Problem 2 — AES Side Channel Analysis (Real Traces)

Team: Renita J and Surya K
Advisor: Ms. Suganya A

Executive Summary

This report documents the analysis performed on the provided real AES hardware power traces. *It summarizes the preprocessing pipeline, the enhanced CPA method applied to the 10th round, the results (per-byte ranked candidates and recovered keys), and the reconstruction of the AES-128 master key via inverse key schedule.*

Status: Unsuccessful Key Recovery

Code 1 (without SVD):

Recovered 10th-round key (K10): **99989E871EADCBD1A51431BB298D1D0C**

Reconstructed AES-128 master key (K0): **824E888CF0AD1CC6FF0C850FD37D27F9**

Code 2 (with SVD):

Recovered 10th-round key (K10): **6F989E871EADCBD1A514B0CC298D1D0C**

Reconstructed AES-128 master key (K0): **78DBA2144F4C5002E43FFFC2A21BDC43**

1. Dataset

Input file used: real_power_trace.csv

CSV layout expected: column 0 = plaintext (hex, 16 bytes), column 1 = ciphertext (hex, 16 bytes), columns 2.. end = trace samples (float)

2. Preprocessing Pipeline (as implemented in the code)

The preprocessing steps applied (in order):

- Raw overlay plot of first traces (saved as results/raw_overlay.png).
- Bad-trace detection using mean/std z-score thresholds (mean_z_thresh=6.0, std_z_thresh=6.0). Detected indices saved in results/bad_indices.txt.
- Baseline subtraction using the first 100 samples (saved example: results/baseline_corrected_example.png).
- Trace alignment by template (cross-correlation) with max shift ±50 samples (example: results/aligned_example.png).

- Column-wise normalization (z-score per sample) applied: NORMALIZE_COLUMNWISE=True.
- A preprocessing report was saved as results/preproc_report.txt.

Trial: Tried the following but no correct output obtained.

- Savitzky–Golay smoothing (window=21, polyorder=3) (example: results/smoothed_example.png).
- SVD denoising retaining 90% energy via truncated SVD, up to 200 components (example: results/svd_denoised_example.png).

