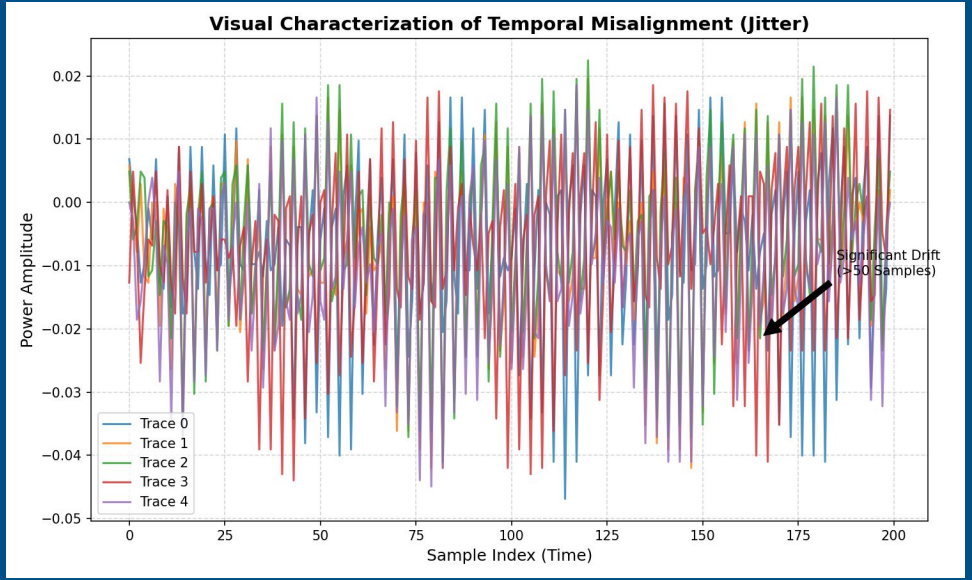
Side-Channel Analysis

A Minimal-Trace Approach to Side-Channel Analysis



Presented by Team Metamorphosis

1. Defining the Objective
2. Making Observations
3. Critical Algorithmic Parameters
4. Attack Pipeline Architecture
5. Optimizations

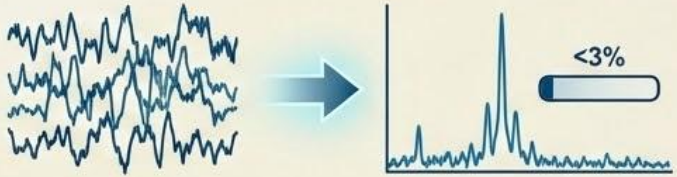
1. Defining the Objective

Primary Goal: Recover the specified secret key S1 indices (0, 14…252) from the CW305 dataset.

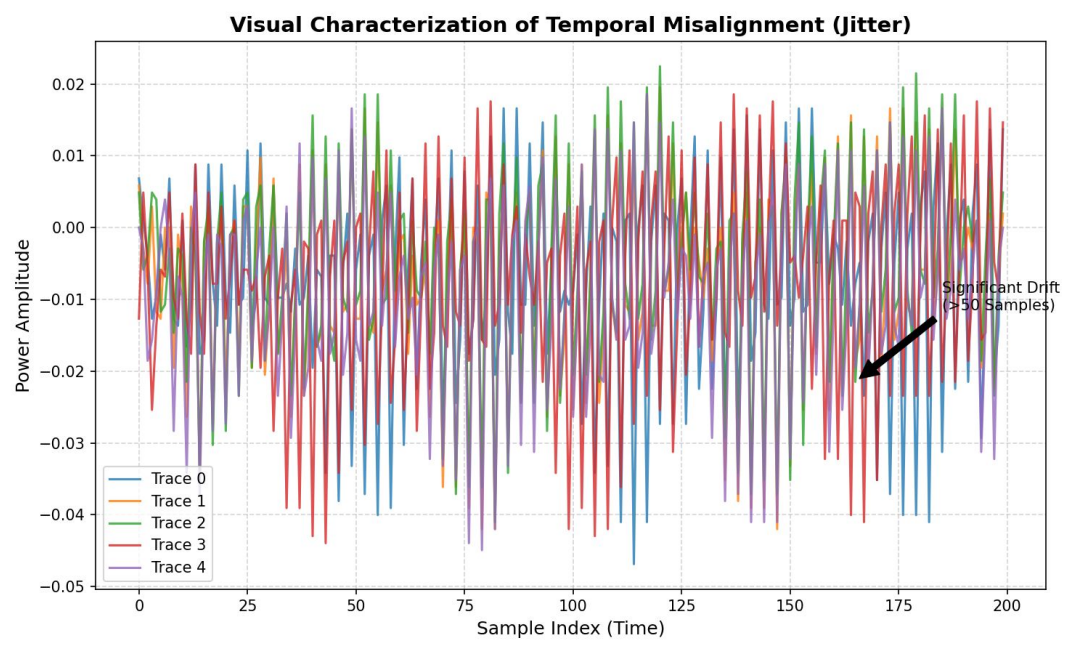
Optimization Criterion: Achieve successful retrieval using the **fewest possible number of traces**.

