Certified Quantum Randomness with Coherent Detection

Vitor L. Sena[1], Moisés Alves[1,2], Santiago Zamora[2], Tailan S. Sarubi[2], Alexssandre de Oliveira Junior[3], Alexandre B. Tacla[1]

[1]QuIIN – Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, SENAI CIMATEC Av. Orlando Gomes 1845, 41650-010, Salvador, BA, Brazil.

[2]International Institute of Physics and School of Science and Technology, Federal University of Rio Grande do Norte, 59078-970, Natal, RN, Brazil.

[3]Center for Macroscopic Quantum States bigQ, Dept. of Physics, Technical University of Denmark, Fysikvej 307, 2800 Kgs. Lyngby, Denmark.

vitor.sena@fbter.org.br

Abstract. *In this work, we analyze a semi-device-independent technique for quantum random number generation (QRNG) certification based on coherent detection. We consider a prepare-and-measure scenario, in which pure quantum states are prepared and sequentially measured using homodyne detection, a continuous-variable measurement, and evaluate dimension witness (DW) inequalities to certify quantum randomness. We extend the DW framework to this continuous-variable setting through phase-space binning optimization and demonstrate that symmetric binning maximizes DW violation across single-, double-, and triple-partition configurations. We additionally explore heterodyne (double homodyne) detection as a complementary coherent measurement; no witness violation is observed under this scheme for several discretization schemes. This work provides additional analysis to the study of certifiable QRNG based on homodyne detection, a mature and widely available technology with natural applicability in secure network communications.*

1. Introduction

Random numbers are essential to a broad range of processes, spanning computer simulations, data analysis, security, and cryptography [Johnston 2018]. Fundamentally, effective random number generation (RNG) requires uniformity and independence: generated numbers must be uniformly distributed and statistically uncorrelated. In network security in particular, high-quality randomness underpins cryptographic key generation, making its certified production a fundamental concern for secure communications infrastructure. Classical pseudo-random number generators fall short of this demand: being ultimately deterministic, they cannot guarantee true unpredictability, leaving security systems vulnerable to adversaries equipped with quantum computing capabilities [Acín and Masanes 2016]. This limitation has driven the growing global interest in quantum random number generation (QRNG) [Ma et al. 2016, Herrero-Collantes and Garcia-Escartin 2017, Mannalatha et al. 2023], which exploits the inherent probabilistic nature of quantum processes to produce genuinely random outcomes, with commercial deployments already reaching consumer devices and critical infrastructure

[ID Quantique , Pivetta 2024]. While classical statistical tests such as NIST SP 800-22 [Bassham et al. 2010] remain useful benchmarks, they cannot by themselves certify the quantum origin of randomness.

In this work, we further analyze a semi-device-independent (semi-DI) technique for certifiable QRNG [Alves et al. 2025] that relies on bounded dimensionality assumptions. Within a prepare-and-measure (P&M) scenario, we apply dimension witness inequalities to homodyne detection by discretizing continuous outcomes through phase-space binning. We additionally explore heterodyne (double homodyne) detection as a complementary coherent scheme. Systematic optimization across one-, two-, and three-partition binning configurations consistently converges to the same solution: maximum certifiable randomness is achieved by splitting outcomes at the midpoint of the quantum state's probability distribution.

2. System Configuration and Dimension Witnesses

The physical context we address operates within a P&M scenario (Figure 1). This experimental paradigm involves preparing a quantum state ρ_x from an input value x, followed by a measurement M_y, defined by an input y. This process yields a discrete outcome b as the measurement result. Mathematically, $x \in \{0, 1, \ldots\}$, $y \in \{0, 1, \ldots\}$, and $b \in \{0, 1\}$ are realizations of random variables X, Y, and B. Scenarios are formally characterized by the cardinality triplet $(|B|, |X|, |Y|)$, which constrains the problem dimension. For instance, a $(2, 3, 2)$ scenario generates binary outputs ($|B| = 2$), allows three preparations ($|X| = 3$), and two measurement choices ($|Y| = 2$).

