How to exploit Bell non-locality to advance communication technologies?

Lecture 5: Quantum Random Number Generators

Nicolas Sangouard
Institut de Physique Theorique, CEA Paris Saclay
October 31 / Nov 1, 2022

1 Introduction

What do we mean when saying that a process generate good randomness? What constitutes good randomness may depend on the application, but here we are interested in the strongest definition: N bits are perfectly random if they are unpredictable, not only to the user of the device, but to any observer. Note that unpredictability by any observer may not be needed for some applications, like in Montecarlo simulation for example. However, from a fundamental perspective, it is difficult to argue that a process is random if there could exist observers able to predict its outcome. Note also that by demanding that the outcome is unpredictable to any observers, the randomness is guaranteed to be private: the user, by running the process in a secure location, has the guarantee that nobody knows the obtained results.

According to this definition of randomness, assumptions are needed for randomness generation. This follows from the unfalsifiable hypothesis of the existence of a super-deterministic model in which everything, including all the history of our universe, was pre-determined in advance and known by the external observer. From a fundamental point of view, a random number generator (RNG) is better than another if it is based on fewer or weaker assumptions.

Here we assume that the actions of any observer are constrained by the laws of quantum physics. In this context, we say that a given device generates good randomness if its output is produced by a process corresponding to a state indistinguishable from

$$\rho_{UE} = \left(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\right)^{\otimes N} \otimes \rho_E \tag{1}$$

where ρ_E is the state of adversary (including all the environment). This corresponds to N realizations of a perfect random bit, taking the value 0 and 1

with equal probability, which are totally uncorrelated with the state of the environment.

We distinguish three types of approaches for generating randomness. Pseudo-random-number generators (PRNG) typically use an algorithm to process an initial random seed. They are fast, cheap and the properties of the generated sequences are good enough for some applications. However, the random character of the output and their privacy is based on assumptions on the computational power of the adversary. But this is not the criterion adopted here, as we demand unpredictability to any observer, independently of its computational power. There are true random number generators (TRNG), that generate numbers as results of a complicated physical process. The second type of RNG are called true RNG, and exploit physical processes that are hard to predict. The difficulty is in this case either related to the required computational power and to the required precision on the knowledge of the initial state, as for chaotic systems. While sequences of random numbers obtained form TRNG are very challenging to predict, they are in principle deterministic. The last type of RNG are quantum RNG (QRNG), which exploit a quantum process believed to be fundamentally random. We consider one such a QNRG in the next section.

2 A simple QRNG with qubits

Consider a realization of a QNRG in which Alice receives an unknown single qubit state ρ and performs a measurement along the X direction of the Block sphere. The result is stored in a classical register Y with the convention that when the measurement result is -1, a 0 is written in the classical register while when $+1$ is obtained, 1 is written in the classical register. When repeating the process, Alice finds that both outcomes ± 1 happen with probability $1/2$, that is

$$\mathrm{tr}\rho\,\sigma_x = 0 \Leftrightarrow p(\pm 1|X) = \frac{1}{2}. \tag{2}$$

Each bit of the classical register Y is random for Alice. However, this does not mean that it is also random for any observer. For example, if an adversary, Eve, sets the state of the source ρ, she could first produce a random bit (e.g. by flipping a coin or using a QRNG), store the result in a classical register X and then prepare a state $\rho = |-\rangle\langle -|$ or $\rho = |+\rangle\langle +|$, depending on the bit value. The source state is given by $\rho_{XE} = \frac{1}{2}(|0\rangle\langle 0|\,|-\rangle\langle -| + |1\rangle\langle 1|\,|+\rangle\langle +|)$ and the post-measurement state is $\rho_{XAY} =$

$\frac{1}{2}((|0\rangle\langle 0|\,|-\rangle\langle -|\,|0\rangle\langle 0| + |1\rangle\langle 1|\,|+\rangle\langle +|\,|1\rangle\langle 1|)$. We can check that the uncertainty per bit $H(Y|X) = 0$ (or the information gain is $I(Y;X) = H(Y) - H(Y|X) = 1$), i.e. the register of Alice is fully correlated to the register of Eve.

