Lab 01 report: QRNG

Trusted & Source-DI QRNGs implementation

Author: **David Polzoni**

Student ID: **2082157**

Course: **Quantum Cryptography & Security**

Prof. **G. Vallone**, Prof. **N. Laurenti**

Università degli Studi di Padova

A.Y. 2023-2024

Date: February 4, 2024

Contents

1 Introduction

Random Number Generators (RNGs) are a key element in many fields, such as cryptography, AI and Monte Carlo like simulations. In particular, RNGs must be designed in order to find the proper trade-off between how much randomness they provide and how much they can be invulnerable to predictions and biases. However, it is impossible to generate true randomness with any classical algorithmic method, thus classical RNGs are usually addressed as Pseudo Random Number Generators. To avoid such issue, research has explored non-classical approaches, leading to the design of new devices: Quantum Random Number Generators (QRNGs). The advantage of QRNGs is that they do not depend on algorithms, but rather on a physical process. Indeed, since quantum phenomena are intrinsically probabilistic, they represent a source of true randomness that can be exploited to generate random bits. In particular, a leading strategy consists of employing quantum optical processes, which can be easily controlled and subjected to projective measurements. QRNGs can be divided into different categories according to the level of trustworthiness on the entropy source and on the measurements. In general, the security of a QRNG depends on the number of assumptions that we require to its physical realization: the more we trust devices, the more our system could potentially be subjected to external attacks. The two extremes are represented by Device Independent (DI) and trusted protocols. In the first case we do not have requirements on the system, while in the latter we assume to know everything about the apparatus. Our specific discussion focuses on trusted QRNG and a specific Semi-DI protocol in which we trust the measurements, but not the source of entropy: a Source-DI QRNG.

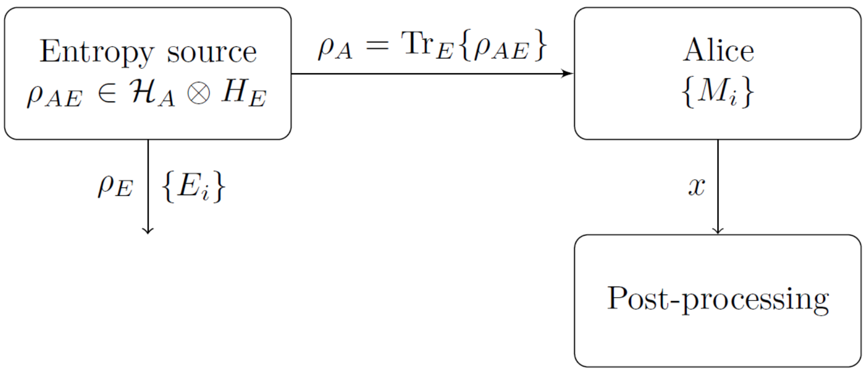


Figure 1: General scheme of a QRNG. An entropy source generates a state ρ_{AE}, and the state obtained by tracing out Eve's system is sent to Alice. Eve performs operations and measurements on her state ρ_E, while Alice on the state ρ_A. The outcome of Alice's measurements is then subjected to post-processing in order to reduce biases and provide a sequence of *iid* samples.

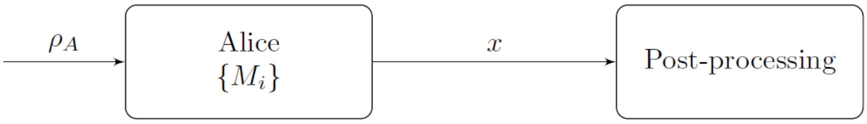


Figure 2: General scheme of a trusted QRNG. An entropy source generates a state ρ_A and Alice performs a series of measurements on it, to provide an output x. The outcome of Alice's measurements is then subjected to post-processing in order to reduce biases and provide a sample of *iid* items.

2 Background

In this section, we introduce the reader to the theoretical aspects of a QRNG, focusing on its general description and on the different methods to quantitatively compute the amount of randomness. Let us refer to the legitimate user of a given system as Alice and to an eavesdropper as Eve: Alice wants to generate a series of random bits, protecting her bits from a possible attack by Eve. The general scheme of a QRNG is shown in figure 1. Here, an entropy source generates a state ρ_{AE} in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_E$ which considers both the space $\mathcal{H}_A$ where Alice can operate, and $\mathcal{H}_E$ which is under the control of Eve. Then, Alice receives a state ρ_A which is obtained by tracing out the system of Eve:

$$\rho_A = \mathrm{Tr}_E\{\rho_{AE}\} \tag{1}$$

Finally, the legitimate user performs a set of measurement $\{M_i\}$ on the given state, and she obtains an output x. The outcome of Alice's measurement is employed to generate random bits: first it is converted into a binary raw bit sequence, then bits are post-processed in order to reduce the presence of biases and provide a sample of *iid* items. On the other side, Eve performs measurements on her state ρ_E to draw information about the outcome of Alice's measurements. We are interested in computing quantitatively the amount of information that Eve can obtain about x by performing measurements on ρ_E. First, it is worth to introduce the conditional min-entropy $H_{\min}(x|E)$, a quantity that allows us to evaluate the amount of private randomness that can be extracted out of a generated bit string. Moreover, by means of another quantity, the guessing probability, we are able to measure the amount of information about x, which is available to an attacker that performs operations only on a given state ρ_E. Thus, in our scenario, the guessing probability $P_g(x|E)$ is the probability that an agent, Eve, correctly guesses x just by its knowledge of the system E, with an optimal strategy. That concept can be mathematically expressed as follows:

$$P_g(x|E) = \max_{\{E_x\}} \sum_x P_x(x)\,\mathrm{Tr}\{E_x \rho_E^x\} \tag{2}$$

where ρ_E^x is the state of the system E that depends on a classical random variable x. The POVM that maximizes the expression above corresponds to the strategy that allows to acquire the maximum amount of information available for Eve.

