Verification of qRNG Using qGAN and Classification Models

Hubert Kołcz [1] Tushar Pandey [2] Yug Shah [3]

[1]Warsaw University of Technology, Poland [2]Texas A&M University, the United States [3]University of Toronto, Canada

Abstract

The study presents a multi-modal framework for quantum Random Number Generator (qRNG) verification, integrating quantum Generative Adversarial Networks (qGANs) with classical machine learning. Benchmarking IBM Qiskit simulations against Rigetti Aspen-M-3 (80 qubits) and IonQ Aria-1 (25 qubits) hardware, we analyze CHSH game scores (Rigetti: 0.8036, IonQ: 0.8362) and gate fidelities (Rigetti: 93.6% vs. IonQ: 99.4% two-qubit fidelity). Three parallel methods are developed:

(a) A neural network classifier (58.7% accuracy in quantum-state discrimination);
(b) Markov chain-enhanced logistic regression identifying bit biases (59% '1' frequency in Type 2 vs. 54% in Types 1/3);
(c) A 12-qubit qGAN quantifying distribution similarity via relative entropy (near-zero) and discriminator loss (3.7–16).

Results show hybrid models enable platform-agnostic validation, with IonQ's higher-fidelity systems yielding superior certifiable randomness despite lower qubit counts, while classical simulators exhibit predictable biases.

Introduction

qRNGs exploit intrinsic quantum uncertainty to produce true randomness. The shot noise limit imposes a fundamental constraint on quantum measurements quality, particularly in Bell tests, where photon-counting statistics introduce statistical fluctuations that reduce the maximum achievable score below its theoretical quantum mechanical limit of $2\sqrt{2} \approx 2.72$ for maximally entangled states [2]. For this reason, a CHSH game was introduced as a way to certify quantum devices, where S-value above 2 confirms non-local origin of generated numbers.

In contrast to established qRNGs, emerging quantum platforms like KwanTeach[5] or Low-cost Home-based Quantum Computer[4] require robust verification protocols to assess quantum mechanical nature of their outputs. For these uncertified RNG devices, comprehensive benchmarking - including statistical tests batteries (e.g. NIST, Dieharder) is essential to uncover potential implementation flaws, classical noise contamination, or biases that could compromise randomness. The drawback of these assessment methods is their statics nature, what might not follow potential regressions in once certified devices. In the age of AI, the more dynamic tooling may be designed to monitor a device capabilities to generate random numbers, and guide potential tuning. For this reason, this study focuses on exploring ML methods, with emphasis on qGANs as relevant judge of entropy assessment.

Datasets

With the proposed approach, we tackled 6000 rows of 100-bit entries, each classified as one of the configurations presented in the table 1. The Bell value in a single trial i and the CHSH game value are defined as following, where $\frac{3}{4}$ is the classical threshold.

$$J_i = \begin{cases} 1, & \text{if } x_i \oplus y_i = a_i b_i \\ 0, & \text{otherwise} \end{cases} \qquad J = \frac{1}{n}\sum_{i=1}^{n} J_i - \frac{3}{4}$$

	IBM Qiskit Simulator	Rigetti Aspen-M-3	IonQ Aria-1
Qubit Technology	Classical simulation	Superconducting	Trapped Ion
Qubit Count	Flexible	80	25
CHSH Game Score	Ideal (1.0)	0.8036	0.8362
2-Qubit Fidelity (%)	Ideal (100)	93.6	99.4
Connectivity	User-defined / full	Local, limited	All-to-all

Table 1. Summary of characteristics and benchmarking metrics for benchmarked platforms [1].

Methods

Our methodology integrates qGANs and classical machine learning to verify qRNG outputs across multiple hardware platforms [3]. Figure 1 presents entropy scores between tested qRNGs results.

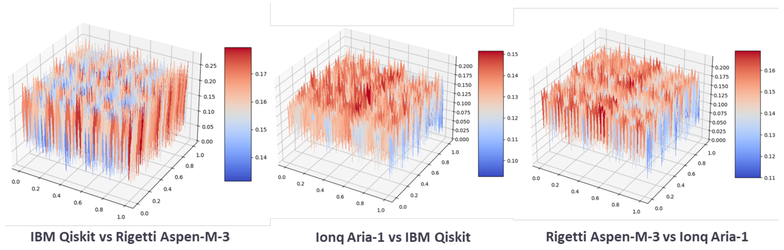

Figure 1. Entropy analysis for the evaluated quantum hardware platforms.

