundamental to answer the question: *is it still possible to get true random numbers from a partially pure state?* The answer is *yes* by introducing into the quantum framework the quantum version of *randomness extractors*. In classical cryptography, a randomness extractor is an algorithmic post-processing which is applied to a set of not identically distributed random numbers with the purpose to reduce the statistical distance between the probability distribution of such numbers and the uniform one. Basically then if one has a string $s$ of $n$ not uniformly distributed random bits, applying the extractor function $f$ to $s$, one gets a string $f(s)$ of length $n' < n$. The string $f(s)$ is shorter than the input one, however it features truly random bits. More specifically, by properly calibrating the function $f$ one can get that an output distribution which is arbitrarily close to the uniform one.

In recent years Renner et al. were demonstrated how these techniques can be extended to the case of random variables associated with some quantum side information. The quantity $H_{\min}(Z|E)$ becomes a tool of paramount importance because it allows to properly set the randomness extractors. With a properly set randomness extractor one

can make the bits $\epsilon$ close to the uniform also in presence of quantum side information. The conditional min-entropy is indeed equivalent to the **the number of uniformly random bits that can be extracted using an optimal extraction strategy**. This can be easily seen considering an extracting function $f$ which maps $Z$ on a bit string $f(Z)$ with length $l$ perfectly uniform conditioned on the side information $E$: the probability to correctly guess $f(Z)$ given $E$ is $p_{guess} = 1/2^l$ so we get

$$H_{min}(f(Z)|E) = l$$

In terms of quantum states, the condition of independence can be expressed as

$$\frac{1}{2}\left\|\rho_{ZE} - \rho_{\bar{Z}} \otimes \rho_E\right\|_1 \leq \epsilon \ ,$$

with $\rho_{\bar{X}} = \frac{1}{|X|}\mathrm{id}$ is the fully mixed density operator on $X$ and $\|\cdot\|_1 = \mathrm{tr}(|\cdot|)$ is the trace norm.

According to [124] and [125] one then can demonstrate the *Generalized Leftover Hash Lemma*: given the class $\mathcal{F}$ of the so-called *two universal hash functions*, i.e. functions from $Z$ to $\{0,1\}^l$ with the property that given $z$ and $z'$ the collision probability $P(f(z) = f(z')) \leq 1/2^l$ and given a classical quantum state $\rho_{ZE}$ then

$$\frac{1}{2}\left\|\rho_{F(Z)EF} - \rho_{\bar{Z}} \otimes \rho_{EF}\right\|_1 \leq 2^{-\frac{1}{2}(H_{\min}(Z|E)-\ell)} = \epsilon' \ ,$$

where

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

and where $\rho_{\bar{Z}}$ is the fully mixed density operator on the space encoding $\{0,1\}^\ell$.

The neat result of this lemma is then that by picking uniformly and independently a function $f$ from the set $\mathcal{F}$, e.g. a linear map with Toeplitz matrices, such that the output string $f(Z)$ has length $l$, then $f(Z)$ is $\epsilon' = 2^{\frac{1}{2}(l-H(Z|E))}$ truly random. The importance of estimating $H(Z|E)$ lies in the fact that it provides the length the final string $f(X)$ needs to have in order to be indistinguishable from a string generated by measuring a state uncorrelated from $E$ with probability at most $\epsilon' < 1$.

### 5.1.1 Estimating the Min-Conditional Entropy

We will present a method, based on the Uncertainty Principle (UP), to estimate the conditional min-entropy and then the amount of true randomness that can be obtained by a given source. We will show and experimentally test that, by measuring the system in conjugate observables $\mathbb{Z}$ and $\mathbb{X}$, it is possible to obtain the following bound on the conditional min-entropy

$$H_{\min}(Z|E) \geq \log_2 d - H_{1/2}(X)\,, \tag{5.10}$$

where $d$ is the dimension of the Hilbert space and $H_{1/2}(X)$ the max-entropy of $\mathbb{X}$ outcomes (see below). The measurement $\mathbb{Z}$ is used to generate the random sequence $Z$, while the measurement $\mathbb{X}$ is used to quantify the amount of true-randomness contained in $Z$. In our protocol we do not use any assumption on the source $\rho_A$: an adversary, called Eve can have full control on the source and the environment $E$. The bound (5.10) is achieved by only assuming trusted measurements device, meaning that Eve has no access to it and that the device performs a given POVM that are only sensitive to a subspace of dimension $d$. To prevent the possibility that an adversary controls the detection efficiency, as reported in quantum hacking against detectors [145, 146, 147], it is necessary to monitor all detector parameters, such as bias voltage, current, and temperature [148]. The advantage of the presented method resides on its simplicity: no Bell inequality violation is required but it is only necessary to measure the system in two conjugate bases. With an initial seed of true randomness, our protocol is able to expand the randomness by taking into account all possible side quantum information possessed by Eve. In particular, with the trusted measurement assumption, we do not need to bound the dimension of the Hilbert space, but we only need that the POVM span a subspace of dimension $d$ of the whole Hilbert space. E.g., if the measurement device performs a projection into $\{|H\rangle, |V\rangle\}$ basis, and the photons have other degrees of freedom, such extra degrees of freedom are completely ignored by the device and the effective Hilbert space is 2.

## 5.2 The Uncertainty Principle for randomness generation

In this section we derive our main result (5.10). We first start by reviewing the uncertainty relation for min- and max- conditional entropies introduced in [149, 150, 151].

### 5.2.1 Uncertainty principle

Let's consider three quantum systems $A$, $B$ and $E$ and $\rho_{ABE}$ a tripartite state. Define $\mathbb{Z}$ and $\mathbb{X}$ as two POVMs on $A$ with elements $\{\hat{\mathcal{M}}_z\}$ and $\{\hat{\mathcal{N}}_x\}$, and random outcomes $Z$ and $X$ encoded in two orthonormal bases $\{|z\rangle\}$ and $\{|x\rangle\}$. Then, the uncertainty principle is written as

$$H_{\min}(Z|E)_\rho + H_{\max}(X|B)_\rho \geq q\,, \tag{5.11}$$

where the min-entropy and max-entropy (see Appendix D.1 and [144] for min- and max-entropy definition) are evaluated on the post-measurement states $\rho_{ZE} \equiv \sum_z |z\rangle\langle z| \otimes \mathrm{Tr}_{AB}[\hat{\mathcal{M}}_z \rho_{ABE}]$, $\rho_{XB} \equiv \sum_x |x\rangle\langle x| \otimes \mathrm{Tr}_{AE}[\hat{\mathcal{N}}_x \rho_{ABE}]$ and

$$q \equiv \log_2 \frac{1}{c}\,, \qquad c \equiv \max_{z,x} \|\sqrt{\hat{\mathcal{M}}_z}\sqrt{\hat{\mathcal{N}}_x}\|_\infty^2\,. \tag{5.12}$$

The parameter $c$ represents the maximum "overlap" between the two POVMs and $q$ quantifies the "incompatibility" of the measurements. If $\hat{\mathcal{M}}_z$ and $\hat{\mathcal{N}}_x$ are projective measurements corresponding to Mutually-Unbiased bases in dimension $d$, then $c = \frac{1}{d}$.

### 5.2.2 Proof of the bound

In a QRNG, Alice measures its system $\rho_A$ by using a POVM measurement $\mathbb{Z} \equiv \{\hat{\mathcal{M}}_z\}$[1]. The state $\rho_A$ is in general correlated with an external system $E$ such that $\rho_A = \mathrm{Tr}_E[\rho_{AE}]$. The possible outcomes of the POVM can be encoded in an orthonormal basis $\{|z\rangle_A\}$, such that the post-measurement state is $\rho_{ZE} \equiv \sum_z |z\rangle\langle z| \otimes \mathrm{Tr}_A[\hat{\mathcal{M}}_z \rho_{AE}] = \sum_z P_z |z\rangle\langle z| \otimes \rho_E^z$ with normalized $\rho_E^z$. Eve's knowledge about the possible outcomes of the $\mathbb{Z}$ measurements is given by the min-entropy $H_{\min}(Z|E)$, evaluated over $\rho_{ZE}$. If Alice sometimes measures her system with a different POVM $\mathbb{X}$, the UP allows to bound the min-entropy $H_{\min}(Z|E)$ and then the guessing probability by eq. (5.9). In fact, by using eq. (5.11) and by considering the system $B$ as a trivial space, the uncertainty relation becomes $H_{\min}(Z|E) \geq q - H_{\max}(X)$, where the max-entropy must be evaluated on the state obtained by the $\mathbb{X}$ measurement, namely $\rho_X \equiv \sum_x p_x |x\rangle\langle x|$, with $p_x = \mathrm{Tr}_{AE}[\hat{\mathcal{N}}_x \rho_{AE}]$. In this case $H_{\max}(X) = 2\log_2 \mathrm{Tr}[\sqrt{\rho_X}]$ (see Appendix D.1 and [144]), i.e. the max-entropy is equal to $H_{1/2}(X)$, the Rényi entropy [2] of order $1/2$ of the classical outcome $X$.

Our result can be summarized as follows: the conditional min-entropy of the $\mathbb{Z}$ outputs can be bounded by using the Rényi entropy of order $1/2$ of the $\mathbb{X}$ outputs, namely

$$H_{\min}(Z|E) \geq q - H_{1/2}(X)\,. \tag{5.13}$$

that reduces to (5.10) in case of conjugate observables in $d$ dimensions. We would like to point out that, thanks to the inequality $H_{1/2}(X) + H_\infty(Z) \geq q$ derived by Maassen and Uffink [152], the bound $q - H_{1/2}(X)$ is always lower than the classical min-entropy $H_\infty(Z)$ evaluated on the probabilities $P_z$.

## 5.3 UP-certified QRNG

Let's now evaluate the bound in two particular cases. Let's consider the $\mathbb{Z}$ POVM as projective measurements in the computational basis, $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ and the $\mathbb{X}$ measurement chosen as its discrete-Fourier transform $|x\rangle = \frac{1}{\sqrt{d}} \sum_{z=0}^{d-1} e^{i\frac{xz}{2\pi d}} |z\rangle$ for which $q = \log_2 d$. If the system $A$ is prepared in the state $|\psi\rangle_A = \frac{1}{\sqrt{d}} \sum_z |z\rangle$, then $H_{1/2}(X) = 0$ and (5.13) bounds $H_{\min}(Z|E)$ to the classical min-entropy $H_\infty(Z) = \log_2 d$. The random variable $Z$ is then uniformly distributed and independent from any adversary. However, in practical implementations of a QRNG, it is impossible to prepare the system $A$ in a perfect pure state $|\psi\rangle_A$. When the state $\rho_A$ is not pure, the entropies $H_\infty(Z)$ and $H_{\min}(Z|E)$ can be different. Our result is thus particularly effective with real sources (that cannot generate pure states) since it bounds the effective achievable randomness without requiring any assumption on them. Even if Eve has complete control on the source $\rho_A$, the bound given in (5.13) evaluates the amount of true random bits that

[1] We employed POVMs to present our method in a general framework, but projective measurements not only are more suited for practical applications but they permit to reach the maximum overlap $c \equiv \max_{z,x} |\langle x||z\rangle|^2$ [126].

[2] We recall that the Rényi entropy of order $\alpha$ is defined as $H_\alpha(X) = \frac{1}{1-\alpha} \log_2 \sum_{x=0}^{d-1} p_x^\alpha$.

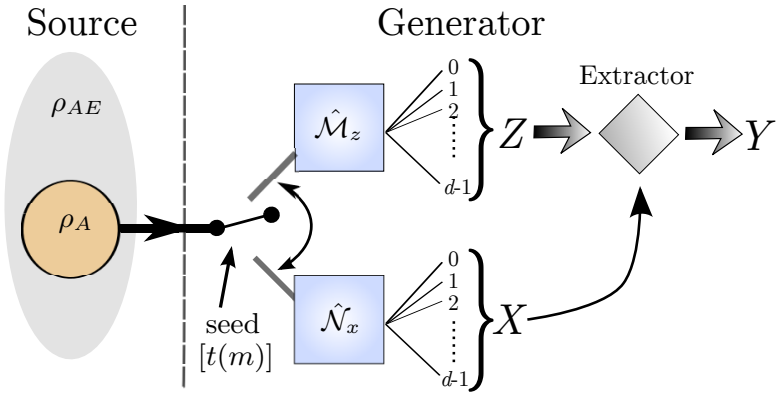


Figure 5.1: Scheme of the QRNG. The source of randomness is the state $\rho_A$ that can be correlated with a larger system $E$. An initial perfect random seed of length $t(m)$ is used to switch between the $\{\hat{\mathcal{M}}_z\}$ and $\{\hat{\mathcal{N}}_x\}$ POVMs, from which the random variables $Z$ and $X$ are extracted. The variable $Z$ is used to generate the random sequence, while the variable $X$ is used to evaluate how many true random bits can be extracted by $Z$. $Y$ represents the final true random sequence.

can extracted from $Z$. This randomness has complete quantum origin and no side information can be used to predict the generated random bits.

Another important example is represented by the system described in the introduction: Eve sends to Alice one photon of a two-photon maximally entangled state, and thus can perfectly predict the outputs of Alice's measurements. In this case, Alice holds a completely mixed state $\rho_A = \frac{1}{2}\mathrm{Id}_2$ and the max-entropy is $H_{1/2}(X) = 1$. Thanks to eq. (5.13) and (5.9), the bound on the min-entropy becomes trivial, $H_{\min}(Z|E) \geq 0$ and $p_{guess}(Z|E) \leq 1$: our result correctly predicts that the guessing probability can reach unity and so no true random bits can be extracted in this case.

In order to exploit the result of eq. (5.13) it is necessary to estimate the max-entropy of the source $\rho_A = \mathrm{Tr}_E[\rho_{AE}]$. However, since the POVM $\{\hat{\mathcal{M}}_z\}$ and $\{\hat{\mathcal{N}}_x\}$ are incompatible, it is not possible to measure them at the same time. We then need to switch randomly between $\hat{\mathcal{M}}_z$ and $\hat{\mathcal{N}}_x$ during the random bit generation (see Figure 5.1). The measurements are chosen by using a seed of true randomness that our method is able to expand. From this point of view, our method can be seen as a random number expansion protocol.

We now show that the number of random extracted bits is greater than the required seed. Let $m$ the total number of runs. We decide that, over $m$, the number of runs in the POVM $\{\hat{\mathcal{N}}_x\}$ will be $n_X = \lceil\sqrt{m}\rceil$, such that the probability of measuring in the $\mathbb{X}$ basis is approximately $\frac{1}{\sqrt{m}}$. To randomly choose $n_X$ among $m$ runs we need a number of bits given by $t(m) = \lceil \log_2 \frac{m!}{n_X!(m-n_X)!} \rceil$. This is the length of the random seed required for the randomness expansion.

The probabilities of outcomes in the $\mathbb{X}$ basis are given by $p_x = \mathrm{Tr}_A[\hat{\mathcal{N}}_x \rho_A]$ and the

asymptotic lower bound of the min-entropy is $H_{\min}(Z|E) \geq q - H_{1/2}(X)$. From the experimental point of view we need to estimate the max-Entropy $H_{1/2}(X)$ by using the $n_X$ outcomes. If we denote by $n_x$ the number of outcomes such that $X = x$, we can estimate the max-entropy by using the Bayesian estimator defined in [153] (with a uniform prior distribution):

$$\widetilde{H}_{1/2}(\{n_x\}) = 2\log_2[\frac{\Gamma(n_X + d)}{\Gamma(n_X + d + \frac{1}{2})}\sum_{x=0}^{d-1}\frac{\Gamma(n_x + \frac{3}{2})}{\Gamma(n_x + 1)}]\,. \tag{5.14}$$

The Bayesian estimator has a lower variance with respect to the frequentist estimator $\widetilde{H}^f_{1/2} = 2\log_2[\sum_{x=0}^{d-1}\sqrt{\frac{n_x}{n_X}}]$. Moreover, for low max-entropies, the frequentist estimator has a negative bias that overestimates the bound on the min-entropy.

Then, given $m$ runs, the number of extracted random bits are the outputs of the $\mathbb{Z}$ measurement, given by $m - n_X$: due to the bound (5.13), at least $(m - n_X)(q - H_{1/2}(X))$ are true random bits. If we subtract the number of bits $t(m)$ required for the seed, we can estimate the random bits generation rate per measurement as

$$\widetilde{r}(\{n_x\}) = \frac{b_{\text{sec}}}{m}\,, \tag{5.15}$$

where $b_{\text{sec}}$ is the number of generated true random bits :

$$b_{\text{sec}} = (m - n_X)[q - \widetilde{H}_{max}(\{n_x\})] - t(m)\,. \tag{5.16}$$

It is worth noticing that, in the infinite size limit $m \to +\infty$, the seed length is given by $t(m) \sim \sqrt{m}\log_2\sqrt{m}$, the estimator $\widetilde{H}_{1/2}(\{n_x\}) \sim H_{1/2}(X)$, and the rate approaches the asymptotic limit $\widetilde{r} \longrightarrow r(Z) = q - H_{1/2}(X)$. Since the number of extracted random bits are quadratically larger than the initial seed bits, the generator can work in loop: an initial seed is expanded and part of the extracted randomness is fed as a new seed.

## 5.4 Experimental realization

We wanted to give a proof of principle of the protocol with an experiment aimed to demonstrate how the min-classical entropy is an inaccurate over-estimator the QRNG randomness also for an optimized source of state in a controlled environment as a laboratory. On the contrary the min-conditional entropy yields the correct estimation of the true extractable random bits. It is worth to stress in a practical scenario, with a QRNG realized in a compact device one has indeed to cope with an unavoidable amount of preparation noise which arises not only from the non-ideality of the optical elements used but also from the environment itself and the aging of the system.

### 5.4.1 Photon source

Photons used in experimental demonstration of the method were generated by spontaneous parametric down conversion (SPDC), as illustrated in Figure 5.2.

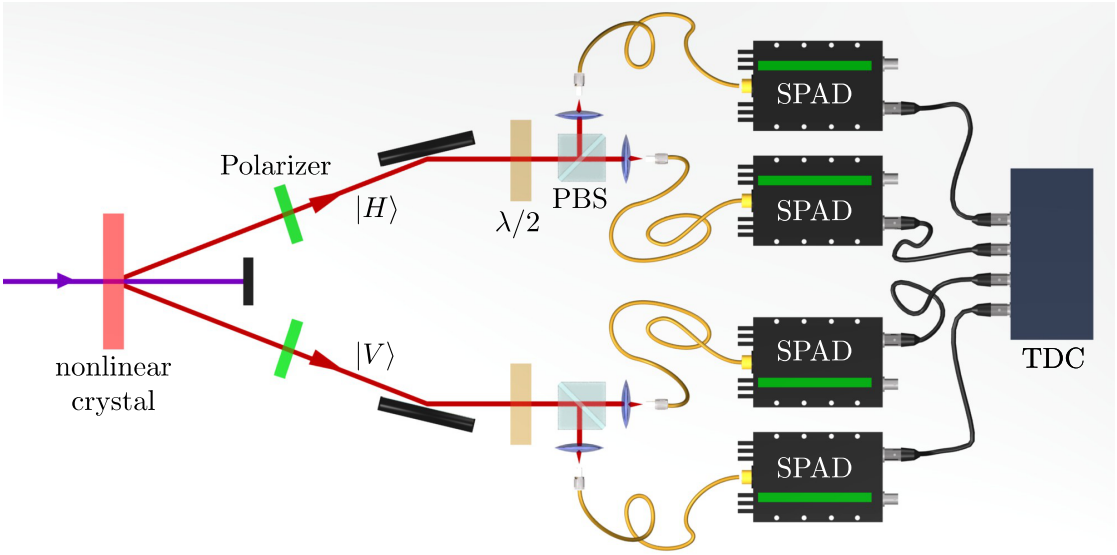


Figure 5.2: (Color online) Scheme of the experimental setup generating the SPDC photons. TDC=Time to digital converter; SPAD=single-photon avalanche diode; PBS=polarizing beam splitter, $\lambda/2$=waveplates.

To generate the states we used a source of photon pairs generated by spontaneous parametric down conversion (SPDC). We used a laser **Coherent MIRA-HP** with $\lambda =$ 808 nm with pulse width of 130 fs and repetition rate of 76 MHz shining a BIBO crystal for second harmonic generation at 404 nm. Then beam is then focused on a nonlinear BBO crystal where pairs of photons are probabilistically emitted over two correlated directions (channels). The bi-photon system features entanglement in polarization and the BBO crystal is oriented in order to have a state $|\Psi^{\pm}\rangle = \frac{|HV\rangle \pm |VH\rangle}{\sqrt{2}}$, with $|H\rangle$ and $|V\rangle$ the horizontal and vertical polarized photon respectively (in the setup we have also walk-off crystals in order to have time uncertainty and correct the relative phase).

In Figure 5.3, the results of a typical tomography for an optimized state the density matrix $|\Psi^{-}\rangle$ is reported, with an high fidelity of 0.975 and a purity of 0.962. The typical coincidence rate for this source is of $\approx 3.5 - 4$ kHz.

It is worth stressing that for the experiment the entangled state was just the *pre-preparation* stage. The entanglement was indeed destroyed when the photons were prepared in a given polarization. Indeed, the advantage of using a bi-photonic system is that we could easily test also the generator based on a 4 dimensional space, ququart. In the two channels we placed a vertical and a horizontal polarizers respectively, in order to generate the product state $|HV\rangle$. The part up to the polarizers then can be regarded as the *preparation stage*. The *measure stage*, was realized by collocating half-wave plates $\lambda/2$ and polarizing beam-splitters (PBS) in both channels. The beam -plitters were then coupled to fibers which brought the signals to the single photon detectors **Exceli-**

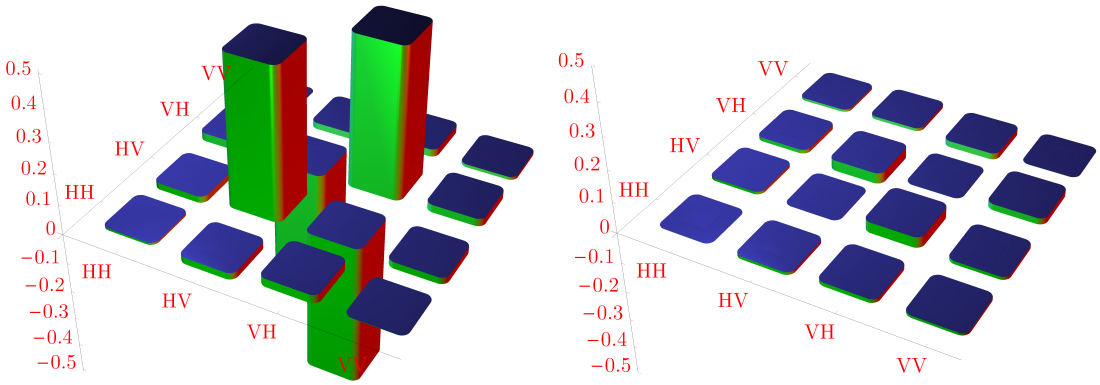


Figure 5.3: Typical plot for the real and imaginary part for the density matrix of $|\Psi^-\rangle$

**tas**. The detection signals were delivered to a time-to-digital converter (TDC) **QuTools QUTAU** which allowed to store in a PC the time tags of the coincidence events.

As first try however, we implemented a qubit generator employing just one photon, i.e. we used the pair as an heralded single photon source. The photon in $|V\rangle$ basis represented the signal, i.e.the state used to extract the random bits, while the photon in the $|H\rangle$ state was used as trigger: with its detection heralded the presence of the $|V\rangle$ photon.

The switching between the measurement basis $\mathbb{Z}$ and the check basis $\mathbb{X}$ was done by manually operating the half-wave plates. More specifically, by measuring the signal photon in the $\mathbb{Z} = \{|+\rangle, |-\rangle\}$ and $\mathbb{X} = \{|H\rangle, |V\rangle\}$ bases, we generate the random variables $Z$ and $X$. Here we denote with $|\pm\rangle$ the diagonal polarization states $\frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$. From the measurements in $\mathbb{Z}$ basis the random bits 0 and 1 were extracted and, in the ideal case, expected to be in the same percentage (50:50). Instead from the measurements in $\mathbb{X}$ basis it was expected to have detections only for the state $|V\rangle$. The results of the runs for the qubit are presented in Table 5.1. As one can see the state is not completely pure, and the max-entropy evaluated on the data of the check basis let us to properly estimate the true amount of random bits (see below).

| **Qubit (prepared in $\|V\rangle$)** | | | |
|---|---|---|---|
| $\mathbb{Z}$ (random basis) | | $\mathbb{X}$ (check basis) | |
| $P_0$ | $P_1$ | $P_V$ | $P_H$ |
| 0.5020 | 0.4980 | 0.9973 | 0.0027 |

Table 5.1: The results for both the check and random bases for the qubit prepared in the state in $|V\rangle$. As one can see the s

The second generator was a 4-level system (ququart) QRNG, represented by the whole pair of photons. In this case the $\mathbb{Z}$ and $\mathbb{X}$ bases are respectively given by $\{|++\rangle, |+-\rangle, |-+\rangle, |--\rangle\}$ and $\{|HV\rangle, |VV\rangle, |HH\rangle, |VH\rangle\}$. In Table 5.2 the values obtained from the measurements are reported. As for the qubit, also the ququart presented some

mixedness which caused a reduction of the percentage of true random bits extractable per run, with respect to the simple classical min-entropy (evaluated on the random basis).

| **Ququart (prepared in $\|HV\rangle$)** | | | | | | | |
|---|---|---|---|---|---|---|---|
| $\mathbb{Z}$ (random basis) | | | | $\mathbb{X}$ (check basis) | | | |
| $P_{00}$ | $P_{01}$ | $P_{10}$ | $P_{11}$ | $P_{HH}$ | $P_{HV}$ | $P_{VH}$ | $P_{VV}$ |
| 0.2527 | 0.2412 | 0.2608 | 0.2453 | 0.00359 | 0.9937 | 0.00266 | 0.00005 |

Table 5.2: Results for the measurements of the ququart QRNG.

Concerning the rate of raw bits extraction, the source has a coincidence rate of 12 kHz: this rate was achieved by using multi-mode fibers in order to reduce the time required to collect a reasonable amount of data to be tested effectively by the suite test. It is worth stressing that the use of multimode fibers do not represent an issue for what concerns side information: the detectors indeed are not sensitive to the spatial mode. Besides we would like to point out that we were not interested in the speed of the generator, but on the demonstration of the method here presented. However, it is worth noticing that sources producing photon pairs at the rate of few MHz are currently available [156, 157] (e.g. Sagnac sources).

### 5.4.2 Analysis of the results

We first analyze the qubit QRNG. By choosing different values of $m$ we performed $n_X = \lceil \sqrt{m} \rceil$ measurements in the $\mathbb{X}$ basis and $n_Z = m - n_X$ measurements in the $\mathbb{Z}$ basis, obtaining the sequences $X$ and $Z$. The two sequences are used to estimate the classical max-entropy $\widetilde{H}_{1/2}(\{n_x\})$ and the rate $\widetilde{r}(\{n_x\})$. For each $m$, in figure 5.4 we show the average rate $\widetilde{r}$ and its standard deviation experimentally evaluated over 200 different $X$ sequences of $n_X$ bits (see Section 5.4.3 for the rate achieved, for each $m$, by a single $X$ sequence of $n_X$ bits). The experimental rates can be compared with the predicted average rate $\langle \widetilde{r} \rangle = \sum_{\{n_x\}} \Pi(\{n_x\}) \widetilde{r}(\{n_x\})$, obtained by averaging $\widetilde{r}(\{n_x\})$ over the multinomial distribution $\Pi(\{n_x\}) = \frac{n_X!}{n_0! n_1! \cdots n_{d-1}!} p_0^{n_0} p_1^{n_1} \cdots p_{d-1}^{n_{d-1}}$. We also show the classical min-entropy $\widetilde{H}_\infty(Z)$ evaluated on a sequence $Z$ with $n_Z$ bits. The figure shows a very good agreement between the experimental result and the theoretical prediction. It is worth noticing that at least $m > 150$ measurements are necessary to obtain a positive rate $\widetilde{r}$, while with just $m \simeq 10^6$ the rate is very close to the asymptotic bound $r(Z)$. The difference between $H_\infty(Z)$ and $\widetilde{r}$ corresponds to the possible knowledge that an adversary holding the system $E$ may have. The limit $H_\infty(Z)$ is often and erroneously taken as the amount of true randomness used to calibrate the extractor: in this way, even if the output string appears statistically good, possible side information held by Eve is not completely erased. In our experimental analysis, since we are mainly interested in demonstrating the physical principles, we did not use active switches to change between the two bases (we first measured the $Z$ sequence and afterwards the $X$ sequence). For practical applications, however, the QRNG should contain an active switch controlled

by the seed $t(m)$.

