Trusted and Source-Device independent QRNGs implementation

Nicole Zattarin

1 Introduction

Random Number Generators (RNG) 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 the randomness that they can 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 (QRNG).

QRNGs do not depend on complex algorithms but rather on a physical process to provide true randomness, indeed quantum phenomena are intrinsically probabilistic, thus 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 easily controlled and measured.

QRNGs can be divided into different categories according to the level of trustworthiness on the quantum 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 the devices, the more our system could be potentially subjected to external attacks. The two extremes are represented by Device Independent (DI) protocols, in which we do not have requirements on the system, and trusted models, in which we assume to know everything about the apparatus. Our specific discussion focuses on trusted QRNGs and a Semi-DI protocol in which we trust the measurements but not the source of entropy: Source-Device Independent QRNGs.

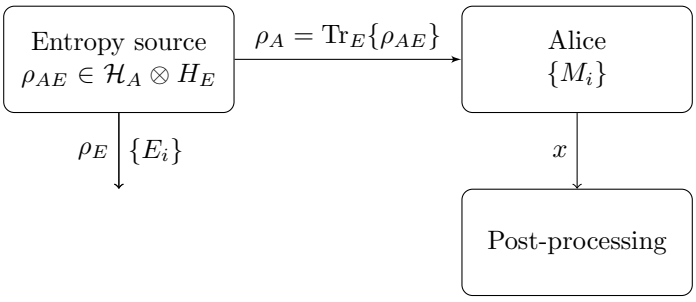


Figure 1: General scheme of a QRNG. An entropy source generates a state ρ_{AE}, whose purification from Eve's system is sent to Alice. Eve performs operations and measurements on her state ρ_E, while Alice on the state ρ_A. The outcome of Alice's measurements is then subjected to post-processing in order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

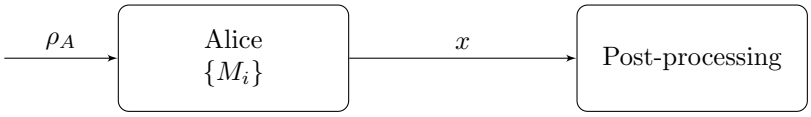


Figure 2: General scheme of a trusted QRNG. An entropy source generates a state ρ_A and Alice performs a series of measurements on it, to provide an output x. The outcome of Alice's measurements is then subjected to post-processing in order to reduce biases and provide a sequence of iid samples.

2 Background

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, while Eve aims to discover the corresponding information. In this context, the general scheme of a QRNG is shown in Figure 1. Here, an entropy source generates a state ρ_{AE} in the Hilbert space obtained as tensor product of both the spaces of Alice and Eve: $\mathcal{H}_A \otimes \mathcal{H}_E$. Then, Alice receive a state ρ_A which is obtained by tracing out the system of Eve:

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

Alice performs a set of measurement $\{M_i\}$ on the given state, the result of such measurement is the value x of the observable. The outcome of Alice 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 strings. Moreover, by means of another quantity, the guessing probability, it is also possible 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, in formula:

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

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. It can be proved that $H_{min}(x|E)$ can be written in terms of $P_g(x|E)$ as follows:

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

H_{min} measures the amount of randomness that characterises x.

2.1 Trusted QRNG

Let us first consider the trusted scenario, in this case we completely trust the source, which is equivalent to say that our protocol is not subjected to external attacks. Formally we can think about this situation by employing the scheme exposed in Figure 1 and imposing $\mathcal{H}_E = \mathbb{1}_E$, the equivalent scheme is represented in Figure 2. Alice receives a state ρ_A, which is a pure state, and she performs measurements on it.

Since no side information is available, the guessing probability can be easily computed as follows:

$$P_g(x) = \max_x P_x(x), \tag{4}$$

thus min-entropy reads:

$$H_{min}(x) = -\log_2 \max_x P_x(x). \tag{5}$$

Therefore, it is clear that the outcomes of a POVM on a state in such scenario allows us to compute easily the amount of secure random raw bits that can be generated through a trusted QRNG.

2.2 Source-Device Independent QRNG

In practice, the trusted scenario shows several limitations, it is worth to mention that preparing a perfect pure state is impossible. To overcome such issues Semi-DI and DI protocols have been developed, as models in which such strong assumptions are relaxed. Let us consider in particular 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, about which we do not have any knowledge. Thus, 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.

In this framework computing (2) is not straightforward, thus 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. [2007] method based on the full tomography of the given state, and Tomamichel and Renner [2011] approach, that applies the uncertainty principle.