This attack can be easily detected by Alice if she sometimes chooses to measure her state in the Z basis. Consider the case where Alice obtains the outcome $+1$ with probability p_+, i.e.

$$\mathrm{tr}\rho\,\sigma_z = n_z = p_+ - (1 - p_+). \tag{3}$$

For $p_+ = 1$, Alice can conclude that the state she receives is $\rho = |0\rangle\langle 0|$, and thus the bits in Y she generates with σ_x measurements are unpredictable for Eve. Yet, in practice, it is difficult (if not impossible) to realize such an ideal situation. Hence, let us compute how much randomness Alice gets in Y when $p_+ < 1$. Again we consider a situation where Eve samples a random value x_i from some alphabet with probabilities p_i and sends different states ρ_i to Alice. Alice measures the state and store the result in the form of a 0 or 1 in the register Y as before. We want to bound the information per bit $I(Y, X)$ that Eve can have about Alice's register. To do so, we first notice that mutual information is symmetric $I(Y, X) = I(X, Y)$. Furthermore $I(X, Y)$ can be bounded from the Holevo bound

$$I(X,Y) \leq S(\sum p_i\rho_i) - \sum_i p_i S(\rho_i) \leq S(\sum p_i\rho_i) = S(\rho). \tag{4}$$

We also know that the density matrix received by Alice has to satisfy the constraint given in Eq. (3). Hence the maximal information available to Eve is given by

$$I(Y,X) \leq \max_{\rho|\mathrm{tr}\rho\,\sigma_z = n_z} S(\rho). \tag{5}$$

It is easy to see that the entropy is maximized for the state $\rho = \frac{1}{2}(\mathbb{1} + n_z\sigma_z)$. Since the eigenvalues of ρ are $1/2(1 \pm n_z)$, we have

$$I(Y,X) \leq -\frac{1+n_z}{2}\log_2\left(\frac{1+n_z}{2}\right) - \frac{1-n_z}{2}\log_2\left(\frac{1-n_z}{2}\right). \tag{6}$$

This corresponds to the binary entropy, i.e. the entropy of a Bernoulli random variable with probabilities $p = 1/2(1 + n_z)$ and $1 - p = 1/2(1 - n_z)$. The value of the binary entropy is depicted in Fig. 1. We see that as long as $n_z > 0$, the information gain $I(Y, X) < 1$. Since $I(Y, X) = H(Y) - H(Y|X)$ and $H(Y) = 1$ (Alice receives either $|0\rangle$ with probability $1/2(1 + n_z)$ and $|1\rangle$ with probability $1/2(1 - n_z)$ that she systematically measures with σ_x and hence the result is fully random), we conclude that $I(Y, X) < 1$ implies