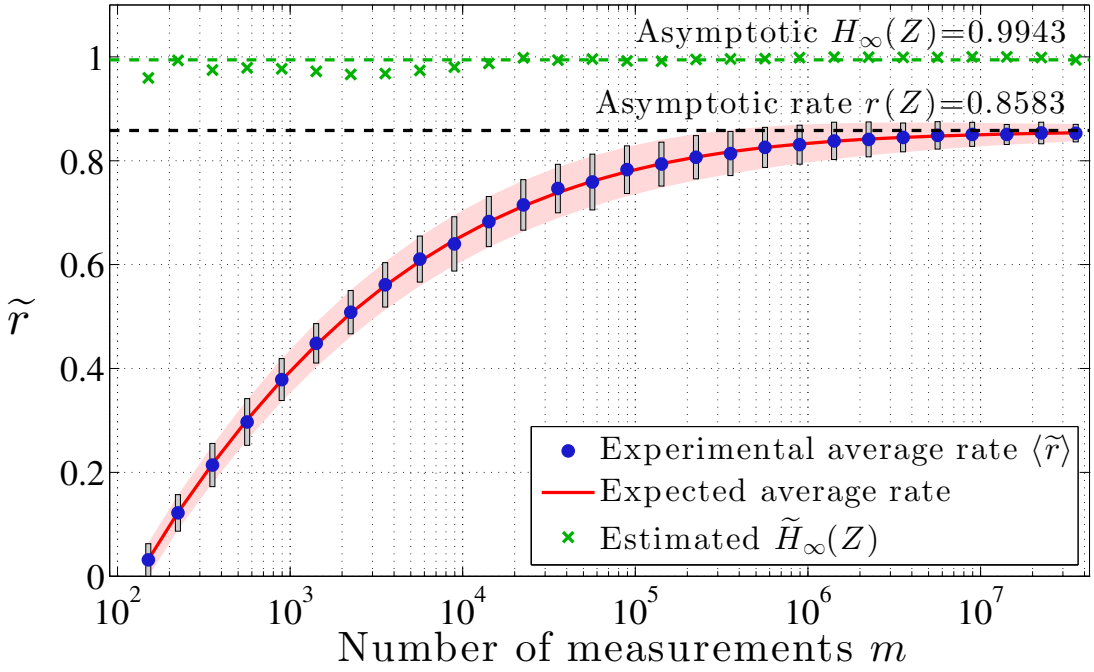


Figure 5.4: (Color online) Average experimental rate for the qubit QRNG. Blue circles represent the experimental average rate $\widetilde{r}$ of true random bits per measurement, while the continuous red line is the theoretical prediction with $\rho_X = \sum_{x=0}^{1} p_x|x\rangle\langle x|$ where $p_0 = 0.9973$ and $p_1 = 0.0027$. Shaded red area represents the theoretical standard deviation of the rate, while gray rectangles show the experimental standard deviation of the rate. Green crosses show the classical min-entropy estimated on the $Z$ random variable. The asymptotic limit $H_\infty(Z)$ is evaluated on the state $\rho_Z = \sum_{z=0}^{1} P_z|z\rangle\langle z|$ with $P_0 = 0.5020$ and $P_1 = 0.4980$.

In figure 5.5 the results for the ququart QRNG, are presented. Also in this case, for each $m$, the average rate $\widetilde{r}$ and its standard deviation are experimentally obtained by 200 different $X$ sequences of $n_X(m)$ bits. Again, there is a very good agreement between the experimental results and the theoretical predictions and a positive (average) rate is obtained for $m > 70$. As before, for $m \simeq 10^6$ the rate is very close to the asymptotic bound $r(Z)$: thanks to the larger Hilbert space, we can asymptotically obtain 1.685 bits per measurement, that should be compared with the value 0.8437 achieved with the qubit QRNG. Our method shows then to be resilient also increasing the dimension of the system: once that the state is checked in the $d$ dimensional preparation basis the ideal content of true random bits, i.e. 2, is correctly scaled according the degree of purity of the state.

For the complete proof of our protocol, we performed the extraction on a long random

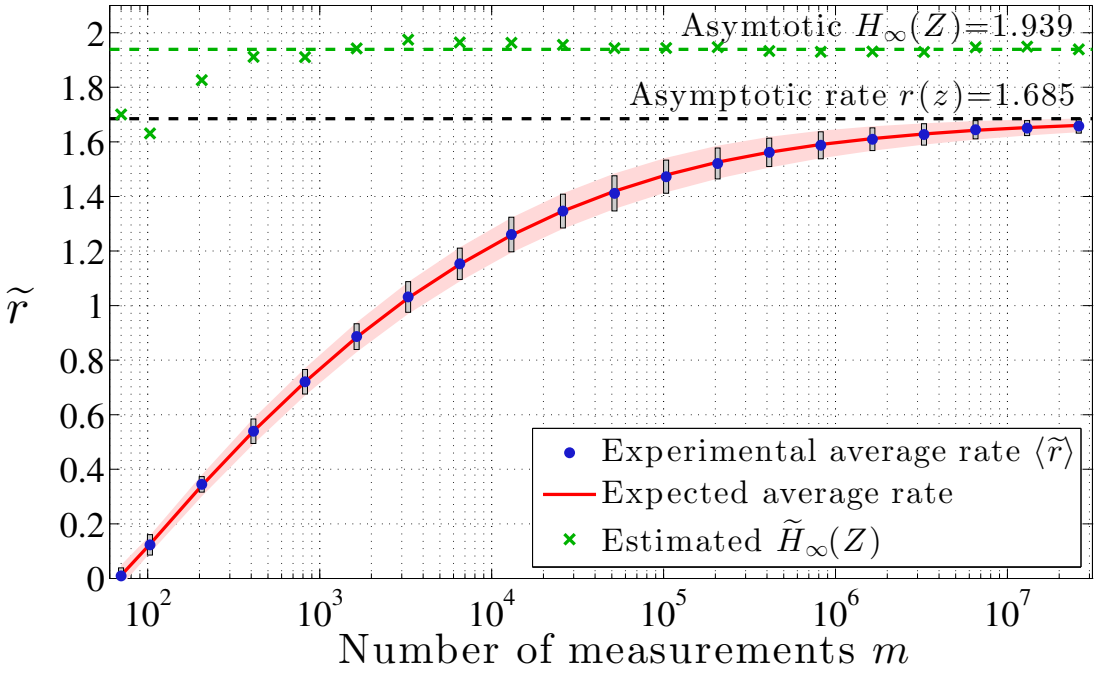


Figure 5.5: (Color online) Average experimental rate for the ququart QRNG. See figure 5.4 for notations. In this case $\rho_X = \sum_{x=0}^{3} p_x|x\rangle\langle x|$ with $p_0 = 0.9937$, $p_1 = 0.00359$, $p_2 = 0.00266$ and $p_3 = 1 - p_0 - p_1 - p_2$ and $\rho_Z = \sum_{z=0}^{3} P_z|z\rangle\langle z|$ with $P_0 = 0.2527$, $P_1 = 0.2412$, $P_2 = 0.2608$ and $P_3 = 0.2453$.

sequence $Z$ and the results are presented in Section 5.4.5.

### 5.4.3 Analysis of the random bit generation rate

In this section we show the experimental rate obtained with a single control $X$ sequence for the rate achieved with the qubit QRNG. We here recall that, given $m$ measurement on the state $\rho_A$, we obtained two classical $X$ and $Z$ sequences with $n_X$ and $n_Z$ bits respectively, whose lengths are respectively given by $n_X = \lceil\sqrt{m}\rceil$ and $n_Z = m - n_X$. The state of the system $A$ after the measurement is given by $\rho_Z = \sum_{z=0}^{1} P_z|z\rangle\langle z|$ or $\rho_X = \sum_{x=0}^{1} p_x|x\rangle\langle x|$, depending on the used POVM.

Given $m$, we would like to evaluate the "single shot" rate $\widetilde{r}$ given by:

$$\widetilde{r}(n_0, n_1, m) = (m - n_X)(1 - \widetilde{H}_{1/2}(n_0, n_1)) - t(m)\,, \tag{5.17}$$

with $n_0$ and $n_1$ the number of 0's and 1's in the $X$ sequence.

For the single qubit QRNG, since $n_0 + n_1 = n_X$, the single shot rate is function of

only $m$ and $n_1$:

$$\begin{aligned}\widetilde{r}(n_1,m) =&(m-n_X)\left\{1-2\log_2[\frac{\Gamma(n_X+2)}{\Gamma(n_X+\frac{5}{2})}]\right.\\ &\left.-2\log_2[\frac{\Gamma(n_X-n_1+\frac{3}{2})}{\Gamma(n_X-n_1+1)}+\frac{\Gamma(n_1+\frac{3}{2})}{\Gamma(n_1+1)}]\right\}\\ &-\lceil\log_2\binom{m}{n_X}\rceil\,.\end{aligned} \tag{5.18}$$

For different values of $m$ we show in figure 5.6 the achieved rate: each point represents the rate $\widetilde{r}$ evaluated over a single $X$ sequence of $n_X$ bits obtained by the measurement in the $\mathbb{X}$ POVM. Each sequence is taken from a sample with the following property:

$$\rho_X=\sum_{x=0}^{1}p_x|x\rangle\langle x| \quad \text{with} \quad p_0=0.9973\,,p_1=0.0027. \tag{5.19}$$

For perfect state preparation we would like to have $p_0=1$ and $p_1=0$: by this reason, the number of 1 in the $X$ sequence are defined as the "number of errors" in the sequence. The "errors" can be caused by the presence of the eavesdropper, or by imperfections in the preparation devices. Since $p_1$ is very low, in Figure 5.6 it is possible to see that, for $m<10^3$, few sequences have 1 errors and the most have 0 errors. By increasing $m$, the number of errors increases to follow the prediction $n_1\sim p_1 n_X$. For low $m$, the possible rates are "quantized", since the rate is evaluated on integer values $n_0$ and $n_1$. In figure 5.7 we show estimated max-entropy $\widetilde{H}_{1/2}(X)$ in function of the number of errors for the $n_X=100$ and $n_X=1000$ case. We also report the probability of obtaining $n_1$ errors, given by $\Pi(n_1)=\binom{n_X}{n_1}p_0^{n_0}p_1^{n_1}$. The figure shows that $\widetilde{H}_{1/2}(X)$ has discrete values corresponding to different values of $n_1$.

### 5.4.4 Detailed comparison with Ref. [128]

Here we give a detailed comparison between our method and the result of Fiorentino *et al* [128], where the conditional min-entropy of a qubit state is evaluated by measuring its density matrix $\rho=\frac{1}{2}(\mathrm{Id}+\vec{r}\cdot\vec{\sigma})$ ($\sigma_i$'s are the Pauli matrices and $\vec{r}$ is a three-dimensional vector such that $|\vec{r}|\leq 1$). By extracting the random bits by measuring the qubit in the computational basis $\mathbb{Z}=\{|0\rangle,|1\rangle\}$ such that $r_z=\langle 0|\rho|0\rangle-\langle 1|\rho|1\rangle$, the conditional min-entropy was estimated to be $H_{\min}(Z|E)=1-\log_2(1+\sqrt{1-r_x^2-r_y^2})$ [128].

Our method estimates the min-entropy of the $Z$ outcomes by measuring in the $\mathbb{X}=\{|\pm\rangle\}$ basis giving the asymptotic bound of $H_{\min}(Z|E)\geq 1-\log_2(1+\sqrt{1-r_x^2})$. Our result is a lower bound, since $q-H_{1/2}(X)=1-\log_2[1+\sqrt{1-r_x^2}]$: the bound is tight when $r_y=0$. If the state is pure, the result of [128] allows to achieve the upper limit $H_{\min}(Z|E)=H_\infty(Z)$. The advantage of our approach resides in the fact that it is not necessary to measure the full density matrix but only measurements on two mutually-unbiased basis. Indeed, in order to evaluate the density matrix, it is necessary to measure

the system also in the $\mathbb{X}$ and $\mathbb{Y} = \{\frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)\}$ basis beside the basis chosen to obtain the random sequence. Also in the case of [128], a random seed is needed to switch between the tomography bases and the random sequence basis. As a final consideration, the result of Fiorentino *et al.* applies only to qubit systems, while our result can be applied to a general qudit systems, as we have demonstrated by analyzing the ququart QRNG.

We now give a detailed comparison for finite $m$: let's consider the following parameters $r_z = 0.9947 \pm 0.001$ and $r_x = 0.004 \pm 0.002$ corresponding to the experimental measured parameter of our qubit QRNG. Since the norm of the vector $\vec{r}$ cannot be greater that 1, it implies that $|r_y| \leq \sqrt{1 - r_z^2 - r_x^2} \leq 0.1027$ corresponding to a purity greater that $\mathcal{P}_{\min} = 0.9947$. We recall that purity of the state $\rho$ is defined as $\mathcal{P} = \mathrm{Tr}[\rho^2] = \frac{1+r_x^2+r_y^2+r_z^2}{2}$. The measurement in the $Y$ basis will allow to determine the $r_y$ parameter.

We performed the detailed comparison, in the finite $m$ case ($m$ is the total number of measurements), between our method and Ref. [128]. To obtain a fair comparison we set $n_X^* = n_Y^* = \lceil \sqrt{m}/2 \rceil$ as the number of measurements in the $X$ and $Y$ basis respectively for the tomographic method of [128]. Then the number of measurements in the $Z$ basis is given by $n_Z^* = m - 2\lceil \sqrt{m}/2 \rceil$. From such measurements the $r_x$ and $r_y$ parameters are estimated as (we used Bayesian estimators):

$$r_x = \frac{n_{0x} - n_{1x}}{n_{0x} + n_{1x} + 2} \qquad r_y = \frac{n_{0y} - n_{1y}}{n_{0y} + n_{1y} + 2} \tag{5.20}$$

To randomly choose the $X$ and $Y$ measurements over the total number of measurements $m$ we need a number of bits given by $t^*(m) = 2\lceil \log_2 \frac{m!}{(2n_X^*)!(m-2n_X^*)!} \rceil$.

In Fig. 5.9 we show the comparison between the two rates in case of perfect pure state $\mathcal{P} = 1$ and in the case of $r_y = 0$, corresponding to $\mathcal{P} = 0.995$: the figure show that our results are slightly outperformed by the tomographic extractor only for high purity states $\mathcal{P} > 0.995$ and in the large $m$ regime ($m > 10^5$). A maximum of 15% improvement with respect to the results shown in Fig. 2 is expected if the generated state is pure $\mathcal{P} = 1$ and $N > 10^8$. However, to obtain such limited advantage, a complication in the scheme, namely the measurement in the $Y$ basis, is required.

### 5.4.5 Tests on the extracted random numbers

As a quantitative example for the complete proof of our method, we performed the extraction on a long random sequence $Z$. For the qubit case we use a random sequence $Z$ of length $n_Z = 35.6 \cdot 10^6$ and a control sequence $X$ of length $n_X = 5967$, requiring a seed length $t(m) = 83443$. The estimated lower bound for the min-entropy is $1 - H_{1/2}(X) \simeq 0.8437$ giving an output random sequence $Y$ of $b_{\text{sec}} \simeq 29.951 \cdot 10^6$ bits. For the qudit case, we have $n_Z = 25.770 \cdot 10^6$ and $n_X = 5100$ with a seed length $t(m) = 70163$. The estimated lower bound for the min-entropy is 1.690, giving $b_{\text{sec}} \simeq 43.886 \cdot 10^6$ true random bits. In both case, the initial $Z$ strings are fed to an extractor by two-universal hashing [158, 142] to obtain the $Y$ strings.

As we did in Chapter 3 we tested the strings with the most stringent tests [159] for the *statistical* assessment of i.i.d. hypothesis for random bits. The results are presented in Appendix : in Table E.1 and E.2 we report the results applied on the secure bits extracted by measuring the qubit and the ququart respectively.

All the tests were passed, as expected when an extractor is properly calibrated with the entropy. More specifically, the extractor is implemented by taking the matrix-vector product (performed modulo 2 cfr. [142]) between strings $n$ raw-bit long and a $l \times n$ matrix of random bits[1]. To calibrate properly means that the ratio $l/n$ is the same as $H_{\min}(Z|E)/\log_2(d)$, i.e. the output strings have to be shorter than the input ones, in proportion to content of randomness.

In order to make clear the contribute of this work, it is important to consider that also calibrating the extractor using the classical min entropy lets one to pass all the *statistical tests*. However those extra bits that Alice obtains with respect to the use of the conditional min-entropy, could be in possess of Eve. In other words, the use of statistical tests does not give information about the true content of randomness of the numbers produced by a QRNG.

## 5.5 Conclusions

We provided a bound, given by equation (5.13), to directly compute the conditional min-entropy $H_{\min}(Z|E)$ of the random variable $Z$, by using the classical random variable $X$. The variables $Z$ and $X$ are obtained by measuring the system in two mutually unbiased bases. $H_{\min}(Z|E)$ represents the amount of true randomness that can be extracted from $Z$. No assumption is made on the source and/or the dimension of Hilbert space. Our result is based on the fact the measurement device is trusted: we assumed that the measurement system (waveplates and PBSs) works properly and the detector efficiency is not dependent on the input state or on an external control. In order that detection system is only sensitive to a well known and characterized finite dimensional subspace of the total Hilbert space, photon number resolving detectors or the squashing model of QKD [154, 155] can be implemented. It is important to stress that if the source does not generate a perfect pure state (and this always happens in experimental realizations), the randomness extracted by standard methods, namely by measuring the system in a single basis, is not a true randomness: an eavesdropper can have (partial or full) information about the generated random bits. We have also tested our bound with a qubit and a ququart QRNG with good agreement between theory and experiment.

Our method can be extended by taking into account possible imperfections in the measurement device, as illustrated in [142]. We believe that our method can be very useful for the extraction of true randomness and can be applied in the framework of practical high-speed QRNG [132, 134], since it guarantees protection against quantum side information without the need of complex Bell violation experiment.

[1] For purpose of demonstration we used random matrix obtained by our software of analysis. In reality how these matrix should be chosen and embed in a generator is matter of discussion. The important point is however that the matrix can be chosen once and then used for all the bits [142].

On this respect the whole UP protocol might be regarded as a *dynamic quantum extractor*. Indeed, the typical scenario of QRNG use, as required by the certification institutions such as the German BSI, one has to continuously or periodically check if the physical source is emitting the so-called raw-random numbers with a degree of independence and uniformity which would lead to the passing of statistical tests once a given extractor is applied on them. On one hand, this approach is dynamic because it evaluates in real time the goodness of the numbers and it varies on feedback the parameters of the extractors in order to get more entropy or to eventually stop the generator, but on the other hand it is not quantum because it is not able to identify the origin of the randomness coming from the physical source.

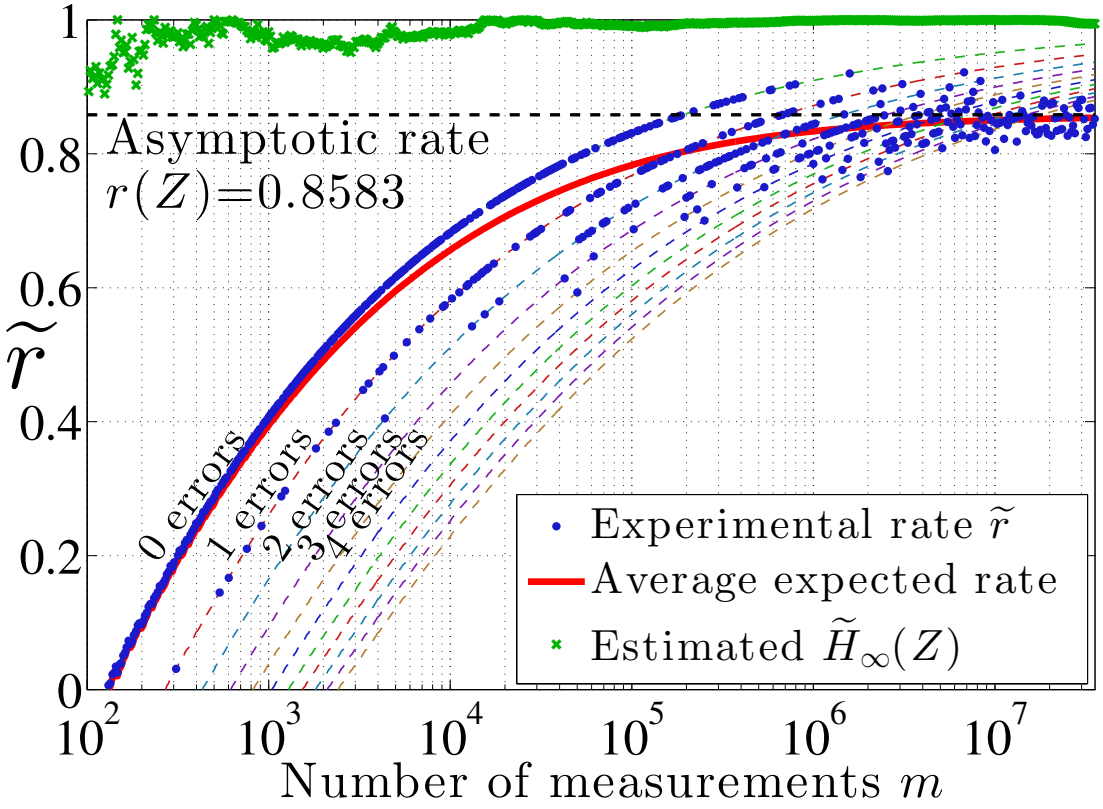


Figure 5.6: (Color online) Experimental rate for the qubit RNG. Blu circles represents the experimental rate $\widetilde{r}$ of true random bits per measurement, while continuous red line represent the theoretical average prediction with $\rho_X = \sum_{x=0}^{1} p_x |x\rangle\langle x|$ where $p_0 = 0.9973$ and $p_1 = 0.0027$. Dashed lines represent the rate achieved with different number of "errors" in the $X$ sequence. Green crosses show the classical min-entropy estimated on the $Z$ random variable obtained from the state $\rho_Z = \sum_{z=0}^{1} P_z |z\rangle\langle z|$ with $P_0 = 0.5020$ and $P_1 = 0.4980$.

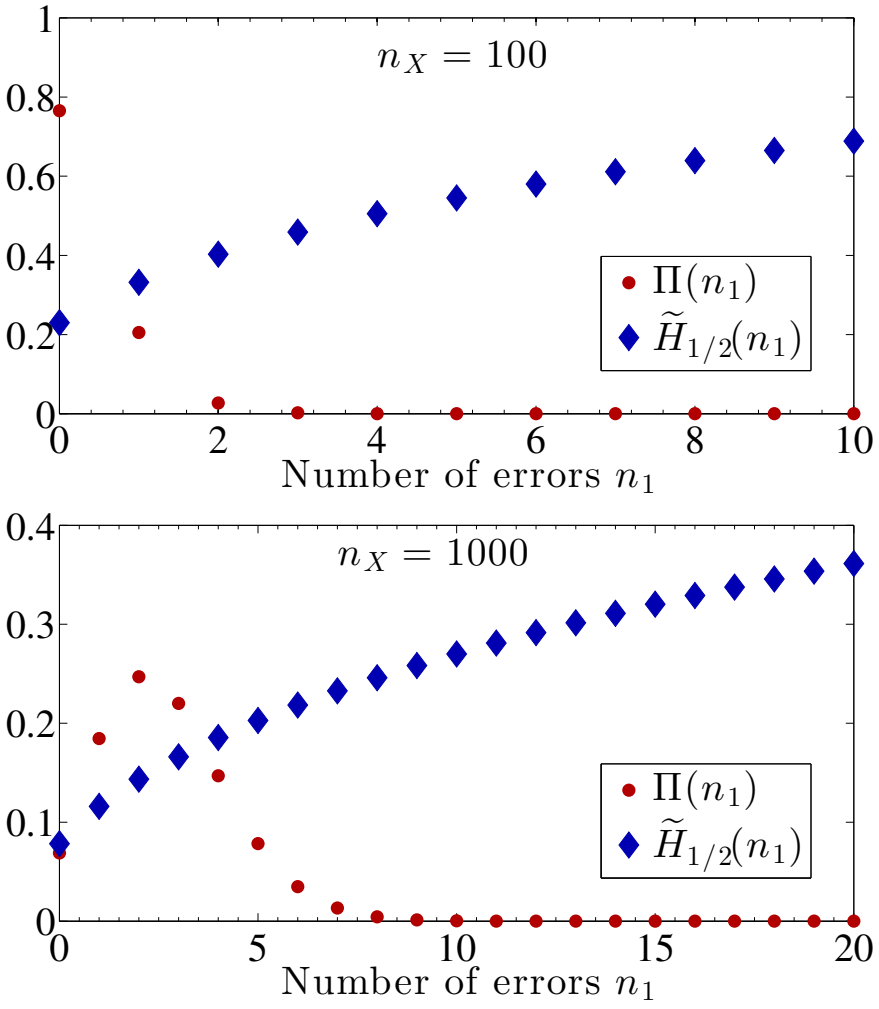


Figure 5.7: (Color online) Extimated max-entropy $\widetilde{H}_{1/2}(X)$ and error probability $\Pi(n_1)$. Due to the low value of $p_1 = 0.0027$, the $\Pi(n_1)$ is peaked around the low values of $n_1$.

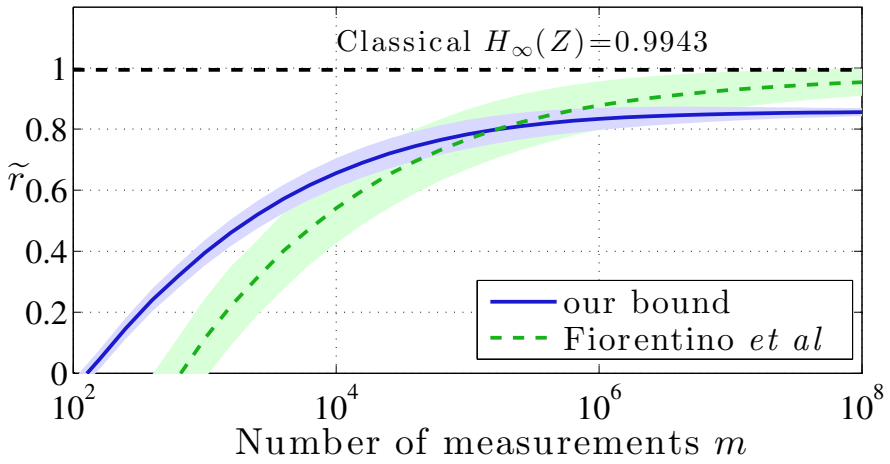


Figure 5.8: (Color online) Comparison between the rate achievable by our bound (continuous blu line) and the rate achievable with the min-entropy estimation of Ref. [128] (dotted green line) in the case of perfect pure state with purity $\mathcal{P} = 1$.

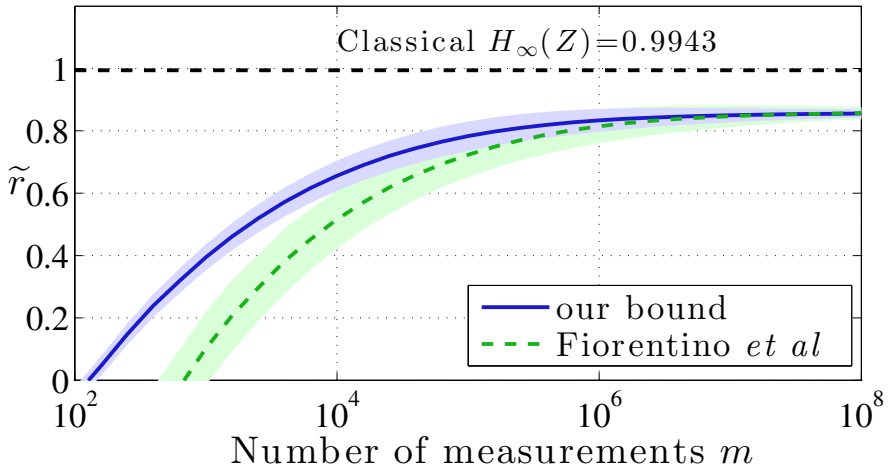


Figure 5.9: (Color online) Comparison between the rate achievable by our bound (continuous blu line) and the rate achievable with the min-entropy estimation of Ref. [128] (dotted green line) in the case of slightly mixed state with purity $\mathcal{P} = 0.995$.

# Chapter 6

# Entropic Uncertainty Principle to bound the randomness of a Continuous Variable QRNG.

In the previous Chapter we showed how min-conditional entropy is a tool of paramount importance in order to distil secure true random bits in presence of quantum side information. There the QRNG was based on a finite dimensional quantum system. In this Chapter infinite dimensional quantum systems will be considered, i.e. we will work on a *continuous variable* QRNG possibly quantum correlated with some other infinite dimensional quantum system. The Chapter is structured as follows. In Section 6.1 we will introduce the working scheme of a CV-QRNG based on Gaussian states of the electromagnetic field. In Section 6.2 the *entropic uncertainty principle* (EUP) for infinite dimensional systems will presented: the CV-EUP is a very recent result of Quantum Information Theory and it is the tool that let us to expand the results of previous Chapter to the CV framework. In Section 6.2 we will adapt the principle to the case of secure random number generation: in particular we will show how the fraction of true random bits depends on the precision of the measurements and most importantly, we will explain how the EUP can be suitable for real CV-QRNG which are unavoidably affected by electronic noise. In Section 6.4, the experimental realization of CV-QRNG will be presented which let us the generate secure random bits at a rate of 5 Gbit/s. In Section 6.5 we will discuss the obtained results.

