Entropy analysis of a QRNG based on photon time of arrival statistics

Vitor Tavares, Elisabeth Monteiro, Guilherme Temporão, Daniel Magalhães and Filippo Ghiglieno

***Resumo*— Geradores de Números Aleatórios (RNGs) são essenciais para a criptografia e diversas outras aplicações. Este trabalho apresenta uma avaliação metrológica de um Gerador Quântico de Números Aleatórios (QRNG) baseado em contagem de fótons, operando no comprimento de onda de telecomunicações de 1550nm. Os resultados indicam que a largura de 20 ns é a mais adequada para a implementação deste tipo de QRNG, pois gera o maior valor de entropia, conforme esperado.**

***Palavras-Chave*— Criptografia Quântica, Comunicações Quânticas, Informação Quântica**

***Abstract*— Random Number Generators (RNGs) are essential for cryptography and various other applications. This paper presents a metrological evaluation of a Quantum Random Number Generator (QRNG) based on photon counting, operating at the telecom wavelength of 1550 nm. The results indicate that a gate width of 20 ns is the most suitable for implementing this type of QRNG, as it yields the highest entropy value, as expected.**

***Keywords*— Quantum Cryptography, Quantum Communications, Quantum Information**

I. Introduction

Random numbers play a fundamental role in cryptography, ensuring the generation of secure keys, and are also widely applied in simulations [1], statistical analysis [2], and clinical trials [3]. In security applications, the quality of randomness is crucial. While pseudo-random number generators (PRNGs) are widely used, their algorithmic nature may lead to predictability. True random number generators (TRNGs), which exploit physical phenomena, offer high-quality entropy and are therefore attractive for cryptographic use.

This work investigates a TRNG based on weak coherent states, where a laser source is attenuated and randomness is extracted from photon time-of-arrival measurements using a single-photon avalanche diode (SPAD). We present a metrological evaluation of the influence of the detection gate width of an InGaAs/InP SPAD, operating in the third telecommunications window, on the entropy generation of a quantum random number generator (QRNG) [4].

Vitor Tavares, Departament of Physics, Federal University of São Carlos, São Carlos-SP, e-mail: vstavares@colaborador.inmetro.gov.br; Elizabeth Monteiro, Postgraduate Program in Metrology, Pontifical Catholic University of Rio de Janeiro, Rio de Janeiro, e-mail: beth@puc-rio.br; Guilherme Temporão, Center for Telecommunications Studies, Pontifical Catholic University of Rio de Janeiro, Rio de Janeiro, Rio de Janeiro-RJ, e-mail:temporao@opto.cetuc.puc-rio.br; Daniel Magalhães, Institute of Physics, University of São Paulo, São Carlos-SP, e-mail: daniel@sc.usp.br; Filippo Giovanni Ghiglieno, Federal University of São Carlos, São Carlos-SP, e-mail: filippo.ghiglieno@df.ufscar.br. Este trabalho foi parcialmente financiado por (Conselho Nacional de Desenvolvimento Científico e Tecnológico) – Brazil – Código 315160/2025-0

II. Quantum theory of photon detection

The randomness is obtained from a quantum coherent state. A random bit generator can be defined as a device that yields bits with equal probabilities of ones and zeros (p(0) = p(1) = 50 %), all statistically independent from each other. It is known that the photon number distribution of a weak coherent state follows a Poissonian distribution [5]:

$$P(n) = \frac{(\bar{\mu}\eta)^n}{n!} e^{-\bar{\mu}\eta} \tag{1}$$

where the effective average number of photons, given by the product$\bar{\mu}\eta$ where $\bar{\mu}$ is the average number of photons per gate and η is detection efficiency of the SPAD, is an important parameter that must be measured, knowing that $\bar{\mu}\eta \approx 0.7$ to reach the condition (p(0) = p(1) = 50 %) [5]. Thus, it is guaranteed that the entropy produced by the QRNG will reach the unit. In this analysis, noise contributions from the detector are not considered.

III. Materials and methods

Experimental setup used a laser with the values of optical attenuation and wavelength fixed at 10 ± 0.03 dB and 1556.5 nm respectively. The laser was connected to an variable optical attenuator 1 (AOV - 1), in which the optical attenuations were modulated in the range of -42 to -25 dB and in the variable optical attenuator 2 (AOV-2), it was maintained with a fixed optical attenuation at $-20 \pm 0,05$ dB. This second optical attenuator was connected to the ID Quantique SPAD detector to count the photons by the detector. In Figure 1, the schematic diagram described of QRNG.

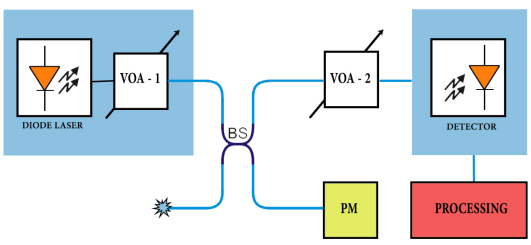

Fig. 1. Schematic diagram of the experimental setup.

