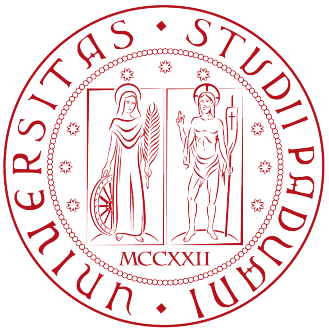


UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Fisica e Astronomia "Galileo Galilei"

Dipartimento di Ingegneria dell'Informazione

Corso di Laurea in Fisica

Tesi di Laurea

Quantum random number generation by using POVM

Relatore

Prof. Giuseppe Vallone

Correlatore

Dr. Marco Avesani

Laureando

Paolo Frazzetto

Anno Accademico 2017/2018

The generation of random numbers is too important to be left to chance
— Robert R. Coveyou, Oak Ridge National Laboratory, 1969

Abstract

The generation of random numbers goes beyond pure academic interests: random numbers are required for countless application, such as cryptography, simulations or gambling. However, most of these numbers are currently generated by implementing mathematical algorithms leading to limited security, incorrect results or predictable outcomes. Actually, true randomness is found only at microscopic level, where Nature obeys to the laws of Quantum Mechanics. In this thesis, after an overview about the theory of Quantum Information, the state of the art of this filed is presented. Eventually, a new Quantum Random Number Generator protocol is proposed and its implementation is being studied in order to get secure and reliable random strings. This work has been carried out in the framework of the "QuantumFuture" Research Group of the University of Padua.

Sommario

La generazione di numeri casuali va oltre il puro interesse accademico: i numeri casuali sono richiesti per innumerevoli applicazioni, come la criptografia, simulazioni o gioco d'azzardo. Ad ogni modo, la maggior parte di questi numeri sono attualmente generati da algoritmi matematici che portano a sicurezza limitata, risultati incorretti o esiti prevedibili. In realtà, la vera casualità si trova solamente a livello microscopico, dove la Natura segue le leggi della Meccanica Quantistica. In questa tesi, dopo una panoramica sulla teoria dell'Informazione Quantistica, viene presentato lo stato dell'arte di questo campo. Infine, si propone un nuovo Generatore Quantistico di Numeri Casuali e se ne studia la sua implementazione per ottenere bit casuali sicure e affidabili. Questo lavoro è stato realizzato nel contesto del Gruppo di Ricerca "QuantumFuture" dell'Università di Padova.

Ringraziamenti

Ci tengo a ringraziare esplicitamente il dott. Marco Avesani e il dott. Hamid Tebyanian per il loro fondamentale aiuto prestato in laboratorio e per avermi fatto da guida nel mondo dell'Informazione Quantistica. Grazie anche a tutti i dottorandi del gruppo QuantumFuture che hanno reso questa esperienza piacevole, stimolante e produttiva.

Contents

Chapter 1

Introduction to Quantum Information

Since the dawn of computer science and information theory in the 1940s, computers and electronics have been becoming more and more relevant in our society. In fact, we are now living in the *Information Age* characterized by the acquisition, storage and manipulation of all kind of data. Quantum information and computation are the study of these processes and tasks that can be accomplished using quantum-mechanical phenomena [1].

In this chapter, after a short introduction on qubits and quantum optics, the required theoretical framework to treat these kind of quantum systems is presented. Eventually, we will be dealing with the concept of randomness and the operative quantity used to describe it, *entropy*.

1.1 The Qubit

While the fundamental unit of classical information is the *bit*, whose value can be either 0 or 1, in quantum information it is the *qubit*. The two possible states of a qubit are represented as $|0\rangle$ and $|1\rangle$, in analogy with the classical bit; but unlike a classical system where the bit would have to be in one state or the other, the remarkable properties of quantum mechanics allow the qubit to be in a linear *superposition* of states, so that the most general state $|\psi\rangle$ can be written as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha, \beta \in \mathbb{C} \tag{1.1}$$

This property is fundamental to quantum computing: in this way, the state of a qubit is a vector in a two-dimensional complex vector, where the states $|0\rangle$ and $|1\rangle$ form an orthonormal base for this space and they are called *computational basis states*. However, just as the bit, the measurement of a qubit must be either $|0\rangle$ with probability $|\alpha|^2$, or $|1\rangle$ with probability $|\beta|^2$. Consequentially, $|\alpha|^2 + |\beta|^2 = 1$ since the total probability must sum to one, and the qubit general state is therefore a unit vector. It is because of these underlying probabilities that qubits can be used to get random numbers, exploiting this intrinsic randomness of quantum mechanics.

Given these conditions, Eq. 1.1 can be rewritten as:

$$|\psi\rangle = e^{i\gamma}\Big(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\Big) \qquad \gamma, \theta, \varphi \in \mathbb{R} \tag{1.2}$$

In quantum mechanics, the global phase $e^{i\gamma}$ can be ignored since it does not result in observable effects as physical states are determined by ray vectors on a Hilbert space. From Eq. 1.2 it follows that the qubit can be geometrically represented as a point on the surface of a 3-dimensional sphere, as known as the *Bloch Sphere*, shown in Fig. 1.1. This useful depiction illustrates once more that the qubit can

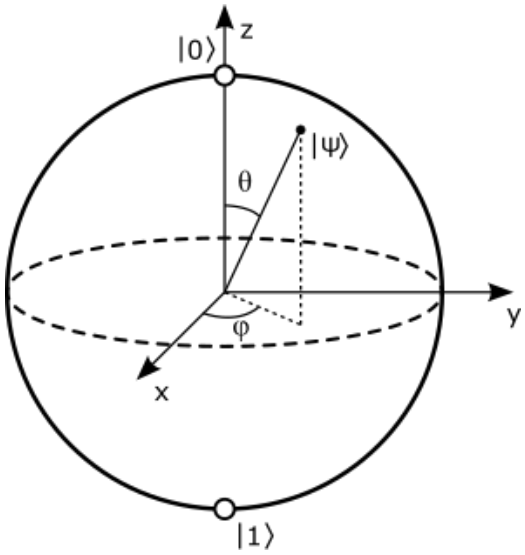


Figure 1.1: Qubit representation in the Bloch Sphere

span an infinite continuous set of states, the sphere surface, and this means that in principle it could be possible to store an infinite amount of information. However, accessing (by measuring) this information will cause the collapse of the state into one of its eigenstates, giving only a single-bit outcome. What are the advantages of qubits then?
The relevant point is that until a measurement is performed, *all* information is preserved and the states evolve accordingly the laws of quantum mechanics, so in manners that would not be classically possible (counterintuitively, the measurement actually decreases information).

In practice any quantum two level system, such as the electronic spin, can be consider as a qubit. For the sake of this work, qubits are physically implemented by single photon polarization and here the computational basis states can be choose as the horizontal $|H\rangle = |0\rangle$ and vertical $|V\rangle = |1\rangle$ polarization.

1.2 Polarization and Quantum Optics

Classically, the polarization of light is defined as the time evolution of the direction of the electric field vector. Given a monochromatic plane wave of a certain frequency ν traveling in the z direction with velocity c, the electric field vector lies in the x-y plane, it traces an ellipse and it is characterized by the amplitude a and phase φ of oscillations in the two components of the polarization plane. This can be conveniently represented in the form of a complex vector, known as *Jones vector* [2]:

$$\mathbf{J} = \begin{pmatrix} A_x \\ A_y \end{pmatrix} \quad \text{with} \quad A_i = a_i e^{i\varphi} \in \mathbb{C} \tag{1.3}$$

Some special polarization states, their Jones vector representation and corresponding bra-ket notation are shown in Tab. 1.1. From a quantum perspective, photons can have two helicities corresponding

to two orthogonal quantum states $|L\rangle$ and $|R\rangle$. More generally, it can be in any superposition state $\alpha|L\rangle + \beta|R\rangle$, providing the linear, circular, or elliptical polarization.

