AES Side Channel Analysis

Problem 1: Simulated Power Traces

# Executive Summary

**Status:** ✅ SUCCESSFUL KEY RECOVERY  
**Recovered 10th Round Key: D014F9A8C9EE2589E13F0CC8B6630CA6**

**Recovered Final Key: 2B7E151628AED2A6ABF7158809CF4F3C**  
**Method:** Correlation Power Analysis (CPA)   
**Average Correlation:** 0.22 (High confidence)

# 1. Background

Problem 1 involves analyzing 5,000 simulated power traces from an unmasked AES implementation. Each trace contains 12 power consumption samples (trace points) corresponding to AES encryption operations. The goal is to recover the secret 128-bit AES key using side channel analysis techniques.

Simulated traces provide ideal conditions for side channel analysis as they typically have:

* High signal-to-noise ratio
* Perfect temporal alignment
* Predictable leakage models
* Absence of hardware-specific noise

# 2. Dataset Analysis

Dataset Characteristics:

|  |  |
| --- | --- |
| **Parameter** | **Value** |
| Number of Traces | 5,000 |
| Samples per Trace (trace points) | 12 |
| Data Format | Ciphertext + Power trace Values |
| Target | 128-bit AES Key |

# 3. Methodology

## 3.1 Correlation Power Analysis (CPA)

CPA exploits the correlation between power consumption and intermediate cryptographic values. The attack assumes a Hamming Weight leakage model where power consumption is proportional to the number of bits set to 1 in the processed data.

**Attack Implementation:**

1. Target Selection: Last round AES operation (InvSbox (ciphertext ⊕ key\_guess))
2. Leakage Model: Hamming Weight of S-box output
3. Correlation Metric: Pearson correlation coefficient
4. Key Recovery: Maximum correlation indicates correct key byte