2.2.1 Uncertainty principle method

Tomamichel and Renner [2011] propose to exploit a fundamental quantum property, the uncertainty principle, to provide a bound for the min-entropy. In particular, let us consider the same quantum system of Figure 1, where an entropy source generates a state ρ_{AE}, while Alice receive the purified 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 show that there exists an analogue of the uncertainty relation for smooth entropies:

$$\begin{aligned} &H_{min}(x|E) + H_{max}(z) \geq -\log_2 C, \\ &\text{with} \quad C \equiv \max_{x,z} \left\| \sqrt{M_x}\sqrt{N_z} \right\|_\infty^2 . \end{aligned} \tag{6}$$

Moreover, Vallone et al. [2014] show that the conditional min-entropy of the X outputs can be bounded with the Rényi entropy of order 1/2 of the X outputs as follows:

$$H_{min}(x|E) + H_{1/2}(z) \geq -\log_2 C, \tag{7}$$

where we can compute explicitly Rényi entropy:

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

In the particular case of mutually unbiased basis on a d-dimensional Hilbert space, the constant C can be easily computed as follows:

$$\log_2 C = -\log_2 d. \tag{9}$$

Such result allow us to compute a bound to the conditional min-entropy of the variable X, with a random variable Z, where measurements are performed on two mutually unbiased basis.

2.2.2 Full tomography method

Following the procedure exposed by Fiorentino et al. [2007], thus by performing a full tomography of a 2-dimensional state, we can obtain a lower bound for the min-entropy of the system. The authors of the mentioned work 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 $\rho = \frac{1}{2}(\mathbb{1} + \vec{S}\vec{\sigma})$. As a consequence, P_g is upper bound reads:

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

The procedure is based on performing measurements on different basis, 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 Leftover Hashing Lemma (LHL) for security parameter estimation

The discussion that we have 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 consists of independent and uniform samples. Thus, to distill real quantum randomness and generate a series of iid values, we need to introduce post-processing procedures that allows us to *extract* randomness from raw bits. We refer to such post-processing protocols as *random extractors*.

A leading strategy to extract randomness is represented by universal hashing, since universal hashing families can be employed for such purpose. Indeed, in a classical scenario in which there is classical side information available to an eavesdropper, the classical Leftover Hasting Lemma (LHL) provides a bound on the security parameter of the protocol: unconditional distinguishability. It can be shown that the bound ϵ on unconditional distinguishability, to have a ϵ-unconditional secure protocol, depends on H_{min} and the length of the extracted bits ℓ_z. Thus ,the LHL asserts that the number of bits that we can extract stands in a specific relation with the guessing probability: the more the eavesdropper knows about the random variable X generated by Alice, the less $\epsilon-$unconditional secure bits we can extract.

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. [2011] provide such generalization, stating the Lemma that follows.

Lemma 1 *(General Leftover Hashing Lemma) 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 $\{0,1\}^{\ell_z}$. 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 reads:*

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

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:

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

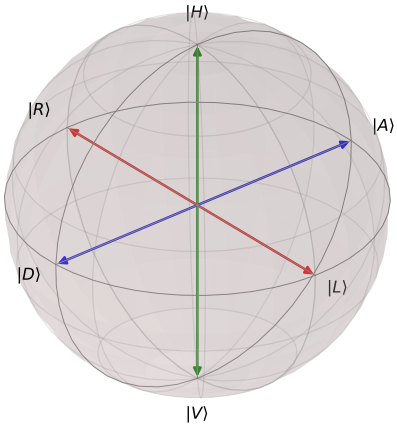


Figure 3: Representation of the polarization states on the Bloch sphere. $|H\rangle$ and $|V\rangle$ are the actual implementation of the more abstract states $|0\rangle$ and $|1\rangle$, thus $|D\rangle$ and $|A\rangle$ are states $|+\rangle$ and $|-\rangle$. Finally, $|R\rangle$ and $|L\rangle$ represent the third orthogonal basis.

where $d_v(\rho_{ZSE}, \rho^*_{ZSE})$ is 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

We perform the physical realization of 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: vertical $|V\rangle = |1\rangle$ and horizontal $|H\rangle = |0\rangle$. In particular diagonal $|D\rangle$, antidiagonal $|A\rangle$, right-circular $|R\rangle$, and left-circular $|L\rangle$ photons states can be written in H/V basis as:

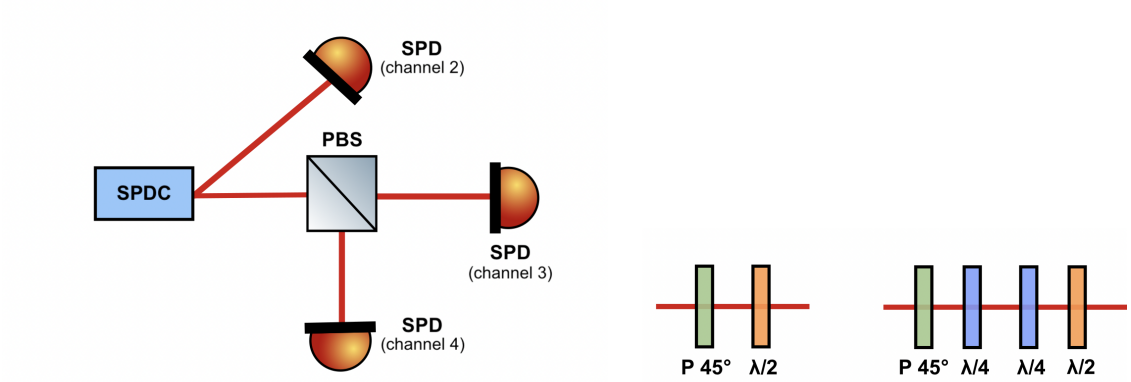
$$\begin{aligned} |D\rangle &= \frac{|H\rangle + |V\rangle}{\sqrt{2}}, \quad |A\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}}, \\ |R\rangle &= \frac{|H\rangle + i\,|V\rangle}{\sqrt{2}}, \quad |L\rangle = \frac{|H\rangle - i\,|V\rangle}{\sqrt{2}}. \end{aligned} \tag{14}$$

In Figure 3 we report the representation of such states on the Bloch sphere. Eventually, it is worth to point out that in D/A basis a pure L state reads:

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

Our approach is based on measuring the state ρ on the three basis discussed above. We are interested in recovering information about the original state my means of projective measurements, thus we measure the state on different elements of a given basis in order to get an estimation of the probabilities.

In particular, this approach allows us to reconstruct ρ by measuring on all the three polarization basis discussed above, as it it discussed by James et al. [2001]. Once we have the projections on each state, we



((a)) The general scheme of the apparatus is made up by a SPDC, a PBS and multiple SPD. The SPDC splits a photon into two entangled photons, both in a mixed state. The heralded photon is detected by a SPD and time-tagged by the time-to-digital converter in channel 2. The second photon passes through the PBS, thus finally the time-to-digital converter registers transmitted photons in channel 3 and reflected in channel 4.

((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). On the left: a pure D state is generated by means of a 45° polarizer and measured on D/A basis with a half-waveplate and a PBS. On the right: a pure L state is generated by means of a 45° polarizer and a quarter-waveplate, then it is measured on L/R basis with a quarter- and half-waveplate before the PBS.

Figure 4: Scheme of the apparatus for the experimental realization of a QRNG. In 4(a) we report the general scheme to measure a mixed state on H/V basis, in 4(b) we report two examples to generate a pure state and to measure it on a specific basis.

can 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 compute the density matrix:

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

where $\sigma_= \mathbb{1}_2$ and σ_i with $i = 1, 2, 3$ are Pauli matrices.

4.1 Apparatus and measurements

Let us describe the experimental setup, in order to understand how the procedure described can be implemented in practice. The general scheme for the experiment is described in Figure 4(a). 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 *heralded*, 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 basis. Thus, the second photon can

Measurement basis	Channel 3 (transmitted)	Channel 4 (reflected)
H/V	H	V
D/A	D	A
L/R	R	L

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. For instance, if we are measuring on the H/V basis the detection of a photon in channel 3 corresponds to a measurement on H, while channel 4 corresponds to the state V.

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 Polarization Beam Splitter (PBS), which transmits horizontally polarized photons and reflects vertically polarized photons, that are detected by two SPD. Eventually, a time-to-digital converter registers, in picoseconds, the time-tag of heralded photon detections in its channel 2, transmitted photons are registered in channel 3, while reflected photon in channel 4.

Let us now summarize the different setups:

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

In Figure 4(b) 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 basis of both a mixed state and a pure D state, then we repeat the measure of the same states on D/A basis. Eventually, we realize a full tomography of a pure L state by measuring it on the three basis H/V, D/A and L/R. In Table 1 we report the corresponding channel for each measurement basis.

4.2 Coincidence events

The only events we are interested in are the coincidences between channel 2 and either channel 3 or 4, 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 detection of a photon in channel 2. Indeed, if we evaluate the time that occurs between the detection of the heralded photon and a photon on channel 3 or 4 we obtain the exponential distribution in Figure 5. Since most of the Δt exhibit an exponential distribution, the corresponding events are independent, therefore those data do not correspond to coincident detections of the two photons.

