Why Kyber Collapses and AES Resists: A Symbolic Cryptanalysis Comparison

QSymbolic Research Team

1. Introduction

The transition to post-quantum cryptography has introduced fundamentally new classes of cryptographic primitives, including lattice-based schemes such as Kyber. These constructions rely on algebraic structures like the Learning With Errors (LWE) problem to provide quantum-resistant security.

At the same time, symbolic entropy-guided models of cryptanalysis—such as the CollapseRAM framework—have emerged to take advantage of structural properties and partial key leakage. In comparative testing, CollapseRAM shows a marked effectiveness against Kyber while demonstrating little utility against AES-256. This document explains the reasons for this contrast and outlines the implications for future cryptanalytic techniques.

2. Structural Comparison of AES-256 and Kyber

2.1. Kyber: A Structured Cryptosystem

Kyber is based on the LWE problem. At its core, Kyber encryption involves solving approximate linear equations:

$$t = A \cdot s + e \mod q$$

Here, A is a public matrix, s is the small secret vector to be recovered, and e is a bounded error vector. This algebraic structure allows for symbolic modeling: each unknown in s can be represented as a symbolic Δ, and CollapseRAM uses entropy convergence to collapse these Δ symbols into actual bit values.

2.2. AES-256: A Nonlinear Permutation Cipher

AES-256 is a symmetric block cipher operating over 14 rounds of nonlinear transformations including S-box substitution, row shifting, column mixing, and key expansion. A small change in the key causes a total change in output—this is the *avalanche effect*. As a result, partial guesses or symbolic approximations yield no useful intermediate signal. Unlike Kyber, AES is intentionally structured to resist approximation and prediction.

3. Symbolic Collapse vs. Brute Force

CollapseRAM is not a brute-force engine. Rather, it collapses symbolic registers (denoted Δ) based on their entropy alignment with observed ciphertexts or residuals. For example, in Kyber, a guess for s produces a prediction of $t' = A \cdot s$, which can be compared to the actual t. The residual $e' = t - t'$ provides a signal that allows CollapseRAM to prune and guide the collapse of unknowns.

In AES, there is no such entropy signal. A wrong key produces an entirely unrelated plaintext. The lack of structure means that no entropy-guided collapse is possible unless the key is exactly correct.

4. Quantitative Observations

In testing, CollapseRAM successfully recovered full Kyber secrets with only 20 unknown Δ bits (out of 64), completing recovery in fewer than one million guesses. This is consistent with side-channel leakage scenarios where some bits of the secret vector are exposed.

By contrast, in AES-256, even recovering 4 unknown bytes (out of 32 total) requires 2^{32} guesses. Moreover, without known plaintext, no entropy signal exists to guide the collapse. Even with known plaintext, the symbolic collapse engine lacks a gradient to follow.

5. Implications for Post-Quantum Cryptography

These results demonstrate that entropy-guided symbolic collapse is viable for cryptosystems that exhibit approximate linearity and bounded error—such as Kyber and other LWE-based schemes. CollapseRAM is especially effective in contexts involving:

- Partial secret leakage (e.g., fault injection, side-channel traces)
- Sparse or ternary key structures
- Systems where residuals can be computed and scored

AES-256 remains secure not just because of its key size, but because of its inherent resistance to approximation. Its nonlinearity, diffusion, and lack of error tolerance make it unsuitable for symbolic collapse models.

6. Conclusion

Symbolic entropy-guided frameworks like CollapseRAM represent a shift in cryptanalysis strategy. Rather than enumerating entire keyspaces, these systems leverage symbolic ambiguity and entropy minimization to recover partial secrets efficiently. Kyber, with its algebraic transparency and bounded error model, is highly susceptible to such attacks when partial information is available. AES-256, with no exploitable structure, continues to resist.

As post-quantum cryptography becomes standardized, understanding which primitives lend themselves to symbolic analysis will be critical. CollapseRAM offers a viable path forward for structured schemes—but highlights the enduring value of unstructured ciphers like AES.