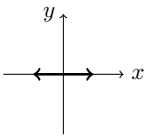
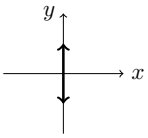
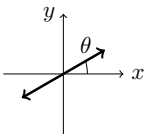
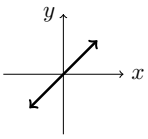
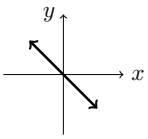
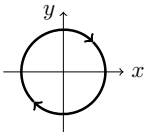
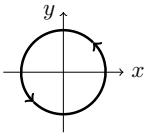
Polarization States		**Jones Vectors**	**Ket Notation**
Linearly pol. wave in x direction		$\begin{pmatrix}1\\0\end{pmatrix}$	$\|H\rangle$
Linearly pol. wave in y direction		$\begin{pmatrix}0\\1\end{pmatrix}$	$\|V\rangle$
Linearly pol. wave at angle θ from x axis		$\begin{pmatrix}\cos\theta\\\sin\theta\end{pmatrix}$	$\cos\theta\|H\rangle + \sin\theta\|V\rangle$
Linearly pol. wave at 45° with x axis		$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$	$\|+\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$
Linearly pol. wave at −45° with x axis		$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$	$\|-\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$
Right circularly pol. wave		$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$	$\|R\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - i\|V\rangle)$
Left circularly pol. wave		$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$	$\|L\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + i\|V\rangle)$

Table 1.1: Polarization states

This vectorial formalism is suitable for modeling optical system in which the polarization of the incoming wave is altered by polarizers or phase retarders, since they can be similarly written in matrix notation by defining a 2×2 *Jones matrix* $\mathbf{T}$ so that:

$$\mathbf{J_{out}} = \mathbf{T}\mathbf{J_{in}} \tag{1.4}$$

Hence, the combination of optical devices is reduced to matrix multiplication so that one can easily determine the final wave state from any given input. The following is a list of some of these simple devices and their corresponding Jones matrices, under the assumption that the optical axis is vertical in the considered frame of reference:

Linear Polarizers As the name suggests, these devices linearly polarize the wave along a specific direction. For example, for a ideal linear horizontal (LHP) and linear vertical (LVP) polarizer

the Jones matrices are respectively:

$$\mathbf{T_{LHP}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \mathbf{J_{LVP}} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{1.5}$$

Quarter-wave plate QWP It converts a $\pm 45°$ linearly polarized light into circularly polarized light and vice versa, while for other angles the output will be elliptically polarized:

$$\mathbf{T_{QWP}} = e^{\mp i\pi/4} \begin{pmatrix} 1 & 0 \\ 0 & \pm i \end{pmatrix} \tag{1.6}$$

Half-wave plate HWP It rotates the plane of polarization by 90°, thus transforming $|H\rangle$ into $|V\rangle$ or $|R\rangle$ into $|L\rangle$ and vice versa:

$$\mathbf{T_{HWP}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1.7}$$

In conclusion, if the coordinate system is not aligned with the devices optical axes, the Jones matrices can be composed with an appropriate change of the reference system:

$$\begin{cases} \mathbf{J}' = \mathbf{R}(\theta)\mathbf{J} \\ \mathbf{T}' = \mathbf{R}(\theta)\mathbf{T}\mathbf{R}(-\theta) \end{cases} \qquad \text{with} \quad \mathbf{R}(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \tag{1.8}$$

1.3 The Density Matrix

When doing experiments, one must take into account that the state of a physical system is often not perfectly determined. In fact, the information about the system could be *incomplete* since the experimenter does not know which particular states are being manipulated. This is a common situation in quantum information applications, for instance we may not control the state source or if our pure state is actually not isolated and interacts with another system.
We consider that the system is in a state taken from the ensemble

$$\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_d\rangle\} \tag{1.9}$$

with probabilities $\{p_1, p_2 \ldots, p_d\}$ satisfying the condition $\sum_i p_i = 1$, so the pure states $|\psi_k\rangle$ constitute what is called a *mixed state* with weights p_k. In order to treat this within the laws of quantum mechanics, it is necessary to introduce the *density operator* ρ defined as [3]:

$$\rho := \sum_k p_k |\psi_k\rangle\langle\psi_k| \tag{1.10}$$

Given a generic orthonormal basis $\{|i\rangle\}$, this operator can be consistently represented as a matrix, kmown as the *density matrix*, that has elements

$$\rho_{ij} = \langle i|\rho|j\rangle \tag{1.11}$$

The measurement postulate of quantum mechanics states that given any observable A with eigenvalues a_i, so that $A|i\rangle = a_i|i\rangle$, and the mixed state 1.9, the outcome a_i appears with probability

$$p(a_i) = \sum_k p_k \langle\psi_k|P_i|\psi_k\rangle \tag{1.12}$$

where P_i is the projection operator over the subspace corresponding to a_i. The average value of the observable is then given by

$$\langle A\rangle := \sum_i a_i p_i = \sum_k p_k \sum_i a_i \langle\psi_k|P_i|\psi_k\rangle = \sum_k p_k \langle\psi_k|A|\psi_k\rangle \tag{1.13}$$

and similarly, this can be computed by means of the density operator trace:

$$\langle A\rangle = \mathrm{Tr}(\rho A) = \sum_i \langle i|\rho A|i\rangle = \sum_i \sum_k p_k \langle i|\psi_k\rangle\langle\psi_k|A|i\rangle = \sum_i \sum_k p_k \langle\psi_k|A|i\rangle\langle i|\psi_k\rangle \tag{1.14}$$

that is equal to Eq. 1.13 due to the completeness relation $\sum_i |i\rangle\langle i| = \mathbb{1}$.
It can be easily shown that it is completely equivalent to describe a pure system using either the wave function $|\psi\rangle$ and projection operators or the density matrix $\rho = |\psi\rangle\langle\psi|$; but the density matrix is especially useful for mixed states, since it completely characterizes the systems and it combines the intrinsic quantum mechanical probabilities with the lack of information described by the weights p_k.
If we expand any pure state over an orthonormal basis, $|\psi_k\rangle = \sum_i c_i^{(k)}|i\rangle$, the density operator ρ satisfies the following properties[1]:

1. ρ is *Hermitian*: $\rho_{ji}^\star = \rho_{ij}$;
2. it has *unit trace*, $\mathrm{Tr}\,\rho = 1$, and $\mathrm{Tr}\,\rho^2 < 1$ for a mixed state while $\mathrm{Tr}\,\rho^2 = 1$ for a pure state;
3. ρ is a *non-negative* operator, that is $\langle\varphi|\rho|\varphi\rangle \geq 0$ for any $|\varphi\rangle$;
4. its spectral decomposition is $\rho = \sum_j \lambda_j |j\rangle\langle j|$ with eigenvalues $0 \leq \lambda_j \leq 1$. Besides, $\sum_j \lambda_j = 1$ and for a pure state $\lambda_{\bar{j}} = 1$ for just one $j = \bar{j}$, $\lambda_j = 0$ otherwise;
5. if the weights p_k follow the uniform probability distribution, i.e. $p_k = \frac{1}{d}$, the state is *maximally mixed*, because it is a mixture where all states occur with the same probability. In a finite dimensional space, this is the same as saying that ρ is proportional to the identity $\mathbb{1}$.

This formalism can be applied to the qubit pure state 1.2 so that the corresponding density operator is

$$\rho(\theta,\phi) = |\psi(\theta,\phi)\rangle\langle\psi(\theta,\phi)| = \begin{pmatrix} \cos^2\frac{\theta}{2} & \sin\frac{\theta}{2}\cos\frac{\theta}{2}e^{-i\phi} \\ \sin\frac{\theta}{2}\cos\frac{\theta}{2}e^{i\phi} & \sin^2\frac{\theta}{2} \end{pmatrix} \tag{1.15}$$

whereas the density operator for a mixed qubit state is obtain from a 2×2 Hermitian matrix, that can be expanded over the bases $\{I, \sigma_x, \sigma_y, \sigma_z\}$ of Pauli matrices, requiring that the properties of a density matrix are satisfied. In this case we can therefore express ρ as

$$\rho = \frac{1}{2}\left(I + x\sigma_x + y\sigma_y + z\sigma_z\right) = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix} \tag{1.16}$$

and the vector $\mathbf{r} = (x, y, z)$ corresponds to the desired point of the Bloch sphere.

[1] The proofs can be found in [3].

1.4 Entanglement

Suppose we have physical systems A and B. The state space of the composite system is the tensor product of the state spaces of the component physical subsystems $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ and therefore we can express a generic state $|\psi\rangle \in \mathcal{H}$ as

$$|\psi\rangle = \sum_{i,j} c_{ij} |i\rangle_A \otimes |j\rangle_B = \sum_{i,j} c_{ij} |ij\rangle \tag{1.17}$$

where $\{|i\rangle_A\}$ and $\{|j\rangle_B\}$ are basis sets for $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. By definition, a state $|\psi\rangle$ in $\mathcal{H}$ is said to be *entangled* if it cannot be factorized as a simple tensor product of states:

$$|\psi\rangle \neq |\alpha\rangle \otimes |\beta\rangle \qquad |\alpha\rangle \in \mathcal{H}_A, |\beta\rangle \in \mathcal{H}_B \tag{1.18}$$

This intriguing non-classical propriety puzzled scientists such as Einstein, Podolsky and Rosen in 1935. They showed that, assuming the locality and reality principles, quantum theory lead to contradictions. This paradox was investigated by Bell in 1964 and he demonstrated that at least one of these assumptions is not correct. For these reason, entanglement is a fundamentally new resource with no classical analogue, exploited by quantum computation and information to accomplish new tasks that would be otherwise classically impossible.