Technical Challenge: The documentation indicates operations occur at “different time instances,” introducing significant temporal misalignment (jitter).

Strategy: Implement spectral alignment to maximize Signal-to-Noise Ratio (SNR), allowing for recovery with <3% of the total dataset.



2. Making Observations



Visual Jitter: Target shifts >100 samples across traces.

Signal Potency: Distinct, high-amplitude spikes are visible.

Statistical Failure: Standard CPA yields correlation 0.0.

Root Cause: Destructive Interference (Signal Cancellation).

Conclusion: Resynchronization is mandatory.

3. Critical Algorithmic Parameters

Montgomery Domain Correction R_inv = 2704

Action: Derived modular inverse of hardware factor (R=4096).

Impact: Correctly aligns leakage model with FPGA internal state.

Exhaustive Key Search :

Action: Validated all 3,329 hypotheses for every target index.

Impact: Zero assumptions made on key distribution

64-bit Precision Enforcement:

Action: Used np.int64 to handle intermediate products.

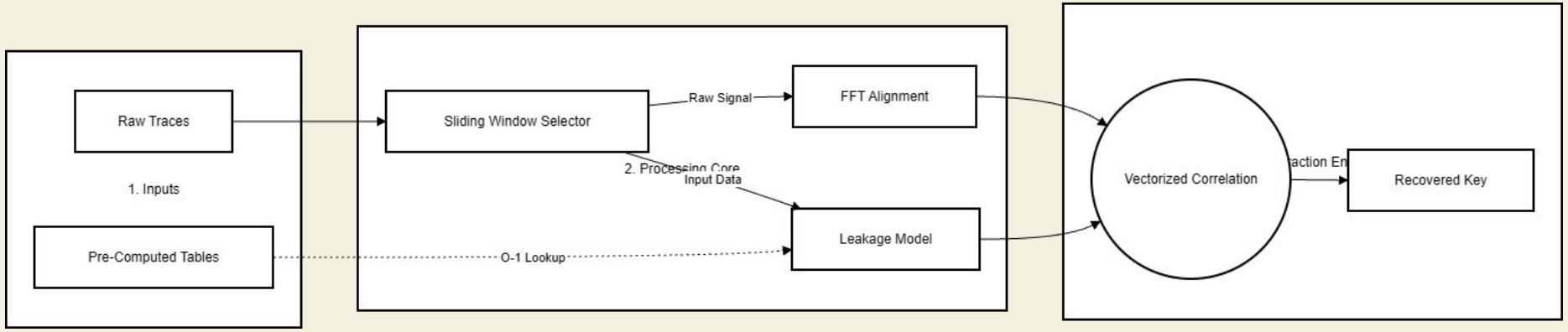
Impact: Prevented silent integer overflow bugs common in Kyber implementations.

O(1) Hamming Weight Lookup:

Action: Replaced runtime bit-counting with a pre-computed memory map.

Impact: Reduced leakage modeling latency to constant time.

