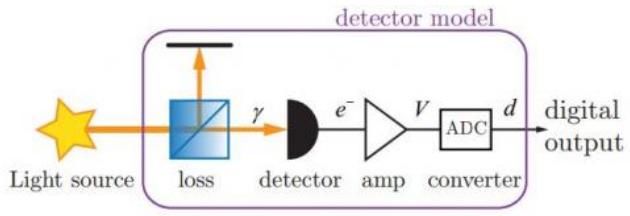
Geneva scientists focus on phone cameras for random number generation

18 May 2014, by Nancy Owano



A detector, or indeed each pixel of an image sensor, can be modelled as having 100% efficiency, but being preceded by a lossy element (beamsplitter) with transmission. For each absorbed photon, the detector generates an electron. This charge is then converted into a voltage and amplified, before being digitised and sent to further processing, i.e. a randomness extraction stage. Credit: arXiv:1405.0435 [quant-ph]

A paper submitted on May 2 to *arXiv* begins its discussion by noting that quantum random number generators (QRNGs) can improve the security of cryptographic protocols by ensuring that generated keys cannot be predicted, The paper is the work of four scientists from the Group of Applied Physics at the University of Geneva. Bruno Sanguinetti, Anthony Martin, Hugo Zbinden and Nicolas Gisin have shown how random numbers can be extracted from an illuminated image sensor. This is a big deal, because with their approach the quest for truly random numbers does not have to be such a big deal. They wrote that "the cost, size, and power requirements of current QRNGs has prevented them from becoming widespread. In the meantime, the quality of the cameras integrated in mobile telephones has improved significantly, so that now they are sensitive to light at the few-photon level. We demonstrate how these can be used to generate random numbers of a quantum origin."

Today, cameras are integrated in many common devices such as cell phones, tablets and laptops.

In turn, could this show of working out how to generate random numbers on a smartphone using quantum processes have an impact on information security? In their paper, "Quantum random number generation on a mobile phone," the authors wrote, "We believe that the simplicity and performance of this device will make the widespread use of quantum random numbers a reality, with an important impact on information security."

Fundamentally, their work will attract interest because they managed to create a QRNG using low-cost electronic components. Co-author Bruno Sanguinetti, senior researcher, University of Geneva, told *Physics World* that all of the components of his team's QRNG could be integrated on a chip that would cost a few dollars and could be easily integrated in portable electronic devices, including mobile phones. The key actor here is the mobile-phone camera.

Why was the camera so valuable for this experiment?

Said *The Verge*: "Cellphone cameras could offer a clean way to fix the problem. The solution focuses on camera noise, the pixely haze that appears when you try to take a cellphone picture in low light."

Physics World explained: "The system exploits the fact that the camera is so sensitive that it can be used to count the number of photons that impinge on each of its individual pixels. The light is supplied by a conventional LED, in which electrons and holes combine to create photons. This is a quantum mechanical process and therefore the number of photons produced in a fixed period of time is not fixed, but is random. The camera and LED are adjusted so that each pixel detects about 400 photons in a short exposure time. The photon numbers of all the camera pixels are combined in an 'extractor' algorithm that outputs a sequence of random numbers. The scientists used an eight-

megapixel camera from a Nokia N9 to create a device capable of delivering random numbers at 1.25 Gbit/s.

Writing in the results and tests section of their experiment, they said, "We collected 48 frames corresponding to approximately 5 Gbits of raw random numbers and processed them on a computer through an extractor with a 2000 bit input vector and a 500 bit output vector to generate 1.25 Gbits of random numbers."

More information: Quantum random number generation on a mobile phone, arXiv:1405.0435 [quant-ph] arxiv.org/abs/1405.0435

Abstract
Quantum random number generators (QRNGs) can significantly improve the security of cryptographic protocols, by ensuring that generated keys cannot be predicted. However, the cost, size, and power requirements of current QRNGs has prevented them from becoming widespread. In the meantime, the quality of the cameras integrated in mobile telephones has improved significantly, so that now they are sensitive to light at the few-photon level. We demonstrate how these can be used to generate random numbers of a quantum origin.

APA citation: Geneva scientists focus on phone cameras for random number generation (2014, May 18) retrieved 23 October 2019 from https://techxplore.com/news/2014-05-geneva-scientists-focus-cameras-random.html