QUANTUM PHYSICS

The certainty of randomness

Communication systems rely on random-number generators for the encryption of information. A method for producing truly random numbers even from untrustworthy devices could lead to improvements in security. SEE LETTER P.223

STEFANO PIRONIO

Encryption schemes used in modern cryptography make extensive use of random, unpredictable numbers to ensure that an adversary cannot decipher encrypted data or messages. Reliable random-number generators are therefore crucial. For instance, an Internet-wide analysis identified tens of thousands of servers that are vulnerable to basic attacks because of the use of poor-quality random-number generators[1]. On page 223, Bierhorst *et al.*[2] exploit effects at the crossroads of quantum physics and special relativity to demonstrate the ultimate random-number generator, achieving unprecedented security.

Although schemes to generate random-looking numbers are easy to come up with, assessing their security — the extent to which they are truly unpredictable to a potential adversary — is notoriously difficult. Much of the trouble stems from the fact that such schemes cannot be tested by merely looking at their output from a black-box perspective: that is, a perspective from which the internal workings are unknown. For instance, certain arithmetic operations known as pseudorandom number generators produce sequences of numbers that are completely predictable. However, these sequences do not have any recognizable patterns and thus, from the perspective of someone who does not know how the numbers have been generated, they cannot easily be distinguished from sequences obtained by truly random methods.

It would therefore seem that security can be established only if the random-number generator satisfies two conditions. First, the user must know how the numbers have been generated to verify that a valid procedure is being implemented. And second, the system must be a black box from the adversary's perspective to prevent them from exploiting knowledge about its internal mechanism.

However, the first condition is unrealistic. A random-number generator can deviate from its intended design because of imperfections, component ageing, accidental failures or explicit tampering by an adversary, leading to undetected biases. And monitoring the internal mechanism of a random-number generator in real time is both impractical and difficult[3]. Moreover, the second condition violates Kerckhoffs's principle — a central tenet of modern cryptography that was reformulated by the father of information theory, Claude Shannon[4], as "the enemy knows the system being used". In other words, cryptographic systems should be designed under the assumption that an adversary will quickly gain familiarity with them.

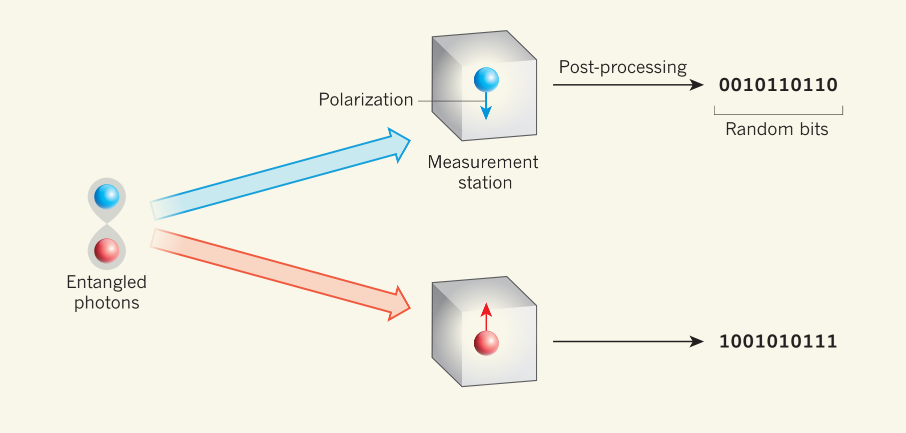

Figure 1 | A quantum random-number generator. Bierhorst *et al.*[2] report an experiment that produces strings of truly random bits (0s and 1s), which are desirable for improving the security of a wide range of communication systems. The authors prepared a pair of photons (blue and red) that were entangled, meaning that their properties were strongly correlated. They then sent each photon to a different remote measurement station, where the photons' polarizations were recorded. The measurement outcomes from the two stations were unpredictable, thanks to the strong correlated behaviour and large separation of the photons. However, the randomness was small, even after millions of runs. The authors used a powerful post-processing technique to generate truly random bits from these measurements, with minimal physical assumptions about the photons' behaviour.