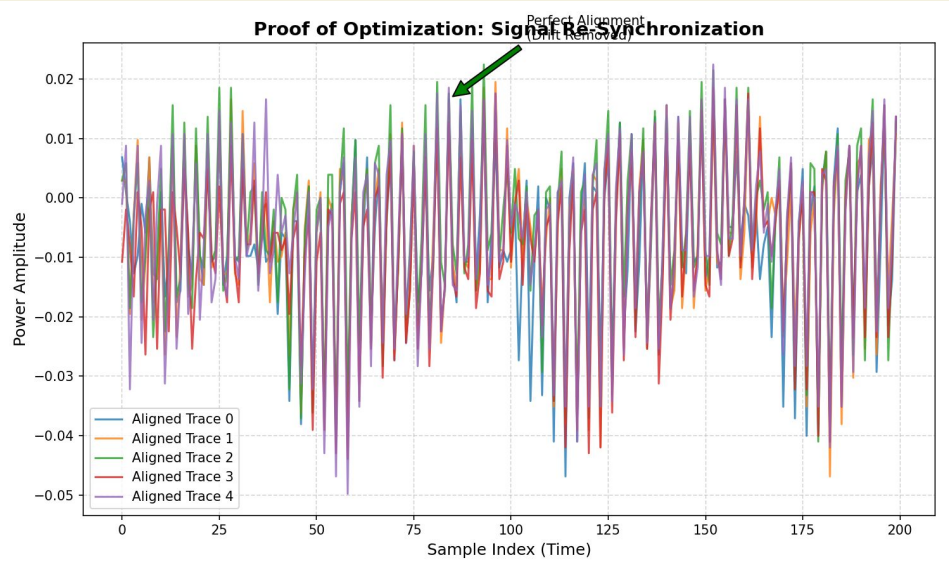
4. Attack Pipeline Architecture



1. Ingestion: Load 20,000 raw traces (Non-stationary).
2. Curation (The "Turbo Search"): Apply **Sliding Window** (Stride=500) to scan for stability.
3. Conditioning: Execute **FFT Alignment** to fix temporal jitter in the active window.

4. Modeling: Generate hypotheses using **Montgomery constants** (R_inv=2704) and **Lookup Tables**.
5. Extraction: Compute **Vectorized Correlation** to isolate the key index.

5. Optimization I - Localized Spectral Alignment



The Physics Constraint: Clock drift is non-linear. Aligning 20,000 traces globally is mathematically impossible.

The Strategy: Divide & Conquer.

- We slice data into independent **Local Windows** (N=500) where drift is linear.

The Engine (FFT):

- Inside each window, we apply **Spectral Cross-Correlation** to snap traces into sub-sample alignment.

The Selection: "Winner-Takes-All" Logic.

- Algorithm dynamically scores each window and keeps only the "Golden Window" (Highest SNR), discarding the rest.

Optimization II: Adaptive Window Search

The Challenge: Leakage location is unknown in both **Time** (Samples) and **Stability** (Trace Batch).
The Solution: A simultaneous 2D Search Algorithm.

- **Vertical Search (Trace Domain):** "Turbo Search" slides through the dataset (Stride=500) to find the most stable clock region.
- **Horizontal Search (Time Domain):** Vectorized ArgMax scans all time samples instantly to pinpoint the exact leakage moment.

Outcome: Pinpoints the target signal coordinates (t, n) automatically, even if it shifts between windows.

Optimization III: Vectorized Statistical Engine

- **The Challenge:** Traditional CPA uses nested loops.
- **The Solution: Vectorized Matrix Multiplication (Broadcasting)**.
- **The Mechanism:**
  - Replaced Python loops with optimized Linear Algebra (BLAS).
  - **Code:** Correlation = Trace_Matrix.T @ Hypothesis_Matrix
- **Result:** Computed millions of Pearson correlations simultaneously, reducing execution time from **Hours to Minutes**.

Experimental Results

Recovery Success: 19/19 Sub-keys recovered.

Signal Strength:

- Peak Correlation: **0.2904** (Index 0).
- Average Correlation: **~0.28** (High Confidence Margin).

Validation of Adaptive Search:

- Leakage location varies wildly (e.g., **Range 0-500** vs **Range 17500-18000**).
- **Conclusion:** Proves that leakage is localized; global analysis would have failed.

Precision: Leakage Sample Position identified with single-sample accuracy (e.g., Index 0 @ Sample 544).

```
[*] Starting TURBO Search on 19 keys.
[*] Scanning 20000 traces with Stride 500...
```

Idx	Best Window Range	Key	Corr	Sample Pos
0	17500-18000	2883	0.2904	544
14	16500-17000	1432	0.2902	2001
28	10500-11000	621	0.2721	6248
42	9500-10000	578	0.2731	21
56	5000-5500	2762	0.2797	5058
70	16000-16500	1949	0.2866	7120
84	0-500	3205	0.2779	4464
98	13000-13500	2697	0.2700	7507
112	11000-11500	2293	0.2650	9184
126	1000-1500	1922	0.2690	7298
140	5000-5500	510	0.2660	1644
154	15000-15500	2264	0.2833	3790
168	12000-12500	1978	0.2706	6716
182	5500-6000	1554	0.2654	9125
196	14500-15000	1643	0.2661	934
210	8500-9000	590	0.2739	6694
224	13500-14000	2698	0.2742	3154
238	18000-18500	3170	0.2796	3916
252	12000-12500	2163	0.2829	6177

Thank You

Team Metamorphosis