QUANTUM COMMUNICATION AND CRYPTOGRAPHY
Quantum Random Number Generators

Marcomini Alessandro - 2024286

16/12/2021

1 Project goals

This project aims to explore an optical implementation of quantum random number generators. The experimental setups are based on an heralded single photon source with polarization measurements and can be used to study trusted and Source-Device-Independent (SDI) protocols. The whole data acquisition has been carried out in a lab in Padova, exploiting different photon quantum states and measurement in multiple basis. Starting from this dataset, here we estimate some information parameters and security indicators to have a glimpse at the experimental limits of this implementation.

2 Experimental apparatus and theoretical background

Implementation description

The system exploits polarization encoding for the photons quantum states. The experimental setup is prepared for pairs of photons generated by spontaneous parametric downconversion (wavelength of photons: $\lambda = 810\ nm$, input CW laser: $\lambda = 405\ nm$): one of them has an heralding role, i.e, it is directly connected to an avalanche photodiode Single Photon Detector (SPD) to register its time of arrival as reference. The other one is instead directed towards an optical path where it is possible to act directly by inserting and removing elements such as polarizers and lambda half/quarter plates. At the end of this section, the photon is directed towards a couple of single photon detectors which can perform projective measurement in orthogonal states by the means of a polarized beam splitter. We can in principle measure in the H/V, D/A or L/R bases: for the sake of random bit generation, we will always use the rectangular one; measurements in other bases are exploited for parameter estimation and security bounds.

Theoretical picture

We can picture the apparatus described above in the following way: a source (either trusted or not) creates an initial state ρ_{AE} and sends to a legitimate party (Alice) a single photon state $\rho_A = \mathrm{Tr}_E\left(\rho_{AE}\right)$. The rest of the state ρ_E is, in the most general case, lost in the environment (side information) and while performing security analysis it is common to consider the worst-case scenario where all this information is fully exploited by an attacker (Eve).

We assume that upon receiving their states Alice and Eve can perform a set of (generalized) measurements $\left\{\hat{A}_i\right\}_i$ and $\left\{\hat{E}_i\right\}_i$, respectively. Of course, the measure outcome will depend on the measurement operator chosen and on the amount of (quantum) correlations shared by the two subsystems states (which are maximum if ρ_{AB} is a pure state). Naturally, the goal of a malicious Eve will be to guess the output of Alice's measure. After Alice performs its operation, the joint state is given by the post-measurement state:

$$\rho_{ZE} = \sum_z P_z \left(|z\rangle\langle z|\right)_A \otimes \rho_E^z \tag{1}$$

where P_z is the classical probability of getting output z. The probability of Eve guessing the outcome is given by

$$P_g\left(Z|E\right) = \max_{\{\hat{E}_z\}} \sum_z P_z \operatorname{Tr}_E \left[\rho_{AE}\hat{E}_z\right]. \tag{2}$$

In particular, for the case of no-side information (trusted scenario) the joint state of Alice and Eve is separable and thus the expression above reduces to its classical form: $P_g\left(Z\right) = \max_z P_z$.

Min-entropy computation

From the guessing probability one can estimate the min-entropy H_{min}, which is in general a function of the random variable Z obtained by measuring ρ_A, conditioned to Eve's information ($H_{min} = H_{min}\left(Z|E\right)$). It quantifies the amount of true random bits that can be extracted from the random variable Z, under requirement of uniformity and independence from the environment system. Hence, optimal QRNG implementation will aim to maximize this quantity (between 0 and 1 for a binary variable).

If we consider a fully trusted scenario where there are no correlations among Z and E, then this quantity reduces to the classical min-entropy $H_{min}\left(Z\right) \equiv -\log_2 P_g\left(Z\right)$. If quantum correlations are present among Z and E, then the estimate of the conditional min-entropy $H_{min}\left(Z|E\right)$ is less straightforward.