The corresponding density operator for entangled states is given by its definition: $\rho^{AB} = |\psi\rangle\langle\psi|$ with $|\psi\rangle$ defined as in 1.17. Note that in general the density matrix for the entire system is not equal to the tensor product of the reduced density matrices $\rho_A \otimes \rho_B$.
One of the reasons why the density matrix formalism is convenient is as a descriptive tool for *subsystems* of a composite quantum system. Given a bipartite state ρ^{AB}, the *reduced* density operator for subsystem A is

$$\rho^A := \mathrm{Tr}_B(\rho^{AB}) \tag{1.19}$$

where Tr_B is the *partial trace* over subsystem B, defined by

$$\mathrm{Tr}_B(|\alpha_1\rangle\langle\alpha_2| \otimes |\beta_1\rangle\langle\beta_2|) := |\alpha_1\rangle\langle\alpha_2| \,\mathrm{Tr}(|\beta_1\rangle\langle\beta_2|) \qquad \alpha_i \in \mathcal{H}_A, \beta_i \in \mathcal{H}_B \tag{1.20}$$

In quantum information, A and B are commonly named Alice and Bob. They represent the legitimate users opposed to Eve, the eavesdropper.

One remarkable example of the reduced density operator application and surprising results is given by the maximally entangled state of two qubits, historically known as Bell state:

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\Big(|HV\rangle + |VH\rangle\Big) \tag{1.21}$$

This has density operator $\rho = |\psi^+\rangle\langle\psi^+|$, so the first qubit is described by

$$\rho^1 = \mathrm{Tr}_2(\rho) = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{1}{2}\mathbb{1} \tag{1.22}$$

that is a mixed state since $\mathrm{Tr}((\mathbb{1}/2)^2) = 1/2 < 1$. Therefore, the state of the joint two qubis system is a perfectly known pure state, whereas a single qubit is a *maximally* mixed state (the identity) that encodes no information at all, since it results like a balanced coin in every base it is measured.

1.5 POVM

Positive Operator-Valued Measurements (POVMs) generalize the usual projective measurement and can be useful for many specific purposes. A POVM is described by a set of Hermitian non-negative operators $\{\Pi_i\}$, called POVM elements, that sum to the identity operator

$$\sum_i \Pi_i = \mathbb{1} \tag{1.23}$$

and if the measurement is performed on a state $|\psi\rangle$, the probability of obtaining the outcome i is simply given by

$$p_i = \langle\psi|\Pi_i|\psi\rangle \tag{1.24}$$

The POVM formalism can also be used with mixed states ρ and in this case $p_i = \mathrm{Tr}(\rho\Pi_i)$.
An important difference from projective measurements is that the elements of a POVM are not necessarily orthogonal, with the consequence that the number of elements in the POVM can be larger than the dimension of the Hilbert space they act in. In this case the POVM is said to be *overcomplete*.

Let us assume that a quantum system is known to be in a state drawn from a given set of pure non-orthogonal states as in 1.9. POVMs are suitable to discern conclusively which state the system was in. This task is called Unambiguous State Discrimination (USD) but the drawback is that there is a non null probability of inconclusive outcomes. This impossibility of perfectly discriminating between a set of non-orthogonal states is the basis for quantum information protocols and, as the title suggests, this thesis.
Consider the following example, taken from [1]. It is impossible to distinguish between $|0\rangle$ and $|+\rangle$ with projective measurements. However, this can be achieved using the following (overcomplete) POVM:

$$\Pi_1 = \frac{\sqrt{2}}{1+\sqrt{2}}|1\rangle\langle 1| \tag{1.25}$$

$$\Pi_2 = \frac{\sqrt{2}}{1+\sqrt{2}}\frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2} \tag{1.26}$$

$$\Pi_3 = \mathbb{1} - \Pi_1 - \Pi_2 \tag{1.27}$$

If Π_1 clicks, the incoming state must be $|+\rangle$ since $|0\rangle$ will never cause a click in Π_1. For the same reasons, if Π_2 clicks the incoming state must be $|0\rangle$, in fact $p_2 = \langle +|\Pi_2|+\rangle = 0$. However, if Π_3 clicks nothing can be stated and therefore the outcome is inconclusive (and random).
This example reveals that even if the incoming state is fully known, an overcomplete set of POVM will always result in a non-null set of random events and therefore this feature can be exploited to generate secure and private randomness. In addition, this concept can be extended to generate randomness without any assumption on the incoming state.

1.6 Entropies Measures

Quantum mechanics has revolutionized our understanding of the world. Besides entanglement, another major difference from classical physics is that there are limits to the precision with which quantities can exist in nature, thus the quantum world is inherently unpredictable. This is expressed by the famous

Heisenberg's uncertainty principle, originally formulated as $\sigma_x \sigma_p \geq \frac{\hbar}{2}$, that states the impossibility to prepare a quantum particle for which both position and momentum are clearly defined. This principle applies much more in general: for arbitrary observables X and Y it holds that

$$\sigma(X)\sigma(Y) \geq \frac{1}{2}\langle\psi| [X, Y] |\psi\rangle \tag{1.28}$$

so the commutator $[\cdot, \cdot]$ represents the fundamental limit to our knowledge.

The proper mathematical quantity to express uncertainty in information theory is *entropy*. Entropies are functionals on random variables or quantum states that aim to quantify their inherent uncertainty. Entropy is a natural measure of surprise or uncertainty, perhaps even more than standard deviation, that is better suited to measure the deviation from the mean. In fact, consider the following example (courtesy of [4]) where standard deviation has a counterintuitive behaviour: a spin-1 particle with equal probability $Pr(s_z) = 1/3$ of obtaining one of the three possible outcomes of Z angular momentum $s_z \in \{-1, 0, 1\}$. It is easy to see that the standard deviation is $\sigma(Z) = \sqrt{2/3}$. Now suppose we gain additional information such that the spin does not take the value $s_z = 0$, so the new probability distribution is $Pr(-1) = Pr(1) = 1/2$, $Pr(0) = 0$. In this case, the standard deviation increases, $\sigma(Z) = 1$, even though the uncertainty is decreased since we got more information.

Formally, if we have a discrete random variable X distributed according to a probability distribution P_X that takes values $x = \{1, \ldots, d\}$ (entropies do not depend on the specific labels of the elements of this set), the average surprise or information associated to X is given by:

$$H(X) := \sum_x -P_X(x) \log_2(P_X(x)) \tag{1.29}$$

which is called *Shannon entropy*[2]. Intuitively, this works because outcomes that occur with high probability P_X give less information (and surprise) respect to events with low probability. For example, a text containing only a string of "aaa...aaa" will have much less information respect the text you are reading. So Shannon Entropy associate high information gain to low probability events ($\log(P_X(x))$) and averages them respect the number of times they will appear ($P_X(x)$).
In classical information theory, we can view entropy either as a measure of our uncertainty before we learn the value of X, or as a measure of how much information we have gained after we learn the value of X.

In recent years, entropy and the uncertainty principle have emerged as a central ingredient for new discoveries and applications of quantum information theory, as in [5]. The uncertainty relation for measurements of two complementary observables can be formulated by means of Shannon entropy as well [4]. Messages in quantum information are encoded in states taken from an "alphabet", as in 1.9, described by the density matrix ρ (1.10) and eigenvalues λ_j. The quantum analogue of Shannon entropy is called the *von Neumann entropy* and is defined as

$$H(\rho) := -\operatorname{Tr}(\rho \log \rho) = -\sum_j \lambda_j \log \lambda_j \tag{1.30}$$

Note that $0 \leq H(\rho) \leq \log d$ where $H(\rho) = 0$ for pure states ($\lambda_{\bar{j}} = 1$) and $H(\rho) = \log d$ for maximally mixed states.

[2] All logartihms are base-2 unless otherwise indicated.

The amount of gained information, and hence the entropy, depends also from the information already available to us (or some adversary). Take for example the expansion to 100 digits of e: if we don't know that we will get the digits of e, the amount of entropy will be high since every digit is different and it is impossible to predict the next one. However, if we already have the information that we will get the digits of e, the amount of entropy will be 0, because we will not have any surprise looking at the output, nor we will gain any new information.
To consider this previously available information (associated with the random variable Y), we need to introduce the *conditional entropy*

$$H(X|Y) := -\sum_{x,y} P(X=x, Y=y) \log(P(Y=y|X=x)) \tag{1.31}$$

where $P(X=x, Y=y)$ and $P(Y=y|X=x)$ are the standard joint and conditional probabilities. For composite quantum systems, the conditional entropy is given by

$$H(X|Y) = H(\rho_{XY}) - H(\rho_Y) \tag{1.32}$$

where $\rho_Y = \mathrm{Tr}_X(\rho_{XY})$.
Anyhow, these entropies are not the proper quantity to consider for our purposes. In fact, since they are defined via probability measures, the Shannon entropy can be interpreted as the average amount of randomness available but in the asymptotic limit of an infinite set of outcomes. This limit is thus usually considered for an infinite and identical repetition of a certain process (i.i.d assumption). In our case, we deal with less ideal setting and in practice the protocol can be repeated a finite number of times. Therefore we need a one-shot (i.e. for a single instance of the protocol) worst-case bound for the entropy, that is given by the conditional min-entorpy $H_{min}(X|Y)$. This quantity can be defined in many different ways, depending if it is conditioned and it such conditioning is only respect classical or quantum side information [6]. Here, we will present the most general definition (which is conditioned respect quantum information E) since it gives the most conservative bound:

$$H_{min}(X|E) := -\log(P_{guess}(X|E)) \tag{1.33}$$

$$p_{guess}(X|E) := \max_{\hat{E}_x^E} \sum_x^d P_X(x) \,\mathrm{Tr}\left(\hat{E}_x^E \rho_x^E\right) \tag{1.34}$$