Once we exclude independent events, coincidences are gaussian distributed with a standard deviation of a few ns. Moreover, channel 3 and channel 4 are affected by constant delays for each data acquisition,

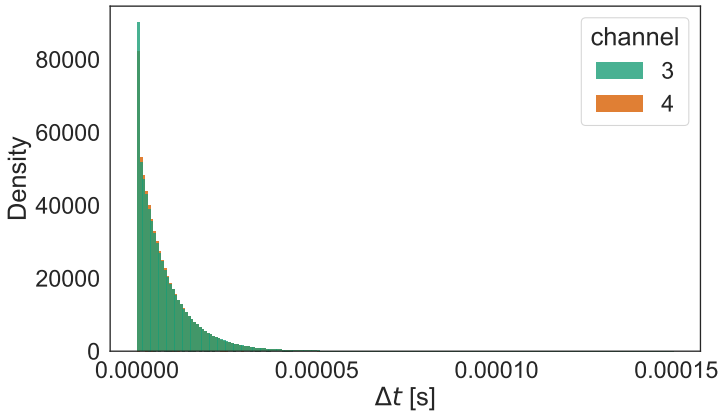


Figure 5: The majority of time differences between the detection of a photon in channel 2 and in either channel 3 or 4 are independent events. The Δt between the revelation of photons exhibits an exponential distribution, which means that the single events are independent. We are not interested in such behaviour, since we take into account only those detections of a photon in channel 3 or 4 which happen in coincidence with channel 2, thus correlated to observations in channel 2.

see for instance Figure 6(a). Indeed, fibers that connect optocouplers to single photons detectors can have 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. The only data that we take into account in our analysis are those events within the gaussian distribution. Note that in general, the detection on channel 2 can either anticipate or follow the detection in the other channels.

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 reads:

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

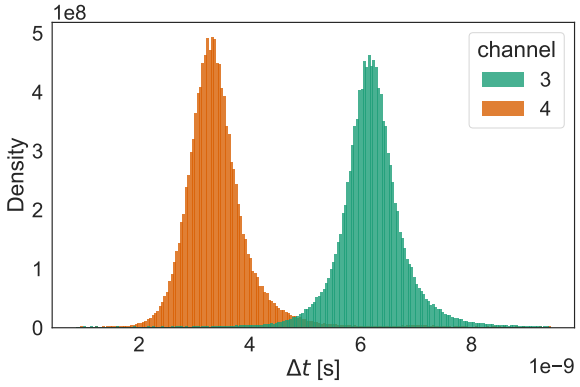
5 Randomness in QRNGs

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

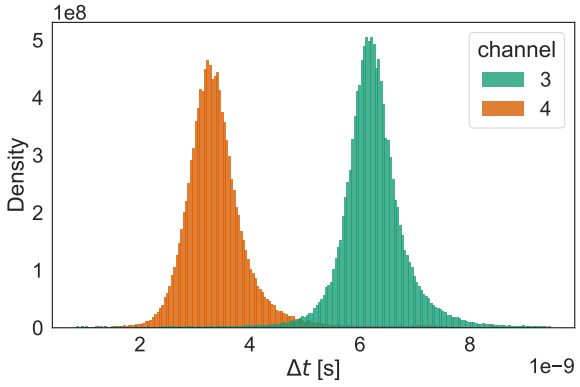
5.1 Trusted QRNG

In the trusted scenario we can evaluate the amount of randomness as discussed in Section 2.1, in particular, considering measurements errors, Equations (4) and (5) become:

$$\begin{aligned} P_g(x) &= \max_x P_x(x) \pm \sigma_{\max_x P_x(x)}, \\ H_{min}(x) &= -\log_2 P_g(x) \pm \frac{\sigma_{P_g(x)}}{P_g(x)\log 2}. \end{aligned} \tag{19}$$



((a)) Histograms of coincidences events in a window of 3ns for measurements of a mixed state on H/V basis.



((b)) Histograms of coincidences events in a window of 3ns for measurements of a D state on H/V basis.

Figure 6: Histograms of coincidences events in a window of 3ns 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 10ns exhibits a gaussian distribution. This is coherent with the fact that such events are not independent.

State	H probability	V probability	P_g	H_{min}
mixed	0.491±0.001	0.508±0.001	0.508±0.001	0.975±0.003
D	0.519±0.002	0.481±0.002	0.519±0.002	0.946±0.005

Table 2: Probabilities of measuring a mixed 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.

