n-states in Time-bin Encoding for Semi-Device-Independent Quantum Random Number Generators based on Unambiguous State Discrimation

Xavier Valcarce
Claude Bernard University, Lyon1

July 20th, 2017

Abstract

We generalize the time-bin encoding implementation of the semi-device-indenpendent quantum random number generator (QRNG) of (*Brask et al.*)[1], from two states to n states. In ordrer to use a prepare-and-measure protocol, n nonorthognal states can be prepared, with a constant overlap between each pair, encoded by weak coherent pulses and emitted by n-packet of time bins. States are then measure using unambiguous quantum states discriminator (USD). Relation between the number of time-bin and the min-entropy according to detector efficiency, and mean photon number will be detailed, and some implications will be discussed.

1 Introduction

Random number are a fundamental part of science and technology, as for Monte Carlo simulation, key generation for cryptography, satistical sampling, and other. A good random number generator is one with an high output frequency and a high entropy[2]. Furthemore, for security applications, randomness must be certified relative to any untrusted parties[3].

This work is based on the (*Brask et al.*)[1] QRNG wich tries to answer those random number needs. A simple scheme of this QRNG can be found in Fig. 1. In the preparation part, this protocol takes a binary input and emits a quantum system in a state corresponding to that binary value. Here, we increase the number of inputs possibility from $x \in \{0,1\}$ to $x \in \{0,...,n\}$. Our main goal was to test the n-inputs hypothesis to kow if and how it can improve the (*Brask et al.*) QRNG protocol.

2 n-states generalisation

The first part of our work was to design a way to create a prepare device that takes n possibilities and generate n-states with a constant overlap between each pair or $|\langle\psi_i|\psi_j\rangle| = \delta \quad \forall i \neq j$. This will allow to have some inconclusive output when measuring with USD[4].
Using the time-bin encoding this can be achieved by sending n-packets of time bin composed of $n-1$ vaccum states, $|0\rangle$, and one coherent state, $|\alpha\rangle$, with mean photon number $|\alpha|^2$ (see Appendix A). The position in time of the coherent state is the value of the input taken by the prepare device.

$$|\psi_0\rangle = |\alpha\rangle\,|0\rangle\,...\,|0\rangle\,, \quad |\psi_1\rangle = |0\rangle\,|\alpha\rangle\,...\,|0\rangle\,, \quad |\psi_n\rangle = |0\rangle\,|0\rangle\,...\,|\alpha\rangle \tag{1}$$

Between each pair the overlap will be

$$\delta = |\langle\psi_i|\psi_j\rangle| = \exp\left(-|\alpha|^2\right) \tag{2}$$

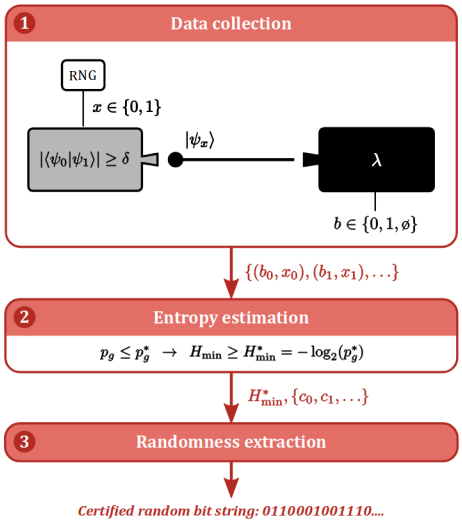


Figure 1: Steps of *Brask et al.* QRNG protocol. **(1)** Data is generated in a prepare-and-measure setup. The prepared states are known to have a certain minimal overlap, hence the preparation device is a 'gray box', while nothing is assumed about the measurement device, which is a 'black box'. **(2)** From the collected data, a conditional probability distribution for outputs given inputs is estimated, and from this, a bound on the entropy in the output data is evaluated. **(3)** Based on the entropy bound, a string of certified perfectly random bits are extracted from the output data.