Let us better discuss the terms of these equations. In the most general (and worst for Alice's security) case, Eve controls a bipartite quantum state ρ_{AE} and her intention is to guess with a certain probability, precisely $p_{guess}(X|E)$, the outcome of Alice's POVM $\{\Pi_X^A\}$ given the quantum side information E. In order to do that, Eve implements a POVM taken from an arbitrary set $\hat{E}_x^E$ to examine the state ρ_x^E held by Eve after that Alice has performed her measurements on ρ_{AE}. Alice's side is consequently projected in the eigenstate $|x\rangle$ related to the outcome x. This post-measurement state can be written as:

$$\rho_{XE} = \sum_x P_x(x) |x\rangle\langle x|^A \otimes \hat{\rho}_x^E \tag{1.35}$$

where ρ_x^E is the same state appearing in 1.34 and it is the following reduced density matrix:

$$\rho_x^E = \mathrm{Tr}_A\left((\Pi_X^A \otimes \mathbb{1}^E)\rho_{AE}\right) \tag{1.36}$$

The state ρ_{AE} can be any state, but the one that gives Eve the most information is the one that *purifies* $\sum P_X(x)|x\rangle\langle x|$, meaning that ρ_{AE} can be considered pure without loss of generality. In other words, *purification* is a purely mathematical procedure that allows us to associate pure state with mixed systems: given a state ρ^A belonging to subsystem A, it is always possible to introduce another system, which we denote E, and define a pure state ρ_{AE} such that $\rho^A = \mathrm{Tr}_E(\rho_{AE})$.

To get an idea about the definition in Eq. 1.34 we can think in terms of Eve optimal guessing strategy: at the beginning of the protocol Alice and Eve hold a bipartite (pure) quantum state ρ_{AE} crafted by Eve that sends one part to Alice, namely ρ_A. Then Alice uses her POVM $\left\{\Pi_x^A\right\}$ to measure it and gets an outcome x, projecting her state in the respective eigenstate $|x\rangle$ which now can be considered classical. Eve's state ρ_E, since it was correlated with Alice's part, is also projected in ρ_x^E depending on Alice's outcome. Now Eve's best strategy to maximize her probability to guess Alice's outcome is to find a POVM $\left\{E_x^E\right\}$ that always clicks when ρ_x^E is sent, meaning that it must maximize $\mathrm{Tr}\left(\hat{E}_x^E \rho_x^E\right)$. The factor $P_X(x)$ takes into account how many times Alice measures with the POVM element Π_x^A. Despite the simplicity of the definition for the min-entropy, the estimation of this quantity is extremely hard since it involves the maximization over an infinite and continuous set of POVM $\hat{E}_x^E$, but it is crucial to extract secure random strings, as it is further discussed in section 2.4.

Chapter 2

Quantum Random Number Generation

What is random? One simple non-philosophical answer is that randomness is the lack of pattern or predictability in events of any kind. In ancient history, the concepts of chance and randomness were associate with that of fate or gods' will. It was only in the 1800s with the advent of calculus, and with probability theory later, that randomness underwent a process of formal analysis. Although randomness and uncertainty are often viewed as an obstacle and a nuisance, today random numbers have an essential role in many fields. Some of them are cryptography, gambling, scientific simulations (as Monte Carlo) and research methods.

2.1 Random Number Generators

There are a lot of ways to generate random numbers. The first that come to mind are tossing a coin, trowing a dice or drawing a ball from a lottery machine. These generators are common in everyday life, where actually a small amount of randomness is required.
Nowadays computers are used to obtain random numbers. Methods that produce them from a deterministic algorithm are called pseudorandom number generator (PRNG). PRNGs normally take as input a small string, the *seed*, and they output a long sequence simulating the discrete uniform distribution, from which other distributions can be obtained by means of different algorithms, such as the inverse transform sampling. While it is clear that such a sequence cannot be truly random and it is in fact predictable, PRNG are suited for simulations that demand just the "appearance" of randomness and fast reproducible results.

However, for many other applications, unpredictability is a fundamental requisite. True random number generators (TRNG) measure some difficult-to-predict physical process, such as thermal noise in electronic circuits or quantities in chaotic systems in general, and use the results to create random numbers. In particular, quantum random number generators (QRNG) are physical generators based on quantum systems.
Although classical TRNGs seem more advisable than PRNGs, there are some inconveniences that one must take into account: they have limited generation rate, the randomness relies on our ignorance of the process description and failures are difficult to detect. QRNGs offer a solution to these problems: as discussed in section 1.6, the inherent randomness in quantum mechanics can be exploited for generating *true* random numbers.

2.2 QRNG Classification

On the basis of the degree of trustworthiness on devices, QRNG can be grouped into three categories [7]. The first, trusted-device QRNG, is built on fully trusted and calibrated devices and typically they have high performances. The second category is self-testing QRNG, in which randomness can be generated without trusting the actual implementation and it is guaranteed by quantum mechanical properties. The third category, semi-self-testing QRNG, is an intermediate category that provides a trade-off between the trustworthiness on the device and the random number generation speed. The security of QRNG will be further covered in the next section.

Let us now present a brief overview of representative QRNGs and their inner workings.
Because of the availability of high quality optical components, the relative low costs and the potential of chip-size integration, most of today's practical QRNGs are implemented in photonic systems. Such QRNG usually includes a an entropy source for generating well-defined quantum states (a laser) and a detection systems (photon detectors), whose dead time and efficiency are the major limit of generation rates. One way to increase this rate is to perform a measure of the temporal or spatial mode of the photon. Temporal QRNGs measure the arrival time of a photon emitted by a weak coherent laser pulses such that within a chosen time period there is one detection event. This detection time is randomly distributed within the time period providing the required random numbers. On the other hand, spatial QRNGs measures the spatial mode of a single photon with a space-resolving detection system. For example, a photon is sent through a beam splitter and the output position is detected. Other QRNG are based on photon counting, attenuated pulses, vacuum fluctuation or phase noise. Besides optical systems, there have also been proposals for QRNG based on radioactive decays or atomic quantum systems. For a more exhaustive dissertation about the history and classification of QRNG, see [8].

2.3 Security of QRNG

One of the most basic QRNG consists of diagonally polarized single photons $|+\rangle$ (or equally $|-\rangle$) going through one Polarizing Beam Splitter (PBS) as shown in Fig. 2.1:

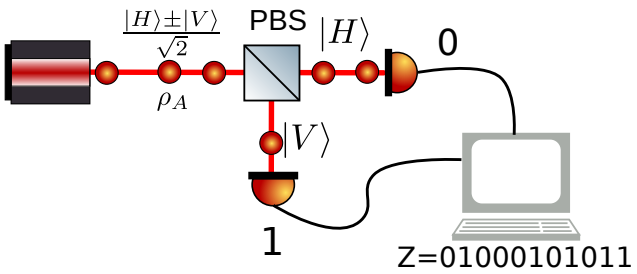


Figure 2.1: Example of a simple but insecure QRNG

Provided that the state is trusted and the PBS is perfectly balanced, Alice will get a true random string since she exactly detects $|H\rangle$ or $|V\rangle$ with probability 1/2 for every photon. On the other hand, if a malicious eavesdropper, Eve, can access quantum side-information on the system, she could use it to guess Alice's string within a certain amount of reliability. For example, if Eve controls the quantum state source, she might send a maximally entangled state (as in Eq. 1.21) to exactly know every bit of Alice's string. Besides, in this way Alice cannot know that her string is being spied on.

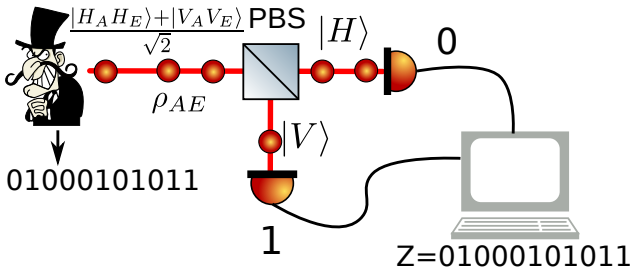


Figure 2.2: Example of an optimal attack on the simple QRNG

For this reason in critical applications, such as cryptography, randomness is required to be also *private*.

