Your Encryption Has an Expiration Date

QSPARC Labs

www.qsparclabs.com

Harvest Now, Decrypt Later

The Reality

Foreign adversaries are collecting your encrypted data **today**: classified communications, defense secrets, satellite transmissions.
Waiting for quantum computers to break it.

- Quantum computers **will** break RSA and ECC, the foundation of current encryption
- Every secure transmission is being recorded for future decryption
- Long-lived platforms (satellites, defense systems) cannot be upgraded after deployment
- NIST recognized the urgency: new post-quantum standards released 2024

The window to protect long-term secrets is closing.

Most “Quantum-Resistant” Algorithms Have Already Failed

The Failures

SIKE: Broken within weeks of NIST selection

CRYSTALS-Kyber: Side-channel vulnerabilities expose keys

Rainbow: Broken by classical computers

The Survivor

McEliece: 47 years unbroken

But there’s a problem:

Large public keys, too large for satellites and constrained systems

The QSPARC Answer

McEliece security.

Smaller keys.

47 years of proven security, now compact enough for any platform.

McEliece Security at a Fraction of the Size

- ✓ Satellite-ready key sizes
- ✓ Low-bandwidth handshakes
- ✓ McEliece-level security
- ✓ Proven mathematical foundation

Why this matters:

- **Fits on satellites** and bandwidth-constrained devices
- **Faster key exchanges**: reduced handshake latency
- **No security compromise**: same 47-year proven foundation

QSPARC CN: Early Engineering Signals

Directional, **non-optimized** measurements from a reference implementation (laptop-class CPU).

Public Key Size (128-bit security, order-of-magnitude)

- Classic McEliece: **250–300 KB**
- **QSPARC CN: 30–40 KB**
- HQC: **2–3 KB**

Approximately 10× smaller than McEliece; intentionally larger than HQC.

Decapsulation Behavior (Observed)

- Deterministic decoding (no probabilistic retries)
- Naturally parallelizable component decoding
- Single-digit millisecond decapsulation in a **non-optimized** build

QSPARC CN is a quasi-cyclic, decoding-based construction inspired by Can–Naig. Results shown are directional, not optimized benchmarks.

Engineered for Zero Surprises

No Random Failures

Deterministic decryption: every operation succeeds predictably, not probabilistically. Defense systems need certainty, not “usually works.”

Parallel Processing

Scales with modern hardware. GPU-ready architecture for high-throughput environments like data centers and network gateways.

Guaranteed Reliability

Provable failure rate: less than 1 in 2^{128} operations. Not a guess, a mathematical guarantee.

Small enough for satellites. Fast enough for data centers.
Secure enough for decades.

Built for Systems That Cannot Fail

Where cryptographic failure isn't a bug,
it's a national security event.

- **Satellite Operators**: High-latency environments where retransmissions are expensive
- **Defense Contractors**: Platforms that must remain secure for decades
- **Critical Infrastructure**: Systems that cannot be upgraded after deployment

Platforms where replacing encryption is expensive, difficult, or impossible.

Deep Expertise Where It Matters

Mahir Bilen Can, PhD

Co-Founder

70+ publications

Algebraic coding theory

Eli Naig

Co-Founder

PQC system design

Hardware security architecture

Aamon Tate

Partner

Strategic Development

Schedule a Technical Deep-Dive

www.qsparclabs.com | info@qsparclabs.com