Time-interleaved quantum random number generation within a coherent classical communication channel

Maurício J. Ferreira[1,2], **Daniel Pereira**[2,3], **Nelson J. Muga**[2], **Nuno A. Silva**[2], **Armando N. Pinto**[2,3]

[1]Department of Physics, University of Aveiro, Aveiro, Portugal

[2]Instituto de Telecomunicações, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal

[3]Department of Electronics, Telecommunications and Informatics, University of Aveiro, Aveiro, Portugal

{mauricioferreira, danielfpereira, muga, nasilva, anp}@ua.pt

Abstract. *We propose and analyse a suitable setup for a time-interleaved vacuum-based quantum random number generator (QRNG) within a classical communication channel, which removes the need for a dedicated generation device. The experimental setup was characterized to assess the conditions where quantum fluctuations are dominant, and support for generation rates up to* $1.3\,\mathrm{Gbps}$ *is observed. Finally, the random bit stream is subjected to the NIST randomness test suite, consistently passing all evaluations.*

1. Introduction

Random number generation assumes a crucial role in the security of many cryptographic protocols, from data encryption to digital signatures [Gennaro 2006]. Typically, pseudo-random number generators (PRNGs) are used to easily provide apparently unpredictable sequences at very high rates. Unfortunately, their deterministic nature is not suitable for critical applications such as quantum key distribution (QKD) [Bouda et al. 2012], as it implies the existence of an underlying pattern that becomes predictable to an adversary with enough computational resources [Kelsey et al. 1998]. In answer to these shortcomings, QRNGs, which explore the inherently probabilistic nature of quantum measurements, have materialized as a viable source of high-quality randomness [Herrero-Collantes and Garcia-Escartin 2017]. In particular, generation schemes based on measurements of vacuum fluctuations are attractive for their ability to provide high-speed generation rates with low-cost implementations [Zheng et al. 2019, Huang et al. 2020b, Gehring et al. 2021]. These typically employ a balanced homodyne detection (BHD) scheme to obtain measurements proportional to the amplitude quadrature of the optical vacuum state, which follows an inherently random Gaussian distribution [Gabriel et al. 2010]. In practice, a laser acts as the local oscillator (LO) and is split on a balanced beamsplitter (BS), which has one of its input ports blocked to guarantee the purity of the vacuum state [Huang et al. 2020a]. The resultant output signals are detected on a balanced detector, and the respective photocurrents subtracted. Thus, ideally, any amplitude fluctuations will be cancelled, and only the LO shot noise remains. However, measurements will always be tampered with by additional non-random noise sources such as electrical noise, which opens security loopholes that can be explored by an eavesdropper [Ferreira et al. 2021, Silva et al.

2020]. Consequently, a randomness extractor such as a Toeplitz matrix is typically applied to remove these unwanted contributions [Haw et al. 2015]. Unfortunately, QRNGs frequently require bulky dedicated implementations that render them unattractive in face of algorithmic alternatives. On the other hand, balanced homodyne detectors have been widely adopted in the field of optical communications, and are easily commercially available. Coherent receivers in particular can easily be re-purposed for randomness generation, which allows the integration of a vacuum-based QRNG into optical communication links [Milovančev et al. 2020].

In this paper, we propose and demonstrate an implementation of a vacuum-based QRNG that is time-interleaved with a quadrature phase shift keying (QPSK) tributary signal within a classical coherent optical transmission system. With this objective, the measured homodyne measurements were characterized to assess the conditions where the shot noise is dominant and a RNG can be implemented. Finally, we applied a set of statistical tests to quantify the statistical quality of its output.

