The Quantum Threat to Mobile Communications

Why Physics-Based Entropy is Essential

for Secure Communications in a Post-Quantum World

A Technical White Paper by Real Random LLC

October 2025

Executive Summary

The cryptographic foundation of mobile security depends entirely on the unpredictability of random numbers. When randomness fails, everything fails.

Mobile devices are the primary communication tools for intelligence professionals, military personnel, corporate executives, and billions of consumers. Yet the random number generators that underpin mobile cryptography are fundamentally vulnerable to both current and emerging threats. As quantum computing advances from laboratory demonstrations to practical capability, the window for securing communications infrastructure is closing rapidly.

This white paper examines why traditional mobile entropy sources are inadequate for high-security applications and explains how physics-based random number generation provides quantum-secure protection. Real Random's technology has achieved an 88% entropy strength rating on NIST Statistical Test Suite testing with 0.999996 bits per byte entropy, independently validated by Rochester Institute of Technology, demonstrating that true randomness is not just theoretical but a practical, measurable reality.

Key Findings

- Mobile hardware RNGs are vulnerable to supply chain attacks, state-level backdoors, and side-channel exploitation
- Algorithmic random number generators (PRNGs) are fundamentally deterministic and breakable with sufficient computational power
- Quantum computers will decrypt communications secured with compromised entropy sources, retroactively exposing data encrypted today
- Physics-based entropy from macroscopic physical processes provides verifiable randomness immune to computational attacks
- Real Random has achieved 88% NIST entropy strength rating with 0.999996 bits per byte, independently validated by Rochester Institute of Technology
- Enterprise adoption of quantum-secure entropy is economically viable today through Entropy-as-a-Service models

The Entropy Problem in Mobile Security

Every cryptographic operation begins with random numbers. Key generation, session tokens, initialization vectors, nonces, and salts all require unpredictable values. If an attacker can predict these values, the entire cryptographic system collapses regardless of algorithm strength or key length.

Mobile devices face unique entropy challenges. Unlike server environments with access to hardware noise sources and entropy pooling from diverse system events, mobile devices operate in constrained environments with limited entropy sources. Battery optimization requirements discourage continuous sensor polling, and hardware design choices prioritize cost and power efficiency over cryptographic perfection.

Current Mobile Entropy Sources

Hardware Random Number Generators

Modern mobile processors include hardware random number generators (HWRNGs) based on thermal noise, oscillator jitter, or quantum effects in semiconductors. While these provide high-quality randomness under normal conditions, they suffer from critical vulnerabilities for high-security applications.

Supply Chain Risks

Hardware RNGs are black boxes manufactured by semiconductor vendors in global supply chains spanning multiple countries. Intelligence agencies have documented capabilities to introduce backdoors during chip design or fabrication. The 2013 Dual_EC_DRBG backdoor in random number generation, allegedly compromised by the NSA, demonstrates that even standardized cryptographic components can contain deliberate weaknesses.

Side-Channel Attacks

Hardware RNGs can be compromised through power analysis, electromagnetic emanations, or timing attacks. Academic research has demonstrated practical attacks against commercial hardware RNGs by manipulating environmental conditions (temperature, voltage) or observing physical side channels during operation. Mobile devices in hostile environments cannot guarantee physical security.

Verification Challenges

Unlike software where source code can be audited, hardware RNG implementations are proprietary and opaque. Organizations must trust vendor claims about randomness quality without independent verification capability. This trust model is unacceptable for intelligence and national security communications.

Pseudorandom Number Generators

Software-based PRNGs use deterministic algorithms to generate sequences that appear random. Even cryptographically secure PRNGs (CSPRNGs) like AES-CTR-DRBG or HMAC-DRBG are fundamentally predictable if the internal state is compromised or if the seed entropy is weak.

