quantropi

Quantropi TRNG

Closing the entropy gap: True randomness for the post-quantum security era

The Challenge: Strong Security Requires Strong Entropy

As the world prepares for the post-quantum era, cryptographic systems are evolving to resist quantum attacks. Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and next-generation secure protocols all rely on one critical foundation – high-quality randomness.

Every secure system — from encryption keys and digital signatures to authentication tokens and secure communications — depends on true entropy. If the random source is biased, predictable, or degraded, even the strongest cryptographic algorithm can fail.

This creates a critical vulnerability. While new algorithms are being standardized for quantum resistance, many digital systems today still lack reliable, high-quality entropy sources. Without strong randomness, quantum-safe cryptography cannot deliver true security.

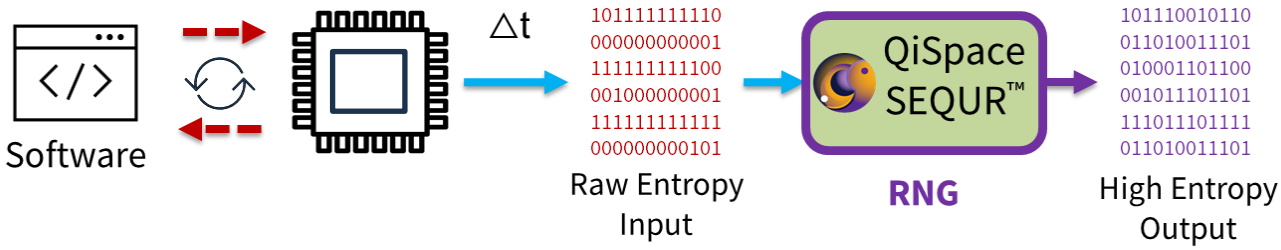
The Solution: True Randomness from Everyday Hardware

Quantropi TRNG closes this entropy gap by transforming everyday digital devices into their own high-quality entropy sources. Recently published in Nature Scientific Reports and Phys. Rev. E, this breakthrough technology extracts true randomness from unpredictable system-level jitter which naturally exist in modern processors and digital systems.

Instead of requiring specialized quantum hardware or external entropy modules, Quantropi TRNG:

- Harvests natural fluctuations already present in computing systems
- Converts them into high-quality true random numbers
- Enables true random number generation from the device itself

This approach provides the strong randomness required for secure cryptography in the quantum era — using the device you already own.



Key Features

True Randomness Without Special Hardware

- No specialized silicon required. Harvests the true randomness that exists on the devices you already own.

Universal Compatibility

- Compatible across Windows, macOS, Linux, ARM, and x86, bringing PQC-ready security to IoT, edge, and cloud environments via a simple integration.

High Performance, Low Overhead

- Lightweight and suitable for embedded systems, IoT devices, and cloud applications.

Drop-In Integration

- Strengthen any cryptographic stack immediately using standard APIs or SDKs to replace or enhance legacy generators

Uniformity and Consistency Across Systems and States

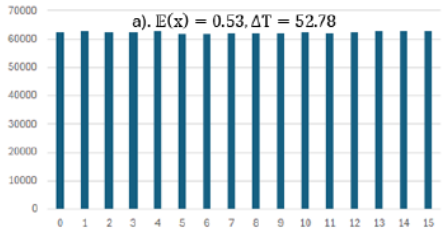
The unpredictability in Quantropi TRNG arises naturally from system-level jitter, a non-deterministic phenomenon shaped by the totality of the system and its environment. However, to satisfy cryptographic requirements it must also exhibit uniform statistical distribution to ensure that no byte value is favored over another.

This shows that Quantropi TRNG can transform the unpredictable system-level jitter into a uniformly random outputs with no detectable skew or structural patterns. The uniformity is governed by the composition law and convergent theorem within the Random Permutation Sorting Stochastic (RPSS) system which forms the foundation of computational jitter modulation mechanism (see Phys. Rev. E 2026).

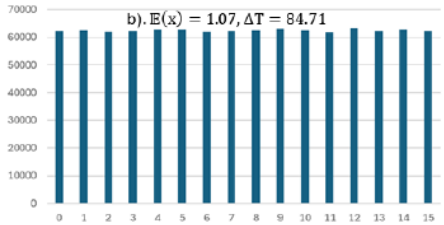
Load Independence: High-grade uniformity is maintained whether the system is Idle, Normal, or Busy. This proves that the entropy source is resilient against CPU workload fluctuations and system noise.

Broad Compatibility: Identical results are observed across the entire spectrum of hardware, from simple Cortex-M0+ and M33 cores to high-performance Cortex-M7 and SAMV71 systems.

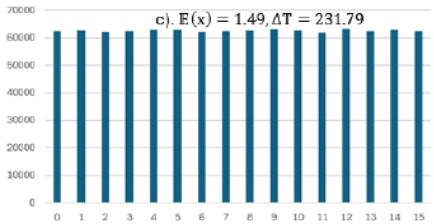
No Specialized Hardware: By extracting the true randomness that already exists in the system, robust security is achieved on even the simplest MCU architectures without the need for specialized hardware.



(a) Near idle



(b) Normal



(c) Busy

Reliability at Scale

Large-scale testing confirms that as sample size increases, the system's performance converges with theoretical perfection. Even over 100 million samples, the quality of randomness remains indistinguishable from the mathematical ideal.

Sustained Security: Consistent results over large datasets ensure that the entropy source does not degrade or become predictable during extended operation.

Exceeding Standards: The system consistently meets and exceeds the stringent "Min-Entropy" bounds required for modern cryptographic security.

Empirical Validation: These results provide real-world proof that the underlying theory translates perfectly into reliable, high-grade security on physical hardware.

Sample Size (Bytes)	Shannon (bits/byte)	Min-Entropy (bits/byte)	χ^2 –	π –	Mean –	Corr. –
1M	7.9998006	7.941	276.6	3.13458	127.50	0.000025
10M	7.9999782	7.980	273.0	3.14273	127.50	0.000391
100M	7.9999969	7.991	260.2	3.14199	127.49	0.000118
Theoretical Limit	8.000000	7.932	255	3.14159	127.50	0.0