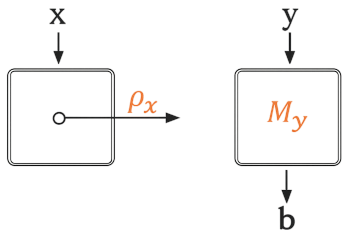

Figure 1. Prepare-and-Measure (P&M) scenario. An input x labels the system state, while y labels the measurement. The process yields outcome b.

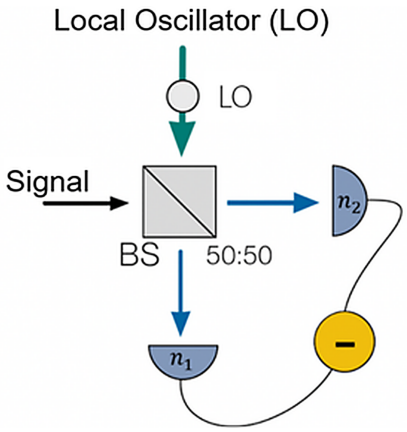

Figure 2. Homodyne detection scheme for measuring a quadrature of the electromagnetic field. BS denotes the 50:50 beam splitter and (LO) the local oscillator, which is tuned to the same frequency and phase-locked to the input signal.

Building upon this framework, QRNG implementations are classified by device trust assumptions. Device-dependent protocols assume perfectly calibrated devices and certify randomness through physical modeling, but offer no protection against implementation flaws [Ma et al. 2016, Mannalatha et al. 2023]. Device-independent (DI) approaches

eliminate all trust requirements via Bell tests on entangled states [Agresti et al. 2020], but require experimentally demanding loophole-free implementations [Hensen et al. 2015]. Semi-device-independent (semi-DI) techniques strike an operational equilibrium: by incorporating weak physical assumptions such as bounded system dimension or energy, they circumvent DI's experimental overhead while surpassing device-dependent security [Cheng et al. 2024]. Here, we investigate QRNG certification through dimension witnesses – mathematical inequalities that bound the dimensionality of a system, without requiring full device knowledge or entanglement resources.

To distinguish classical from quantum behavior, we analyze the conditional probability $p(b|x, y)$ of obtaining result b given preparation x and measurement setting y. The theoretical foundation of dimension witnesses originated with Brunner et al. [Brunner et al. 2008], who established Hilbert space dimension as an experimentally quantifiable quantum resource. Subsequent work generalized this formalism to black-box and P&M contexts [Gallego et al. 2010] while exploring its connections to semi-DI approaches [Bowles et al. 2014].

A dimension witness is a linear inequality in probabilities that distinguishes classical and quantum systems given a specific constraint on the system's dimensionality. For an event $e = b|x, y$, these witnesses take the general form:

$$W = \sum_i c_i \cdot p(e_i) \leq \beta, \tag{1}$$

where $c_i = \pm 1$ and β is the classical bound. For quantum systems, $W > \beta$ is achievable. Thus the condition $W > \beta$ serves as a certificate of quantumness, as it cannot be achieved by any classical system. Our investigation focuses on the $(2, 4, 2)$ scenario, where any classically realizable correlation is bounded by [Li et al. 2011]:

$$\begin{aligned} W_2 = {} & p(0|0,0) - p(0|0,1) + p(0|1,0) + p(0|1,1) \\ & - p(0|2,0) + p(0|2,1) - p(0|3,0) - p(0|3,1) \leq 2. \end{aligned} \tag{2}$$

Quantum randomness certification within this setup proceeds in three steps: collect experimental data to reconstruct $p(b|x, y)$; compute W via Eq. (1); and check for a violation $W > \beta$. If a violation is detected, the system is confirmed quantum and randomness extraction can proceed; otherwise the results may be classical or predictable.