As shown in Figure 1, the SPAD detector was connected to a processing unit consisting of a microcomputer and an FPGA, which generated a 1 MHz “clock” (periodic digital signal) for the detector. This signal enabled data acquisition in trigger mode, with each acquisition lasting 5 s. For this test,

the average number of windows (Nj) was on the order of 10^6. SPAD gate widths of 4 ns, 8 ns, 12 ns, 16 ns, and 20 ns were used, with optical attenuation ranging from -56 dB to -38 dB, corresponding to an optical power range of 2.51 nW to 158.48 nW estimated before the single-photon detector. The detection efficiency and dead time were fixed at 15 % and 1 μs, respectively. In this configuration, random bits were generated by assigning a bit value of 0 when no photon was detected and a bit value of 1 when a photon was detected.

IV. Results

In scientific literature, one of the most widely used estimators of unpredictability is Shannon entropy [7], given by:

$$H = -[p(i)\log_2 p(i) + (1-p(i))\log_2(1-p(i))] \quad (2)$$

Thus, Figure 2 characterizes the entropy generated for each window width.

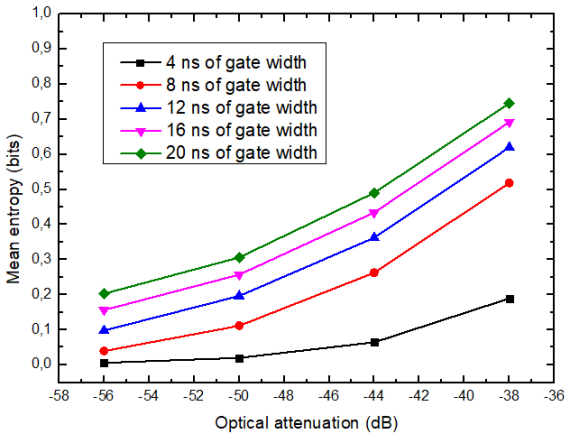

Fig. 2. Characterization of mean entropy as a function of the optical attenuation, from -56 dB to -68 dB (2.51 nW to 158.48 nW) setup.

In Figure 2, it is important to note that the optical attenuation values differ by six units from each other, resulting in a significant variation in the effective average number of photons. As mentioned, it is necessary to obtain an average effective number of photons equal to 0.7 to achieve H = 1. In this experimental setup, the best value of gate width and optical attenuation for this optimal situation were 20 ns and -38 dB respectively, as can be seen in Figure 2.

V. Conclusions

In this work, we propose an analysis of the influence of the detection gate width of an InGaAs/InP SPAD when implemented for the purpose of generating a QRNG through variations in optical attenuation. The evaluation was performed for gate width values of 4 ns, 8 ns, 12 ns, 16 ns, and 20 ns, and for optical attenuation values of -56 dB, -50 dB, -44 dB and -38 dB. Shannon's entropy was estimated for each combination of optical attenuation and gate width. The optimal optical attenuation for the QRNG was found to be -38 dB under the tested conditions (15% detection efficiency, 1 μs dead time, 1556.5 nm source). The key parameter for achieving maximum entropy ($H = 1$) is the product $\bar{\mu}\eta \approx 0.7$; the closest experimental value obtained was 0.23 for -38 dB and a 20 ns gate width. Results show that smaller gate widths require higher optical power to reach $H = 1$, while larger gate widths reduce this power requirement. This work is still in progress. We intend to further optimize the experimental system in order to achieve the condition for $H = 1$. In addition, we will evaluate the QRNG through statistical tests in order to verify the quality of the randomness generated.

Agradecimentos

Authors acknowledge the financial support provided by the Brazilian research agencies CAPES, FINEP, FAPESP and CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico) – Brazil – Finance Code 315160/2025-0.

Referências

[1] S. Jun, P. Canal, J. Apostolakis, A. Gheeta, L. Moneta, "Vectorization of random number generation and reproducibility of concurrent particle transport simulation," in *Journal of Physics: Conference Series*, vol. 1525, IOP Publishing, 2020, p. 012054.

[2] B. Rainer, J. Pilz, M. Deutschmann, "Assessing the statistical quality of RNGs," in *Quantum Random Number Generation*, Springer, 2020, pp. 45–64.

[3] K. Suresh, "An overview of randomization techniques: an unbiased assessment of outcome in clinical research," *Journal of Human Reproductive Sciences*, vol. 4, no. 1, 2011, p. 8.

[4] C. Kollmitzer, S. Petscharnig, M. Suda, M. Mehic, "Quantum random number generation," in *Quantum Random Number Generation*, Springer, 2020, pp. 11–34.

[5] E. F. Carneiro, F. Calliari, G. C. Amaral, G. P. Temporão, "Random bit generation using coherent state and threshold detectors at 1550 nanometers," *Applied Optics*, vol. 56, no. 24, 2017, pp. 6855–6860.

[6] A. Banerjee, D. Aggarwal, A. Sharma, G. Yadav, "Unpredictable and uniform RNG based on time of arrival using InGaAs detectors," *arXiv preprint* arXiv:2010.12898, 2020.

[7] C. H. Bennett, P. W. Shor, "Quantum information theory," *IEEE Transactions on Information Theory*, vol. 44, no. 6, 1998, pp. 2724–2742.

[8] D. Stucki, S. Burri, E. Charbon, C. Chunnilall, A. Meneghetti, F. Regazzoni, "Towards a high-speed quantum random number generator," in *Emerging Technologies in Security and Defence II; and Quantum Security II; Unmanned Sensor Systems X*, vol. 8899, International Society for Optics and Photonics, 2013, p. 88990R.