Using this, we kept the advantage of realising the (optimal) USD measurement since the experimental setup would still simply require a single-photon detector with a timing resolution not bigger than for a distinction between two time bins. Depending on when the coherent state is detected this will set the outputs value b within $\{0,1,...,n\}$. If no click is detected the output is inconclusive $b = \varnothing$. Because the overlap between each pair of states is constant we still have $p(b = \varnothing) = \exp(-|\alpha|^2)$ in the absence of loss and noise.

In practice we may have some imperfections on the USD measurement due to imperfections in the experimental setup. Given probabilites $p(b|x)$ containing noise (i.e. $p(\varnothing|x) = \delta$, $p(b \neq \varnothing|x = b) = 1 - \delta - n * \epsilon$, $p(b \neq \varnothing|x \neq b \,\&\, x \neq \varnothing) = \epsilon$), and the overlap δ, one can bound the probability p_g of guessing the output of the prepare-and-measure device with a complete knowledge of all the system, such as the input state, every measurement details and so on. As for the (*Brask et al*) QRNG, the guessing propabilty is averaged over every inputs and measurement startegies, occuring with $p(x)$ and $p(\lambda)$, with λ a measurement strategy, respectively, we have

$$p_g = \sum_x p(x) \sum_\lambda p(\lambda) \max\{\mathrm{Tr}[\rho_x \Pi_\varnothing^\lambda], 1 - \mathrm{Tr}[\rho_x \Pi_\varnothing^\lambda]\} \tag{3}$$

where $\rho_x = |\psi_x\rangle \langle\psi_x|$ and $\Pi_\varnothing^\lambda$ are the elements of a $(n+1)$-outcome positive-operator-value measure POVM describing the measurement. Upper bounding p_g certifies randomness. One can use semi definite programming (SDP), as (*Brask et al.*) did but generalized to n-states (Annexe B). A good and practical bound of p_g is obtain by

$$p_g \leqslant p_g^* = \sum_{b,x} \nu_{bx} p(b|x) \tag{4}$$

For any ν_{bx} wich fulfill that there exists 2^n n x n Hermitian matrices $H^{\lambda_0,\lambda_1,...,\lambda_n}$, with $\lambda_0, \lambda_1, ..., \lambda_n = 0, 1,$

such that

$$\sum_x \rho_x \left(\frac{1}{2}\delta_{\lambda_x,0}\delta_{b,\varnothing} + \frac{1}{2}\delta_{\lambda_x,1}(1-\delta_{b,\varnothing}) - \nu_{bx}\right) + H^{\lambda_0,\lambda_1,\ldots,\lambda_n} - \frac{1}{n}\operatorname{Tr}[H^{\lambda_0,\lambda_1,\ldots,\lambda_n}]\mathbb{1} \leqslant 0. \tag{5}$$

Coefficients ν_{bx} that are optimal for particular data $p(b|x)$ are found *via* SDP (Annexe B). Thanks to the bound on p_g, one can extract the min-entropy[1]

$$H_{min} = -\log 2(p_g) \tag{6}$$

wich quantifies the number of certified random bit that can be extracted per bit of raw data[5].

3 Results and Implications

Bounding the guessing probabilty p_g for different number of inputs, mean number photon and efficiency allow one to derivate some new statements.
The more one increase the number of input taken by our QRNG, the more the min-entropy H_{min} increase as one can see in Fig. 2. This difference is significant around the mean number photon value wich gives the maximum of the min-entropy. However one might neglect this difference when sufficiently far away from that maximum (where min-entropy takes approximately the same value independently of the number of input).
The gap of min-entropy between n and $(n+1)$ inputs decrease exponentially as n increase.
The maximum min-entropy value is reach arround the same value of mean number photon. One can notice that the more inputs they are, the more the min-entropy peak-shape function is sharper. Since in an experimental setup a laser used in the prepare device send a number of photon around a certain value, increasing the number of inputs will, at a certain point, lack of usefulness, especially with low cost laser. I.e. between 4 and 5 inputs the only gain in min-entropy are for a range of mean photon number of around .3 (with an efficiency $\eta = .77$), wich is too thin for being useful.