2. Experimental Implementation

A schematic representation of the experimental setup is shown in Fig. 1. Here, a heterodyne detection scheme was considered for the classical data transmission. Although this requires a more complex digital signal processing (DSP), it allows us to greatly simplify the experimental setup [Kleis et al. 2017]. A $1550\,\mathrm{nm}$ continuous-wave laser at $10\,\mathrm{dBm}$ and with a $100\,\mathrm{kHz}$ linewidth is split by a 35/65 beamsplitter (BS1) formed by the combination of a polarization beamsplitter (PBS) and a polarization controller (PC). The $8.10\,\mathrm{dBm}$ beam is posteriorly sent towards a balanced beamsplitter (BS2) where it becomes the local oscillator in the coherent receiver. Single sideband modulation is performed upon the remaining optical signal with an I/Q optical modulator (SCMO2125, u^{2}t) using an electrical signal provided by a digital-to-analog converter (DAC38J84, Texas Instruments) at a $1474.56\,\mathrm{MSa/s}$ sampling rate. The electrical modulation contains a QPSK signal $y(t) = q(t)exp(j2\pi f_Q t)$ upconverted to $f_Q = 92.16\,\mathrm{MHz}$. Here, $q(t)$ denotes the convolution of the complex-valued symbols and root-raised-cosine filter [Kleis et al. 2017]. A symbol rate of $46.08\,\mathrm{MBd}$ was chosen, which yields an optical link capacity of $184.32\,\mathrm{Mbps}$. After the QPSK modulation, an acousto-optic amplitude modulator (Gooch & Housego 26035-2-1.55-LTD) with a $40\,\mathrm{dB}$ extinction ratio and a $35\,\mathrm{MHz}$ operating frequency was added to impose on-off shift keying (OOK) upon the QPSK signal.

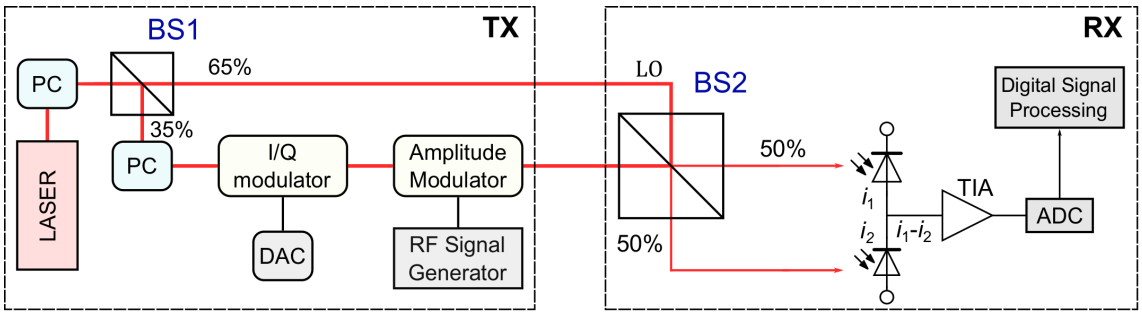

Figure 1. Schematic representation of the experimental setup. An amplitude modulator is introduced on a classical coherent communication link and allows to alternately perform heterodyne detection over the QPSK signal, or obtain a BHD scheme with a vacuum state at one of the input ports.

The signal was thus pulsed at $700\,\mathrm{Hz}$ by rectangular pulses with an amplitude of $5\,\mathrm{V}$ and a 50% duty cycle. This regularly removes the QPSK signal, and thus reduces the experimental setup to the vacuum-based QRNG implementation described in Section 1. Obviously, in reality, the impinging optical power will never be completely removed, and the vacuum state can be compromised. To mitigate this problem we have chosen an amplitude modulator with a high extinction ratio. At the receiving site, heterodyne detection is performed with a $1.6\,\mathrm{GHz}$-balanced receiver (Thorlabs PDB480AC). Finally, the resulting electric signal is digitized at $2949.12\,\mathrm{MSa/s}$ by a 12-bit ADC (Texas Instruments ADC32RF45), and a DSP routine is used to either extract the transmitted symbols [Kleis et al. 2017], or apply a randomness extraction algorithm [Haw et al. 2015]. Here, to correctly retrieve the sequence, the frequency shift of $35\,\mathrm{MHz}$ induced by the acousto-optic modulator in the QPSK signal needs to be considered in the DSP routine.

3. Results and Discussion

As shown in Fig. 2a, we confirm that the introduction of OOK modulation allows to time-interleave a QRNG in the communication channel. Here, periods of higher variance correspond to the data transmission, while those of lower amplitude states indicate the QRNG operation. With the chosen parameters, we obtain roughly $0.714\,\mathrm{ms}$ of QPSK communication every pulse period, which is enough to transmit a periodic sequence of $65\,536\,\mathrm{bit}$. Naturally, a realistic communication system will rarely obey to these characteristics, and no fixed period will be able to guarantee the detection of all symbols transmitted. Thus, although not here considered, a synchronization method between the data transmission and the amplitude modulator is expected for a complete application.