## 6.1 Introduction

A drawback of DV-QRNG working in the single photon regime is that they are limited by the count rate of the single photon detectors which, at the present time, do not allow to extract random numbers at a rate higher than tens of megabits per second. A way to overcome this limit is by shifting the paradigm from *discrete quantum variables*, e.g. the number of polarized photons which takes a given path in a beam-splitter, to *continuous*

*quantum variables*, e.g. the quadrature amplitudes of the electromagnetic field modes. CV-QRNGs are typically based on the process of measuring the quadrature fluctuations of Gaussian states of the field. These quantum fluctuations are amplified by a strong classical field, the so-called *local oscillator*, whose intensity is detected by photodiodes in a *homodyne scheme* (see below). Photodiodes generate a current signal fluctuating according the field quantum fluctuations. Random numbers are then generated by sampling the difference current signal with an analog to digital converter (ADC). The key point lies in the fact that the random signal has an infinite bandwidth and then can be limited only by the bandwidth of the detectors. At present time, commercial photodiodes feature operating bandwidths of tens of GHz. Therefore by combining large bandwidth receivers with ultrafast ADC, generation rates of hundreds or Gigabit/s are achievable.

The possibility to estimate the real entropy of a CV-QRNG is relevant because this kind of generators seems to be a promising candidate

An N bosonic mode system corresponds to the N modes of a quantized electromagnetic field. The Hilbert space of such a system is the tensor product $\mathcal{H} = \otimes_{k=1}^{N} \mathcal{F}_k$ where $\mathcal{F}_k$ is an infinite dimensional Fock space spanned by a countable basis $\{|m\rangle_k\}_{m\in\mathbb{N}}$, the so-called Fock basis, where each $|m\rangle_k$ is an eigenstate of the number operator $\hat{n} := \hat{a}^\dagger \hat{a}$. The operators $\hat{a}^\dagger$ and $\hat{a}$ associated to a bosonic mode are the so-called creation and destruction operators respectively for which the commutation relation $[\hat{a}, \hat{a}^\dagger] = 1$ holds. These operators are typically used to provide a quantization of a classical electromagnetic field and indeed $\hat{a}$ is usually regarded as the quantized version of the field complex amplitude. Starting from the creation and destruction operators, one can define the so-called *quadratures* operators which correspond to *in-phase* and *out-of-phase* components of the electric field amplitude of a mode $\hat{q} = 2^{-\frac{1}{2}} (\hat{a}^\dagger + \hat{a})$ and $\hat{p} = i(2)^{-\frac{1}{2}} (\hat{a}^\dagger - \hat{a})$ of the electromagnetic field. A generic quadrature is expressed as $\hat{q}(\varphi) = 2^{-\frac{1}{2}} (e^{i\frac{\varphi}{2}} \hat{a}^\dagger + e^{-i\frac{\varphi}{2}} \hat{a})$: note that $\hat{p} = \hat{q}(\pi)$. Practically the quadratures corresponds to real and imaginary part of the complex amplitude $\hat{a} = {}^1\!/\!\sqrt{2}(\hat{q} + i\hat{p})$. The quadrature operators are associated to canonically conjugate observables because $[\hat{q}, \hat{p}] = i$, with $\hbar = 1$. One then usually refers to them as the *momentum* and *position* of field although they live in the complex phase space, i.e. they do not measure the position and momentum of photons.

For position and momentum we have eigenvalues equations, $\hat{q}|q\rangle = q|q\rangle$ with $q \in \mathbb{R}$ and $\hat{p}|p\rangle = p|p\rangle$ with $p \in \mathbb{R}$, where the sets of eigenvectors $\{|q\rangle\}_{q\in\mathbb{R}}$ and $\{|p\rangle\}_{p\in\mathbb{R}}$ correspond to two mutually unbiased bases. This can be seen by considering that the states belonging to the two bases are related by means of Fourier transforms

$$|q\rangle = \frac{1}{\sqrt{2\pi}} \int dp e^{-iqp} |p\rangle \,, \;\; |p\rangle = \frac{1}{\sqrt{2\pi}} \int dq e^{iqp} |q\rangle \tag{6.1}$$

such that $\langle q|p\rangle = (2\pi)^{-1/2} e^{iqp}$ and so the condition for mutual unbiasedness $|\langle q|p\rangle|^2 = (2\pi)^{-1}$ holds. The eigenstates of the operators turn out to be useful to give momentum and position representations of the field wave functions. In particular, for the wave function corresponding to the lowest energy state of a mode and solution of the equation

$\hat{a}|\psi_0\rangle = 0$

$$\psi_0(q) = \langle q|\psi_0\rangle = \pi^{-\frac{1}{4}} e^{-q^2/2} \tag{6.2}$$

$$\tilde{\psi}_0(p) = \langle p|\psi_0\rangle = \pi^{-\frac{1}{4}} e^{-p^2/2} \tag{6.3}$$

By means of homodyne detection (see below), one collapses the wave functions into some *unpredictable* quadrature eigenstate $|p\rangle$ or $|q\rangle$ (depending on whether momentum of position is measured) relative to the eigenvalues $p$ and $q$. Eigenvalues outcome are random but *do not* have the same probability of being measured. Indeed, by taking the modulus square of the wave functions one obtains that the outcome probability distributions

$$P_0(q) = |\psi_0(q)|^2 = \frac{1}{\sqrt{\pi}} e^{-q^2} \tag{6.4}$$

$$P_0(p) = |\psi_0(q)|^2 = \frac{1}{\sqrt{\pi}} e^{-p^2} \tag{6.5}$$

are Gaussian functions. It is worth stressing that most of the experimental realizable states of the electromagnetic field, e.g. coherent states (displaced vacuum states), thermal states, squeezed states, etc., feature Gaussian probability distribution for their quadrature outcome spectrum. It can be useful to introduce the Wigner functions $W(q,p)$, which correspond to *quasi-probability* distributions in the phase-space. Indeed quadrature probability distributions can be derived as marginal probability distributions of $W(q,p)$. In particular, the vacuum state Wigner function one has

$$W_0(q,p) = {}^1\!/\!_\pi \exp\left(-q^2 - p^2\right) \tag{6.6}$$

such that $P(q) = \int_{-\infty}^{+\infty} dp\, W_0(q,p)$ and $P(p) = \int_{-\infty}^{+\infty} dq\, W_0(q,p)$.

Experimentally quadratures measurement are performed by means of homodyne detection, according the scheme of Figure 6.1. A coherent electromagnetic field, the so called *local oscillator* is mixed with the vacuum field entering from the unused port of a 50/50 beam-splitter. The local oscillator selects then one of the possible modes of the vacuum field. With respect to the single photon DV approach, here the local oscillator is intense such that it can be treated as a classical field with amplitude $\alpha = |\alpha|e^{i\theta}$, playing the role of vacuum fluctuations *amplifier*. The mixed fields exiting from the beamsplitter outputs are intercepted by a couple of large bandwidth photodiodes which generate a current signal $\Delta I$ proportional to the light intensity hitting them. The two currents are respectively subtracted, so that one is left with a signal whose fluctuations are proportional to the quantum fluctuations of the field Fig.**??** and in addition local oscillator noise of classical origin, which would affect both the incoming beams, is in this way eliminated.

In particular, if we label $A$ and $B$ the detectors intercepting the fields at the output arms 3 and 4 respectively, we have that the output current of the setup is proportional to the difference of photons numbers given by the homodyne measurement operator $\hat{\Delta} = \hat{n}_A - \hat{n}_B$, where $\hat{n}_A = \hat{a}_3^\dagger \hat{a}_3$ and $\hat{n}_B = \hat{a}_4^\dagger \hat{a}_4$. By expressing the output operators in

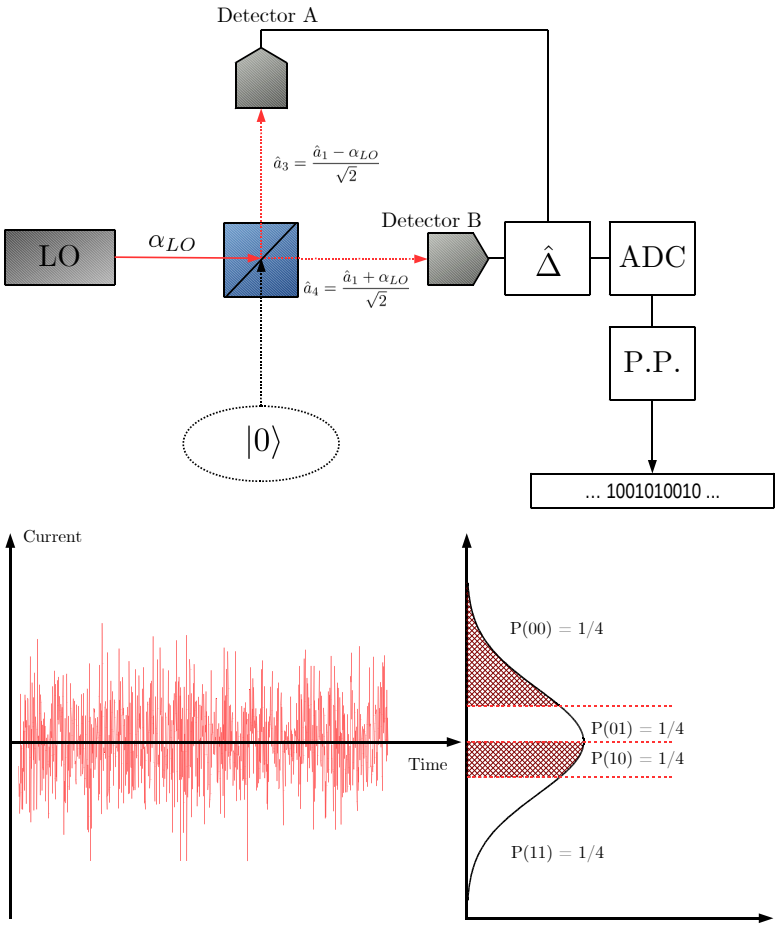


Figure 6.1: **Top:** the basic scheme of a QRNG based on homodyne detection of the vacuum state of the electromagnetic field is represented. **Bottom:** Because the outcome probability of the quadrature measurement is a Gaussian function, outcomes do not feature the same probability of appearance. In order then to make uniform such probability, the range of the possible outcomes is divided into intervals with different lengths in order that the integrated probability is equal.

function of the input ones and considering the local oscillator classically, explicitly one

has

$$\begin{aligned}\hat{\Delta} &= \hat{n}_A - \hat{n}_B \\ &= \frac{1}{2}\left((\alpha^* + \hat{a}_1^\dagger)(\alpha + \hat{a}_1) - (\hat{a}_1^\dagger - \alpha^*)(\hat{a}_1 - \alpha)\right) \\ &= \frac{1}{2}\left((\hat{a}_1^\dagger \alpha) + (\hat{a}_1 \alpha^*)\right) \\ &= \frac{1}{2}|\alpha|\left(\hat{a}_1 e^{i\theta} + \hat{a}_1 e^{-i\theta}\right)\end{aligned} \tag{6.7}$$

At this point it is easy to see that if the local oscillator is in- (out) phase, $\theta = 0$ ($\theta = \pi/2$), with the field entering at input 1 it is possible to measure its $q$ ($p$) quadrature. For example if $\theta = 0$, and the input state at arm 1 is the vacuum, one will get a $\Delta I$ proportional to $\Delta = \sqrt{2}|\alpha|\hat{q}$. Random numbers are then obtained by sampling with an analog-digital converter (ADC) the $\Delta I$ signal. However, since the quadrature values are normally distributed according equation (5.4) or (5.5), it is necessary to make equal the appearance probability of every number. For this purpose, applying techniques from CV-QKD [161], a post-processing algorithm splits in *equal probability* intervals the range of possible current values, as in Fig. 6.1, and then outputs a given number according the interval where the measured current value falls in. This approach for random number generation was presented in [109] and for further details see [162].

## 6.2 The Entropic Uncertainty Principle for Continuous Variables systems

In the following, we will introduce and give a brief presentation of the main theoretical tools necessary to understand the expansion of the EUP protocol to the CV framework. In contrast with the discrete case, the authors of [163] give an algebraic approach required fundamentally by the fact that one is dealing with states having an infinite number of Bosonic modes: the reference objects are not the infinite dimensional Hilbert spaces but the observables and their generated algebras. The main structures are then the Von Neumann algebras $\mathcal{M}$ which can be regarded as *a full set of bounded linear operators on a possibly infinite-dimensional Hilbert space:* $\mathcal{B}(\mathcal{H})$[164].

As in the discrete case, one has a multipartite system formed by three different quantum subsystems $A, B, C$. To every subsystem a von Neumann algebra is associated, i.e. $\mathcal{M}_A, \mathcal{M}_B, \mathcal{M}_C$ acting on the same Hilbert space $\mathcal{H}$ and with $\mathcal{M}_{ABC} = \mathcal{M}_A \vee \mathcal{M}_B \vee \mathcal{M}_C$ the algebra of the composite system. The quantum state of the system is given $\omega_{ABC}$ with $\omega_{ABC} \in \mathcal{M}_{ABC}$. In analogy with the discrete case, classical systems $X, Z$ with continuous degrees of freedom are used to encode the outcomes of the measurements performed on the system $A$. In this framework one operates with continuous classical system, i.e. $X = \mathbb{R}$. In general for a classical system, one introduces a proper parametrization by considering the triplet $(X, \Sigma, \mu)$: $X$ a measure space with $\sigma$-algebra $\Sigma$, and measure $\mu$. Formally then, according to the algebraic characterization, one has that the von Neumann algebra is given by $L^\infty(X)$ (that is the set of the essentially

bounded functions) such that a classical state on $X$ can be represented by the normalized positive and normal functional on $L^\infty(X)$. In particular, a classical state is given by an element of $L^1(X)$ satisfying the condition $\int_X \omega_X(x)\mathrm{d}\mu(x) = 1$, that is a classical state can identified with a probability distribution on $X$.

A key concept of the EUP protocol are the post-measurement state one has after the measurement on the system $A$ and on which the entropies are evaluated. In [163], according to the Heisenberg picture, measurements are regarded as maps on the observable algebra. More specifically one has that a measurement maps $L^\infty(X)$ to a von Neumann algebra $\mathcal{M}_A$, i.e. $E : L^\infty(X) \to \mathcal{M}_A$ and with $\mathrm{Meas}(\mathrm{X}, \mathcal{M}_\mathrm{A})$ one identifies the set of all the measurements $E$. Given a bipartite state $\omega_{AB}$ of a bipartite system $\mathcal{M}_{AB}$, if one measures the system $A$ with a measurement $E_X \in \mathrm{Meas}(\mathrm{X}, \mathcal{M}_\mathrm{A})$ the post-measurement state is given by the composition $\omega_{XB} = \omega_{AB} \circ E_X$. Since $X$ is a classical system and $B$ a quantum one, the post-measurement state is a classical-quantum state, i.e. $\omega_{XB} \in \mathcal{M}_{XB} = L^\infty(X) \vee \mathcal{M}_B \cong L^\infty(X, \mathcal{M}_B)$, with $L^\infty(X, \mathcal{M}_B)$ the space of essentially bounded functions with values in $\mathcal{M}_B$ and which represents the von Neumann algebra for the classical-quantum system. Considering the previous characterization of a classical state, one has that a classical-quantum state on $\mathcal{M}_{XB}$, which can be indicated also by $\omega_{XB} = (\omega_B^x)_{x\in X}$, is given by normal, positive functionals on $L^\infty(X, \mathcal{M}_B)$ and specifically one has that it may be represented with an integrable function on $X$ with values in $\mathcal{M}_B$, i.e. $L^1(X, \mathcal{P}(\mathcal{M}_B))$, which satisfy the condition $\int_X \omega_B^x(\mathbb{1})\mathrm{d}\mu(x) = 1$.

Basically, one has that in a real experiment a measurement on a continuous system can be performed only with the finite precision $\delta$ of the used apparata. In other words, one can performs only a *coarse grained* measurement. Formally, for a fixed $\delta$ one covers the space $X$ with a *partition* $\mathcal{P}_\delta = \{I_\delta^k\}_{k\in\Lambda}$ ($\Lambda$ any countable index set) with $I_k \in \Sigma$ measurable intervals such that $\mu(\mathcal{P}_\delta) = \delta$. A coarse graining corresponds to a family $\{\mathcal{P}_\delta\}_\delta$ of partitions which have an order relation according to $\delta$: in general then, a classical system can parametrized by $(X, \Sigma, \mu, \{\mathcal{P}_\delta\}_\delta)$. In the following, we will consider a given $\delta$ and we will denote as coarse graining the associated partition. Since we are interested in measuring the observables associated to momentum and position of the electromagnetic field, whose classical systems $Q$ and $P$ (the outcome distribution) have range in the real line, we can consider as measure space $Q = P = \mathbb{R}$. Fixed $\delta q$ and $\delta p$ precisions for position and momentum respectively, we set $\mathcal{Q}_{\delta q} = \{I_{\delta q}^k\}_k$ and $\mathcal{P}_{\delta p} = \{J_{\delta p}^k\}_k$. For $Q$ and $P$, coarse graining can be implemented by using half-open intervals $I_{\delta q}^k = (k\delta q, (k+1)\delta q]$ and $J_{\delta p}^k = (k\delta p, (k+1)\delta p]$ with $k$ integer.

As last step, given a measurement $E_X \in \mathrm{Meas}(\mathrm{X}, \mathcal{M}_\mathrm{A})$, we consider its discretized version $E^{\mathcal{P}_\delta} \in \mathrm{Meas}(\mathrm{X}_\mathcal{P}, \mathcal{M}_\mathrm{A})$ (with $X_\mathcal{P}$ is the discretized classical system). In particular for the position and momentum we have $Q^k = E_Q(I_{\delta q}^k)$ and $P^k = E_P(J_{\delta p}^k)$, with $Q^k$ and $P^k$ which element of the POVMs $\{E_Q\}_k$ and $\{E_P\}_k$ respectively. Practically $P^k$ and $Q^k$ correspond to measurements of $q$ and $p$ which project into intervals $I_{\delta q}^k$ and $J_{\delta p}^k$ respectively.

The notions so far introduced, are just a basic framework in order to introduce the EUP for infinite dimensional systems as in [163]. There the principle is demonstrated in two versions, for finite and infinite precision. In particular, the first case is used as

intermediary result to demonstrate the latter in the limit $\delta \to 0$. The EUP in case of finite precision is however the one of interest because accounts for the precision of the instruments. The discretized EUP finds its natural application in protocol of QKD and indeed it was also applied in a experiment of CV-QKD with EPR states [165] of the electromagnetic field.

As in the previous Chapter the scenario has three parties Alice $A$, Bob $B$, and an adversary Eve, $E$, who share a tripartite quantum system $\omega_{ABE}$. The tripartite quantum state shared between the three parties generalizes the case of Alice and Bob which aim to share an entangled state $\omega_{AB}$ to establish a QKD protocol but because of the presence of an eavesdropper, Eve or because the state suffered some decoherence, the state is purified by $\omega_{AB} = \mathrm{Tr}_E[\omega_{ABE}]$. Alice performs POVMs $P^k$ on her part storing the outcomes into the classical system $P(\delta p)$. Alice and Bob then aim to quantify the uncertainty of Eve about the post-measurement state $\omega_{P_{\delta p}E} = \omega_{ABE} \circ P$. This uncertainty can expressed with the conditional min-entropy $H_{\min}(P(\delta p)|E)_\omega$ and it can be bounded by using the entropic uncertainty principle. Indeed if Alice measures an observable of $A$ complementary to previous one, i.e. $Q^k$, and she stores the outcomes in the classical system $Q(\delta q)$, Eve's quantum side information can be estimated by evaluating the max-conditional entropy $H_{\max}(Q(\delta q)|B)_\omega$ on the classical-quantum state $\omega_{Q_{\delta p}B} = \omega_{ABE} \circ B$. The quantity $H_{\max}(Q(\delta q)|B)_\omega$ quantifies indeed the information Alice has to provide Bob to reconstruct $Q$: it is clear that the higher the correlation the less the amount of information required. Therefore Eve's knowledge can be bounded by exploiting the upper bound to the sum of $H_{\min}(P(\delta p)|E)_\omega$ and $H_{\max}(Q(\delta q)|B)_\omega$: the sum must be smaller or equal to a quantity $c(\delta q, \delta p)$ which depends on the degree of observables complementarity and to the precision of the measurements. Practically the entropic uncertainty principle merges together the monogamy of the entanglement and the uncertainty principle for non commuting observables (if Alice and Bob are maximally correlated, for Eve the post-measurement states are completely mixed).

Finally, we state the EUP as in *Corollary 13* of [163] for finite precision measurements of position and momentum:

**Corollary 1.** Let $\mathcal{M}_{ABC} = \mathcal{B}(L^2(\mathbb{R})) \otimes \mathcal{M}_{BC}$ with $\mathcal{M}_{BC}$ a von Neumann algebra, and consider position and momentum measurements with spacing $\delta q > 0$ and $\delta p > 0$ on system $A$. Then, we have that

$$H_{\max}(Q(\delta q)|B)_\omega + H_{\min}(P(\delta p)|C)_\omega \geq -\log c(\delta q, \delta p) \ , \tag{6.8}$$

where $c(\delta q, \delta p)$ is given by

$$c(\delta q, \delta p) = \frac{1}{2\pi} \delta q \delta p \cdot S_0^{(1)}\left(1, \frac{\delta q \delta p}{4}\right)^2 \ . \tag{6.9}$$

with $S^{00}(1, \cdot)$ being the $0^{\text{th}}$ radial prolate spheroidal wavefunction of the first kind.

## 6.3 The EUP protocol for RNG

For what concerns random numbers generation, the tripartite scheme can be adapted by setting trivial the party $B$. Alice has the quantum system $A$, i.e. the electromagnetic field prepared in some given state $\omega_A$ and she wants to measure one of the quadrature in order to extract random numbers. Alice does not trust her system and two possible scenarios are given. In the first one, which is also the most general, untrustedness can be intended as mixedness of the state $\omega_A$, e.g. it has undergone a process of decoherence in the preparation stage (past with respect the space time coordinate of the measurement) and now, is possibly correlated with some other purifying system $E$; in this scenario Alice could have tried to forge the quantum state by herself or she could have been provided of it by a neutral manufacturer. The second scenario is strictly cryptographic: untrustedness corresponds to the case of Eve malicious manufacturer who posses a quantum system $E$ correlated to the QRNG she provides to Alice. In both the cases Alice doubts the purity of her state and she hypothesize that $\omega_A = \mathrm{Tr}_E[\omega_{AE}]$. As in the discrete case then, Alice can use the EUP to estimate a lower bound on the number of true random bits she can extract in the likely presence of quantum side information E. The protocol runs in the following way:

- Alice chooses a quadrature to measure, let say the momentum; according to the precision $\delta_P$ of her measurement apparatus, she fixes a coarse graining $\mathcal{P}_{\delta p} = \{J^k_{\delta p}\}_k$ for the positive operators

$$P^k = \int_{k\delta p}^{(k+1)\delta p} |p\rangle\langle p| dp \tag{6.10}$$

  and consequently for the discrete classical system $P_{\delta_P}$. She applies the measurement to the state $\omega_{AE}$ obtaining the discrete classical outcomes $p_k \in P_{\delta_P}$ with probability $p(p_k) = \mathrm{Tr}[\omega_A P^k]$. These values represent the *raw random numbers* and $\mathcal{P}$ is then denoted as *random basis*;

- Alice chooses an observable maximally complementary of the random basis, i.e. the position; according to the precision $\delta_Q$ of her measurement apparatus, she fixes a coarse graining $\mathcal{Q}_{\delta q} = \{I^k_{\delta q}\}_k$ for the positive operators

$$Q^k = \int_{k\delta q}^{(k+1)\delta q} |q\rangle\langle q| dq \tag{6.11}$$

  and consequently for the discrete classical system $Q_{\delta_Q}$. She applies the measurement to the state $\omega_{AE}$ obtaining the discrete classical outcomes $q_k \in Q_{\delta_Q}$ with probability $p(q_k) = \mathrm{Tr}[\omega_A Q^k]$. These values represent the *check numbers* because they are employed to check the purity of the state $\omega_A$ and $\mathcal{Q}$ is then denoted as *check basis*;

- Alice lower bounds the number of true random bits achievable per measurements by using

$$H_{\min}(P_{\delta_P}|E)_\omega \geq -\log \frac{1}{2\pi}\delta q\delta p \cdot S_0^{(1)}\left(1, \frac{\delta q\delta p}{4}\right)^2 - H_{\max}(Q_{\delta_Q})_\omega \tag{6.12}$$

  where the $H_{\max}(Q)_\omega$, equivalent to the Renyi entropy of order 1/2, and for the CV-discretized takes the form of

$$H_{\max}(Q_{\delta_Q}) = 2\log_2 \sum_{l=-\infty}^{\infty} \sqrt{\int_{l\delta x}^{(l+1)\delta q} dq|\omega_A|^2}\ . \tag{6.13}$$

The idea of the protocol is reported in Figure 6.3: the state measured by Alice corresponds to the vacuum state of the electromagnetic field whose Wigner function is reported. Measuring the position and momentum quadratures with precisions $\delta_P$ and $\delta_Q$ respectively, the two discretized probability distribution $P_{\delta_P}$ and $Q_{\delta_Q}$ are obtained. From the Figure one can better understand that the measurements in the $\mathcal{Q}$ basis are necessary to check if the state one is measuring is the one which was supposedly prepared. The estimation of $H_{\min}(P|E)$ is a more adequate measurement of the actual content of randomness than the Shannon classical min-entopy. But in addition to that, it is worth stressing that the EUP can be considered as an universal measure of randomness for the generator. Indeed with respect to the discrete case where the EUP accounts only for the distance between a pure and a mixed state, in the CV framework the EUP accounts also for the finite resolution of the measurement.

This can be appreciated in Figure 6.3, where the minimal amount of true random bits extractable from a pure coherent state are plotted as function of the quadrature measurement precision $\delta$ and estimated according the classical min-entropy $H_\infty(P)$ (red line) and the quantum conditional min-entropy $H_{\min}(P|E)$ (green line). Contrary to the discrete case where one has equivalence between these two quantities, in the CV discretized framework the same correspondence can be reached only by increasing the precision. Otherwise, as one can see from the inset, for low precision $H_\infty(P)$ gives a higher estimation of the real content of entropy associated to a measurement. It is worth noting that the additional bits corresponding to the red shaded area, come from a systematic uncertainty due to a measurement operator taken on a interval too wide. Indeed the quantum state cannot be discriminate with enough resolution to make possible to understand whether the measured distribution belongs to the expected state or to something else. In particular, for $\delta^{-1} \to 0$ one has that $H_\infty(P) = 1$ because only two intervals are left $I_0 = (-\infty, 0]$ and $I_1 = (0, \infty)$ so for a symmetric gaussian state one has the two outcomes probability both equal to 1/2.

Otherwise if Alice holds a mixed state, i.e. a thermal one, the conditional min-entropy does not reach the level of the Shannon entropy also in the infinite precision limit.

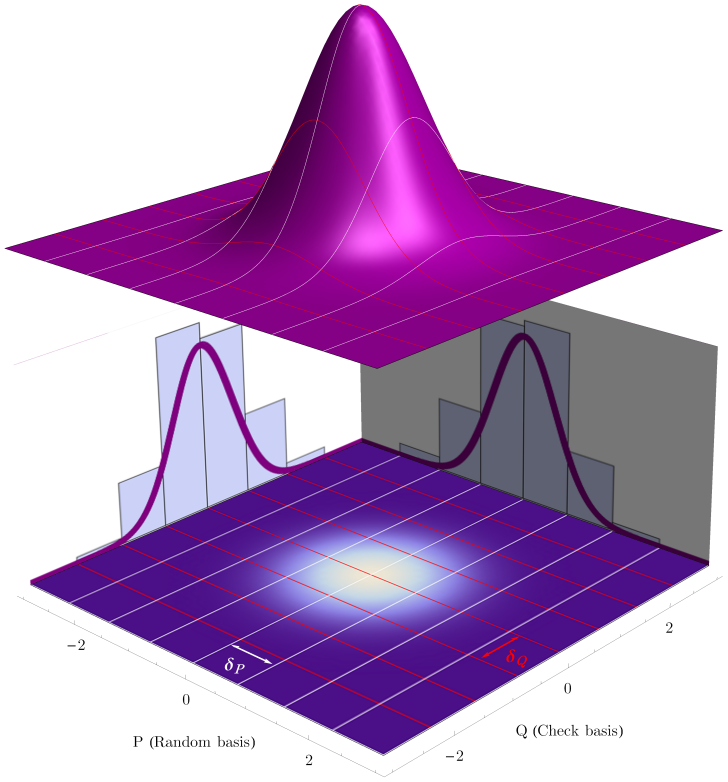


Figure 6.2: The image represents how the protocol for the CV is intended: the top plot represent the Wigner probability density function for the vacuum state. Position and momentum are measured with precision $\delta_q$ and $\delta_p$ respectively. The outcomes of the momentum measurement are employed for the number generation, while the outcomes of the position are used to check the purity of the state.