3. QRNG Certification with Homodyne Detection

The dimensionless quadrature operators of a single-mode electromagnetic field, $\hat{q} = (\hat{a}^\dagger + \hat{a})/\sqrt{2}$ and $\hat{p} = -i(\hat{a}^\dagger - \hat{a})/\sqrt{2}$ (in shot-noise units), are continuous-spectrum observables analogous to the position and momentum operators of a quantum harmonic oscillator [Gerry and Knight 2023]. They can be directly measured via homodyne detection, yielding continuous real outcomes: the optical signal is mixed with an intense local oscillator at a beam splitter, and the generated photocurrent is proportional to the quadrature amplitude (Figure 2). Both quadratures can be accessed simultaneously via heterodyne detection, which splits the signal at a balanced beam splitter and performs two homodyne measurements on the resulting modes, producing a two-bit output.

Constructing dimension witnesses directly for continuous-variable systems remains an open challenge [Brunner et al. 2014]. We therefore propose an alternative route by

formulating witnesses for qubit systems and mapping the continuous homodyne outputs into a two-dimensional space via *binning*: we partition the real line into $R_0 \subset \mathbb{R}$ and $R_1 = \mathbb{R} \setminus R_0$, defining:

$$M_{\text{hom}}^{(b)} = \int_{R_b} dq \, |q\rangle\langle q|, \tag{3}$$

where $b = 0, 1$. The Born rule gives $p(b|x, y) = \text{Tr}\left(\rho_x \, M_{\text{hom}}^{b|y}\right)$. States are prepared in the two-dimensional Fock subspace as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, with $|\alpha|^2 + |\beta|^2 = 1$, so $\rho_x = |\psi\rangle\langle\psi|$, such states can be prepared using low-photon-number sources. We consider three binning configurations illustrated in Figure 3: single-partition (a), two-partition (b), and three-partition (c). For the two-partition case, patterns 001, 100, 011, and 110 reduce to the single-partition case, leaving the alternating pattern, 101 and 010, as the only genuinely new (but worse) configuration; the three-partition case similarly reduces to the one-partition case when optimized, even in alternating sequences such as 1010 and 0101.

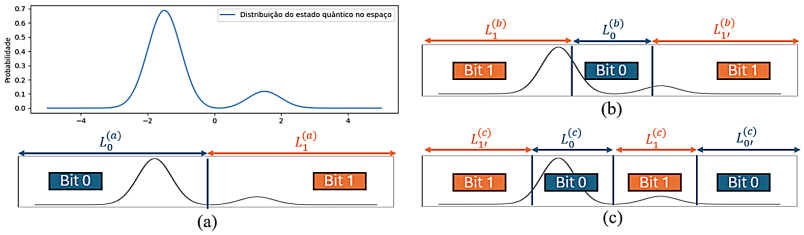

Figure 3. Illustration of a continuous measurement outcome distribution and the corresponding binning configurations for an arbitrary input state: (a) single-partition, (b) two-partition, and (c) three-partition. Orange and blue regions represent bit 1 and bit 0 assignments, respectively.

4. Results

To find the states and homodyne configuration maximizing W_2 in the $(2, 4, 2)$ scenario (classical bound $W_2 \leq 2$, quantum maximum $W_2^{(\max)} = 2\sqrt{2} \approx 2.828$), we solve:

$$\begin{aligned} &\text{maximize} \quad W_2 \\ &\text{subject to} \quad p(b|x, y) = \text{Tr}\left(\rho_x \, M_{\text{hom}}^{b|y}\right). \end{aligned} \tag{4}$$

The optimization in Eq. (4) is numerically performed over state amplitudes and bining thresholds. Figure 4 summarizes the results for all three configurations. For the single-partition case, we scanned different values of $L_1^{(a)} - L_0^{(a)}$ and found that the optimal configuration is the symmetric bisection (Figure 4a), with no other partition achieving a higher violation. The maximal value found was $W_2 \approx 2.25$. For the two-partition case, the best configuration again reduces to the symmetric single-partition limit for patterns 001, 100, 011, and 110; the alternating patterns 101 and 010 perform strictly worse (Figure 4b). Finally, the three-partition configuration introduces two free parameters $L_0^{(c)}$ and $L_1^{(c)}$: the three-dimensional optimization surface (Figure 4c) shows that the maximum $W_2 \approx 2.25$ is reached precisely when both central widths vanish, recovering the symmetric single-partition case. In all configurations, the maximum witness value remains $W_2 \approx 2.25$.