Many methods that have been developed in order to give an estimate of this quantity. This work exploits two of them:

- **Entropic Uncertainty Principle (EUP):** as illustrated in [4], under some mild hypotheses that we consider satisfied in this implementation it holds

$$H_{min}\left(Z|E\right) \geq \log_2 d - H_{1/2}\left(X\right) = 1 - 2\log_2\left(\sum_x \sqrt{P_x}\right) \tag{3}$$

  which provides a lower bound for the min-entropy in terms of system dimensionality ($d = 2$ for qubits) and the Rényi entropy of order 1/2 calculated over X, the random variable associated to measurements in a conjugate basis w.r.t. Z.

- **Quantum tomography:** as reported in [1], Alice does not know which strategy the eavesdropper is in principle adopting. Hence, it is possible to consider in the general case all possible decompositions of $\hat{\rho_A}$ and lower bound the min-entropy with its minimum over all these. In fact, a single qubit density matrix $\hat{\rho}_A$ can be written as ([2]):

$$\hat{\rho}_A = \frac{1}{2}\begin{pmatrix} 1+S_3 & S_1 - iS_2 \\ S_1 + iS_2 & 1 - S_3 \end{pmatrix} \text{ where } \vec{S} = \begin{pmatrix} S_1 \\ S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} P\left(D\right) - P\left(A\right) \\ P\left(L\right) - P\left(R\right) \\ P\left(H\right) - P\left(V\right) \end{pmatrix} \tag{4}$$

Using Stokes parameters S_1, S_2, S_3 and Pauli matrices formalism. With this notation, the results in [1] show that the min-entropy of $\hat{\rho}_A$ (which is in fact $H_{min}(Z|E)$ for the measurement of Z over $\hat{\rho}_A = Tr_E(\hat{\rho}_{AE})$) follows:

$$H_{min}(Z|E) = -\log_2 \left(\frac{1 + \sqrt{1 - |S_1 - iS_2|^2}}{2} \right) \tag{5}$$

The previous methods have different advantages: the EUP approach is in principle easier to implement, since it only requires measurements on two conjugated bases (i.e, requires to determine the position of the state on an equatorial plane of the Bloch sphere); on the other hand, the full tomography of the state requires measurement in all three Bloch axes but can provide a more precise estimate. As the results suggest, there is actually no particular gain in absolute value while using the one or the other method on our data (see analysis below).

Security bounds

While the min-entropy helps us to estimate the amount of private bits we can generate, the actual transformation from raw bit strings to secure ones can be done by the means of a seeded randomness extractor (e.g., random Toeplitz matrix hashing). This process sacrifices a certain amount of non-secret information to produce a shorter string of true random (and secure) ones, i.e, bits drawn independently from a uniform distribution.

As reported in [3], the Leftover Hashing Lemma certifies that under a proper choice of the hashing function the statistical distance between the distribution of Z given E and an uniform distribution is upper bounded by

$$\Delta = \frac{1}{2}\sqrt{2^{L - NH_{min}(Z|E)}} \tag{6}$$

Where L is the number of secure bits, N the size of the raw sequence and $N \cdot H_{min}(Z|E)$ quantifies the total quantum conditional min-entropy for the single measurement (according to [3], $NH_{min}(X|E)$ is the maximum number of secure bit that we can extract from the raw sequence given its conditional H_{min}). As a result, by calculating the min-entropy of a raw sit string we can quantify the amount of pure randomness that we can extract at a given level of security Δ (it is sufficient to invert relation 6 to express L).

Specific setups and data acquisition

Overall, three different setups were built and used for data acquisition:

- **Trusted QRNG:** in this case, both the preparation and measurement devices are assumed to be fully trusted. As a result, there is no side information (classical min-entropy). Random bits are generated by Alice's measurements in the H/V basis of polarization. Here two dataset were collected: one with Alice receiving a mixed state and another with a pure D state (obtained exploiting polarizers and half-wave plate).

