QUANTUM COMMUNICATION NETWORKS WORKSHOP

PTQCI PORTUGUESE QUANTUM COMMUNICATION INFRASTRUCTURE

instituto de telecomunicações

IQC quantum communications

Prime Number Generation Based on Quantum Noise

Maurício J. Ferreira[1,2,*], Nuno A. Silva[1], Armando N. Pinto[1,2], Nelson J. Muga[1]

[1]Instituto de Telecomunicações, Universidade de Aveiro, Campos Universitário de Santiago, 3810-193 Aveiro, Portugal;

[2]Departamento de Eletrónica, Telecomunicações e Informática, Universidade de Aveiro, Campos Universitário de Santiago, 3810-193 Aveiro, Portugal;

***mauricioferreira@ua.pt**

Abstract

Quantum Random Number Generators (QRNGs) based on quadrature fluctuations of the optical vacuum state are cost-effective devices able to yield information-theoretic security at high generation rates. However, the use of a Quantum Source (QS) to generate random prime numbers, which are necessary for asymmetric cryptographic protocols such as RSA, has not yet been explored. In this poster, we comparatively analyze such a probabilistic prime number generator against one exploring a purely classical noise source (CS).

A Vacuum-based QRNG

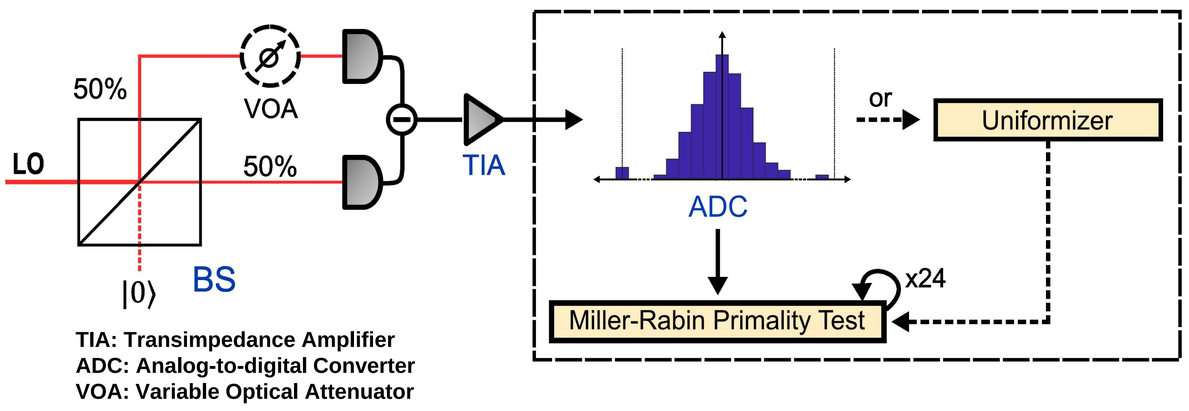

Figure 1. Schematic representation of the vacuum-based QRNG and postprocessing algorithm.

A homodyne detection (HD) scheme amplifies the quadrature fluctuations of the optical vacuum field through its interaction with a strong local oscillator (LO) in a balanced beamsplitter (BS) (Fig. 1). The BS condition is further adjusted by a VOA. Then, the resulting output beams are detected, and the respective photocurrents are subtracted. The normally-distributed output signal thus contains a mixture of contributions from the QS and CSs such as electronic noise. To obtain the latter component, the LO is simply removed.

To compare the performance of the CS and QS, the biased output measurements are additionally mapped into uniform distributions by an equiprobable binning algorithm. The resulting candidate numbers (CNs) are passed through 24 iterations of a Miller-Rabin primality test, yielding an expected error probability of 3.5×10^{-15}.

We found that the overall number of primes generated does not depend on the noise source considered (Fig. 2). However, the QS outperforms the classical scheme at small prime number generation (Fig. 3), increasing prime diversity by an order of magnitude. This difference remains even for the uniformized sources, ruling out CN distribution bias as an explanation.

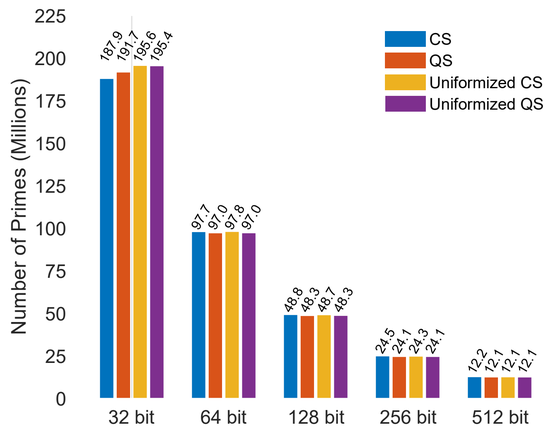

Figure 2. Total number of primes found for increasing lengths of candidate numbers in a 1 GB dataset. Solid line represents the expected lower bound.