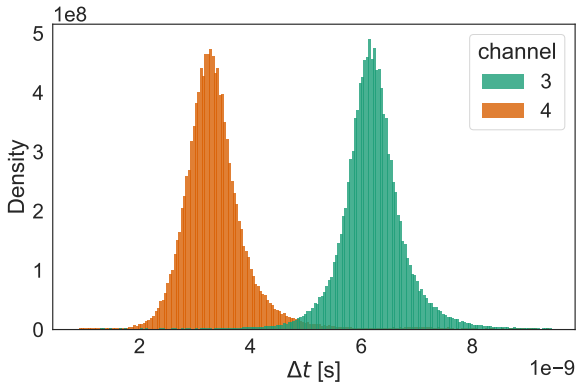
We collect data by measuring a mixed and a pure D state on H/V basis, in Figure 6 we report the distribution of coincidences for these datasets. The probabilities and the corresponding H_{min}, P_g are reported in Table 2, note that such observations are coherent with the theoretical definition given in Equation (14). The main outcome is that measurements of a single basis with a trusted source do not allow us to distinguish between a pure and a mixed state, since the distributions are equivalent. Such observation is important since when there is an eavesdropper in the system, he prepares a pure state and he sends the purification to Alice, thus Alice receives a totally mixed state. As a consequence, distinguishing between pure and mixed states turns out to be fundamental if we want to identify the presence of an eavesdropper. Trusted QRNGs do not give us the capability to identify such presence.

5.2 Source Device Independent QRNGs

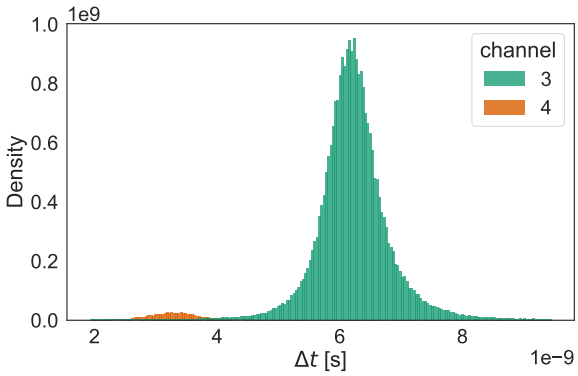
The limit of trusted QRNG is that the procedure that we have discussed does not allow us to distinguish between a pure and a mixed state. To overcome such issue we introduce Semi-DI protocols.

5.2.1 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 proposed by Tomamichel and Renner [2011] and



((a)) Histograms of coincidences events in a window of 3ns for measurements of a mixed state on D/A basis.



((b)) Histograms of coincidences events in a window of 3ns for measurements of a D state on D/A basis.

Figure 7: Histograms of coincidences events in a window of 3ns 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 exhibit a huge amount of observation on channel 3, as expected.

State	D probability	A probability	P_g	H_{min}
mixed	0.502±0.001	0.498±0.001	0.99±1e-08	8e-06±0.003
D	0.971±0.002	0.0293±0.0003	0.6686±0.0007	0.581±0.004

Table 3: Probabilities of measuring a mixed 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 [2011] and Vallone et al. [2014]. 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.

Vallone et al. [2014], as discussed in 2.2.1.

We consider measurements of a mixed and a pure D state in the D/A and in the H/V basis. Thus, with the first setup we generate the random variables X and Z by considering as POVMs the projective measurements on the two basis $Z = \{|D\rangle, |A\rangle\}$ and $X = \{|H\rangle, |V\rangle\}$. In this context, the bound expressed in Equation (7) can be written as:

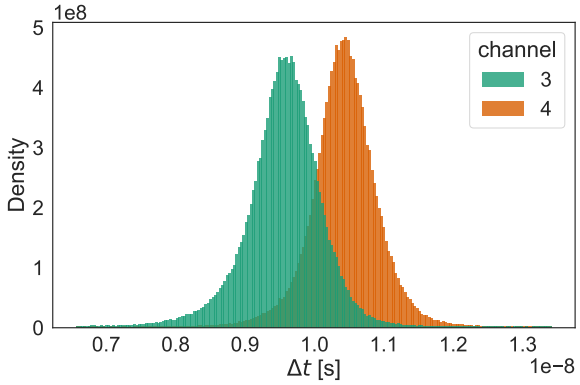
$$H_{min}(x|E) \geq 1 - 2\log_2\left(\sqrt{P_A} + \sqrt{P_D}\right). \tag{20}$$

Errors on bounds are computed as follows:

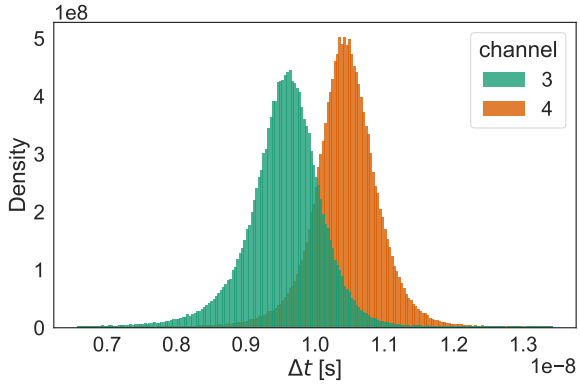
$$\begin{aligned} \sigma_{H^b_{min}} &= \frac{1}{\log 2}\frac{1}{\sqrt{P_A}+\sqrt{P_D}}\sqrt{P_A^{-1}\sigma^2_{P_A} + P_D^{-1}\sigma^2_{P_D}}, \\ \sigma_{P^b_g} &= H^b_{min} 2^{-H^b_{min}-1}\sigma_{H^b_{min}}, \end{aligned} \tag{21}$$

where the apex b indicates the bound. Our purpose is indeed to provide a bound on the amount of randomness that we can extract on the basis H/V by measuring on a mutually unbiased basis, D/A in this case.

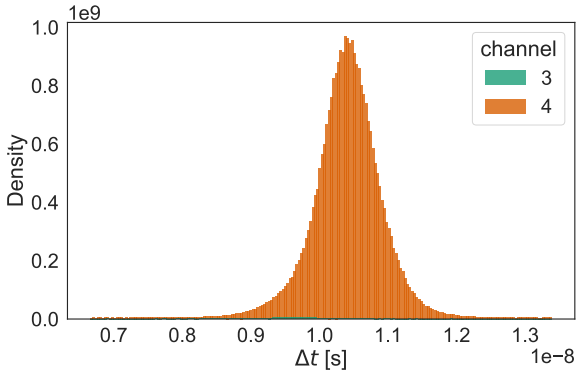
The distributions of coincidences for the D/A measurements are shown in Figure 7, while in Table 3 we report the observed probabilities and the amount of randomness quantified by the min-entropy. In



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



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



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

Figure 8: Histograms of coincidences events in a window of 3ns 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 clannel corresponding tox state L.

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, thus it is possible to extract randomness from the process with a given level of security.

For what concern the final set of measurements we consider a pure L state measured on all the basis H/V, D/A, L/R. In this case we can bound the amount of randomness available for the random variable X associated to projective measurements on H/V basis both with measurements on D/A and L/R, by

State	Channel 3 probability	Channel 4 probability	P_g	H_{min}
Bounding X with Z	0.500±0.001	0.499±0.001	0.99±6e-12	5e-9±0.002
Bounding X with Y	0.00570±0.00008	0.994±0.002	0.5753±0.0006	0.798±0.003

Table 4: Probabilities of measuring a pure L state on $Z = \{|D\rangle, |A\rangle\}$ and $Y = \{|R\rangle, |L\rangle\}$. 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.

defining $Z = \{|D\rangle, |A\rangle\}$ and $Y = \{|R\rangle, |L\rangle\}$. The two bounds read:

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

Error are computed by applying Equation (21), once one consider the correct basis. The distributions of coincidences are shown in Figure 8, while in Table 3 we report the observed probabilities and the bounds for P_g and H_{min}. Note that measurements of a pure L state on its corresponding 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 measurements performed on a pure D state on D/A basis.

5.2.2 Full tomography

Let us now consider the method proposed by Fiorentino et al. [2007] 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 of the quantum state, thus we need to perform measurements on all the orthogonal basis H/V, D/A and L/R. Such measurements allow us to compute the Stokes parameters, see Equation (16). For what concerns the evaluation of the error, since every Stokes parameter S is the algebraic sum of two probabilities P_i and P_j, their errors can be computed as $\sigma_S = \sqrt{\sigma_{P_i}^2 + \sigma_{P_j}^2}$. Therefore, from Equations (10) and (11), we can retrieve the error on H_{min} and P_g:

$$\begin{aligned} \sigma_{P_g^b} =& \frac{(1 - S_1^2 - S_2^2)^{-1/2}}{2} \sqrt{S_1^2 \sigma_{S_1}^2 + S_2^2 \sigma_{S_2}^2}, \\ \sigma_{H_{min}^b} =& \frac{\sigma_{P_g(x)}}{P_g(x) \log 2}. \end{aligned} \tag{23}$$

Let us first consider data concerning measurements of a mixed and a pure D state on H/V and D/A basis, to perform a full tomography of such states we assume that the second Stokes parameter is null $S_2 = 0$. The density matrix of the mixed and the pure D state are reported respectively in Figure 9(c) and Figure 9(a), while numerical results are shown in Table 5. The guessing probability corresponding to a mixed state is $P_g^{mix} = 0.99 \pm 4\text{e-}6$, 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 $P_g^D = 0.668 \pm 0.003$, with $H_{min}^D = 0.580 \pm 0.007$.