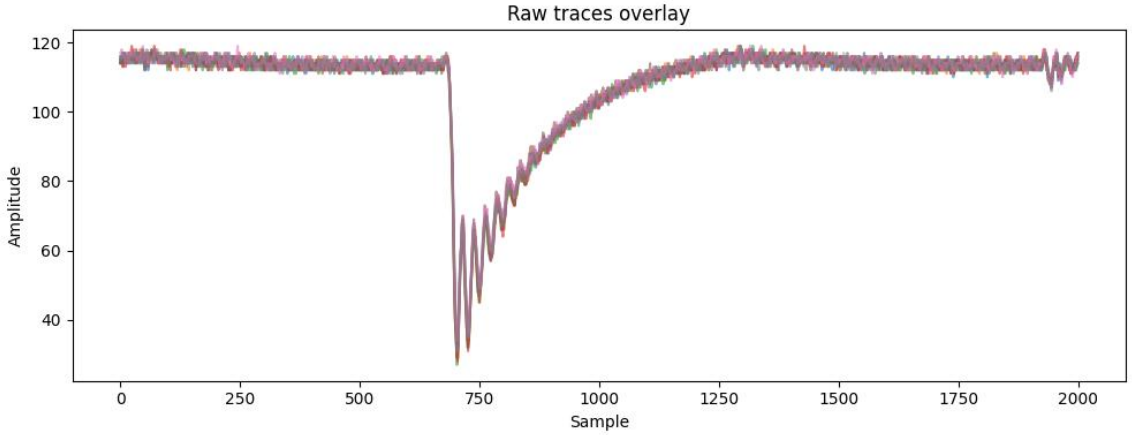

Figure: Raw overlay

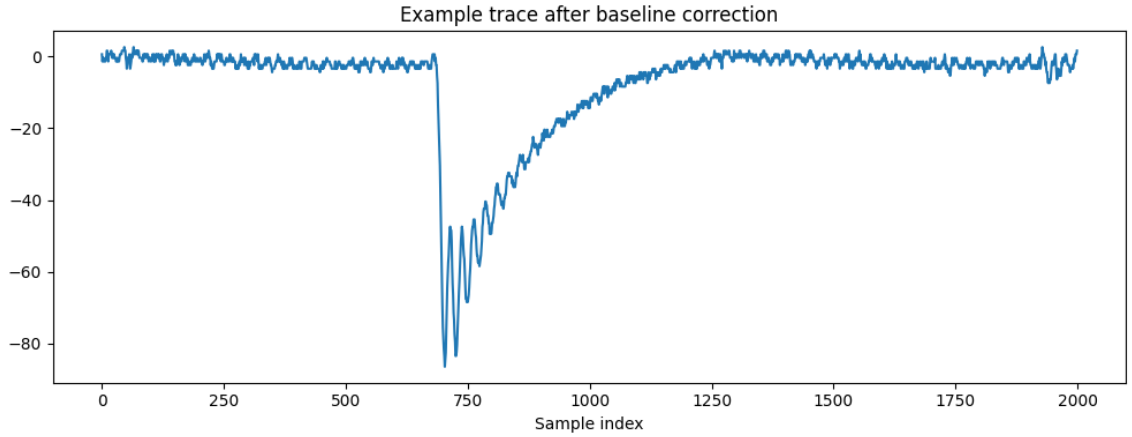

Figure: Baseline-corrected example

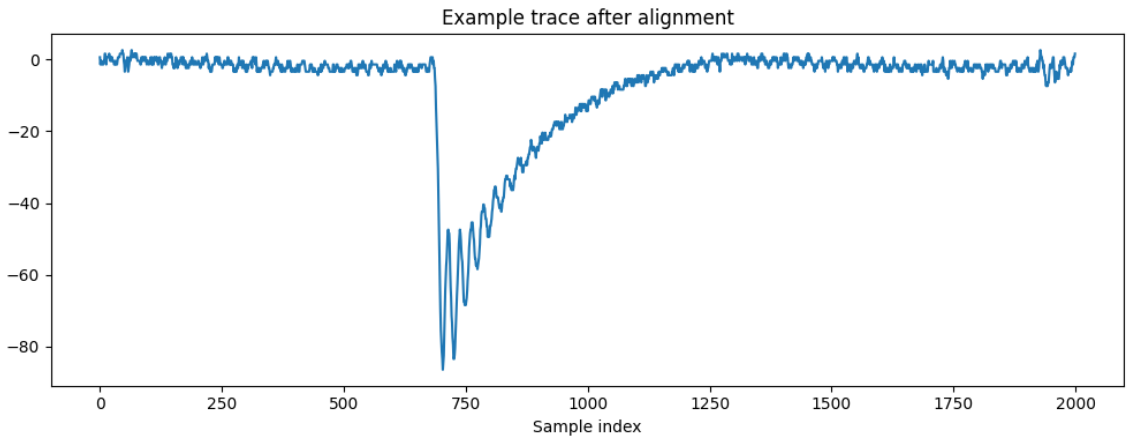

Figure: Aligned example

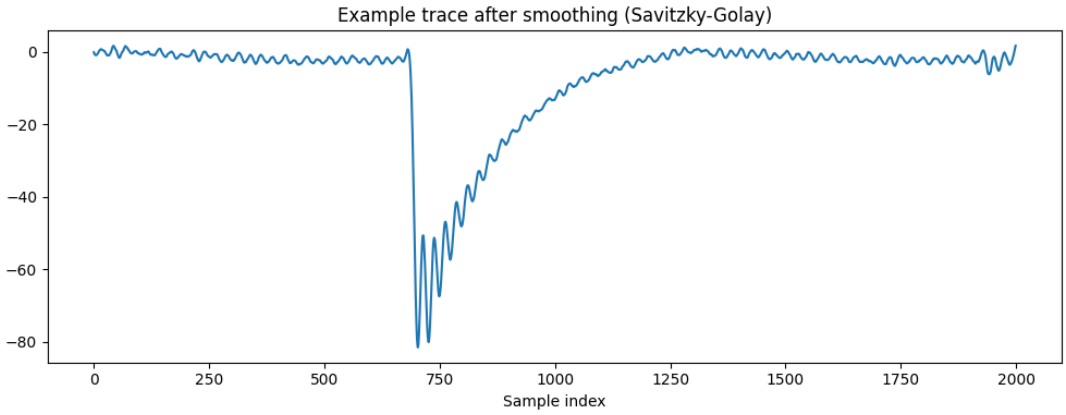

Figure: Smoothed example (Savitzky-Golay)

