ICFO - The Institute of Photonic Sciences
White Paper, rev.1
August 2016

Ultra-Fast Quantum Random Number Generator

For the most demanding applications,
the most trusted source

Randomness is Essential

Random number generators (RNGs) are essential in a wide range of applications, such as secure communications[1], stochastic simulations[2] and gambling[3]. Data encryption uses RNGs to generate cryptographic keys. Stochastic simulations depend on random numbers to accurately price financial derivatives or model nuclear fusion. Random numbers are essential yet producing them with perfect unpredictability is still very challenging[4]. A device developed at ICFO enabled landmark experiments in Quantum Physics proving the non-local and random nature of our universe. This device is the first ultra-fast, and true random number generator.

Entropy and Randomness

Claude Shannon, the founding father of communications, defined the concept of entropy by quantifying how much a message can be compressed without losing information[5-6]. If a message has low entropy, for example a large sequence of ones “11111… 111”, it can be compressed significantly. In contrast, a truly random sequence of ones and zeros has high entropy because it cannot easily compress into a smaller number. All of the bits are relevant to reconstruct the message.

In other words, **entropy is the measure of how uncertain and unpredictable something is.** For example, if one observed a fair coin toss with no other information, the results would have high entropy for the observer. However, if this observer knew the starting position of the coin and the surrounding forces, the result would have low entropy because it could be predicted and simplified into a formula.

Randomness and entropy are abstract concepts in information and communication technologies. Moreover, entropy has different meanings for different applications. For example, Shannon entropy is only tangentially related to the concept used in thermodynamics[4]. In cryptography, high entropy means that random numbers are unpredictable and **an observer cannot guess future values given present information.** In stochastic simulations, high entropy means that random numbers are independent and non-correlated.

High entropy means random numbers are unpredictable, independent and non-correlated.

How are random numbers generated?

Pseudo RNG (PRNG)

PRNGs are computer software programs commonly used to generate substitutes for true random numbers. They are deterministic algorithms that rapidly generate bit sequences with long repetition lengths. **They are designed to eliminate statistical anomalies but not withstand an intelligent observer.** While they pass the statistical tests for randomness, they are not random at all. Similar to the coin toss example, if an observer knows the code, current state and inputs, it can reliably predict the output. Regarding Stochastic Simulations, Marsaglia famously demonstrated correlations between PRNGs in his landmark publication that reduced confidence in results using these numbers[7]. **PRNGs have advanced considerably since Marsaglia but risk of bias remains.**

Hardware RNG (HRNG)

HRNGs take input data from physical random processes to generate random bits. Some examples include electronic and thermal noise[8] and chaotic dynamics in semiconductor lasers[9]. HRNGs derive randomness from classical physical phenomena that pass statistical tests for randomness. As with the coin toss example, however, **they have far less entropy under observation.** HRNGs are further criticized because they can be damaged or their measurement devices can be tampered with[4].

Cryptographically Strong PRNG (CS-PRNG)

The cryptography community is mistrustful about RNG that cannot be understood and scrutinized. FreeBSD blocked HRNGs from directly seeding their cryptographic systems over suspicion the devices were compromised[10].

CS-PRNGs address the shortcomings discussed in pseudo and hardware RNG. Fortuna is a well-regarded example because it can recover to an unknown state even under observation, making it difficult for an observer to predict future outputs[4]. It accomplishes this by frequently refreshing its internal state using entropy collected from multiple sources in the operating system. This is analogous to substituting our coin-tosser with another and moving to a new room. Additionally, Fortuna is open-source and peer reviewed to build trust[11].

Even Fortuna is susceptible to attack however, as its **entropy sources may not be independent**[12]. This might apply if our coin-tossers trained at the same academy and the tossing rooms were similar. To address this concern, sensitive applications like data encryption add entropy from HRNGs to CS-PRNGs. Since HRNGs are still vulnerable, data is encrypted in a Hardware Security Module (HSM), a separate hardened device designed to protect against tampering and observation.

Quantum RNG (QRNG)

QRNGs are a subset of HRNGs. **Randomness is obtained using quantum phenomena, a non-deterministic process where all outcomes are possible and nothing is certain until it is observed.** QRNGs have been around for some time, however they have suffered either from poor speed or measurement bias. Until now...

The QRNG made @ICFO

Using commercially available optical components we demonstrated a QRNG with a multi gigabit per second bit rate. The patented technology* is based on the phase-diffusion process occurring in semiconductor lasers widely used for optical communications. The process relies on the quantum mechanical principle of spontaneous emission to generate true random numbers.

*US9218160 (B2) and US14/923,495

The Benefits of Quantum

Entropy estimation is an experimentally hard problem. There is no solution using classical physics because one cannot reliably determine how much an observer knows. In the context of cryptography, one must assume that an observer cannot sustain knowledge of the RNG in order for it to safely generate keys. This is folly because an observer does not remain still and increases their ability to collect information with technology, practice and time.

