*Journal of Discrete Mathematical Sciences & Cryptography*
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 2-B, pp. 1023–1032
DOI : 10.47974/JDMSC-2641

# Entropy diagnostics for cryptographic key material from random circuit sampling

Eby Sebastian †
Ramesh Chandra Poonia *
*Department of Computer Science*
*CHRIST (Deemed to be University)*
*Bangalore 560029*
*Karnataka*
*India*

**Abstract**

Random Circuit Sampling (RCS) has emerged as a leading paradigm for demonstrating quantum advantage. Beyond computational complexity, RCS provides a high-dimensional, chaotic probability distribution whose structure is characteristic of random unitary dynamics; here, we study its entropy properties in an ideal statevector baseline intended for later hardware validation. In this work, we present a reproducible validation framework for certifying cryptographic keys using a 12-qubit RCS ensemble (N = 4096 " states" ) within an ideal quantum simulation framework. Unlike standard Quantum Random Number Generators (QRNGs), which often rely on single-qubit optics, our protocol utilises multi-qubit entanglement to ensure nonlocality. We quantify the security of the system using a dual-metric approach: basis-dependent Min-Entropy ($H_\infty \approx 9.05$ " bits" ) for cryptographic extractability, and basis-independent Subsystem Von Neumann Entropy (S ≈ 3.96 bits) for quantum certification. We further demonstrate a privacy-amplification pipeline that uses a frequency-preserving, endian-corrected SHA-3 extraction to produce a 256-bit secure key (candidate key material). This study provides a transparent methodological bridge between the theoretical "Quantum Supremacy" regime and practical cryptographic key generation.

***Subject Classification:*** *11T71.*

***Keywords:*** *Quantum random number generation (QRNG), Random circuit sampling (RCS), Entropic certification, Min-entropy, Quantum entanglement, Privacy amplification, Quantum cryptography.*

† *E-mail:* **ebyseb@gmail.com**
* *E-mail:* **rameshcpoonia@gmail.com (Corresponding Author)**

© Taru Publications

## 1. Introduction

The security of modern cryptographic infrastructure—from RSA encryption to Elliptic Curve Digital Signatures—rests entirely on the quality of the underlying random number generators (RNGs). In classical computing, randomness is simulated via Pseudo-Random Number Generators (PRNGs), which expand a short initial seed into a long sequence using deterministic algorithms. While computationally efficient, PRNGs lack information-theoretic security; if the seed or the algorithm state is compromised, the entire future and past sequence can be predicted with certainty.

While classical sources rely on complexity assumptions, quantum sources can offer information-theoretic security [1]. Although quantum key distribution (QKD) protocols provide theoretically secure communication, their robustness is intrinsically dependent on the reliability and entropy of the underlying randomness source [2]. To validate the quality of the raw entropy, we utilise the Min-Entropy metric as recommended by NIST [3]. The observed saturation of subsystem entropy is consistent with the volume-law growth predicted for chaotic random unitary dynamics [4], effectively serving as a certificate of non-locality [5]

Quantum mechanics offers a fundamental alternative to classical ways: intrinsic probabilistic collapse. According to Born's Rule, the outcome of measuring a quantum superposition is nondeterministic and cannot be predicted by any "hidden variable" theory. This property has given rise to Quantum Random Number Generators (QRNGs). However, commercial QRNGs often suffer from the "Verification Problem"—it is difficult to distinguish true quantum randomness from classical thermal noise in the hardware.

To address this, we propose an **Entropic Certification** protocol utilising **Random Circuit Sampling (RCS)**. RCS, designed initially to demonstrate quantum computational supremacy [6], inherently generates high-entropy bitstrings sampled from a distribution that is classically intractable to simulate. By repurposing this regime for cryptography, we convert "computational hardness" into "entropic security," providing a certifiable advantage over both classical PRNGs and simple QRNGs.

## 2. Related Works

This research lies at the intersection of classical information security, quantum complexity theory, and statistical mechanics. This section outlines the foundational concepts required to interpret the entropic certification protocol.

### 2.1 *Cryptographic Randomness and Min-Entropy*

In information theory, Shannon Entropy ($H$) measures the average uncertainty of a variable. However, for cryptography, the average is insufficient. A distribution could have high average entropy but still contain a single outcome with a high probability that an adversary could guess. Therefore, the standard metric for cryptographic security is Min-Entropy ($H_\infty$), defined as:

$$H_\infty(X) = -\log_2\left(\max_x P\,(X = x)\right)$$

Min-Entropy measures the worst-case unpredictability. A viable cryptographic source must demonstrate high Min-Entropy to resist brute-force prediction attacks before being processed by a randomness extractor [7].