- **Source-Device-Independent QNRG:** here the source is not trusted anymore, while the measurement device is still legit. We collected measurements in the D/A basis for the same mixed and D states of the previous point, as collateral information to provide better estimation of security bounds via either entropic uncertainty principle or tomography with (assumed) $S_2 = 0$.

- **Study on Entropy Uncertainty Principle and Tomography:** to check the different security boundaries provided by the two methods exploited, we prepare a pure L state and measure it in the three bases H/V, D/A, L/R. The generation basis is still considered the rectangular, but now data are enough to perform a full state tomography on the three axes and to compare the results of the EUP using either D/A or L/R as conjugate basis.

3 Data analysis

Loading and cleaning

The data acquired over measurement windows of some minutes were loaded and cleaned in the following way. First of all, a division was performed according to the SPD registering the photon (either "herald", "transmitted" or "received"). The most challenging task of this first part is to correctly recognize coincidences between an herald photon and a counterpart in one of the other detectors. To do so, it is necessary to correctly estimate the time delay between the optical path of the heralded and the signal photons. Therefore, given a time-ordered dataset containing all the occurrences and knowing that a suitable coincidence time is $\mathcal{O}\big(10^3\ ps\big)$, a stable enough analysis can be carried out by considering the sub-dataframes with the heralded channel events and either the transmitted or reflected signal ones, studying the distribution of the absolute time-of-arrival differences $\Delta t_i \equiv t_i - t_{i-1}$ (multiplied by a sign factor that keeps track of the channel). In fact, the dead time of SPDs ($\mathcal{O}(10\ ns)$) forbids the same detector to click twice in a temporal range compatible with a coincidence and while minimizing external sources of lights this methods highlights a well-defined peak, which defines the coincidence time. This approach does not filter double-clicks nor afterpulses nor dark counts; however, these spurious events account for a negligible part. Due to the large amount of detections and physics behind the phenomena, it is possible to fit these curves with a shifted-Gaussian model:

$$f\left(\Delta t\right) = h + A \cdot \mathcal{N}\left(\Delta t; \mu, \sigma\right)$$

with parameters h (constant height, noise background), A, μ σ.

The Gaussian fit allows to determine a range in the time differences axis where to consider valid coincidences (range is different for each dataset, given the changes in the optical path). As a general rule, we set the valid range to be the 3σ interval of the Gaussian fit ($\Delta t \in [\mu - 3\sigma, \mu + 3\sigma]$). This allows to get rid of noise properly as well as keeping a sufficiently large set of events.

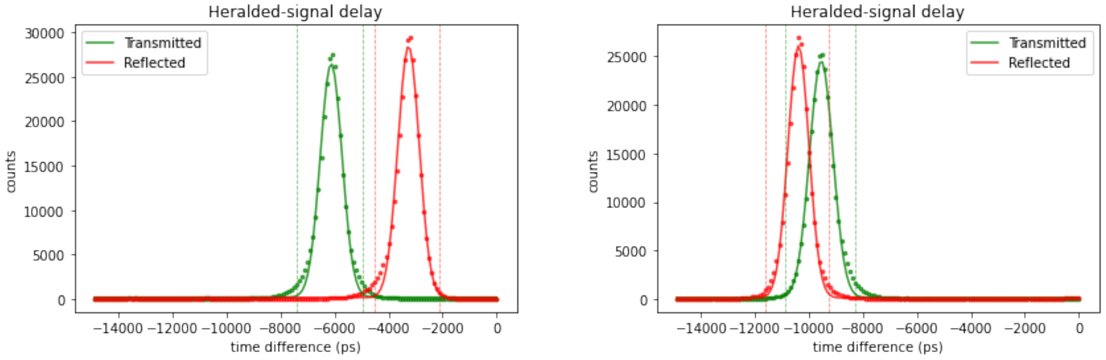
Examples of this results are reported in figure 1, for two differently prepared states. The 3σ range is highlighted. The negative values in the Δt axis imply that the heralded photon is indeed anticipating the signal one (on absolute scale).