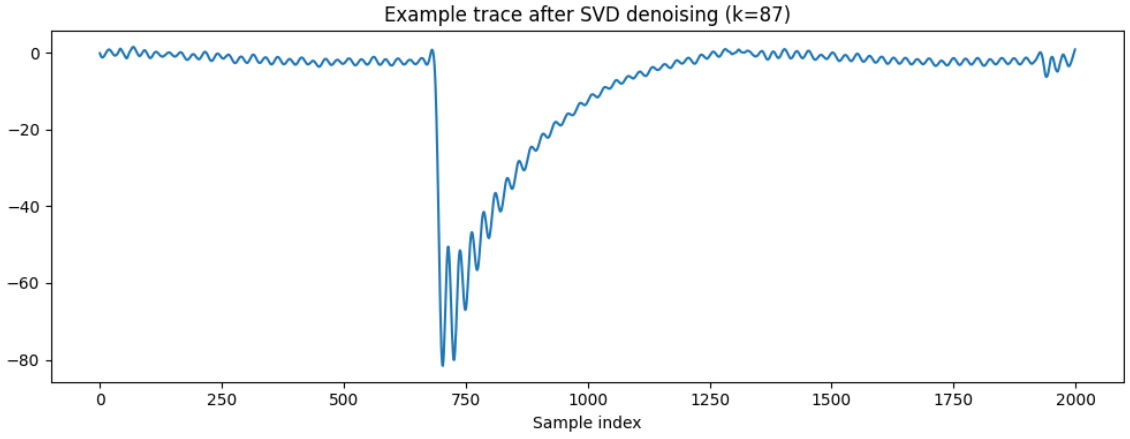

Figure: SVD denoised example

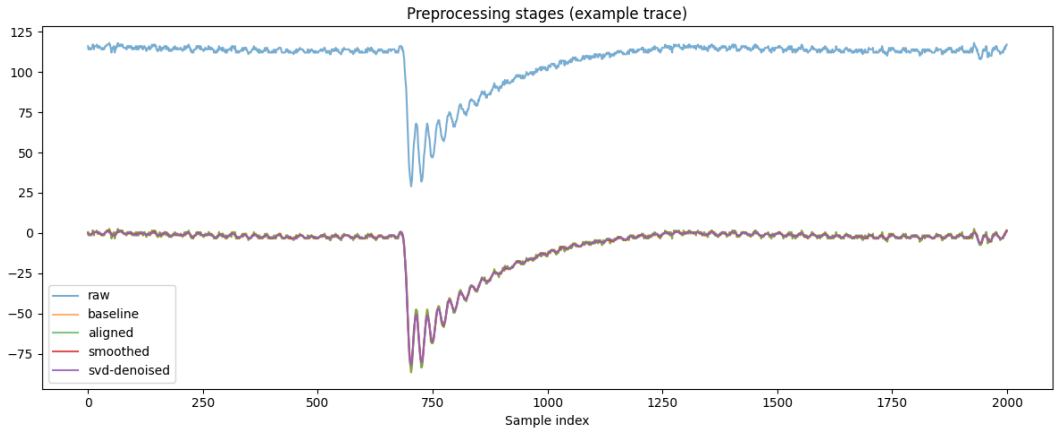

Figure: Preprocessing stages (raw -> baseline -> aligned -> smoothed -> svd)

3. CPA Methodology (10th round)

Attack details (as implemented):

- • Target: 10th round AES (last round) byte-wise attack.
- • Leakage model: Hamming-weight of inverse-SBox output (HW(inv_sbox[ciphertext_byte ⊕ key_guess])).
- • Correlation metric: Pearson correlation per sample between hypothetical HW vector and trace sample; then select POIs and compute RSS (root-sum-square) across POI samples as score.
- • POI selection: per-sample maximum absolute correlation across key guesses, take top POI_TOP_SAMPLES (default 60).
- • Refinement (optional): top REFINE_TOP_K (default 6) candidates are re-scored over a larger POI (REFINE_POI_SAMPLES, default 200).
- • Output per byte: full ranking of 256 candidates saved in results/byte_XX_rank.txt and a per-byte score plot results/byte_XX_score_poi{POI}.png.