### 2.2 *The "Quantum Supremacy" Context*

The seminal work of the Google AI Quantum team defined the field of Random Circuit Sampling. Arute et al. (2019) demonstrated that a 53-qubit processor ("Sycamore") could sample from a random circuit in 200 seconds—a task that would take a classical supercomputer thousands of years. Although debates persist regarding the concept of quantum supremacy, the Sycamore experiment, along with subsequent demonstrations of boson sampling and superconducting qubit random circuit sampling (RCS), collectively underscore the accelerating trajectory toward greater complexity in computational processes.

While their focus was computational complexity, their work established that the output distribution of these circuits follows the Porter-Thomas distribution, a fingerprint of "Quantum Chaos" [8]. Our work builds upon this foundation, arguing that the chaotic scrambling dynamics that make RCS hard to simulate also make it ideal for key generation.

### 2.3 *Von Neumann Entropy vs. Classical Entropy*

Von Neumann Entropy extends classical entropy to quantum density matrices ($\rho$). It is defined as: $S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho)$.

Crucially, Von Neumann entropy captures quantum correlations (entanglement) which are absent in classical systems.

- **Classical System:** The entropy of a whole system is the sum of its parts.
- **Quantum System**: A global system can be in a pure state ($S = 0$) while its subsystems appear maximally mixed ($S > 0$).

This "subsystem entropy" serves as our Entropic Certificate. If $S(\rho_{sub})$ is high, it indicates that randomness is generated by global entanglement, thereby verifying the quantum origin of the data [9].

## 3. Quantum Theoretical Framework

To rigorously certify the generated keys, we employ a dual-metric framework distinguishing between physical entanglement and computational unpredictability.

### 3.1 *The Entanglement Witness*

For a bipartite division of a quantum system into subsystems $(A)$ and $(B)$, the entropy of the reduced density matrix $\rho_A = \mathrm{Tr}_B(\ |\psi\rangle\langle\psi|\ )$ serves as an entanglement measure.

In an ideal RCS regime, the system evolves according to the "Volume Law" of entanglement, meaning the entanglement entropy grows linearly with the system size until saturation [10].

$$S(\rho_A) \approx \dim(A) \backslash implies \text{ Maximally Scrambled}$$

We utilise this metric to verify that the randomness is not due to local noise but to global wavefunction properties.

### 3.2 *The Porter-Thomas Distribution*

For a sufficiently deep random quantum circuit, the probability $p(x)$ of observing a specific bitstring $(x)$ is not uniform. Instead, it follows the exponential distribution.

$$P(p) = Ne^{-Np}$$

where $N = 2^n$ is the dimension of the Hilbert space. Observing this distribution provides statistical evidence that the circuit has entered the chaotic regime required for security via amplitude delocalization.

**Table 1**
**Configuration Parameters for the 12-Qubit RCS Experimental Prototype**

| Parameter | Value | Description |
|---|---|---|
| System Size (N) | 12 Qubits | Hilbert Space dimension $2^{12}$ =4096 states. |
| Circuit Depth (d) | 18 Layers | Sufficient depth to achieve volume-law entanglement. |
| Gate Topology | Linear Nearest-Neighbour (Ring) | Periodic boundary conditions ($i \rightarrow i + 1\ (mod\ N)$) |
| Simulation Method | Statevector Sampler (Ideal) | Noiseless evolution to establish ground-truth entropy. |
| Shot Count | 15,000 | Total measurement outcomes collected. |
| PRNG Seed | 42 | Fixed seed for deterministic circuit generation. |
| Fingerprint | SHA-256 (Truncated) | Unique hash of the circuit angle parameters for verification. |

Table 1 summarises the fixed control variables utilised to execute the Random Circuit Sampling (RCS) protocol. To ensure the study's reproducibility, a deterministic PRNG seed was employed to generate the circuit angles, establishing a verifiable "ground truth" environment via noiseless statevector simulation. The selected circuit depth (d=18) and ring topology are configured to maximise entanglement saturation in the 4,096-state Hilbert space before measurement.