Eventually, it can be proved that $H_{\min}(x|E)$ can be written in terms of $P_g(x|E)$ as:

$$H_{\min}(x|E) = -\log_2(P_g(x|E)) \tag{3}$$

2.1 Trusted QRNG

Let us first consider the trusted scenario, in this case we completely trust both the source and the measurements. Formally, we can depict this situation by employing the scheme presented in figure 1 and imposing $\mathcal{H}_E = \mathbb{1}_E$, the specific scheme is represented in figure 2. Thus, Alice receives a pure state ρ_A, and she performs trusted measurements on it. Since no side information is available, the guessing probability can be easily computed classically in the subsequent way:

$$P_g(X) = \max_x P_X(x) \tag{4}$$

thus min-entropy could be calculated as follows:

$$H_{\min}(X) = -\log_2(\max_x P_g(x)) \tag{5}$$

Therefore, it is clear that, in the trusted scenario, the outcome of a POVM allows to easily compute the amount of secure random raw bits that can be generated with the QRNG.

2.2 Source-DI QRNG

Despite its simplicity, the trusted scenario exhibits several limitations, in particular it is worth to mention that preparing a perfect pure state is impossible in practice. To overcome such issues, Semi-DI and DI protocols have been developed, since in these models such strong assumptions are relaxed. Let us consider a Semi-DI device, a Source-Device Independent protocol, in which we trust the measurement scheme, but we treat the source of entropy as a black box (we do not have any knowledge about it!). The scheme is still the one described in figure 1, in which Alice does not know the state ρ_{AE} generated by the entropy source, while Eve does. Computing the guessing probability in this framework is not straightforward as in equation 2. Therefore, different strategies must be exploited to provide, at least, an upper bound for the guessing probability (i.e. a lower bound for the min-entropy). Here we propose two approaches: Fiorentino et al. [1] method based on performing a full tomography of the state, and Tomamichel and Renner [2] approach, that applies the entropic uncertainty principle.

2.2.1 Entropic uncertainty principle method

Tomamichel and Renner [2] propose to exploit a fundamental quantum property, the entropic uncertainty principle, to provide a bound for the min-entropy. Let us consider the quantum system of figure 1, where an entropy source generates a state ρ_{AE}, while Alice receives the state ρ_A on which she can perform measurements.

Consider also two POVMs acting on ρ_A, X with elements $\{M_x\}$, and Z with elements $\{N_z\}$. Then, it is possible to prove an uncertainty relation for smooth entropies:

$$H_{\min}(X|E) + H_{\max}(Z) \geq -\log_2(c) \tag{6}$$

where $c \equiv \max_{x,\,z} \|\sqrt{M_x}\sqrt{N_z}\|_\infty^2$. Moreover, Vallone et al. [3] show that the conditional min-entropy of the X outputs can be bounded with the Rényi entropy of order $r = \frac{1}{2}$ as follows:

$$H_{\min}(X|E) + H_{\frac{1}{2}}(Z) \geq -\log_2(c) \tag{7}$$

where we can compute explicitly Rényi entropy as:

$$H_{\frac{1}{2}}(Z) = 2\log_2 \sum_z \sqrt{P_Z(z)} \tag{8}$$

In the particular case of mutually unbiased bases on a d-dimensional Hilbert space, the constant c can be easily computed in the subsequent way:

$$\log_2(c) = -\log_2(d) \tag{9}$$

Such result allows to compute a bound to the conditional min-entropy of the random variable X, by measuring on another basis with projective measurements Z.

2.2.2 Full tomography method

Following the procedure exposed by Fiorentino et al. [1], thus by performing a full tomography of a 2-dimensional state, it is possible to provide a lower bound for the min-entropy of the system. Indeed, the authors prove that, considered the generic case of a mixed state ρ, the min-entropy is lower bounded as follows:

$$-\log_2\left(\frac{1+\sqrt{1-|S_1 - iS_2|^2}}{2}\right) \leq H_{\min}(\rho) \tag{10}$$

where S_i are Stokes coefficients obtained by decomposing the density matrix as $\rho = \frac{1}{2}\left(\mathbb{1} + \vec{S}\vec{\sigma}\right)$. As a consequence, $P_g(X|E)$ is upper bounded by:

$$P_g(X|E) \leq \frac{1+\sqrt{1-|S_1 - iS_2|^2}}{2} \tag{11}$$

This procedure is based on performing measurements on different bases, in order to reconstruct the density matrix of the unknown state through a full tomography. Once the density matrix is known, it is possible to write it in terms of Stokes parameters and compute the bound.

3 LHL for security parameter estimation

The discussion developed in the previous sections shows that a QRNG can theoretically produce random numbers with provable randomness. In practice, the generated series of random bits does not consist of independent and uniform samples. Thus, in order to have real quantum randomness and generate a series of *iid* values, we need to introduce post-processing procedures that allow to extract randomness from raw bits. We refer to such post-processing protocols as *strong seeded extractors.* A leading strategy to extract randomness is based on the usage universal of hashing families. In particular, in the classical scenario in which there is classical side information available to an eavesdropper, the Leftover Hasting Lemma (LHL) provides a bound on the security parameter of the protocol, the unconditional distinguishability. It can be shown that the security parameter ϵ to design a ϵ-unconditional secure protocol depends both on H_{min} and the length of the extracted bits l_z. To be more specific, the LHL asserts that the number of bits that we can extract stands in a well defined relation with the guessing probability: the more an attacker knows about the random variable X generated by Alice, the less secure bits she can extract by means of universal hashing families. Let us now move to the quantum scenario, and consider the framework of Source-DI QRNGs. In this context, there is quantum side information available to the eavesdropper, thus a generalization of the LHL is required. Tomamichel et al. [5] provide such generalization, stating the subsequent lemma:

Lemma 1. *Let X be a random variable, let E be a quantum system, and let $\mathcal{F}$ be a δ-almost two-universal family of hash functions from X to $\{0,1\}^{l_z}$. Then, on average over the choices of f from $\mathcal{F}$, the output Z = f(X) is Δ-close to uniform conditioned on E. In particular, if $\mathcal{F}$ is two-universal, Δ can be derived as follows:*

$$\Delta = 2^{\,(l_z/2\,-\,H_{\min}(X|E)/2\,-\,1)} \tag{12}$$

The connection with the security parameter is straightforward: Δ provides a bound on the trace distance, thus, if we want our protocol to be ϵ-unconditional secure we must impose $\epsilon = \Delta$, such that:

$$d_{\text{v}}(\rho_{ZSE},\ \rho^*_{ZSE}) \leq \epsilon = 2^{\,(l_z/2\,-\,H_{\min}(X|E)/2\,-\,1)} \tag{13}$$

where $d_{\text{v}}(\rho_{ZSE},\ \rho^*_{ZSE})$ represents the trace distance between the real state and the ideal one, Z refers to the range of the hash function and S to the seed employed.

4 Experimental realization

Let us now go deeper into the discussion of a possible physical implementation of such protocols. We realize a QRNG by employing qubits encoded into the electric field polarization of photons. Indeed, all the possible pure polarization states can be obtained from coherent superposition of two linear polarizations: horizontal $|H\rangle = |0\rangle$ and vertical $|V\rangle = |1\rangle$. In particular, diagonal $|D\rangle$, anti-diagonal $|A\rangle$, left-circular $|L\rangle$ and right-circular $|R\rangle$ photons states can be written in H/V basis as:

$$\begin{aligned} |D\rangle &= \frac{|H\rangle + |V\rangle}{\sqrt{2}},\ |A\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}}, \\ |L\rangle &= \frac{|H\rangle - i\,|V\rangle}{\sqrt{2}},\ |R\rangle = \frac{|H\rangle + i\,|V\rangle}{\sqrt{2}} \end{aligned} \tag{14}$$

Eventually, it is worth to point out that, in D/A basis, a pure L state can be described as:

$$|L\rangle = \left(\frac{1-i}{2}\right)|D\rangle + \left(\frac{1+i}{2}\right)|A\rangle \tag{15}$$

Our approach is based on measuring the state ρ on the three bases discussed above. The main interest is indeed to recover information about the original state ρ_A my means of projective measurements. In particular, this approach allows to reconstruct ρ by measuring on all the three polarization bases discussed above, as it is discussed by James et al. [4]. Once the probabilities are known, it is possible to compute the corresponding Stokes parameters as follows:

$$\begin{aligned} S_0 &= \langle H|\rho|H\rangle + \langle V|\rho|V\rangle \\ S_1 &= \langle D|\rho|D\rangle - \langle A|\rho|A\rangle \\ S_2 &= \langle R|\rho|R\rangle - \langle L|\rho|L\rangle \\ S_3 &= \langle H|\rho|H\rangle - \langle V|\rho|V\rangle \end{aligned} \tag{16}$$

Such parameters are then employed to reconstruct the density matrix:

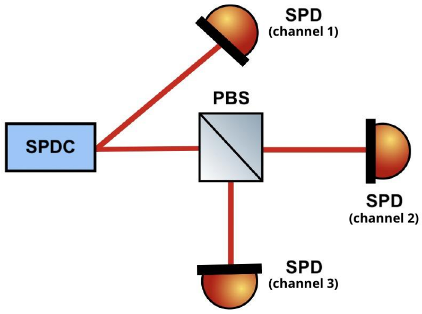
$$\rho = \frac{1}{2}\sum_{i=0}^{3}\frac{S_i}{S_0}\,\sigma_i \tag{17}$$

where $\sigma_0 = \mathbb{1}_2$ and σ_i for $i = 1, 2, 3$ are the Pauli matrices.

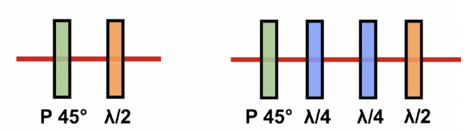
4.1 Apparatus and measurements

Let us describe the experimental setup, in order to understand how the procedure can be implemented in practice. The general scheme for the experiment is described in figure 3a. We first employ a Spontaneous Parametric Down-Converter (SPDC) to split a photon into two entangled photons of lower energy. One photon is referred as *tagged*, it is detected by a Single Photon Detector (SPD) in order to individuate coincidences with the other photon, which is the real object of our measurements.

Indeed, the SPDC generates the second photon in a mixed state, on which we can operate in order to generate a pure state and perform measurements on different bases. Thus, the second photon can be prepared both in a mixed or in a pure state, by employing a polarizer and waveplates. It is then subjected to projective measurements performed through a Polarizing Beam Splitter (PBS), which transmits horizontally polarized photons and reflects vertically polarized photons, that are detected by two SPDs. Eventually, a time-to-digital converter registers time-tags in ps: the tagged photon is detected in channel 1, while transmitted photons in channel 2, and reflected in channel 3.



(a) General scheme of the apparatus is made up by a SPDC, a PBS and multiple SPDs.



(b) Optical setup to generate, from a mixed state, a pure D state to measure on D/A basis (on the left) and a pure L state to measure on L/R basis (on the right).

Figure 3: Scheme of the apparatus for the experimental realization of a QRNG. In 3a we report the general scheme to measure a mixed state on H/V basis, instead in 3b we report two examples to generate a pure state and to measure it on a specific basis.