From the theoretical point of view attacks are possible because the measurements do not give to Alice the possibility to estimate the purity of the incoming state, that can be, in principle, totally mixed. For such incoming state there exists a bipartite purification ρ_{AE} (in this case the maximally entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$) that gives to Eve the maximal amount of information. In order to estimate the purity of the incoming state a full *tomography* approach can be used, as in [9] or a basis switching scheme as in [5]. Having information from another basis helps to put a non trivial bound on the secure randomness extractable, whereas the general principle behind quantum state tomography is that by repeatedly performing many different measurements on quantum systems described by identical density matrices, frequency counts can be used to infer probabilities to determine a density matrix which fits the best with the observations and ultimately the randomness can be bounded with the formula 1.33. Although in many protocols one has to trust his devices, they could misbehave or could be manufactured/controlled by the eavesdropper himself. For security reasons one would like to trust his devices as little as possible. A solution is offered by Device-Independent (DI) protocols: they offer the highest level of security since they are able to certify the randomness without any assumption on the inner working of the devices. However, since they require a loophole-free violation of a Bell inequality, their experimental realization is extremely demanding and the generation rates are too low to be useful in any practical scenario. For this reason, Semi-DI protocols have been proposed. They trust only part of the apparatus but they can achieve rates extremely bigger than DI.

In chapter 3 we propose a Semi-DI protocol, based on the inconclusive outcomes of overcomplete POVM.

2.4 Randomness Estimation of the QRNG

In section 1.6 we have seen how entropies objectively quantify the amount of randomness of a random variable or obtained from a quantum state. In practical realizations, we must additionally consider that the measurement are subjected by experimental errors and instrumental noise, so QRNG protocols will expect some amount of classical randomness arising from the non-ideal components. In our case, a photonic implementation, classical noise could arise from the laser photon generation rate, the optical fibres or the single photon detectors (SPAD). All these sources of classical noise will be inevitably mixed with the "quantum" randomness belonging to the quantum measurements, with the difference that they will bring a security flaw. Indeed, any phenomenon that can be described by the laws of classical physics can, at least in principle, be predicted by solving the corresponding equations.

There is nevertheless hope to separate the classical (and insecure) randomness from the quantum part thanks to the Leftover Hashing Lemma (LHL) [10]. Informally this theorem affirms that if a n-bits string is given and we know that it contains at least $m < n$ bits of randomness (i.e. its min-entropy is m-bits), there exist a particular set of function, called randomness extractors, that get as input the n-bits string and output a m-bits string which is arbitrary close to a random string (it is ε close from a string sampled from the uniform distribution).

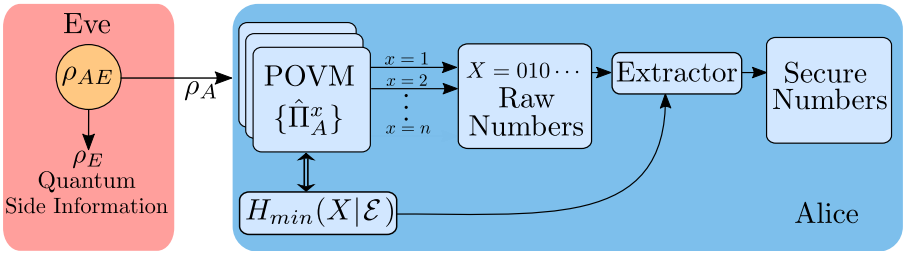


Figure 2.3: Representation of the randomness generation protocol

This explains why the right min-entropy estimation is crucial for the security of the protocol: if we are able to bound the min-entropy of the string generated by the QRNG, we can always apply the LHL to get a perfectly random string. But how can we tackle this hard problem of estimating, or bounding, the min-entropy? We will see in 3.3 that for our specific case, some solutions have been proposed.

2.5 Randomness Testing

Once we generate a secure random sequence, we need to check if everything has worked correctly. Unfortunately, there is no way to absolutely determine if a finite sequence is truly random. For example, considering the extreme case of a 1-bit string, it is like asking whether 1 is fundamentally more random than 0. Anyhow, there are methods to detect suspicious sequences: while the string 11111 is just as likely as 10110, if our generator consistently outputs more ones than zeroes we have the reason to suspect that it may be not so random but it shows some kind of pattern.

The established approach to randomness testing is using a series of statistical test to uncover these patterns or biases. The main suit is developed by the NIST [11] and it includes different tests. They check, for instance, the frequency of zeros and one, the oscillation between them, periodic features or correlations. The result is a *p-value* that indicate how likely it is for a purely RNG to produce the tested sequence, similarly to the standard chi-squared test.

These tests, while useful to detect faulty generators, actually cannot prove that a generator produces truly random outputs. PRNG can pass the tests but are predictable or even a perfect RNG would statistically fail a test from time to time. In spite of that, any good QRGN should be able to pass all the tests in any given suite.

Chapter 3

Semi-Device-Independent QRNG: The experiment

The idea behind this experiment came from the article "Secure heterodyne-based quantum random number generator at 17 Gbps" [12], in which a Source Device Independent (SDI) QRNG was presented in the framework of Continuous Variable (CV) systems. In this situation, the overcompleteness of the POVM implemented by Heterodyne Detection ($\hat{\Pi}_\alpha = \frac{1}{\pi}|\alpha\rangle\langle\alpha|$) was exploited, together with the properties of the Husimi Q-Function, to bound the conditional quantum min-entropy $H_{min}(X|E)$ and certify randomness without any assumption on the quantum states measured.

In this work, this concept is brought to finite dimensional Hilbert spaces and arbitrary POVMs. In particular, we start analysing the case of the equiangular three-state POVM. Then, by employing a new numerical tool, it will be derived a bound of extractable randomness for an arbitrary number of POVMs for a fixed dimension.

3.1 Three state POVM

We have seen in section 1.5 that POVM can be exploited to generate secure and private randomness more successfully than projective measurements, as it has been experimentally proved in [13].
In a two dimensional Hilbert space, one simple overcomplete POVM is given by the following elements:

$$\Pi_1 = \frac{2}{3}|V\rangle\langle V| = \frac{2}{3}|\psi_1\rangle\langle\psi_1| \tag{3.1}$$

$$\Pi_2 = \frac{2}{3}\left(\frac{\sqrt{3}}{2}|H\rangle + \frac{1}{2}|V\rangle\right)\left(\frac{\sqrt{3}}{2}\langle H| + \frac{1}{2}\langle V|\right) = \frac{2}{3}|\psi_2\rangle\langle\psi_2| \tag{3.2}$$

$$\Pi_3 = \frac{2}{3}\left(\frac{\sqrt{3}}{2}|H\rangle - \frac{1}{2}|V\rangle\right)\left(\frac{\sqrt{3}}{2}\langle H| - \frac{1}{2}\langle V|\right) = \frac{2}{3}|\psi_3\rangle\langle\psi_3| \tag{3.3}$$

This overcomplete POVM uses states that form an equilateral triangle in the X-Z plane of the Bloch Sphere (see Fig. 3.1).

As previously said, even if the incoming state is perfectly aligned with one of the measurements (that are not orthogonal), the probability to obtain the right outcome is less than one, in contrast

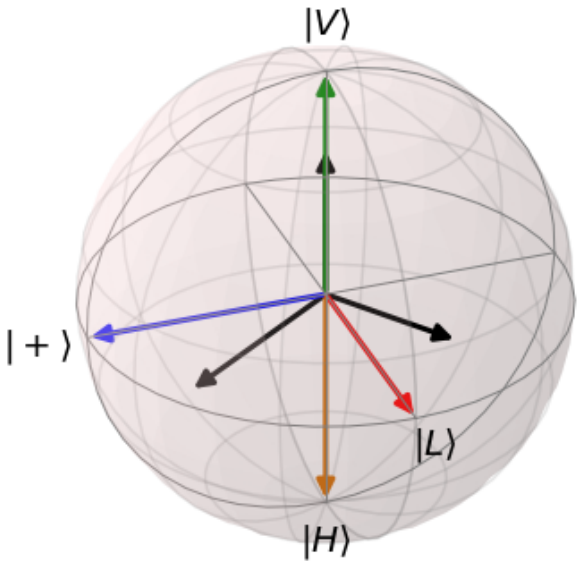


Figure 3.1: Visual representation of the three-state POVM (black) on the equator of the Bloch sphere. The states $|V\rangle$ (green), $|H\rangle$ (orange), $|+\rangle$ (blue) and $|L\rangle$ (red) are also plotted.

with projective measurement. For example, if the incoming state is $|V\rangle$, Π_1 clicks with probability $p = \langle V|\Pi_1|V\rangle = 2/3$. Since this impossibility to predict with certainty the outcomes remains valid also for an eavesdropper that could try to obtain the same output as the legitimate user, this POVM assures that the obtained randomness is also private.

In particular we will analyse three different scenarios, which are gradually more and more paranoid:

Trusted scenario We assume to known and trust how our devices, especially the source and the measurements, are perfectly working. In this case both the state ρ and the measurements $\{\Pi\}$ are known and fixed in every run of the experiment. Clearly this is the easier scenario to analyse but also the less secure, since the security relies on the demanding assumptions and trust that we put on the devices.

Source-Device-Independent with measurement information In this scenario we assume we have a characterized, but not ideal, measurement station so that we can settle the POVM $\{\Pi\}$, but we do not assume anything about the source, that can be even controlled by the eavesdropper himself. In our analysis he can share both classical and quantum correlation with the system, for example he can control a maximally entangle state. Using the information of the outcome statistic from the POVM measurement we estimate a lower-bound on the extractable secure randomness.

