A True Random Number Generator based on quantum-optical noise

André de Almeida Ruegger[1], Geraldo A. Barbosa[2], Jeroen van de Graaf[3], Gilberto Medeiros[1], Julio Cezar de Melo[4], Roberto Nogueira[1], Wagner Rodrigues[1], Fernando Soares[1]

[1]Departamento de Física, UFMG

[2]QuantaSec—Consulting, Projects and Research in Physical Cryptography Ltd.

[3]Departamento de Ciência da Computação, UFMG

[4]Departamento de Engenharia Eletrônica, UFMG

Contact author: geraldoabarbosa@gmail.com

Abstract. *In this note we report a project to construct a True Random Number Generator based on quantum noise (shot noise of light). It achieves speeds of 1Gb/s and above which is about 3 orders of magnitude faster than the known bit generator Quantis (from IDQuantique). This generator is part of a platform for secure communications called KeyBITS.*

1. Motivation and problem

Suppose you have a bundle of fiber optics cable consisting of several hundred channels connecting two end points. You control the physical security of these end points, but you fear that the cable has been intercepted (maybe by some foreign spying agency). What can you do to protect your communications?

Here, quantum cryptography can be of help. The security of protocols such as BB84 [1], which can be run over fiber optics cables, is based on a principle of quantum mechanics, called the inference-disturbance principle[3]. It says that if an adversary is able to obtain information about bits sent over the channel, then the legitimate parties can quantify how much of the secret is leaked. This makes the quantum channel tamper proof, so it can be used to transport random bits to be used as a one-time pad key. Alternatively one can use this quantum channel for key transportation, and use symmetric encryption algorithms in order to encrypt all traffic. However, the optical technology used in quantum cryptography is very delicate since the protocol requires single photon pulses, which are both difficult to produce and to detect. For a thorough overview of this technology including all its problems, see [2].

A different approach, called mesoscopic optics, uses medium-intensity light of ≈ 100 to 10000 photons per pulse, which is still well below the high-intensity pulses used in conventional telecom systems ($> 10^{15}$photons/sec). Contrary to single-photon pulses, medium-intensity light can be produced and detected using off-the-shelve products of low cost, giving a significant advantage over BB84 and similar protocols. However, the underlying quantum-mechanical description of mesoscopic optics is different, and so is the underlying physical principle on which the security of the KeyBits Platform is based.

By sharing a preliminary seed between sender and receiver, the receiver know which basis to use in order to perform the right measurement and can therefore distinguish perfectly between a 0 and 1. But the adversary, who does not have this additional information, does not know how to measure correctly. The signal he measures will not be pure because of the shot noise or quantum-optical noise. In this context this noise manifests itself as an uncertainty in the phase angle as measured by the adversary, it is of an intrinsic quantum-mechanical nature, *not* an imperfection of the measurement equipment. This fact puts the adversary at a disadvantage compared to legitimate parties, leading to high imprecision when it tries to distinguish between a 0 or 1 sent over the channel.

Another manifestation of quantum-optical noise in a coherent field is the well-known fact that the amount of photons sent is not constant, but will always fluctuate, following a Poisson distribution. This fluctuation can be used as a source of true randomness, which is exactly what we use to construct the TRNG. For more details on shot noise see [**?**].

2. A True Random Number Generator

As a first step towards implementing the tamper-proof protocol outlined above, we focussed on implementing a True Random Number Generator (TRNG). (Actually it is a *bit* generator but we conform to traditional terminology.) In order to be useful for an optical channel one needs a true random bit generator at speeds compatible with fiber-optical technology, say 1 gigabit per second or more. This is a challenging problem since most TRNGs are very slow and have difficulties reaching even 1 megabit per second. Most designs are based on chips leading to PRNGs (Pseudo Random Number Generators) that may use thermal light fluctuations to enhance the randomness characteristics. But as part of the noise created in this process is of a thermal nature, it implies high correlations within the light field. For instance, the state-of-the-art TRNG implemented by Intel as a special instruction uses the physical randomness to create a random seed, which is then expanded using the AES cipher in order to obtain high speeds [4].

We are in the process of constructing a TRNG which uses quantum optics as the basis for randomness, by exploiting the quantum-optical noise of a laser in a coherent state.

3. Schematics of our quantum-optical TRNG

Fig. 1 shows a diagram of the TRNG. Basically, a laser excites a detector that produces a fluctuating current as its output. Upon amplification the voltage output presents fluctuations around an average voltage. After a signal processing stage, the $\pm$ fluctuations will be coded as V_+ and V_- signals that will correspond to the stream of bits K. Fig. 2 shows an extended view of a bench prototype of the TRNG. At the fundamental level the laser is in a coherent state in which the photon statistics has a Poissonian distribution in the number of photons n:

$$p(n) = \frac{e^{\langle n \rangle} \langle n \rangle^n}{n!} \, . \tag{1}$$

The most important characteristics of this distribution is that the photons present no correlation among themselves: $\langle n_1 n_2 \rangle = \langle n_1 \rangle \langle n_2 \rangle$. Similarly, a small group of photons

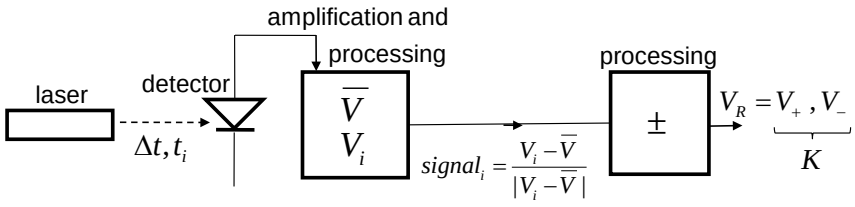


Figure 1. Schematics of the TRNG.

