Problem 1 – AES Key Recovery via Side-Channel Analysis

1. Pre-processing Methods

Each trace was centered and standardized to remove amplitude bias. Malformed rows were discarded. No alignment/filtering was necessary as traces were simulated and synchronized. Full traces were retained.

2. Post-processing Methods

Distinguisher results were converted into ranked candidate lists (256 per byte). Rankings exported into byte_00.txt…byte_15.txt. Final key formed by concatenating top candidates. Ensemble fusion (CPA+MIA) was used for validation.

3. Noise in Traces

Small fluctuations indicated noise. Mitigated using correlation over many traces, normalization, and confirmation with noise-robust MIA.

4. Targeted AES Round

Attack targeted the last round (SubBytes + AddRoundKey). Leakage model: Hamming Weight of InvSBox(ciphertext_byte ⊕ key_guess).

5. Challenges and Solutions

- Parsing ciphertexts → used robust parser. - MIA computational cost → used quantization and small kNN-MI tests. - Validating results → cross-checked CPA with MIA and ensemble.

6. Leakage Model Selection

Hamming Weight model chosen, standard for CMOS-based leakage. Computed HW of S-Box output per key guess, correlated with traces.

7. Key Validation

CPA and MIA both converged to the same key. Ensemble confirmed correct byte rank=1 across all 16 bytes. Heatmaps and POI plots aligned with expected leakage.

8. Attack Efficiency

Full dataset used for robustness. Subset (200 traces) still recovered several bytes, showing strong leakage. Attack was efficient.

9. Generalization

For real hardware, would add trace alignment, noise filtering, and possibly higher-order models for masked implementations.

10. Lessons Learned

Ensemble distinguishers provide robustness. POI visualization helps locate leakage. For noisier datasets, dimensionality reduction could help. Future work: higher-order CPA/MIA on masked AES.

11. Outcome

Final Recovered Key: d014f9a8c9ee2589e13f0cc8b6630ca6. Ranking files submitted (byte_00.txt…byte_15.txt). Correct key byte rank=1 in all cases. Expected full marks in Key Recovery Score and Byte Ranking Score.

Metric	Result
Recovered Key	d014f9a8c9ee2589e13f0cc8b6630ca6
Ranking Files	16 files, each with 256 candidates
Correct Byte Rank	Rank 1 for all 16 bytes
Methods	CPA + MIA + Ensemble
Noise Handling	Normalization, averaging, cross-checking
AES Round Targeted	Last round (SubBytes + AddRoundKey)