Remarkably, thanks to the unusual laws of quantum physics, it is possible to create a provably secure random-number generator for which the user has no knowledge about the internal generation mechanism, whereas the adversary has a fully detailed description of it.

To understand how this works, consider the experiment carried out by Bierhorst and colleagues (Fig. 1). The authors prepared two photons in a peculiar quantum condition known as an entangled state. They then sent each photon to a different remote measurement station, where the photons' polarizations were recorded. During measurement, the photons were unable to interact with each other — the stations were so distant that this would require signals travelling faster than the speed of light. Nevertheless, the measurement outcomes were strongly correlated because of the photons' entangled nature. Such correlations can be detected experimentally through statistical criteria known as violations of Bell inequalities[5].

The strong correlated behaviour of the two remote photons suggests that they could be used to devise a faster-than-light communication device. This would indeed be possible unless the photons' measurement outcomes were unpredictable, in which case any attempt to use such photons in a communication device would fail, because it would result in scrambled, indecipherable messages. Because faster-than-light communication is impossible, it follows that violations of Bell inequalities imply random measurement outcomes. That is, the violations provide an experimental signature of randomness.

This conclusion depends only on the impossibility of faster-than-light signalling and not on any detailed description of the associated quantum systems. It must therefore be true from an adversary's perspective, regardless of their particular knowledge of the quantum processes being carried out. And because violations of Bell inequalities can be verified by a user only from the statistics of the observed outputs of such processes, the verification procedure represents a black-box test of randomness.

Violations of Bell inequalities have been observed in numerous experiments over the past three decades[5], and their qualitative connection to randomness has been known for many years. However, quantum-information researchers have started to develop the tools to exploit this connection only in the past few years[6].

A key difficulty has been that most experiments that violate Bell inequalities are affected by loopholes, meaning that they cannot be considered as black-box demonstrations. For instance, the constraint that the two photons cannot exchange signals at subluminal speeds was not strictly enforced in the two previous demonstrations of randomness generation based on Bell inequalities[7,8]. In the past few years, loophole-free experiments have been carried out[9–11], but they remain a technological challenge. In particular, the magnitude of the Bell-inequality violations observed in these experiments, although sufficient to confirm the correlated behaviour of the photons, was too low to verify the presence of randomness of sufficient quality for cryptographic purposes.

Bierhorst and co-workers have improved existing loophole-free experimental set-ups to the point at which the realization of such randomness becomes possible. However, this threshold is barely reached. Every time a photon is measured in the authors' experiment, the randomness that is generated (expressed as bits; 0s and 1s) is equivalent to tossing a coin that has 99.98% probability of landing on heads.

Over many runs, the sequence of measurement outcomes should have accumulated enough uncertainty that truly random bits could be extracted through clever post-processing. However, no existing methods for analysing such sequences would have been efficient enough to reach this goal. Bierhorst *et al.* therefore introduced a powerful statistical technique, tailored to the weak Bell-inequality violations they observed, that achieved this aim. Ultimately, the authors were able to generate 1,024 random bits in about 10 minutes of data acquisition — corresponding to the measurement of 55 million photon pairs.

Bierhorst and co-workers' random-number generator represents the most meticulous and secure method for producing randomness that has ever been demonstrated. However, its generation rate is much lower than in more-conventional commercial quantum random-number generators, which can produce millions of random bits per second[12]. Nevertheless, improvements in the generation rate can reasonably be expected to the point at which this will no longer be a strong limiting factor.

More problematic is the size of the authors' random-number generator: it is comprised of measurement stations that are 187 metres apart to prevent subluminal signalling between the photon pairs. This distance might be reduced in the future, but it is hard to imagine how it could reach the dimensions of more-standard electronic hardware (at most, a few centimetres) using foreseeable technology.