SDI without measurement information This scenario is similar to the previous, but we don't use any information about the statistics of the outcomes. Basically the randomness is lower bounded respect the worst state ρ that is physically allowed by quantum mechanics.

3.2 Experimental Setup

The experimental setup is loosely based on [14] and it is shown in Fig. 3.2. Firstly, the photons are emitted by a weak coherent pulses laser source at $\lambda = 808$ nm and they are guided through a single mode fibre to a collimator. Secondly, the desired polarization is adjusted by means of a HWP and a QWP. Then the POVM is implemented by using a partially polarizing beam-splitter (pPBS) that completely transmits the the horizontal polarization and it has a reflectivity of 66.7% for the vertical polarization, followed by a HWP at $\theta = 22.5°$ and a polarizing beam splitter (PBS) that split the incident beam into two beams of orthogonal polarization. Finally, the photons are detected by three single photon avalanche diodes (SPAD). These detection events are time-tagged and stored in a computer where eventually the data are analysed by means of `Python` programs. The LASER is

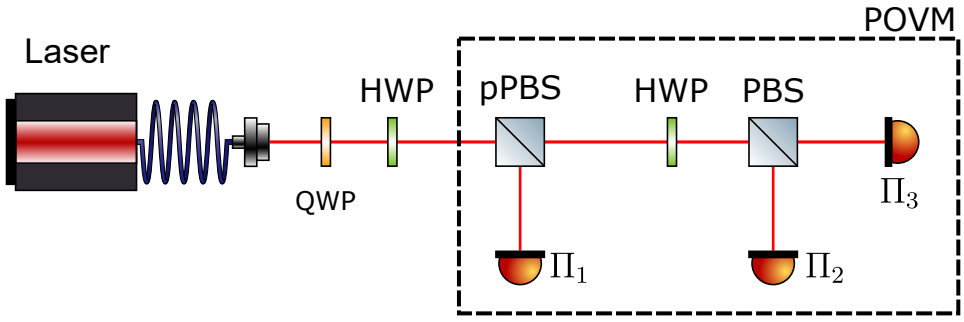


Figure 3.2: Three-state POVM setup.

manufactured by *Thorlabs* (model LP808-SF30) and it is operated by a controller that provides extreme precision at the current level of operation and absolute control over working temperature. The SPADs (*Excelitas Technologies' SPCM-NIR*) are characterized by a dead time of 20 ns, an efficiency of $\sim 68\%$ and a maximum amount of 100 dark counts/s. Lastly, the time-tagger "quTAU" made by *qutools* has a resolution of 81 ps. The final result is shown in the following photo, where two polarizers are added to reduce noise:

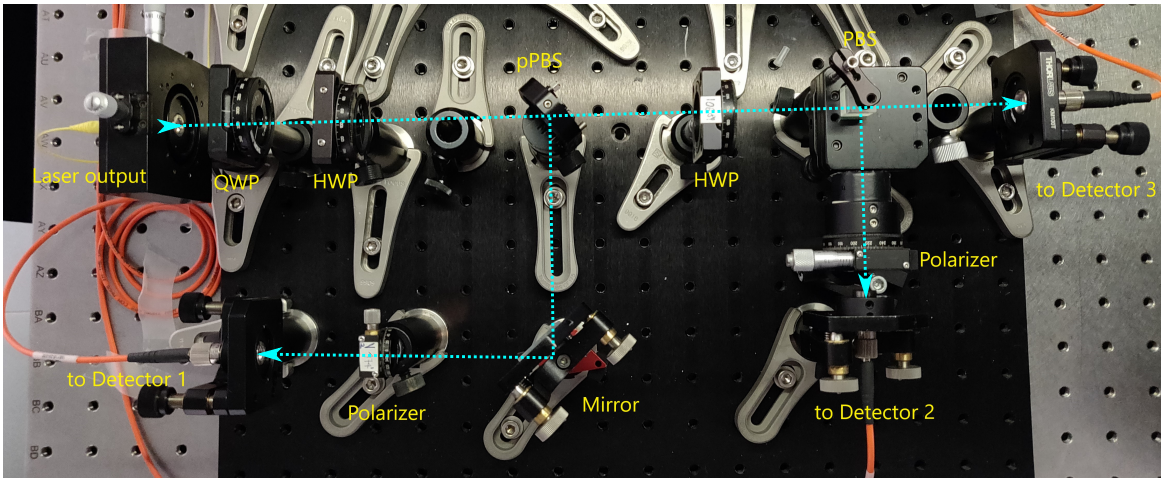


Figure 3.3: Photo of the experimental setup.

3.3 Entropy Estimation and Results

In section 2.4 we left open the question about the estimation of the min-entropy. In this section we analyse the three different scenarios and methods to deal with this problem.

Trusted Scenario

If Alice knows for sure the incoming ρ_A and if she trusts her POVM, she can simply generate random numbers by acquiring the POVM elements clicks, even though theirs security is not assured. In fact, if her state is pure it cannot be correlated with anyone else and her results are secure, otherwise the more her state is mixed the more it could be correlated with an adversary, since Eve could purify the system. The classical example is if $\rho_{AE} = |\phi^+\rangle$ (defined in 1.21) or any other maximally entangled state: in this case $\mathrm{Tr}_E(\rho_{AE}) = \mathbb{1}_A$, the classical min-entropy is 1.58 since the outcomes are perfectly balance among the POVM elements. However, since the state could be purified, the quantum conditional min-entropy $H_{min}(X|E)$ is zero, leading to no secure random numbers.

With our specific setup, the states can be prepared by tuning the plates and checking the clicks distribution, that can be computed beforehand with 1.24. These outcomes and the corresponding Shannon entropy H are shown in Tab. 3.1:

Incoming State	Π_1	Π_2	Π_3	H
$\|H\rangle$	0	1/2	1/2	1
$\|V\rangle$	2/3	1/6	1/6	0.58496
$\|+\rangle$	1/2	$\frac{1}{6}\left(2+\sqrt{3}\right)$	$\frac{1}{6}\left(2-\sqrt{3}\right)$	0.68499
$\|L\rangle$	1/3	1/3	1/3	1.58446

Table 3.1: Probabilities distribution and entropy for some different incoming states.

Note that $|H\rangle$ is equidistant from two POVM elements and so it gives 50% outcomes, like a fair coin toss, whereas $|V\rangle$ is aligned with Π_1 so its clicks more frequently and the entropy is lower. Finally, $|L\rangle$ is orthogonal to the three POVM elements, as it is shown in Fig. 3.1, and for this reason they click with the same probability so that the most randomness can be obtained, as if it were an ideal discrete uniform distribution generator.

SDI with measurement information

In the other two scenarios the source is not trusted and the estimation of the min-entropy is harder because the state ρ_{AE} is unknown. This issue has been elegantly solved by Coles, Metodiev, and Lütkenhaus in [15]. They proposed a new numerical method to solve this problem but due to technicalities we will leave the details to the original article. Using the technique described there QuantumFuture

researchers have expressed our optimization problem into an Semi-Definite Program (SDP) which can be efficiently solved by computers and so we are able to lower-bound the min-entropy of our protocol.

As far as the second scenario is concerned, the p_{guess} (1.34) must be also optimized over all the ρ compatible with the statistics that we observe. The new quantity to estimate (or bound) can be written as

$$p_{guess}(X|E) = \max_{\rho_{AE}\in\mathcal{C}} \max_{\hat{E}_x^E} \sum_x^d P_X(x) \operatorname{Tr}\left(\left(\Pi_x \otimes \hat{E}_x^E\right)\rho_{AE}\right) \tag{3.4}$$

where $\mathcal{C}$ is the set of all physical states compatible with the measurements observed:

$$\mathcal{C} = \{\rho_{AE} \in \mathcal{H} \mid \operatorname{Tr}(\Gamma_i \rho_{AE}) = \gamma_i\} \tag{3.5}$$

where Γ_i are POVM and γ_i are the experimental outcomes.

For experimental purposes we sent the usual states $|H\rangle$, $|V\rangle$ and $|L\rangle$, knowing that they are not pure because of the unavoidable experimental errors related to the (untrusted) source, so we denote them between quotation marks (e..g "$|H\rangle$"). In Tab 3.2, there are the experimental counts probabilities and an estimate of their errors following the Poisson distribution. The bound for the experimental min-entropy H_{min}^{exp} has been computed with the above-mentioned numerical method that takes into account finite-key effects, namely it gives the worst case value considering the probabilities confidence intervals as well. Moreover, we simulated the min-entropy H_{min}^{th} for the corresponding ideally pure states:

Incoming State	Π_1	Π_2	Π_3	H_{min}^{exp}	H_{min}^{th}
"$\|H\rangle$"	0.00374 ± 0.00001	0.49869 ± 0.00009	0.49757 ± 0.00009	0.8599	0.9998[3]
"$\|V\rangle$"	0.66576 ± 0.00009	0.16639 ± 0.00007	0.16785 ± 0.00007	0.58496	0.58496
"$\|L\rangle$"	0.3337 ± 0.0001	0.3319 ± 0.0001	0.3344 ± 0.0001	0.58496	0.58496

Table 3.2: Experimental probabilities and comparison of both numerical and theoretical H_{min} lower bounds for different assumed incoming states.

