PRESS RELEASE

Photonic quantum chip for fast and reliable random number generation

The German Ministry for Research and Education BMBF is funding the CBQD project - chip-based quantum random device - for research into quantum-safe high-speed communications. In the CBQD project, a compact chip will be developed that generates random numbers at high speed based on quantum photonic effects. It meets the requirements of the Common Criteria for IT product security. The chip will become the basis for numerous IT security applications. Fraunhofer IPMS is responsible for coordination and QNRG chip integration in the project.

In IT security, random numbers are of enormous importance as they are used for cryptographic procedures such as key generation, thus ensuring the security of data in terms of confidentiality, integrity and authenticity. Quantum random number generators (QRNGs) use quantum mechanical phenomena such as the decay of atoms or photon phase noise from laser sources to generate unpredictable and random data, promising the highest possible security because the output values are based on the quantum mechanical principles of indeterminacy and superposition. They provide secure random number generation for future communication systems and can be used in various fields such as government, banking, critical infrastructure and the Internet of Things.

"In the project, we will develop a compact QRNG chip with a noise bit rate of 5 Gbit/s. The noise bit rate is a decisive factor for the speed in random number generation," explains Christoph Posenau, project manager at Fraunhofer IPMS. "The goal is to combine high speed with a compact design, while meeting the requirements of Common Criteria AIS 20/31 PTG.3, a standard for security requirements for IT products of the German Federal Office for Information Security (BSI)."

The project to implement the QRNG chip uses advanced silicon-germanium technologies to develop electrophotonic integrated circuits (EPIC) to create a fully integrated solution with laser source, waveguide structures, photodiodes and analog/digital signal processing. The QRNG solution will be tested in two Quantum Key Distribution (QKD) applications in the project. The interdisciplinary project team brings extensive expertise from quantum theory to security proofs, security-by-design experience for RNGs, silicon photonics to QKD systems and their integration in applications.

Fraunhofer IPMS will be working with four partners and one associated partners to develop the chip:

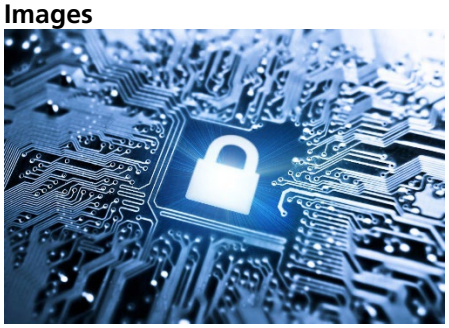
Editor
Franka Balvin | Fraunhofer Institute for Photonic Microsystems IPMS | +49 351 8823-1144 |
Maria-Reiche-Straße 2 | 01109 Dresden, Germany | www.ipms.fraunhofer.de | franka.balvin@ipms.fraunhofer.de

- Fraunhofer Institute for Applied Optics and Precision Engineering (IOF)
- Leibniz University Hannover (LUH)
- Leibniz Institute for High Performance Microelectronics (IHP)
- Technical University of Darmstadt (TUDa)
- Adva Network Security GmbH (assoziierter Partner)

About Fraunhofer IPMS

The **Fraunhofer Institute for Photonic Microsystems IPMS** researches microelectronic and micromechanical sensors, actuators, and active and passive waveguide elements. Wireless microsystems, high-speed FPGA and mixed-signal ASIC design are also part of the portfolio. The focus is on electronic control and evaluation of qubits and active photonic single elements up to computing accelerators via dedicated integrated electronics (CMOS, BJT, BiCMOS). In addition, new materials, processes and integration concepts for cryoelectronics as well as superconducting metallizations are being researched.

Images



The BMBF-funded project CBQD – Chip-Based Quantum Random Device – will develop a compact chip which generates random numbers at high speed on the basis of quantum-photonic effects. It meets the requirements of the Common Criteria for IT product security.