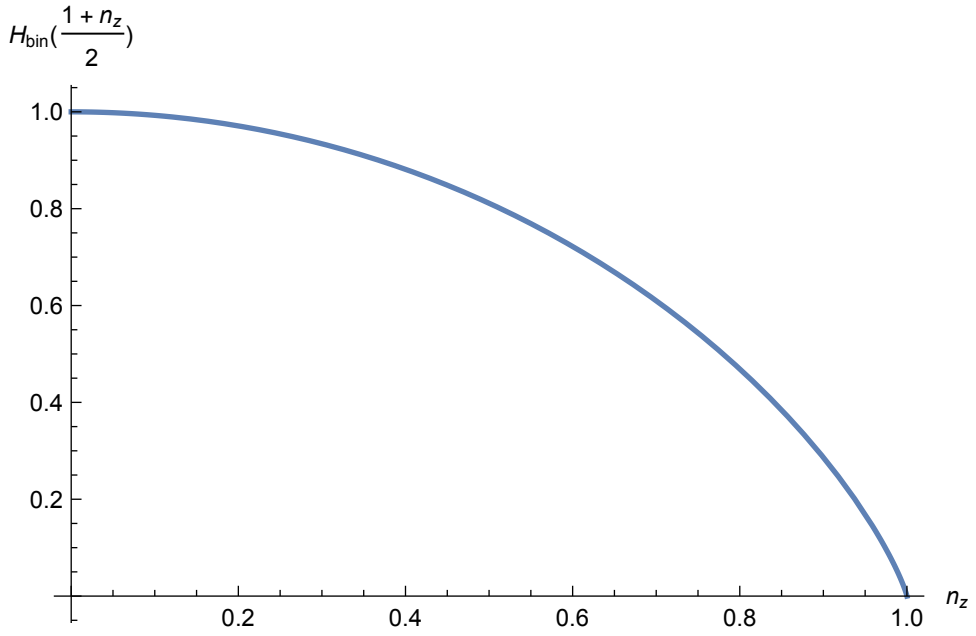

Figure 1: The binary entropy function $H_{\text{bin}}(\frac{1+n_z}{2})$.

$H(Y|X) > 0$, i.e. Eve does not have full information about Y.

3 An attack on our QRNG

In section 2, we have considered a QNRG in which bits are obtained by measuring qubits in a state ρ with a σ_x measuring and checking that $\text{Tr}\,\rho\sigma_z = n_z$. The bound on Eve's information that we derived only holds in experimental realizations where σ_x and σ_z measurements are implemented. The privacy of the randomness can be completely corrupted if this is not the case. To see this, consider the following two-qubit realisation of Alice's measurements

$$A_X = \sigma_x \otimes \mathbb{1} \quad \text{and} \quad A_Z = \mathbb{1} \otimes \sigma_z. \tag{7}$$

The possible outcomes of such measurement are also ± 1 as in the original scenario. Yet, it is very easy for Eve to trick Alice. As before, she can sample a random bit x which can take two values 0 and 1 and, depending on its values, send the state

$$\rho_0 = |+\rangle\langle+| \otimes |0\rangle\langle 0| \quad \text{or} \quad \rho_1 = |-\rangle\langle-| \otimes |0\rangle\langle 0| \tag{8}$$

to Alice. It is easy to see that for both states, the result of the measurement

A_Z is systematically $+1$ while the outcome of A_X seems random to Alice as she receives the results ± 1 with probability $1/2$, but the outcome is fully determined by Eve's bit x.

5 Device-independent QRNG with CHSH

The randomness guarantees of commercially available QRNG rely on a quantum model of their implementation. We have seen that if the device do not work as expected, the randomness guarantees can be completely corrupted. We here introduce device-independent (DI) QRNG, i.e. randomness generators with randomness guarantees that do not rely on the assumption that the underlying quantum devices are perfectly characterized and trusted. As you might expect the central resource is Bell non-locality. As in previous lecture we will focus our attention on a particular Bell test – the CHSH inequality.

5.1 Self-testing as guarantee of randomness: basic idea

Let us start with a simple question. With what we already know about selftesting, can we conclude anything about the randomness of measurement outcomes observed in CHSH test, if Alice and Bob observe its maximal score $2\sqrt{2}$? We have shown in particular, that from the maximal CHSH score of $2\sqrt{2}$, we can deduce that state and the measurement operators are of the following form

$$\rho = |\Phi^+\rangle\langle\Phi^+| \otimes \rho_{\text{junk}}, \quad A_i = \sigma_i \otimes \mathbb{1}^A_{\text{junk}} \quad \text{and} \quad B_j = \sigma_j \otimes \mathbb{1}^B_{\text{junk}}. \tag{9}$$

Given the form of the measurements, it follows that the auxiliary subsystem ρ_{junk} has no effect on the measurement outcomes

$$\text{tr}\rho\, A_i \otimes B_j = \text{tr}\, |\Phi^+\rangle\langle\Phi^+|\ \sigma_i \otimes \sigma_j. \tag{10}$$

Furthermore, because the state $|\Phi^+\rangle$ is pure it can not be correlated to any other system. In particular the joint state of Alice, Bob and Eve can only be of the form

$$\rho_{ABE} = |\Phi^+\rangle\langle\Phi^+| \otimes \rho_E \tag{11}$$

where ρ_E includes the auxiliary subsystem not contributing to the measurement results. Hence, After Alice's measurement, the classical-quantum state of Alice and Eve state is indistinguishable from the state $\rho_{UE} = \left(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\right) \otimes \rho_E$. This corresponds to a good randomness, taking the value 0 and 1 with

equal probability, which is totally uncorrelated with the state of Eve. A natural question for practical purpose is : what can we say about randomness in case the CHSH score is smaller than $2\sqrt{2}$?

