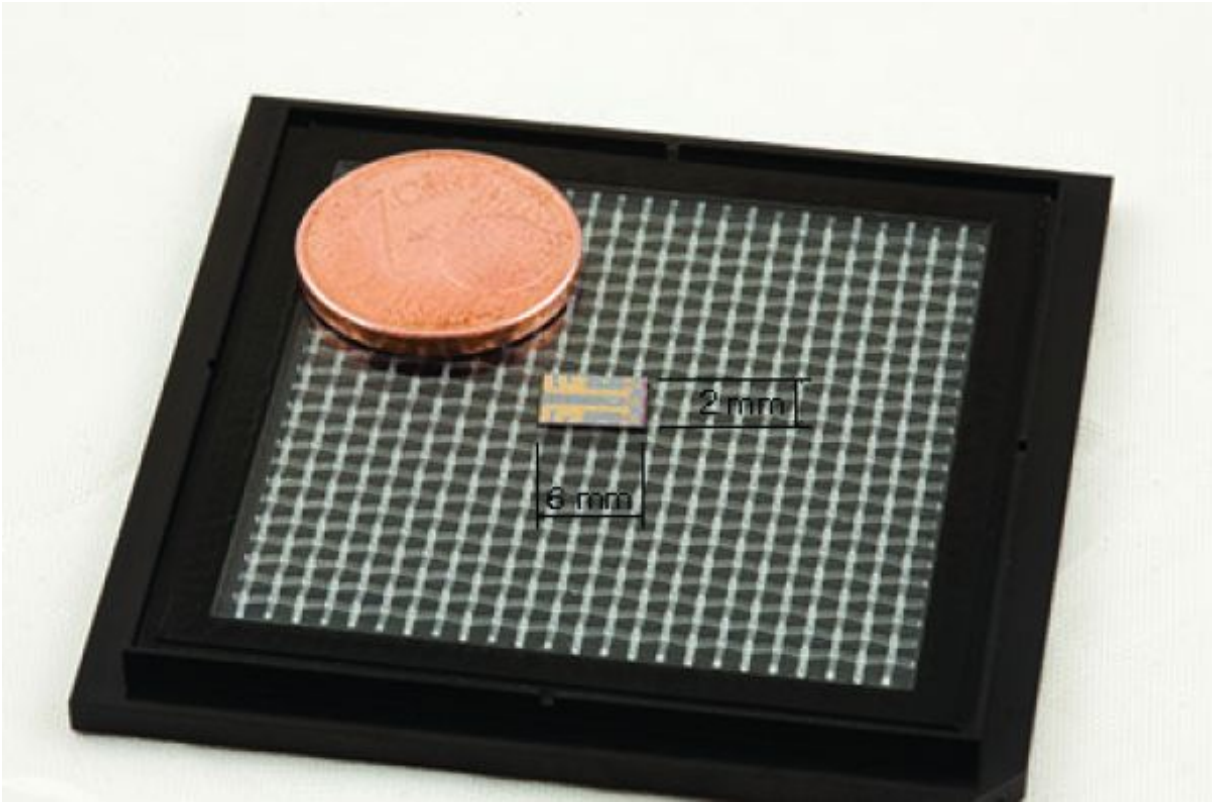

ICFO Quantum Random Number Generators go tiny and fast

ICFO publishes White Paper on the fastest and tiniest quantum random number generator so far, coinciding with the scientific paper published in Optica.

September 08, 2016

Most random number generators (RNGs) are based on computer algorithms known as pseudo-random number generators, which are fast but not truly random. A short string of bits from a pseudo-RNG appears random, but eventually the sequences repeat. Moreover, if you know the inner workings of the algorithm, you can predict the exact sequence. This is troubling in communications security, where random numbers are used to choose encryption keys. In contrast, quantum random number generators (QRNGs) extract randomness from quantum mechanical processes that are believed to be truly random and unpredictable.

In a study recently published in the journal Optica, ICFO researchers Carlos Abellan, Waldimar Amaya, led by ICREA Professors at ICFO Morgan Mitchell and Valerio Pruneri, in collaboration with David Domenech, Pascual Munoz, and Jose Capmany, from VLC and ITEAM and Stefano Longhi, from Politecnico di Milano, 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 parallel, ICFO has also published a White Paper on this device, putting forward the commercial applications that can highly benefit from this state-of-the-art technology.

In their work, the researchers used photonic integrated circuit (PIC) technology to create two quantum number generators integrated into a photonic chip that measures 6 by 2 millimeters in size. By using phase diffusion and two DFB lasers, the researchers were able to produce a train of pulses with nearly equal amplitudes and random phases. Then, with the help of an interferometer, they were able to interfere the pulses, generating random-amplitude pulses, which were subsequently detected and digitized to produce the high-rate random sequence of numbers.

This 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.

QRNGs have important implications for improvements not only in secure communications, cryptography, and quantum key distributions, among other applications. The results obtained in this study represent 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.