Measurements of the power spectral density taken during the QRNG operation are presented in Fig. 2b. As expected for white noise, we attain a relatively flat power density level. However, strong spectral contributions can be observed at low frequencies as a consequence of electric hum, or an imperfect subtraction due to the finite common-mode rejection ratio of the detector. Since these can compromise the quality of the QRNG

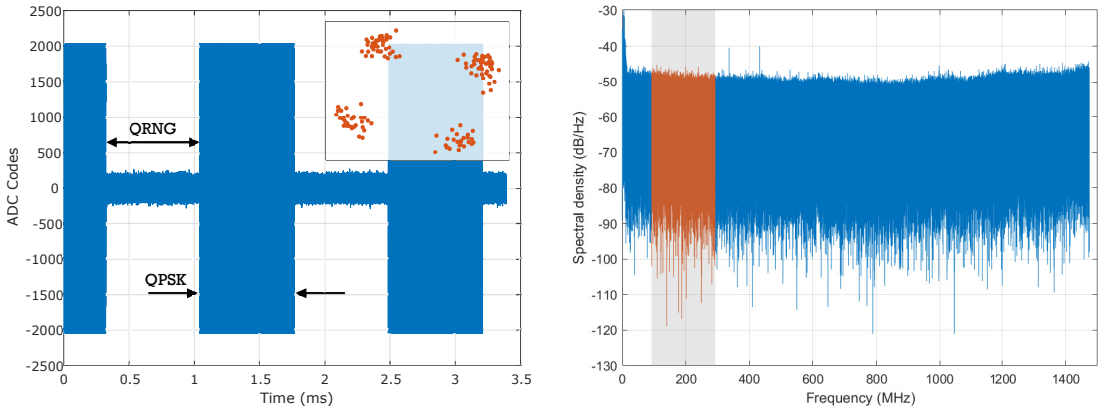

Figure 2. a) Time representation of the signal observed during the interleaved operation. Periods with higher amplitude correspond to QPSK transmission. Inset shows a retrieved QPSK constellation with 157 symbols. b) Power spectral density taken during the QRNG operation. Highlighted frequencies are selected to perform randomness extraction.

output, we digitally selected a $200\,\mathrm{MHz}$ flat frequency range free of strong contributions through a rectangular bandpass filter. The same filter was applied to the detector's electric noise measurements taken without impinging optical power, which are necessary to estimate the available entropy in the randomness extraction algorithm. In the selected interval, we observe a quantum clearance level of at least $10\,\mathrm{dB}$, which confirms that there is preponderance of quantum fluctuations over classical contributions.

3.1. Noise Characterization

Ideally, as given by the Nyquist sampling theorem, a sampling rate inferior to $3.2\,\mathrm{GSa/s}$ should be chosen to avoid randomness overlapping. Although the chosen sampling rate already complies with this condition, the previously spectral selection limits the signal to a frequency band of $200\,\mathrm{Hz}$, and thus a maximum sampling rate of $400\,\mathrm{Hz}$ is expected. Consequently, to avoid temporal correlations between samples introduced by the transimpedance amplifier, we downsampled the measured signal by a factor of 10, obtaining an effective sampling rate of $294.912\,\mathrm{MSa/s}$. This effect can be seen in Fig. 3a, where clear correlations emerge for the signal without downsampling applied. By contrast, the analysis of the correlation coefficients for the downsampled signal shows a rapid drop to a value of 1.62×10^{-3}. In fact, although residual correlations occur as a consequence of the finite bandwidth of the signal, a delay of just one sample guarantees values inferior to 10^{-1}. This suggests negligible correlations between samples, which is essential for any reliable RNG. Finally, a histogram with $7.5\,\mathrm{M}$ homodyne measurements, and $1.9\,\mathrm{M}$ samples of electronic noise is shown in Fig. 3b. Results show that all noise follows the expected Gaussian distribution, and a quantum to classical noise ratio (QCNR) of roughly $12\,\mathrm{dB}$ can be obtained. Additionally, respective means of approximately $0.0035\,\mathrm{mV}$ and $-0.0011\,\mathrm{mV}$ were calculated for the homodyne and electronic noise samples, which are low enough to be disregarded as indicative of an adequately BHD.