5.2 Existence of good randomness from CHSH test implemented with imperfect devices

Consider a scenario in which Eve chooses a bi-partite state ρ and distributes it to Alice and Bob. Under the assumption

i) $\rho \in L(\mathbb{C}^2 \otimes \mathbb{C}^2)$

ii) the fidelity with the two-qubit maximally entangled state $F = \langle \psi^- | \, \rho \, | \psi^- \rangle$ is in the interval $[1/2, 1]$

there exists a measurement on Alice's subsystem[1] whose outcome cannot be

[1]Consider the strategy in which Eve holds a purification of Alice and Bob's two-qubit state ρ, i.e.

$$\phi_{ABE} = \sum_i \sqrt{p_i}\,|i\rangle \otimes |\psi_i\rangle \tag{12}$$

where $\{|i\rangle\}$ is a family of mutually orthogonal vectors used to store the value i. p_i and $\rho_i = |\psi_i\rangle\langle\psi_i|$ are such that $\rho = \sum_i p_i\rho_i$ has a fidelity F with $|\psi^-\rangle$. Consider the binary measurement described by the Pauli operator σ_z for the choice of Alice's measurement. The post-measurement state

$$\bar{\rho}_{ABE} = \sum_i p_i\,|i\rangle\langle i| \otimes (p(+1|i)\,|0\rangle\langle 0| \otimes \rho^B_{i|0} + p(-1|i)\,|1\rangle\langle 1| \otimes \rho^B_{i|1}) \tag{13}$$

where $p(\pm 1|i) = \mathrm{Tr}\,\frac{1}{2}(\mathbb{1} \pm \sigma_z) \otimes \mathbb{1}\rho_i$ is the probability for Alice to get outcome ± 1 for Eve's choice ρ_i and $\rho^B_{i|0/1}$ is the state of Bob conditioned on Alice's qubit being projected into $|0/1\rangle$. Eve's register contains full information about Alice's outcome in case $p(-1|i) = 1$ or $p(+1|i) = 1$ and no information if $p(+1|i) = p(-1|i) = 1/2$. In other words, Eve's best guessing probability for any state ρ_i is given by

$$P^i_{\text{guess}} = \max_{s=\pm 1} \mathrm{Tr}\,\frac{1}{2}(\mathbb{1} + s\sigma_z) \otimes \mathbb{1}\rho_i. \tag{14}$$

Note that for every two-qubit state ρ_i achieving some value of $\mathrm{Tr}\,\frac{\mathbb{1}-\sigma_z}{2} \otimes \mathbb{1}\,\rho_i$, the state $\tilde{\rho}_i = (\sigma_x \otimes \sigma_x)\rho_i(\sigma_x \otimes \sigma_x)$ fulfills $\mathrm{Tr}\,\frac{\mathbb{1}-\sigma_z}{2} \otimes \mathbb{1}\,\rho_i = \mathrm{Tr}\,\frac{\mathbb{1}+\sigma_z}{2} \otimes \mathbb{1}\,\tilde{\rho}_i$ while the two states have the same singlet fidelity. We thus deduce that it is sufficient to optimize Eq. (14) for $s = +1$ only (Indeed, let ρ_i be the state maximizing $\mathrm{Tr}\,\frac{1}{2}(\mathbb{1} + \sigma_z) \otimes \mathbb{1}\rho_i$. If there is a state ρ'_i giving a value for $\mathrm{Tr}\,\frac{1}{2}(\mathbb{1} - \sigma_z) \otimes \mathbb{1}\rho'_i$ which is larger than $\mathrm{Tr}\,\frac{1}{2}(\mathbb{1} + \sigma_z) \otimes \mathbb{1}\rho_i$ then the state $\bar{\rho}_i = (\sigma_x \otimes \sigma_x)\rho'_i(\sigma_x \otimes \sigma_x)$ would give a value for $\mathrm{Tr}\,\frac{1}{2}(\mathbb{1} + \sigma_z) \otimes \mathbb{1}\bar{\rho}_i$ larger than $\mathrm{Tr}\,\frac{1}{2}(\mathbb{1} + \sigma_z) \otimes \mathbb{1}\rho_i$, which is not possible.).