Min-entropy computation

The coincidence events found before have the meaning of correctly detected bits, i.e. the temporal sequence of these detections creates the raw bit sequence. The total number of events over the "transmitted" and "reflected" channels corresponds to the total length N of the sequence while the single channel counts $T \pm \sqrt{T}$ and $R \pm \sqrt{R}$ allow to estimate statistical probabilities:

$$P_T = \frac{T}{N} \pm \sigma_{P_T}\ ,\ P_R = \frac{R}{N} \pm \sigma_{P_R} \tag{7}$$

Where the statistical error over the number of counts is calculated considering a Poissonian statistics (errors on P and all the other derived quantities are calculated by proper propagation).



(a) Mixed state on H/V basis

(b) L state on H/V basis

Figure 1: Example of time differences plots and Gaussian fits

Following formulas in section 2 and combining together multiple datasets, the analysis returns the results reported in table 1, where the min-entropy is classical or quantum conditional, according to the scenario.

Scenario	**A's input**	**Method**	$\mathbf{H_{min}}$ per measure
Trusted	Pure D	Classical	0.955 ± 0.005
Trusted	Mixed	Classical	0.968 ± 0.003
SDI	Pure D	EUP (D/A basis)	0.59 ± 0.08
SDI	Mixed	EUP (D/A basis)	0.000 ± 0.002
SDI	Pure D	Tomography ($S_2 = 0$)	0.59 ± 0.03
SDI	Mixed	Tomography ($S_2 = 0$)	$(0 \pm 1) \times 10^{-6}$
SDI	Pure L	EUP (D/A basis)	0.000 ± 0.002
SDI	Pure L	EUP (L/R basis)	0.803 ± 0.003
SDI	Pure L	Full tomography	0.8030 ± 0.0008

Table 1: Min-Entropy per measurement for cases under investigation

The values computed suggest some interesting insights. In the trusted scenario, the values of min-entropy for a pure or mixed input state are indeed quite compatible. This is reasonable: while performing projective measurement in the H/V basis the populations of the two basis states are identical, and therefore the statistical probability of measuring $0, 1$ bits are the same ($\sim 50\%$ each). This is not a problem in a trusted scenario, but it is a warning for the SDI case: measuring in a single basis there is no way to distinguish a pure input from a fully mixed one.

Moving to the SDI, understanding the purity of the state can be done by measuring in a basis conjugate w.r.t. the H/V one (in this case, D/A): in fact, the Entropic Uncertainty Principle shows that the boundary on the min-entropy obtained measuring in the conjugate basis is useless for a mixed input (H_{min} is ≥ 0 by definition), while ensures a certain amount of true randomness in the case of a pure D input.

Another interesting result is obtained comparing the bounds provided by the EUP and the tomography methods for a D input state and for a mixed one: the values are indeed the exact same, meaning that no particular gain is achieved using the one or the other. Of course, this holds in the assumption of looking just on the equatorial plane of the Bloch sphere where $S_2 = 0$ (no L/R component). In any case, one can notice how the error on the bounds is orders of magnitude different for the dataset under investigation.

Finally, while looking at the analysis for a pure L input for Alice, we can see how the EUP method fails to provide useful information while using the "wrong" conjugate basis w.r.t. the measure one: in fact, considering the D/A measure the H_{min} bound is equal to zero (since the projection onto this space of the input space is indeed null). On the other hand, if we consider for the EUP the L/R basis we obtain a fairly high bound, which is the same one achieved by the full state tomography. As a result, we can conclude that the former method has an efficiency which is greatly dependent on the choice of the basis used to estimate the bound. The latter is more efficient and precise but requires a larger number of measurements anyway (all three directions).

Security parameter

From the estimate of the min-entropy we can estimate the Δ security parameter as a function of the length of the raw key N and the length of the secure hashed string L we want as input, as shown in equation 6 (recollecting that $L_{max} = N \cdot H_{min}$, for which $\Delta = 0.5$). Figure 2 highlights the linear dependence between $\log(\Delta)$ and L for the raw key generated with input L and min-entropy estimate via quantum tomography.