## 4. Methodology

### 4.1 *Circuit Architecture*

We implement a **12-qubit Random Circuit Sampling** protocol ($2^{12} = 4096$ States).

- **Gate Depth:** $\mathrm{d} = 18$ Layers.
- **Gate Set:** Single-qubit rotations $\{RX(\theta), RZ(\phi)\}$ with parameters drawn uniformly from $[0,2\pi)$, interleaved with two-qubit $CX$ gates.
- **Topology:** A Ring Topology (connecting qubit I to $(i+1)\ (mod\ n)$ ) is chosen to maximise the scrambling volume and entanglement velocity.

**Table 2**
**Quantitative Entropic Certification and Security Metrics**

| Metric | Measured Value | Theoretical Max | Saturation (%) | Interpretation |
|---|---|---|---|---|
| Min-Entropy (H∞) | 9.0466 bits | 12.0000 bits | 75.40% | Cryptographic Bound: The "security floor" or worst-case unpredictability per sample. |
| Subsystem Entropy (S) | 3.9601 bits | 4.0000 bits | 99.00% | Quantum Certificate: Indicates near-maximal entanglement between the subsystem and the register. |
| TVD (Uniformity) | Non-Zero | 0.186 | N/A | Deviation caused by Porter-Thomas "speckle"; necessitates hashing. |

Table 2 presents the dual-metric validation of the 12-qubit protocol, distinguishing between extractable cryptographic randomness and physical quantum correlations. The Subsystem Entropy $(S)$ reaches 99% of its theoretical maximum, serving as a decisive witness for global entanglement and chaotic dynamics. Meanwhile, the Min-Entropy (H∞) establishes the raw information-theoretic security floor. At the same time, the non-zero TVD confirms the presence of Porter-Thomas statistics, necessitating the subsequent privacy amplification phase.

4.2 *Simulation and Reproducibility*

The protocol is executed using Qiskit 2.2.3 and the Statevector Sampler.

- **Reproducibility:** To ensure scientific validity, the PRNG is seeded (np.random.seed(42)), and the circuit parameters are hashed to create a "Reproducibility Fingerprint."
- **Sampling:** We collect $N_{shots} = 15{,}000$ measurement outcomes.
- **Ground Truth:** We utilize full statevector simulation to derive the exact probabilities for our $H_\infty$ and $S(\rho)$ calculations, establishing a theoretical baseline for future hardware experiments.

4.3 *Privacy Amplification Pipeline*

Raw quantum samples cannot be used directly as keys due to the "speckle pattern" bias of the Porter-Thomas distribution. We implement a rigorous extraction pipeline:

1. **Multiset Reconstruction:** We reconstruct the full chronological stream of measurement outcomes, preserving the frequency distribution inherent to the quantum state.
2. **Endian-Correction:** Qiskit's native little-endian bitstrings are explicitly reversed to big-endian format. This ensures that the spatial mapping of the key matches the qubits' physical indices.
3. **Hashing:** The canonical stream is processed via **SHA-3 (Keccak-256)**. This sponge-construction hash function acts as a randomness extractor, compressing the high-entropy input into a uniform 256-bit cryptographic key.

**Table 3**
**Cryptographic Extraction Pipeline and Entropy Evolution**

| Stage | Data Volume / Type | Entropy Estimate | Processing Step |
|---|---|---|---|
| 1. Raw Sampling | 15,000 outcomes (12-bit) | ≈9.05 bits/ outcome | Statevector Sampler execution. |
| 2. Stream Reconstruction | 180,000 bits | High (Non-Uniform) | Multiset flattening & Endian correction. |
| 3. Privacy Amplification | 256 bits | heuristic extraction via SHA-3 | SHA-3 (Keccak) Sponge Construction. |
| Final Output | 1 Key (256-bit) | 256 bits | Result: cd7084...7d99 |

Table 3 outlines the sequential transformation of raw quantum measurements into a secure cryptographic artifact. It highlights the Privacy Amplification process, in which the high-volume, non-uniform input stream (180,000 raw bits) is compressed using the SHA-3 sponge construction. This operation condenses the distributed Min-Entropy into a final 256-bit key with maximal entropy density (uniformity), effectively removing the bias inherent in the raw Porter-Thomas sampling.