Let us consider the decomposition of $\frac{\mathbb{1}+\sigma_z}{2} \otimes \mathbb{1}$ as

$$\underbrace{-\left(\tilde{z}(r)\left|\omega(r)^+\right\rangle\!\left\langle\omega(r)^+\right| + (z(r)-1)\,|00\rangle\langle 00| + z(r)\,|11\rangle\langle 11|\right)}_{G} + z(r)\mathbb{1} - t(r)\left|\psi^-\right\rangle\!\left\langle\psi^-\right| \tag{15}$$

with

$$|\omega(r)^\pm\rangle = \frac{1}{\left(2 - 4\sqrt{r(1-r)}\right)^{1/2}}\left(\left(1 - 2\sqrt{r(1-r)}\right)|01\rangle \pm (2r-1)\,|10\rangle\right) \tag{16}$$

and

$$\tilde{z}(r) = \left(2\sqrt{r(1-r)}\right)^{-1},\ z(r) = \left(\sqrt{\frac{r}{1-r}} + 1\right)/2,\ t(r) = \frac{2r-1}{2\sqrt{r(1-r)}}. \tag{17}$$

The guessing probability can be rewritten as

$$\begin{aligned} P^i_{\text{guess}} &= -\,\mathrm{Tr}\,G(r)\,\rho_i + z(r)\,\mathrm{Tr}\,\rho_i - t(r)\,\langle\psi^-|\,\rho_i\,|\psi^-\rangle \\ &\leq z(r) - t(r)F_i \text{ for any } r \in [1/2, 1] \end{aligned} \tag{18}$$

guessed by Eve with a probability larger than

$$P_{\text{guess}}^{\max} = \frac{1}{2} + \sqrt{F(1-F)}. \tag{20}$$

In a CHSH scenario in which a CHSH score higher than the self-testing threshold is observed, there exists a choice of extraction maps allowing one to identify a two-qubit state with a singlet fidelity bounded by a function of the CHSH score, cf lecture note on self-testing. This suggests, together with Eq. (20), that the guessing probability can be bounded directly from the CHSH score. Let us show this in detail.

In a CHSH test, we have seen that the hermitian operators A_x are block diagonal with blocks of dimension 2, i.e. there are of the form $\sum_i \Pi_i A_x \Pi_i$ where Π_i is the projector on block i. From Alice's point of view, the measurement of A_x thus amounts at projecting first in one of the two-dimensional subspaces and then performing a qubit measurement in this subspace. It cannot be worth for Eve to perform the projection herself. This can be done by choosing a state of the form $\rho = \sum_{ij} p_{ij}\rho_{ij}$ with p_{ij} the probability to get a successful projection into the blocks i for Alice and j for Bob, and ρ_{ij} the resulting two qubit state. Let S_{ij} be the CHSH score obtained from ρ_{ij}. We gave a lower bound in the lecture note 3 (see formula given in Eq. (42)) on the fidelity using the CHSH score. A tighter bound can be obtained when considering qubit states. It has been shown in particular that there exist local unitaries U_A^{ij} and U_B^{ij} such that (see arXiv:0907.2170)

$$F_{ij} = \langle\psi^-|U_A^{ij} \otimes U_B^{ij} \rho_{ij} (U_A^{ij})^\dagger \otimes (U_B^{ij})^\dagger |\psi^-\rangle \geq g(S_{ij}) = \frac{1}{2}\left(1 + \sqrt{\frac{S_{ij}^2}{4} - 1}\right).$$

Note that

$$F_{ij} = \langle\psi^-|(U_B^{ij})^\dagger U_A^{ij} \otimes \mathbb{1} \rho_{ij} (U_A^{ij})^\dagger U_B^{ij} \otimes \mathbb{1} |\psi^-\rangle.$$