Quantum processes are inherently unpredictable, even under observation. As a result, entropy estimation is possible and we quantify the amount of entropy present in the raw output of our device through open algorithms. We also quantify entropy present from non-trustable sources such as classical phase noise, digitization errors, and finite bandwidth effects. These entropy measurements, along with the QRNG developed at ICFO, were crucial for the recent landmark experiments proving the nonlocal and random nature of our universe.

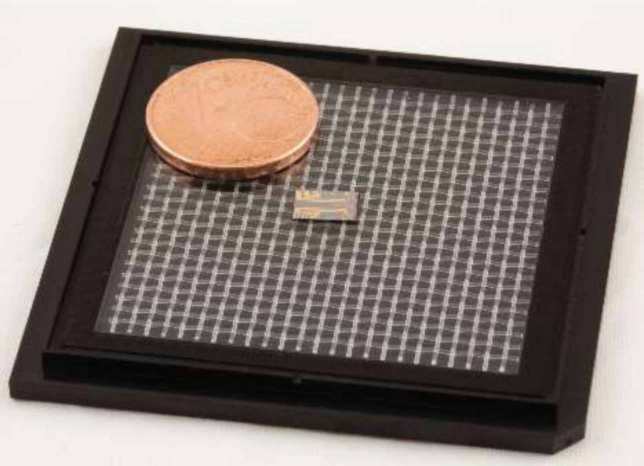

Figure 1. ICFO QRNG integrated in an Indium Phosphide chip[E]. A one-cent euro coin is shown for reference.

The findings depended on true randomness, and using ICFO's technology were published in well regarded scientific journals, including Nature and Physical Review Letters[A-D], and covered by mainstream media including the New York Times and The Economist[13-14].

From the perspective of stochastic simulations, our technology offers two important features. First, it generates random numbers at a very fast rate. Second, it produces *truly* random numbers that are independent and unbiased.

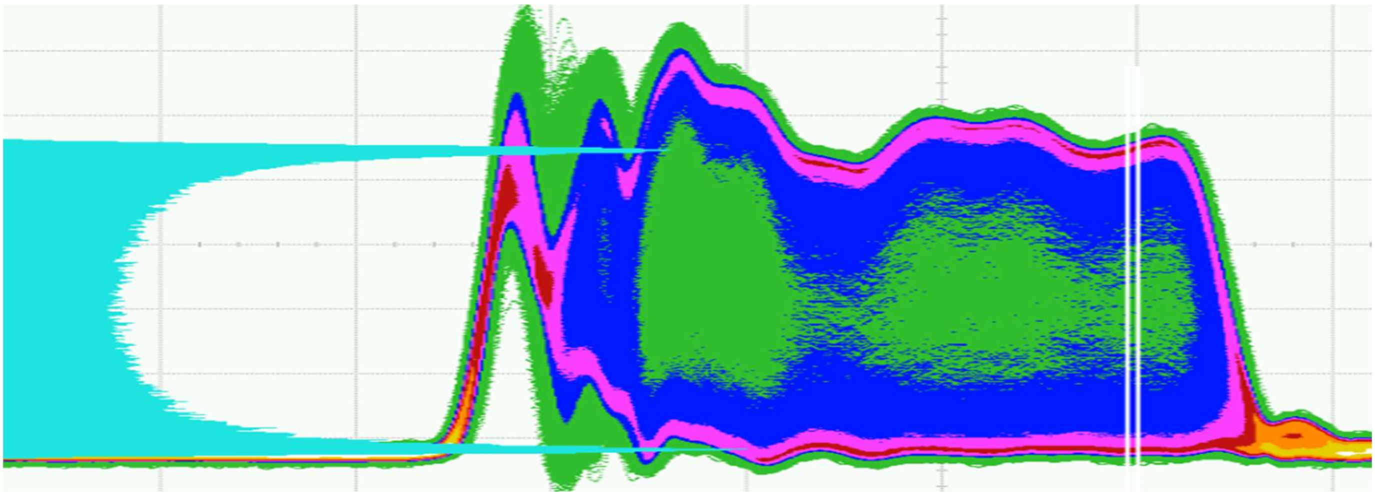

Figure 2. ICFO QRNG analog output from the device developed for the loophole-free Bell tests. The histogram on the left shows an arcsine distribution, expected from the foundations of quantum mechanics. The sharp edges of the distribution indicate very high interference visibility and stability.

Innovate, Prototype, Demonstrate

We are experts in quantum physics, photonics and technology. **We are looking to partner** with experts in non-core industries such as cryptography, stochastic simulations, telecommunications and others that require ultra-fast and true random number generators. **Through these partnerships we plan to further develop our technology and maximize its industrial and social impact**, both through academic publications and commercial ventures. We are sharing our scientific devices with laboratories across the globe, testing our commercial devices in diverse environments and seeking more opportunities to demonstrate our technology [F].

The QRNG technology developed at ICFO was trusted by the three landmark experiments proving the nonlocal and random nature of our universe.