Let us now summarize the different setups:

- To generate a state:
  - Mixed state: SPDC generates a mixed state, which is immediately available for measurements;
  - Pure D state: 45° polarizer applied to the mixed state;
  - Pure L state: 45° polarizer and a quarter-waveplate applied to the mixed state.
- Measurement bases:
  - H/V: photon passes through a PBS;
  - D/A: half-waveplate before the PBS;
  - L/R: quarter and half-waveplate before the PBS.

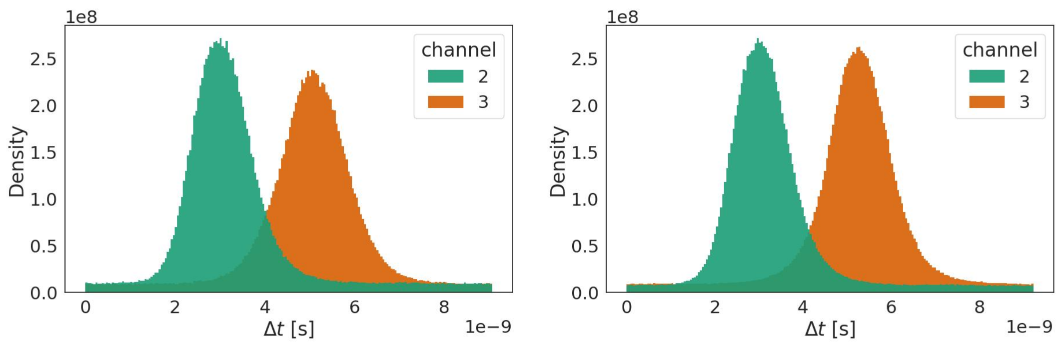
In figure 3b we report as an example the optical transformations that must be applied to a mixed state in order to measure a D state on H/V basis and to measure a L state on L/R basis. We perform measurements on H/V and D/A basis of both a mixed and a pure D state. Eventually, we realize a full tomography of a pure L state by measuring it on the three bases H/V, D/A and L/R. In table 1 we report the corresponding channel for each measurement basis.

Measurement basis	Channel 2 (transmitted)	Channel 3 (reflected)
H/V	H	V
D/A	A	D
L/R	L	R

Table 1: Correspondence between the channel in which a photon is detected by the time-to-digital converter and the corresponding basis measurements for the different setups considered.

5 Coincidences events

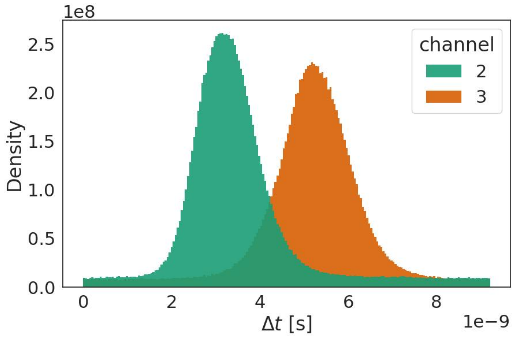
Since we are interested only in coincidences between channel 1 and either channel 2 or 3, thus in order to evaluate the probabilities of measuring a photon in a specific basis we have to take into consideration only such events which happen within a coincidence window from the photon detection in channel 1. Once we exclude independent events, coincidences are gaussian distributed, and we select only those detections of the second photon which are within a window of 4 ns from the detection of the tagged one. For counting coincidences, events on channel 1 are matched with the closest corresponding events on the other channels. Most events occur before a time difference of 4 ns. This implies that using a window of the previously specified size is sufficient to capture the majority of coincidences. It is also worth to notice that channel 2 and channel 3 are affected by constant delays for each data acquisition, see for instance figure 4a. In the following, we present the histograms of coincidences for all the cases described in the preceding sections.



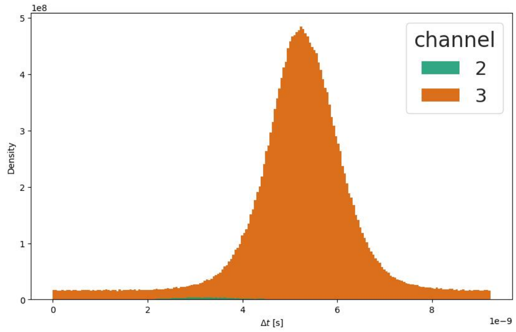
(a) Histograms of coincidences events for a mixed state measurements on H/V basis.

(b) Histograms of coincidences events for a D state measurements on H/V basis.

Figure 4: Histograms of coincidences events in a window of 4 ns for measurements of a mixed and a pure D state on H/V basis. Both the outcomes show that the probability of measuring a photon either in H or V basis is around 50%. Note that the distribution of coincidences with Δt lower than about 4 ns exhibits a gaussian distribution. This is coherent with the fact that such events are not independent.

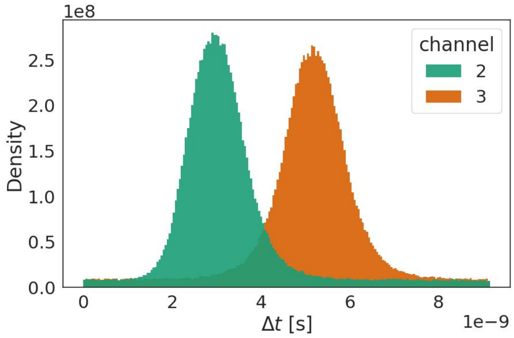


(a) Histograms of coincidences events for a mixed state measurements on D/A basis.