Although Bierhorst and colleagues' study will therefore not directly lead to practical, consumer-grade random-number generators, it sets a new direction and ideal for the secure production of random bits. The authors' approach and theoretical methods could be adapted to much more practical and simple designs for random-number generators that potentially retain many of the conceptual and security benefits of their work. ■

Stefano Pironio *is in the Quantum Information Laboratory, Université libre de Bruxelles, 1050 Brussels, Belgium.*
e-mail: stefano.pironio@ulb.ac.be

1. Heninger, N., Durumeric, Z., Wustrow, E. & Halderman, J. A. *Proc. 21st USENIX Security Symp.* 205–220 (USENIX, 2012).
2. Bierhorst, P. *et al. Nature* **556**, 223–226 (2018).
3. Becker, G. T., Regazzoni, F., Paar, C. & Burleson, W. P. in *Cryptographic Hardware and Embedded Systems – CHES 2013* 197–214 (Springer, 2013).
4. Shannon, C. E. *Bell Syst. Tech. J.* **28**, 656–715 (1949).
5. Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. *Rev. Mod. Phys.* **86**, 419–478 (2014).
6. Acín, A. & Masanes, L. *Nature* **540**, 213–219 (2016).
7. Pironio, S. *et al. Nature* **464**, 1021–1024 (2010).
8. Liu, Y. *et al. Phys. Rev. Lett.* **120**, 010503 (2018).
9. Hensen, B. *et al. Nature* **526**, 682–686 (2015).
10. Giustina, M. *et al. Phys. Rev. Lett.* **115**, 250401 (2015).
11. Shalm, L. K. *et al. Phys. Rev. Lett.* **115**, 250402 (2015).
12. Herrero-Collantes, M. & Garcia-Escartin, J. C. *Rev. Mod. Phys.* **89**, 015004 (2017).

OPTICAL PHYSICS

Mirrors made of a single atomic layer

Researchers have demonstrated that atomically thin materials can be highly reflective, contrary to general thinking. This finding could have technological implications for nanophotonics, optoelectronics and quantum optics.

KIN FAI MAK & JIE SHAN

The discovery of a single layer of carbon atoms, known as graphene[1], led to great interest in 2D materials. Whereas graphene is highly transparent to visible light[2], 2D materials that are highly reflective could be used as lightweight mirrors in optical or optoelectronic systems. The existence of such materials has been questioned, but, writing in *Physical Review Letters*, Back *et al.*[3] and Scuri *et al.*[4] report that single layers of molybdenum diselenide can have high levels of reflectance.

The importance of the authors' work can be understood by considering the reflection of light from a homogeneous, free-standing thin film of material. When a wave of light of a particular colour — or, equivalently, frequency — hits the film, the oscillating electric field that is associated with the light wiggles the charged particles in the material. This drives the oscillation of electric dipoles (separations between positively and negatively charged particles) at the same frequency as that of the incident light (Fig. 1a).

The oscillating dipoles re-radiate light waves in both the forward and backward directions with respect to the direction of the incident wave. Whereas the latter occurrence gives rise to reflection, the former destructively interferes with the incident wave, producing transmitted light that has a lower intensity than that of the incident light. The material's response to an oscillating electric field is, in general, not uniform with respect to incident waves from across the electromagnetic spectrum. At a particular frequency, the dipoles have a large oscillation amplitude — a phenomenon known as resonance — which results in more reflection and less transmission of light than at any other frequency.

Like all oscillators in real physical systems, the oscillations of the dipoles are damped, which means that they die out if the event that drives them is stopped. There are two ways in which the energy that is stored in the dipoles can be lost: it can be re-radiated (as discussed previously) or it can be absorbed by the material and converted into heat. These processes are known as radiative and non-radiative damping, respectively. In most materials, both mechanisms of damping operate. The incident light is therefore partly reflected, partly absorbed and partly transmitted.

However, in a material in which radiative damping dominates, the absorption losses would be negligible, and all of the incident electromagnetic energy would be re-radiated. Furthermore, the re-radiation in the forward direction would perfectly cancel out the incident light, through destructive