

A Continuous Variable Based Quantum Random Number Generator

Frédéric Grosshans (1), Vincent Jacques (2), Jean-François Roch (3)

1: Laboratoire de Photonique Quantique et Moléculaire, UMR 8537, CNRS / ENS Cachan, 61 Avenue du Président Wilson, 94235 Cachan Cedex, France. frederic.grosshans@ens-cachan.fr

2: Laboratoire de Photonique Quantique et Moléculaire, UMR 8537, CNRS / ENS Cachan, 61 Avenue du Président Wilson, 94235 Cachan Cedex, France. jean-francois.roch@ens-cachan.fr

3: Laboratoire de Photonique Quantique et Moléculaire, UMR 8537, CNRS / ENS Cachan, 61 Avenue du Président Wilson, 94235 Cachan Cedex, France. vincent.jacques@ens-cachan.fr

Abstract

Intrinsic randomness of quantum mechanics is one of its key fundamental properties. Radioactive decay has been used for a long time to generate random number tables and, more recently, single photon based quantum random number generators (QRNG) are commercially available for cryptographic applications. We describe here a QRNG based on the sampled shotnoise of a white lamp. The random bit stream is a 4.2 Mhz TTL signal, and the improvement of this QRNG to 100 Mhz should not be difficult. We also give a lower bound on its Shannon entropy, under the pessimistic assumption that the adversary has a full control over all classical noise. (105 words)

Introduction

Random number generation has many uses, from its trivial application to games to more serious ones, like Monte-Carlo simulation and cryptography. The latter is a heavy consumer of random numbers and needs the random bits at a high rate. Furthermore, the security of many cryptographic protocols, and specially quantum key distribution, relies heavily on the supposed impossibility of an adversary to have any knowledge on a random bit string.

Their intrinsic randomness make quantum phenomena ideal for random number generation, and quantum optics allows to build high-rate quantum random number generators (QRNG). While recent quantum-optics based QRNGs rely on single photon detectors, we describe here a shotnoise based QRNG. The main advantage of such a QRNG is its experimental simplicity and low cost: it only needs an ordinary photodiode, a light source, and a standard amplifier. Furthermore, this simplicity, and the use of standard telecom components allows us to hope for QRNG with a rate in the 100 Mbits/s in the near future.

Furthermore, we carefully study our experimental set-up, and quantify the quantum contribution to the random bits, in terms of a lower bound on the Shannon entropy of its bit stream, under the pessimistic hypothesis that the adversary knows —and controls — perfectly the classical noise sources.

Description of the experimental set-up

The QRNG construction is very simple and only needs standard a light source, a standard photodiode, an amplifier and a comparator (see figure 1); it therefore only took us a few hours to find the required components build a working prototype! To extract our output bits, we sample the amplified shotnoise of a white lamp and take its sign with a comparator. The

output of our generator is a 4.2 MHz TTL bit stream. This rate was close to the limit of our amplifier, but the construction of similar QRNG in the 100 MHz range should not be difficult and the GHz seems to be attainable with today's technology.

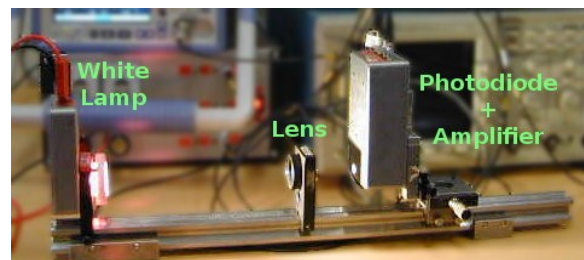


Figure 1: Photograph of the QRNG

Quantum contribution to the randomness

However, if the randomness of such a QRNG is sufficient for fundamental quantum mechanics tests [1–3], its use in cryptographic protocols needs a careful theoretical analysis. The use of a continuous variable (the light intensity) as noise source and the finite bandwidth amplifiers makes this analysis more complex than the analysis of discrete variable based QRNG, where the physical data is binary from the start and presents negligible time correlations.

