Quantum Cryptography and Security 2021/22
Report 1 - Quantum Random Number Generators
Prof. Giuseppe Vallone
Prof. Nicola Laurenti

Samuele Piccinelli

(Dated: 15 December, 2021)

In this work we discuss the implementation of two types of quantum random number generators (QRNGs), characterised by different degrees of trust on their elements. In particular, we use an experimental setup based on a heralded single photon source and polarisation measurements to study the trusted and source-device-independent protocols.

1 Theoretical background

The general framework is that of an apparatus in the hands of an attacker Eve (E): Alice (A), the legitimate user, will receive a quantum state from a source that E will try to control to her advantages. The best strategy E can adopt in order to maximise correlations is to send pure entangled states: whenever E sends a maximally entangled state, A will see a totally mixed state.

We analyse two different scenarios, based on the different degrees of trust on their components: trusted and source-device-independent.
In the trusted scenario the source is fully characterised and the system of interest is isolated and completely uncorrelated with the environment: this translates to $\rho_{AE} = \rho_A \otimes \rho_E$. Moreover, we assume that the state coming from the source is pure ($\rho_A = |\psi\rangle\langle\psi|$) and that no side information in the measurement is present. In the other framework, we do not have full control over the environment and we can only put some bounds on the information acquired by a potential eavesdropper (quantum side-information). The trade-off in this case is a question of higher security at the price of a lower generation rate due to the smaller number of hypotheses we impose on the apparatus - that is often not trivial to characterise experimentally - thus making it less susceptible to noise and imperfections. Higher security implies reducing the ease of implementation.

In order to quantify the goodness of a QRNG we use the min-entropy, a measure of the amount of trusted randomness (security) we can extract from the source. For a random variable X that takes value in an alphabet $\mathcal{A}$ with a corresponding probability $P_X(x)$, the min-entropy is obtained from the family of Rényi entropies of order α,

$$H_\alpha(x) = \frac{1}{1-\alpha} \log_2 \sum_{x\in\mathcal{A}} P_X(x)^\alpha \tag{1}$$

by taking the limit for $\alpha \to \infty$: since it holds that for any distribution $H_\alpha(X) \geq H_\beta(X)$ for $\alpha \leq \beta$, the min-entropy gives a lower, worst-case bound to all the Rényi entropies.
In the trusted scenario, after the measurement where A has obtained x, the state will be a classical quantum state in the form

$$\hat{\rho}_{AE} \underset{\text{MEASURE}}{\longrightarrow} \hat{\rho}_{AE} = \sum_X P_X |X\rangle\langle X| \otimes \hat{\rho}_E^x \qquad \langle X|X'\rangle = \delta_{X,X'} \tag{2}$$

(i.e. a classical register on the outcome of Alice weighted by their probabilities), where ρ_E^x is the state of E conditioned on the outcome of X. In this case, the min-entropy is defined as the negative logarithm of the probability of the most likely outcome,

$$H_\infty(x) \equiv H_{\min}(x) = -\log_2(\max_{x\in\mathcal{A}} P_x). \tag{3}$$

Consequently,

$$P_{\text{guess}} = 2^{-H_\infty(X)} = 2^{-H_{\min}(X)} \tag{4}$$

corresponds to the probability of guessing at the first attempt the outcome from measuring a random variable X with a known distribution.

For the non-trusted scenario, the definition extends to joint quantum systems: in this case the P_{guess} must take into account the strategies of E, for E has to find the set of (generalised) measurements (POVMs) $\{\hat{F}_X\}$ that maximise the information she gets about the state, i.e.

$$P_{\text{guess}} = \max_{\{\hat{F}_X\}} \sum_X P_X \operatorname*{Tr}_E (\hat{F}_X \rho_X^{\hat{E}}). \tag{5}$$

The problem in this case cannot be solved analytically but only numerically: the solution is to put instead some bounds on $H_{\min}$. The two approaches we will explore are based on the entropic uncertainty principle [1] and the full quantum tomography [2].