Method	Accuracy (%)	KL Divergence	p-value
Baseline (Dorahacks)	54.00	–	–
NN (batch=16, split=3:1)	54.80	1.1	–
Logistic (split=7:3)	56.10	–	–
NN (batch=8, split=4:1, L1 Reg.)	58.67	0.75	–
qGAN (Set 1 vs 2)	–	3.7	0.01
qGAN (Set 2 vs 3)	–	17	0.01
qGAN (Set 1 vs 3)	–	16	0.01

Table 2. Performance comparison of quantum-classical verification methods. The hybrid approach shows improvement over baseline DoraHacks models.

Our methodology combines quantum generative adversarial networks (qGANs) with classical machine learning to verify quantum randomness generation. Key components include:

- **Neural Network Classifier:** PyTorch-based feedforward architecture (100-bit input, 30/20-neuron hidden layers, ReLU, dropout 0.2) achieving 58.7% accuracy in device identification through statistical pattern recognition.
- **Markov Chain-Enhanced Logistic Regression:** Combines sequential dependency analysis with logistic regression, detecting hardware-induced biases.
- **Quantum GAN Verification:** 12-qubit architecture quantifies distribution similarity through relative entropy (KL divergence <0.1) and discriminator loss metrics (3.7-17), with Variational Quantum Eigensolver as presented on figure 2.

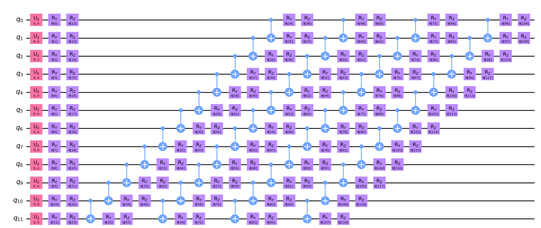

Figure 2. Variational Quantum Eigensolver within qGAN model [6]

New Metric for qRNG Verification: qGAN Training Dynamics

We introduce a novel metric for qRNG validation based on the dynamics of qGAN model training. Specifically, we analyze generator and discriminator loss curves, as well as the convergence of relative entropy, to assess the quality and unpredictability of the generated random numbers.

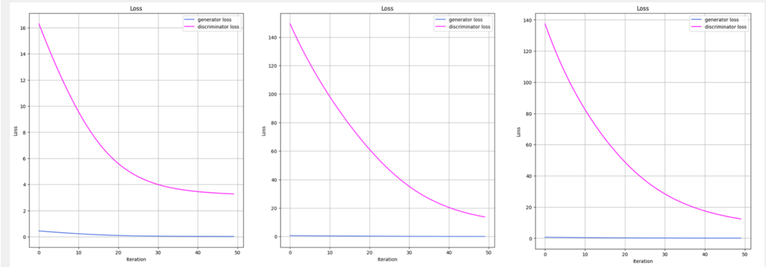

Figure 3. Representative learning curves from qGAN training. The stability and convergence behavior of generator/discriminator losses and relative entropy serve as quantitative indicators of data randomness.

Conclusion

DI-QRNG ensures that the generated numbers are completely independent of the measurement devices used to obtain them-so if a device is distinguishable, it means that the given number sequence is not device-independent. This study aimed to examine methods that can challenge certification, as well as guide changes in devices that are still in the certification stage. The classifier being developed may also be used as a module in an existing solution, the so-called "randomness extractor". The results of this study show that distinguishing qRNG devices based on entropy measures and entropy learning ratio is possible with the use of QML methods, and therefore, these methods open the way to use that metric as a guide for device tuning.

Acknowledgment

We want to thank Yale University and DoraHacks for organising the YQuantum 2024 hackathon, where this project was developed using the datasets provided by the organisers, as well as prof. Teodor Buchner and prof. Jerzy Balicki from Warsaw University of Technology for consultations on RNG and qGAN.

References

[1] DoraHacks Global. Quantum randomness generator, 2023. URL `https://github.com/dorahacksglobal/quantum-randomness-generator`.

[2] Jungwon Kim, Changmin Ahn, and Hubert Kołcz. Stabilization of 10-GHz micro-combs for stable soliton pulse generation. Warsaw, Poland, June 2024. MIRAQLS. Poster presentation.

[3] Hubert Kołcz, Tushar Pandey, Yug Shah, Amala Nikitha George, and Anya Kondamani. Noise vs randomness. `https://dorahacks.io/buidl/11295`, 2025. Accessed: 2025-05-12.

[4] Hubert Kołcz, Gabriela Przybyła, Paweł Rukat, Filip Łabaj, and Piotr Maruszak. Low-cost, home-made quantum computer. 2025.

[5] KWAN-TEK. Kwanteach: Quantum physics education platform, 2024.

[6] Christa Zoufal, Aurelien Lucchi, and Stefan Woerner. Quantum generative adversarial networks for learning and loading random distributions. *npj Quantum Information*, 5:103, 2019.