QUANTINUUM
QUANTUM ORIGIN

BEYOND STATISTICAL TESTING:

From Hope to Certainty in Cryptographic Randomness

ABSTRACT

Quantum Origin enables a fundamental shift in cryptographic security: from statistical testing to mathematical proof. Leveraging quantum processes verified through Bell tests and strong randomness extractors, it delivers randomness with provable quality. This paper explains how quantum physics enables a mathematical proof of randomness quality, how mathematical theory makes this practical for deployment, and how software-based implementation transforms accessibility of quantum-enhanced security.

Introduction

Cryptography has long accepted a fundamental limitation: **the impossibility of proving randomness quality.** Statistical testing can detect obvious flaws but cannot guarantee the absence of exploitable patterns, forcing cryptographic systems to operate on statistical hope rather than mathematical certainty[1].

Recent breakthroughs in quantum computing have made it practical to generate and deliver randomness whose quality can be mathematically proven from its origin, rather than statistically estimated at the output. This enables a shift from hoping randomness is secure to knowing it is.

While our Technical Whitepaper[2] details the foundational challenges of classical randomness, this paper expands on how Quantum Origin delivers provable quantum randomness through quantum physics, Bell test verification, and strong randomness extractors. The approach enables operational properties that redefine what's possible with traditional approaches: seeds that can be public without compromising security, systems that never require seed rotation, and software-based deployment delivering quantum-enhanced security without requiring continuous access to quantum hardware.

For cryptographers and security professionals trained in classical methods, understanding these quantum capabilities is essential for navigating the evolving security landscape. This paper bridges that knowledge gap, explaining how mathematical proof transforms both the theory and practice of cryptographic randomness.

1. SP 800-22 and GM/T 0005-2012 Tests: Clearly Obsolete, Possibly Harmful, 169.pdf
2. Quantum Origin Technical White Paper: Technical Whitepaper

SECTION 1

The Limits of Classical Randomness

Establishing trust in the randomness derived from classical physical processes presents fundamental and well-documented challenges for cryptography.

The Verification Problem in Cryptographic Randomness

The core challenge for cryptographers isn't merely generating randomness, but establishing confidence in its quality. The lack of testability creates a problem: the systems we rely on for security lack security proofs at their foundation.

Statistical testing—the standard approach to randomness verification—cannot provide absolute guarantees about unpredictability or randomness quality, as acknowledged by NIST[3].

Consider This: While obvious RNG failures can be detected by standard tests, adversarial biases specifically designed to evade detection may require an impractically large number of samples to uncover. For example, detecting a subtle single-bit bias designed to pass standard tests could require up to 4.9×10^{25} samples—taking billions of years to collect at gigabit speeds[4]. Yet these small biases can still be exploited by attackers who know they exist—as in lattice sieving attacks on ECDSA signatures that exploit biased nonces[5].

3. https://csrc.nist.gov/pubs/sp/800/90/b/final (Sections 4.1, 1.1)
4. This estimate is from Table 1 in Quantum Origin Technical Whitepaper. The table illustrates the practical limits of statistical detection for subtle, adversarially chosen biases.
5. For example, lattice sieving attacks against ECDSA signatures exploit biased nonces and passed statistical tests. See Breitner & Heninger, 'Biased Nonce Sense: Lattice Attacks against Weak ECDSA Signatures in Cryptocurrencies,' IACR ePrint 2019/023

The Trust and Supply Chain Challenge

Classical randomness generation and traditional hardware-based QRNGs introduce additional trust requirements beyond statistical verification. Organizations must trust:

1. **Hardware manufacturers and their setup procedures**
2. **Supply chain integrity throughout component production**
3. **Ongoing device health and calibration maintenance**
4. **Absence of backdoors or compromised components**
5. **Environmental stability and proper operating conditions**

These trust dependencies create multiple failure points. Research from KeyFactor[6] revealed that 1 in 172 public-facing RSA certificates contain keys weak enough to be broken by today's classical computers. These vulnerabilities often stem from insufficient entropy during key generation—a problem that cannot be retrospectively detected through statistical methods alone.

The Epistemological Challenge

This presents a fundamental question: how can we know that randomness is sufficient for cryptographic purposes without the ability to prove it? This core limitation means cryptographic systems must operate without certainty about their randomness quality.

