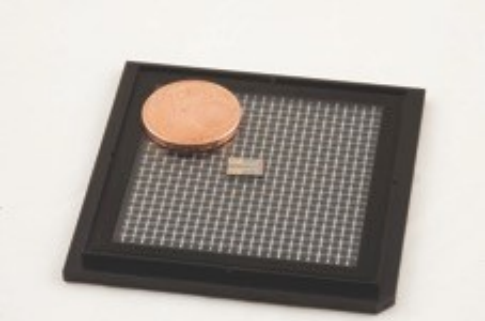
New chip could bring highest level of encryption to any mobile device

September 8 2016



Using photonic integrated circuit technology, researchers made a tiny, yet fast quantum random number generator. The small chip in the middle of the picture contains two of the random number generators, which together measure 6 by 2 millimeters. For comparison, the coin is 16.25 millimeters in diameter. Credit: Daniel Bartolome & Ona Bombí, ICFO

Random number generators are crucial to the encryption that protects our privacy and security when engaging in digital transactions such as buying products online or withdrawing cash from an ATM. For the first time, engineers have developed a fast random number generator based on a quantum mechanical process that could deliver the world's most secure encryption keys in a package tiny enough to use in a mobile device.

In The Optical Society's journal for high impact research, *Optica*, the researchers report on their fully integrated device for random number

generation. The new work represents a key advancement on the path to incorporating quantum-based random number generators—delivering the highest quality numbers and thus the highest level of security—into computers, tablets and mobile phones.

"We've managed to put quantum-based technology that has been used in high profile science experiments into a package that might allow it to be used commercially," said the paper's first author, Carlos Abellan, a doctoral student at ICFO-The Institute of Photonic Sciences, a member of the Barcelona Institute of Science and Technology, Spain. "This is likely just one example of quantum technologies that will soon be available for use in real commercial products. It is a big step forward as far as integration is concerned."

The new device operates at speeds in the range of gigabits per second, fast enough for real-time encryption of communication data, such as a phone or video calls, or for encrypting large amounts of data traveling to and from a server like that used by a social media platform. It could also find use in stock market predictions and complex scientific simulations of random processes, such as biological interactions or nuclear reactions.

Shrinking the truly random

The random number generators used today are based on computer algorithms or the randomness of physical processes—essentially complex versions of rolling dice over and over again to get random numbers. Although the numbers generated appear to be random, knowing certain information, such as how many "dice" are being used, can allow hackers to sometimes figure out the numbers, leaving secured data vulnerable to hacking.

The new device, however, generates random numbers based on the quantum properties of light, a process that is inherently random and thus

impossible to predict no matter how much information is known. Although other researchers have developed quantum random number generators, they have all been either larger or slower than the device reported in the *Optica* paper.

"We have previously shown that the quantum processes taking place exhibit true randomness," said Valerio Pruneri, who led the collaborative research effort. "In this new paper, we made a huge technological advance by using a new design that includes two lasers that interfere with each other in a confined space. This makes the device smaller while keeping the same properties that were used in the past experiments."

Creating a practical device

The researchers used photonic integrated circuit (PIC) technology to create two quantum number generators that together measure 6 by 2 millimeters. PIC technology offers a way to integrate photonic components—such as the lasers and detectors used by the new quantum random generator—onto a chip with a small footprint and low power consumption. Most importantly, PIC-based devices can be integrated with traditional electronics, which could allow the random number generator to be used with the driving, reading and processing electronics necessary for computation or communications.

"We proved that quantum technologies are within practical reach by exploiting PICs," said Pruneri. "Quantum random number generation as well as quantum cryptography and other quantum-based technologies will benefit from PIC-based technology because it allows one to build commercial and innovative products. Ours is a first demonstration."

This work was a multi-institutional effort that included researchers from ICFO-The Institute of Photonic Sciences, VLC Photonics S.L., Universitat Politècnica de Valencia, ICREA- Institució Catalana de

Recerca i Estudis Avancats, all in Spain, as well as Politecnico di Milano in Italy.

More information: C. Abellan, W. Amaya, D. Domenech, P. Muñoz, J. Capmany, S. Longhi, M.W. Mitchell, V. Pruneri. "A quantum entropy source on an InP photonic integrated circuit for random number generation," *Optica*, 3, 9, 989 (2016). DOI: 10.1364/OPTICA.000989

Provided by Optical Society of America