3.2. Statistical Validation

With this analysis, $27.7\,\mathrm{M}$ samples were subjected to the randomness extraction algorithm. To estimate the entropy, we calculate the min-entropy of the measurement homodyne noise conditioned on the classical noise, $H_{\min} = -\log_2(\max[p_{M|E}(x)])$, where

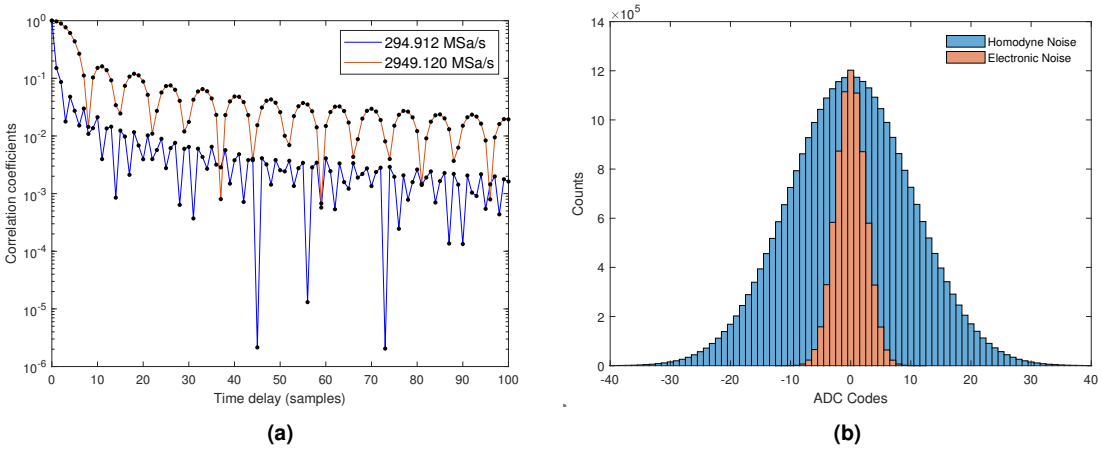

Figure 3. a) Correlation coefficients for noise samples over 8.3 M samples for two different sampling rates. b) Distribution of 7.9 M homodyne measurements and 1.9 M electronic noise samples.

$p_{M|E}(x)$ is the conditional power distribution function between the measured signal M and the classical noise E [Haw et al. 2015]. Considering a maximum excursion of the classical noise of $5\sigma_E$ yields a min-entropy of $4.58\,\mathrm{bit}$ per $12\,\mathrm{bit}$ sample. Here, the SHA-512 cryptographic hash function was chosen as a randomness extractor. The data is thus divided into subsets of length determined by $H_{\min}$, and a one-way projection into a shorter set of 512 bits. The desired output bit length is posteriorly achieved by composing the results of each subset. This process is equivalent to perform privacy amplification and yields a sequence of approximately $126.8\,\mathrm{M}$ uniformly distributed true random bits. With these conditions, a maximum theoretical generation rate of $1.3\,\mathrm{Gbps}$ is achieved, which yields around $928.2\,\mathrm{Mbit}$ in each QRNG operation cycle. Unfortunately, the offline processing is limited to $1.68\,\mathrm{Mbps}$. Finally, to evaluate the quality of the extracted RN, we applied the NIST SP 800-22 randomness test suite. As can be seen in Table. 1, the QRNG passes all evaluations, which is a good indicator of quality for the implemented generator.

Table 1. Results of the NIST SP 800-22 test battery, with 0.01 significance level for a sequence of 1268689 bits. The minimum proportion to pass is 96/100, except for the *random excursions* tests where 60/63 is accepted. For results with multiple *p-values*, the one with the smaller proportion is shown.

Statistical Test	P-value	Proportion	Result
Frequency	0.249284	100/100	PASSED
BlockFrequency	0.867692	99/100	PASSED
CumulativeSums	0.514124	100/100	PASSED
Runs	0.574903	100/100	PASSED
LongestRun	0.122325	100/100	PASSED
Rank	0.759756	100/100	PASSED
FFT	0.213309	97/100	PASSED
NonOverlappingTemplate	0.162606	96/100	PASSED
OverlappingTemplate	0.334538	100/100	PASSED
Universal	0.514124	100/100	PASSED
Approximate entropy	0.319084	98/100	PASSED
Random excursions	0.392456	62/63	PASSED
Random-excursions variant	0.723129	61/63	PASSED
Serial	0.153763	99/100	PASSED
LinearComplexity	0.739918	99/100	PASSED