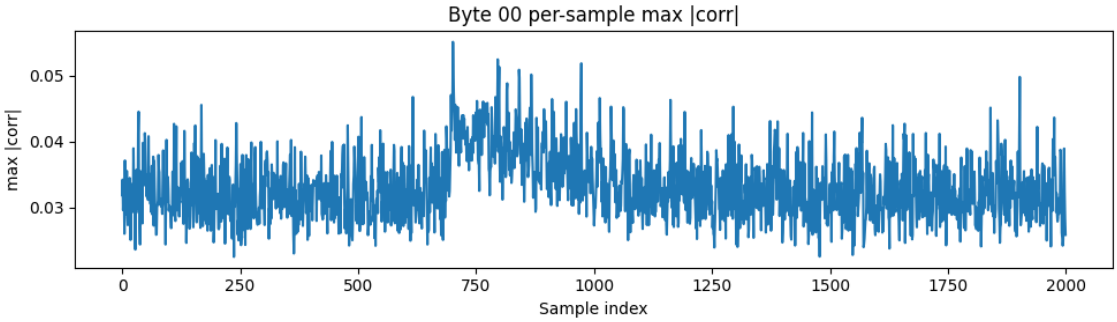

Figure: Byte 00 per-sample max |corr|

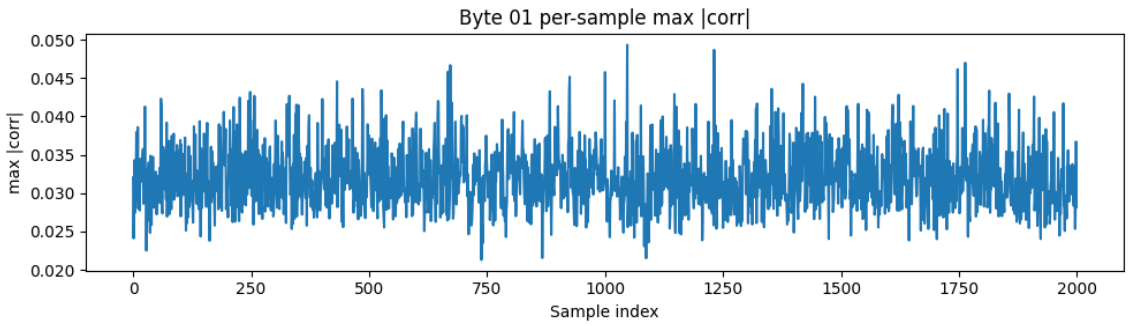

Figure: Byte 01 per-sample max |corr|

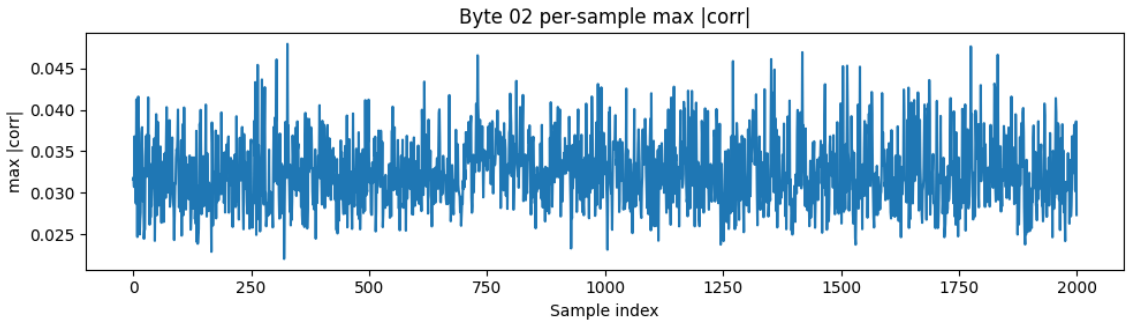

Figure: Byte 02 per-sample max |corr|

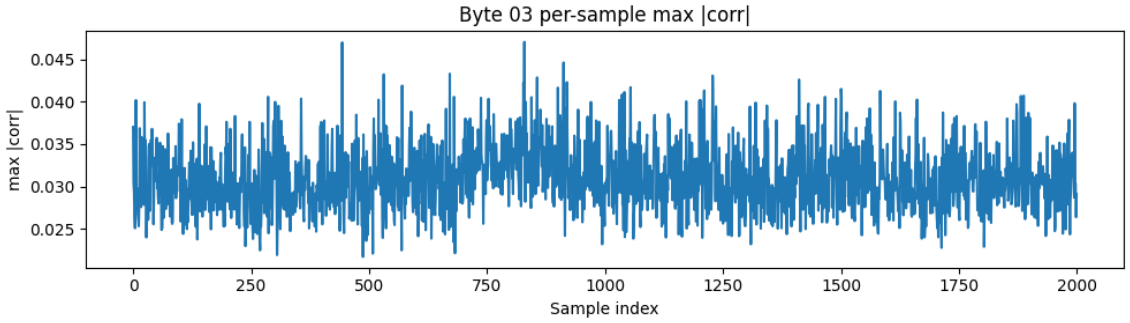

Figure: Byte 03 per-sample max |corr|

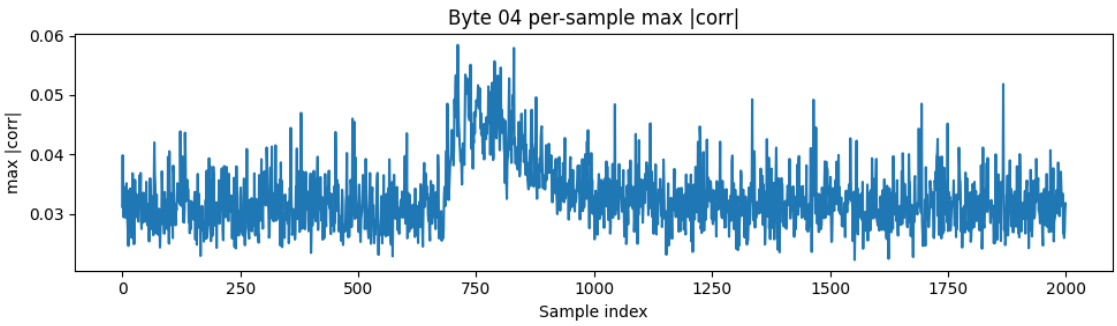

Figure: Byte 04 per-sample max |corr|

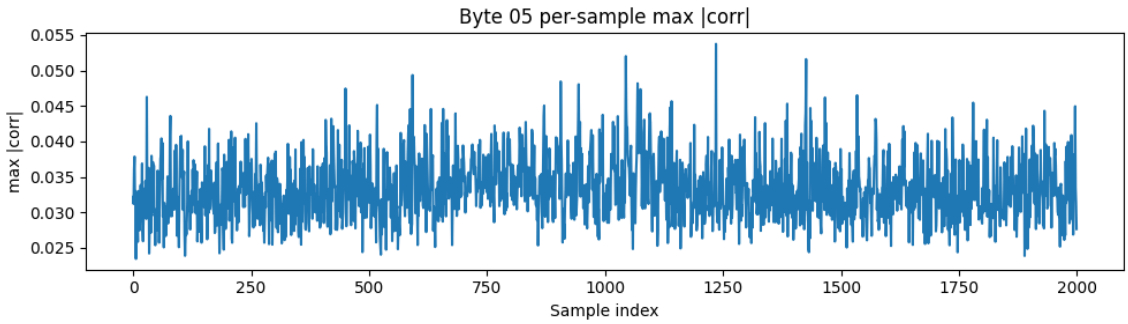

Figure: Byte 05 per-sample max |corr|

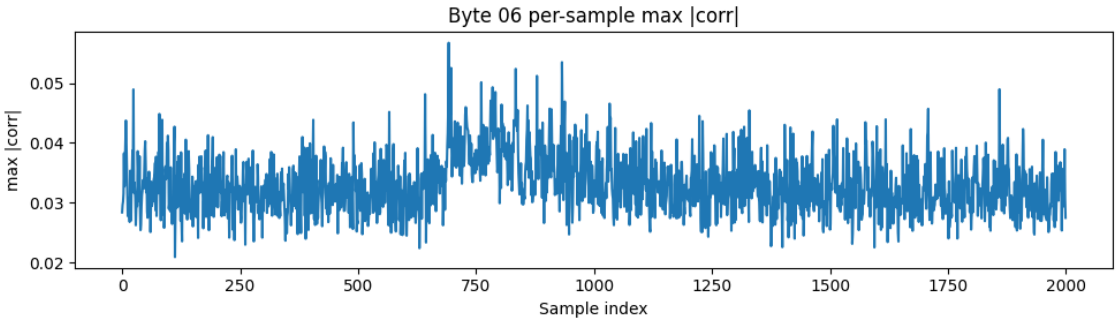