The final random bit string is generated depending on the conclusiveness of the measurement. Final bits are a simple function of the measurement b which goes as follow

$$c(b) = \delta_{\varnothing,b} \quad b = \varnothing, 0, 1, ..., n \tag{7}$$

So increasing the number of inputs should not affect the min-entropy of the system. However, because the min-entropy seems to increase with the number of inputs, one can sates that the more inputs they are, the more robust to loss and noise the system is.

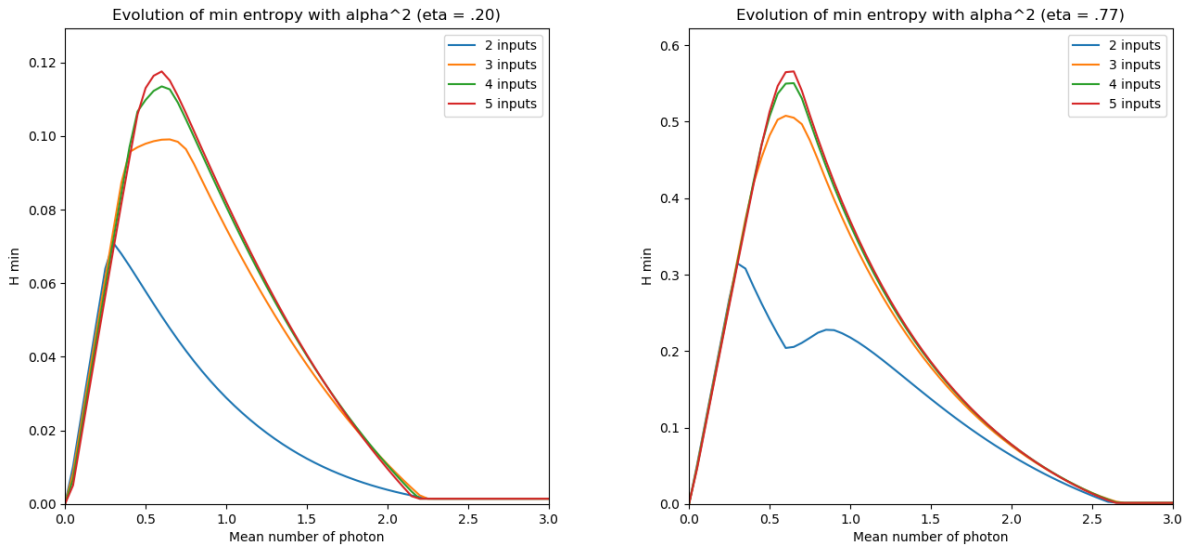
We also derive the evolution of maximum value min-entropy can take for different efficiency value as in Fig. 3. Increasing the number of inputs leads this function to fit a linear function with a slope $a < 1$. One can deduce that increasing the number of inputs for highering the maximum min-entropy become mostly significant for high measurement efficiency.

An other implication of a n-states inputs QRNG is on the output fequency. The more one increase n the more time measurement takes, since for every states added the detector as to wait for a time-bin more.

4 Conclusion

Our n-states generalisation increase the robustness of the (*Brask et al.*) QRNG against noise and loss. We have also explicit some limits of this imporvement, such as output frequency, and limits in experimental number of input. Implementing a n-states system is interesting for a QRNG that use time-bin encoding since it allows one to use a less efficient (so cheaper) detector, while still having a good useable entropy.

[1] Our implementation of the dual formulation of the SDP giving p_g^* and extraction of min-entropy can be found on gitlab : https://gitlab.com/plut0n/SDP-QRNG



(a) (b)

Figure 2: Evolution of H_{min} as a function of mean number of photon $|\alpha^2|$ between 0 and 3, for 2 to 5 inputs. Noise and loss are taken into account into probabilities $p(b|x)$.2a Detector efficiency is $\eta = .20$, this correspond to a low-cost experimental setup. 2b Detector effiency is set to $\eta = .70$.