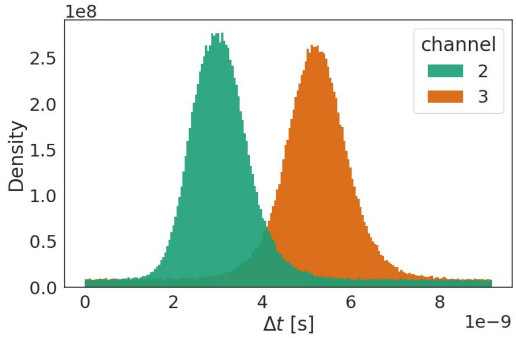


(b) Histograms of coincidences events for a D state measurements on D/A basis.

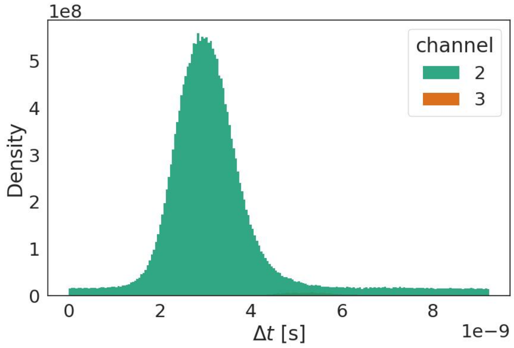
Figure 5: Histograms of coincidences events in a window of 4 ns for measurements of a mixed and a pure D state on D/A basis. The mixed state can be measured either on D and A with the same probability, while D state exhibits a huge amount of observation on channel 3, as expected.



(a) Histograms of coincidences events of a L state measurements on H/V basis.



(b) Histograms of coincidences events of a L state measurements on D/A basis.



(c) Histograms of coincidences events of a L state measurements on L/R basis.

Figure 6: Histograms of coincidences events in a window of 4 ns for measurements of a L state on all the polarization. Note that, as expected, histograms suggest that the probability of measuring L on D or A is 50%, and the same happens for H/V basis. On the other hand, by measuring on L/R basis the photon is detected with almost 100% probability in the channel corresponding to state L.

Indeed, fibers that connect optocouplers to SPDs can exhibit slightly different lengths, as well as cables that connect detectors to the time-to-digital converter. If we get rid of these delays and recenter the distributions, coincidences are normally distributed with average $\mu = 0$ and wide a few ns. Probabilities are computed as the amount of observations in a certain channel, normalized over the total amount of coincidences events considered. In particular, if we measure N events, the error over counting events is given by $\sqrt{N}$. Considering error both on the total amount N of coincidences detected and on the i-th channel N_i, the probability of detecting a photon in channel i can be derived as follows:

$$P_i = \frac{N_i}{N} \pm \sqrt{\frac{N_i}{N^2} + \frac{N_i^2}{N^3}} \tag{18}$$

6 Randomness in QRNG

Now that we have widely discussed the theoretical background and the experimental setup of trusted and Semi-DI QRNGs, we can present the results and draw conclusions concerning both the amount of randomness that can be extracted and the security of the protocol.

6.1 Trusted QRNG

In the trusted scenario we evaluate the amount of randomness as discussed in section 2.1, in particular, considering measurements errors (denoted by σ), equations 4 and 5 become:

$$\begin{aligned} P_g(X) &= \max_x P_X(x) \pm \sigma\{\max_x P_X(x)\}, \\ H_{\min}(X) &= -\log_2(\max_x P_g(X)) \pm \frac{\sigma_{P_g(X)}}{P_g(X)\log_2} \end{aligned} \tag{19}$$

Data are collected by measuring a mixed (M) and a pure D state on H/V basis, while in figure 4 we report the distribution of coincidences for these datasets. The probabilities and the corresponding $H_{\min}$, P_g are reported in table 2. Note that such observations are coherent with the theoretical definition given in equation 19. The main outcome is that measurements on a single basis do not allow us to distinguish between a pure and a mixed state, since the distributions are equivalent. That's why we need to trust the source in the case we measure only on H/V basis.

State	P_H	P_V	P_g	$H_{\min}$
M	0.504 ± 0.001	0.496 ± 0.001	0.504 ± 0.001	0.990 ± 0.002
D	0.483 ± 0.001	0.517 ± 0.001	0.517 ± 0.001	0.952 ± 0.002

Table 2: Probabilities of measuring a mixed (M) and a pure D state on H/V basis and the corresponding guessing probabilities and min-entropies in the trusted scenario. By measuring on H/V basis, it is impossible to distinguish between a pure D state and a mixed state, since all the probabilities are around 50%. As a consequence, the guessing probability is about 50%, and min-entropy tends to 1.

6.2 Source-DI QRNG

We have discussed that a limit of measurements on a single basis is that in this case we cannot distinguish between a pure and a mixed state, so we need to trust the source. To overcome such issue and relax the hypothesis, Semi-DI protocols are introduced.

6.2.1 Entropic uncertainty principle

A possible way to compute the amount of randomness that it is possible to generate with a Source-DI QRNG employs the theoretical results achieved by Tomamichel and Renner [2] and Vallone et al. [3], as discussed in section 2.2.1. We will first consider measurements of a mixed (M) and a pure D state both on D/A and H/V bases.