The entropic uncertainty principle states that by measuring the system in conjugate observables Z and X, it is possible to obtain a bound on the conditional min-entropy, expressed by

$$H_{1/2}(X) + H_{\min}(Z|E) \geq \log_2 d, \tag{6}$$

where d is the dimension of the system and $H_{1/2}(X)$ the max-entropy of X outcomes. By measuring on mutually unbiased basis (MUB) we are able to quantify the amount of true-randomness contained in Z and constrain the min-entropy. If again we want to distinguish between a pure and a mixed state, we can measure not only in H/V basis (key generation basis) but also in the D/A basis: a pure state will be only transmitted, while the mixed state has again a 50/50 transmission/reflection probability. The procedure is however blind to states prepared in the L/R basis (that are thus circularly polarized), since it is able to certify randomness for a measurement in the equator plane of the Bloch's sphere: the states that do not satisfy this requirement will be classified as totally mixed from the protocol.

On the other hand, in the full quantum tomography we measure also in the L/R basis, i.e. we do a full tomography of the state. With a measurement along all components there is no ambiguity on the vector identifying the state, that can be written in the Pauli matrices basis as

$$\hat{\rho} = \frac{1}{2}(\mathbb{1} + \vec{\sigma}\cdot\vec{r}). \tag{7}$$

For pure states $\|\vec{r}\| = 1$, i.e. the vector lies on the surface of the sphere, otherwise is mixed. In order to obtain a lower bound on $H_{\min}$, following the procedure explained in [2], we define a function

$$f(\rho(S_1, \hat{S}_2, S_3)) = -\log_2\left(\frac{1+\sqrt{1-|S_1 - iS_2|^2}}{2}\right), \tag{8}$$

where $\hat{\rho}$ is a generic density matrix and $S_{1,2,3}$ are the real Stokes parameter, computed as difference of transmitted and reflected probabilities in the different basis (e.g. $S_1 = P_D - P_A$ where $P_{D,A}$ are the probabilities to detect a photon along D and A). Using the fact that the function $f(\rho(S_1,\hat{S}_2,S_3))$ is a convex function of $S_{1,2,3}$ in the Poincaré sphere, we obtain

$$f(\rho(S_1,\hat{S}_2,S_3)) \leq H_{\min}(\hat{\rho}) \tag{9}$$

i.e. the wanted lower bound.

Finally, once we bound the min-entropy, we can apply a seeded randomness extractor to the raw data generated in order to obtain the final string of private random numbers: the leftover hashing lemma (LHL) described in [3] gives an expression of the security parameter Δ (i.e. a measure of the distance of the distribution of the output $Z \equiv f(X)$ from the uniform distribution conditioned on E) as a function of the min-entropy and the block size used for the matrix,

$$\Delta = \frac{1}{2}\sqrt{2^{\ell} - H_{\min}(X|E)}. \tag{10}$$

The LHL implies that for a fixed joint distribution of X and E, there is a fixed function f that extracts almost uniform randomness: given any $\Delta > 0$, there exists a function f that produces

$$\ell = \left\lfloor H_{\min}(X|E) - 2\log\frac{1}{2\Delta} \right\rfloor \tag{11}$$

bits that are Δ-close to uniform and independent of E.

In the following analysis we will show that

$$\ell \geq H_{\min}(X|E), \tag{12}$$

a bound on the length of the output string (i.e. the number of extractable random bits) that can be demonstrated using arguments of classical probability.
Moreover, we will analyse the block length ℓ as a function of the Δ parameter, both in case of hashing on the whole string of raw bits and in the case of hashing on blocks of size N/m (with N the number of bits in the input string and m integer). In fact, to process all available bits in one go would require extremely large matrices (the complexity of the most efficient extraction algorithm is of the order of $\mathcal{O}(N(\log N))$). Therefore the original block of N bits is often divided into many smaller blocks and extraction is done separately on each of them. Clearly this comes at a price: we will see that typically to achieve the same Δ as before we will have to choose ℓ such that the ℓ/N ratio will be smaller than if we were to do the processing on a single block.

In this analysis we will ignore errors due to finite size statistics.

2 Experimental apparatus

The experimental setup consists in a laser source and a non-linear crystal that emits pairs of photons γ_1, γ_2 via spontaneous parametric down conversion (SPDC). This phenomenon, also known as parametric fluorescence or parametric scattering, is a nonlinear optical process that converts one photon of higher energy (namely, a pump photon), into a pair of photons (namely, a signal photon, and an idler photon) of lower energy, in accordance with the law of conservation of energy and law of conservation of momentum. The detection of γ_1 (heralded photon) acts as a trigger for a gate generator, enabling two single photon detectors (SPD) - which specifically are avalanche photodiodes (APD) - in view of γ_2. These two are placed on both sides of a 50/50 beam splitter

(BS): since the qubit information is encoded in the polarisation degree of freedom, we perform a projective measurement on the polarisation of γ_2 for different setup configurations.
A time-to-digital converter (with a resolution of 1 ps and with a time jitter of ~ 4 ps) collects the the time tags of the photon incidences identified by the corresponding channels, marked by a numerical tag:

- **2** for the herald channel;
- **3** for the transmitted channel;
- **4** for the reflected channel.