### 6.3.1 Input: squeezed vacuum state

The interplay between a faithful estimation of the true extractable random bits and the precision of measurements can be made more clear with *squeezed states*. The wavefunction of a squeezed vacuum state in position and momentum representation are given by

$$|\psi_{\text{sq}}(q)\rangle = \frac{e^{\frac{1}{2}(\zeta - e^{2\zeta}q^2)}}{\sqrt[4]{\pi}} \qquad |\psi_{\text{sq}}(p)\rangle = \frac{e^{\frac{1}{2}(\zeta - e^{-2\zeta}p^2)}}{\sqrt[4]{\pi}\sqrt{e^{2\zeta}}} \tag{6.14}$$

and a Wigner distribution

$$W_{\text{sque}}(q,p) = \frac{e^{-e^{-2\zeta}p^2 - e^{2\zeta}q^2}}{\pi} \tag{6.15}$$

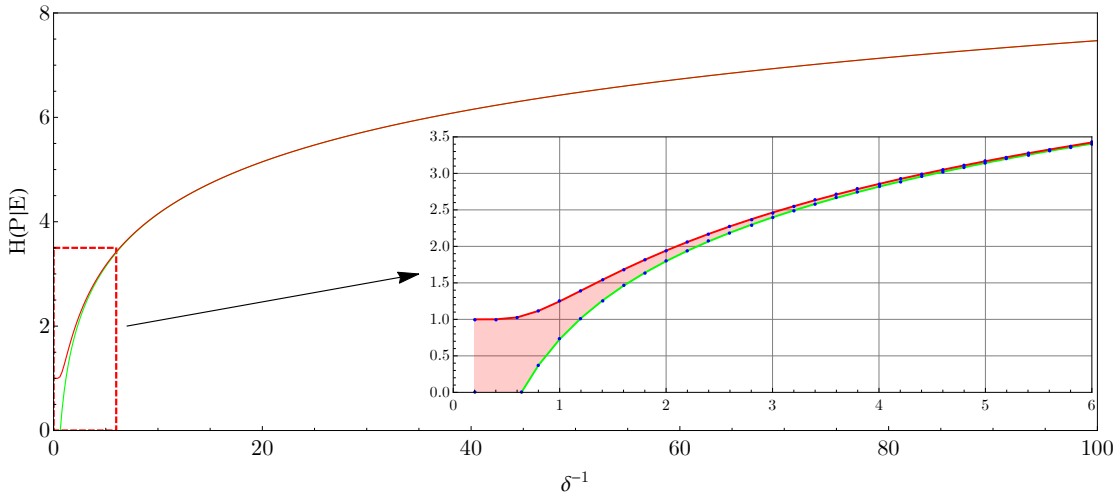


Figure 6.3: In the plot the green line represents the min-conditional entropy, $H_{\min}(P|E)$, while the red one is the min-classical entropy, $H_{\infty}(P)$, evaluated for a pure vacuum state. When the precision of the measurement increases $\delta^{-1} \to \infty$, one has both the estimators attain in the same value. However, for $\delta^{-1} \to 0$ classical min-entropy becomes a not reliable entropy quantifier. Indeed the quantum state cannot be discriminate with enough resolution to make possible to understand whether the measured distribution belongs to the expected state or to something else. Accordingly $H_{\min}(P|E)$ for low precision is not meaningful.

The parameter $\zeta$ is the degree of squeezing: in Figure 6.3.1 $W_{\text{sque}}(q,p)$ is reported for $\zeta = 1/2$, with the position quadrature squeezed $\sigma_q^2 = \frac{e^{-2\zeta}}{2} < \frac{1}{2}$ and the momentum quadrature anti-squeezed $\sigma_p^2 = \frac{e^{2\zeta}}{2} > \frac{1}{2}$, such that the product of the uncertainty is anyway $\sigma_q^2\sigma_p^2 \geq \frac{1}{4}$. In particular one has that for $\zeta = 0$ we have again the vacuum state.

If this state is employed to generate random numbers, the optimal choice would be to sample the anti-squeezed basis because one has a broader spectrum with outcome probabilities higher with respect to the squeezed one. Therefore, for the following example the check basis is the position, instead the random numbers are obtained from the momentum. On this regard, in Figure 6.3.1 the dependence of the number of true bits extractable as a function of the degree of squeezing $\zeta$ (left) and of the precision $\delta^{-1}$ (right) are reported. In the left plot we arbitrarily fixed the precision $\delta_Q^{-1} = \delta_P^{-1}$ equal to 2 and 5 respectively: the green and the red blue representing $H_{\min}(P_{\delta_P}|E)$, while the red and the purple representing the classical min-entropy $H_{\min}(P_{\delta_P})$. One sees that for $\zeta$ increasing, both classical and conditional entropies increase. However the classical min-entropy, evaluated on the position, continues to increase with respect to the conditional one which instead reaches an asymptotic constant value. The reason for this behavior is that the higher the squeezing, the better the squeezed quadrature fits into the precision interval $\delta_Q$: when the state is inside just one bin the maximal information extractable

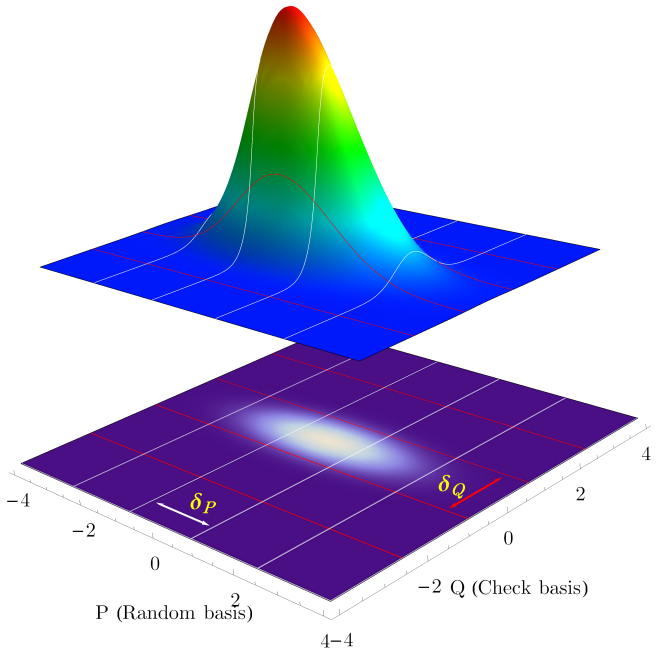


Figure 6.4: The Wigner function of a squeezed vacuum state with $\zeta = 1/2$. In particular one has that the higher the degree of squeezing the better the state fit inside an interval for a given precision, e.g. $\delta_Q$. Correspondingly the state becomes anti-squeezed on the other basis such that more random numbers can be generated.

with that precision is reached. The classical min entropy increases correspondingly because the antisqueezed quadrature becomes wider and then more number have a larger outcome probability.

On the right plot instead, one can compare the estimation for a vacuum state and a squeezed one with $\zeta = 1/2$ as function of the precision. For what concerns the dependence on the precision, the same considerations of the previous Section are valid. In this case however from a squeezed vacuum a higher number of bits can be extracted being wider than the simple one.

### 6.3.2 Input: thermal state

A single mode of the field at thermal equilibrium at temperature $T$, has mean number of photons $\langle n \rangle = \frac{1}{e^{\hbar\omega/k_B T}-1}$ being $\hbar\omega$ the energy of the mode and $k_B$ the Boltzmann constant, and the density matrix of the field $\rho_{\text{therm}}$ featuring a Bose-Einstein distribution of the photon numbers

$$\rho_{\text{therm}} = \left(\frac{1}{1+\langle n \rangle}\right) \sum_{n=0}^{\infty} \left(\frac{\langle n \rangle}{1+\langle n \rangle}\right)^n |n\rangle\langle n| \,. \tag{6.16}$$

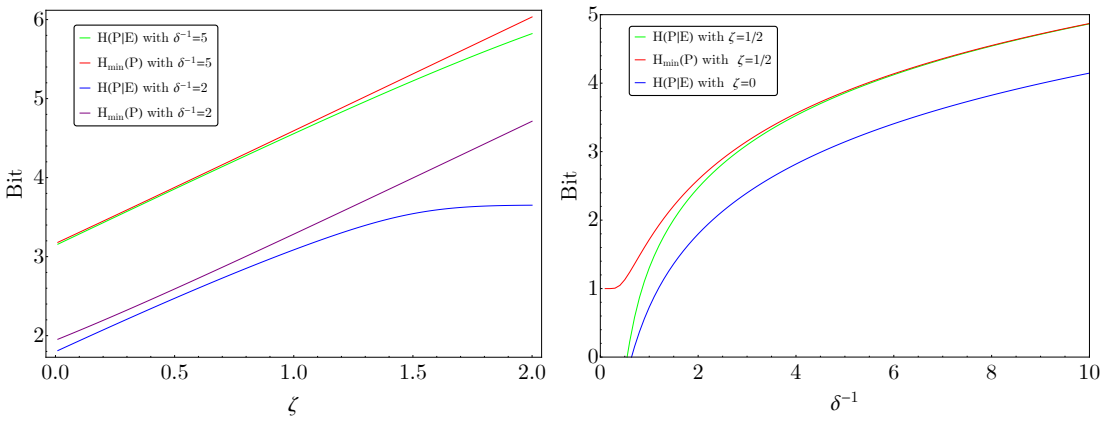


Figure 6.5: On the right plot the min conditional and classical entropies are reported as function of the degree of squeezing for two differnt precisions. On the right plot, $H_{\min}(P)$ (red line) and $H_{\min}(P|E)$ (green line) are reported as function of the precision for a squeezed vacuum state with $\zeta = 1/2$. The blue line is the conditional min-entropy for a vacuum state

The corresponding Wigner function is given by

$$W_{\text{therm}}(q,p) = \frac{1}{\pi(2\langle n\rangle + 1)} e^{-\frac{q^2+p^2}{2\langle n\rangle+1}} \tag{6.17}$$

this function is still a Gaussian with a null average value for the position and momentum but with variance $\sigma_P^2 = \sigma_Q^2 = \frac{1}{2} + \langle n\rangle$. A thermal state is practically a vacuum state with a larger variance. The degree of mixedness is indeed related to the average number of photons excited by the temperature. Therefore, given a thermal state the number of extractable true random bits, will be always lower with respect to the quantity which can extracted by a pure state, *also if the resolution is increased*. This can be appreciated in Figure 6.3.2: on the left $H_{\min}(P_{\delta_P}|E)$ is plotted as a function of the measurement precision $\delta_Q$ for a thermal state with $\langle n\rangle = 2$. Differently from the vacuum state, one can notice how the classical min-entropy overestimates the real amount of randomness for any value of the precision. On the right plot, the min-conditional entropy is reported as function of the $\langle n\rangle$, for a fixed precision $\delta_Q^{-1} = 10$: the two entropy estimators reach the same value (cfr. Figure 6.3) only for $\langle n\rangle = 0$, as indeed expected for a pure vacuum state. These results are relevant because, like in the discrete case of the previous Chapter, one has that min-classical entropy does not account for possible side information.

### The case of a malicious provider

In a hypothetical scenario, a malicious Eve, could provide Alice with a QRNG featuring an engineered source of quantum states from which she can extract side information. Eve could implement her evil plan by preparing a *two mode squeezed vacuum state*. This

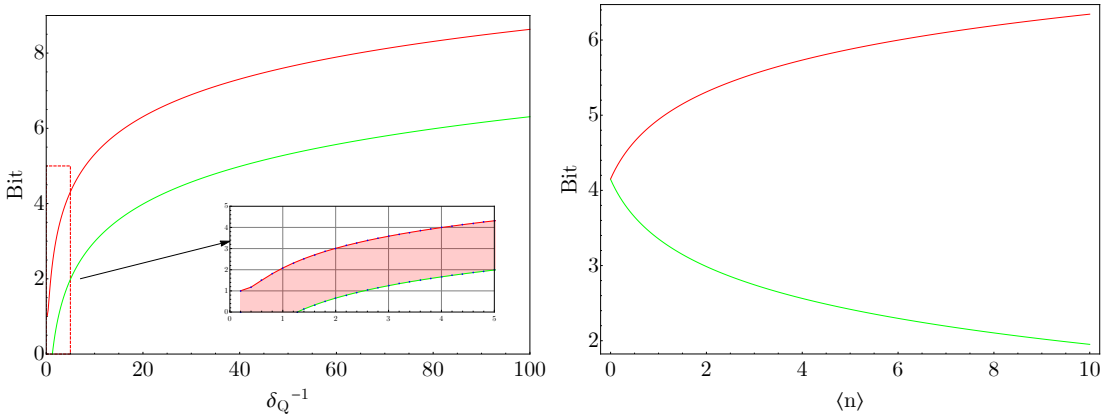


Figure 6.6: $H_{\min}(P)$ (red line) and $H_{\min}(P|E)$ (green line) are reported as function of the precision (left plot) and of the the mean number of photons of the thermal state (right plot).

state is an approximate optical version of an EPR state: it is achieved by interfering two squeezed vacuum states on a beam splitter as in Figure 6.3.2, where a beam is squeezed in $P$ and the other in $Q$. In particular one has that the Wigner function of the system is given by

$$W(q_1, q_2, p_1, p_2) = \frac{1}{\pi^2} \exp\left(-\frac{(p_1 - p_2)^2}{2\exp(2\zeta)} - \frac{(p_1 + p_2)^2}{2\exp(-2\zeta)}\right) \exp\left(-\frac{(q_1 - q_2)^2}{2\exp(-2\zeta)} - \frac{(q_1 + q_2)^2}{2\exp(2\zeta)}\right) \tag{6.18}$$

where the subscripts 1 and 2 refer to the two parties and $\zeta$ is the degree of squeezing. Eve engineers the source in order that beam 1 is sent to her while Alice has to measure beam 2.

This well known CV-QKD scheme works on the principle that the measurements performed on each pair of the entangled system give (anti-) correlated outputs with high probabilities. Eve is aware that by tracing out one of the system, Alice is left with a thermal state $\rho_{\text{Alice}}$ whose Wigner function is

$$W_{\text{Alice}}(q_2, p_2) = \frac{\exp(-\left(p_2^2 + q_2^2\right)\operatorname{sech}(2\zeta))}{\pi\sqrt{\cosh^2(2\zeta)}}\ . \tag{6.19}$$

When Alice projects, for example, in the P basis to extract the random numbers, she

obtains an outcome probability distribution given by

$$\begin{aligned} \mathrm{pr}(\mathrm{p}_2) &= \mathrm{tr}\left\{|\mathrm{p}_2\rangle\langle \mathrm{p}_2|\rho_{\mathrm{Alice}}\right\} && (6.20)\\ &= \int_{-\infty}^{\infty} W_{\mathrm{Alice}}(\mathrm{q}_2,\mathrm{p}_2)d\mathrm{q}_2 && (6.21)\\ &= \frac{\sqrt{\mathrm{sech}(2\zeta)}\exp\left(-\mathrm{p}_2^2\,\mathrm{sech}(2\zeta)\right)}{\sqrt{\pi}}\ . \end{aligned}$$

One can easily check that $\mathrm{pr}(\mathrm{p}_2)$ is equivalent to the outcome distribution one would get by measuring in the anti-squeezed basis a vacuum state squeezed by a factor

$$\zeta' = -\frac{1}{2}\log(\mathrm{sech}(2\zeta))\ . \tag{6.22}$$

To recap then, Eve prepares an EPR state with a pair of $\zeta = 0.5$ squeezed vacuums but tells to Alice that the QRNG generates random numbers by measuring in the P basis a vacuum state squeezed with $\zeta' = 0.217$ in the Q quadrature. Alice obtains a probability distribution which is the same she expects and she evaluates the classical min-entropy $H_{\min}(P)$. In Figure 6.3.2 (Left) the estimation of $H_{\min}(P)$ and of the min-conditional entropy $H_{\min}(P|E)$ is reported as function of the measurements precision inverse $\delta^{-1}$. As expected the classical min-entropy over-estimates the amount of bits that can be

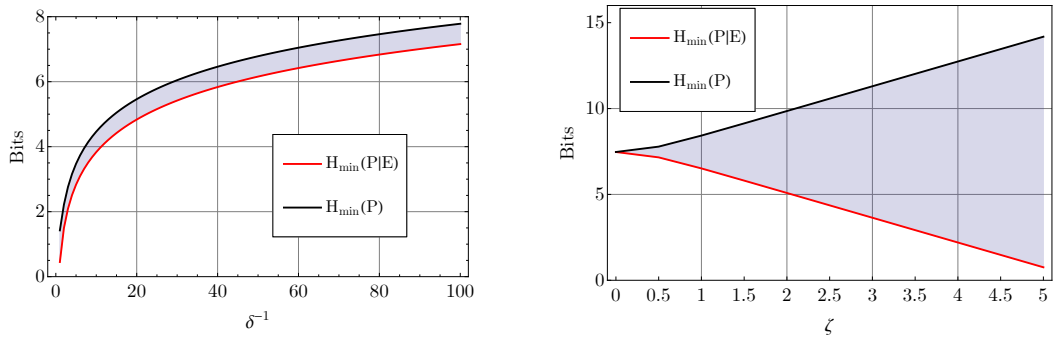


Figure 6.7: $H_{\min}(P)$ (black line) and $H_{\min}(P|E)$ (red line) are reported as function of the precision (left plot) and of the degree of squeezing (right plot).

extracted and in particular one can see that Eve holds an amount of correlated bits which asymptotically reach the value of $\Delta_H = 0.6258$ bits. It is worth to point out that for an approximate EPR state, the higher the squeezing the stronger the level of correlation between the two beams: in Figure 6.3.2 $H_{\min}(P)$ and $H_{\min}(P|E)$ are plotted as function of the squeezing for a fixed precision: by increasing $\zeta$ Eve gains more information about Alice system and the conditional min-entropy accordingly decreases, while the classical min entropy increases, giving clearly a wrong estimation of the true content of random bits.

### 6.3.3 EUP as a model to comprehend the technical noise of a QRNG

The issue of the precision and the consequent discretization of the measurements are related to the practical implementation of the protocol in real life. Another fundamental point however lies in the fact that, in a real life homodyne measurement, the process of allocating a given quadrature outcome $p$ or $q$ into a specific discrete interval, is the final result of a long signal processing chain. In theory, at end of this chain, one should have currents $i_P$ and $i_Q$ featuring variances $\sigma^2_{i_P}$ and $\sigma^2_{i_Q}$ proportional to the measured quadrature variance and to the intensity of the local oscillator. The currents then are measured with the finite precision of a sampler and the outcome probability distributions are formed. Actually, at every stage of the chain, unavoidable technical noise due to the non-ideality of the experimental devices, leaks inside the quantum signal. The main sources of noise are the local oscillator intensity noise $i_{LO_{noise}}$, the detector dark noise $i_{D_{dark}}$, detector thermal noise $i_{D_{th}}$, detector's classical noise $i_{D_{cl}}$, sampler noise $i_{ADC}$. As we will show in the next Section, in the realization of a QRNG, one can choose devices and experimental conditions which minimize the impact of the noise. However the problem is that, also if one one were able to individuate all the possible noise sources, it would not be possible to eliminate their contribution from the random and check signals, being these noises intrinsic to the devices themselves[1]. The fluctuations of the noise currents add in quadrature to the original quantum signal, therefore at the end of the chain one measures the variance $\sigma'^2_{i_P} = \sigma^2_{i_P} + \sigma^2 i_{D_{dark}} + \sigma^2_{i_{D_{th}}} + \sigma^2_{i_{D_{cl}}} + \sigma^2_{i_{ADC}} + \dots$ . Since most of these electronic noises do not depend on the local oscillator power or they scale differently with respect to $\sigma^2_{i_P}$ ($\sigma^2_{i_Q}$), one could think to increase the intensity in order to maximize the SNR: this would help partially because detectors can sustain only a given amount of power, usually not so high to make negligible the impact of the electronic noise. At this point, it appears clear that the neat effect of the technical noise is to increase the value of the measured variance. The result is then a wider probability distribution as if we were measuring a *thermal state*. Practically also if the state is pure, the measured outcome probability distribution results wider. For an effective implementation of the EUP protocol we put forward the following model for a real QRNG. **Model:** because the several noise factors can not be distinguished in the measured outcome probability distribution and also if it was possible to discriminate them, anyway they could not be eliminated, we model a QRNG as if the measurement part is *ideal* and the quantum state is *mixed*. In this model the flaws of the measurement apparatus are adsorbed into the input state which is made "more mixed" with respect to the input one (which could be also pure in absence of quantum side information). Within this model, the EUP can be efficiently applied to account also for the technical noise which represents a source of accidental randomness, i.e. randomness due to the ignorance about the degree of freedom involved in the system. This is relevant because also the classical noise could be exploited by an eavesdropper as a source of side information. Notably, our assumption automatically puts Eve in control of an unprecedented set of resources, both classical

[1]The homodyne configuration indeed, by taking the difference of the two light signals, can get rid only of the noise *common* to both the signals)

and quantum that she can take advantage of to predict the outcome of the generator. In both the cases with the EUP protocol one can distil true quantum bits.

## 6.4 Experimental realization

An experiment was set up in order to give a concept proof of the protocol and to demonstrate the applicability of the method for a QRNG assembled by using off-the-shelves and commercially available devices. This approach might fit a scenario where QRNGs are compact devices of common use, manufactured on industrial scale with a possibility of optimization far more limited than the one achievable in a laboratory. Indeed a continuous calibration of the optical parts would be out of reach and the generator would be unavoidably affected by the aging of the components. With the model introduced in the previous Section, our protocol becomes relevant in order to minimize the impact of classical noise contaminating the system and to *filter* the quantum randomness left. It is worth to stress that said scenario could represent a case with a trusted manufacturer Eve who directly manufactures generators which embed the EUP. Otherwise, from another perspective, our experiment could also represent a case where Alice does not trust Eve and then she opens the device in order to check whether the amount of true quantum entropy is the one claimed by Eve. For the experiment we then implemented the classical scheme of vacuum homodyne presented in the introduction of this Chapter with the addition of the estimation of the min-conditional entropy. In this proof of principle, a random subsamples of the measurements was extracted to represent the measurements in the check basis, as if the phase of the Local oscillator was increased of $\frac{\pi}{2}$. The the validity of this approach lies in the fact that a vacuum state is still Gaussian also after a process of decoherence.

In practical terms, since we were in the position to safely exclude the action of an eavesdropper, the method adopted for this experiment was completely equivalent to the random switching between the bases. The setup for the generator is reported in Figure 6.4 and as one can notice a full-fiber scheme was preferred to a free-space one. This choice was motivated by two facts: the first one is that fibers are more functional in the perspective of embedding the generator in a compact device; the second fact is the availability, in the field of coherent communications, of very wide band fiber coupled balanced detectors which represent promising candidate to expand in the future the generation rate to the range of Terabit/s.

### The local oscillator

As local oscillator was individuated a single mode fiber coupled laser diode **Covega - Single Frequency Laser (SFL) 1550S** with a nominal of $\lambda = 1549.8\ nm$ and a maximal output power of $50\,mW$. This laser was selected on the basis of its ultra-narrow spectrum of about 0.5 $nm$, cfr. Figure 6.4-Left, which is a relevant feature under a theoretical point of view, because it limits the number of modes involved in the generation. The laser diode has a standard 14 pins butterfly packaging, so it was mounted

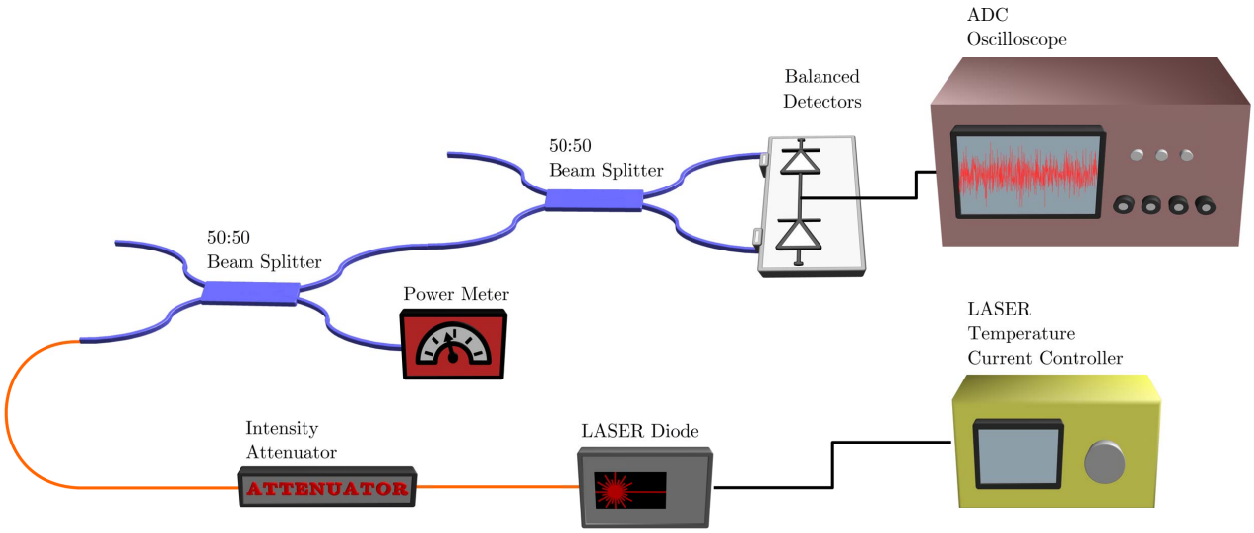


Figure 6.8: The experimental setup used to test the entropic uncertainty principle in the continuous variable framework is reported. The generator was realized using all off the shelves devices and all fiber-coupled. Using fibers, the generator takes a plug-and-play configuration which eases the tuning of the setup.

into a socket **LM14S2** driven by a **Thorlabs ITC4001** laser driver which controlled both current and temperature in feedback. Setting up this configuration was necessary in order to guarantee a fine tuning of the lasing current and of the diode temperature. Indeed, the laser operation is strictly dependent on these two parameters: on this regard in Figure 6.4-Right a plot of the cavity side modes suppression ratio (SMSR) as function of the injected current for fixed temperature, $T = 24\,C$ is reported. In order to minimize the leaking of sides modes into the main one, the best operating zone is approximately in the range $210 - 250\,mA$ where one can achieve a suppression of $52\,dB$ at $228.5\,mA$ and it corresponds also to the linewidth reported on the Figure 6.4-Left. Practically, one has several operating zone where single mode regime is granted depending on the current and temperature. The driver was then set to feed the diode with a current of $228.5\,mA$ corresponding to an output power of approximately $31\,mW$. The controller was also set keep fixed the diode temperature to $24\,C$ in order to contrast the rapid heating of the laser. It is worth to stress that to cool-off the device was necessary to avoid the regime of multi-mode oscillation rather than to prevent damaging: e.g. one has that an increase of 1 degree $C$, requires the current to be raised to $245\,mA$ (7.5%)to re-establish the single mode operation.