# 4. Results

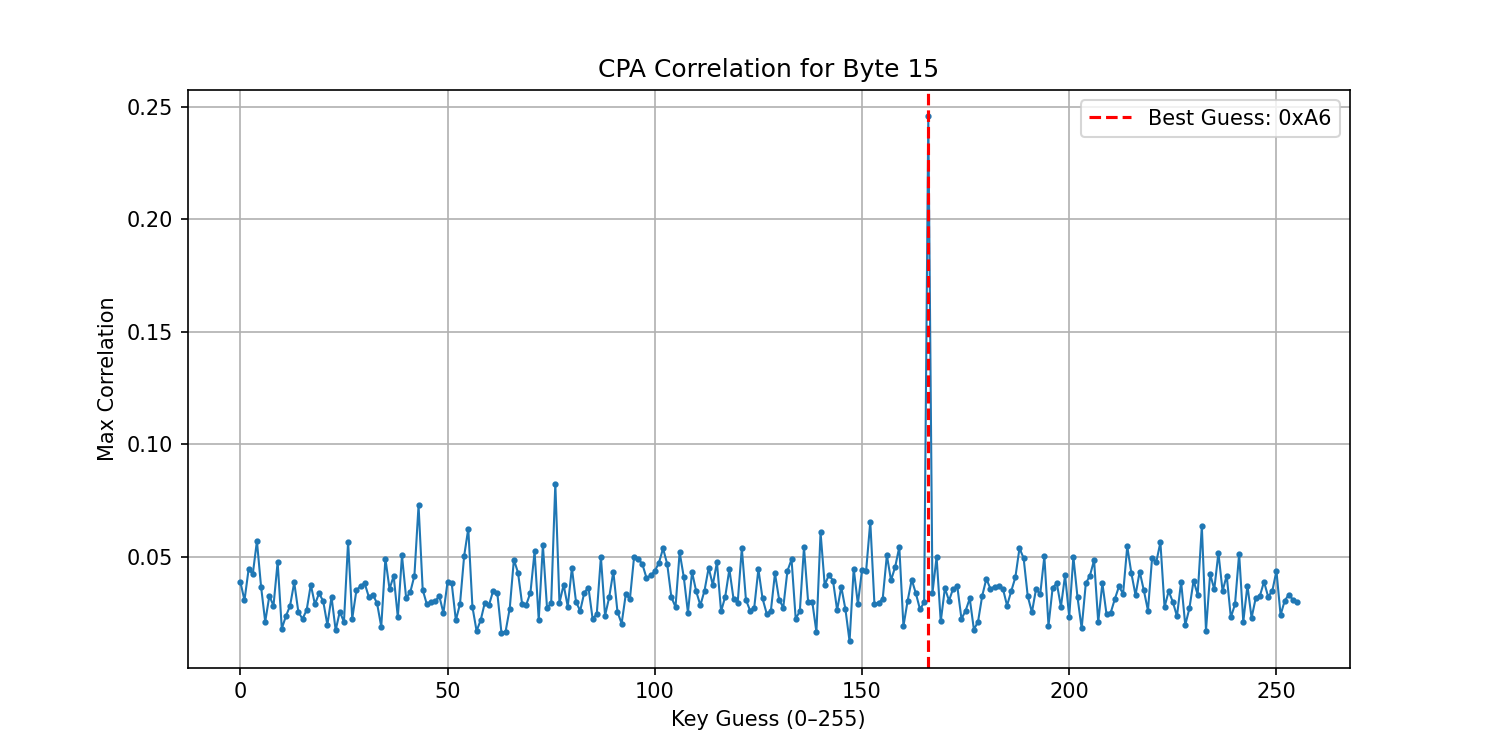