State	P_g	H_{min}
mixed	0.99±4e-6	8e-6±6e-6
D	0.668±0.003	0.580±0.007
L	0.575±0.005	0.79±0.01

Table 5: Bounds on guessing probability and min-entropy computed with Fiorentino et al. [2007] method. The guessing probability corresponding to a mixed state is $P_g^{mix} \approx 1$, 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 setup is negligible. On the other hand the guessing probabilities corresponding to D and L states lead to non null values of min-entropy.

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 basis. The density matrix is reported in Figure 9(b). The worst case guessing probability is $P_g^L = 0.575 \pm 0.005$, with $H_{min}^L = 0.79 \pm 0.01$. 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. The specific amount of randomness is lower bounded by the values reported in 5.

6 Security parameter

Finally, to complete our analysis it is worth to compute quantitatively the security of the protocol discussed above. To do so we employ the strategy proposed by Tomamichel et al. [2011] that we briefly summarized in Section 3.

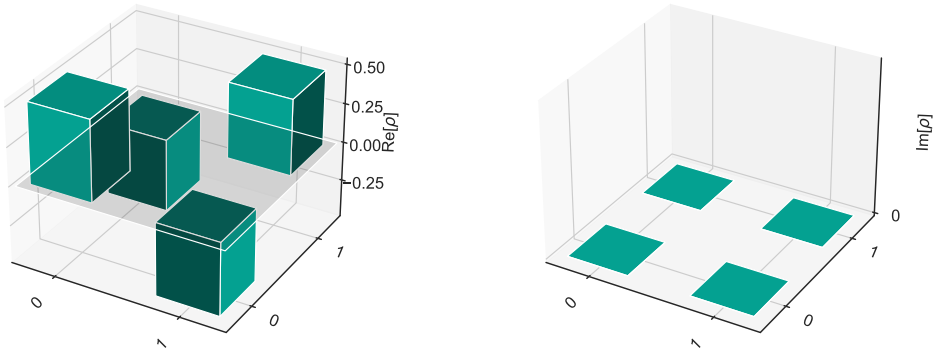
Let us now consider the statistical uncertainty, from Equation 13 error on the ϵ security parameter reads:

$$\sigma_\epsilon = 2^{\ell/2 - H_{min}(X/E)/2 - 2} \log 2 \sigma_{H min}. \tag{24}$$

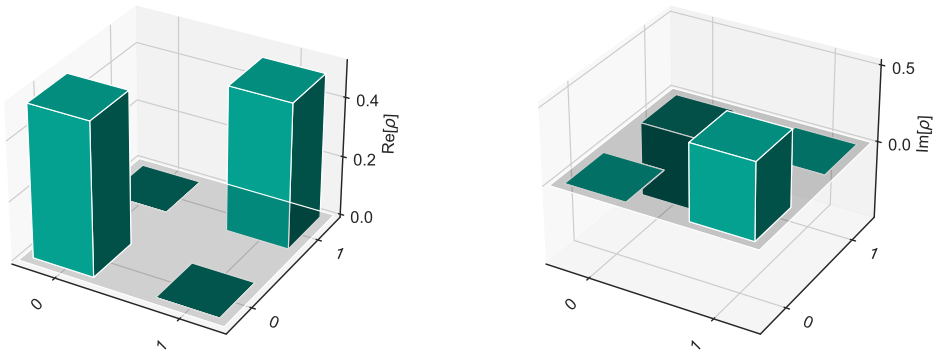
In Figure 10 we report the security parameter ϵ from the LHL as function of the block length, for fixed values of min-entropy. In particular, we consider the values of min-entropies computed in the previous sections: we consider both the results obtained with Fiorentino et al. [2007] method reported in Table 5 and in the trusted scenario, see Table 2. The main outcome is 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 to be precise, while higher values of H_{min} are associated with more secure randomness available.