Let us analyse these results thoroughly. "$|H\rangle$" has a lower numerical bound because of said experimental problems and detector dark counts, that eventually make the state look mixed because there are counts when there should not be. If Eve were to send the pure state $|H\rangle$, Alice would be able to recognize it since Π_1 never clicks and the remaining elements click with the same probability, as a binary random variable from which no more than 1 bit of entropy can be extracted. For these reasons, if the incoming state is $|H\rangle$, there is no difference between trusted and untrusted source.
Alice's worst cases are for "$|V\rangle$" and "$|L\rangle$". Regarding the former, Eve could take advantage of the unbalance of "$|V\rangle$" probabilities (her most optimal strategy would be to sent this state and bet on Π_1) whereas the latter is indistinguishable from a maximally-mixed state. Therefore, as we will see in the next section, the entropy bound is close to its minimum and the minimization program reaches machine precision, regardless of the probabilities error intervals.

[3] The correct value shoud be 1. This difference is due to numerical issues.

In the end, these estimated min-entropies and the raw data are given as input to the extractor and the requested secure random string is obtained. The size of the data sets and the generation rates are shown in Tab. 3.3. Each of the data sets refers to slightly different experimental condition and system configuration, this explains the discrepancy between "$|V\rangle$" and "$|L\rangle$" generation rate, even though they have similar entropy and acquisition time. Higher rates could be achieved by increasing the laser intensity and with a finer instruments calibration, although this generator is not built for this purpose.

Data Set	Acquisition Time [s]	Raw Data Size [MB]	Extracted Data Size [MB]	Generation Rate [kbps]
"$\|H\rangle$"	67.3	7.06	3.08	385
"$\|V\rangle$"	64.3	5.91	1.70	223
"$\|L\rangle$"	61.8	4.68	1.35	183

Table 3.3: Randomness extraction and generation rates.

The trustworthiness of the final data has been checked as described in 2.5. Those tests output a *p-value* that is the probability that a perfect random number generator would have produced a sequence less random than the sequence that was tested, given the kind of non-randomness assessed by the test. If a *p-value* for a test is determined to be equal to 1, then the sequence appears to have perfect randomness. On the contrary, a *p-value* of zero indicates that the sequence appears to be completely non-random. A significance level of $\alpha = 0.01$ was chosen, i.e. one would expect 1 sequence in 100 to be rejected. A *p-value* > 0.01 would mean that the sequence would be considered to be random with a confidence of 99%. All the datasets passed the tests, thus confirming actual randomness. To give just one example, the results for the state "$|H\rangle$" are shown in Tab. 3.4 and Fig. 3.4.

SDI without measurement information

In the last scenario, the entropy estimation is independent from the incoming state and it coincides with the min-entropy calculated in the most conservative case, i.e. for $\rho_A = |V\rangle$. In this case we have:

$$H_{min} = -\log_2(2/3) \simeq 0.58496\ldots \tag{3.6}$$

The same happens for $\rho_A = |L\rangle$ or $\rho_A = |R\rangle$ since from the point of view they of the outcome statistics they are like the maximally mixed state $\mathbb{1}$. In the case of $\rho_A = |H\rangle$, which is maximally far from two adjacent POVM Π_2 and Π_3, using the full statistic can be beneficial because it is possible to certify 1 bit of randomness for measurement instead of $-\log_2(2/3)$.

	Test Name	*p-value*
1	Monobit Frequency Test	0.54
2	Block Frequency Test	0.27
3	Runs Test	0.28
4	Longest Runs Ones 10000	0.14
5	Binary Matrix Rank Test	0.67
6	Spectral Test	0.79
7	Non Overlapping Template Matching	0.64
8	Overlaping Template Matching	0.06
9	Maurers Universal Statistic Test	0.68
10	Linear ComplexityTest	0.84
11	Serial Test	0.79
12	Approximate Entropy Test	0.36
13	Cumulative Sums Test	0.93
14	Random Excursions Test	0.16
15	Random Excursions Variant Test	0.04
16	Cumulative Sums Test Reverse	0.70

Table 3.4: Tests and corresponding p-values. For the tests which give more than a p-value, the smallest is reported.

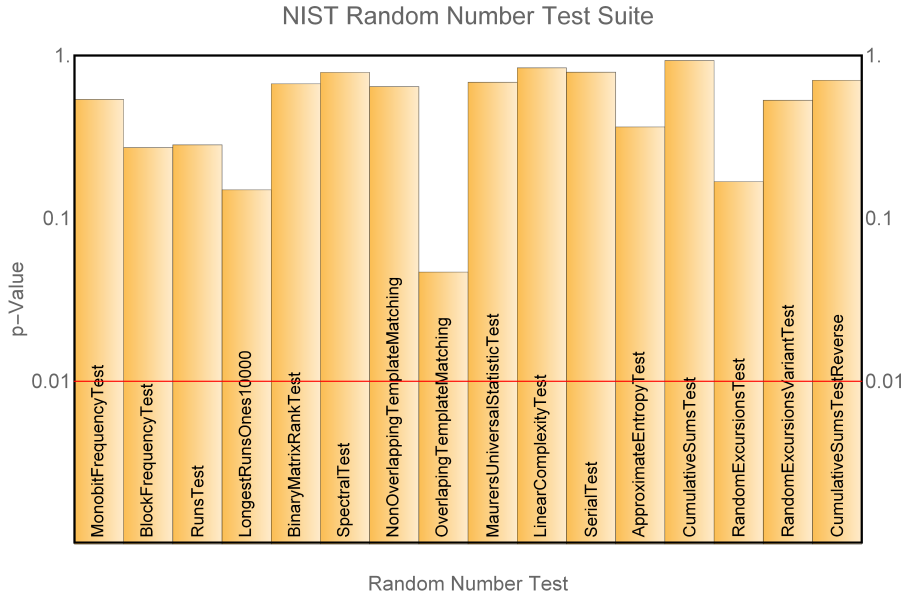


Figure 3.4: Summary of the results of tests effective in detecting defects in TRNG. All the p-values are above the significance level threshold (red).

These results can be extended by means of a simulation: the min-entropy is plotted in Fig. 3.5 as a function of the number of elements in the POVM for a two-dimensional Hilbert space.

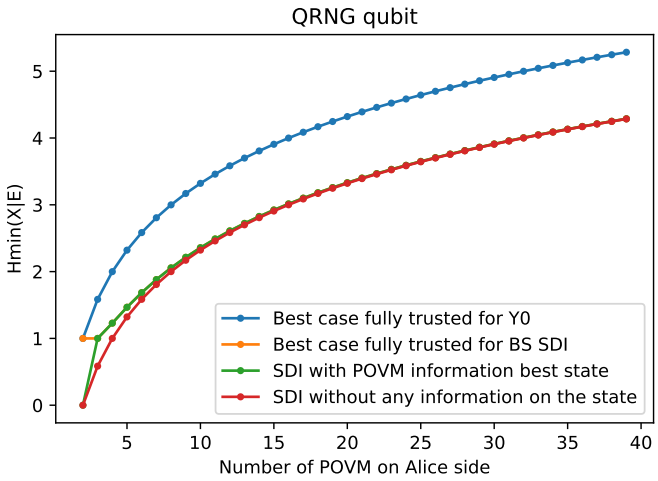


Figure 3.5: Min-entropy estimation as a function of the POVM elements number. Y0 corresponds to the incoming state $|L\rangle$, eigenvalue 0 of Pauli matrix σ_y. The orange line stands for the Best State relative to the SDI.

If we deem the Hilbert space dimension as a fixed resource, it is remarkable that the amount of extractable randomness increases indefinitely. Besides, note that, as we would expect, in the second and third scenarios $n = 2$ POVM elements do not permit to get secure randomness, but indeed this becomes possible from $n > 2$.

We also simulated the second and third scenarios for all the incoming states in the case of the three-state POVM described at the beginning:

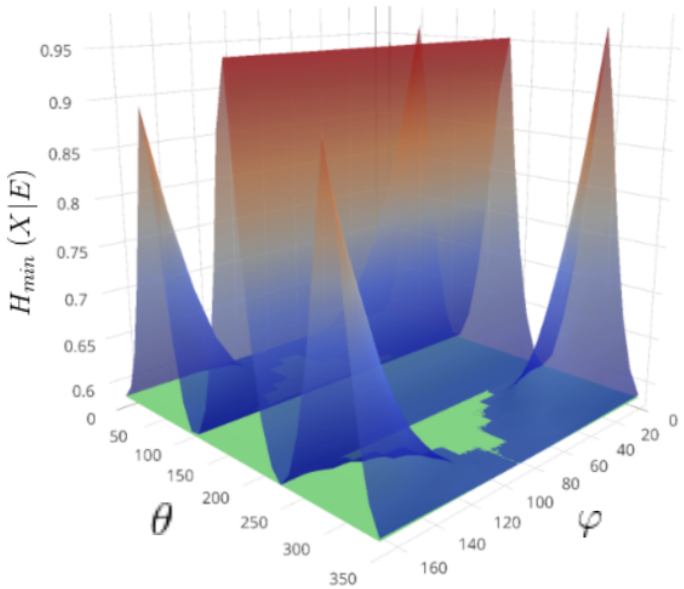


Figure 3.6: Min-entropy estimation as a function of the state. φ and θ stands for the polar qubit representation (Eq. 1.2). The surface plot represents the second scenario, whereas the green layer is the unique entropy value of the third scenario. Note that for $\varphi = 0°$ the three peaks stand for equidistant states from the POVM elements, whereas the φ-invariant ridge is $|H\rangle$.

