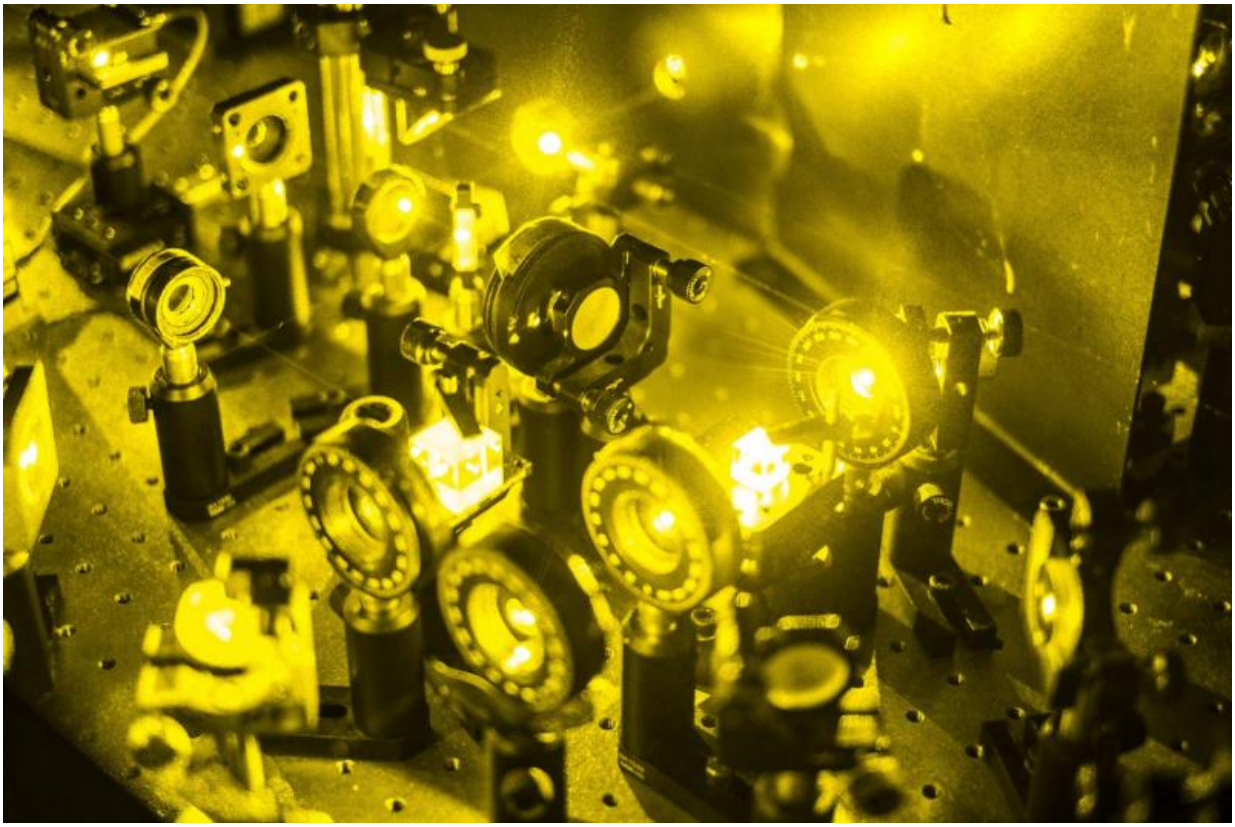
Random numbers—hard times ahead for hackers

May 31 2017



Researchers can generate perfectly random numbers by using the quantum properties of light. Credit: Thomas Le Provost

Whenever we need to communicate in secret, a cryptographic key is needed. For this key to work, it must consist of numbers chosen at

random without any structure – just the opposite of using the birthdate of our favourite pet. But, for a human, it is extremely difficult to choose without creating any bias, even by hitting the keyboard chaotically. To solve this problem, researchers from the University of Geneva (UNIGE), Switzerland, have developed a new random numbers generator based on the principles of quantum physics. This physical theory, full of phenomena that run counter to our common sense, shows that certain physical events occur perfectly at random, making them impossible to predict. Unlike previous methods, the new system allows the user to verify the reliability of the random numbers it generates in real time. This work, to appear in the scientific journal *Physical Review Applied*, will greatly complicate the tasks of hackers who can no longer exploit bias resulting from human fallibility or possible imperfections in existing devices.

To generate a good cryptographic key, one must alternate randomly between 0's and 1's, the values of the so-called bits which form the basic unit of information in digital devices like computers. However, when we humans try to generate a sequence of numbers which we believe to be random, it always ends up being partly predictable, as revealed by behavioural studies and statistics. In addition, apart from having a poor grasp on randomness, the human brain is also much slower than machines, which can output millions of numbers per second. This gives hackers an opportunity to crack passwords, which the user thought to be safe.

Quantum physics as key to security

For the past twenty years, researchers have turned to quantum physics, characterised by its completely random and unpredictable processes, for developing new cryptographic techniques, and in particular the generation of random numbers. "Send a photon (a particle of light) onto a semi-transparent mirror. Either it gets transmitted through the mirror,

or it gets reflected. But it is impossible, even in principle, to predict beforehand which of these two behaviours it will adopt. This is the basic idea behind quantum random number generation" explains Nicolas Brunner, professor at the Department of Applied Physics at the Faculty of Science of UNIGE and responsible for the theoretical aspects of the new research. Powerful quantum random number generators are today available commercially. However, one limitation of existing devices is that it is impossible for the user to independently verify that the numbers generated are in fact genuinely random and not, for example, composed of digits of π. The user must trust the device (and so its manufacturer) to function correctly, even after years of use. So, it makes sense to ask if current systems could be improved from this point of view.

A new self-testing random number generators

"We wanted to create a device which can be continuously tested to ensure it functions correctly at all times and thus guarantee that the random numbers generated are reliable" says Nicolas Brunner. To achieve this, the UNIGE physicists have developed a "self-testing" quantum random number generator, which allows the user to verify in real time that the apparatus performs optimally and delivers unbiased random numbers. "The generator should solve a tasks for which we have calibrated it. If the tasks is solved correctly, the output numbers are guaranteed to be random. If the apparatus does not find the correct solution, randomness is not guaranteed, and the user should then recalibrate the device. This avoids the risk of using numbers with little (or no) randomness for example to generate passwords, which hacker could then crack" professor Hugo Zbinden enthusiastically points out. He has been responsible for the experimental aspects of the research. Indeed, the new generator allows to measure precisely the quality of the output random numbers. Perfectly random numbers can then be distilled and used for security applications, such as generating passwords which are safe against hacking.

The self-testing quantum random number generator will allow the security of passwords and cryptographic protocols to be increased yet another notch. Here, security is guaranteed by the laws of physics themselves, and not by the hackers' technological limitations. This research, conducted by physicists at the UNIGE allows for a better understanding of quantum randomness as well as its use in information technology.

More information: Jonatan Bohr Brask et al. Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination, *Physical Review Applied* (2017). DOI: 10.1103/PhysRevApplied.7.054018

Provided by University of Geneva