Quantum Randomness on a Chip

Online banking, e-commerce and data protection are currently secured by pseudo-random numbers which could, eventually, one day be cracked due to the fact that they are not truly random. A new approach based on quantum optics may soon allow for safer operations by efficiently generating truly random numbers.

Heads or tails? The result of flipping a coin can appear random because we are not able to control what side the coin will land on. This is random enough for everyday use, but not inherently random. Scientists have long been looking for ways to create truly random number generators based on the only area of physics in which randomness genuinely exists: quantum physics. While current experimental setups remain relatively slow, large, and expensive, a new approach proposed by Alireza Marandi, from Stanford University (California, USA) and collaborators may soon produce fast, cheap random number generators on a simple chip, which could then be integrated in a laptop or tablet for high-security applications such as internet banking, more efficient statistical sampling, and ever increasing levels of security in games of chance.

In today's world, random numbers take center stage in many areas of our daily lives, and more so since the advent of online commerce and banking. Put simply, the codes we use to secure these services rely on the fact that a potential adversary cannot predict said numbers. Thus, whenever we need to reveal our credit card information or bank account number, random numbers are used to encrypt this information, and to prevent criminals from obtaining it.

"Actually, most 'random numbers' appear 'random' because of the convoluted algorithms used to produce them. Strictly speaking, these are *deterministic* algorithms, and after some large number of iterations they (the pseudo-random numbers) will show cyclic repetitions," Boris Zeldovich [1], from CREOL at the University of Central Florida (USA) says. Security when dealing with large data volumes is therefore reduced. Moreover, two identical conventional random number generators can be synchronized to predict a random number sequence, as Yoon-Ho Kim [2] from the Pohang University of Science & Technology (South Korea) explains, but synchronization would be impossible with a genuine random number generator.

How can truly random numbers be generated, then? As it turns out, quantum physics offers a solution. Countless experiments indicate that a quantum system that has to choose between one of two states does so completely randomly. This probabilistic aspect of quantum physics is in stark contrast with the deterministic nature of classical physics. Not surprisingly, it has taken a long time for the scientific community to fully embrace the inherent randomness of quantum physics.

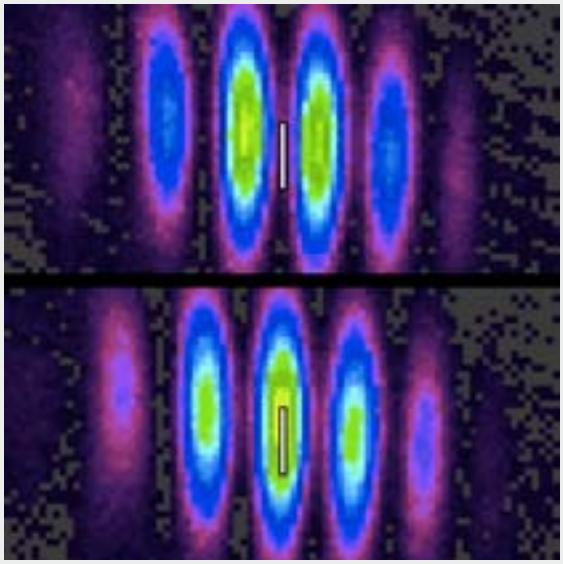

Figure 1: How to generate random numbers. The setup toggles between two complementary fringe patterns (heads or tails). The center (white line) will coincide with a minimum or maximum of the pattern, which can be interpreted as a random 0 or 1. Image: Alireza Marandi, Stanford University.

Marandi's experiment shows how to exploit quantum randomness in an otherwise classical system. "Intuitively speaking," he says, "we gradually start generating photons while forcing them to decide between heads or tails. Then, we amplify them to the point where we can treat them with conventional, classical optics. This means we can avoid the usual complicated quantum setup, and it clears the way towards high-speed, cheap, and on-chip truly random numbers." Concretely, Marandi and his team use a crystal that converts one photon into two photons of double the original wavelength. During this conversion, they are able to make these photons choose between one of two possible states — heads or tails. Once the resulting photons have been ampli-

fied beyond the point where quantum physics is necessary, conventional classical optics can be used, and the need to use cumbersome quantum techniques avoided.

"The biggest advantage of our setup is its conceptual simplicity," Marandi says. Because of this, he expects that it will soon be possible to put his setup onto a single chip, which could then be used in security and statistical devices.

"The idea by Marandi, Leindecker, Vodopyanov, and Byer is really extremely nice and beautiful," Zeldovich summarizes. "Good ways to generate random numbers are becoming more and more important," Kim adds. "The bit-rate reported in this work (theoretically up to Giga-bits per second) is quite impressive," he concludes, envisioning possible uses that could range from enhancing quantum cryptography to affording greater safety in Las Vegas casinos.

[1] B. Ya. Zeldovich & D. N. Klyshko, Field statistics in parametric luminescence, ZhETF Pis. Red. 9, 69-72 (1967), in Russian; Sov. Phys. JETP Lett. 9, 40-43 (1969), in English.

[2] Y.-S. Kim, J.-C. Lee, O. Kwon & Y.-H. Kim, Protecting entanglement from decoherence using weak measurement and quantum measurement reversal, Nat. Phys. 8, 117–120 (2012).

[3] O. Kwon, Y.-W. Cho & Y.-H. Kim, Quantum random number generator using photon-number path entanglement, Appl. Opt. 48, 1774-1778 (2009).

Armand Niederberger

Alireza Marandi, Nick C. Leindecker, Konstantin L. Vodopyanov & Robert L. Byer, **All-optical quantum random bit generation from intrinsically binary phase of parametric oscillators**, Optics Express **20**, 19322-19330 (2012).