We also explored heterodyne detection as a complementary coherent measurement strategy. Four output-combination strategies were investigated: retaining a single quadrature (A or B), or combining both via XOR, OR, and AND logic gates (Figure 4d). No strategy yielded a witness violation, with the maximum reaching $W_2 \approx 1.59$. Notably, the best result was achieved by simply discarding one quadrature, suggesting that the additional degree of freedom introduced by heterodyne detection confers no advantage within the present binning framework. This can be understood from the fact that the beam splitter at the core of heterodyne detection entangles the two output modes, such that tracing over one mode necessarily reduces the coherence of the other, degrading the quantum character of each individual measurement outcome.

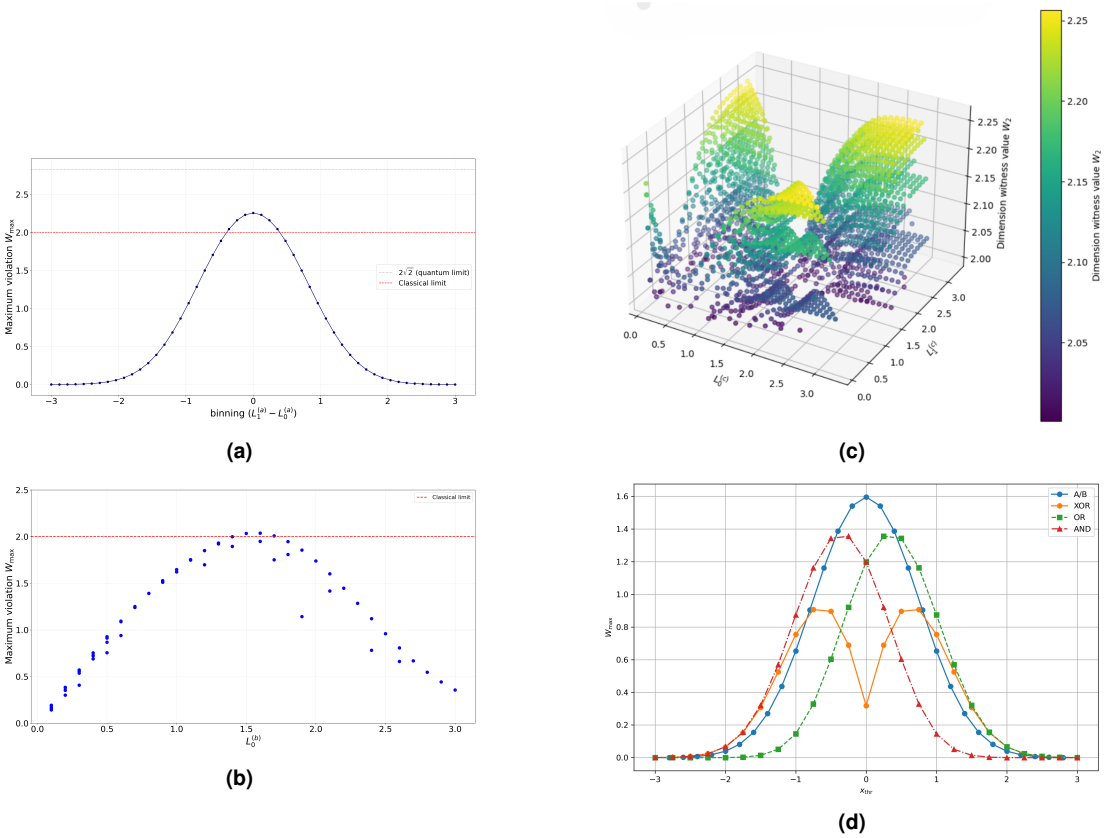

Figure 4. Maximum dimension witness W_2 for each measurement configuration. (a) Single-partition homodyne: $W_{\max}$ vs. offset $L_1^{(a)} - L_0^{(a)}$; optimum at symmetric bisection ($W_{\max} \approx 2.25$). (b) Two-partition alternating (101/010): peak near $L_0^{(b)} \approx 1.5$ does not surpass (a). (c) Three-partition: maximum $W_2 \approx 2.25$ (yellow) at vanishing central widths. (d) Heterodyne: $W^{\max}$ vs. threshold x_{thr} for strategies A, B (single quadrature) and XOR, OR, AND (logic gates); no strategy yields a violation.