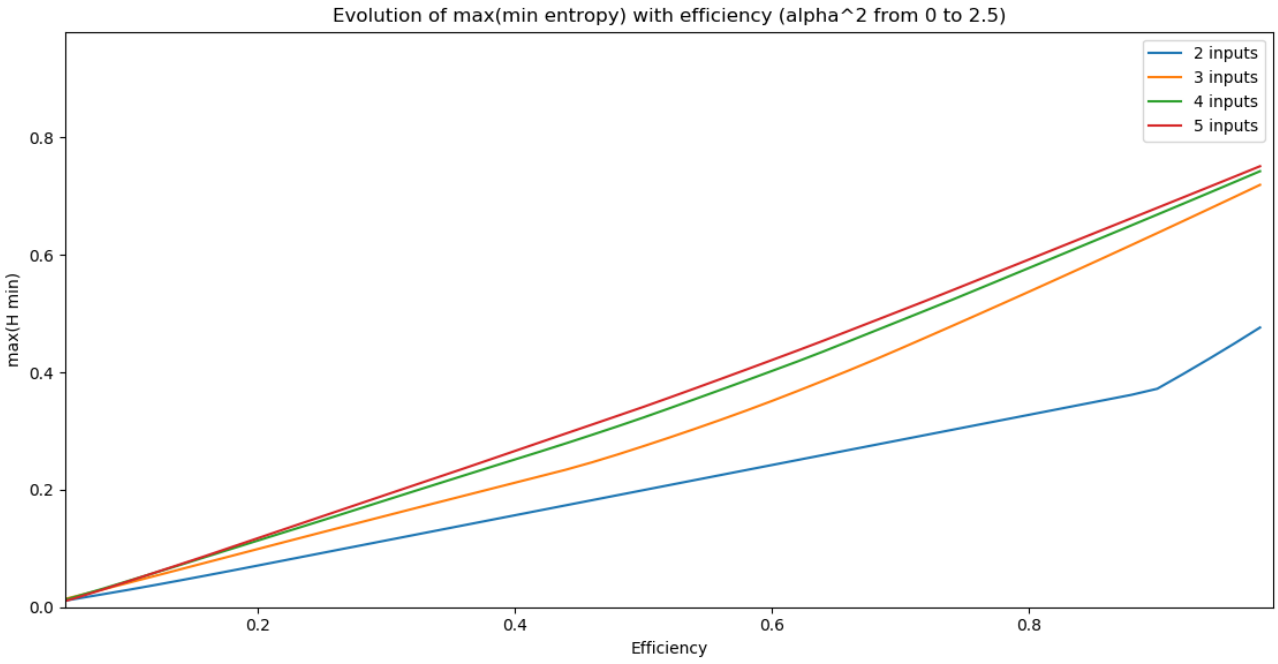


Figure 3: Evolution of the the maximum value of min-entropy H_{min}, taken for $|\alpha|^2$ between 0 and 2.5, as a function of efficiency η between 0 and 1

Appendices

A Creating n-states with constant overlap

In this Appendix, I show how one can create n-states with the same constant overlap between each pair. One can create the two first states in some basis $\{|0\rangle, |1\rangle\}$ as follow :

$$|\psi_0\rangle = |0\rangle, \quad |\psi_1\rangle = \delta\,|0\rangle + \sqrt{(1-\delta^2)}\,|1\rangle \tag{8}$$

Then, one can generate $n-2$ other states adding extra orthogonal basis, in order to have our n states, as follow :

$$|\psi_i\rangle = |\psi_{i-2}\rangle + x\,|i-1\rangle + y\,|i\rangle \quad \forall i \geqslant 2 \tag{9}$$

Where x comes from the constant overlap condition, and y comes from the normalisation condition,

$$x = \frac{\delta - \sum_{j=0}^{i-2} \langle j|\psi_{i-2}\rangle}{\langle i-1|\psi_{i-1}\rangle} \tag{10}$$

$$y = \sqrt{1 - \sum_{j=0}^{i-1} (\langle j|\psi_{i-1}\rangle)^2} \tag{11}$$

One can note that we should have a phase every time a basis appear more than once, exept for the $|0\rangle$ basis where one can absorb the phase into the basis. However creating states with this method, and thanks to the constant overlapping condition, set all phases to 0. The demonstration goes as follow

$$|\psi_j\rangle = \delta\,|0\rangle + ... + \exp(i\phi)x\,|j-1\rangle + y\,|j\rangle \quad \forall j \geqslant 2 \tag{12}$$

