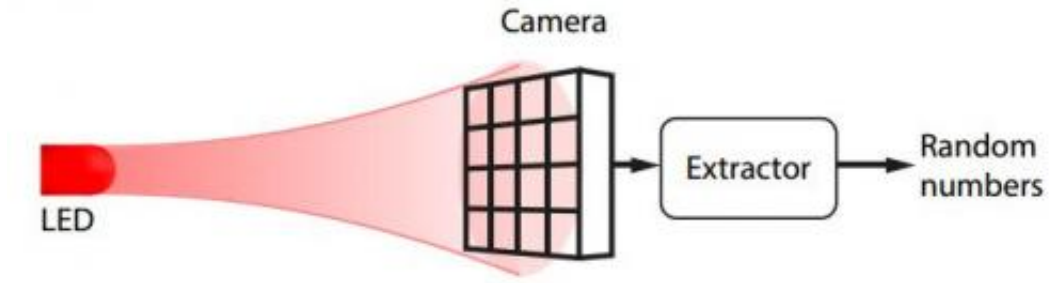
Physics team uses pixel sensitivity of smartphone as a random generator for encryption

September 18 2014, by Bob Yirka



Random number generator setup: a camera is fully and homogeneously illuminated by a LED. The raw binary representation of pixel values are concatenated and passed through a randomness extractor. This extractor outputs quantum random numbers. Credit: arXiv:1405.0435 [quant-ph]

(Phys.org) —A team of physicists led by Bruno Sanguinetti of the University of Geneva has found a way to use an ordinary smartphone as a true random number generator to provide secure communications. In their paper uploaded to the *arXiv* preprint server (soon to be published in *Physical Review X*), the team describes how they used the photon sensitivity of a Nokia N9 smartphone camera lens to generate truly random numbers that could be used in encryption schemes.

Modern encryption schemes rely on random numbers—long strings of them are generated to conceal sensitive information such as credit card or pin numbers, passwords, etc. The problem with doing it this way is that computers, because of their step-by-step processing processes, are not very good at generating random numbers. In fact, they can only approximate them. Because of that, those looking to subvert an encryption scheme, first look to see if they can access the random number generator used by a computer or smartphone—that can lead to subverting the entire scheme. To get around this problem, scientists have been looking to the natural world for a way to convert random happenings into random numbers that can be used for encryption. In this latest effort, the researchers turned to the quantum world—the part that deals with atoms emitting light—theory says that it's impossible to predict when an atom will emit a particle of light, which looked at another way means that it's impossible to predict how many such particles will be emitted over a given time. It's this property that the researchers sought to use as a random generator.

They started with a Nokia N9, because it was the only smartphone they could find that had open source software that could be used to monitor the light from a laser striking the phone's camera lens. Each pixel in the camera is sensitive enough that it can detect how many photons strike it—and since they come in random fashion, all that was needed was software to convert the rate to a constant stream (1.25 billion bps) of truly random numbers.

After extensive testing the team reports that the randomness of the generator is such that it would have to run 10^{96} times before any deviation from a perfectly random string of bits would be seen. They note also that it would be relatively easy to design such a random generator into virtually any smartphone.

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.