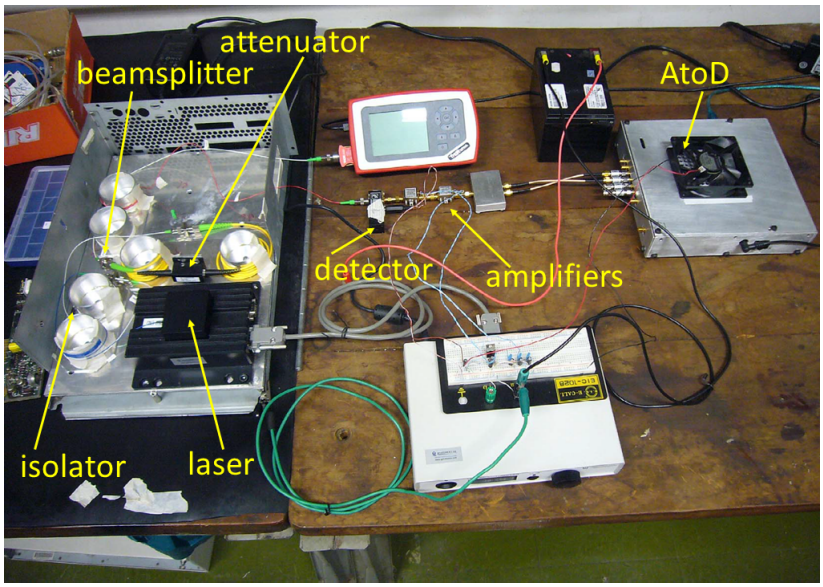
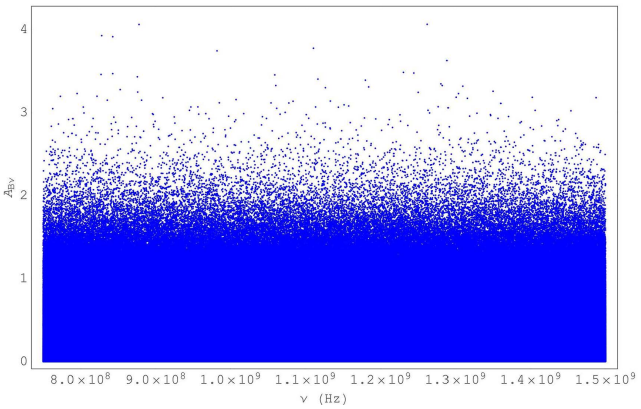


Figure 2. Bench prototype of TRNG.

measured within a short time interval Δt is independent of another group and this leads to the generation of uncorrelated bits. To achieve this characteristics the laser and detection system has to be prepared such that the noise associated to the optical field is much larger than all electronic noises present. This is known as "shot-noise" limited state.

Under this condition, bits are generated from the V_+ and V_- signals at the detector output. The average value of photons within Δt, $\langle n \rangle$, will lead to an average voltage $\overline{V}$. Δt is set such that $\Delta t \ll \tau$, the laser coherence time. This assures that the laser is with a given phase and, therefore, amplitude fluctuations are maximized. Photon number and phase have associated operators that do not commute, similarly as complementary pairs in a Heisenberg uncertainty principle.

The fluctuations around this value produce the bits. As an example, a sample of 19660800 bits were generated and its Fourier spectrum taken. Fig. 3(left-side) shows the "white-noise" characteristics of the Fourier spectrum of 19660800 bits. The right side shows results of the NIST tests on the 19660800 bits. All tests are plenty satisfactory. There is no parallel worldwide of a physical random generator with such functional simplicity and speed. The actual speed, $1.5GHz$ (bits/per second) is just due to the AtoD digitizer used and much higher speeds can be achieved with a faster electronics. Fundamentally, the optics field fluctuations has a white-noise characteristic for all light frequencies. Therefore, our scheme is not bounded by the physical principle used but just by the electronics – that can be improved according to the current state of art.



Teste	P-Value
ApproximateEntropy	0.812035
BlockFrequency	0.751001
CumulativeSums	0.784649
CumulativeSums(reverse)	0.842644
FFT	0.669945
Frequency	0.607710
LinearComplexity	0.709032
LongestRun	0.948537
NonOverlappingTemplate	146/148
OverlappingTemplate	0.672652
RandomExcursions	8/8
RandomExcursionVariant	18/18
Rank	0.695808
Runs	0.511987
Serial	2/2
Universal	0.953639

Figure 3. Left-side: "White-noise" spectrum of 19660800 bits. Right side: Results of the NIST tests on the 19660800 bits.

4. Conclusions

An essential part of a plataform for secure communication, a fast TRNG, has been constructed. It has an original and simple design and besides the use within this platform, it presents many possible independent uses, such as games. Its speed is high, compatible with current optical communication hubs and can still be increased with no fundamental bounds besides techological ones. The presented TRNG can follow those advances with no fundamental obstacle.

References

[1] C. Bennett, G. Brassard. *Quantum cryptography: Public key distribution and coin tossing.* In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.

[2] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dusek, N. Lutkenhaus, M. Peev. *The Security of Practical Quantum Key Distribution.* `http://arxiv.org/abs/0802.4155`

[3] C. Fuchs. *Distinguishability and Accessible Information in Quantum Theory*. `http://arxiv.org/abs/quant-ph/9601020`.

[4] G. Taylor, G. Cox. *Digital randomness.* IEEE Spectrum, Vol. 48(9), pgs 32 – 58, September 2011