With the overlapping condition already respected when constructing state, and taking into account the phase we have

$$|\langle\psi_j|\psi_{j-1}\rangle| = \delta\exp(i\phi) = \delta \quad \forall j \geqslant 2 \tag{13}$$

$$\Leftrightarrow \quad \phi = 0 \tag{14}$$

B Bounding p_g by semidefinite programming

In this appendix, we bound the guessing probability using SDP. Let's simply generalise to a n-states system the primal formulation of the (*Brask et al.*) SDP, and then derive the dual formulation.
Using the (*Brask et al.*) method, one can bound the guessing propability, knowing the constant overlap between each pair of states δ and some data $p(b|x)$. As in [1] we will assume that all inputs are balanced, $p(x) = 1/n$, and we will denote $q_\lambda = p(\lambda)$ distribution of measurement strategies, and $\rho_x = |\psi_x\rangle\langle\psi_x|$ density matrices. With a n-states generalisation, we are now working in a n-dimensional Hilbert space, with n-states generating as in (Appendix A) in some basis $\{|0\rangle, |1\rangle, ..., |n\rangle\}$. Furthemore we no longer have two measurement strategies but n of them ; they are labeled λ_x where x determine wich term is maximal for the input x. For the following we keep the same notation as in [1].

This leads to the primal formulation of the SDP generalised to n-states,

$$\bar{p}_g = \frac{1}{n} \max_{M_b^{\lambda_0,\ldots,\lambda_n}} \sum_{x=0}^{n} \sum_{\lambda_0,\ldots,\lambda_n=0}^{1} \mathrm{Tr}\left[\rho_x \widetilde{M}_{\lambda_x}^{\lambda_0,\ldots,\lambda_n}\right], \tag{15}$$

such that,

$$M_b^{\lambda_0,\ldots,\lambda_n} = \left(M_b^{\lambda_0,\ldots,\lambda_n}\right)^\dagger \tag{16}$$

$$M_b^{\lambda_0,\ldots,\lambda_n} \geqslant 0, \tag{17}$$

$$\sum_b M_b^{\lambda_0,\ldots,\lambda_n} = \frac{1}{n} \mathrm{Tr}\left[\sum_b M_b^{\lambda_0,\ldots,\lambda_n}\right] \mathbb{1}, \tag{18}$$

$$\sum_{\lambda_0,\ldots,\lambda_n} \mathrm{Tr}\left[\rho_x M_b^{\lambda_0,\ldots,\lambda_n}\right] = p(b|x). \tag{19}$$

Using the Lagragian method to find the dual formulation of this SDP, one can obtain,

$$p_g^* = \min_{H^{\lambda_0,\ldots,\lambda_n},\nu_{bx}} -\sum_{bx} \nu_{bx} p(b|x) \tag{20}$$

such that,

$$H^{\lambda_0,\ldots,\lambda_n} = (H^{\lambda_0,\ldots,\lambda_n})^\dagger, \tag{21}$$

$$\sum_x \rho_x \left(\frac{1}{n}\delta_{\lambda_x,0}\delta_{b,\emptyset} + \frac{1}{n}\delta_{\lambda_x,1}(1-\delta_{b,\emptyset}) + \nu_{bx}\right) + H^{\lambda_0,\ldots,\lambda_n} - \frac{1}{n}\mathrm{Tr}[H^{\lambda_0,\ldots,\lambda_n}]\mathbb{1} \leqslant 0. \tag{22}$$

This dual formulation of the SDP conserve propreties (*Brask et al.*) derived.

References

[1] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, "Mhz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination," 2016.

[2] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," 2016.

[3] T. V. Himbeeck, E. Woodhead, N. J. Cerf, R. Garca-Patrn, and S. Pironio, "Semi-device-independent framework based on natural physical assumptions," 2016.

[4] D. Dieks, "Overlap and distinguishability of quantum states," *Physics Letters A*, vol. 126, pp. 303–306, jan 1988.

[5] R. Koenig, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," 2008.