For this experience we are only interested in the coincidence events where we have a simultaneous detection between channel 2 and a detection either in channel 3 or channel 4.

We denote with N_2 the number of idler events detected at SPD_2; $N_{23,24}$ are the coincidences between $\text{SPD}_{2,3}$, $\text{SPD}_{2,4}$ inside the time window τ_c respectively. During τ_c, the probability for the detection of a photon γ_2 coming from the same event that generated γ_1 is much bigger than the probability of detecting a photon γ_2 emitted by any other event - for instance, a photon not belonging to the pair that comprises γ_1 or noise: we are then in a situation close to an ideal single-photon state emission.

The polarization beam splitter transmits horizontally polarized photons and reflects vertically polarized photons: this allows us to measure the polarization of the photon in the H/V basis. By inserting a half-wave or a quarter-wave waveplate before the polarization beam splitter, we perform measurements in the D/A and L/R basis, respectively. In a few configurations, a 45°-polarizer is used before the measurement station to prepare a pure diagonal state instead of a mixed state.

3 Dataset

The dataset is composed of the time tags of the photon incidences (in ps) and the corresponding channels and are divided for each of the configurations under study: these latter are listed below, together with a code to ease their identification.

- Mixed state measured in H/V (m-HV);
- Pure D state measured H/V basis (pD-HV).

Both the state preparation and the measurement stations are trusted and assumed to be working correctly. The H/V basis is considered the basis for randomness generation. The amount of randomness which can be certified can be quantified by the classical min-entropy.

- Mixed state measured D/A basis (m-DA);
- Pure D state measured D/A basis (pD-DA).

In this case the source is untrusted but the measurement station is trusted. The previous datasets acquired in the H/V basis basis are still used for the generation, while the data in the D/A basis (which is the check basis) are used to bound the amount of randomness which can be certified, quantified by the quantum conditional min-entropy.
As explained in Section 1 we will focus on approaches based on the entropy uncertainty principle and the tomographic method.

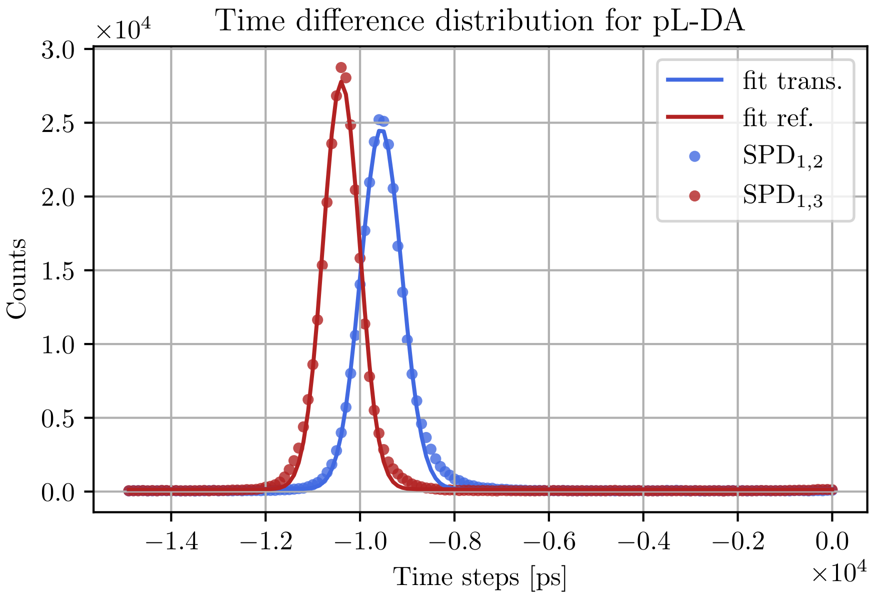

Figure 1. Time difference distribution for the pL-DA case to the nearest heralding event.

- Pure L state measured D/A basis (pL-DA);
- Pure L state measured H/V (pL-HV);
- Pure L state measured L/R basis (pL-LR).

