

# Side Channel Analysis of Quantum Secure ML-KEM(CRYSTALS-Kyber)

Priyanshu Raj, Nishant Das, Dishita Tanwar

Team Metamorphosis

Ramanujan College (University Of Delhi)

This work presents a side-channel attack on the CRYSTALS-Kyber (ML-KEM) decapsulation operation using software-simulated power traces. The objective is to recover secret key polynomial coefficients from provided polynomial inputs and corresponding power traces under high-noise conditions. A correlation power analysis (CPA) approach is implemented using a Hamming Weight leakage model targeting the pointwise multiplication in the NTT domain. To improve robustness, the method incorporates leakage localization, multi-window correlation analysis, and stability-based key ranking across windows. Experimental evaluation on the provided datasets demonstrates the presence of exploitable leakage and enables the recovery of stable key candidates for multiple coefficients, even in a much noisier trace set.

*Index Terms*— Correlation power analysis, CRYSTALS-Kyber, Hamming weight model, leakage localization, side-channel analysis, multi-window analysis

## INTRODUCTION

Side-channel attacks pose a serious threat to post-quantum cryptographic implementations, particularly when deployed on constrained hardware platforms. In this work, we target the CRYSTALS-Kyber key encapsulation mechanism and aim to recover secret key coefficients using simulated power traces of the pointwise multiplication (PWM) operation.

The provided dataset includes ciphertext polynomial coefficients and corresponding noisy power traces. While standard correlation power analysis (CPA) can recover key information in low-noise settings, its effectiveness significantly degrades in the much-noisier dataset. Therefore, the main challenge addressed in this work is designing a practical and robust attack pipeline capable of extracting exploitable leakage under high noise.

## ATTACK METHODOLOGY

### I. Leakage Model

We adopt a standard Hamming Weight (HW) leakage model on the intermediate value resulting from the multiplication of a secret coefficient  $k$  and a known ciphertext coefficient modulo 3329. For a key hypothesis  $k$  and input coefficient  $r$ , the predicted leakage is computed as:

$$L = \text{HW}((k \times r_i) \bmod 3329)$$

This model is consistent with common assumptions in software-based leakage simulations.

### I. Leakage localization

Instead of performing CPA over the entire trace, we first perform a leakage discovery step. For each time sample, we compute the maximum absolute correlation across all key hypotheses. This produces a correlation-versus-time curve, from which a clear peak is observable.

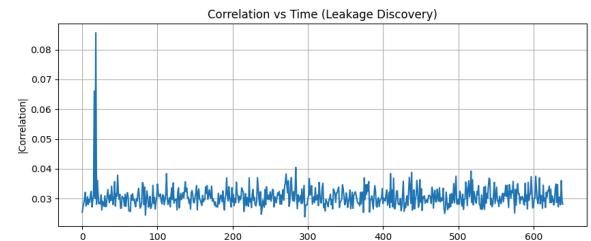


Fig. 1 shows the correlation profile for coefficient 6, where a strong leakage peak is visible around time sample 18. This confirms the presence of exploitable side-channel leakage despite high noise.

### III. Multi-window CPA

After identifying the leakage peak, we perform CPA within multiple windows centered around the detected peak ( $\pm 1, \pm 2, \pm 3, \pm 4$  samples). Each window produces a ranked list of key candidates.

We observe that incorrect candidates fluctuate significantly between windows, while correct candidates tend to appear consistently across multiple windows.

### IV. Stability-Based Key Ranking

To improve robustness, we introduce a stability-based ranking method. For each coefficient, we count how often each key candidate appears in the Top-10 results across the four windows. Keys with higher appearance counts (e.g., 4/4 or 3/4 windows) are considered stronger candidates.

This approach significantly improves reliability compared to relying on a single-window CPA result.

## EXPERIMENTAL RESULTS

Table 1. Leakage peak locations and stable key candidates for the first ten secret coefficients obtained using multi-window CPA on the 15000-trace dataset (top-4 candidates per window considered).

Coeff	Peak t	Peak Corr	Stable Keys (4/4 windows )	Near-stable (3/4 Keys)
0	3	0.0817	2482, 1241, 1635, 847	2341, 2835, 988
1	4	0.0758	2383, 1437, 2856, 1892	946, 311, 280, 140
2	8	0.0709	3232, 3135, 1616	2322, 2941, 388, 194
3	9	0.0816	3089, 2849, 3209, 480	240, 960, 2369, 1970
4	13	0.0660	740, 370, 1480	58, 1849, 29, 3271
5	14	0.0752	2046, 763, 1023, 1283	1803
6	18	0.0856	2461, 1593, 2895, 3186	88, 176, 44, 3241
7	19	0.0822	1921, 513, 2303, 1026	2052, 775, 2680, 1989
8	23	0.0673	2205, 2767, 1081	2248, 206, 412, 2162
9	24	0.0685	1872, 415, 830	1279, 771, 2499, 2050

## DISCUSSION

The experiments highlight several important observations. First, leakage localization is critical, as performing CPA over the full trace significantly reduces accuracy. Second, window selection strongly affects key ranking, motivating the use of multiple windows rather than relying on a single fixed window. Third, stability across multiple windows emerges as a strong indicator of promising key candidates under high-noise conditions.

The main limitation of the current implementation is computational cost, particularly during the leakage scanning phase. To mitigate this in practice, parallel processing was employed to evaluate multiple coefficients simultaneously, reducing overall execution time. However, this does not reduce the inherent complexity of the attack. Future work could explore algorithmic optimizations such as chunk-based scanning or early-stopping heuristics to further reduce runtime.

## CONCLUSION

This work demonstrates a practical side-channel attack on noisy Kyber power traces using a CPA-based approach enhanced with leakage localization and stability-based ranking. Despite high noise levels, consistent key candidates were recovered across multiple coefficients. The proposed pipeline is fully automated and generalizable, and further optimization could improve its efficiency and scalability for real hardware traces.

## References

- [1] NIST, “FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM),” 2024.
- [2] Challenge organizers, “IITK Innovation Challenge – Kyber Side-Channel Dataset and Problem Description,” provided materials (dataset, README, tutorial video), 2026.
- [3] S. Nkotto, “Template and CPA Side Channel Attacks on the Kyber/ML-KEM Pair-Pointwise Multiplication,” 2025.  
<https://eprint.iacr.org/2025/1577.pdf>
- [4] E. Brier, C. Clavier, and F. Olivier, “Correlation Power Analysis with a Leakage Model,” CHES 2004.