Quantum-Noise Based True Random Number Generation

Maurício J. Ferreira[1], Nuno A. Silva[1], Nelson J. Muga[1,2]

[1]*Instituto de Telecomunicações, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal*
[2]*Department of Physics, University of Aveiro, 3810-193 Aveiro, Portugal*
mauricioferreira@ua.pt

Abstract: A real-time quantum random number generator based on quadrature fluctuations of a vacuum state was implemented and validated, showing support for rates up to 8.23 Gbps. The scheme passes all state-of-the-art randomness evaluation tools. © 2022 The Author(s)

1. Introduction

Random numbers (RNs) are currently an essential resource in security-critical cryptographic applications. So far, pseudorandom number generators have been able to suppress this demand, but such methods yield inherently periodic sequences that become predictable to an adversary with access to enough computational power [1]. Quantum random number generators (QRNGs) address these questions by exploring the probabilistic nature of quantum measurements as their randomness source [2]. Here, we implement and validate a real-time QRNG based on homodyne measurements of the quadrature fluctuations in a vacuum state of the electromagnetic field.

2. Methods and Results

In the proposed scheme, a strong laser acts as the local oscillator (LO) and interacts with a vacuum state in a balanced beam splitter. Its purity can be guaranteed, at room temperature, by simply blocking one of the input ports [2]. The output signals are posteriorly measured by a balanced detector and the resulting photocurrents are subtracted. Thus, a signal proportional to the amplitude quadrature of the probed state is obtained, which follows a Gaussian distribution [1]. Unfortunately, measurements also contain classical contributions such as electronic noise. Consequently, a randomness extraction (RE) algorithm based on Toeplitz-hashing is applied to suppress them [2].

As seen in Fig.1a, a preponderance of quantum noise was obtained, with an observed quantum-to-classical noise ratio of approximately 11.7 dB, neglecting any LO excess noise. Moreover, we verify that all noise follows the expected null-mean Gaussian distribution. In these conditions, approximately 8.39 random bits per sample can be obtained, supporting generation rates up to 8.23 Gbps. Unfortunately, the real-time RE algorithm limits this to an effective throughput of 75 Mbps. Nonetheless, as seen in Fig.1b, the RE is effective in removing any low-order correlations present in the raw sequence, and true RNs are extracted with upper security bound of 2^{-105}, illustrating the quality of this scheme. Finally, the QRNG was validated and verified to pass all the statistical tests of the NIST, DieHarder, and TestU01's *SmallCrush* batteries, as well as most of TestU01's *Crush* evaluations.

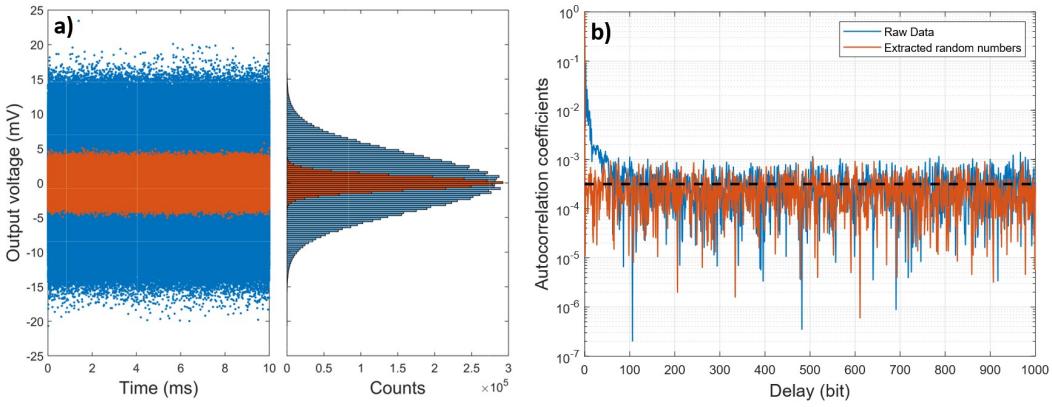

Fig. 1. (a) Distribution of the total (blue) and electronic (orange) noise. (b) Autocorrelation coefficients of the measured noise. Dashed line represents the theoretical standard deviation for the autocorrelation function.

Acknowledgements: This work is supported by FCT/MEC through national funds under the project QuantumPrime (PTDC/EEI-TEL/8017/2020), and by FCT/MCTES through national funds and when applicable co-funded EU funds under the projects UIDB/50008/2020 and UIDP/50008/2020 (actions QuRUNNER, and DigCORE).

3. References

[1] M. Herrero-Collantes et al., "Quantum random number generators," APS **89**, 015004 (2017).
[2] M. J. Ferreira et al, "Characterization of a Quantum Random Number Generator Based on Vacuum Fluctuations," Appl **11,** 7413 (2021).