Figure: Byte 06 per-sample max |corr|

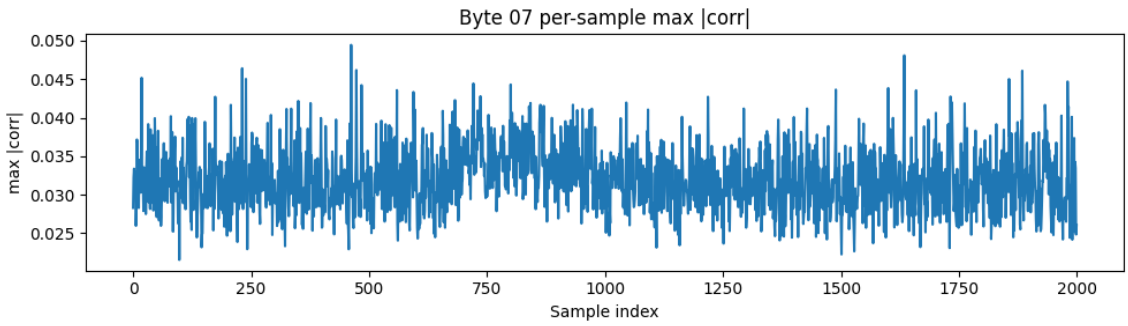

Figure: Byte 07 per-sample max |corr|

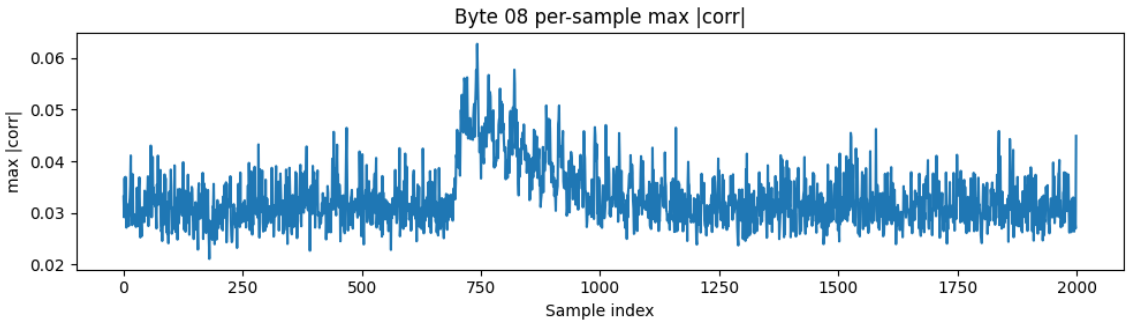

Figure: Byte 08 per-sample max |corr|

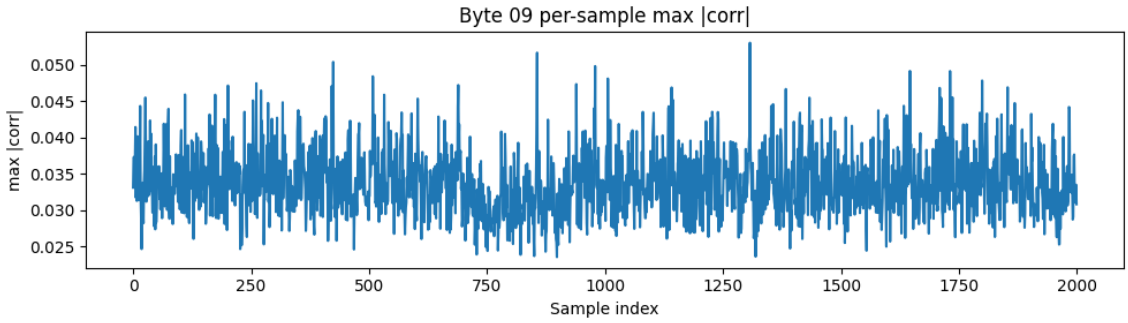

Figure: Byte 09 per-sample max |corr|

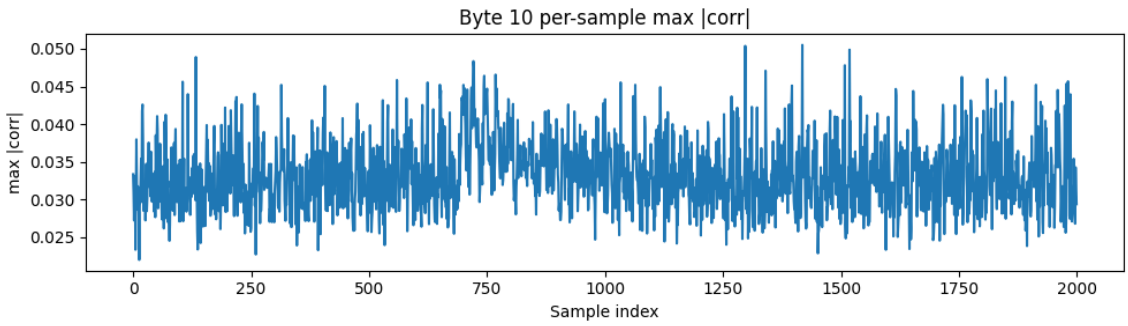

Figure: Byte 10 per-sample max |corr|

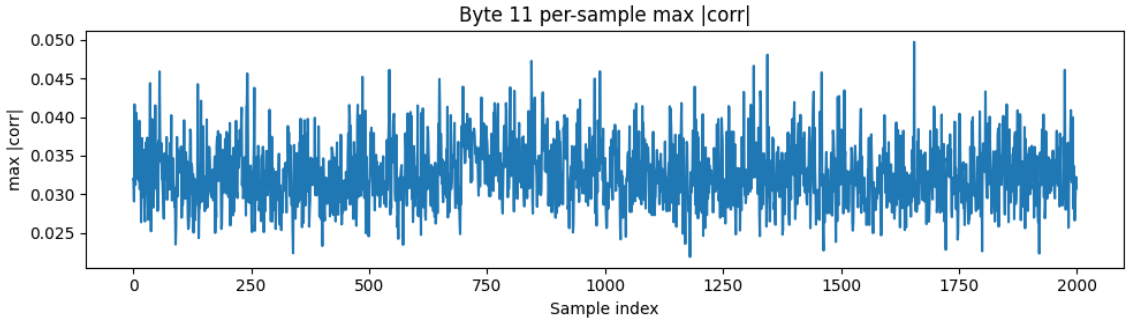

Figure: Byte 11 per-sample max |corr|

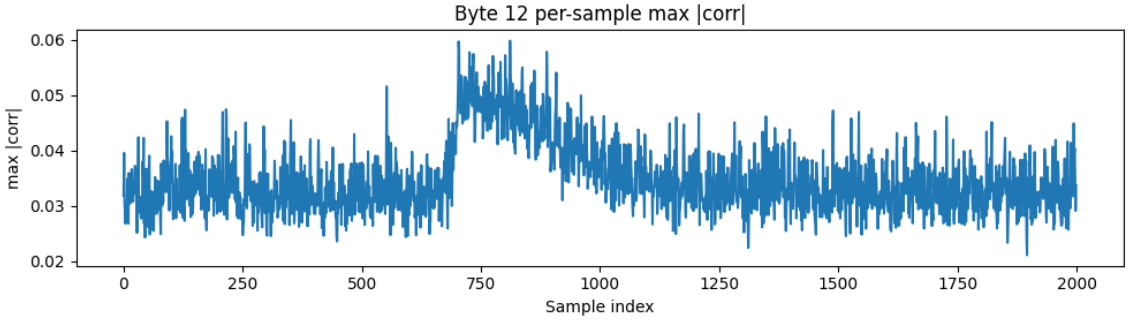