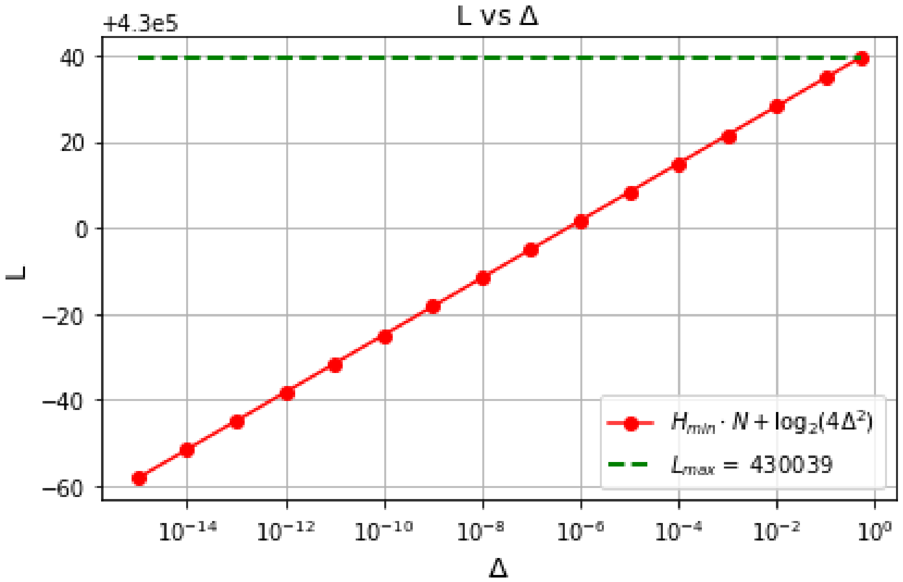


Figure 2: Length of secure hashed string L vs security parameter Δ for an input pure state L (generation basis: H/V, H_{min} estimated via full quantum tomography)

Looking at figure 2 looks clear how a sacrifice of few bits over the whole set of secure ones (order 0.01%) can ensure a security many orders of magnitude larger.

As mentioned, practical realizations of such protocols exploit hashing for the conversion of the raw bit string into a shorter, secure one. From a theoretical point of view this can be achieved both processing the whole string at once and dividing it in m blocks of length N/m and perform local hashing over these, before concatenating the output hashed strings and computing the total security parameter $\Delta_{tot} = \sum_{i=1}^{m} \Delta_i$. Under the assumption that the overall H_{min} is representative of the single blocks ones and that the same amount of hashed bits are extracted from each block ($L_{tot} = mL_i$) it holds (from equation 6):

$$\Delta_i = \frac{1}{2}\sqrt{2^{L_i-(N/m)H_{min}}} \implies \Delta_{tot} = m\Delta_i = \frac{m}{2}\sqrt{2^{(L_{tot}/m)-(N/m)H_{min}}} = m2^{1/2m} \cdot \frac{1}{2}\sqrt{2^{L_{tot}-NH_{min}}} \tag{8}$$

The last term in the equation above is equal in form to the right handside of equation 6. Since the term $m2^{1/2m}$ is ≥ 1 for $m \geq 1$, one can conclude that dividing the original sequence in multiple blocks and looking to achieve the same amount of output secure bits L_{tot}, the global security of the protocol decreases (since Δ grows). Looking at it from another perspective, this means that by fixing a certain security threshold (e.g., $\Delta = 10^{-10}$), using several smaller blocks allows to produce less and less secret random bits.

