Contribution ID: **50** Type: **Talk**

A real-time QRNG-to-QKD stream exploiting FPGA for high security Quantum Communication

Thursday 4 May 2023 11:00 (30 minutes)

Most of the modern Quantum Key Distribution (QKD) and Quantum Random Number Generation (QRNG) systems require the usage of the Field Programmable Gate Array (FPGA) technology as it can guarantee the deterministic behavior necessary for dealing with qubit generation and readout. Nevertheless, the System-on-a-Chip (SoC) technology, which integrates both an FPGA and a CPU and allows for a very high level of flexibility, is not as common as the FPGA. Therefore, we exploited the SoC technology to realize a high performance QKD/QRNG system, implementing what we called "1-random-1-qubit"(QRN2Qubit) encoding. Such encoding grants a higher level of security, as each qubit is encoded with a unique random number. This is possible thanks to a real-time architecture that can continuously stream random data from a high speed QRNG (>300 Mbps) to a QKD transmitter (qubit repetition rate equal to 50 MHz) for BB84 protocol exploiting polarization degree of freedom of single photons. The system was tested for 55 hours and showed no interruptions and correctly delivered the data from the QRNG to the QKD transmitter. Most of the nowadays systems exploit a low-rate QRNG (few Mbit/s) and algorithm expansions to reach the required bitrate but with a major drawback in security as the transmitted qubit sequence is not fully random due to the expansion algorithms. Thus, this system offers a higher level of security for QKD thanks to the true randomness of the qubit sequence. This SoC-based system was used in real scenarios for demonstration of urban QKD networks as well in several QKD/QRNG experiments realized by the QuantumFuture research group. Recently, it was also integrated into the QKD systems provided by ThinkQuantum, a spin-off company from University of Padova.

Abstract category

Presenter: Dr STANCO, Andrea (Università di Padova)