The Determinism Problem

PRNGs produce infinite output from finite internal state. This mathematical impossibility of true randomness means that with sufficient computational power, PRNG output becomes predictable. Quantum computers will dramatically reduce the computational cost of breaking PRNG-based cryptography, making systems secured with algorithmic randomness vulnerable to future attacks.

State Compromise

If an attacker gains access to PRNG internal state through memory dumps, debugging interfaces, or side-channel attacks, all future and potentially past output becomes predictable. Mobile operating systems face persistent threats from malware, OS vulnerabilities, and physical device compromise that can expose PRNG state.

The Quantum Computing Threat

> **Harvest now, decrypt later: Adversaries are collecting encrypted communications today to decrypt when quantum computers become available.**

Cryptographically Relevant Quantum Computers

Quantum computers exploit superposition and entanglement to perform certain calculations exponentially faster than classical computers. Shor's algorithm, demonstrated in principle on small systems, can factor large numbers and compute discrete logarithms efficiently, breaking RSA and elliptic curve cryptography that secure most internet communications.

While fully fault-tolerant quantum computers capable of breaking 2048-bit RSA don't yet exist, intelligence community assessments suggest this capability may emerge within 10-15 years. Organizations protecting information with longer secrecy requirements must act now, as encrypted communications captured today will be vulnerable to future quantum decryption.

The Entropy Connection

Quantum computing's threat to cryptography has focused primarily on algorithm vulnerabilities, leading to the development of post-quantum cryptographic algorithms. However, quantum computers will also accelerate attacks on weak entropy sources in three critical ways:

1. PRNG State Recovery

Quantum algorithms like Grover's search reduce the computational cost of brute-forcing PRNG internal states. A PRNG with 128-bit internal state, considered classically secure, offers only 64-bit quantum security. PRNGs used in mobile cryptography become tractable targets for well-resourced quantum adversaries.

2. Weak Seed Detection

If initial PRNG seeding uses insufficient entropy, quantum computers can more efficiently search the seed space. Mobile devices booting in controlled environments may have predictable system state at initialization, creating exploitable weakness in the entropy pool foundation.

3. Retroactive Decryption

Even if post-quantum algorithms protect the cryptographic primitive, weak entropy in key generation undermines the entire system. A 256-bit post-quantum key generated from 64 bits of actual entropy provides only 64 bits of security, regardless of algorithm strength.

Physics-Based Random Number Generation

True randomness comes from physics, not mathematics. Physical processes provide verifiable unpredictability immune to computational attacks.

The Physics Foundation

True random number generators extract entropy from physical processes governed by fundamental uncertainty. Unlike algorithmic approaches constrained by deterministic logic, physical entropy sources tap into irreducible randomness in nature.

While quantum phenomena offer the purest randomness, macroscopic physical processes also provide high-quality entropy that resists both classical and quantum computational attacks. The key requirement is that the physical process has sensitivity to initial conditions and environmental factors that cannot be fully controlled or predicted, even with complete knowledge of system design.

Real Random's Physical Dice Approach

Real Random generates entropy using physical dice tumbling in viscous fluid, captured by high-speed computer vision. View the demonstration video here, https://youtu.be/yUK2AawDbUU

This approach combines several advantages:

Macroscopic Chaos

Dice tumbling exhibits chaotic dynamics with extreme sensitivity to initial conditions. Microscopic variations in dice surface properties, fluid turbulence, and launch conditions create unpredictable outcomes that cannot be simulated even with detailed system knowledge. The entropy emerges from classical physics at scales far removed from quantum effects, providing robustness against quantum computational attacks.

Visual Verifiability

Unlike semiconductor noise sources or radioactive decay, dice tumbling is directly observable and recordable. Organizations can audit the physical process, verify mechanical design, and confirm that entropy extraction doesn't introduce backdoors. This transparency addresses supply chain concerns inherent in hardware RNGs.

