Quantum Optics and Laser 2021/22
Report 4 - QRNGs and QKD
Prof. Paolo Villoresi

Samuele Piccinelli
(Dated: 30 January, 2022)

In this work we review and compare generation of random numbers via both pseudo-random (software-based) algorithms and quantum processes. We will see how the latter is capable of producing a random bit sequence with noticeably higher randomness quality.
Furthermore, we will a review an example of quantum key distribution (QKD), which makes possible the distribution of the secret key between two parties, Alice and Bob. We will estimate some noteworthy probabilities and the value of the quantum bit error rate (QBER) for all involved bases.

1 Quantum random number generator

1.1 Theoretical background

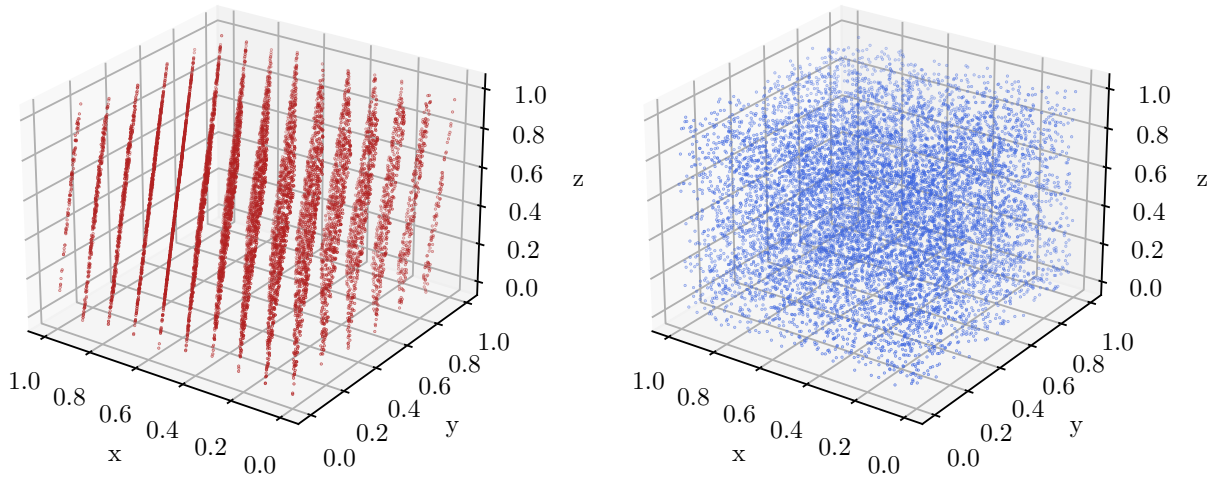
Generation of random numbers is a central problem for many applications in the field of information processing, including, e.g., cryptography, in classical and quantum regime, but also mathematical modelling, Monte Carlo methods, gambling and many others. Both the quality of the randomness and efficiency of the random numbers generation process are crucial for the most of these applications. Software produced pseudo-random bit sequences, though sufficiently quick, do not fulfil required randomness quality demands. Hence, the physical hardware methods are intensively developed to generate truly random number sequences for information processing and electronic security applications.
The proposed investigation, based on the statistical interpretation of the data collected in the laboratory, aims to compare the performance of a quantum process and of some reference pseudo-random algorithms for the generation of random numbers.

1.2 Experimental setup

The measurement setup includes:

- Two single-photon detectors (photon counters);
- A He-Ne laser source and related optical instrumentation;
- A multi-mode fibre, suitably coupled to the preceding modules to direct the light flow to the detectors;
- A 50/50 beam splitter (BS).

The operating principle of the system is based on the property of the indivisibility of photons: two extensions are made from the fibre, one for each detector. An injected photon will randomly take one of the paths, with a probability of exactly 50%. If a digital output is associated with the detection of a photon - 0 if it is collected by the first sensor, 1 if it is collected by the second - it is possible to generate a random sequence of bits.



(a) Values generated with RANDU.

(b) Values generated with a QRNG.

Figure 1: Three-dimensional plot of 10^4 values generated with the RANDU algorithm and a QRNG. Each point represents 3 consecutive (pseudo-random) values.