Thus, with this setup, we will be able to generate the random variables X and Z by considering as POVMs the projective measurements over the bases $Z = \{|D\rangle, |A\rangle\}$ and $X = \{|H\rangle, |V\rangle\}$. In this context, the bound over the amount on randomness that we can extract from x (equation 7), can be written as:

$$H_{\min}(x|E) \geq 1 - 2\log_2\left(\sqrt{P_A} + \sqrt{P_D}\right) \tag{20}$$

while the errors (denoted as σ) can be computed in the subsequent way:

$$\begin{aligned} \sigma_{H^b_{\min}} &= \frac{1}{\log_2}\frac{1}{\sqrt{P_A}+\sqrt{P_D}}\sqrt{P_A^{-1}\,\sigma^2_{P_A} + P_D^{-1}\,\sigma^2_{P_D}}, \\ \sigma_{P^b_g} &= \frac{1}{\log_2}\,2^{-H^b_{\min}}\,\sigma_{H^b_{\min}} \end{aligned} \tag{21}$$

where the apex b stands for the bound. Our purpose is indeed to provide a bound on the amount of randomness that we can extract on H/V by measuring on a mutually unbiased bases, D/A in this case. The distributions of coincidences for the D/A measurements are shown in figure 5, while in table 3 we report the observed probabilities and the amount of randomness quantified by the min-entropy. In particular, observe that the upper bound of the guessing probability is ≈ 1, which is coherent with what we expected. Indeed, when the original state ρ_{AE} is pure, due to the presence of an eavesdropper, Alice receives a state ρ_A which is mixed. Then, such procedure allows us to individuate the presence of an attacker in the protocol. On the other hand, when the measured state is pure, the bound on the guessing probability is lower, while the min-entropy increases.

State	P_D	P_A	P_g	$H_{\min}$
M	0.509 ± 0.001	0.491 ± 0.001	0.999 ± 0.002	8e-06 $\pm$ 1e-06
D	0.991 ± 0.002	0.009 ± 0.0002	0.593 ± 0.002	0.755 ± 0.002

Table 3: Probabilities of measuring a mixed (M) and a pure D state on D/A basis and the corresponding bounds on the guessing probability and min-entropy, computed with the method proposed by Tomamichel and Renner [2] and Vallone et al. [3]. The mixed state can be detected with equal probability on D and A, while, as expected, a pure D state is measured with almost 100% probability on D. Thus, this setup allows us to distinguish between a pure and a mixed state.

For what concerns the final set of measurements, we will consider a pure L state measured on all the bases H/V, D/A, L/R. In this case, we can bound the amount of randomness available for the variable x associated to projective measurements on H/V basis both by measuring on D/A and L/R, by defining $Z = \{|D\rangle, |A\rangle\}$ and $Y = \{|L\rangle, |R\rangle\}$. The corresponding bounds are defined as follows:

$$\begin{aligned} H_{\min}(x|E) &\geq 1 - 2\log_2\sum_z\sqrt{P_Z(z)}, \\ H_{\min}(x|E) &\geq 1 - 2\log_2\sum_y\sqrt{P_Y(y)} \end{aligned} \tag{22}$$

while the errors are computed applying the same approach used in equation 21.

The distributions of coincidences are shown in figure 6, while in table 4 we report the observed probabilities and the bounds for P_g and $H_{\min}$. Note that measurements of a pure L state on L/R basis provide a tighter bound if compared with measurements performed on the D/A. Thus, to define a significative bound to the guessing probability and individuate the presence of an eavesdropper, it is convenient to measure on L/R basis. The situation is then analogue to the one that we have already discussed regarding a pure D state measured on D/A.

State	P_{ch_2}	P_{ch_3}	P_g	$H_{\min}$
Bounding X with Z	0.494 ± 0.001	0.506 ± 0.001	0.999 ± 0.0003	5e-05 $\pm$ 2e-05
Bounding X with Y	0.987 ± 0.002	0.013 ± 0.0002	0.612 ± 0.002	0.708 ± 0.003

Table 4: Probabilities of measuring a pure L state on the following bases: $Z = \{|D\rangle, |A\rangle\}$, $Y = \{|L\rangle, |R\rangle\}$. The state can be detected with equal probabilities on D/A, while, on L/R it is measured with almost 100% probability on L, as expected.

6.2.2 Full tomography

Let us now consider the method proposed by Fiorentino et al. [1] and discussed in section 2.2.2. The idea is to exploit a full tomography of the quantum state to provide a quantitative bound for the min-entropy and the guessing probability in the Semi-DI scenario. To do so, we need to reconstruct the full density matrix, thus we perform measurements on all the orthogonal bases H/V, D/A and L/R. Such measurements allow to compute the Stokes parameters (equation 16). For what concerns the evaluation of the errors, since every Stokes parameter S_i is the algebraic sum of two probabilities P_i and P_j , their errors can be computed as $\sigma_{S_i} = \sqrt{\sigma^2_{P_i} + \sigma^2_{P_j}}$. Therefore, from equations 10 and 11, we can retrieve the statistical uncertainty (denoted as σ) on $H_{\min}$ and P_g in the subsequent way:

$$\begin{aligned} \sigma_{P_g^b} &= \frac{\left(1 - S_1^2 - S_2^2\right)^{-\frac{1}{2}}}{2} \sqrt{S_1^2\, \sigma^2_{S_1} + S_2^2\, \sigma^2_{S_2}} \\ \sigma_{H^b_{\min}} &= \frac{\sigma_{P_g(X)}}{P_g(X) \log_2} \end{aligned} \tag{23}$$