Following the setup scheme, the APC fiber output of the laser is connected to a **Thorlabs VOA50-APC** single mode fiber broadband variable attenuator. This device is essential in order downscale the power reaching the balanced receiver because in the laser single mode operating zone, the output power is a factor thee larger than its damage threshold power. The laser power was then kept fixed, while the one to the detectors

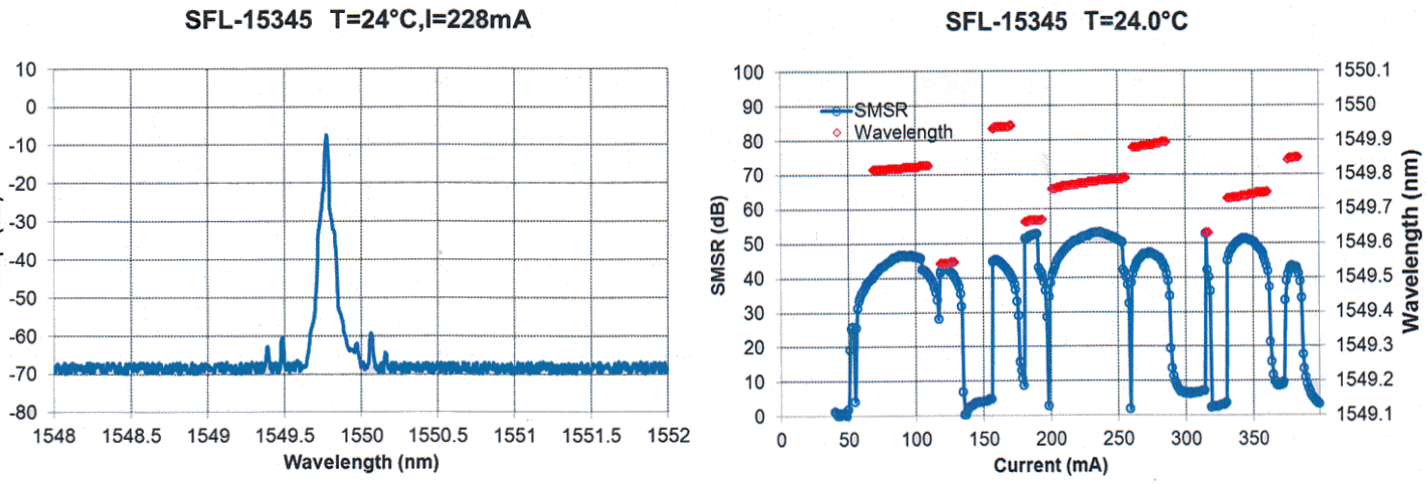


Figure 6.9: LEFT: The measured spectrum for the local oscillator. The lasing line is centered at $\lambda = 1549.8\ nm$, with a FWHM of about $0.5nm$. RIGHT: For a temperature of 24 C, the side modes suppression ratio (SMSR) and the $\lambda$ is plotted in function of the diode current. The operating zone chosen for the experiment was at 210 mA

was adjusted by operating a screw of the attenuator. Basically in a cage at the middle of the head fiber, the beam is sent in free air through a window connected to a screw which varies the coupling efficiency with the tail fiber connected to the other end of the cage. By means of this device it was possible to adjust easily the power in steps of 0.5 mW for the study of the linear response of the receiver.

The output of the attenuator was connected to an fiber beamsplitter APC **Thorlabs** with a splitting ratio of 50:50. One output was sent to a power meter for the constant monitoring of the laser power, while the other to one input of an identical beam-splitter where formally the local oscillator was mixed with the vacuum entering the unused input. Both the output were coupled with the APC input of a balanced receiver.

### 6.4.1 The photodiodes

The second main component of the optical part is the balanced receiver to which the beamsplitter output were connected. In line with the off-the-shelves paradigm, a **Thorlabs PDB480C-AC** with a nominal bandwidth of $B = 1.6\,GHz$ was selected. The first advantage of this device lies in the fact that both the photo-detectors, a couple InGaAs PINs, and the amplifiers are included in a single self-contained packaging. This monolithic configuration helps consistently to reduce the coupling with environmental electromagnetic noise. The noise performances indeed and the bandwidth were the technical parameters considered in the process of selection of this device. Generally, in an experiment of photon detection the sources of signal fluctuations are represented by

- THERMAL NOISE CURRENT: $i_{Th} = \sqrt{\frac{1}{R} 4 k_B T B}$ with $T$ temperature and $R$ load resistor connected to the photodiode;
- DARK CURRENTS SHOT NOISE: $i_{SD} = \sqrt{2 e i_D B}$ with the $i_D$ the level of dark currents.

How these two factors can be detrimental to the measurements, can be understood by considering that, in vacuum homodyne, our main signal practically corresponds to the shot-noise intrinsic to the process of photo-detection. Indeed, this scheme corresponds to the so-called *intensity noise eater* configuration, because it *eats* off any classical spurious noise affecting the LO, leaving only the noise which is not common to both the signals. However, thermal and dark current noise are a sort of intrinsic noise of the two PIN and so they do not cancels out by taking the difference of the signal. Because these two noises are adds in quadrature to the quantum noise, it is of fundamental importance to select a receiver with a low noise fingerprint in order to get a high SNR.

Another pivotal feature of the receiver is its efficiency in getting rid of the modes which are common to both the arms of the detector. For a measurement involving quantum noise, it is necessary that the diodes are highly matched in responsivity: the more the diodes respond similarly, the smaller will be the amplitude difference of a common signal. In particular this characteristic turns out to be useful when the LO is affected by some spurious oscillation which would interfere in the measure of the quantum noise. Our receiver features a common mode rejection ratio (CMRR) of over $30\,dB$, cfr. Figure 6.4.1, in line with the performances of other receivers used in Literature for CV-QRNG.

The final stage of the setup consisted of an oscilloscope **Tektronix TDS6124C** featuring a bandwidth of 20 GHz and a maximum sampling rate of 40 GS/s which was used as ADC. The oscilloscope was remotely controlled with a personal computer for the logging of the waveforms which later analyzed to get the raw random numbers and the check basis numbers to apply the EUP protocol.

### 6.4.2 Data pre-processing

In the following we will present the pre-digital processing we applied on the waveforms acquired with the oscilloscope in order to get the raw random numbers. Indeed, although the receiver has a bandwidth of 1.6 GHz, not the whole measured quadrature spectrum is optimal to generate raw random numbers because of the presence of technical electronic noise. The aim of the processing was then to select the so called quantum noise limited region of spectrum.

When the diode difference signal is sampled, one expects to observe a flat power spectral density (PSD) due to the infinite band of the vacuum shot noise, at most limited by the cut-off frequency of the receiver or of the ADC sampler. However, an actual spectrum presents a more elaborated structure with artifacts which are originated by the physical limitations of the laser and the detectors themselves. More specifically one can identify at least three regions:

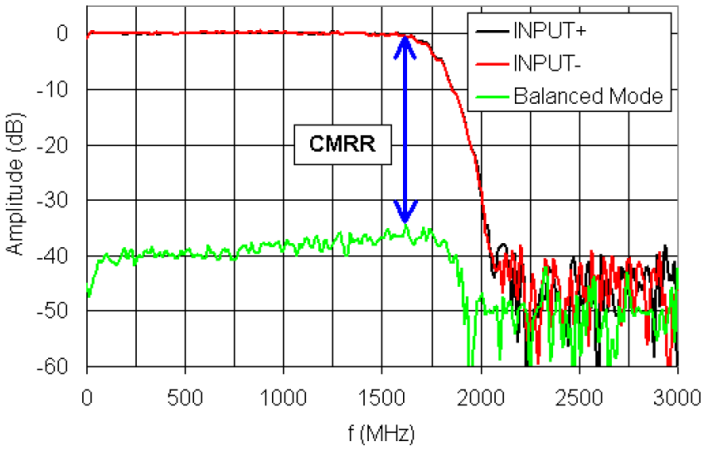


Figure 6.10: For a measurement involving quantum noise, the better the PINs are matched in quantum efficiency and responsivity, the more balanced is the receiver. The ability of eliminating common modes is fundamental in order to achieve the intensity eater configuration, when one is left (mostly) only with quantum noise. The plot show the typical common mode rejection ratio which is over 30 dB.

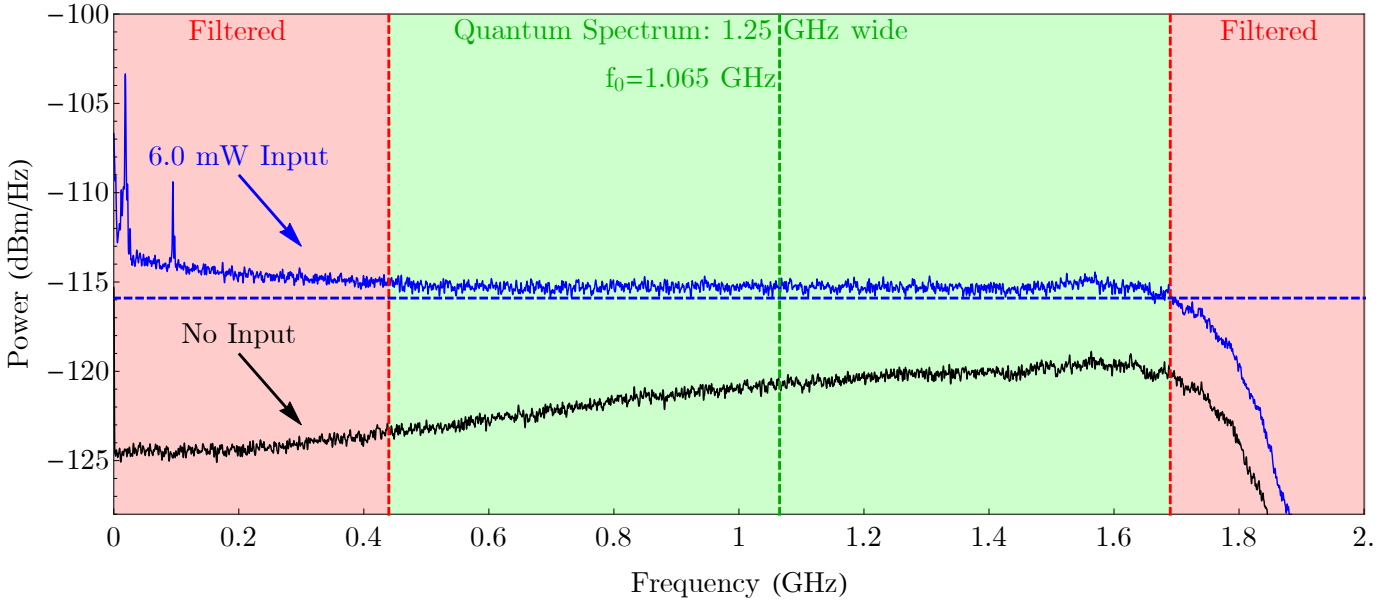


Figure 6.11: The power spectral density function of the signals with no input (black line) and with a LO power of 6 mW (blue line) is reported. The green shaded region identifies the 1.250 GHz wide region of the spectrum which was considered for the extraction of the raw random numbers. The signal has been downmixed with a sinusoidal carrier with frequency $f_0 = 1.065$ GHz and then it was filtered with a low-pass filter with 625 MHz cut off frequency.

- a region with several frequency peaks which is confined in the inferior part of the spectrum
- a middle flat region
- a region of decreasing power in the terminal region of the spectrum.

The first region is a combination of the finite common mode rejection ratio of the detector and the presence of relative intensity noise (RIN) of the laser. In Figure 6.4.2, the typical PSD of the receiver output signal is reported. In particular the PSD for no input (black trace) and an input of 6.0 mW (blue trace) is reported. Both the waveforms were sampled at a rate of 10 GS/s. In order to filter out those regions of the spectrum which were clearly affected by technical noise, we performed the digital equivalent of an analog down-mixing and low-pass filtering. This is the principle at the basis of heterodyne and it is a basic procedure in the field radio frequency (RF) processing. It consists in mixing a target signal $x(t)$ with a sinusoidal carrier with a given frequency $f_0$: the mixed signal $x'(t)$ it is just a copy of the original signal but with the all the frequency components downshifted of $-f_0$, i.e. the frequency $f_0$ of the original signal corresponds to the zero frequency of $x'(t)$. In our case, we considered a flat region 1.250 GHz wide, where we found the optimal central frequency be at $f_0 = 1.065$ GHz. The process of filtering consisted in retaining the $625MHz$ sideband frequency spectrum applying a kind of sharp low-pass filter which set to zero all the higher frequency components.

At this point the signal was not yet useful for number extraction because the sampling rate was a factor 3.125 the Nyquist frequency (assuming a bandlimited signal at 1.6 GHz). Oversampling indeed was a necessary condition to get a faithful reconstruction of the physical signal for the digital processing however, in this way, one is left with a filtered signal which is highly self-correlated. This can be understood considering that if the signal is sampled faster than the intrinsic time scale of the process (roughly the inverse of the receiver bandwidth), one gets that consecutive samples show similar values (typically, decreasing or increasing runs of values). The acquired signals need to be properly downsampled, in order to obtain a raw random uncorrelated signal. More formally, given $x(t)$ a stationary signal, i.e. a signal whose mean value $\mu = \langle x(t) \rangle$ and variance $\sigma = \langle (x(t) - \mu)^2 \rangle$ does not change in time, the autocorrelation depends only on the difference $\tau = t_2 - t_1$ between two times $t_2$ and $t_1$, that is

$$R(\tau) = \frac{\langle (x(0) - \mu)\,(x(\tau) - \mu) \rangle}{\sigma^2}\,; \tag{6.23}$$

in our case the time interval $\tau$ is a multiple of the sampling interval $T_s = {}^1/_{f_S} = 10^{-10}$ s i.e. $\tau(n) = nT_s$ with $n \in \{0, 1, ..., L\}$ and $L$ the last sample of an acquired waveform. Very basically, because $T_s$ is a fixed variable, one can directly evaluate the autocorrelation as function of $n$, i.e.

$$R(n) = \frac{\langle (x(0) - \mu)\,(x(n) - \mu) \rangle}{\sigma^2}\,, \tag{6.24}$$

which measures then the degree of correlation between the samples separated by $n$ time intervals.

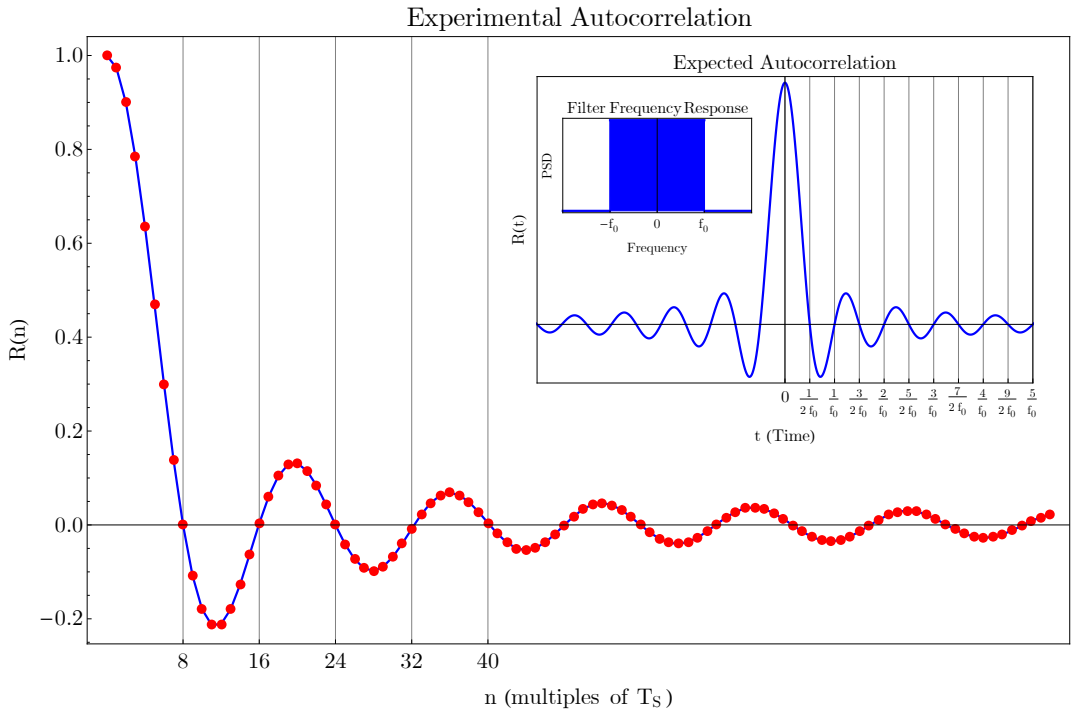


Figure 6.12: The plot reports the experimenatl autocorrelation of the filtered data as function of the temporal separation in multiple of the sampling interval $T_S$. The correlation is modulated according a sinc function. This is indeed the expected behavior once that a signal is filtered by a low pass filter, top inset. By means of the Wiener-Kitchine theorem one can analytically calculate the zeros of the autocorrelation and then the corresponding down sampling frequency in order to achieve a null self-correlation.

The typical dependence of $R(n)$ by $n$ for the acquired waveforms is reported in Figure 6.4.2: one has that the measured autocorrelation values are distributed according a *sinc* function ($\mathrm{sinc}(x) = {}^{sin(x)}/_{x}$), a damped sinusoidal for $n$ increasing, with the expected maximum $R(0) = 1$ (correlation of the samples with themselves). Such a behavior for $R(n)$ was not surprising but perfectly in line with the fact that the signal is filtered with an ideal low-pass filter whose PSD is given

$$P_{\mathrm{LP}(f)} = \begin{array}{ll} \frac{1}{2\pi f_0} & |f| \leq f_0 \\ 0 & |f| > f_0 \end{array} \tag{6.25}$$

indeed one has that by the Wiener-Kitchine theorem, cfr. [166], the Fourier transform of the power density function is equivalent to the autocorrelation

$$R(\tau) = \int_{-\infty}^{\infty} e^{i2\pi f\tau} P_{\mathrm{LP}}(f) df \tag{6.26}$$

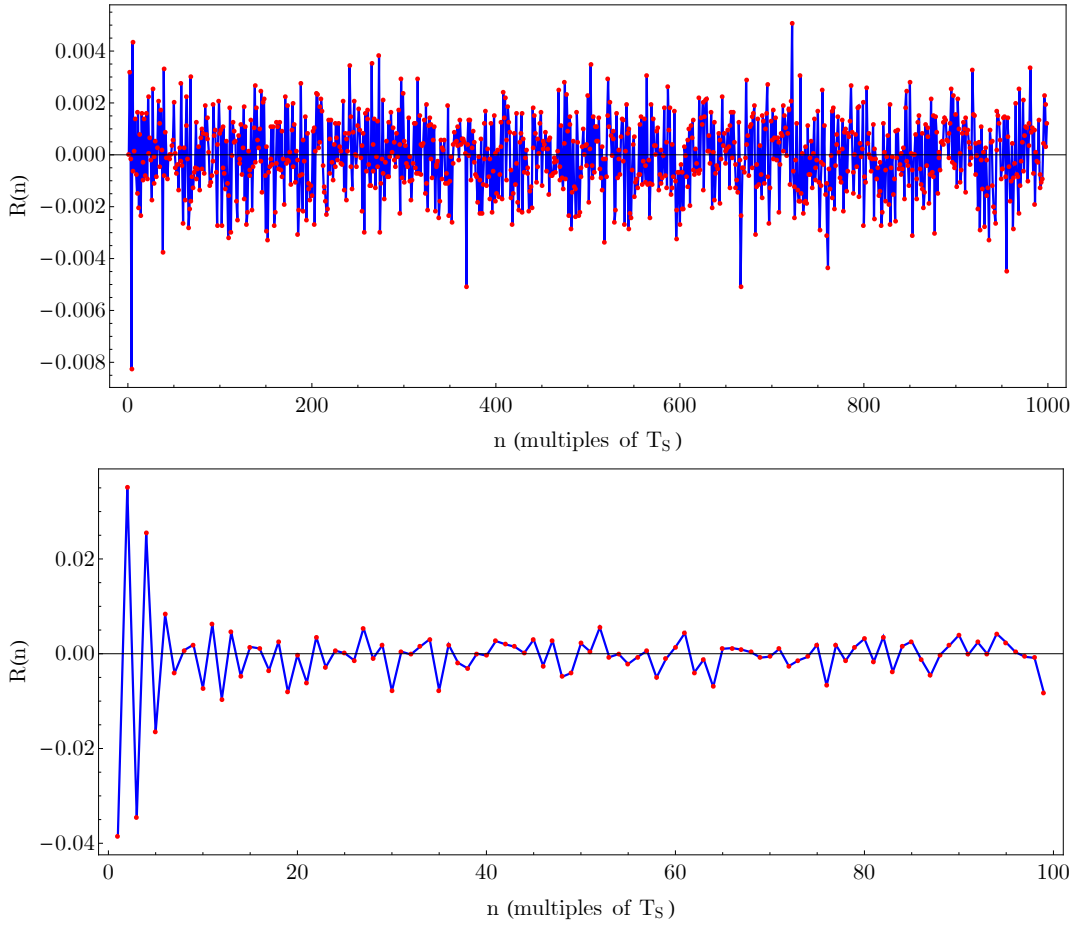


Figure 6.13: **Top:** by downsampling the original waveforms of a factor of 8, i.e. taking a sample every 8, the quadrature measurements become uncorrelated. **Down:** It is interesting to notice that by downsampling with a factor even higher but not a multiple of eight, e.g. 25, one can not achieve the same level of uncorrelation.

and because $P_{\mathrm{LP}(f)}$ is a step function in the frequency domain, its Fourier transform is given by $R(\tau) = \mathrm{sinc}(2\pi f_0 \tau)$ in time. The fact that it is not incidental that the autocorrelation corresponds to a sinc function is relevant because lets one to find the exact sampling interval to get uncorrelated raw random numbers. One then has $R(\tau) = 0$ for $\tau = i/2f_0$ with $i \in \mathbb{Z}$ which implies that

$$n = \frac{i}{2 f_0 T_S} = 8i\,. \tag{6.27}$$

From the inset in Figure 6.4.2, one can appreciate that the expected condition $R(n = 8i) = 0$ holds true for the measured autocorrelation. We then downsampled the waveforms picking one in eight samples, which corresponds to a sampling frequency $f'_S =$

1.250 GS/s. After the downsampling the acquired waveforms presented a typical autocorrelation of the kind reported in Figure 6.4.2: as one can notice, the residual correlation not only decreases in average of two orders of magnitude but becomes incoherent in the sense that there is not a phase relation between samples separated by a given time interval.

As counter proof of the validity of the method adopted, it can be interesting to show that applying the naive principle the rarest are the sample points the smallest is the correlation, does not yield the same results as the one based on an accurate bandwidth estimation: in Figure 6.4.2 the autocorrelation one would get by taking every 25-th sample ($f_S = 400$ MHz) is reported and as one can see there is in average an higher correlation, especially for the samples temporally close.

Although the numbers would be later on processed with an extractor, this stage of the processing was necessary to get as close as possible to the ideal condition of independence of the measurements. It is worth stressing that the probability distribution of the quadratures, in case of high correlation, is still a Gaussian distribution but with the issue that given a measurement, the neighboring measurements yields outcome close to the previous one. Among the works which deal with CV-QRNG, the problem of correlations is explicitly addressed only by [167], while instead in [109] and [162] there is not reference to this issue.

### 6.4.3 Application of the CV-EUP protocol

In a regime of quantum noise limited measurement, a linear relation between a the LO power and the vacuum noise variance is expected. Citing directly [168]

> A reliable measurement of the quantum noise should only be attempted for situations which show a linear dependence of the measured noise level on the optical power.

We studied whether it was possible to find such behavior in the filtered spectra. In the present case however, assessing a linear increase of the noise fluctuations with the laser power is an important procedure for at least four reasons:

- to check the validity of the previous digital processing
- to check the maximum power of the oscillator that can be used before entering in a regime of non-linearity;
- verify the influence of noise of non-quantum origin which is represented as the intercept of the fit line: indeed if the additional electronic noise were absent, for zero level of power one would have a null intercept;
- convert the sampling interval, $\delta_{ADC}$ of the ADC in $\delta$ of the quadrature: in this way can establish a direct relationship between the voltage domain and the quadrature domain.

In Figure 6.4.3 can be considered a typical plot of the measured difference signal variance as function of the total input power, i.e. every PIN of the receiver is reached by half of the value reported in abscissa. The set of points $\{\sigma^2_{V_i}, P_{LO_i}\}$ was obtained by varying the LO power between 0.5 mW and 9 mW in steps of 0.5 mW and evaluating the variance of the corresponding waveforms acquired with the oscilloscope. The relation of linearity is clearly evident between 0.5 and 7.0 mW. After the threshold of 7.5 mW one has that the variance level drops steeply. One can safely exclude that this loss of linearity is due to some sort of PIN saturation, rather it can be ascribed to a regime of saturation attained by the transimpendance amplifiers, cfr. [168] and [169].

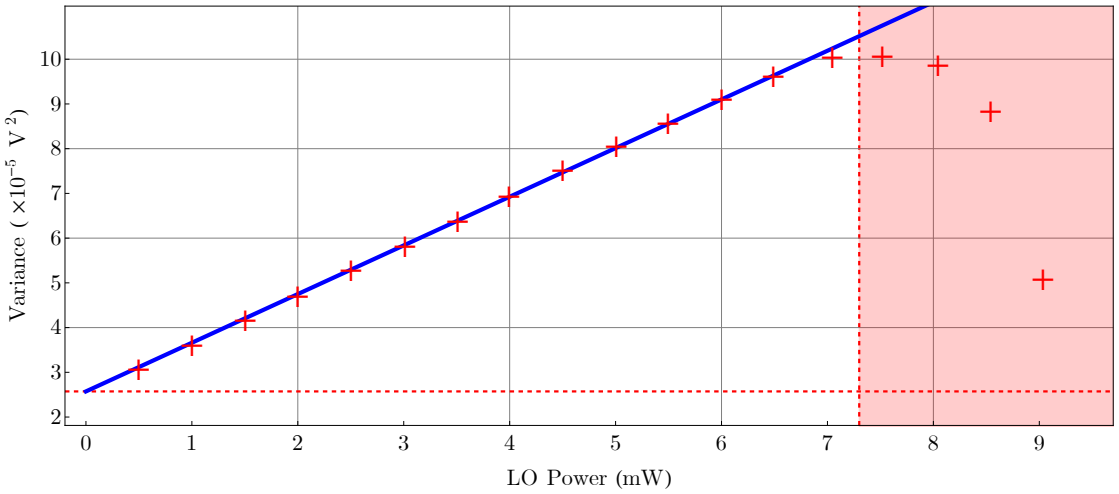


Figure 6.14: The plot shows the linear relation between the LO power and the measured voltages variances. Between 0.5 mW and 7 mW we are in a QNL region whereas at 7.5 mW transimpendance amplifiers start to saturate with a not linear response of the detectors, evidenced in the red shaded region on the right. The red shaded region below represents the contribution of the technical noise.

If then one limits the region between 0.5 mW and 7 mW, by performing a linear fit on the sample points one gets angular coefficient $m = 0.1088 \pm 0.0002$ $^{V^2}/_{W}$ and intercept of $a = (2.573 \pm 0.075) \cdot 10^{-5}$ $V^2$. The presence of a not-null intercept is the signature of an unavoidable noise having a non-quantum origin. At the base of the plot, the red shaded area marks the region where technical noise is dominant. This noise can not be eliminated and it ends up in the signal generating the raw random numbers, affecting their security. Since the neat observed effect is a widening of the quadrature variance, according to our model we do not discriminate whether the source of the extra noise resides in the preparation or in the measurement stage: the input state is treated as an imperfect state (not a completely vacuum pure state) detected by a perfect detector.

To convert the voltage measurements in absolute values of the quadrature oscillations, a the conversion factor $\beta$ can be derived by considering the relation between $P_{LO}$ and

the variance of the difference signal $\sigma_V^2$, given by

$$\sigma_V^2 = \frac{1}{2}\eta P_{LO} \tag{6.28}$$

where the factor $1/2$ is the quadrature value of the vacuum, according the present convention, *amplified* by the local oscillator and $\eta$ a proportionality coefficient. By comparing the angular coefficient $m$ of a regression line of the kind presented before with eq.6.28, one gets $\eta = 2m$ such that

$$\beta = \frac{1}{\sqrt{2mP_{LO}}}\,. \tag{6.29}$$

In Figure 6.4.3, 121 quadrature variances are reported for an acquisition lasted over 3 hours: every point in the plot corresponds to an average sample size of $130 \cdot 10^6$ measurements acquired for 100 s being the transfer rate of about $1.3 \cdot 10^6$ sample per second, in the proprietary file format of the oscilloscope data transfer protocol (every points corresponds approximately to 1 GByte of raw data). These values were obtained by multiplying the voltage data by $\beta = 81.04^1/_V$ with $P_{LO} = 6.9967$ mW the average value of the power during the data collection. By referring to Figure 6.4.3 one can see that during the whole acquisition there was an overall power variation of approximately the 0.3%, which could be addressed as to the laser itself, as to the fiber attenuator or to the beamsplitters. The attenuator was indeed tuned in order to get a power 7 mW entering the last beamsplitter, because of the highest SNR still reachable in the region of linearity, before the saturation regime of the amplifiers. We have then average quadrature value of $\langle\sigma^2\rangle = 0.654 \pm 0.003$, i.e. the 30.8% larger than the expected in the ideal case.