To characterize a QRNG, one needs to discriminate between the classical and quantum contribution to the randomness of its output. While the classical contribution can look random is is deterministic in principle. We will assume that it is known — and even controlled — by the adversary. On the other hand, the result of the measurement of a quantum superposition is impossible in principle and will be assumed here to be the only source of true randomness. In our case, the measurement is an intensity measurement, in the Fock basis, and our lamp sends coherent states $|\alpha\rangle$. The conditional probability $P(n|\alpha)$ to meas-

ure n photons obeys a Poisson distribution with average and variance $|\alpha|^2$. The variable controlled by the adversary are the value of $|\alpha|^2$, as well as the classical noise added by the amplifier. The variance of these classical noises can be experimentally characterized. The characterization of a QRNG is therefore a bound on the conditional probabilities $P(\mathbf{b}|C)$, where \mathbf{b} is the bit-string and C the worst classical noise compatible with the observed variances.

Characterization of the temporal correlations

The precise meaning of “worst” in the previous sentence depends on the application of the QRNG, but a quite generic measure of its quality is the Shannon entropy per bit of its output bit-string. We will therefore compute a lower bound of this entropy $H' = H(\mathbf{b}|C)/N$, for a N bit string $\mathbf{b}=(b_{-N}, \dots, b_0)$. When $N \rightarrow \infty$, if we assume the process to be time invariant, one has $H' = H(b_0|C, b_{-1}, \dots, b_{-\infty})$. We are therefore interested in the conditional probability distribution of the bit b_0 , given the value of the classical noise C and all previous bits.

In order to set bounds on these conditional probabilities and entropies, we approximate the Poisson distribution $P(n|\alpha)$ of the intensity measurement by a Gaussian distribution of same variance and average. The Berry-Esséen theorem [4] guarantees that the error in the cumulative distribution due to this approximation is always smaller than $C_\infty/|\alpha|$ with $C_\infty \approx 0.7164$. This approximation allows us to write $b_0 = \text{sign}(K_0 + U_0)$, where K_0 (resp. U_0) is known (resp. unknown) by the adversary. U_0 's distribution is known and Gaussian, while K_0 is an arbitrary function of the previous bits $(b_{-1}, \dots, b_{-\infty})$ and the classical noises. The conditional probabilities for the two values of b_0 are therefore $P(b_0|K_0) = 1/2(1 \pm \text{erf}(K_0/\sqrt{2\langle U_0^2 \rangle}))$.

The dependence of K_0 on the previous bits only comes from the finite bandwidth of our linear amplifier, which induces correlations between successive values of the quantum noise. Since we are only interested by a lower bound on the bias (or the entropy), we are allowed to overestimate it by supposing the spy knows the previous values of the quantum noise.

We can then directly compute the dependence of K_0 on $(U_{-1}, \dots, U_{-\infty})$ from the measured pulse response of the amplifier.

The classical noise can then be “pessimized”, depending on the application of the QRNG. For example, if the figure of merit of interest is the conditional Shannon entropy H' introduced above, one can easily show that this entropy is a concave function of $|K_0|$, and this reduces the worst possible distribution of K_0 is the one with the most peaked absolute value possible. This allows then to directly compute the value of H' for our QRNG and for various sampling rates

Main achievements

- We have built a low cost QRNG operating at 4.2 MHz.
- We have set lower bounds on the contribution of the quantum noise to its Shannon entropy under pessimistic assumptions.

Conclusions

This work shows that simple continuous variable based QRNG can be competitive with more usual discrete-variable based quantum ones. We are working on our simple prototype, in order to improve its performance. The theoretical analysis presented above can also be extended toward other figure of merits, like smooth entropies.

References

1. DCE Science Vincent Jacques et al Science, 315 (2007), page 966; arXiv:quant-ph/0610241
2. Vincent Jacques et al Annales de Physique, 32 (2007), page 195; arXiv:0710.2597
3. Vincent Jacques et al., Physical Review Letters 100 (2008), 220402; arXiv:0801.0979
4. Po-Ning Chen, unpublished (2002) ; <http://shannon.cm.nctu.edu.tw/html/paper/be02.pdf>