PORTALZ

The Quantum Silence behind the AES Blindspot

"You cannot solve a problem with the same mindset that created it."
— Albert Einstein

NIST PQC does not include AES

- NIST proposed PQC (Kyber, Dilithium) only targets RSA public key exchange.
- NIST does not propose or offer any quantum-safe AES replacement.
- AES remains in CNSA 2.0, despite proof of AES-256 Quantum Key Extraction (QKE).

What We Don't Know

- Was it oversight?
- Was it known and omitted to prevent panic?
- Or because they know there is no PQC AES solution with conventional cryptography?

What We Do Know

- AES is quantum cracked in principle and in practice.
- AES was always interim. It was built on obsolete assumptions in the pre-quantum age.
- QKE bypasses RSA, PQC, TPM and all public-private key layers.
- The military, intelligence, and financial infrastructure of every nation are vulnerable.
- **Quantum DEFCON 3** is active — AES quantum vulnerability known by some agencies.
- **Q-DEFCON 2** is coming — estimated at less than 300 days to active QKE breaches.

What Was Required

- A completely different mindset was required to solve the quantum threat to AES.
- FES, the **Fractal Encryption Standard**—is a new cryptographic foundation.

A shift from:

- - Computational hardness → **Structural Shannon impenetrability**
- - Finite keys → **Infinite OTP compliant fractal streams**
- - Block ciphers → **Whole-of-payload nonlinear transforms**

FES is not an evolution. It is an impenetrable quantum-proof cryptographic paradigm-shift.

DES → AES → FES

- FES transcends AES by engineering infinities, satisfying Shannon's OTP perfect secrecy.
- FES **permanently** replaces the broken AES shield.
- FES restores global security and confidence in the midst of the quantum security storm.
- The only question left is who acts before **Q-DEFCON 1**?

View this document online to navigate links:
https://portalz.solutions/pdf/AES_Blindspot.pdf