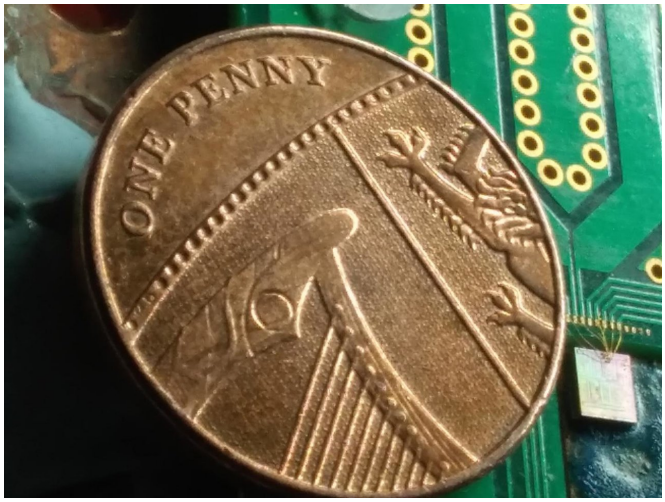
Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-in

24 July 2018



Researchers created a chip-based device measuring a millimeter square that can potentially generate quantum-based random numbers at gigabit per second speeds. The small square to the right of the penny contains all the optical components of the random number generator. Credit: Francesco Raffaelli, University of Bristol

Researchers have shown that a chip-based device measuring a millimeter square could be used to generate quantum-based random numbers at gigabit per second speeds. The tiny device requires little power and could enable stand-alone random number generators or be incorporated into laptops and smart phones to offer real-time encryption.

"While part of the control electronics is not integrated yet, the device we designed integrates all the required optical components on one chip," said first author Francesco Raffaelli, University of Bristol, United Kingdom. "Using this device by itself or integrating it into other portable devices would be very useful in the future to make our information more secure and to better protect our privacy."

Random number generators are used to encrypt data transmitted during digital transactions such as buying products online or sending a secure e-mail. Today's random number generators are based on computer algorithms, which can leave data vulnerable if hackers figure out the algorithm used.

In The Optical Society (OSA) journal *Optics Express*, the researchers report a quantum random number generator based on randomly emitted photons from a diode laser. Because the photon emission is inherently random, it is impossible to predict the numbers that will be generated.

"Compared to other integrated quantum random number generators demonstrated recently, ours can accomplish very high generation rates with relatively low optical powers," said Raffaelli. "Using less power to produce random numbers helps avoid problems such as excess heat on the chip."

Silicon photonics

The new chip was enabled by developments in silicon photonics technology, which uses the same semiconductor fabrication techniques used to make computer chips to fabricate optical components in silicon. It is now possible to fabricate waveguides into silicon that can guide light through the chip without losing the light energy along the way. These waveguides can be integrated onto a chip with electronics and integrated detectors that operate at very high speeds to convert the light signals into information.

The new chip-based random number generator takes advantage of the fact that under certain conditions a laser will emit photons randomly. The

device converts these photons into optical power using a tiny device called an interferometer. Very small photodetectors integrated into the same chip then detect the optical power and convert it into a voltage that can be turned into random numbers.

"Despite the advancements in silicon photonics, there is still light lost inside the chip, which leads to very little light reaching the detectors," said Raffaelli. "This required us to optimize all the parameters very precisely and design low noise electronics to detect the optical signal inside the chip."

The new chip-based device not only brings portability advantages but is also more stable than the same device made using bulk optics. This is because interferometers are very sensitive to environmental conditions such as temperature and it is easier to control the temperature of a small chip. It is also far easier to precisely reproduce thousands of identical chips using semiconductor fabrication, whereas reproducing the necessary precision with bulk optics is more difficult.

Testing the chip

To experimentally test their design, the researchers had a foundry fabricate the random number generator chip. After characterizing the optical and electronic performance, they used it for random number generation. They estimate a potential randomness generation rate of nearly 2.8 gigabits per second for their device, which would be fast enough to enable real-time encryption.

"We demonstrated random number generation using about a tenth of the power used in other chip-based quantum random number generator devices," said Raffaelli. "Our work shows the feasibility of this type of integrated platform."

Although the chip containing the optical components is only one millimeter square, the researchers used an external laser which provides the source of randomness and electronics and measurement tools that required an optical table. They are now working to create a portable device about the size of a mobile phone that contains both the chip and the necessary electronics.

More information: Francesco Raffaelli et al, Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip, *Optics Express* (2018). DOI: 10.1364/OE.26.019730

Provided by Optical Society of America

APA citation: Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-in (2018, July 24) retrieved 24 May 2019 from https://phys.org/news/2018-07-random-phase-fluctuations-laser-diode.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.