The last three set of data are acquired to show the differences between the two source-device-independent estimations when including measurements with pure states outside the equator of the Bloch sphere passing through H,V,D,A (full tomography). The data are again used to bound the quantum conditional min-entropy, using the entropy uncertainty principle and the tomographic method.

4 Analysis and discussion

We load each dataset in a dataframe structure and compute the differences between consecutive elements. We filter the differences to retain only the values below a time windows choose arbitrarily to be $\tau_w = 10\,\text{ns}$. Since the photon counting process is poissonian we associate to each timetag the poissonian uncertainty of $\sqrt{N}$ for N counts. An example is reported in Fig. 1 for the pL-DA case. The fact that the plot extends in the negative region of the x-axis indicates that the heralded photons arrive after the transmitted/reflected photon: this is likely due to a length difference of the acquisition cables from the photodetector to the time-to-digital converter rather than a difference in the branching paths - the heralded photons travel actually for a shorter distance with respect to the other ones.
The time differences distributions are fitted with a gaussian: the whole set of differences is filtered again, this time retaining only those within the $[-3\cdot\sigma, +3\cdot\sigma]$ interval around the mean ($\tau_c \approx 2.4\,\text{ns}$). The probabilities are computed as the ratio $P_{T,R} = N_{23,24}/(N_{23} + N_{24})$.

Using the equations in Section 1 we can estimate the quantum conditional min-entropy in the different scenarios, for each of the inputs and for each method described in Section 3: the entropy

Scenario	**A's input**	**Method**	$\mathbf{H}_{\min}$/meas.
Trusted	Pure D	Classical	0.955 ± 0.005
Trusted	Mixed	Classical	0.968 ± 0.003
SDI	Pure D	EUP	0.59 ± 0.08
SDI	Pure D	TM	0.59 ± 0.03
SDI	Mixed	EUP	0.000 ± 0.003
SDI	Mixed	TM	$(0 \pm 1) \cdot 10^{-6}$
SDI	Pure L	EUP (D/A b.)	0.000 ± 0.002
SDI	Pure L	EUP (L/R b.)	0.803 ± 0.002
SDI	Pure L	FT	0.8030 ± 0.0008

Table 1. Min-entropy per measurement for the different scenarios under investigation.

uncertainty principle (EUP), the tomographic method (TM) (using $S_2 = 0$) and the full tomography (FT). We report the results in Table 1, with the relative uncertainties obtained by error propagation. The entropy is computed per measure (single-shot), $H_{\min}$/meas.< 1.

As it can be seen, in the trusted scenario, sending pure and mixed states produces the same min-entropy, since we fully trust the source and different level of pureness do no affect the amount of randomness we can extract. This implies also that we have no way to discriminate between pure/mixed states (i.e. if there is (not) an attacker).

In the source-device-independent scenario, we obtain the same level of $H_{\min}$ for both the methods of EUP and TM, as it is reasonable to assume. As we mentioned earlier, the entropic uncertainty principle is not able to certify any randomness in the case of pure L state because we are doing the certification measurement in the H/V, D/A equator plane of the Bloch's sphere, so the protocol is effectively blind to it. When we instead switch to the orthogonal plane that contains the L/R basis, the result is in agreement with the one obtained via full tomography.

Lastly, we study how the security parameter of the LHL defined in Eq. (10) changes by varying the block length ℓ. In Fig. 2 we show ℓ vs the security parameter Δ in semi-log scale, where we used the min-entropy computed for the pd-DA case. The trend is as expected: if we increase the number of extracted bits, the security parameter increases with it, thus moving away from the uniform case. In other words, the more randomness we want extract, the more we drift away from the ideal case. The bound described in Eq. (12) is plotted with a dotted line.

In Fig. 3 we report the security parameter Δ vs $\ell_{\text{rem}} \equiv N \cdot H_{\min} - L \cdot m$, defined as the number of bits removed from the sequence. As it is clear to see, in order to obtain the same value of Δ as the block size N/m (defined in powers of 2) decreases, the number of bits we have to remove increases: to obtain the same security parameter as for $m = 1$ (supposing $\Delta_{m=1} = 10^{-10}$) we have to throw away $\approx 0.8 \cdot 10^5$ bits. This trend reflects the expectations, as anticipated in Section 1.