As we explained in the previous Section, according the model *perfect detector - imperfect state* we treated the fact that the variance is almost one third larger than $1/2$, as if our system did not introduce any noise but the input state was mixed, resulting in a wider thermal state. It is worth specifying that the photodiodes efficiency is not unitary, however this fact is

### 6.4.4 Estimation of the conditional min-entropy

The purpose of this proof of principle was to test the resiliency of the EUP protocol as an active way to extract the maximal quantum randomness also in conditions where the devices are introducing noise. Consequently, we exploited the advantage of the off line analysis applying the protocol in the worst conditions, i.e. when we registered the highest deviation of the quadrature variance from $^1/_2$, marked with a red circled in Figure 6.4.3. By comparing the time tags relative to this set of data with the power meter logs, one finds that said variance increment was during the time interval of lowest power (circled red shaded area of Figure 6.4.3). It is worth noting that this correspondence could be just incidental, considered that by studying the variance distribution it is hardly recognizable some kind of correlation with the $P_{LO}$. In general however, one has that the higher the LO power, the higher the contrast between vacuum oscillations and classical noise. In the following, the basis for the *raw* random numbers corresponds to $\mathcal{P}$ instead

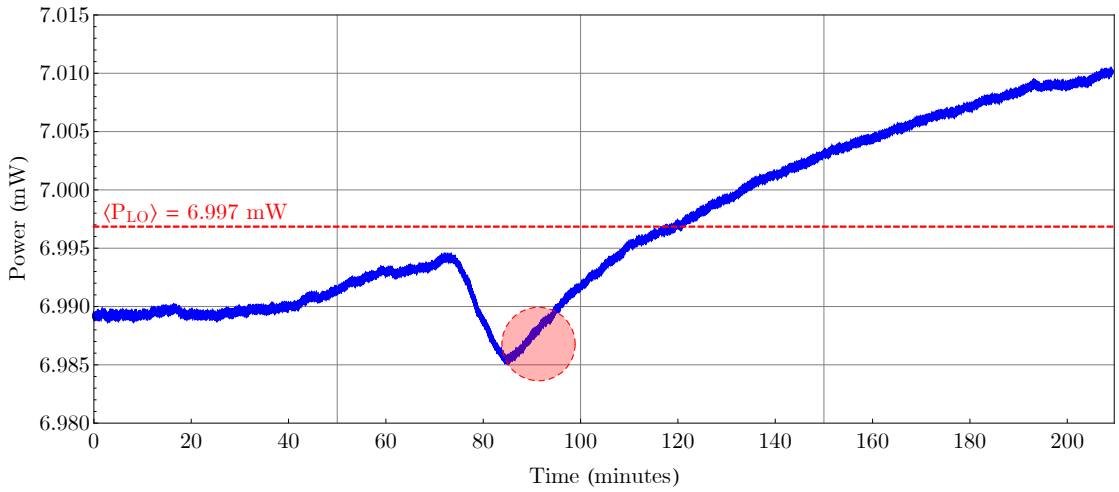


Figure 6.15: The plot shows the power meter logs before the last beam splitter. As one can see the power readings show an overall increasing trend, although the relative variation is less than 0.5%. It is worth to point out that power variation could be addressed as to the laser, as to thermal/mechanical change of the combination optical attenuator + beam splitter.

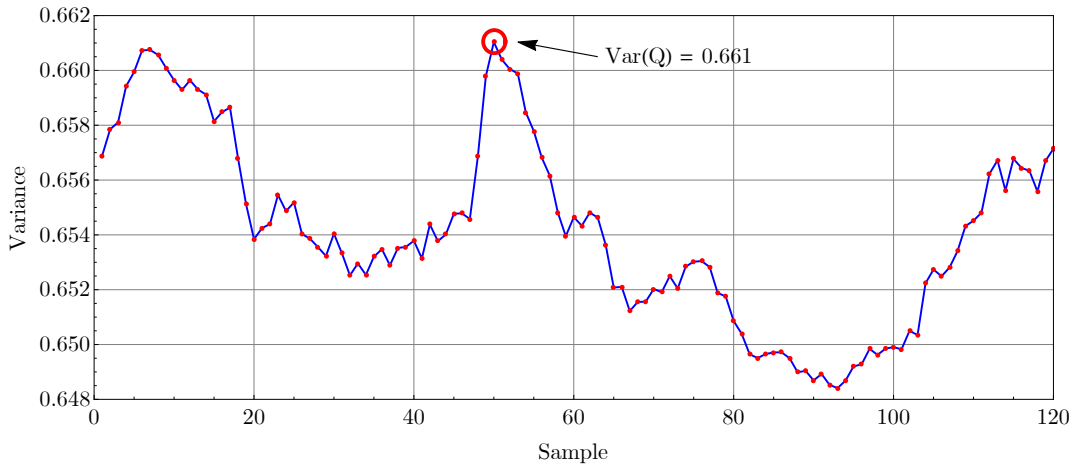


Figure 6.16: In the plot the variances of the field quadratures are reported. These values were obtained by converting in quadrature values the voltage readings acquired with the oscilloscope in a total of three hours of acquisition. Every point corresponds to an acquisition of 100 s. The red circled spot marks the measurement with the largest variance that we used as reference for the estimation of the conditional min-entropy.

$\mathcal{Q}$ is the check basis (this choice was arbitrary because, for the vacuum state, one has a symmetric Wigner distribution).

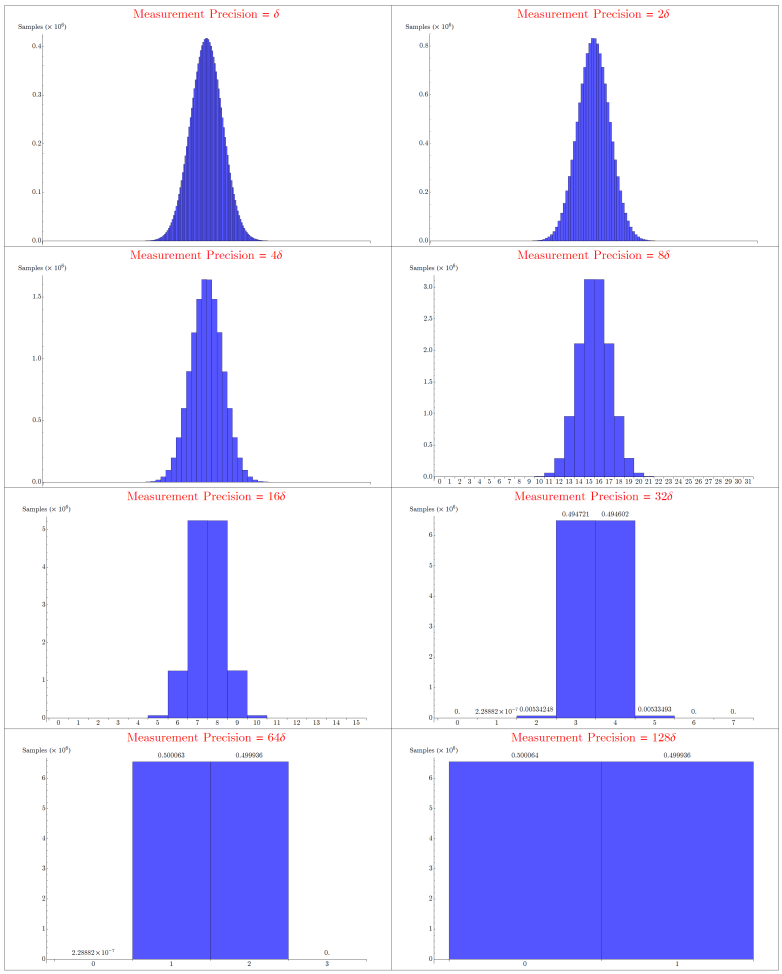


Figure 6.17: The histograms refer to the data set featuring the largest variance and that it was selected as sample set to extract the check measurement, i.e. the measurements that in a real implementation would refer to $Q$ quadrature. The different outcome distributions are listed for precision varying from $\delta_1$ corresponding to 8 bit depth of the ADC (256 bins), to $\delta_8$ corresponding to 1 bit (2 bits). For high precision, the gaussian distribution of variThe distributions show how lowering the resolution make not possible to discern what kind of state has been sent. However, the symmetry of the of the histograms indicate that good experimental conditions were matched in order to generate raw random numbers.

In this study then, for the reasons said before, the check basis measurements for the estimation of $H_{\max}(Q)$ were randomly extracted from the data set with the variance

$\sigma_Q^2 = 0.661$. Although these measurements were chosen randomly and in small fraction compared with the size of the set, a real implementation of the protocol in a QRNG would obviously require the check measurements to be done uniformly and independently during the whole process of data acquisition, rather than be confined in a given time interval. If the presence of Eve is neglected, i.e. if we assume that the possibility of existence of an elaborated mechanism to adapt the preparation of the state in order to trick the entropy estimation, the method of randomly distributing in time the base switching is still recommended because one makes small the chance of skipping anomalies or defects in the operation of the generator (that is the opposite that was done in this analysis).

We evaluated different bounds

$$H_{\min}(P(\delta_j)|E) \geq \log_2 \left( \frac{2\pi}{\delta^2} S^{00} \left[ 1, \frac{\delta^2}{4} \right]^{-2} \right) - H_{\max}(Q(\delta_j)) \tag{6.30}$$

as function of an interval $\delta_j = \delta q_j = \delta p_j$ of increasing width. More in detail, since the highest precision $\delta_8$ of the ADC has a depth of 8-bits, the resolution was halved 7 times in order to form intervals $\mathcal{I}_j$ with cardinality $2^j$ and $j \in \{7, 6, 5, 4, 3, 2, 1\}$ respectively. Since $H_{\max}$ is equivalent to the Renyi entropy of order $1/2$, we expressed it considering its bayesan estimator which provides

$$H_{\max}(Q(\delta_j)) = 2 \log_2 \left( \frac{\Gamma\left[n_Q + 2^j\right]}{\Gamma\left[n_Q + 2^j + 1/2\right]} \sum_{k=0}^{2^j - 1} \frac{\Gamma\left[n_k^j + 3/2\right]}{\Gamma\left[n_k^j + 1/2\right]} \right) \tag{6.31}$$

where $n_k^j$ is the number of measurements which fall inside the bin $I_k^j$ of the set $\mathcal{I}_j$ and such that for every fixed $j$ one has $n_Q = \sum_k n_k^j$.

With this approach we were able to simulate ADC with lower bit resolution and then study how the min-conditional entropy changes. The probability distributions $Q_{\delta_j}$ used in the previous relation are reported in Figure 6.4.4. The remarkable symmetry of the histograms, which feature the expected bell Gaussian shape, is a proof that the experimental conditions were properly set for the extraction of the raw numbers. Indeed, it is worth stressing that this unbiasedness would be an advantageous starting point if we aimed to implement a classic CV-QRNG. In particular, with the precision $\delta_7$, which is equivalent to extract just a single bit per measurement having only two intervals left, we registered a difference in the proportion of 0s and 1s of just 0.025%. This slight deviation from uniformity implies a value of the min-classical entropy close to 1, i.e. the distance between the raw bit distribution and an ideal is such that a randomness extractor would compress the input strings of just 0.018%.

This example is interesting because it shows the limits of an approach which does not takes in account the tomography of the state. This can be readily understood by considering Figure 6.4.4 where the min-conditional entropies $H(P_{\delta_j}|E)$ are reported as function of the precision. Since we were interested to study also the amount of check measurements to get as close as possible to the exact value, we extracted from the worst

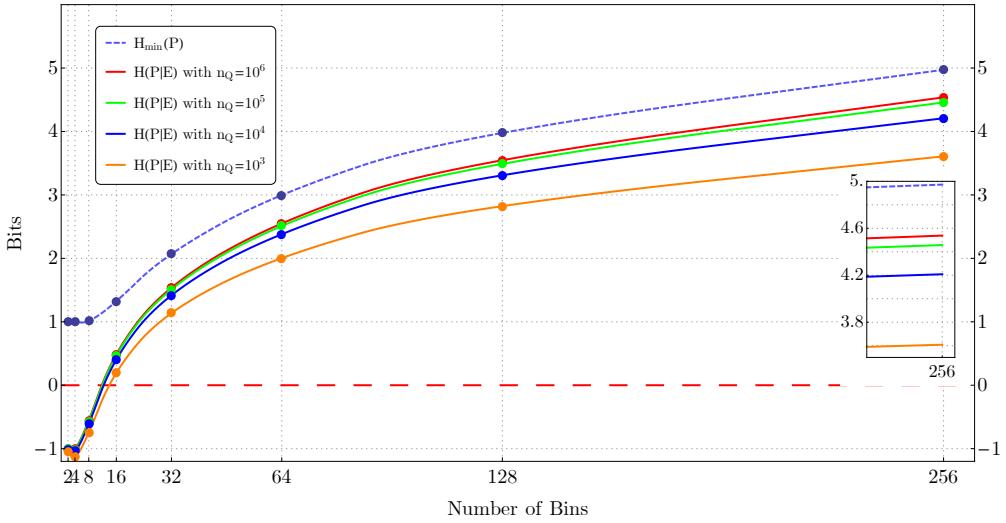


Figure 6.18: Conditional entropies $H_{\min}(P(\delta_j)|E)$ for different sizes of the check measurement sample set are reported as function of the measurement precision $j \in \{1, 2, 3, 4, 5, 6, 7\}$. The dashed purple line correspond to the value of classical min-entropy. It is relevant to notice how the conditional min-entropy overestimates the real amount of true random bits extractable from the measured quantum state. However it has to be pointed out that evaluating the $H_{\min}(P(\delta_j)|E)$ with a too low precision, i.e. $j \in \{1, 2, 3, 4\}$, one has that the min-conditional entropy is not meaningful either because the resolution is too low to distinguish the state.

data set random subsets of size $n_Q = \{10^3, 10^4, 10^5, 10^6\}$. Each point in the plot is an average on 200 entropy values estimated at every round on a different random subset. By looking at the graph the following considerations can be drawn:

- Low Precision ($\delta_5 \to \delta_7$): the conditional min-entropy is negative. This means that the maximum amount of true random bits which can be extracted is zero, giving the bound no-information about the real content of randomness. This is a consequence of the fact that the precision is not enough sharp to accurately distinguish the state, e.g. for $\delta_7$ inputting into the QRNG a symmetric tight squeezed state or a broad thermal one would yield the same binary distribution. The classical min-entropy (dashed purple line) attains, as expected, the unit value. The unity is reached already with $\delta_5$ because *with respect to the variance* of the input state such precision is too wide, i.e. the central intervals already comprise most of the data points.

- High Precision ($\delta \to \delta_4$): increasing the precision one can extract an ever growing number of true random bits. It is interesting to observe that the less the number of measurement performed in the check basis, the less the number of extractable true random bits for a fixed precision. This fact can be interpreted always in terms

of measure precision: if the resolution is high, a higher number of measurements is needed to accurately reconstruct the state; for example, one can see that for $\delta_4$, the distance between the estimated entropy values for different set sizes $n_Q$ is closer than for $\delta$. As expected, being the measured state comparable to a thermal one, given the large variance, for high deltas we have that the conditional min-entropy does not tend to the min-entropy. It is worth stressing that **this gap is not a measurement limitation**: increasing the precision or the number of measurements would not improve the number of true random bits, because the limit of extractable randomness is given by the condition of non-purity of the quantum state.

Following this analysis the final conclusion that can be drawn is that the classical min-entropy is not a reliable quantity in order to evaluate the final length $l$ of the random string associated to the random variable $P$. As we have shown, the $H(P)$ *always* overestimates the true amount of random bits: it can regarded just as a quantifier of statistical randomness, i.e. accidental randomness + quantum randomness. However it does not give information on which percentage they are given: for example we see that for $\delta_1$ the statistical random bits extractable per measurement are 5.7 but out of them only 4.7 are of quantum origin. If a QRNG has to be employed to generate cryptographic keys, the use of min-entropy would be allowable only if quantum side information could be ruled out, e.g by forging a pure state, and only if the measurement operators/devices would not introduce any classical noise. Unfortunately, this represents a hardly achievable condition especially if one aims to build QRNG for common use.

### 6.4.5 Rates

As said before, an implementation of the protocol in a generator requires the switching between the two mutually unbiased basis during the whole generation. The instant when the generator stops to measure in the $\mathcal{P}$ basis to collect a measurement in the $\mathcal{Q}$ basis must be random in order to prevent that some state masking dynamic, malicious or just fortuitous, to be synchronized with the check instant. In the countability of the randomness then one has to take in account the number of bits necessary for the switching. Also for the CV-QRNG, we set $n_Q = \sqrt{m}$ with $m$ the total number of measurements in both the bases. Out of the $m$ measurements the check instants can be chosen in $\begin{pmatrix} m \\ n_Q \end{pmatrix}$ different ways. A given random combination then can be encoded in a *seed* $t(m) = \lceil \log_2 \frac{m!}{n_Q!(m-n_Q)!} \rceil$ bits long. We evaluated then the secure generation rate, i.e. the neat number of true random bits per measurement, according

$$r_{\text{sec}} = \frac{1}{m}(m - n_Q)[-c(\delta_j) - \widetilde{H}_{max}(Q_{\delta_j})] - t(m) \tag{6.32}$$

varying the precision $\delta_j$ with $j \in \{1, 2, 3, 4\}$ with the results are represented in Figure 6.4.5. As for the discrete case, the rates tend to the asymptotic value of $\widetilde{r} \longrightarrow r(P_{\delta_j}) = -c(\delta_j) - \widetilde{H}_{1/2}(Q_{\delta_j})$ for $m \to \infty$. The red lines and the orange areas represent the

expected average rate and the $3\sigma$ uncertainty respectively, obtained by simulating the check measurement with a gaussian probability distribution having the same measured variance $\sigma_Q^2 = 0.661$ of the sample set. Each blue point with $3\sigma$ error bar, corresponds instead the to the averages of $\widetilde{r}$, being every average evaluated on 200 random data set of size $\sqrt{m}$ with $m \in \{2^7, \ldots, 2^41\}$. As one can see, there is a remarkable agreement between the expected and the experimental values. For what concerns a real implementation of the protocol, an advantage in using the highest precision of the ADC, lies in the fact that one would need much more measurements to reach a given rate value but with a lower precision. The green shaded area in the plot marks the regions where the distance to the asymptotic limit is less than the 5% and which starts at $m = 2.1 \cdot 10^9$: if a QRNG was provided with the equivalent of a squashed quantum state with this same $\sigma_Q^2$, with a sampling rate of 2 GS/s and a resolution of 8 bits, the generator could provide a quantum secure rate of roughly 8.71 Gbit/s.

### 6.4.6 Statistical Randomness Assessment

For the post-processing of the numbers, we implemented the fast computable two-universal hash function introduced in [125] which we used also for the DV-QRNG. Given the total amount of measurements being $m = 1604845568$ we invested $n = \lceil sqrtm \rceil \simeq 40000$ bits to evaluate the min-conditional entropy, which was estimated to be $H(P(\delta p)|E) = 4.3394$ bits in average per measurement and a corresponding rate of $r = 4.3385$ bits. Considering that every measure was taken with an equivalent sampling rate of 1.25 GS/s, we have a theoretical secure rate of 5.4 Gbit/s. The final neat total amount of secure random bits amounted to $6.96 \cdot 10^9$ which were obtained by taking the modulo sum 2 of the product between substrings $n = 10000$ bits long and a $n \times l$ matrix with $l = 5424$ (corresponding to the ratio between $H(P|E)$ and the binary encoding of a single measurements, i.e. 8 bits). In this proof of principle, the hash matrix was generated for every substring using the pseudo-random number generator of the processing software: naturally a real implementation would require a seed of true random numbers to be stored inside the generator. As we did in the previous Chapter we tested the numbers with standard NIST statistical tests in order to assess the *statistical* quality of the numbers: it is worth stressing that once the extractor is properly calibrated and the hash matrix is truly random, the post-processed numbers are expected to pass the tests, as explained in the previous Chapter. This was indeed the case as one can see from Figure 6.4.6 where the results on 6 strings $10^9$ bit longs are reported.

### 6.4.7 Comparisons with other CV-QRNG

At present time, CV-QRNG based on the vacuum state quadrature homodyne were presented by Gabriel et al. [109], by Shen et. al [167] and by Symul et. al [162].

The purity of the state is assumed, in all the works. In particular, in [109] this hypothesis is motivated explicitly by considering that the open arm of the beam splitter was blocked so an adversary could not influence the state from that input. The treatment of security is then completely classical with a characterization of the randomness based

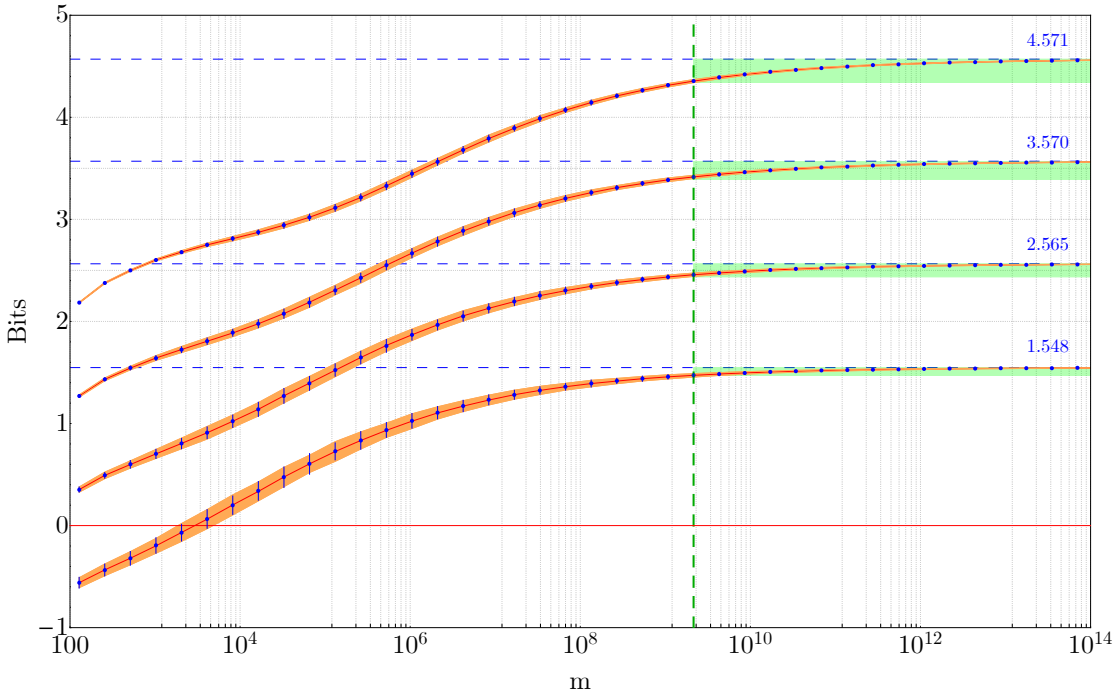


Figure 6.19: In Figure the theoretical and experimental rates, red lines and blue points respectively, are reported for different precisions $\delta_j$ with $j \in \{1, 2, 3, 4\}$ as function of the total number of measurements $m$. For every $m$, theoretical lines were obtained averaging 200 rate values calculated on simulated sample gaussian distributions with the same variance of the used dataset, $\sigma_Q^2 = 0.661$. The orange shaded areas correspond to expected the $3\sigma$ errors. The blue points are the averages of the rates evaluated on 200 random samples of size $\lceil \sqrt{m} \rceil$. As one see there is a remarkable agreement between experimental points and expected results. In particular one has that for $m \to \infty$, the rates tend to an asymptotic value equal to the min conditional entropy. The green dashed line marks the regions where one has less than the 5% of distance from the asymptotic value.

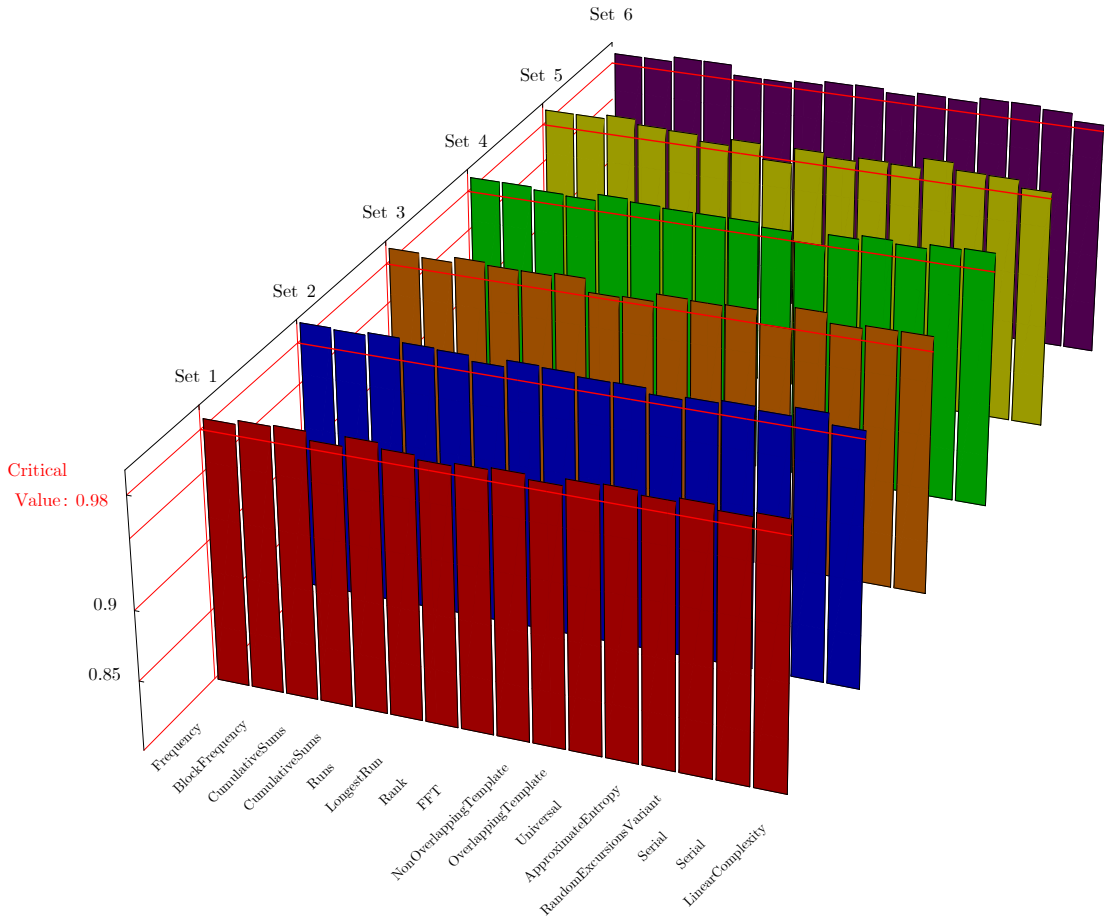


Figure 6.20: The stacked plots represents the passing ratio for the NIST test suite SP-800-22. Histograms correspond to six different strings $10^9$ bit long. Each of the 16 tests was applied on 1000 substrings $10^6$ bits long and a bin represents the fraction of strings which passed a given test. The red line corresponds to the critical passing ratio.

only on the electronic noise. In [109] the quantum entropy is obtained by subtracting the entropy of the electronic noise measured without signal inputs to the entropy of the quadrature measurement. Randomness extractors (one way hash functions or the classical seedless extractors) are then calibrated on this value of entropy which corresponds only to an upper bound. Indeed the authors employed the Shannon entropy instead of the min-classical: as it is pointed out in [125] the use of this estimator did not guarantee the independence from the noise.

In the other two works, the independence from noise is achieved by considering least significative bits in the binary encoding of the measurements. This approach is adopted in order to pass the statistical tests of randomness: regarded in the perspective of the EUP protocol, with this approach one looses information about the real measured state. The generation rates are of 6 Mbit/s for [109], 12 Mbit/s for [167] and from 25 Mbit/s to 2 Gb/s according to the number of discarded bits for [162]. Compared with these generators, the EUP method not only does not need the strong assumption of the purity of the states, but it takes also into account also the electronic noise, filtering out any non-quantum source of noise.

## 6.5 Conclusions

The considerations that can be done are similar to the one of the previous Chapter. However here, not only we have demonstrated that the EUP protocol can be applied to infinite dimensional quantum systems in order to extract the true content of random bits, but we have also shown that the amount of extracted bits depend also on the precision of the measurement. This point is relevant because CV-EUP protocol lets one then to extract true randomness as function of the classical noise affecting the state and of the resolution of the instrument employed. The CV-EUP protocol then can be regarded as resilient dynamic extractor which can offer improved quantum security for the upcoming generation of fast CV-QRNG.

# Chapter 7

# Conclusions

Quantum Key Distribution and Quantum Random Number Generation are technologies which are becoming increasingly more common and in a not distant future will be available in every day life. In this thesis different methods were presented to characterize and exploit the noises affecting these protocols, in order to improve their future implementation.

With the ARTS method of Chapter 2 we presented and demonstrated the validity of a procedure which enables the exchange of secure bits also when the level of losses would not permit it. This improvement is made possible by exploiting the *optical turbulence noise*, i.e. the peaks of transmissivity due to the log-normal distribution. The point of strength of ARTS, is the fact that it is a real time protocol and then it is resilient when the losses of the channel are rapidly varying.

Clearly ARTS represents a resource for the upcoming satellite Quantum Communications, a scenario where the losses are high by default: the satellite will be available above the two parties Alice and Bob only for a limited amount of time so it is vital to take advantage of every single transmissivity window to generate the key.