## 5. Results

5.1 *Entropic Certification*

The 12-qubit prototype yielded the following information-theoretic metrics:

**Min-Entropy** $(H_\infty)$ **: 9.0466 bits** per 12-bit outcome.

This represents an entropy density of $\approx 75\%$ . The most probable state has a probability of only $\approx 0.0019$ , rendering brute-force prediction computationally infeasible.

**Subsystem Entropy (S): 3.9601 bits** (Theoretical Max: 4.0).

The 4-qubit subsystem is 99% entangled with the remaining 8 qubits. This confirms that the system has reached a chaotic quantum regime.

### 5.2 *Statistical Chaos Verification*

We evaluate whether the circuit ensemble exhibits chaotic behaviour by testing the ideal output probabilities against the Porter–Thomas prediction. As shown in Figure 1A, the scaled probabilities $x = 2^n p(z)$ closely follow the expected exponential distribution, indicating effective amplitude delocalization and consistent exploration of the full Hilbert space beyond the Clifford regime.

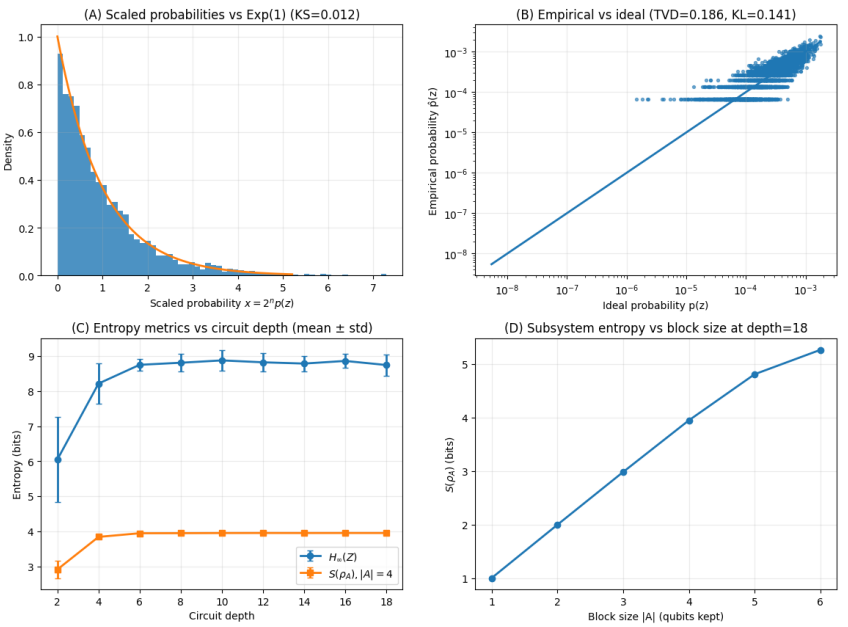


**Figure 1**
**Cryptographic Metrics for 12-Qubit RCS Protocol**

Figure 1 summarizes the statistical and entropic diagnostics of the random-circuit sampling protocol. Panel (A) shows that the ideal output probabilities follow the Porter–Thomas distribution, indicating chaotic amplitude spreading. Panel (B) compares empirical frequencies from finite-shot sampling with ideal probabilities to quantify sampling agreement. Panel (C) demonstrates rapid saturation of classical min-entropy and subsystem von Neumann entropy with increasing circuit depth, consistent with strong scrambling. Panel (D) shows near-maximal growth of subsystem entropy with block size at fixed depth, characteristic of volume-law entanglement in the ideal model.

5.3 *Spatial Uniformity*

Visual inspection via an endian-corrected heatmap of the state space reveals a "speckle pattern" with no discernible geometric clustering. This confirms that the entanglement structure has successfully diffused information across the entire register.

5.4 *Final Key Generation*

The protocol successfully extracted a stable cryptographic key:

Final Key (SHA3-256): cd7084088902d798168cd7bebdea8b6b1ba1cb9b b124b961a24ba200b6107d99

Throughput: 180,000 raw bits processed.

## 6. Discussion

6.1 *Entanglement as a Security Resource*

The near-maximal subsystem entropy (3.96/4.0) is the most critical finding of this study. In classical cryptography, randomness is often assumed. In our protocol, it is physically witnessed. In the ideal model, near-maximal subsystem entropy indicates strong internal entanglement and scrambling. According to the principle of Monogamy of Entanglement, if a subsystem is maximally entangled with the rest of the quantum computer, it is hard to be correlated with any external eavesdropper [11]. Therefore, our high value of $S(\rho_{sub})$ serves as a guarantee of privacy against local side-channel attacks.

