A logo of a science company

AI-generated content may be incorrect.

# Simulated Quantum Entropy Fusion

## Comprehensive Random Number Generator Performance Comparison

Developer: Luminareware LLC Date: 8/8/2025

Patent Status: USPTO applications pending (19/198,077 and 19/267,394)

Document Version: 1.0

#### Overview

This document presents a comparative analysis of Luminareware's SQEF (Simulated Quantum Entropy Fusion) system relative to established random number generation technologies. SQEF performance metrics are based on empirical testing, while comparison systems are evaluated using published specifications and manufacturer documentation.

#### SQEF Two-Stage Architecture Performance

SQEF employs a two-stage cryptographic architecture with configurable security levels:

##### Stage 1 - Master Generation:

* Each seed expands via SHA3-256 based on security level:
  + STANDARD: 1:512 expansion per seed
  + ENHANCED: 1:128 expansion per seed
  + MAXIMUM: 1:32 expansion per seed
* Larger masters use multiple seeds (e.g., 4GB = 8 seeds at STANDARD)
* Measured: 1.92 MB/s for 512MB master generation (STANDARD security)

##### Stage 2 - Key Slicing:

* Extracts keys from pre-computed masters at 273 MB/s
* All sliced keys maintain 7.96-7.99 bits/byte entropy

This architecture enables high-throughput key delivery by amortizing the computational cost of entropy generation across millions of derived keys, with security level selection based on application requirements.

#### Comparative Performance Analysis of Random Number Generation Systems

##### **Important Note**: Performance metrics for SQEF are based on empirical testing conducted on Intel Core i9 hardware with 128GB RAM. All other systems' metrics are derived from manufacturer specifications, published documentation, or academic literature. Direct performance comparisons should consider that these systems were not tested under identical conditions.

##### Software RNGs (CPU-based)

| **RNG Type** | **Speed** | **Keys/ms (256-bit)** | **vs SQEF** |
| --- | --- | --- | --- |
| **SQEF** | **273 MB/s** | **9,943** | **Baseline** |
| Mersenne Twister | 500 MB/s | 15,625 | 1.6x faster |
| PCG | 2 GB/s | 62,500 | 6.3x faster |
| xoshiro256++ | 3 GB/s | 93,750 | 9.4x faster |
| ChaCha20 | 2-3 GB/s | 78,125 | 7.9x faster |
| AES-CTR (with AES-NI) | 10-15 GB/s | 390,625 | 39x faster |

##### Hardware RNGs

| **RNG Type** | **Speed** | **Keys/ms (256-bit)** | **vs SQEF** |
| --- | --- | --- | --- |
| Intel RDRAND | 500 MB/s - 3 GB/s | 15,625-93,750 | 1.6-9.4x faster |
| Intel RDSEED | 100-500 MB/s | 3,125-15,625 | 0.3-1.6x |
| VIA Padlock | 30 MB/s | 937 | 0.09x slower |
| TPM 2.0 | 1-10 MB/s | 31-312 | 0.003-0.03x slower |
| USB Hardware RNG | 1-100 Mbps | 4-390 | 0.0004-0.04x slower |
| PCIe RNG Card | 1-10 Gbps | 3,906-39,062 | 0.4-4x |

##### Quantum RNGs

| **QRNG Type** | **Speed** | **Keys/ms (256-bit)** | **vs SQEF** |
| --- | --- | --- | --- |
| ID Quantique | 4-16 Mbps | 16-62 | 0.002-0.006x slower |
| QuintessenceLabs | 1 Gbps | 3,906 | 0.4x slower |
| NIST Quantum RNG | 8.5 Gbps | 33,203 | 3.3x faster |
| Cambridge QRNG | 1-10 Gbps | 3,906-39,062 | 0.4-4x |
| Research QRNGs | Up to 100 Gbps | 390,625 | 39x faster |