5. Conclusion

We have investigated coherent detection schemes in prepare-and-measure scenarios for certifiable QRNG via dimension witnesses. For homodyne detection, we established binning strategies mapping continuous outcomes into binary classifications and found that the maximum witness violation ($W_2 \approx 2.25$) is universally achieved by symmetric single-partition binning across one-, two-, and three-partition configurations.

Notably, the certified violation ($W_2 \approx 2.25$) attains approximately 35% of the quantum-classical gap (classical bound $W_2 = 2$, quantum maximum $W_2 = 2\sqrt{2}$), demonstrating that dimension witness violation, and therefore certified quantum randomness, is achievable using coherent detection. Heterodyne detection, explored as a complementary coherent scheme, yielded no witness violation under any output-combination strategy, indicating that simultaneously accessing both quadratures confers no advantage within the present binning framework. These properties are especially attractive for practical network security infrastructure, where simple, low-loss optical components are desirable.

Acknowledgements

This work has been fully funded by the project "Certificação de Aleatoriedade Quântica" supported by QuIIN – Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, with financial resources from the PPI IoT/Manufatura 4.0 of the MCTI grant number 053/2023, signed with EMBRAPII.

References

Acín, A. and Masanes, L. (2016). Certified randomness in quantum physics. *Nature*, 540(7632):213–219.

Agresti, I. et al. (2020). Experimental device-independent certified randomness generation. *Communications Physics*, 3(1):110.

Alves, M. et al. (2025). Semi-device-independent randomness certification on discretized continuous-variable platforms. *arXiv:2511.05672 [quant-ph]*.

Bassham, L. E. et al. (2010). A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical Report SP 800-22, NIST.

Bowles, J., Quintino, M. T., and Brunner, N. (2014). Certifying the dimension of classical and quantum systems in a P&M scenario. *Physical Review Letters*, 112(14):140407.

Brunner, N. et al. (2008). Testing the dimension of Hilbert spaces. *Physical Review Letters*, 100(21):210503.

Brunner, N. et al. (2014). Bell nonlocality. *Reviews of Modern Physics*, 86(2):419–478.

Cheng, J. et al. (2024). Semi-device-independent QRNG with a broadband squeezed state of light. *npj Quantum Information*, 10(1):20.

Gallego, R., Brunner, N., Hadley, C., and Acín, A. (2010). Device-independent tests of classical and quantum dimensions. *Physical Review Letters*, 105(23):230501.

Gerry, C. C. and Knight, P. L. (2023). *Introductory Quantum Optics*. Cambridge Univ. Press.

Hensen, B. et al. (2015). Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686.

Herrero-Collantes, M. and Garcia-Escartin, J. C. (2017). Quantum random number generators. *Reviews of Modern Physics*, 89(1):015004.

ID Quantique. Samsung Galaxy Quantum 5: quantum security in your pocket. `https://idquantique.com`. Accessed: Jul. 2025.

Johnston, D. (2018). *Random Number Generators: Principles and Practices*. De Gruyter.

Li, H.-W. et al. (2011). Semi-device-independent random-number expansion without entanglement. *Physical Review A*, 84(3):034301.

Ma, X. et al. (2016). Quantum random number generation. *npj Quantum Information*, 2(1):1–9.

Mannalatha, V., Mishra, S., and Pathak, A. (2023). A comprehensive review of quantum random number generators. *Quantum Information Processing*, 22(12):439.

Pivetta, M. (2024). Quantum startup develops random-number generator used in lottery. *Revista Pesquisa FAPESP*, (339).