A High-Speed QRNG for Security Applications

Mathilde Soucarros[1], Samuel Burri[2], Edoardo Charbon[3], Christopher Chunnilall[4], Daniela Frauchiger[5], Alessio Meneghetti[6], Jean-Benoît Page[1], Francesco Regazzoni[3], Renato Renner[5], Damien Stucki[1]

[1]ID Quantique, 1227 Carouge, Switzerland.
[2]EPFL, School of Engineering, 1015 Lausanne, Switzerland.
[3]Delft University of Technology, 2628 Delft, Netherlands.
[4]National Physical Laboratory (NPL), Teddington, TW11 0LW, UK.
[5]ETHZ, Institute for Theoretical Physics, 8093 Zurich, Switzerland.[6]University of Trento, Trento, Italy.

Random numbers are a fundamental building block for a number of applications such as cryptography, numerical simulations or the gaming industry. There are two types of random number generator: pseudo-random number generators and true random number generators. The first type is implemented to be deterministic: a specific input seed will always generate the same output sequence. The second type relies on classical or quantum physical processes. Random number generators based on classical physics are fundamentally deterministic – as is classical physics – even if the complexity of the system can hide the determinism. Random number generators based on quantum physics are true random number generators as quantum physical phenomena are intrinsically random. With this last type of generators, called QRNGs (Quantum Random Number Generators), we aim at providing users with a source of random numbers suitable for applications with the most stringent security standard. This means that it is not enough to rely on the quantum characteristic of the randomness source but it is also necessary to provide proofs of the "amount" of quantum randomness actually delivered by the device. This work is divided into three parts. The first one concerns the randomness source and its technical specifications. The second part covers metrology techniques applied to QRNGs for the creation of standard testing procedures. The last part deals with ways to ensure the quality of the numbers produced by the QRNG.

A simple design for a QRNG is based on a construction with a photon source, a 50/50 beam-splitter and two identical single photon detectors. This construction ensures a random and balanced probability of detection of the photon at each detector. However, a drawback is that it can only produce one raw bit at a time. In order to increase the bit rate of the QRNG, a new design has been considered. In this work, instead of using only two single photon detectors, we exploit the properties of matrices of single photon detectors. Whereas previously the randomness was restricted by the beam-splitter to two possible outcomes, it is now based on the fact that it cannot be predicted where a photon will collapse on the matrix of detectors. In this construction we use detectors with low dark-count rate, low after-pulsing probability and low cross-talk. In addition we use a spatially monomode source. This design was developed in the Swiss project NCCR-QP FastQ, with the goal of achieving a bit rate of 625 Mbits/s.

A thorough characterization of the performance of the components, and how they interact, is important for evaluating the randomness of the generated sequences.
The reliability of the QRNG can be obtained from the repeatability of the different measurements. In this work, which is part of the European project MIQC (Metrology for Industrial Quantum Communications) (http://www.miqc.org/), two QRNG designs are evaluated. One is composed of the simple design based on a photon source, a beam-splitter and two detectors. The other one is derived from our new construction and comprises a line of detectors. The aim of this project is to establish all important characteristics of these designs and define the optimal measurement techniques. To estimate the entropy, a model has been developed. The model takes account of the detection efficiencies, the

spatial distribution of the photons, and the probabilities of dark-counts, after-pulsing and cross-talk.

The last part of our work is oriented towards the use of our QRNG in security applications. More precisely, we want the device to conform to security standards. Indeed, even though the design of the QRNG is based on quantum theory, noise due to the practical realization of the device automatically reduces the quantum entropy that can be delivered. The aim of this Swiss project NCCR-QSIT CREx is to create an entropy extractor to remove classical noise and extract only quantum entropy. In order to do this, our QRNG is precisely modeled with all the potential sources of noise (dark-counts, after-pulses, cross-talk, etc.). The extractor is tailored so that we get the maximal entropy with a very small chance of deviating from it and with an output rate of 400 Mbits/s. A post-processor based on the information theory completes our final design. The implementation of these algorithms will be done on a FPGA, as well as the handling of the QRNG. Additional tests of the entropy or hardware failure shall also be inserted in the FPGA. This will be done to improve the security of the whole design and facilitate a certification of the device. The compliance of the device to security standards is thus realized at every step of this project.

Acknowledgments

The research leading to these results has received funding by Swiss NCCR-QP and NCCR-QSIT, and EMRP (project IND06-MIQC). The EMRP is jointly funded by the EMRP participating countries within EURAMET and the European Union.