Figure: Byte 12 per-sample max |corr|

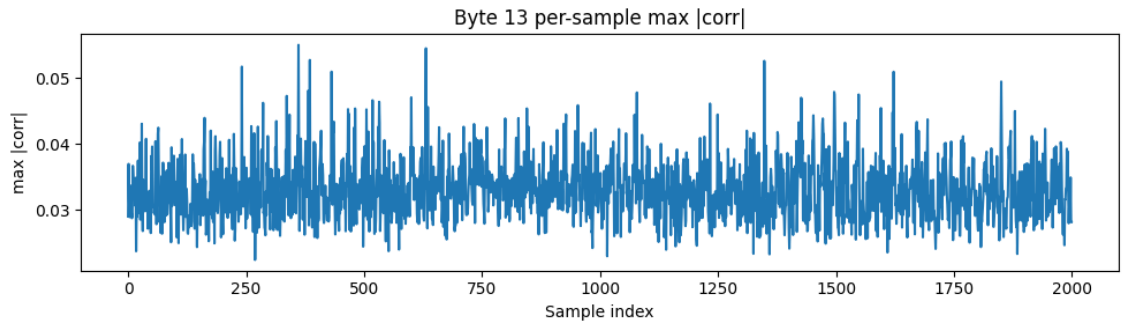

Figure: Byte 13 per-sample max |corr|

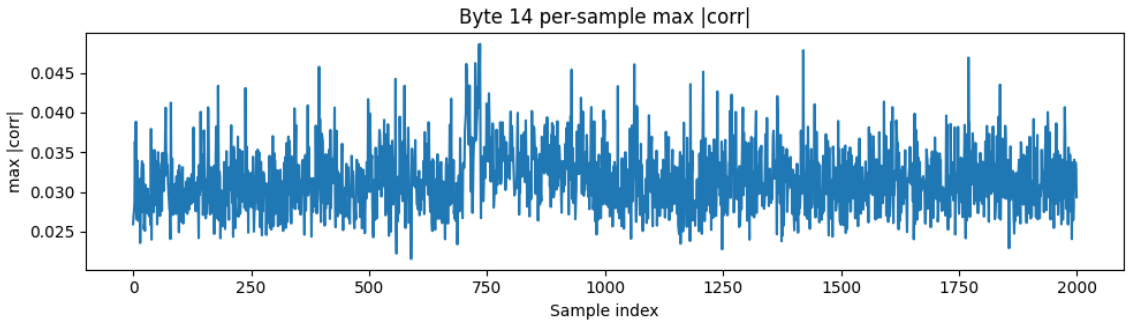

Figure: Byte 14 per-sample max |corr|

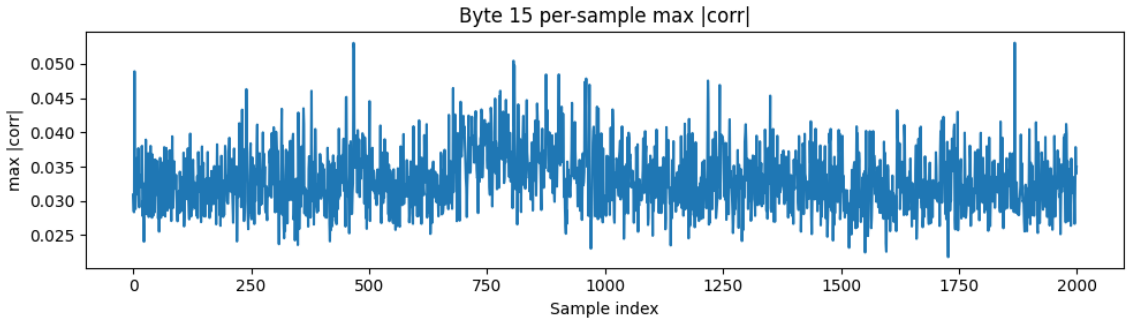

Figure: Byte 15 per-sample max |corr|

4. Results and Files Produced

The analysis produces the following files in the results/ directory (fixed):

Filename	Description
recovered_key.txt	Recovered 10th-round key (space-separated hex bytes)
master_key.txt	Reconstructed AES-128 master key (K0) in