Noise was also the subject of Chapter **??** and 6: in both the cases, noise corresponds to the apparently random behavior of a physical quantum state which is not pure but mixed. Here the method devised to improve the unpredictability in a strict quantum sense, is to carefully quantify the amount of randomness which is extractable by employing a quantum mechanical tool, the *entropic uncertainty protocol*. Without any doubt the main advantage of this protocol lies in the fact that a quantum information quantity, the min-entropy conditioned on a quantum adversarial system E, is used for a quantum information process. In the QRNG Literature, classical entropies are typically used to estimate the content of randomness. Consequently also the post-processing methods are classical. It is clear that with this classical approach all the advantages of using a quantum random number generator are lost, because nothing certifies that the stream of bits has still a quantum origin. With the EUP protocol instead, on one hand we address the demanding security scenario of an adversary with quantum side information. On the other hand we provide a method which can extract true randomness also in case of a generator affected by noise as we did in 6. Also in this case we think that the

QRNG methods presented in this thesis can be a resource to match the strict security requirements for the generators to be employed in present and future Quantum Key Distribution protocols.

# Appendix A

# Min-entropy estimation

In this section we show how to estimate the expected min-entropy. In a sample with $L$ bytes, the single byte occurrence $\ell_i$ $(i = 1, \cdots 256)$ are random variables distributed according the Poisson distribution with mean $\lambda = \frac{L}{256}$. In order to estimate the expected min-entropy we need the distribution of the maximum of the occurrences and we can proceed as follow. Given a sample of $n$ random variables $X_1, X_2, \ldots, X_n$ whose cumulative distribution function (CDF) is $D(x)$ and the probability density function (PDF) is $F(x)$, they can be re-ordered as $X_{\pi(1)} \leq X_{\pi(2)} \leq \cdots \leq X_{\pi(n)}$: the $X_{\pi(k)}$ is called statistic of order $k$, such that $\min\{X_1, X_2, \ldots, X_n\} = X_{\pi(1)}$ and $\max\{X_1, X_2, \ldots, X_n\} = X_{\pi(n)}$. In order to derive the distribution function of an order $k$ statistic, given $h$ the number of $X_i \leq x$, one can note that

$$\begin{aligned} D_k(x) = P(X_{\pi(k)} \leq x) = P(h \geq k) &= \sum_{i=k}^{n} P(h = i) \\ &= \sum_{i=k}^{n} \binom{n}{i} [D(x)]^k [1 - D(x)]^{n-k} \end{aligned} \tag{A.1}$$

Working with integer random variables the PDF is then obtained by

$$F_k(x) = D_k(x) - D_k(x - 1) \tag{A.2}$$

Being interested in the byte frequencies maximal values, that is $k = n$, the previous equation becomes

$$F_n(x) = [D(x)]^n - [D(x - 1)]^n \tag{A.3}$$

In a sample with size $L$, the distribution of the maximum $\ell_M$ of the single byte occurrence $\ell_i$ can be computed by using the previous equation with $D(x) = e^{-\lambda} \sum_{j=0}^{x} \frac{\lambda}{j!}$, $\lambda = \frac{L}{256}$ and $n = 256$:

$$\begin{aligned} \Pi(\ell_M) &= (e^{-\lambda} \sum_{j=0}^{\ell_M} \frac{\lambda}{j!})^n - (e^{-\lambda} \sum_{j=0}^{\ell_M - 1} \frac{\lambda}{j!})^n \\ &= \left( \frac{\Gamma(\ell_M + 1, \lambda)}{\ell_M!} \right)^n - \left( \frac{\Gamma(\ell_M, \lambda)}{\Gamma(\ell_M)} \right)^n \end{aligned} \tag{A.4}$$

The expected value and variance of the maximum of the $\ell_i$'s, are then easily evaluated by applying the definitions $\langle \ell_M \rangle = \sum_{x=0}^{\infty} x\Pi(x)$ and and $\sigma^2 = \langle \ell_M^2 \rangle - \langle \ell_M \rangle^2$ respectively. With a sample size of $L = 1399852$ bytes and $n = 256$, the theoretical reference values are then evaluated to be $\langle \ell_M \rangle = 5678.4 \pm 29.4$ counts with corresponding expected relative frequency $f_M = \frac{\langle \ell_M \rangle}{L} = (4.056 \pm 0.021) \cdot 10^{-3}$. This value corresponds to a theoretical min-entropy of $H_{min} = -\log_2 f_M = 7.946 \pm 0.007$ bits per byte. If the obtained experimental min-entropy is compatible with the predicted theoretical value, the sample can be considered as uniformly distributed.

# Appendix B

# Statistical suites

### B.0.1 NIST suite

The Statistical Test Suite developed by NIST [159] applies stringent tests in order to check the reliability of PRNGs and TRNGs for cryptographic applications. This suite is widely used to study in general the output of TRNGs and thus become a standard.

| **Statistical Test Suite v. 1.8** | | |
|---|---|---|
| | **Test** | **Defect Individuated** |
| 1 | Frequency | Deviation from uniform distribution of 0s and 1s. |
| 2 | Block Frequency | Deviation from uniform distribution of 0s and 1s within a block |
| 3 | Cumulative Sums | Deviation from uniform distribution at the beginning of the sequence. |
| 4 | Longest Runs Of Ones | Deviation of the distribution of long runs of ones. |
| 5 | Runs | Large (small) total number of runs indicates that the oscillation in the bit stream is too fast (too slow). |
| 6 | Rank | Deviation of the rank distribution from a corresponding random sequence, due to periodicity. |
| 7 | Spectral | Periodic features in the bit stream. |
| 8 | Non-overlapping Template Matchings | Too many occurrences of non-periodic templates. |
| 9 | Overlapping Template Matchings | Too many occurrences of m-bit runs of ones. |
| 10 | Universal Statistical | Compressibility (regularity). |
| 11 | Random Excursions | Deviation from the distribution of the number of visits of a random walk to a certain state. |
| 12 | Random Excursion Variant | Deviation from the distribution of the total number of visits (across many random walks) to a certain state. |
| 13 | Approximate Entropy | Non-uniform distribution of m-length words. |
| 14 | Serial | Non-uniform distribution of m-length words. |
| 15 | Linear Complexity | Deviation from the distribution of the linear complexity for finite length (sub)strings. |

Table B.1: Descriptions of the tests implemented in the NIST suite.

In Table B.1 the tests implemented in the suite are listed. Test 1 and 2 control the uniformity of the distribution of bits in the whole substring as in smaller blocks (128

bit), respectively.

The NIST suite applies also tests based on the theory of *random walks*: given a binary string of length $n$, the random walk $S_n$ is defined as $S_n = \sum_{i=1}^{n}(2 \cdot x_i - 1)$ where $x_i$ is the i-$th$ bit in the string and $S_0 = 0$. The random walk is then a function which oscillates according to the distribution of underlying bits. Since the statistical properties of random walks are well known, it is possible to study if these oscillations agree with the theory. The test statistic of test 3 is the maximal value reached by $S_n$, that is the absolute value of the largest partial sum of the random walk: the test is applied two times to every string, calculating the sum starting from the beginning (forward mode) and from the end (reverse mode); for a uniform distribution of bits the random walk should not depart too much from the origin while, when the string is strongly biased, the sum will reach large values, not in agreement with the null hypothesis. For test 10 the test statistics is given by the number of excursions (intervals between two zero crossings) in which a given state of the walk (a partial sum $S_i$, $i < n$) is visited: the test is applied 8 times for the visits to the states between -4 and 4. The test 11 takes into account the number of times a given state is visited during the entire walk (not only in a single excursion): the test is applied 18 times for the states between -9 and 9.

Tests 4 and 5 use test statistics based on runs, uninterrupted sequences of 0s and 1s: the first test checks for the total number of runs into the string, which under $\mathcal{H}_\prime$ should correspond to half of the length, while the second one has the test statistic function of the frequency of the longest runs of 1s into fixed blocks of the string. In particular, it has been found that the test 4 more is sensitive with respect to the others since the test statistic is more directly affected by bias and correlation: a highly anticorrelated string tends to present many changes between 0 and 1, increasing the number of runs, while in a correlated one the number of runs tends to be low.

Tests 7, 8, 13 and 14 check for the independence and uniformity of the distribution of patterns, adopting the serial approach: test 7 has test statistics based on the frequencies of non-overlapping aperiodic patterns (of length 9 for the following analysis) like i.e. [01001101]; in 8, the test statics is a function of the frequency of the pattern [11111111], which is searched in an overlapped way; test 13 is a serial overlap one but the test statistics is redefined like an entropy function; test 14 is a simple serial overlap test on 16 bit words.

The spectral test, 6, employs a discrete Fourier transform on the bits in order to reveal the presence of periodic features.

The Universal test to detect deviation from randomness, considers the bit length separation between given bit patterns in a string and whether it is compatible or not with the null hypothesis: a bit string is divided in $Q + K$ not overlapped blocks of length $L$. Then the first $Q$ blocks are used for initialization. The $K$ blocks are scanned evaluating at every step the number $A_i$ of blocks which separate the current $i - th$ $L$ bit pattern from its last appearance in the bit string. [**?**] proofs that the test statistics $U = \frac{1}{K}\sum_{i=Q+K}^{K} \lg_2 A_i$ is distributed according to the normal distribution and also an expression for the variance is given: the NIST suite adopts expressly the original results of Maurer which can be found also in [**?**]. However, in Coron adds some corrections

improving the sensitivity of the test. This last version is implemented in the AIS31 suite. The interesting point about the Universal test is the fact that the average value of the test statistics corresponds asymptotically to the entropy per-bit of the $L$ bit word, the application of the test gives also a measure of cryptographic strength of the string analyzed.

The length of substrings chosen to run the suite is $1024^2 = 1'048'576$ bits: this is a common choice since it is the minimal length required by some tests (i.e. Universal Test) to be applied in the proper way and it permits to limit the computational time to few hours for all tests; generally, hundreds of substrings are tested, but some tests (7,10,11) apply more variants: for example the Non-Overlapping Template Matchings test is applied 147 times on every substring, as the number of non periodic patterns of 9 bits. The suite allows a great level of customization since it permits to change different parameters for the tests: for the analysis the parameters were set according to the length of substrings as suggested by the developers.

After the application of the tests, the suite prints a detailed report where, for every test, the distribution of p-values calculated for every substring, a p-value on the uniform distribution of the p-values, and the proportion of bit strings that passed the test, namely those ones with a p-value $\geq 0.01$, being set the significance level $\alpha = 0.01$ are given. This level of significance is a standard choice selected also in all the references studied and it implies that at least 100 substrings has to be tested in order to make the test meaningful (being expected 1 failure on 100). A test is not passed if: the proportion of sub strings which do not pass the tests are below given a threshold calculated on the base of the number of strings analyzed or if the distribution of p-values is not uniform, more specifically if the p-value calculated the on the resulting p-values frequencies is $\leq 10^{-4}$: in the final report strong failures are flagged with an asterisk.

Between the two ways of failure, the last one is the most serious since it implies the presence of persistent problems which affect every substring causing a non uniform distribution of p-values: this kind of failure does not necessarily cause a low rate of success because the p-values can all be a little higher than 0.01 but it is usually accompanied by the failure of other tests.

Differently, the failure of a test due to a rate of success smaller than that one predicted by the theory is possible and more frequent when, due to chance or to some temporary instability, a generator produces an excess of non-random strings: if the deviation from the threshold is not very large the suite indeed does not flag the failure.

### B.0.2 The AIS31 suite

The AIS31 [**?**] suite is a cryptographic suite developed by the BSI agency (Bundesamt f“ur Sichereit in der Informationstechnik) on the basis of the theoretical work made by W. Schindler in [170][171] in order to define and coding a reliable method for the evaluation of TRNGs.

The tests individuated by Schindler are divided in two classes: the first class checks that the random bit do not present *conspicuous statistical features* while the second

class checks that *they are practically impossible to determine even if the predecessors or successors are known.*

The first class comprises 6 tests: the first one is a preliminary test to check the pairwise disjointness of 48 bit long substring, while the other five (frequency, correlation, longest run, runs, poker test) are based on the dismissed NIST requirements for randomness testing [**?**]. These tests are applied 257 times on substrings 20000 bits long: the expected rate of success is very high in presence since the failure is given when p-value are smaller than $10^{-6}$.

The second class is expressly oriented for the testing of TRNGs since it checks that the eventual presence of bit hardware induced bit dependencies are not strong to determine an excessive cryptographic weakness of the strings. Indeed while the tests of the first class can be applied on numbers produced after a postprocessing unit, the tests of the second class must be applied *directly on the raw data* coming from the sampling of the digitized noise signal. Three tests are given: the first one is a simple frequency test (*uniform distribution* test); the second test checks the absence or, at least, the limited presence of bit dependencies evaluating if the output takes with the same probability the values 1 or 0 independently by the words of 2, 3 and 4 bits previously appeared (*comparative test for multinomial distributions*). The last test is Universal Test in the improved version of Coron (*entropy test*).

### B.0.3 The Alphabit battery

The last suite of tests applied to the generator is the library of tests TESTU01 developed by L'Ecuyer [160]. This suite is the most recent and comprises the largest spectrum of tests at present time available.

Also if most of the tests are oriented for the analysis of PRNGs, the TESTU01 provides a specific battery, the *Alphabit battery*, "designed primarily to test *hardware* random bits generators": this battery analyzes directly bits and applies tests sensitive to the typical problems of bit uniformity and independence.

Tests are grouped in three categories:

*Multinomial Bits Over Tests*: serial overlap tests on patterns of length $L$ =2, 4, 8 and 16;

*Hamming Tests*: two tests intended to check if the Hamming weights $H_i$, the number of 1s, into adjacent blocks of length $L$ =16 and 32 are independent: a test, HammingCorr, evaluate the linear correlation between the weight in blocks of 32 bits, while the other checks the uniform distribution of all the possible $(L+1)^2$ ;

*Random Walk Test*: these tests compares the statistical properties of the random walks built starting from the bit strings with their theoretical expectations.

Between the tests the most effective, without any doubt, are the Multinomial Bits Over ones, which were the first to be failed and those ones which reached the extreme p-values. These results confirmed then also the choice made to use the serial overlap test on pair as main tool for the first level analysis.

Formally the suite signals the failure of a test if the resulting p-value (or one of second order p-value) is out the interval [0.001,0.999]: L'Ecuyer however considers in

[160] passed a test which not present any p-value out the range $[10^{-10}, 1 - 10^{-10}]$.

# Appendix C

# Results of the suites for the Turbo-RNG

| Suite | Test | Set 1 | Set 2 | Set 3 |
|---|---|---|---|---|
| RABBIT | MultinomialBitsOver | 0.86 | 0.0082 | 0.89 |
| | ClosePairsBitMatch (t=2) | 0.04 | 0.11 | 0.2 |
| | ClosePairsBitMatch (t=4) | 0.44 | 0.11 | 0.59 |
| | AppearanceSpacings | 0.26 | 0.46 | 0.58 |
| | LinearComp | 2/2 | 2/2 | 2/2 |
| | LempelZiv | 0.64 | 0.14 | 0.0032 |
| | Fourier1 | 0.19 | 0.41 | 0.62 |
| | Fourier3 | 3/3 | 3/3 | 3/3 |
| | LongestHeadRun | 2/2 | 2/2 | 2/2 |
| | PeriodsInStrings | 0.79 | 0.65 | 0.21 |
| | HammingWeight (L = 32) | 0.9917 | 0.14 | 0.85 |
| | HammingCorr (L = 32) | 0.33 | 0.69 | 0.12 |
| | HammingCorr (L = 64) | 0.28 | 0.16 | 0.13 |
| | HammingCorr (L =128 | 0.7 | 0.87 | 0.04 |
| | HammingIndep (L = 16) | 0.19 | 0.53 | 0.02 |
| | HammingIndep (L = 32) | 0.62 | 0.31 | 0.6 |
| | HammingIndep (L = 64) | 0.32 | 0.74 | 0.47 |
| | AutoCor with a lag d = 1. | 0.09 | 0.42 | 0.58 |
| | AutoCor with a lag d = 2. | 0.98 | 0.35 | 0.71 |
| | Run | 2/2 | 2/2 | 2/2 |
| | MatrixRank (32 x 32) | 0.51 | 0.5 | 0.33 |
| | MatrixRank (320 x 320) | N.P. | 5/5 | 0.98 |
| | MatrixRank (1024 x 1024) | N.P. | N.P. | N.P. |
| | RandomWalk1 (L = 128) | 5/5 | 5/5 | 5/5 |
| | RandomWalk1 (L = 1024) | 5/5 | 5/5 | 5/5 |
| | RandomWalk1 (L = 10016) | 5/5 | 5/5 | 5/5 |

| Suite | Test | Set 1 | | Set 2 | | Set 3 | |
|---|---|---|---|---|---|---|---|
| ALPHABIT | MultinomialBitsOver (L = 2) | 0.13 | | 0.25 | | 0.45 | |
| | MultinomialBitsOver (L = 4) | 0.28 | | 0.75 | | 0.41 | |
| | MultinomialBitsOver (L = 8) | 0.62 | | 0.45 | | 0.18 | |
| | MultinomialBitsOver (L = 16) | 0.16 | | 0.04 | | 0.16 | |
| | HammingIndep (L = 16) | 0.19 | | 0.53 | | 0.02 | |
| | HammingIndep (L = 32) | 0.32 | | 0.31 | | 0.6 | |
| | HammingCorr (L = 32) | 0.33 | | 0.69 | | 0.12 | |
| | RandomWalk1 (L = 64) | 5/5 | | 5/5 | | 5/5 | |
| | RandomWalk1 (L = 320) | 5/5 | | 5/5 | | 5/5 | |
| | | **P-Val** | **Ratio** | **P-Val** | **Ratio** | **P-Val** | **Ratio** |
| NIST | Frequency | 0.421 | 0.9912 | 0.415 | 0.9855 | 0.158 | 0.9928 |
| | BlockFrequency | 0.893 | 1.0000 | 0.072 | 0.9807 | 0.208 | 0.9893 |
| | CumulativeSums | 0.694 | 0.9912 | 0.252 | 0.9855 | 0.059 | 0.9928 |
| | CumulativeSums | 0.091 | 0.9823 | 0.821 | 0.9855 | 0.343 | 0.9928 |
| | Runs | 0.784 | 0.9912 | 0.024 | 0.9952 | 0.856 | 0.9928 |
| | LongestRun | 0.139 | 0.9912 | 0.101 | 0.9807 | 0.850 | 0.9946 |
| | Serial (M=8) | 0.373 | 0.9912 | 0.124 | 1.0000 | 0.468 | 0.9857 |
| | Serial (M=8) | 0.113 | 0.9912 | 0.570 | 0.9952 | 0.370 | 0.9875 |
| AIS-31 | Disjointness test | N.P. | | N.P. | | Passed | |
| | Monobit test | N.P. | | N.P. | | 257/257 | |
| | Poker test | N.P. | | N.P. | | 257/257 | |
| | Runs test | N.P. | | N.P. | | 257/257 | |
| | Autocorrelation test | N.P. | | N.P. | | 257/257 | |
| | Uniform distribution test | N.P. | | N.P. | | 2/2 | |
| | Test for homogeneity | N.P. | | N.P. | | 2/2 | |
| | Entropy estimation | N.P. | | N.P. | | 1/1 | |

Table C.1: Summary of the results of selected tests of batteries particularly effective in detecting defects in TRNG. The *Alphabit* and *Rabbit* batteries belong to the TESTU01: critical results are if $\mathcal{P}$-val $\leq 10^{-3}$ or $\mathcal{P}$-val $\geq 0.990$. The NIST SP-800-22 suite has passing ratio critical values for the three sets equal to 0.95575, 0.96618 and 0.97674 respectively. The test on the distribution of p-values must be $\mathcal{P}$-val $\geq 10^{-5}$. The AIS31 suite could be applied only on the larger set of bits: as it can be seen all the 263 tests of this suite were passed (N.P. correspond to those tests which are not possible to apply because of the files size, however those tests are already covered by the other batteries.

# Appendix D

# Min and Max-entropy

We here briefly review the definition of conditional min- and max- entropies introduced in [144]. The conditional min-entropy of a bipartite quantum state $\rho_{AE}$ is defined as:

$$H_{\min}(A|E)_{\rho_{AE}} = \max_{\sigma_B} \sup\left\{\lambda \in \mathbb{R} \middle| \frac{\mathrm{Id}_A \otimes \sigma_E}{2^\lambda} \geq \rho_{AE}\right\}, \tag{D.1}$$

where $\sigma_E$ is a normalized positive state.

The conditional max-entropy is the dual of the min-entropy. In fact, by using a purification $\rho_{ABC}$ of $\rho_{AB}$, the max-entropy is defined by

$$H_{\max}(A|B)_{\rho_{AB}} = -H_{\min}(A|C)_{\rho_{AC}}\,, \tag{D.2}$$

where $\rho_{AB} = \mathrm{Tr}_C[\rho_{ABC}]$ and $\rho_{AC} = \mathrm{Tr}_B[\rho_{ABC}]$. We here recall that the purification of a state $\rho_{AB}$ is a pure state $\rho_{ABC}$ in the extended Hilbert space $A \otimes B \otimes C$, such that $\mathrm{Tr}_C[\rho_{ABC}] = \rho_{AB}$.

For the QRNG we need to evaluate the max-entropy for the state $\rho_X \equiv \sum_{x=0}^{d-1} p_x |x\rangle\langle x|$, where the space $B$ is a trivial space. By definition (D.2) we have:

$$H_{\max}(X)_{\rho_X} = -H_{\min}(A|C)_{\rho_{AC}} \tag{D.3}$$

with $\rho_{AC}$ a purification of $\rho_X$. A possible purification is given by

$$\rho_{AC} = |\Psi\rangle_{AC}\langle\Psi|\,, \qquad |\Psi\rangle_{AC} = \sum_{x=0}^{d-1} \sqrt{p_x}|x\rangle_A \otimes |v_x\rangle_C \tag{D.4}$$

with $\{|v_x\rangle\}$ on orthonormal basis on the space $C$ with dimension $d$. By (D.1) we have

$$\begin{aligned} H_{\max}(X)_{\rho_X} &= -H_{\min}(A|C)_{\rho_{AC}} \\ &= -\max_{\sigma_B} \sup\left\{\lambda \in \mathbb{R} \middle| \frac{\mathrm{Id}_A \otimes \sigma_C}{2^\lambda} \geq |\Psi\rangle\langle\Psi|\right\}, \end{aligned} \tag{D.5}$$

The state $\sigma_C$ that maximize min-entropy definition is $\sigma_C = \mathrm{Id}/d$. The maximum $\lambda$ such that $\mathrm{Id}_A \otimes \mathrm{Id}_C \geq d2^\lambda |\Psi\rangle\langle\Psi|$ is $\lambda = -\log_2[\sum_x (\sqrt{p_x})]^2$, such that

$$H_{\max}(X)_{\rho_X} = \log_2[\sum_x \sqrt{p_x}]^2 = 2\log_2 \sum_x \sqrt{p_x} = H_{1/2}(X) \tag{D.6}$$

# Appendix E

# Statistical tests of randomness for Qubit and Ququart

| Suite | Test | P-Value | Suite | Test | P-Value |
|---|---|---|---|---|---|
| Rabbit | MultinomialBitsOver | 0.94 | Alphabit | MultinomialBitsOver (L = 2) | 0.72 |
| | ClosePairsBitMatch (t=2) | 0.10 | | MultinomialBitsOver (L = 4) | 0.38 |
| | ClosePairsBitMatch (t=4) | 0.10 | | MultinomialBitsOver (L = 8) | 0.81 |
| | AppearanceSpacings | 0.76 | | MultinomialBitsOver (L = 16) | 0.38 |
| | LinearComp | 0.23 | | HammingIndep (L = 16) | 0.02 |
| | LempelZiv | 0.32 | | HammingIndep (L = 32) | 0.64 |
| | Fourier1 | 0.60 | | HammingCorr (L = 32) | 0.72 |
| | Fourier3 | 0.53 | | RandomWalk1 (L = 64) | 0.04 |
| | LongestHeadRun | 0.59 | | RandomWalk1 (L = 320) | 0.03 |
| | PeriodsInStrings | 0.950 | | Test | P-Val. Pass Ratio |
| | HammingWeight (L = 32) | 0.24 | SP-800-22 | Frequency | 0.066882 149/150 |
| | HammingCorr (L = 32) | 0.72 | | BlockFrequency | 0.299251 148/150 |
| | HammingCorr (L = 64) | 0.65 | | CumulativeSums | 0.431143 149/150 |
| | HammingCorr (L =128) | 0.54 | | CumulativeSums | 0.588652 148/150 |
| | HammingIndep (L = 16) | 0.02 | | Runs | 0.671779 150/150 |
| | HammingIndep (L = 32) | 0.64 | | LongestRun | 0.911413 149/150 |
| | HammingIndep (L = 64) | 0.89 | | Rank | 0.132132 149/150 |
| | AutoCor with a lag d = 1. | 0.79 | | FFT | 0.142602 148/150 |
| | AutoCor with a lag d = 2. | 0.86 | | NonOverlappingTemplate | 148/148 (subtests) |
| | Run | 0.20 | | OverlappingTemplate | 0.056546 150/150 |
| | MatrixRank (32 × 32) | 0.56 | | ApproximateEntropy | 0.520767 148/150 |
| | RandomWalk1 (L = 128) | 0.12 | | RandomExcursion | 26/26 (subtests) |
| | RandomWalk1 (L = 1024) | 0.12 | | Serial (M=16) | 0.712961 149/150 |
| | RandomWalk1 (L = 10016) | 0.01 | | Serial (M=16) | 0.236810 150/150 |
| | | | | LinearComplexity | 0.092784 148/150 |

Table E.1: (left) Summary of the results of selected tests of batteries particularly effective in detecting defects in TRNG. The *Alphabit* and *Rabbit* batteries belong to the TESTU01: critical results are if $\mathcal{P}$-val $\leq 10^{-3}$ or $\mathcal{P}$-val $\geq 0.990$. For tests which give more than a p-values, the smallest is reported . For NIST SP-800-22 suite, the file was partitioned in sub-strings 200 000 bits long for a total of 150 strings: this length was chosen in order to obtain a sample sizes enough large such that it is likely to fail the tests in case of poor randomness with a significance level of $\alpha = 0.01$; a test is failed if more than 6 strings fail it. In addition, a test is passed if the a chi-square test on the distribution of p-values, gives it self a p-value $\mathcal{P}$-val $\geq 10^{-5}$.

| Suite | Test | P-Value | Suite | Test | P-Value | |
|---|---|---|---|---|---|---|
| | MultinomialBitsOver | 0.27 | Alphabit | MultinomialBitsOver (L = 2) | 0.19 | |
| | ClosePairsBitMatch (t=2) | 0.20 | | MultinomialBitsOver (L = 4) | 0.23 | |
| | ClosePairsBitMatch (t=4) | 0.58 | | MultinomialBitsOver (L = 8) | 0.64 | |
| | AppearanceSpacings | 0.67 | | MultinomialBitsOver (L = 16) | 0.94 | |
| | LinearComp | 0.19 | | HammingIndep (L = 16) | 0.73 | |
| | LempelZiv | 0.84 | | HammingIndep (L = 32) | 0.73 | |
| | Fourier1 | 0.50 | | HammingCorr (L = 32) | 0.52 | |
| | Fourier3 | 0.38 | | RandomWalk1 (L = 64) | 0.29 | |
| | LongestHeadRun | 0.04 | | RandomWalk1 (L = 320) | 0.15 | |
| | PeriodsInStrings | 0.37 | | Test | P-Val. | Pass Ratio |
| Rabbit | HammingWeight (L = 32) | 0.51 | SP-800-22 | Frequency | 0.759756 | 97/100 |
| | HammingCorr (L = 32) | 0.52 | | BlockFrequency | 0.964295 | 100/100 |
| | HammingCorr (L = 64) | 0.70 | | CumulativeSums | 0.096578 | 97/100 |
| | HammingCorr (L =128) | 0.13 | | CumulativeSums | 0.911413 | 97/100 |
| | HammingIndep (L = 16) | 0.73 | | Runs | 0.779188 | 98/100 |
| | HammingIndep (L = 32) | 0.73 | | LongestRun | 0.494392 | 99/100 |
| | HammingIndep (L = 64) | 0.71 | | Rank | 0.011791 | 100/100 |
| | AutoCor with a lag d = 1. | 0.36 | | FFT | 0.657933 | 100/100 |
| | AutoCor with a lag d = 2. | 0.26 | | NonOverlappingTemplate | 148/148 (subtests) | |
| | Run | 0.02 | | OverlappingTemplate | 0.816537 | 99/100 |
| | MatrixRank (32 × 32) | 0.39 | | Universal | 0.289667 | 99/100 |
| | MatrixRank (320 × 320) | 0.84 | | ApproximateEntropy | 0.867692 | 100/100 |
| | RandomWalk1 (L = 128) | 0.21 | | RandomExcursion | 26/26 (subtests) | |
| | RandomWalk1 (L = 1024) | 0.51 | | Serial (M=16) | 0.798139 | 98/100 |
| | RandomWalk1 (L = 10016) | 0.24 | | Serial (M=16) | 0.514124 | 99/100 |
| | | | | LinearComplexity | 0.401199 | 100/100 |

Table E.2: Summary of the results of selected tests of batteries particularly effective in detecting defects in TRNG. The *Alphabit* and *Rabbit* batteries belong to the TESTU01: critical results are if $\mathcal{P}$-val $\leq 10^{-3}$ or $\mathcal{P}$-val $\geq 0.990$. For tests which give more than a p-values, the smallest is reported . For NIST SP-800-22 suite, the file was partitioned in sub-strings 400 000 bits long for a total of 100 strings: this length was chosen in order to obtain a sample sizes enough large such that it is likely to fail the tests in case of poor randomness with a significance level of $\alpha = 0.01$; a test is failed if more than 4 strings fail it. In addition, a test is passed if the a chi-square test on the distribution of p-values, gives it self a p-value $\mathcal{P}$-val $\geq 10^{-5}$.