1.3 Analysis and discussion

In this context, the detection of a photon is assimilated to a Bernoulli extraction, with $p = 0.5$. It is, therefore, to be expected that the arithmetic mean of a sufficiently long series of independent extractions collapses around the value of p. Indeed, computing the mean and variance, one gets

$$\begin{aligned} p &\approx 0.4924 \\ \text{var} &= pq = p(1-p) \approx 0.2499, \end{aligned}$$

the latter being near to the expected theoretical value of p^2.
As comparison with the values generated from the experimental setup, we use IBM's RANDU generator. The latter is defined by the recurrence:

$$V_{j+1} = 65539 \cdot V_j \mod 2^{31}$$

with the initial seed number, V_0 as an odd number. It generates pseudo-random integers V_j which are uniformly distributed in the interval $[1, 2^{31} - 1]$, but in practical applications are often mapped into pseudo-random rationals X_j in the interval $(0, 1)$, by the formula:

$$X_j = \frac{V_j}{2^{31}}.$$

RANDU is widely considered to be one of the most ill-conceived random number generators ever designed [1].
The dataset consists of 603k 0/1 bits; we group the binary stream into bytes (8 bits), and then each byte to a triplet of coordinates and plot the resulting points in the 3D space, alongside the ones obtained via RANDU. The results are reported in Fig. 1. It can be easily seen that the points in the case of the RANDU generator fall in 15 two-dimensional planes, while for the case of the QRNG under study the values explore the whole 3D space.

2 Quantum key distribution (QKD)

2.1 Theoretical background

Quantum key distribution (QKD) provides the only physically secure and proven method for the transmission of a secret key between two distant parties, Alice and Bob, who are connected by an authenticated classical channel and an (insecure) quantum channel. The security of QKD is based on the no-cloning theorem (which prohibits perfect cloning of an unknown quantum state with perfect fidelity) and also on the Heisenberg uncertainty principle.
Wootters and Zurek showed in [2] that it is impossible to construct a device that will produce an exact copy of an arbitrary quantum state. If perfect cloning was allowed then Eve would duplicate exact copies of the signal states being transmitted between legitimate parties. However imperfect cloning is possible, but it comes at a cost of being easily detectable.
In a QKD protocol, the quantum-bit-error-rate (QBER) refers to the fraction of positions where Alice's and Bob's bit strings differ. The QBER is generally a direct measure for the secrecy of Alice and Bob's strings since any eavesdropping strategy would perturb the correlations between them.

The QKD implementation under study is the BB84 protocol, which consists of a public classical channel (where each party, including the eavesdropper, can listen to conversations but cannot change the contents of the message) and of a quantum communication channel used for the transmission of quantum signals. Alice sends a stream of qubit, A, selected randomly encoded in two bases $A = \{X, Z\}$. In particular, $a = \{H, V\}$ if the basis is $A = Z$, while if $A = X$ the transmitted state is just $a = D$. This optimises the encoding strategy, minimising the resources to be used. Bob chooses at random the measurement base $B = \{X, Z\}$ and can obtain the state $b = \{H, V\}$ if $B = Z$ or $b = \{D, A\}$ if $B = \{X\}$. The chance to have the same basis on Alice and Bob is 50%. In these cases the measurement is correlated with the coding by Alice: in the other cases, the output is random and thus useless for the purposes of QKD.

2.2 Dataset

The experimental data of the transmitter and receiver are contained in two separate files. The events with no detections due to the channel attenuation are already discarded: there is thus a direct correspondence between what A sent and the related measurement of B.

2.3 Analysis and discussion

To characterise the QKD system, we use the data in pairs from Alice's and Bob's files and estimate the following quantities:

- The probability that A encodes in the base X, $P(A = X)$, and Z, $P(A = Z)$;
- The probability that B chooses the base X, $P(B = X)$ and Z, $P(B = Z)$;
- All the possible conditioned probabilities at the receiver, $P(b|a)$, where $b = \{H, V, D, A\}$ and $a = \{H, V, D\}$;
- The QBER achieved in the state s with $s = \{H, V, D\}$, $P(a \neq b|a = s)$;
- The QBER achieved in the base X, $P(a \neq b|A = X, B = X)$ and Z, $P(a \neq b|A = Z, B = Z)$.

Bob \ Alice	H	V	D
H	0.5 ± 0.7	0.01 ± 0.08	0.2 ± 0.5
V	0.0 ± 0.1	0.5 ± 0.7	0.3 ± 0.5
D	0.3 ± 0.5	0.2 ± 0.5	0.5 ± 0.7
A	0.2 ± 0.5	0.3 ± 0.5	0.01 ± 0.07

Table 1: Possible conditioned probabilities at the receiver, $P(b|a)$, where $b = \{H, V, D, A\}$ and $a = \{H, V, D\}$. The sum over each column yields 1 as expected.