4. Conclusion

In conclusion, a framework to time-interleave a QRNG into a coherent optical communication link was presented. By imposing OOK modulation on the transmission channel, we remove the input signal and obtain a simple BHD. Here, an extraction ratio of approximately 0.38 bits per sample was measured, yielding a maximum output rate of $1.3\,\mathrm{Gbps}$. In a realistic application, a method to synchronize the two operation modes with the transmitted data should be explored. Meanwhile, the finite extinction rate of the amplitude modulator can lead to contamination of the vacuum state, which opens security loopholes, and thus further security analysis is required. Nonetheless, the RNs pass the standard NIST randomness test suite, indicating the output of high-quality randomness.

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 projects DSPMetroNet (POCI-01-0145-FEDER-029405), QuantumPrime (PTDC/EEI-TEL/8017/2020), Q.DOT (POCI-01-0247-FEDER-039728), and UIDB/50008/2020-UIDP/ 50008/2020 (actions DigCORE and QuRunner). The authors also acknowledge support from the Programme New Talents in Quantum Technologies of the Gulbenkian Foundation (Portugal).

References

Bouda, J., Pivoluska, M., Plesch, M., and Wilmott, C. (2012). Weak randomness seriously limits the security of quantum key distribution. *Phys. Rev. A*, 86:062308.

Ferreira, M. J., Silva, N. A., Pinto, A. N., and Muga, N. J. (2021). Homodyne noise characterization in quantum random number generators. In *2021 Telecoms Conference (ConfTELE)*, pages 1–6.

Gabriel, C., Wittmann, C., Sych, D., Dong, R., Mauerer, W., Andersen, U. L., Marquardt, C., and Leuchs, G. (2010). A generator for unique quantum random numbers based on vacuum states. *Nature Photonics*, 4(10):711–715.

Gehring, T., Lupo, C., Kordts, A., Solar Nikolic, D., Jain, N., Rydberg, T., Pedersen, T., Pirandola, S., and Andersen, U. (2021). Homodyne-based quantum random number generator at 2.9 gbps secure against quantum side-information. *Nature Communications*, 12.

Gennaro, R. (2006). Randomness in cryptography. *IEEE Security Privacy*, 4(2):64–67.

Haw, J. Y., Assad, S. M., Lance, A. M., Ng, N. H. Y., Sharma, V., Lam, P. K., and Symul, T. (2015). Maximization of extractable randomness in a quantum random-number generator. *Phys. Rev. Applied*, 3:054004.

Herrero-Collantes, M. and Garcia-Escartin, J. C. (2017). Quantum random number generators. *Reviews of Modern Physics*, 89(1).

Huang, M., Chen, Z., Zhang, Y., and Guo, H. (2020a). A gaussian-distributed quantum random number generator using vacuum shot noise. *Entropy*, 22(6).

Huang, W., Zhang, Y., Zheng, Z., Li, Y., Xu, B., and Yu, S. (2020b). Practical security analysis of a continuous-variable quantum random-number generator with a noisy local oscillator. *Phys. Rev. A*, 102:012422.

Kelsey, J., Schneier, B., Wagner, D., and Hall, C. (1998). Cryptanalytic attacks on pseudorandom number generators. In Vaudenay, S., editor, *Fast Software Encryption*, pages 168–188, Berlin, Heidelberg. Springer Berlin Heidelberg.

Kleis, S., Rueckmann, M., and Schaeffer, C. G. (2017). Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals. *Opt. Lett.*, 42(8):1588–1591.

Milovančev, D., Vokić, N., Pacher, C., Khan, I., Marquardt, C., Boxleitner, W., Hübel, H., and Schrenk, B. (2020). Towards integrating true random number generation in coherent optical transceivers. *IEEE Journal of Selected Topics in Quantum Electronics*, 26(5):1–8.

Silva, N. A., Pereira, D., Muga, N. J., and Pinto, A. N. (2020). Practical imperfections affecting the performance of CV-QKD based on coherent detection. In *2020 22nd International Conference on Transparent Optical Networks (ICTON)*, pages 1–4.

Zheng, Z., Zhang, Y., Huang, W., Yu, S., and Guo, H. (2019). 6 Gbps real-time optical quantum random number generator based on vacuum fluctuation. *Review of Scientific Instruments*, 90(4):043105.