Multi-Dimensional Entropy

Computer vision extracts entropy from dice position, orientation, rotation speed, trajectory, and inter-dice collisions. Multiple independent entropy sources combine to provide redundancy and high bitrate generation. Real Random systems have achieved 0.999996 bits of entropy per output byte in independent testing, with an 88% NIST Statistical Test Suite entropy strength rating validated by Rochester Institute of Technology.

No Quantum Vulnerability

Quantum computers offer no advantage in predicting macroscopic mechanical systems governed by chaotic fluid dynamics. The computational complexity of simulating turbulent flow and multi-body collisions exceeds quantum computational capabilities. Physical dice entropy remains secure in a post-quantum world.

Entropy Source Comparison

Characteristic	Mobile HWRNG	PRNG	Physical TRNG
Supply Chain Risk	High	Low	None
Quantum Resistance	Unknown	Vulnerable	Immune
Verifiability	Opaque	Auditable	Transparent
Side-Channel Risk	High	Medium	Low
True Randomness	Yes	No	Yes
Mobile Deployment	Native	Native	API/Network

Implementing Quantum-Secure Mobile Entropy

Entropy-as-a-Service Architecture

Traditional approaches require organizations to deploy and maintain physical random number generation hardware. This creates operational complexity, capital expense, and expertise requirements that limit adoption. Entropy-as-a-Service delivers quantum-grade randomness through secure APIs, making physics-based entropy accessible to any mobile application.

Key Architectural Components:

- **Physical Generation Layer:** Redundant dice tumbling systems in secure data centers
- **Quality Assurance:** Real-time NIST statistical testing ensures entropy quality
- **Secure Distribution:** TLS 1.3 with perfect forward secrecy protects entropy in transit
- **Client Integration:** Drop-in SDK replacement for standard random functions
- **Entropy Pooling:** Client-side buffering enables offline operation and reduces latency

Security Considerations

Transport Security

Entropy delivered over TLS 1.3 benefits from authenticated encryption and perfect forward secrecy. Even if long-term server keys are compromised, previously delivered entropy remains secure. Certificate pinning prevents man-in-the-middle attacks that could substitute predictable data for true randomness.

Hybrid Architecture

Best practice combines physics-based network entropy with local hardware RNG output using entropy combiners. Even if one source is compromised, security degrades gracefully rather than failing catastrophically. This defense-in-depth approach provides maximum assurance for critical communications.

Audit and Compliance

All entropy requests are logged for security audit and compliance verification. Organizations can demonstrate use of certified entropy sources for regulatory requirements. Real-time monitoring detects anomalies in entropy quality or delivery patterns that might indicate attacks.

High-Value Use Cases

Intelligence Community Communications

Classified information has secrecy requirements extending decades. Current mobile cryptography using hardware RNGs or PRNGs cannot guarantee security against future quantum attacks or undisclosed current vulnerabilities. Intelligence professionals require provable quantum-secure entropy for communications and data protection that must resist nation-state adversaries with advanced capabilities.

Military Tactical Communications

Mobile devices in combat zones face hostile electronic warfare environments and physical capture risks. Communications secured with hardware-dependent entropy sources are vulnerable to supply chain compromise and device-specific attacks. Physics-based entropy delivered through secure networks eliminates device-specific vulnerabilities and provides uniform security across heterogeneous mobile fleets.

Executive Communications

Corporate executives discussing mergers, acquisitions, financial results, or strategic plans require communications security that matches classified government standards. Business intelligence has decades-long value, making harvest-now-decrypt-later attacks economically viable. Quantum-secure mobile entropy protects executive communications against both current and future threats.

Healthcare and Legal Communications

HIPAA and attorney-client privilege create legal requirements for protecting sensitive communications. Healthcare and legal information has long-term value and permanence, making it attractive for patient harvesting attacks. Professional obligations and regulatory compliance drive adoption of verifiably secure entropy sources.

Economic Analysis

Cost-Benefit Assessment

Quantum-secure entropy represents incremental security enhancement over standard mobile cryptography. Organizations must evaluate costs against potential breach consequences and regulatory requirements.

