INFORMATION-THEORETIC SECURITY VS. COMPUTATIONAL COMPLEXITY

QUANTUM & PQC SECURITY

Quantum Key Distribution, Shor-Resistant Algorithms, and Lattice Cryptography

An axiomatic guide mapping the physical limits of quantum networks against post-quantum mathematical defenses.

1. QUANTUM CRYPTOGRAPHY: PHYSICS-BASED SECURITY

Quantum Cryptography—specifically Quantum Key Distribution (QKD)—relies on the physical laws of quantum mechanics to guarantee information-theoretic security. It ensures that any attempt by an eavesdropper (Eve) to intercept the key introduces detectable disturbance.

The Information Threat Threshold (BB84 Boundary): Alice encodes key bits into non-orthogonal polarization states. Eve's maximum intercepted information is upper-bounded by the Holevo quantity $\chi(E)$. The net lower bound of the secure key rate R relative to the Quantum Bit Error Rate (QBER), denoted as D, maps as:

$$R \geq 1 - 2H_2(D) \qquad \text{where } H_2(D) = -D\log_2(D) - (1-D)\log_2(1-D)$$

The Abort Limit: Setting $R = 0$ yields the ultimate operational security cutoff: $\mathbf{D}_{\text{threshold}} \approx \mathbf{11.0}\%$. If channel noise spikes past 11%, Eve can successfully map the state vector, and the raw string is discarded.

2. THE THREAT PROFILE: WHY CLASSICAL PUBLIC-KEY INFRASTRUCTURE FAILS

Current classical security architectures rely on asymmetric mathematical problems that are too computationally intensive for classical supercomputers. Shor's Algorithm disrupts this scheme by evaluating hidden matrix periods via the Quantum Fourier Transform (QFT).

The Vulnerability Vectors: Shor's algorithm drops sub-exponential problems down to clean polynomial bounds:

Algorithm	Mathematical Problem	Classical Bounds	Shor Quantum Bounds
RSA	Prime Factorization	$\mathcal{O}\left(\exp\left(c\sqrt[3]{\ln M(\ln\ln M)^2}\right)\right)$	$\mathcal{O}((\log \mathbf{M})^{\mathbf{3}})$
ECC / ECDSA	Discrete Logarithms	$\mathcal{O}(\sqrt{p})$	$\mathcal{O}((\log \mathbf{p})^{\mathbf{3}})$

Grover's algorithm also reduces the security of symmetric encryptions (AES) quadratically ($\mathcal{O}(\sqrt{N})$), requiring a migration to 256-bit key standards to maintain a standard 128-bit security floor.

3. POST-QUANTUM CRYPTOGRAPHY (PQC): COMPLEXITY-BASED DEFENSES

Post-Quantum Cryptography (PQC) updates classical software architectures to rely on alternative high-dimensional math problems that lack structured periodic properties, making them immune to Shor's and Grover's algorithms.

LATTICE-BASED CRYPTOGRAPHY: THE ML-KEM/CRYSTALS-Kyber STANDARD

The primary PQC system approved by NIST relies on the computational hardness of the **Learning With Errors (LWE)** problem embedded inside massive n-dimensional vector modules.

The Module LWE Equation: $\vec{b} = \mathbf{A}\vec{s} + \vec{e} \pmod{q}$

The Core Advantage: $\mathbf{A}$ is a public matrix, $\vec{s}$ is the secret vector, and $\vec{e}$ is a small, random error vector. Due to the injection of the noise vector $\vec{e}$, computing $\vec{s}$ given $\vec{b}$ and $\mathbf{A}$ represents a non-linear problem that scales exponentially for both classical and quantum processors.

4. LEADING ARCHITECTURAL FRAMEWORKS IN PQC STANDARDS

Beyond LWE lattices, the global standard cryptographic infrastructure splits into distinct mathematical disciplines to ensure resilient key exchanges and digital signatures:

1. **Stateful Hash-Based Signatures (ML-DSA / CRYSTALS-Dilithium):** Builds authentication tokens using high-dimensional cryptographic hash trees (Merkle Trees). Its security is directly bounded by collision resistance properties, resisting algebraic shortcuts.

2. **Code-Based Cryptography (Classic McEliece):** Encrypts text strings by masking information inside the generator matrices of error-correcting codes (Goppa Codes), introducing random bit flips. Decoding the arbitrary code remains an NP-hard permutation search challenge.
3. **Multi-Variate Quadratic Equations:** Protects validation protocols by mapping security keys to large systems of non-linear multi-variate quadratic polynomials over finite fields, blocking linear matrix factorization routines.