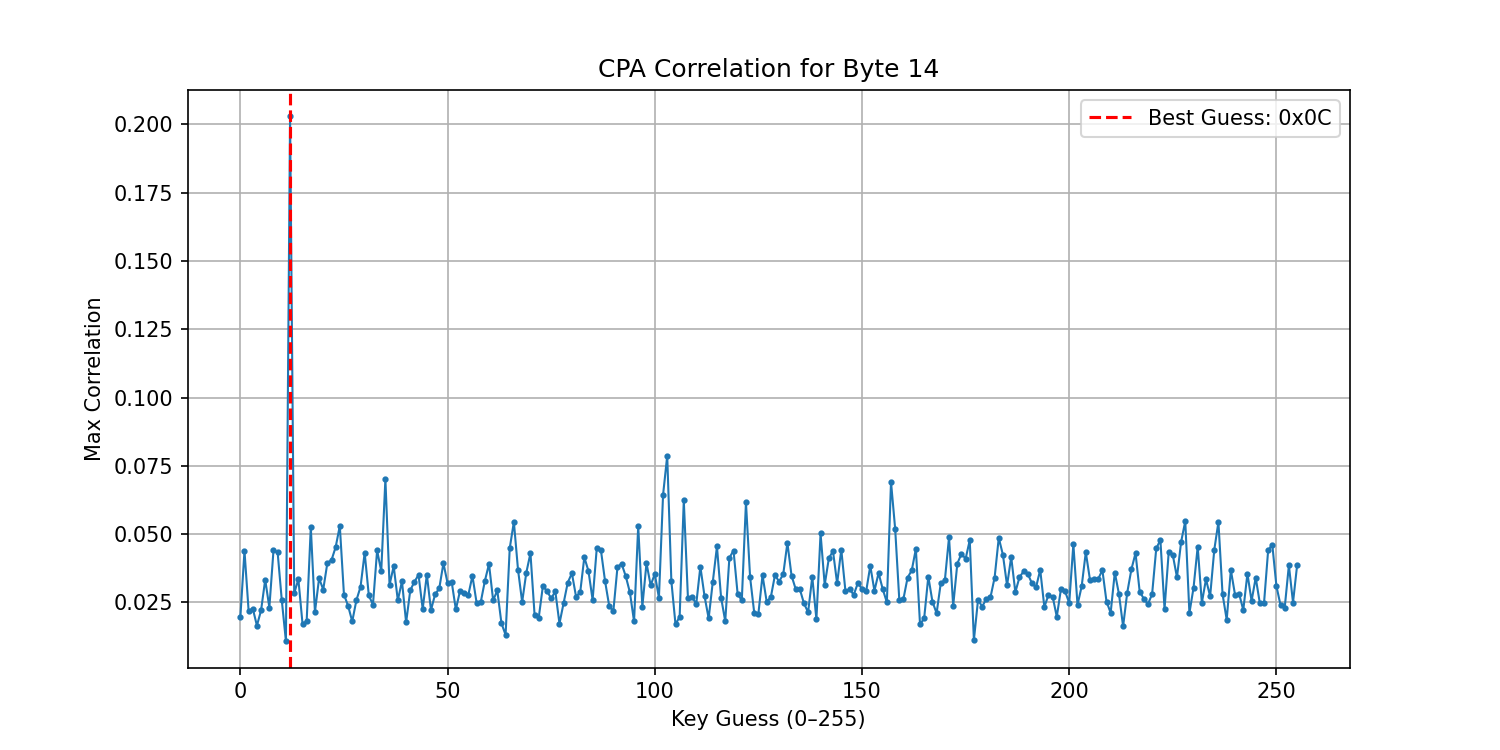
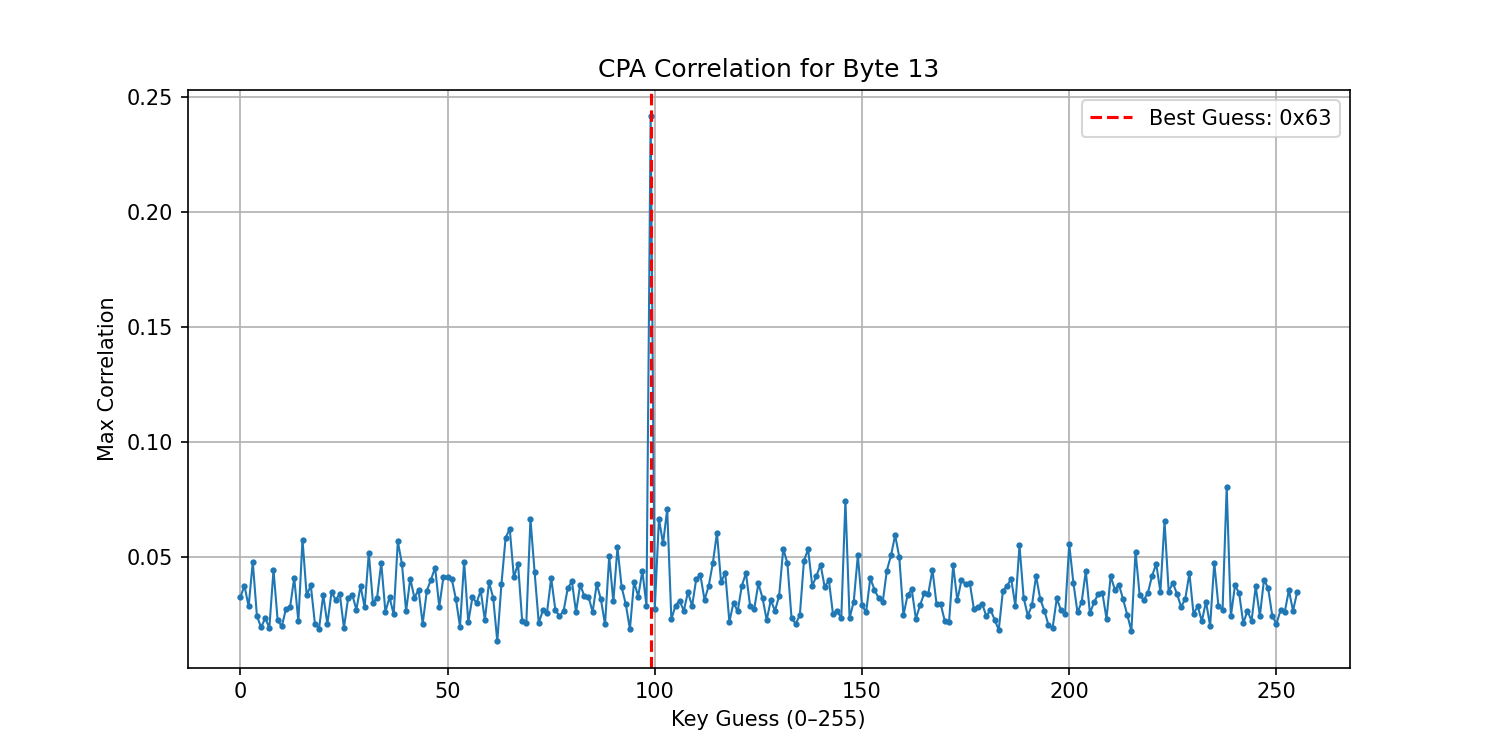