3.4 Conclusions and Further Development

This experiment has shown that just by exploiting POVM on photons polarizations it is possible to generate high-quality *true* random numbers thanks to the astonishing properties of Quantum Mechanics. Moreover, their security is certified by a proper estimation of the min-entropy H_{min} that takes into account both unavoidable impurities of the state and any external intrusions.

This setup can be also easily improved and brought to four (or more) state POVM elements in order to get more randomness. One scheme could be the following: the beam reflected by the pPBS can be split again by means of a PBS, so that the POVM elements are aligned to the states $|H\rangle$, $|V\rangle$, $|+\rangle$ and $|-\rangle$. In addition, with an entangled state source and a copy of this apparatus, it is possible to reproduce the presence of Bob or even the eavesdropper herself. For example, the former can be used in the cases of Quantum Key Distribution (QKD) applications and the latter to test the security of random strings, all within the same experimental setup but with different analysis methods. We actually assembled this entangled version (Fig. 3.7) with the aim to study *heralded* qubits: Bell states are sent as input (e.g. $|HV\rangle$) in both branches and we know for sure that if a POVM element clicks in one branch ($|V\rangle$), because of entanglement the other photon is in the opposite state ($|H\rangle$) and a click is recorded accordingly. The benefit is that the dark counts and experimental errors are highly reduced, thus giving a better min-entropy estimation (and again more randomness). We were able to build, characterize the setup and collect a set of preliminary results, but unfortunately more time is needed to finish the analysis for a conclusive thesis work.

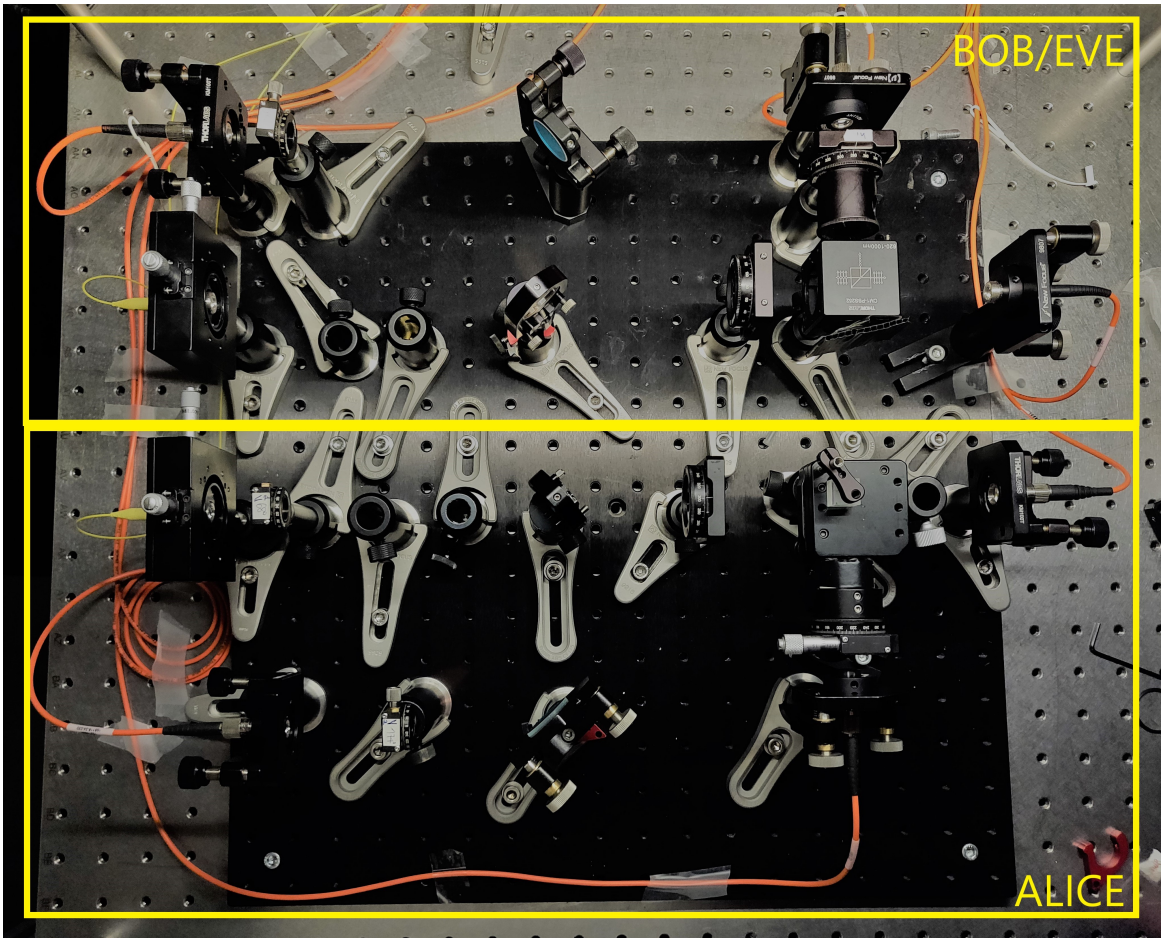


Figure 3.7: Photo of the entangled experimental setup.

List of Figures

Bibliography

[1] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2017.

[2] Bahaa E. A. Saleh and Malvin Carl. Teich. *Fundamentals of photonics*. Wiley-Interscience, 2009. Chap. 6.

[3] Giuliano Benenti et al. *Principles of quantum computation and information*. World Scientific, 2008. Chap. 5.

[4] Patrick J. Coles et al. "Entropic uncertainty relations and their applications". In: *Rev. Mod. Phys.* 89.1 (Feb. 2017), p. 015002. ISSN: 0034-6861. DOI: 10.1103/RevModPhys.89.015002. URL: http://link.aps.org/doi/10.1103/RevModPhys.89.015002.

[5] Giuseppe Vallone et al. "Quantum randomness certified by the uncertainty principle". In: *Physical Review A* 90.5 (2014). DOI: 10.1103/physreva.90.052327.

[6] Robert Konig, Renato Renner, and Christian Schaffner. "The Operational Meaning of Min- and Max-Entropy". In: *IEEE Transactions on Information Theory* 55.9 (2009), pp. 4337–4347. DOI: 10.1109/tit.2009.2025545.

[7] Xiongfeng Ma et al. "Quantum random number generation". In: *npj Quantum Information* 2.1 (2016). DOI: 10.1038/npjqi.2016.21.

[8] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. "Quantum random number generators". In: *Reviews of Modern Physics* 89.1 (2017). DOI: 10.1103/revmodphys.89.015004.

[9] M. Fiorentino et al. "Secure self-calibrating quantum random-bit generator". In: *Phys. Rev. A* 75.3 (Mar. 2007), p. 32334. ISSN: 1050-2947. URL: https://journals.aps.org/pra/pdf/10.1103/PhysRevA.75.032334.

[10] Marco Tomamichel et al. "Leftover Hashing Against Quantum Side Information". In: *IEEE Trans. Inf. Theory* 57.8 (Feb. 2011), pp. 5524–5535. ISSN: 0018-9448. DOI: 10.1109/TIT.2011.2158473. arXiv: 1002.2436. URL: http://ieeexplore.ieee.org/document/5961850/%20http://arxiv.org/abs/1002.2436%20http://dx.doi.org/10.1109/TIT.2011.2158473.

[11] Andrew Rukhin et al. "A statistical test suite for random and pseudorandom number generators for cryptographic applications". In: *NIST Special Publication 800-22* (2010). DOI: 10.6028/nist.sp.800-22.

[12] Marco Avesani et al. "Secure heterodyne-based quantum random number generator at 17 Gbps". In: *arXiv preprint arXiv:1801.04139* (2018).

[13] S. Gómez et al. "Experimental nonlocality-based randomness generation with nonprojective measurements". In: *Physical Review A* 97.4 (Apr. 2018). DOI: 10.1103/physreva.97.040102.

[14] Matteo Schiavon, Giuseppe Vallone, and Paolo Villoresi. "Experimental realization of equiangular three-state quantum key distribution". In: *Scientific Reports* 6.1 (2016). DOI: 10.1038/srep30089.

[15] Patrick J. Coles, Eric M. Metodiev, and Norbert Lütkenhaus. "Numerical approach for unstructured quantum key distribution". In: *Nature Communications* 7 (2016), p. 11712. DOI: 10.1038/ncomms11712.