7 Conclusions

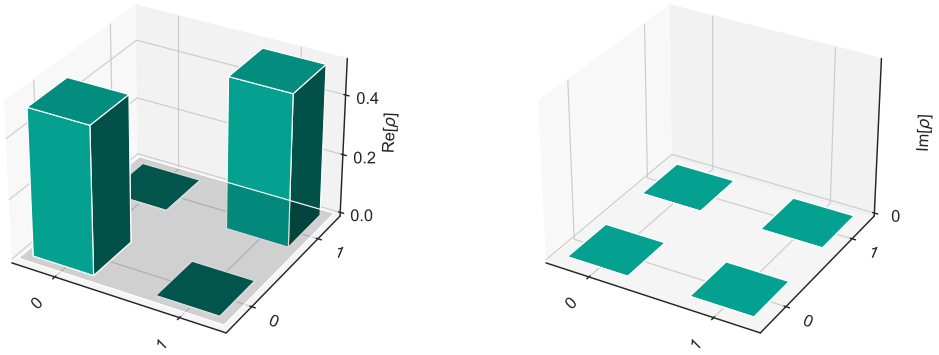
Let us now briefly summarize our results and draw some conclusions. We first implemented a trusted QRNG and measured the amount of secure randomness that can be generated with such protocol. Nevertheless, such approach exhibits some limitations due to the assumptions that we are requiring to the system, in particular we cannot distinguish a pure and a mixed state just measuring on the basis in which we want to generate random bits. To avoid such issues we designed a Source-DI protocol by measuring both a mixed state on H/V and D/A basis, and measuring a pure L state on all the polarization basis. Then, by applying Fiorentino et al. [2007] method and the approach proposed in Vallone et al. [2014], we could give an estimation of the worst case guessing probabilities and min-entropies. Eventually, we



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



((b)) Density matrix of a pure L state. The reconstruction is complete and performed through measurements on all the basis.



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

Figure 9: Real and imaginary part of the density matrices of all the considered states. Indeed, we are able to reconstruct the density matrix by performing a full tomography of the quantum state. For what concerns the mixed and the pure D state we assumed the second Stokes parameter to be null, since we did not measure such states on L/R basis. On the other hand, the pure L density matrix is the complete reconstruction of a pure state L.

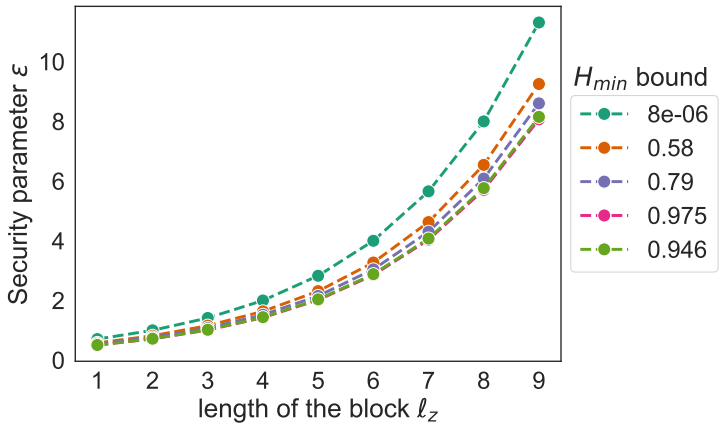


Figure 10: The security parameter ϵ from the LHL is exponential in the block length for every fixed min-entropy. Moreover, ϵ exhibits a decreasing behaviour as the min-entropy increases. We show the trends corresponding to min-entropies computed with Fiorentino et al. [2007] method ($H_{min} = 8e-6, 0.58, 0.79$) and in the trusted scenario ($H_{min} = 0.975, 0.946$).

showed the trend of the security parameter ϵ from the LHL as function of the block length for all the min-entropies computed.

References

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, Mar 2007. doi: 10.1103/PhysRevA.75.032334. URL https://link.aps.org/doi/10.1103/PhysRevA.75.032334.

Marco Tomamichel and Renato Renner. Uncertainty relation for smooth entropies. *Physical Review Letters*, 106(11), Mar 2011. ISSN 1079-7114. doi: 10.1103/physrevlett.106.110506. URL http://dx.doi.org/10.1103/PhysRevLett.106.110506.

Giuseppe Vallone, Davide G. Marangon, Marco Tomasin, and Paolo Villoresi. Quantum randomness certified by the uncertainty principle. *Phys. Rev. A*, 90:052327, Nov 2014. doi: 10.1103/PhysRevA.90.052327. URL https://link.aps.org/doi/10.1103/PhysRevA.90.052327.

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

Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, Aug 2011. ISSN 1557-9654. doi: 10.1109/tit.2011.2158473. URL http://dx.doi.org/10.1109/TIT.2011.2158473.