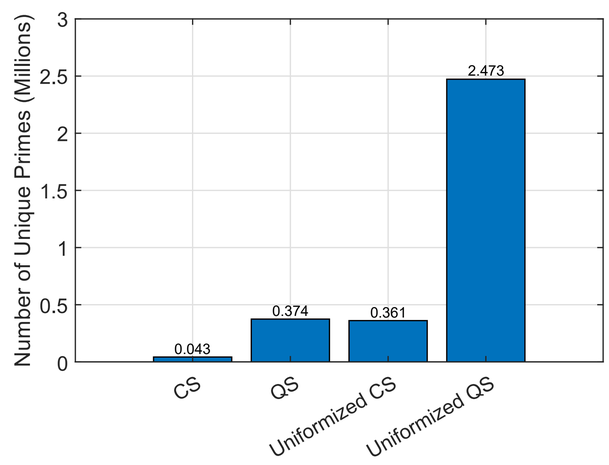

Figure 3. Number of unique 32-bit prime numbers found for each of the randomness source considered. Values were evaluated for 10 M prime numbers.

Statistical Validation

Traditional statistical test suites (STSs) cannot validate prime number sequences as they certify randomness by seeking deviations from a uniform distribution. However, it is possible to bound the proportion of numbers below a certain threshold by using the known bounds of the prime-counting function. When applying an equiprobable binning, an unbiased scheme thus yields uniformly distributed binary sequences. Regardless of prime length, these sequences can then be submitted to an STS.

This analysis revealed the underlying correlations in the prime output of both sources (Fig. 4), which remain present in the CNs due to the absence of a randomness extraction layer. This step would suppress the highly-correlated contributions from the CS. Finally, the prime sequences were additionally submitted to the NIST STS, where the QS and CS passed, respectively, 86.96% and 45.34% of the evaluations applied.

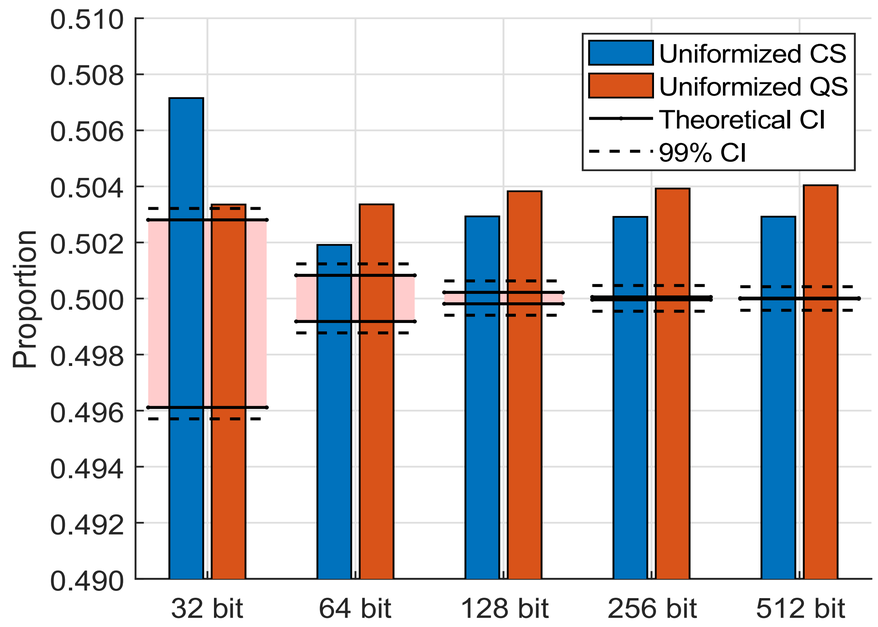

Figure 4. Proportion of 10 M primes below the threshold. Full lines are the theoretical interval. Dashed lines are its 99% confidence interval (CI).

References

Ferreira, Maurício J., et al. "Statistical Validation of a Physical Prime Random Number Generator Based on Quantum Noise." Applied Sciences 13.23 (2023): 12619.

Herrero-Collantes, Miguel, and Juan Carlos Garcia-Escartin. "Quantum random number generators." Reviews of Modern Physics 89.1 (2017): 015004.

Rukhin, Andrew, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Vol. 22. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2001.

Ferreira, Maurício J., et al. "Characterization of a quantum random number generator based on vacuum fluctuations." Applied Sciences 11.16 (2021): 7413.

Acknowlegments

This work was supported in part by Fundação para a Ciência e a Tecnologia (FCT) through national funds, by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the Portugal 2020 framework, under the project QuantumPrime (PTDC/EEI-TEL/8017/2020) and UIDB/50008/2020-UIDP/50008/2020. M. Ferreira also acknowledges the 2022.09584.BD PhD grant from FCT.

universidade de aveiro

fct Fundação para a Ciência e a Tecnologia

REPÚBLICA PORTUGUESA | CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

PORTUGAL 2020

Co-funded by the European Union

EuroQCI