8.9Gb/s real-time quantum random numbers with verified security

Arne Kordts[1], Dino Solar Nikolic[1], Cosmo Lupo[2], Tobias Gehring[1] and Ulrik L. Andersen[1]

[1]Department of Physics, Technical University of Denmark, Fysikvej, Kongens Lyngby 2800, Denmark
[2]York Centre for Quantum Technologies (YCQT), University of York, York YO10 5GH, United Kingdom

Quantum random number generators (QRNG) rely on the laws of quantum physics to produce genuine randomness. Access to proper random numbers is paramount for many applications, including both classical and quantum cryptographic protocols.

Here we present an implementation of a vacuum fluctuation based QRNG [1], where the vacuum noise is measured with a shot noise limited homodyne detector (see Fig. 1). The detector output was digitized and randomness extraction was performed in real-time. We achieved a speed of 8.9 Gbit/s, which is the fastest real-time implementation we are aware of to this date. A new fully quantum secure proof for the QRNG model is provided which takes into account finite-bandwidth effects of a realistic device. A metrological grade characterization of the detector completes the security verification.

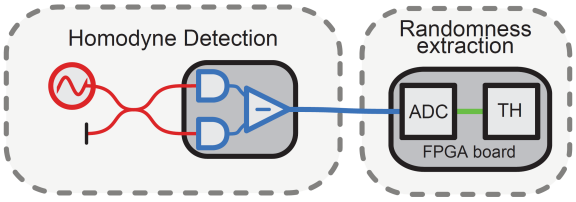

Figure 1: Vacuum fluctuation QRNG scheme. A homodyne measurement on the vacuum state is performed. The recorded noise spectrum is digitized. TH denotes Toeplitz hashing extraction performed in FPGA.

The security of random generators was, so far, mostly verified by running statistical tests on the output. While this approach can detect malfunctioning, it does not improve the security compared to classical RNG. The improved security of a device-dependent QRNG implementation is based on a precise characterization of the devices [2], which in turn needs to be in line with a proven quantum-mechanical QRNG model to verify the unpredictibility of the measured outcomes with respect to the probabilistic interpretations of quantum mechanics [3].

Here, the two approaches, quantum proof security analysis and metrological grade characterization, are combined to achieve security with respect to quantum side information. We model the homodyne detector as a linear time-independent (LTI) system, described by a transfer function and an independent additive noise spectrum. A quantum secure proof of the given model is provided with regard of the added noise and the introduced correlations. We independently characterized the effective LTI transfer function of the detector system in a classical regime as well as the electronic-noise spectrum. From the model, we calculated a min-entropy of 0.6 secure bits per measured bit and the security parameter was determined from the difference between the predicted shot-noise spectrum, based on the detector characterization, and the actual measured shot-noise spectrum.

Efficient and secure classical postprocessing provides the last step for making QRNG technology practical for a wide range of applications. Randomness extraction must not compromise previously analyzed and established security. Toeplitz hashing is a proven method for randomness extraction in both hardware and software implementations [4]. Toeplitz matrices are a universal family of hash functions. Therefore, according to the Leftover Hash Lemma, they can be used as a strong randomness extractor.

We implemented a Toeplitz extractor in a high performance Xilinx Kintex UltraScale FPGA chip. The homodyne detector output is sampled with a 16 bit ADC at 1GS/s and fed to the FPGA. All the sampled data is processed without discarding any bits.This was achieved using the inherent parallel processing feature of the chip and the right tradeoff of the clock frequency and the number of implemented logic elements. Matrix multiplication was done using the submatrix method where the submatrices are generated on every clock cycle [5]. Submatrices are small enough to fit efficiently into FPGA logic, while the full matrix is big enough to provide high extraction efficiency. Timing constraints within the chip are met using pipelining and area constraining. Matrix dimensions are chosen according to leftover hash lemma for particular min-entropy and predefined security parameter. In this experiment we were able to accomplish 8.9Gb/s true random numbers output.

High-rate QRNG implemetation are of great interest to commercial applications. A metrological grade approach, together with a quantum secure proof, gives a clear advantage over classical security verification schemes based on statistical tests.

[1] Gabriel, C., Wittmann, C., Sych, D., Dong, R., Mauerer, W., Andersen, U. L., Marquardt, C., Leuchs, G. (2010). A generator for unique quantum random numbers based on vacuum states. Nature Photonics, 4(10), 711715.

[2] Mitchell, M. W., Abellan, C., Amaya, W. (2015). Strong experimental guarantees in ultrafast quantum random number generation. Physical Review A - Atomic, Molecular, and Optical Physics, 91(1), 110.

[3] Frauchiger, D., Renner, R., Troyer, M. (2013). True randomness from realistic quantum devices. arXiv:1311.4547

[4] Krawczyk, H. (1994). LFSR-based Hashing and Authentication. In: Desmedt Y.G. (eds) Advances in Cryptology CRYPTO 94. CRYPTO 1994. Lecture Notes in Computer Science, vol 839. Springer, Berlin, Heidelberg

[5] Zhang, X., Nie, Y. Q., Liang, H. and Zhang, J. (2016). FPGA implementation of Toeplitz hashing extractor for real time post-processing of raw random numbers. 2016 IEEE-NPSS Real Time Conference (RT), Padua, pp. 1-5.