Each of these is computed as ratio of counts, according to the classical definition of probability as the number of possible cases over the number of total cases.
The results are reported below and in Table 1, together with their respective uncertainties.

$$P(A = Z) = 0.9 \pm 0.9 \qquad P(A = X) = 0.1 \pm 0.3 \tag{1}$$
$$P(B = Z) = 0.5 \pm 0.7 \qquad P(B = X) = 0.5 \pm 0.7 \tag{2}$$

The probability with which Alice sends states in the Z and X basis are biased, while Bob measures with 50/50 probability. Since the probability to have Alice and Bob using the same basis is 50%, in the sifting phase we lose half of the raw key. In an efficient implementation of the protocol [3], both Alice and Bob choose between the two bases randomly, independently but not uniformly. In other words, the two bases are chosen with substantially different probabilities. As Alice and Bob are now much more likely to be using the same basis, the fraction of discarded data is greatly reduced, thus achieving a significant gain in efficiency (almost a factor two in the key generation rate). In this implementation, the two basis have different roles: the key is extracted only from Z-basis measurements, while the X basis is used for checking on the presence of a potential eavesdropper.

Coming to the QBER, using information theoretic arguments concerning the mutual information between Alice, Bob and Eve, an upper bound of $\sim 14.6\%$ (as explained in [4]) can be found on the tolerable error rate for key distribution secure against individual attacks. The estimates found in our analysis are well compatible with this threshold, showing our implementation to be both robust (in terms channel losses) and secure. The amount of information losses, in the absence of eavesdropping, depends strongly on the length of the channel and may be caused by the attenuation of photon signal (due to the weak pulse laser), the detector efficiency mismatch (due to the high dark counts) and the depolarizing channel noise effect. The implementation under study makes use of a relatively short optic fibre cable, justifying the values found in Eq. (3).

$$P(a \neq b|A = Z, B = Z) = (1.603 \pm 0.005)\% \tag{3}$$
$$P(a \neq b|A = Z, B = Z) = (1.12 \pm 0.01)\%$$

Finally, we report the values of the QBER for each state sent by Alice. The results are in line with the fact that Bob chooses a specific base with 50/50 probability: the fraction of mismatched bits reflects this behaviour.

$$P(a \neq b|a = H) = 0.5127 \pm 0.0003 \tag{4}$$
$$P(a \neq b|a = V) = 0.4865 \pm 0.0003 \tag{5}$$
$$P(a \neq b|a = D) = 0.5287 \pm 0.0007 \tag{6}$$

The security of the protocol is based on Alice's and Bob's use of two non-orthogonal complementary measurement bases, which makes the result of a second measurement in the complementary basis random. Thus, any eavesdropper attempting to gain information on the photons being sent to Alice or Bob will inevitably disturb the entangled state and introduce errors into the raw key. Therefore, all Alice and Bob need to do to check the security of their raw key, is to compare a small random subset of the bits from their raw key over the public classical channel to estimate the QBER.
This security argument can be illustrated with a simple eavesdropping approach where Eve intercepts and measures the photons, meant to reach Bob, in one of the two polarization bases. Eve then re-sends another photon to Bob, polarized according to the measurement outcome of the intercepted photon. Alice and Bob only keep results where they measure in the same basis: Eve now has a 50% chance of measuring in either basis. If Eve measures in the same basis as Bob, then she does not introduce any errors and Alice and Bob get the anti-correlated measurement results which they expect. However, 50% of the time Eve measures in the complementary basis and now will introduce an error into Bob's key due to his subsequent complimentary measurement and the Heisenberg uncertainty principle. Thus, Bob will get an error with a probability of 50%. Therefore, the total error rate that Eve induces will be 25%. This is well above the mentioned tolerable QBER of $\sim$ 14.6% for individual attacks and will be detected by Alice and Bob, alerting them to the presence of an eavesdropper.

---

[1] For the Python implementation of the RANDU algorithm we refer to this GitHub repository.
[2] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[3] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and proof of its unconditional security," (2005), arXiv:quant-ph/0011056 [quant-ph].
[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Reviews of Modern Physics **74**, 145–195 (2002).