##### Cloud RNG Services

| **Service** | **Typical Throughput** | **Keys/ms (256-bit)** | **vs SQEF** |
| --- | --- | --- | --- |
| AWS KMS | 10-50 keys/sec | 0.01-0.05 | 200,000x slower |
| Google Cloud KMS | 100 keys/sec | 0.1 | 100,000x slower |
| Azure Key Vault | 10-20 keys/sec | 0.01-0.02 | 500,000x slower |
| Cloudflare (API) | 1000 req/sec | 1 | 10,000x slower |

#### Test Environment and Empirical Results

##### SQEF Testing Configuration

* Processor: Intel Core i9 with 128GB RAM
* Operating System: Windows 11

##### Master Seed Generation (Actual Test Log):

* Target Size: 512MB (536870912 bytes)
* Security Level: STANDARD (1:512 expansion ratio)
* Generation Duration: 266.350 seconds
* Generation Throughput: 1.92 MB/s
* Method: SQEF quantum-mimicry with SHA3-256 expansion
* Security Margin: >2^123 operations against SHA3-256

##### Testing Methodology Notes

¹ SQEF Two-Stage Performance:

* Master Generation: 1.92 MB/s measured for 512MB master seed generation with STANDARD security (1:512 expansion ratio)
* Key Slicing: 273 MB/s measured when extracting cryptographic keys from pre-computed master seeds
* This architecture amortizes generation cost: one 512MB master provides millions of high-entropy keys at memory speeds

² SQEF Entropy Measurements:

* Master seeds consistently achieve >7.99 bits/byte
* Sliced keys measure 7.96-7.99 bits/byte through NIST SP 800-90B assessment
* Min-entropy validated using NIST EA tools on actual generated output

³ NIST SP 800-22 Results: All 33 SQEF configurations tested with 188 individual statistical tests per configuration. Pass rates: 98.40%-100%.

⁴ NIST SP 800-90B Validation: 100% IID compliance achieved across all tested configurations.

⁵ PRNG Limitations: Pseudorandom generators produce deterministic output. Performance figures represent published benchmarks. Entropy quality not applicable.

⁶ Hardware RNG Specifications: Based on manufacturer documentation. These systems were not independently tested in this evaluation.

##### Key Technical Observations

1. Two-Stage Architecture Advantage: SQEF's design separates computationally intensive entropy generation (1.92 MB/s) from high-speed key delivery (273 MB/s), enabling both high entropy quality and practical throughput.
2. Amortized Generation Cost: A single 512MB master seed (taking ~4.4 minutes to generate) can provide millions of cryptographic keys instantly through deterministic slicing.
3. Entropy Preservation: Keys sliced from master seeds maintain cryptographic quality (7.96-7.99 bits/byte) as validated through NIST testing.
4. Hardware Independence: Unlike Intel RDRAND/RDSEED or quantum devices, SQEF operates on any standard processor without specialized hardware.
5. Practical Deployment: Pre-computed master seeds enable instant key availability for time-critical applications while maintaining quantum-comparable entropy quality.

#### Operational Comparison

| **Use Case** | **SQEF Approach** | **Traditional RNG** | **Advantage** |
| --- | --- | --- | --- |
| Bulk Key Generation | Pre-compute masters, slice on demand | Generate each key individually | 142x faster delivery |
| Real-time Applications | Slice from cached masters (273 MB/s) | Wait for generation | Instant availability |
| Air-gapped Systems | Generate masters offline, deploy | Requires local RNG hardware | Software-only solution |
| Cloud Deployments | Distribute master seeds securely | API calls with latency | No network dependency |

#### Conclusion

SQEF's two-stage architecture provides a unique solution to the entropy generation challenge: achieving quantum-comparable quality (7.96-7.99 bits/byte) while enabling practical deployment through pre-computed master seeds. The measured performance demonstrates both the thoroughness of entropy generation (1.92 MB/s for masters) and the efficiency of key delivery (273 MB/s for slicing), validated through comprehensive NIST testing.

*Note: This comparison presents SQEF empirical test results alongside published specifications for other systems. Only SQEF underwent actual testing in our laboratory environment. Performance metrics reflect actual measured results on Intel Core i9 processor with 128GB RAM.*