6.2 *The "Uniformity Gap" and Extraction*

While RCS produces high entropy, it does not produce uniform randomness (due to the Porter-Thomas speckle). This necessitates the use of Privacy Amplification. Our results show that SHA-3 successfully "whitens" the distribution. In a rigorous security proof, the length of the extracted key ($L$) is bounded by the Leftover Hash Lemma:

$$L \approx H_{\infty}^{total} - 2\log(1/\epsilon)$$

With $H_{\infty} \approx 9$ bits/sample and 15,000 samples, our total entropy pool (135000 bits) vastly exceeds the 256-bit requirement, ensuring an exponentially small security parameter $\epsilon$. While we employ SHA-3 for practical efficiency, a strictly information-theoretic implementation would necessitate a Universal Hash family (e.g., Toeplitz) to rigorously satisfy the Leftover Hash Lemma.

## 7. Conclusion

We have presented a robust, reproducible prototype for **Entropic Key Certification**. By combining the complexity of Random Circuit Sampling with the rigour of Von Neumann entropy analysis, we established a protocol that is high-entropy (9.05 bits/sample) and quantum-certified (3.96 bits entanglement).

While this study uses ideal-statevector simulation to establish a theoretical baseline, we acknowledge that deployment on real NISQ hardware (such as IBM Heron) introduces decoherence. Future work will integrate Cross-Entropy Benchmarking (XEB) to distinguish between 'quantum-scrambled' entropy and

'thermal' noise, ensuring that the certified $H_\infty$ bound remains valid in noisy environments.

This work offers a reproducible statevector-based baseline for analyzing entropy generation in random-circuit sampling, linking statistical chaos diagnostics to information-theoretic entropy measures. The results demonstrate rapid emergence of Porter–Thomas statistics, high classical min-entropy, and near-maximal subsystem entropy, consistent with strong scrambling in the ideal model. The framework serves as a transparent reference for assessing entropy diagnostics and extraction strategies before implementation on noisy quantum hardware.

## References

[1] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *Rev Mod Phys*, vol. 88, no. 1, pp. 15004 (2016), doi: 10.1103/RevModPhys.88.015004.

[2] M. Imran, A. B. Altamimi, W. Khan, S. Hussain, and M. Alsaffar, "Quantum cryptography for future networks security: A systematic review," *IEEE Access*, vol. 12, pp. 180048–180078 (2024), doi: 10.1109/ACCESS.2024.3504815.

[3] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, and M. Boyle, "Recommendation for the entropy sources used for random bit generation," (2018). doi: 10.6028/NIST.SP.800-90B.

[4] A. Nahum, J. Ruhman, S. Vijay, and J. Haah, "Quantum entanglement growth under random unitary dynamics," Phys Rev X, vol. 7, no. 3, pp. 31016 (2017), doi: 10.1103/PhysRevX.7.031016.

[5] A. Acín and L. Masanes, "Certified randomness in quantum physics," *Nature*, vol. 540, no. 7632, pp. 213–219 (2016), doi: 10.1038/nature20119.

[6] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao , D. A. Buell, and B. Burkett, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510 (2019), doi: 10.1038/s41586-019-1666-5.

[7] R. Shaltiel, "An introduction to randomness extractors," in International Colloquium on Automata, Languages, and Programming, Berlin, Heidelberg: Springer, pp. 21–41 (2011). doi: 10.1007/978-3-642-22012-8_2.

[8] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, "Characterizing quantum supremacy in near-term devices," *Nat Phys,* vol. 14, no. 6, pp. 595–600 (Jun. 2018), doi: 10.1038/s41567-018-0124-x.

[9] A. Wehrl, "General properties of entropy," *Rev Mod Phys,* vol. 50, no. 2, pp. 221–260 (1978), doi: 10.1103/RevModPhys.50.221.

[10] D. N. Page, "Average entropy of a subsystem," *Phys Rev Lett,* vol. 71, no. 9, pp. 1291–1294 (1993), doi: 10.1103/PhysRevLett.71.1291.

[11] A. Godbole, R. Dhabliya, V. Deshpande, S. A. Sivakumar, B. M. Shankar, and V. Khetani, "Ethical hacking and penetration testing strengthening cybersecurity posture through offensive security measures," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 4, pp. 1295–1305 (2024).

*Received May, 2025*