## E. STATISTICAL TESTS OF RANDOMNESS FOR QUBIT AND QUQUART

# Bibliography


[1] Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Found. Comput. Sci. 1994 Proceedings., 35th Annu. Symp.*, pages 124–134. IEEE, 1994.

[2] Claude Elwood Shannon. Communication in the presence of noise. *Proc. IRE*, 37(1):10–21, 1949.

[3] Charles H Bennett and Gilles Brassard. Advances in Cryptology: Proceedings of Crypto84, August 1984, 1984.

[4] V Scarani and H Bechmann-Pasquinucci. The security of practical quantum key distribution. *Rev. Mod. ...*, pages 1–52, 2009.

[5] Momtchil Peev, Christoph Pacher, Romain Alléaume, Claudio Barreiro, Jan Bouda, W Boxleitner, Thierry Debuisschert, Eleni Diamanti, M Dianati, J F Dynes, and Others. The SECOQC quantum key distribution network in Vienna. *New J. Phys.*, 11(7):75001, 2009.

[6] Grégoire Ribordy, J-D Gautier, Nicolas Gisin, Olivier Guinnard, and Hugo Zbinden. Automated plug & playquantum key distribution. *Electron. Lett.*, 34(22):2116–2117, 1998.

[7] Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani, and Hugo Zbinden. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.*, 87(19):194108, 2005.

[8] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88(5):57902, 2002.

[9] Damien Stucki, Nino Walenta, Fabien Vannel, Robert Thomas Thew, Nicolas Gisin, Hugo Zbinden, S Gray, C R Towery, and S Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.*, 11(7):75003, 2009.

[10] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *arXiv Prepr. quant-ph/0101098*, 74:145–195, 2001.

[11] Masahide Sasaki, M Fujiwara, H Ishizuka, W Klaus, K Wakui, M Takeoka, S Miki, T Yamashita, Z Wang, A Tanaka, and Others. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express*, 19(11):10387–10409, 2011.

[12] Nicolas Gisin and Robert Thomas Thew. Quantum communication technology. *Electron. Lett.*, 46(14):965–967, 2010.

[13] Martin Pfennigbauer, Markus Aspelmeyer, Walter Leeb, Guy Baister, Thomas Dreischer, Thomas Jennewein, Gregor Neckamm, Josep Perdigues, Harald Weinfurter, and Anton Zeilinger. Satellite-based quantum communication terminal employing state-of-the-art technology. *J. Opt. Netw.*, 4(9):549–560, 2005.

[14] J P Bourgoin, E Meyer-Scott, Brendon L Higgins, B Helou, Chris Erven, Hannes Huebel, B Kumar, D Hudson, Ian D'Souza, Ralph Girard, and Others. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication. *New J. Phys.*, 15(2):23006, 2013.

[15] Thomas Jennewein and Brendon Higgins. The quantum space race. *Phys. World*, 26:52–56, 2013.

[16] P. Villoresi, T Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, a. Zeilinger, and C. Barbieri. Experimental verification of the feasibility of a quantum channel between space and Earth. *New J. Phys.*, 10:1–22, 2008.

[17] Giuseppe Vallone, Davide Bacco, Daniele Dequal, Simone Gaiarin, Vincenza Luceri, Giuseppe Bianco, and Paolo Villoresi. Experimental Satellite Quantum Communications. *arXiv Prepr. arXiv1406.4051*, 2014.

[18] Christian Kurtsiefer, P Zarda, Matthus Halder, H Weinfurter, P M Gorman, P R Tapster, and J G Rarity. Quantum cryptography: A step towards global key distribution. *Nature*, 419(6906):450, 2002.

[19] T Schmitt-Manderbach, H Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, T Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John Rarity, Anton Zeilinger, and Harald Weinfurter. Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. *Phys. Rev. Lett.*, 98(1):010504, January 2007.

[20] R Ursin, F Tiefenbacher, T Schmitt-Manderbach, H Weier, T Scheidl, M Lindenthal, B Blauensteiner, T Jennewein, J Perdigues, P Trojek, and Others. Entanglement-based quantum communication over 144 km. *Nat. Phys.*, 3(7):481–486, 2007.

[21] Artur K Ekert. Quantum cryptography based on Bells theorem. *Phys. Rev. Lett.*, 67(6):661, 1991.

[22] Valerio Scarani, Antonio Acin, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92(5):57901, 2004.

[23] Xiang-Bin Wang. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Phys. Rev. A*, 72(1):12322, 2005.

[24] Patrick J Clarke, Robert J Collins, Philip A Hiskett, María-José García-Martínez, Nils J Krichel, Aongus McCarthy, Michael G Tanner, John A O'Connor, Chandra M Natarajan, Shigehito Miki, and Others. Analysis of detector performance in a gigahertz clock rate quantum key distribution system. *New J. Phys.*, 13(7):75008, 2011.

[25] M J García-Martínez, N Denisenko, D Soto, D Arroyo, A B Orue, and V Fernandez. High-speed free-space quantum key distribution system for urban daylight applications. *Appl. Opt.*, 52(14):3311–3317, 2013.

[26] M Jofre, A Gardelein, G Anzolin, G Molina-Terriza, J P Torres, M W Mitchell, and V Pruneri. 100 MHz amplitude and polarization modulated optical source for free-space quantum key distribution at 850 nm. *J. Light. Technol.*, 28(17):2572–2578, 2010.

[27] Z L Yuan, A R Dixon, J F Dynes, A W Sharpe, and A J Shields. Gigahertz quantum key distribution with InGaAs avalanche photodiodes. *Appl. Phys. Lett.*, 92(20):201104, 2008.

[28] Ronald L Fante. Electromagnetic beam propagation in turbulent media-An update. In *IEEE Proc.*, volume 68, pages 1424–1443, 1980.

[29] Sebastian Nauerth, Florian Moll, Markus Rau, Christian Fuchs, Joachim Horwath, Stefan Frick, and Harald Weinfurter. Air-to-ground quantum communication. *Nat. Photonics*, 7(5):382–386, 2013.

[30] Andrey Nikolaevich Kolmogorov. The local structure of turbulence in incompressible viscous fluid for very large Reynolds numbers. In *Dokl. Akad. Nauk SSSR*, volume 30, pages 299–303, 1941.

[31] T Schmitt-Manderbach. Long distance free-space quantum key distribution, 2007.

[32] T Schmitt-Manderbach. *Long distance free-space quantum key distribution.* PhD thesis, 2007.

[33] Ivan Capraro, Andrea Tomaello, Alberto DallArche, Francesca Gerlin, Ruper Ursin, G. Vallone, and P. Villoresi. Impact of Turbulence in Long Range Quantum and Classical Communications. *Phys. Rev. Lett.*, 109(20):200502, November 2012.

[34] Andrea Tomaello. Quantum communication channels between earth and space and space to earth. 2012.

[35] Alberto Dall'Arche. Advanced techniques for quantum communications in free-space channels. 2014.

[36] S. J. van Enk, J. I. Cirac, and P. Zoller, Science **279**, 205 (1998).

[37] C. H. Bennett and P. W. Shor, Science **284**, 747 (1999).

[38] H. Lo and H. F. Chau, Science **283**, 2050 (1999).

[39] R. Hughes and J. Nordholt, Science (New York, N.Y.) **333**, 1584 (2011).

[40] Europe: http://qurope.eu/content/Roadmap and and in particular http://qurope.eu/content/416-towards-long-distances-satellite-quantum-communication;

[41] Japan: http://qict.nict.go.jp/about/50roadmap.html

[42] H. Xin, Science (New York, N.Y.) **332**, 904 (2011).

[43] B. C. Jacobs and J. D. Franson, Optics Letters **21**, 1854 (1996).

[44] W. Buttler, *et al.*, Physical Review Letters **81**, 3283 (1998).

[45] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, New J. Phys. **4**, 43 (2002).

[46] J. E. Nordholt, R. J. Hughes, G. L. Morgan, C. G. Peterson, and C. C. Wipf, in G. S. Mecherle, editor, *Proc. SPIE 4635*, 116–126 (2002).

[47] D. Elser, T. Bartley, B. Heim, C. Wittmann, D. Sych, and G. Leuchs, New Journal of Physics **11**, 045014 (2009).

[48] M. Peev, *et al.*, New Journal of Physics **11**, 075001 (2009).

[49] A. Fedrizzi, *et al.*, Nature Physics **5**, 389 (2009).

[50] M. García-Martínez, N. Denisenko, D. Soto, D. Arroyo, A. B. Orue, and V. Fernandez, Applied Optics **52**, 3311 (2013).

[51] C. Peuntinger, B. Heim, C. R. Müller, C. Gabriel, C. Marquardt, and G. Leuchs, Physical Review Letters **113**, 060502 (2014).

[52] G. Vallone, V. DAmbrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, Physical Review Letters **113**, 060503 (2014).

[53] A. A. Semenov and W. Vogel, Physical Review A **80**, 021802 (2009).

[54] A. A. Semenov and W. Vogel, Phys. Rev. A **81**, 23835 (2010).

[55] C. Erven, B. Heim, E. Meyer-Scott, J. P. Bourgoin, R. Laflamme, G. Weihs, and T. Jennewein, New Journal of Physics **14**, 123018 (2012).

[56] J. Bae and A. Acín, Physical Review A **75**, 012334 (2007).

[57] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, Physical Review A **76**, 032312 (2007).

[58] U. Maurer, IEEE Transactions on Information Theory **39**, 733 (1993).

[59] I. Capraro, A. Tomaello, A. Dall'Arche, F. Gerlin, R. Ursin, G. Vallone, and P. Villoresi, Phys. Rev. Lett. **109**, 200502 (2012).

[60] F. T. Feng Tang and B. Z. Bing Zhu, Chinese Optics Letters **11**, 090101 (2013).

[61] P. W. Milonni, J. H. Carter, C. G. Peterson, and R. J. Hughes, Journal of Optics B: Quantum and Semiclassical Optics **6**, S742 (2004).

[62] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, 175, IEEE, New York (1984).

[63] D. Bacco, M. Canale, N. Laurenti, G. Vallone, and P. Villoresi, Nature Communications **4**, 2363 (2013).

[64] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nature Communications **3**, 634 (2012).

[65] C.S. Petrie and J.a. Connelly. A noise-based IC random number generator for applications in cryptography. *IEEE Trans. Circuits Syst. I Fundam. Theory Appl.*, 47(5):615–621, May 2000.

[66] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter. Ultrahigh-Speed Random Number Generation Based on a Chaotic Semiconductor Laser. *Phys. Rev. Lett.*, 103(2):024102, July 2009.

[67] Berk Sunar, William Martin, and Douglas Stinson. A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks. *IEEE Trans. Comput.*, 56(1):109–119, January 2007.

[68] Toni Stojanovski and L Kocarev. Chaos-based random number generators-part I: analysis [cryptography]. *IEEE Trans. Circuits Syst. I Fundam. Theory Appl.*, 48(3):281–288, March 2001.

[69] Werner Schindler. Evaluation Criteria for Physical Random Number Generators. In *Cryptogr. Eng.*, pages 25–54. Springer, 2009.

[70] Markus Dichtl. How to predict the output of a hardware random number generator. In *Cryptogr. Hardw. Embed. Syst. 2003*, pages 181–188. Springer, 2003.

[71] Persi Diaconis, Susan Holmes, and Richard Montgomery. Dynamical bias in the coin toss. *SIAM Rev.*, 49(2):211–235, 2007.

[72] Ronald L Fante. Electromagnetic beam propagation in turbulent media. In *IEEE Proc.*, volume 63, pages 1669–1692, 1975.

[73] Larry C Andrews and Ronald L Phillips. *Laser beam propagation through random media*, volume 152. SPIE press, 2005.

[74] Pierre Barthelemy, Jacopo Bertolotti, and DS Wiersma. A Lévy flight for light. *Nature*, 453(7194):495–8, May 2008.

[75] J. W. Goodman. Some fundamental properties of speckle. *J. Opt. Soc. Am.*, 66(11):1145, November 1976.

[76] Joseph Marron, Anthony J. Martino, and G M Morris. Generation of random arrays using clipped laser speckle. *Appl. Opt.*, 25(1):26, January 1986.

[77] Roarke Horstmeyer, Richard Y Chen, Benjamin Judkewitz, and Changhuei Yang. Markov speckle for efficient random bit generation. *Opt. Express*, 20(24):26394–410, November 2012.

[78] Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. Physical one-way functions. *Science*, 297(5589):2026–30, September 2002.

[79] T Scheidl, Rupert Ursin, Johannes Kofler, Sven Ramelow, Xiao-Song Ma, Thomas Herbst, Lothar Ratschbacher, Alessandro Fedrizzi, Nathan K Langford, T Jennewein, and Others. Violation of local realism with freedom of choice. *Proc. Natl. Acad. Sci.*, 107(46):19708–19713, 2010.

[80] Xiao-Song Ma, Thomas Herbst, T Scheidl, Daqing Wang, Sebastian Kropatschek, William Naylor, Bernhard Wittmann, Alexandra Mech, Johannes Kofler, Elena Anisimova, and Others. Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 489(7415):269–273, 2012.

[81] Sabino Piazzolla. 8 Atmospheric Channel. *Near-Earth Laser Commun.*, page 237, 2008.

[82] A Comeron, J Bara, A. Belmonte, D. Ruiz, and R. Czichy. Inter-islands optical link tests. *IEEE Photonics Technol. Lett.*, 2(5):380–381, May 1990.

[83] P Elias. The efficient construction of an unbiased random sequence. *Ann. Math. Stat.*, 43(3):865–870, 1972.

[84] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 2010.

[85] Richard Simard and Pierre L'Ecuyer. Test U01: A Software Library in ANSI C for Empirical Testing of Random Number Generators. 2009.

[86] Andrew Rukhin, Juan Soto, James Nechvatal, M Smid, and E Barker. A statistical test suite for random and pseudorandom number generators for cryptographic applications. *NIST Spec. Publ. 800-22 Revis. 1a*, (April), 2010.

[87] W Killmann and W Schindler. A proposal for: Functionality classes for random number generators. (September), 2011.

[88] Atsushi Uchida, Kazuya Amano, Masaki Inoue, Kunihito Hirano, Sunao Naito, Hiroyuki Someya, Isao Oowada, Takayuki Kurashige, Masaru Shiki, Shigeru Yoshimori, Kazuyuki Yoshimura, and Peter Davis. Fast physical random bit generation with chaotic semiconductor lasers. *Nat. Photonics*, 2(12):728–732, November 2008.

[89] F Devos, P Garda, and P Chavel. Optical generation of random-number arrays for on-chip massively parallel Monte Carlo cellular processors. *Opt. Lett.*, 12(3):152–4, March 1987.

[90] Ph. Lalanne, H Richard, JC Rodier, P. Chavel, J. Taboury, K. Madani, P. Garda, and F. Devos. 2-D generation of random numbers by multimode fiber speckle for silicon arrays of processing elements. *Opt. Commun.*, 76(5-6):387–394, May 1990.

[91] Mathilde Soucarros, Cecile Canovas-Dumas, Jessy Clediere, Philippe Elbaz-Vincent, and Denis Real. Influence of the temperature on true random number generators. In *2011 IEEE Int. Symp. Hardware-Oriented Secur. Trust*, pages 24–27. IEEE, June 2011.

[92] Juan Yin, Ji-Gang Ren, He Lu, Yuan Cao, Hai-Lin Yong, Yu-Ping Wu, Chang Liu, Sheng-Kai Liao, Fei Zhou, Yan Jiang, Xin-Dong Cai, Ping Xu, Ge-Sheng Pan, Jian-Jun Jia, Yong-Mei Huang, Hao Yin, Jian-Yu Wang, Yu-Ao Chen, Cheng-Zhi Peng, and Jian-Wei Pan. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature*, 488(7410):185–8, August 2012.

[93] Bruce J Berne and Robert Pecora. *Dynamic light scattering: with applications to chemistry, biology, and physics*. Courier Dover Publications, 2000.

[94] Hector J Rabal and Roberto A Braga Jr. *Dynamic laser speckle and applications*. CRC Press, 2010.

[95] Kyle M. Douglass, Sergey Sukhov, and Aristide Dogariu. Superdiffusion in optically controlled active media. *Nat. Photonics*, 6(12):834–837, November 2012.

[96] Jan Krhovják, V Matyas, and P Svenda. The sources of randomness in mobile devices. *Proceeding Nord.*, pages 73–84, 2007.

[97] P S Laplace, F W Truscott, and F L Emory. *A Philosophical Essay on Probabilities: With an Introductory Note by E. T. Bell*. Dover, 1951.

[98] HF Murry. A general approach for generating natural random variables. *Comput. IEEE Trans.*, (December):1210–1213, 1970.

[99] CH Vincent. The generation of truly random binary numbers. *J. Phys. E.*, 1970.

[100] H Inoue, H Kumahora, Y Yoshizawa, M Ichimura, and O Miyatake. Random numbers generated by a physical device. *Appl. Stat.*, pages 115–120, 1983.

[101] J G Rarity, P C M Owens, and P R Tapster. Quantum random-number generation and key sharing. *J. Mod. Opt.*, 41(12):2435–2444, 1994.

[102] Thomas Jennewein, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. A fast and compact quantum random number generator. *Rev. Sci. Instrum.*, 71(4):1675, 2000.

[103] André Stefanov, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard, and Hugo Zbinden. Optical Quantum Random Number Generator. *Syst. Sci.*, 47(0):3, 1999.

[104] Ma Hai-Qiang, Wang Su-Mei, Zhang Da, Chang Jun-Tao, Ji Ling-Ling, Hou Yan-Xue, and Wu Ling-An. A Random Number Generator Based on Quantum Entangled Photon Pairs. *Chinese Phys. Lett.*, 21(10):1961, 2004.

[105] M. Fiorentino, C. Santori, S. Spillane, R. Beausoleil, and W. Munro. Secure self-calibrating quantum random-bit generator. *Phys. Rev. A*, 75(3):032334, March 2007.

[106] Mario Stipcevic and B Medved Rogina. Quantum random number generator based on photonic emission in semiconductors. *Rev. Sci. Instrum.*, 78(4):45104, 2007.

[107] Martin Fürst, H Weier, Sebastian Nauerth, D. G. Marangon, Christian Kurtsiefer, and Harald Weinfurter. High speed optical quantum random number generation. *Opt. Express*, 18(12):13029–37, June 2010.

[108] Michael Wahl, Matthias Leifgen, Michael Berlin, Tino Rohlicke, Hans-Jurgen Rahn, and Oliver Benson. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. *Appl. Phys. Lett.*, 98(17):171105, 2011.

[109] Christian Gabriel, Christoffer Wittmann, Denis Sych, Ruifang Dong, Wolfgang Mauerer, Ulrik L Andersen, Christoph Marquardt, and G Leuchs. A generator for unique quantum random numbers based on vacuum states. *Nat. Photonics*, 4(10):711–715, August 2010.

[110] Hong Guo, Wenzhuo Tang, Y. Liu, and Wei Wei. Truly random number generation based on measurement of phase noise of a laser. *Phys. Rev. E*, 81(5):051137, May 2010.

[111] Bing Qi, Yue-Meng Chi, Hoi-Kwong Lo, and Li Qian. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Opt. Lett.*, 35(3):312–4, February 2010.

[112] F Xu, Bing Qi, Xiongfeng Ma, He Xu, Haoxuan Zheng, and HK Lo. Ultrafast quantum random number generation based on quantum phase fluctuations. *Opt. Express*, 732(2008):728–732, September 2012.

[113] Xiongfeng Ma, Feihu Xu, He Xu, Xiaoqing Tan, Bing Qi, and Hoi Kwong Lo. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A - At. Mol. Opt. Phys.*, 87:25, July 2013.

[114] M Jofre, M Curty, F Steinlechner, and V Pruneri. True random numbers from amplified quantum vacuum. *Opt. ...*, pages 1–11, 2011.

[115] C. Abellán, W. Amaya, M Jofre, M. Curty, A Acín, J. Capmany, V Pruneri, and M. W. Mitchell. Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. *Opt. Express*, 22(2):1645, January 2014.

[116] A. Uchida, Toshimori Honjo, and Kazuya Amano. Fast physical random bit generator based on chaotic semiconductor lasers: Application to quantum cryptography. *... Eur. Quantum ...*, 728(2008):22317, 2009.

[117] Y. X. Wang, Pu Li, and Jian-Zhong Zhang. Fast random bit generation in optical domain with ultrawide bandwidth chaotic laser. *Photonics Technol. Lett. IEEE*, 22(22):1680–1682, 2010.

[118] André Stefanov, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard, and Hugo Zbinden. Optical quantum random number generator. *J. Mod. Opt.*, 47(4):595–598, 2000.

[119] Roger Colbeck. Quantum and relativistic protocols for secure multi-party computation. *arXiv Prepr. arXiv0911.3814*, (December), 2009.

[120] S Pironio, A Acín, S Massar, a Boyer de la Giroday, D N Matsukevich, P Maunz, S Olmschenk, D Hayes, L Luo, T a Manning, and C Monroe. Random numbers certified by Bell's theorem. *Nature*, 464(7291):1021–4, April 2010.

[121] Roger Colbeck and R. Renner. Free randomness can be amplified. *Nat. Phys.*, 8(6):450–454, May 2012.

[122] Rodrigo Gallego, Lluis Masanes, Gonzalo De La Torre, Chirag Dhara, Leandro Aolita, and A Acín. Full randomness from arbitrarily deterministic events. *Nat Commun*, 4, October 2013.

[123] B G Christensen, K T McCusker, J B Altepeter, B Calkins, T Gerrits, A E Lita, A Miller, L K Shalm, Y Zhang, S W Nam, and Others. Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.*, 111(13):130406, 2013.

[124] Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner. Leftover hashing against quantum side information. *Inf. Theory, IEEE Trans.*, 57(8):5524–5535, 2011.

[125] Daniela Frauchiger, R. Renner, and Matthias Troyer. True randomness from realistic quantum devices. *arXiv Prepr. arXiv1311.4547*, pages 1–20, 2013.

[126] Marco Tomamichel and R. Renner. Uncertainty Relation for Smooth Entropies. *Phys. Rev. Lett.*, 106(11):110506, March 2011.

[127] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Review of Scientific Instruments **71**, 1675 (2000).

[128] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, Physical Review A **75**, 032334 (2007).

[129] W. Wei and H. Guo, Optics Letters **34**, 1876 (2009).

[130] K. Svozil, Physical Review A **79**, 054306 (2009).

[131] M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, Optics Express **18**, 13029 (2010).

[132] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, Optics Express **19**, 20665 (2011).

[133] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita, and A. Acín, Nature Communications **4**, 2654 (2013).

[134] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, Optics Express **22**, 1645 (2014).

[135] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature (London) **464**, 1021 (2010).

[136] C. Dhara, G. Prettico, and A. Acín, Physical Review A **88**, 052116 (2013).

[137] R. Colbeck, *Quantum And Relativistic Protocols For Secure Multi-Party Computation*, Ph.D. thesis (2006), [arXiv:0911.3814v2].

[138] R. Colbeck and A. Kent, Journal of Physics A: Mathematical and Theoretical **44**, 095305 (2011).

[139] U. Vazirani and T. Vidick, Philosophical transactions. Series A, Mathematical, physical, and engineering sciences **370**, 3432 (2012).

[140] S. Pironio and S. Massar, Physical Review A **87**, 012336 (2013).

[141] R. Colbeck and R. Renner, Nature Physics **8**, 450 (2012).

[142] D. Frauchiger, R. Renner, and M. Troyer, [arXiv:1311.4547] (2013).

[143] A. De, C. Portmann, T. Vidick, and R. Renner, SIAM Journal on Computing **41**, 915 (2012).

[144] R. Konig, R. Renner, and C. Schaffner, IEEE Transactions on Information Theory **55**, 4337 (2009).

[145] Y. Zhao, C.-H. Fung, B. Qi, C. Chen, and H.-K. Lo, Physical Review A **78**, 042333 (2008).

[146] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photonics **4**, 686 (2010).

[147] F. Xu, B. Qi, and H.-K. Lo, New Journal of Physics **12**, 113026 (2010).

[148] L. Lydersen, V. Makarov, and J. Skaar, Phys. Rev. A **83**, 032306 (2011).

[149] M. Tomamichel and R. Renner, Physical Review Letters **106**, 110506 (2011).

[150] J. Renes and J.-C. Boileau, Physical Review Letters **103**, 020402 (2009).

[151] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nature Physics **6**, 659 (2010).

[152] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).

[153] D. Holste, I. Groß e, and H. Herzel, Journal of Physics A: Mathematical and General **31**, 2551 (1998).

[154] N. Beaudry, T. Moroder, and N. Lütkenhaus, Physical Review Letters **101**, 093601 (2008).

[155] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, Physical Review A **89**, 012325 (2014).

[156] F. Steinlechner, P. Trojek, M. Jofre, H. Weier, D. Perez, T. Jennewein, R. Ursin, J. Rarity, M. W. Mitchell, J. P. Torres, H. Weinfurter, and V. Pruneri, Optics Express **20**, 9640 (2012).

[157] F. Steinlechner, S. Ramelow, M. Jofre, M. Gilaberte, T. Jennewein, J. P. Torres, M. W. Mitchell, and V. Pruneri, Optics Express **21**, 11943 (2013).

[158] L. Trevisan, Journal of the ACM **48**, 860 (2001).

[159] E. Rukhin, Andrew and Soto, Juan and Nechvatal, James and Smid, M and Barker, NIST Special Publication 800-22 Revision 1a (2010).

[160] P. L'Ecuyer and R. Simard, ACM Transactions on Mathematical Software **33**, 22 (2007).

[161] Christian Weedbrook, AM Lance, and WP Bowen. Quantum cryptography without switching. *arXiv Prepr. quant-ph/ ...*, pages 1–4, 2004.

[162] T Symul, S M Assad, and P. K. Lam. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Appl. Phys. Lett.*, (1):2–5, July 2011.

[163] F Furrer, Mario Berta, Marco Tomamichel, Volkher B. Scholz, and Matthias Christandl. Position-momentum uncertainty relations in the presence of quantum memory. *J. Math. Phys.*, 55(12):122205, December 2014.

[164] Mario Berta, Matthias Christandl, F Furrer, Volkher B. Scholz, and Marco Tomamichel. Continuous Variable Entropic Uncertainty Relations in the Presence of Quantum Memory. *arXiv:1308.5427*, page 27, August 2013.

[165] T Eberle, V Händchen, and Roman Schnabel. Stable control of 10 dB two-mode squeezed vacuum states of light. *Opt. Express*, 21(9):11546–11553, 2013.

[166] Athanasios Papoulis and S Unnikrishna Pillai. *Probability, random variables, and stochastic processes*. Tata McGraw-Hill Education, 2002.

[167] Yong Shen, Liang Tian, and Hongxin Zou. Practical quantum random number generator based on measuring the shot noise of vacuum states. *Phys. Rev. A*, 81(6):063814, June 2010.

[168] Hans-A Bachor and Timothy C Ralph. A Guide to Experiments in Quantum Optics, 2nd. *A Guid. to Exp. Quantum Opt. 2nd, Revis. Enlarg. Ed. by Hans-A. Bachor, Timothy C. Ralph, pp. 434. ISBN 3-527-40393-0. Wiley-VCH, March 2004.*, 1, 2004.

[169] Malcolm B Gray, Daniel A Shaddock, Charles C Harb, and Hans-A Bachor. Photodetector designs for low-noise, broadband, and high-power applications. *Rev. Sci. Instrum.*, 69(11):3755–3762, 1998.

[170] W Schindler and W Killmann. Evaluation Criteria for True ( Physical ) Random Number Generators Used in Cryptographic Applications Generators : Main Differences.

[171] W Schindler and W Killmann. Evaluation criteria for true (physical) random number generators used in cryptographic applications. *Cryptogr. Hardw. Embed. ...*, pages 431–449, 2003.