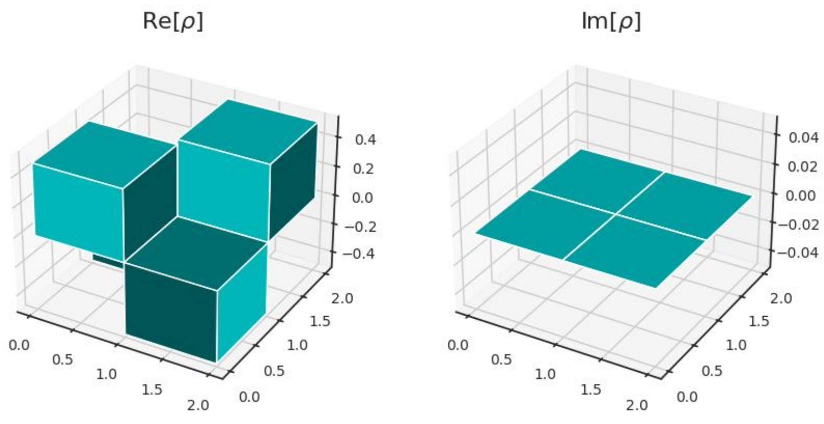
Let us first consider data concerning measurements of a mixed and a pure D state on H/V and D/A bases, to perform a full tomography we assume that the second Stokes parameter is null $S_2 = 0$. The density matrices are reported respectively in figures 7a, 7b and 8, or equivalently in matrix form as follows:

$$\begin{aligned} \rho_D &= \begin{bmatrix} 0.4830 + 0i & -0.491 + 0i \\ -0.491 + 0i & 0.517 + 0i \end{bmatrix} \\ \rho_M &= \begin{bmatrix} 0.503 + 0i & 9.44\text{e-}03 + 0i \\ 9.44\text{e-}03 + 0i & 0.496 + 0i \end{bmatrix} \\ \rho_L &= \begin{bmatrix} 0.493 + 0i & \text{-}5.98\text{e-}03 - 0.487i \\ \text{-}5.98\text{e-}03 - 0.487i & 0.507 + 0i \end{bmatrix} \end{aligned} \tag{24}$$

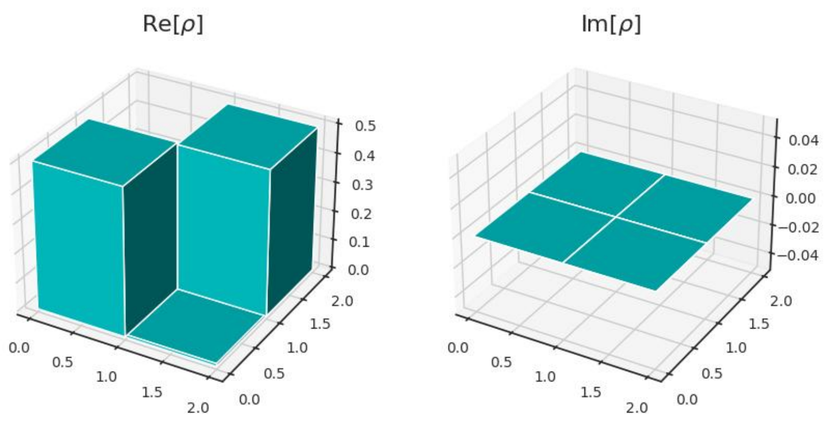
Indeed, the numerical results in terms of P_g and $H_{\min}$ are shown in table 5.

State	P_g	$H_{\min}$
D	0.612 ± 0.004	0.708 ± 0.001
M	$0.999 \pm$ 9e-06	4e-06 $\pm$ 2e-06
L	0.593 ± 0.003	0.755 ± 0.001

Table 5: Bounds on guessing probability and min-entropy computed with Fiorentino et al. [1] method. The guessing probability corresponding to a mixed state (M) is $P_g^M \approx 1$, which is a clear sign of the presence of an eavesdropper and a lack in the security of the model. Moreover, the amount of randomness that can be extracted from such a setup is negligible. On the other hand, the guessing probabilities corresponding to D and L states lead to non-null values of min-entropy.



(a) Density matrix of a pure D state, we assumed the second Stokes parameter to be null $S_2 = 0$.



(b) Density matrix of the generated mixed state, we assumed the second Stokes parameter to be null $S_2 = 0$.

Figure 7: Real and imaginary part of the mixed and pure D state density matrices. Here, we considered the second Stokes parameter to be null, since we did not measure such states on L/R basis.

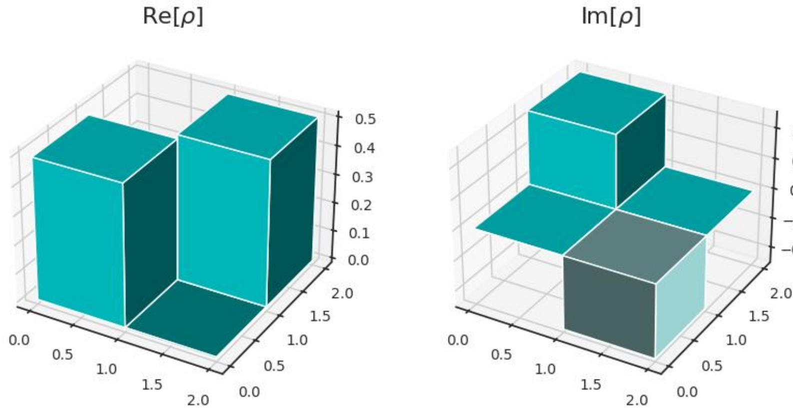


Figure 8: Real and imaginary part of the pure L state density matrix. It serves as a comprehensive representation, providing a complete reconstruction of the pure L state.

As can be seen from the above results, the guessing probability corresponding to a mixed state is $P_g^M = 0.999 \pm$ 9e-06, thus an attacker has high probability of drawing information about Alice's measurements by measuring the state ρ_E. As a consequence, such protocol cannot be employed as QRNG, since the amount of secure randomness that can be extracted from such setup is almost zero. On the other hand, the bound on the guessing probability corresponding to D is $P_g^D = 0.612 \pm 0.004$, with $H_{\text{min}}^D = 0.708 \pm 0.001$. Let us now consider the datasets collected about measurements of a pure L state, in this case we are able to perform a full tomography without assumptions on the system, since we measured L on all the bases. The worst case guessing probability is $P_g^L = 0.593 \pm 0.003$, with $H_{\text{min}}^L = 0.755 \pm 0.001$. Physically speaking, the non null min-entropies computed for the D and L state, mean that we are able to extract secure randomness from the protocol.