Direct Costs

Entropy-as-a-Service pricing scales with consumption:

- Consumer tier: $4.99-$9.99 per user per month
- Professional tier: $19.99 per user per month
- Enterprise tier: Volume-based pricing starting at $10,000 monthly

Integration costs are minimal with SDK providing drop-in replacement for standard random functions. Development effort typically ranges from 8-40 hours depending on application complexity.

Risk-Adjusted Benefits

Breach consequences vary by industry and data sensitivity:

- **National Security:** Intelligence compromise costs measured in strategic disadvantage and lives
- **Financial Services:** Average data breach cost $5.9M (IBM 2024), regulatory penalties, customer churn
- **Healthcare:** HIPAA violations $50,000 per record, reputation damage, patient trust loss
- **Enterprise:** Intellectual property theft, competitive disadvantage, shareholder litigation

Quantum-secure entropy provides insurance against future cryptographic breaks at a fraction of potential breach costs. For organizations with long-term data protection requirements, the risk-adjusted ROI strongly favors proactive adoption.

Competitive Differentiation

Security-conscious customers increasingly demand quantum-secure communications. Mobile security applications that implement physics-based entropy can market quantum-grade protection as a premium feature, differentiating from competitors using standard cryptography. This positioning resonates particularly well with government, defense, financial services, and healthcare buyers who understand cryptographic risks.

Recommendations

Immediate Actions

- **Assess Current Entropy Sources:** Audit mobile applications to identify reliance on hardware RNGs or PRNGs for cryptographic operations

- **Evaluate Quantum Risk:** Determine data secrecy requirements and harvest-now-decrypt-later exposure
- **Pilot Integration:** Deploy physics-based entropy in development environments to validate performance and compatibility
- **Update Security Architecture:** Incorporate quantum-secure entropy into security roadmaps and compliance frameworks

Long-Term Strategy

- Adopt hybrid entropy architecture combining network-delivered physics-based randomness with local hardware sources
- Implement entropy quality monitoring and audit logging for compliance verification
- Plan migration to post-quantum algorithms in conjunction with quantum-secure entropy adoption
- Educate stakeholders about quantum threats and the distinction between post-quantum algorithms and quantum-secure entropy

Conclusion

> **Quantum-secure communications require quantum-secure randomness. The time to act is now, before quantum computers make today's encrypted communications readable.**

Mobile communications security stands at a critical juncture. Quantum computing advances from theoretical possibility to practical threat, while mobile devices proliferate as the primary communication tools for sensitive conversations. The cryptographic foundation of mobile security depends entirely on randomness quality, yet current entropy sources face fundamental vulnerabilities.

Physics-based random number generation offers verifiable quantum-secure entropy that resists both current and future attacks. Real Random's dice-based approach combines macroscopic physical chaos with visual transparency, achieving an 88% NIST entropy strength rating with 0.999996 bits per byte entropy - independently validated by Rochester Institute of Technology and comparable to established commercial TRNG services.

Organizations protecting communications with long-term secrecy requirements must act before quantum computers become operational. Harvest-now-decrypt-later attacks mean that waiting is not an option. Entropy-as-a-Service makes quantum-secure randomness economically viable and operationally simple, enabling immediate deployment without capital investment in physical infrastructure.

The choice is clear: upgrade to quantum-secure entropy now, or accept that today's encrypted mobile communications will become readable in the quantum future.

About Real Random

Real Random LLC is a quantum-secure cryptography company based in Marco Island, Florida. Founded on patented physical random number generation technology, Real Random delivers physics-based entropy to intelligence community clients and security-conscious enterprises worldwide.

Recognition

Gartner Cool Vendor in Data Security 2025

Technology Portfolio

6 granted U.S. patents

36 total patent rights across 10 countries

Contact Information

Real Random LLC
Marco Island, Florida
www.realrandom.com
info@realrandom.com