What cryptographers need is a different approach: randomness whose quality can be mathematically proven at the point of generation rather than statistically estimated from outputs. This distinction represents **the difference between hoping a system is secure and knowing it is.**

6. https://www.keyfactor.com/blog/the-irony-and-dangers-of-predictable-randomness/

SECTION 2

The Quantum Origin Approach

Quantum physics and mathematics offers a different path to randomness generation that avoids classical constraints such as deterministic processes, statistical verification limitations, and supply chain trust requirements. Quantum Origin leverages the intrinsic unpredictability of quantum mechanics to provide mathematically provable randomness with guaranteed quality rather than statistical estimates.

Overcoming Classical Limitations

Quantum Origin represents a departure from traditional randomness generation. Unlike classical physics, quantum physics is non-deterministic. You can prepare a quantum system that behaves unpredictably, even with complete knowledge of the system state. No amount of computational power—classical or quantum—can predict the output with certainty. This unpredictability forms the foundation of Quantum Origin's approach.

For more than twenty years, vendors of quantum random number generators (QRNGs) have attempted to produce high-quality cryptographic randomness from quantum effects. However, these approaches have faced significant limitations for three key reasons:

Inability to isolate quantum randomness from classical noise sources, resulting in output that isn't pure quantum randomness

Reliance on statistical tests to verify randomness quality, which cannot provide guarantees of unpredictability

Hardware-based deployment models that require specialized equipment at each point of use, limiting scalability and introducing supply chain trust dependencies

Quantum Origin overcomes these limitations through an approach that required the breakthrough capabilities of Quantinuum's quantum computers[7]— among the first systems stable and precise enough to execute Bell tests at the scale and reliability necessary to generate our Quantum Seeds for commercial cryptographic applications.

7. https://www.quantinuum.com/blog/setting-the-benchmark-independent-study-ranks-quantinuum-1-in-performance

Quantum Seed Generation

At the core of Quantum Origin is the "Quantum Seed"—a mathematically verified random string of bits with provable quality. This Quantum Seed is not simply claimed to be random; its randomness is demonstrably proven through techniques derived from quantum information theory.

The generation process involves three distinct stages:

1. **Quantum Circuit Execution**
   The quantum computer executes millions of three-qubit circuits, first preparing entangled quantum states and then performing measurements on each qubit. This step can be viewed as a challenge-response protocol, where the challenges are measurement settings for each circuit and the responses are the measurement outcomes.

2. **Bell Test Verification**
   A type of Bell test[8], known as a Mermin game[9], is used to determine the quality of the randomness. Bell tests are fundamental experiments in quantum mechanics—the subject of Nobel Prize-winning[10] physics—that prove the non-local nature of quantum entanglement. By comparing the challenges and responses, a mathematical lower bound on randomness quality is established. This provides rigorous mathematical proof, not a statistical estimate. Typically, this proven quality level is around 85% of theoretical maximum, which is known in cryptography as min-entropy (0.85 on a scale of 0 to 1.0).

3. **Bias Refinement**
   In the final processing step, the response data is distilled to produce the Quantum Seed, which has near-perfect min-entropy. The mathematical proof underlying this process has a protocol security parameter of 2^{-128}, which means an adversary's chance of distinguishing the output from perfectly uniform randomness is vanishingly small (less than 1 in 340 trillion trillion trillion trillion). This process uses a specialized form of randomness extraction that can produce output with proven quality, but only if the min-entropy of the source is known. Since we have a rigorous lower bound from the Bell test, the output quality is mathematically guaranteed.

The result is approximately 8 kilobytes of provably high-quality random data that forms the Quantum Seed.

The Bell Test Advantage

The use of Bell tests to verify randomness represents a fundamental departure from statistical testing approaches. A Bell test doesn't merely check if the output "looks random" according to statistical patterns; it verifies the underlying quantum process itself. When a quantum system violates a Bell inequality, it mathematically proves that the outcomes cannot be predetermined—they must contain genuine randomness.

8. https://plato.stanford.edu/entries/bell-theorem/
9. https://en.wikipedia.org/wiki/Mermin%27s_device
10. https://www.nobelprize.org/prizes/physics/2022/summary/

SECTION 3

The Unique Properties of the Quantum Seed

The mathematically proven Quantum Seed unlocks three operational properties impossible with traditional approaches:

1. Security that doesn't depend on the seed's own secrecy
2. An unlimited operational lifespan without the need for replacement
3. The ability to use the same seed across multiple, independent systems.