Let Eve do the choice of measurement σ' that Alice performs (which is linked to σ_z by $\sigma' = U_A^{ij}(U_B^{ij})^\dagger U \sigma_z U^\dagger (U_B^{ij})^\dagger U_A^{ij}$). What is the probability that Eve

since $\operatorname{Tr}\rho_i = 1$ and $G(r) \geq 0$ for $r \in [1/2, 1]$. The minimum of $z(r) - t(r)F_i$ being obtained for $r = F_i$, we have $P_{\text{guess}}^i \leq z(F_i) - t(F_i)F_i = \frac{1}{2} + \sqrt{F_i(1-F_i)} = h(F_i)$. Since the second derivative of $h(F_i)$ is negative for any value $F_i \in [0,1]$, that is $h(F_i)$ is concave, we have for any state $\rho = \sum_i p_i \rho_i$

$$P_{\text{guess}} = \sum_i p_i P_{\text{guess}}^i \leq \sum_i p_i h(F_i) \leq h\left(\sum_i p_i F_i\right) = h(F). \tag{19}$$

correctly guesses Alice's outcome? We have

$$\begin{aligned} P_{\text{guess}}^{ij} &= \text{Tr}\,\frac{1}{2}\left(\mathbb{1}+\sigma'\right)\otimes\mathbb{1}\rho_{ij} \\ &= \text{Tr}\,\frac{1}{2}\left(\mathbb{1}+\sigma_z\right)\otimes\mathbb{1}\underbrace{U^\dagger(U_B^{ij})^\dagger U_A^{ij}\otimes U^\dagger\rho_{ij}U_A^{ij}(U_B^{ij})^\dagger U\otimes U}_{\rho'_{ij}} \end{aligned}$$

where

$$\langle\psi^-|\rho'_{ij}|\psi^-\rangle = F_{ij}$$

since $U\otimes U\,|\psi^-\rangle = |\psi^-\rangle$. The demonstration leading to Eq. (20) tells us that

$$\begin{aligned} P_{\text{guess}}^{ij} &= \text{Tr}\,\frac{1}{2}\left(\mathbb{1}+\sigma_z\right)\otimes\mathbb{1}\rho'_{ij} \\ &\leq \frac{1}{2}+\sqrt{F_{ij}(1-F_{ij})} \\ &\leq \frac{1}{2}+\sqrt{g(S_{ij})(1-g(S_{ij}))} = h(g(S_{ij})). \end{aligned}$$

The third inequality holds because $h(x)=\frac{1}{2}+\sqrt{x(1-x)}$ is decreasing for $x\in[1/2,1]$. We conclude that the guessing probability for the whole state ρ is given by

$$\begin{aligned} P_{\text{guess}} &= \sum_{ij} p_{ij}P_{\text{guess}}^{ij} \\ &\leq \sum_{ij} p_{ij}h(g(S_{ij})) \\ &\leq h(g(\sum_{ij} p_{ij}S_{ij})) \\ &= h(g(S)) = \frac{1}{2}(1+\sqrt{2-S^2/4}) \end{aligned}$$

where the third inequality holds because $h(g(x))$ is concave for $x\in[2,2\sqrt{2x}]$. We deduce

$$H(A|E)\geq H_{\min}(A|E) = -\log_2(P_{\text{guess}}) \geq 1-\log_2\left(1+\sqrt{2-\frac{S^2}{4}}\right). \quad (21)$$

We conclude that there is no need to assume that the quantum devices are perfectly calibrated to derive a bound on Eve's entropy about Alice's outcomes, see also Ref. arxiv:0911.3427 for another derivation of the previous

formula. There is also no notion of trust in the sense that the choice of measurement operators and state are given to the adversary.

It is important to note that when dealing with CHSH, we always assume that the measurement settings of Alice and Bob are chosen at random, i.e. can not be predicted by Eve who controls the source. Thus to produce device-independent randomness one requires some randomness to start with. Strictly speaking, one has to speak about randomness expansion (random bits obtained from the measurement outcomes is added to an initial string of private random bits). Furthermore, in order to check the CHSH value Alice and Bob sometimes have to reveal some of their measurement inputs, which consumes some of their original random bits. However, in practice Alice and Bob can only check the CHSH value for a small fraction of runs (chosen randomly by one of them), such that the amount of consumed randomness is low.