About ICFO

The Institute of Photonic Sciences is a research centre situated in metropolitan Barcelona. It hosts 350 people, including group leaders, post-doctoral researchers, PhD students, engineers and staff including MBAs. ICFO members are organized in 23 research groups and work in 60 state-of-the-art laboratories equipped with the latest experimental infrastructure and facilities for nanofabrication, characterization, imaging and engineering. The Severo Ochoa distinction (Ministry of Science and Innovation), 13 ICREA Professorships, 19 European Research Council grants and 6 Fundació Cellex Barcelona Nest Fellowships, demonstrate the centre's dedication to research excellence. The centre has a Corporate Liaison Program that aims to link industry with research and participates actively in the European Technological Platform Photonics21. ICFO hosts incubator activities and actively seeks venture capital investment. To date, ICFO has created 5 successful start-up companies[G].

ICFO The Institute of Photonic Sciences
A member of BIST Barcelona Institute of Science and Technology
Generalitat de Catalunya
Universitat Politècnica de Catalunya BarcelonaTech
Fundació Privada CELLEX
Fundació Privada MIR-PUIG
Fundació Catalunya La Pedrera
erc
Excelencia Severo Ochoa 2016-2019
AXA Research Fund
ICREA

Contact

Dr. Silvia Carrasco
Director, Knowledge and Technology Transfer
ktt@icfo.eu

Authors

Elie Calvin Benchimol
Business Development
Knowledge and Technology Transfer
elie.benchimol@icfo.eu

Carlos Abellán
PhD Student
Optoelectronics
carlos.abellan@icfo.eu

Sergi Ferrando
Business Development
Knowledge and Technology Transfer
sergi.ferrando@icfo.eu

Prof. Dr. Morgan Mitchell
Group Leader
Quantum Information with Cold Atoms and Non-Classical Light
morgan.mitchell@icfo.eu

Prof. Dr. Valerio Pruneri
Group Leader
Optoelectronics
valerio.pruneri@icfo.eu

ICFO Publications & Notes

A. B. Hensen et al, "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres", Nature 526, 682-686 (2015).
B. L. K. Shalm et al., "Strong loophole-free test of local realism", Phys. Rev. Lett. 115, 250402 (2015)
C. M. Giustina et al., "Significant-loophole-free Test of Bell's Theorem with Entangled Photons", Phys. Rev. Lett. 115, 250401 (2015).
D. C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, M. W. Mitchell, "Generation of fresh and pure random numbers for loophole-free Bell tests", Phys. Rev. Lett. 115 (2015)
E. C. Abellán et al, "A quantum entropy source on an InP photonic integrated circuit for random number generation", to appear in Optica.
F. Scientific studies typically use q-Fresh, offering low latency (12 ns + 5*k) and low predictability (10^{-4}); commercial prototype use off-the-shelf components and connects to a PC via PCIe or LAN; all offer ultra-fast true random numbers.
G. ICFO Spin-Offs: HemoPhotonics, Signadyne, ProCareLight, Cosingo and Radiantis.

External References

1. Tajima et al., "Practical quantum cryptosystem for metro area applications," IEEE J. Sel. Topics Quantum Electron. 13, 1031–1038 (2007).
2. X. Cai and X. Wang, "Stochastic modelling and simulation of gene networks - a review of the state-of-the-art research on stochastic simulations," IEEE Signal Process. Mag. 24, 27–36 (2007).
3. C. Hall and B. Schneier, "Remote electronic gambling," pp. 232–238 (1997).
4. Ferguson, Schneier and Kohno, "Cryptographic Engineering", Wiley 137-145 (2010)
5. Dougherty, "Claude Shannon", V61.0003, New York University Linguistics Department, Web, accessed Aug. 2016.
6. Shannon, "A Mathematical Theory of Communication", The Bell System Technical Journal Vol.27 (1948).
7. Marsaglia, "Random Numbers Fall Mainly in the Planes", Boeing Scientific Research Laboratories (1968).
8. C. Petrie and J. Connelly, "A noise-based ic random number generator for applications in cryptography," IEEE Trans. Circuits Syst. I, Fundam. Theory Appl 47, 615–621 (2000).
9. Kanter et al., "An optical ultrafast random bit generator," Nature Photon. 4, 58–61 (2010).
10. Goodin, Oct. 2013, arsTECHNICA, Web, accessed Aug. 2016.
11. Dodis et al, "How to Eat Your Entropy and Have It Too", Cryptology ePrint Archive, (2014).
12. Barak and Halevi, "A model architecture for pseudo-random generation with applications to /dev/random", Cryptology ePrint Archive, (2005).
13. Markoff, "Sorry, Einstein. Quantum Study Suggests ´Spooky Action´ is Real", New York Times, Oct. 2015, Web, accessed August 2016, http://nyti.ms/1OIO2WJ
14. From the print edition, "Hidden no more", The Economist, October 2015, Web, accessed Aug 2016, http://www.economist.com/node/21676733/print