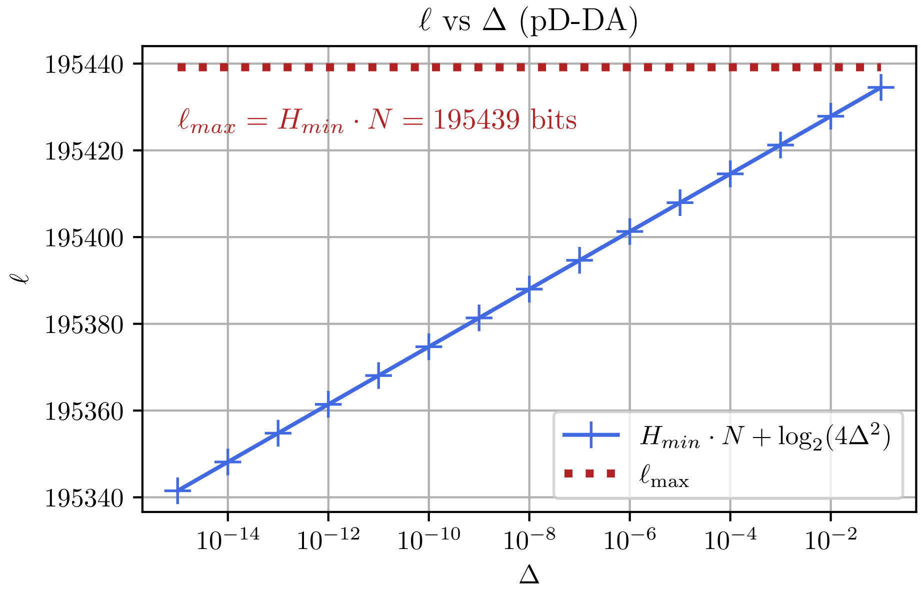

Figure 2. ℓ vs the security parameter Δ: the case for pd-DA is here shown, where the dotted line represent the upper limit to the maximum extractable output length (Eq. (12)).

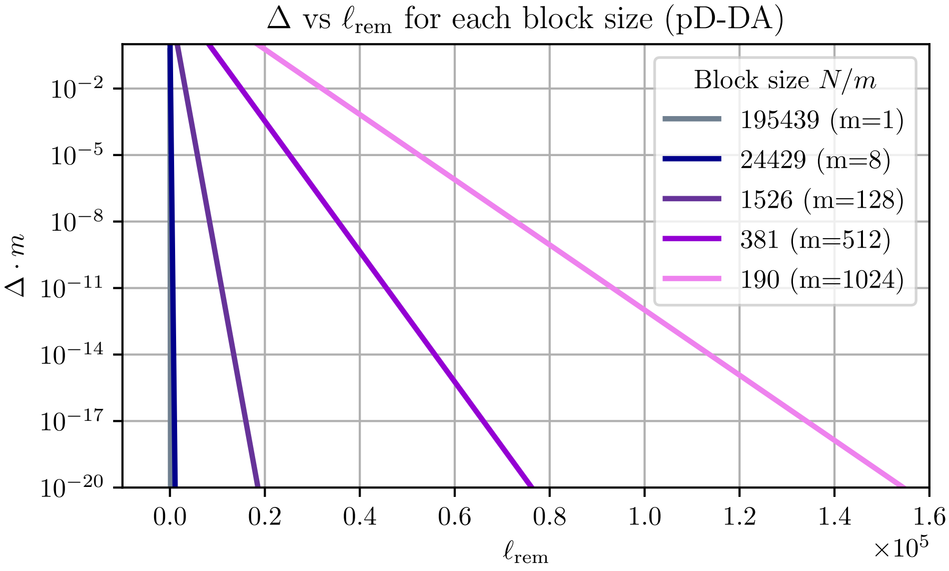

Figure 3. Security parameter Δ vs the number of bits we have to remove from the total string ℓ_{rem} for the pd-DA case.

5 Conclusions and outlook

In this work we have computed the min-entropy in the trusted and source-device-indipendent scenarios via different methods. For each implementation, strengths and weaknesses of each have been briefly described. Moreover, the security parameter for the LHL has been studied for different values of the block length, both by considering the raw string as a whole and by dividing it in smaller-size parts. The results are in accordance to what expected from the theory. A further study could include errors due to finite size statistics and take into account electronic noise effects such as dark counts and afterpulse.

[1] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Physical Review A **90** (2014), 10.1103/physreva.90.052327.

[2] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, Physical Review A **75** (2007), 10.1103/physreva.75.032334.

[3] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Transactions on Information Theory **57**, 5524–5535 (2011).