	hex
round_00_key.txt ... round_10_key.txt	All AES round keys (K0..K10) in hex
correlation_ranks.txt	Summary per byte: best guess and top-5 candidates
byte_00_rank.txt ... byte_15_rank.txt	Ranked candidate lists (256 entries) per byte
byte_XX_maxper_sample.png	Per-byte per-sample max |corr| (one png per byte)
byte_XX_score_poi{POI}.png	Per-byte RSS-over-POI score plot (one png per byte)
preproc_report.txt	Preprocessing report (parameters and detected bad traces)
raw_overlay.png, baseline_corrected_example.png, aligned_example.png, smoothed_example.png, svd_denoised_example.png, preprocessing_stages_example.png	Diagnostic plots for preprocessing

5. Parameters (defaults used in code)

- BASELINE_SAMPLES = 100
- REMOVE_BAD_TRACES = True
- BAD_MEAN_ZTH = 6.0
- BAD_STD_ZTH = 6.0
- ALIGN_MAX_SHIFT = 50
- SAVGOL_WINDOW = 21
- SAVGOL_POLY = 3
- SVD_ENERGY = 0.9
- SVD_MAXCOMP = 200
- NORMALIZE_COLUMNWISE = True
- POI_TOP_SAMPLES = 60
- REFINE_TOP_K = 6
- REFINE_POI_SAMPLES = 200
- USE_REFINEMENT = True