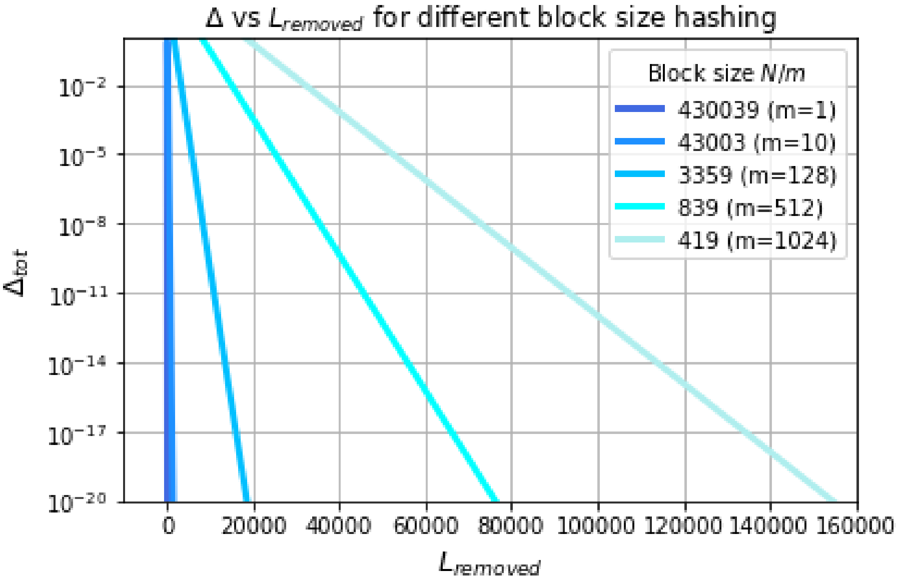


Figure 3: Security parameter Δ vs length of sacrificed bit during hashing (input pure state L, generation basis: H/V, H_{min} estimated via full quantum tomography)

This whole behaviour is displayed in figure 3, where we use the same data from the previous plot and define $L_{removed} \equiv L_{tot} - NH_{min}$ (i.e, the amount of bits we shall remove from the theoretical maximum so to reduce Δ_{tot} to a reasonable level. For $m = 1$ the line $\log \Delta_{tot}\ vs\ L_{removed}$ is almost vertical, meaning that a sacrifice of few bits allows to sweep several order of magnitudes for Δ (in accordance to what already saw in figure 2). On the contrary, while hashing short blocks we pay an expensive cost in terms of bits if we want to diminish Δ.

To sum up, it looks clear how performing hashing on a single block would be the optimal solution so to waste a minimum amount of secret random bits and have a high security. Unfortunately, this is against practical feasibility, since the computational cost of performing hashing of large blocks is enormous. Therefore, in practice one must find the optimal threshold between using short enough blocks to match the lab equipment and long enough blocks to ensure high security without removing too many bits (i.e, set the optimal m).

4 Conclusions

In conclusion, we showed how to implement an experimental photon-based protocol of quantum random number generation, together with some parameter estimations for both the trusted scenario and source-device-independent one. We successfully produced and analysed statistical quantities of interest which are in line with theoretical expectations. We raised awareness of the importance of a proper state preparation and min-entropy estimation, highlighting the pros and cons of tomography and entropic uncertainty principle (the latter is less demanding by requires a careful choice of the conjugate basis, while the former provides higher precision by requires three basis measures).

Finally, even though randomness extraction has not be directly performed, we investigated the scaling of the security level as a function of the raw bits and the secure bits we want to extract. Again, a suitable theoretical explanation for the results is provided. Future development could investigate the finite-length effect we did not take into consideration in this analysis.

References

[1] Marco Fiorentino, C. Santori, S. Spillane, William Munro, and R. Beausoleil. Secure self-calibrating quantum random bit generator. *Physical Review A*, 75, 01 2007.

[2] Alexander Niggebaum. Quantum state tomography of the 6 qubit photonic symmetric dicke state. Master's thesis, Ludwig Maximilians Universität München, 2011.

[3] Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner. Leftover hashing against quantum side information. *Information Theory, IEEE Transactions on*, 57:5524 – 5535, 09 2011.

[4] Giuseppe Vallone, Davide Marangon, Marco Tomasin, and Paolo Villoresi. Quantum randomness certified by the uncertainty principle. *Physical Review A*, 90, 01 2014.