Security That Doesn't Depend on Seed Secrecy

Perhaps the most significant property enabled by the Quantum Seed is that security does not depend on the seed's confidentiality. Strong randomness extractors ensure that knowledge of the Quantum Seed doesn't help an adversary predict the extraction output. The extractor output remains statistically independent of the seed, making confidentiality unnecessary for security.

However, the local randomness source enhanced by the extraction process must remain private to maintain security. This local source provides the private component necessary for security, while the Quantum Seed's proven quality ensures provably random output. Thus, even if the Quantum Seed were to become known to an adversary, the security of Quantum Origin's output would remain intact. By contrast, exposure of traditional cryptographic seeds is catastrophic.

While the Quantum Seed's unique properties eliminate traditional seed secrecy requirements, Quantum Origin follows standard security practices in operations. The Quantum Seed is generated using quantum computers in secure U.S. facilities, and distribution follows robust security protocols, including digital signing.

Unlimited Operational Lifespan

The Quantum Seed never needs to be replaced. Unlike traditional cryptographic seeds that must be regularly refreshed to maintain security, the Quantum Seed has an unlimited operational lifespan.

The randomness extractor used with Quantum Origin allows for 2^{300} uses of each Quantum Seed. To put this number in perspective, 2^{300} is larger than the estimated number of atoms in the observable Universe. It is impossible for an attacker to capture and store that many outputs for analysis in any deployment scenario.

Single Seed Across Multiple Systems

The same Quantum Seed can be used across multiple systems simultaneously without compromising security. Each system must have its own independent local randomness source. With this requirement met, Quantum Origin can be deployed across any number of systems without security degradation.

MATHEMATICAL GUARANTEES IN PRACTICE

Technical Property		Practical Implication
Extractor output is independent of the Quantum Seed	→	Adversaries cannot predict randomness even with seed knowledge
Repeated use does not reduce security	→	One seed secures unlimited systems for their entire operational life
Output quality depends on local source and proven seed quality	→	Local sources need only basic functionality; quantum seed ensures strong output

SECTION 4

The Role of Strong Randomness Extractors

Randomness extractors are mathematical algorithms that transform weak randomness into strong, cryptographically secure randomness. Quantum Origin uses a specific type called a "strong randomness extractor" that combines two inputs: the proven Quantum Seed and a private local randomness source.

This combination yields a powerful result: provably random output that significantly elevates the local source's quality alone.

The Critical Distinction: Public Seed, Private Source

The Quantum Seed can be public without compromising security—a property impossible with traditional cryptographic seeds. However, the local randomness source must remain private to the system using it. This local source provides the confidentiality component, while the Quantum Seed provides the proven quality component.

Software Deployment Without Hardware Dependencies

Traditional quantum random number generators require specialized hardware at every deployment point because they can't separate randomness generation from usage. Quantum Origin breaks this constraint by performing quantum randomness generation once to create the Quantum Seed, then using software-based extraction at deployment points.

The quantum computer interaction happens only during Quantum Seed creation, when Bell tests and bias refinement are executed on Quantinuum's systems. After this one-time process, Quantum Origin operates entirely through software, enabling deployment on any device without network connections or additional hardware.

This separation of randomness seed generation and usage delivers unprecedented scalability. Organizations can deploy quantum-enhanced randomness across thousands of systems using software installation—no specialized hardware, no network dependencies, no ongoing service connections required.

CONCLUSION

From Statistical Hope to Mathematical Certainty

Quantum Origin represents a fundamental departure from the statistical assumptions that have constrained cryptographic randomness for decades. Three advances make this transformation possible:

1. **Quantum Physics:** Bell tests executed on quantum computers leverage physics to provide mathematical proof of randomness quality, moving beyond statistical estimation to physical verification.
2. **Mathematical Foundation:** Decades of research on randomness extractors now enable the use of proven quantum seeds to enhance local randomness sources, delivering high-quality randomness through software deployment.
3. **Software Implementation:** The combination of quantum physics and mathematical advances enables high-quality randomness in an easily deployable software package, making provable randomness broadly accessible.

This shift from assumption to proof addresses a core vulnerability in modern cryptography. As quantum threats intensify and security requirements evolve, establishing cryptographic systems on mathematically verified foundations becomes not just advantageous, but essential.