7 Security parameter estimation

To complete our analysis, it is worth to compute quantitatively the security of the protocols discussed above after the randomness extraction. In order to do so, we employ the strategy proposed by Tomamichel et al. [5] that we briefly summarized in section 3. Let us now consider the statistical uncertainty on ϵ security parameter, from equation 13, as follows:

$$\sigma_\epsilon = \sigma_{H_{\min}} \log(2)\ 2^{\,(l_z/2 - H_{\min}(X|E)/2 - 2)} \tag{25}$$

In figure 9, we report the security parameter ϵ from the LHL as function of the block length, for fixed values of min-entropy. In particular, we consider the values of min-entropies computed in the previous sections and the main outcome turns out to be that the security parameter grows exponentially with the length l_z of the block. Moreover, comparing the trends with different values of min-entropy, it is clear that the security parameter decreases for higher values of $H_{\min}$. This observation is coherent with the definition of min-entropy: low values of ϵ correspond to more security (ϵ-unconditional security) while higher values of $H_{\min}$ are associated with more secure randomness available.

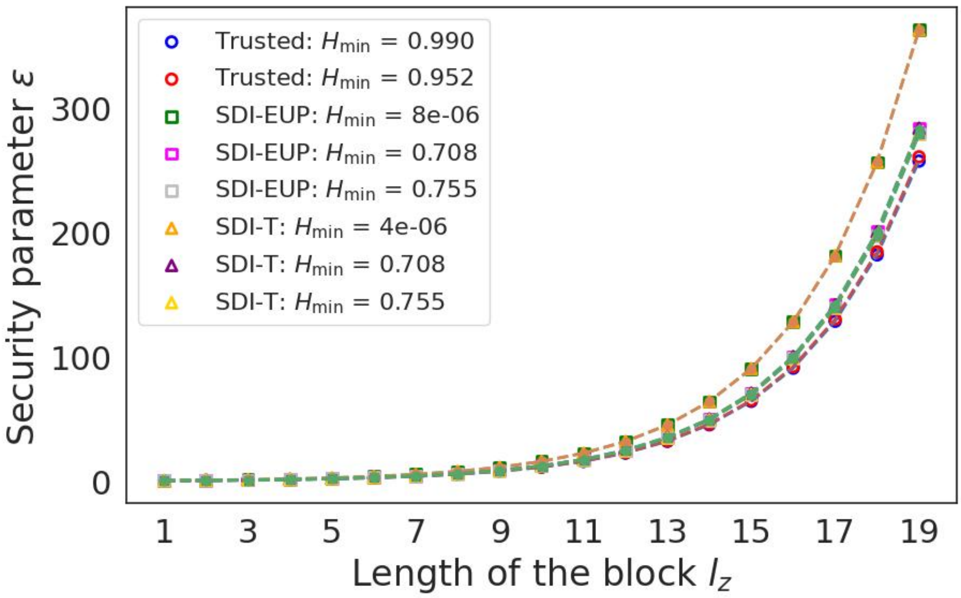


Figure 9: The security parameter ϵ from the LHL is exponential in the block length for every fixed min-entropy. Moreover, ϵ exhibits a decreasing behaviour as the min-entropy increases. We show the trends corresponding to all the min-entropies computed in the previous sections.

8 Conclusions

Let us now briefly summarize our results and draw some conclusions. We first implemented a trusted QRNG and measured the amount of secure randomness that can be generated with such protocol. Nevertheless, such approach exhibits some limitations due to assumptions that we are requiring to the system, in particular we cannot distinguish a pure and a mixed state just measuring on the basis in which we want to generate random bits. Moreover, generating a perfect pure state is a delicate and complex task in practice. To avoid such issues, we designed a Source-DI protocol by measuring both a mixed state on H/V and D/A bases, and measuring a pure L state on all the polarization bases. Then, by applying Fiorentino et al. [1] method and the approach proposed in Vallone et al. [3], we could give an estimation of the worst case guessing probabilities and min-entropies. Eventually, we showed the trend of the security parameter ϵ from the LHL as function of the block length for all the min-entropies computed. If there is an interest in delving into the developed code, it can be found at the following link: `QC&S-Lab-01-QRNG-Report`.

References

[1] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro. Secure self-calibrating quantum random-bit generator. Phys. Rev. A, 75:032334, March 2007. DOI: 10.1103/PhysRevA.75.032334. URL: https://link.aps.org/doi/10.1103/PhysRevA.75.032334;

[2] M. Tomamichel and R. Renner. Uncertainty relation for smooth entropies. Physical Review Letters, 106(11), March 2011. ISSN 1079-7114. DOI: 10.1103/physrevlett.106.110506. URL: http://dx.doi.org/10.1103/PhysRevLett.106.110506;

[3] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi. Quantum randomness certified by the uncertainty principle. Phys. Rev. A, 90:052327, November 2014. DOI: 10.1103/PhysRevA.90.052327. URL: https://link.aps.org/doi/10.1103/PhysRevA.90.052327;

[4] Daniel F. V. James, Paul G. Kwiat, William J. Munro, and Andrew G. White. Measurement of qubits. Phys. Rev. A, 64:052312, October 2001. DOI: 10.1103/PhysRevA.64.052312. URL: https://link.aps.org/doi/10.1103/PhysRevA.64.052312;

[5] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. IEEE Transactions on Information Theory, 57(8):5524-5535, August 2011. ISSN 1557-9654. DOI: 10.1109/tit.2011.2158473. URL: http://dx.doi.org/10.1109/TIT.2011.2158473.