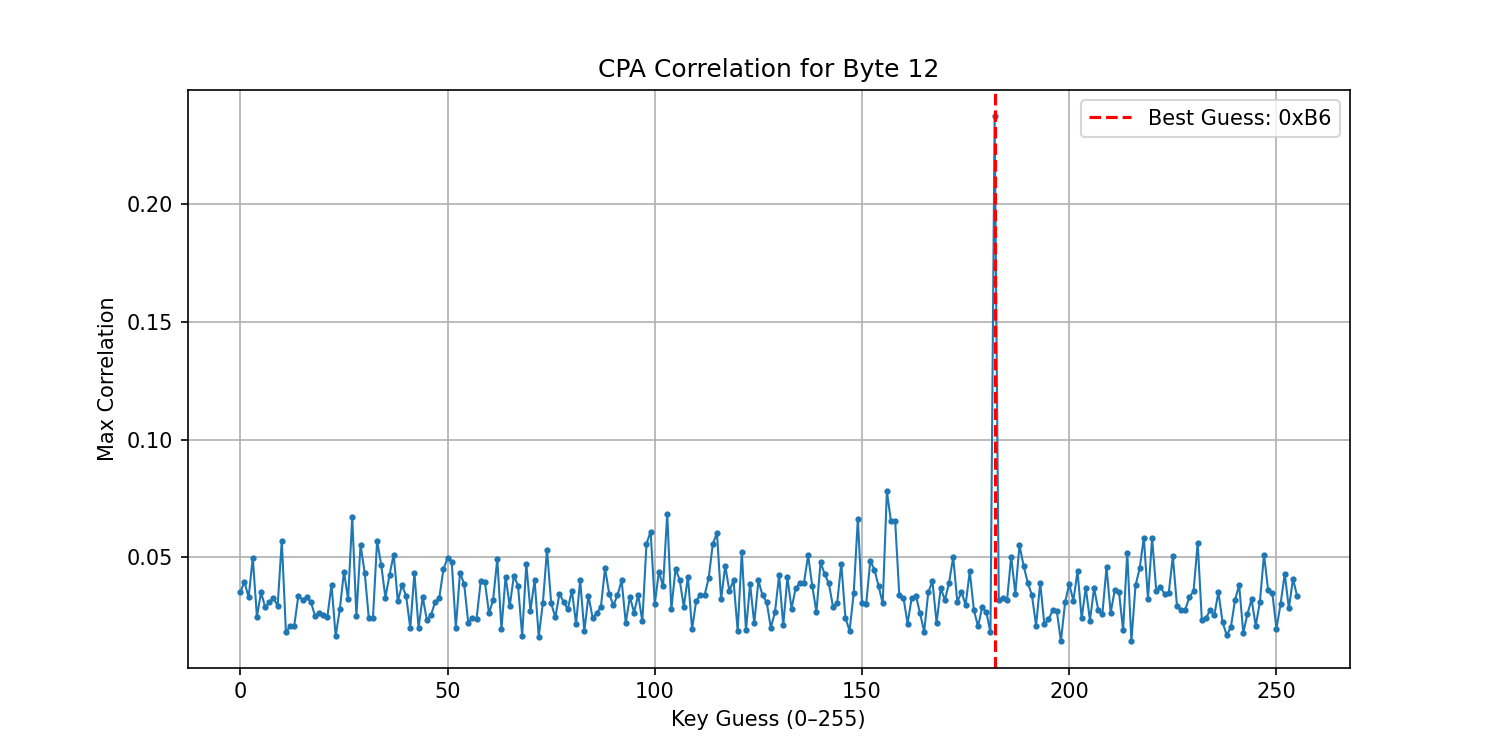
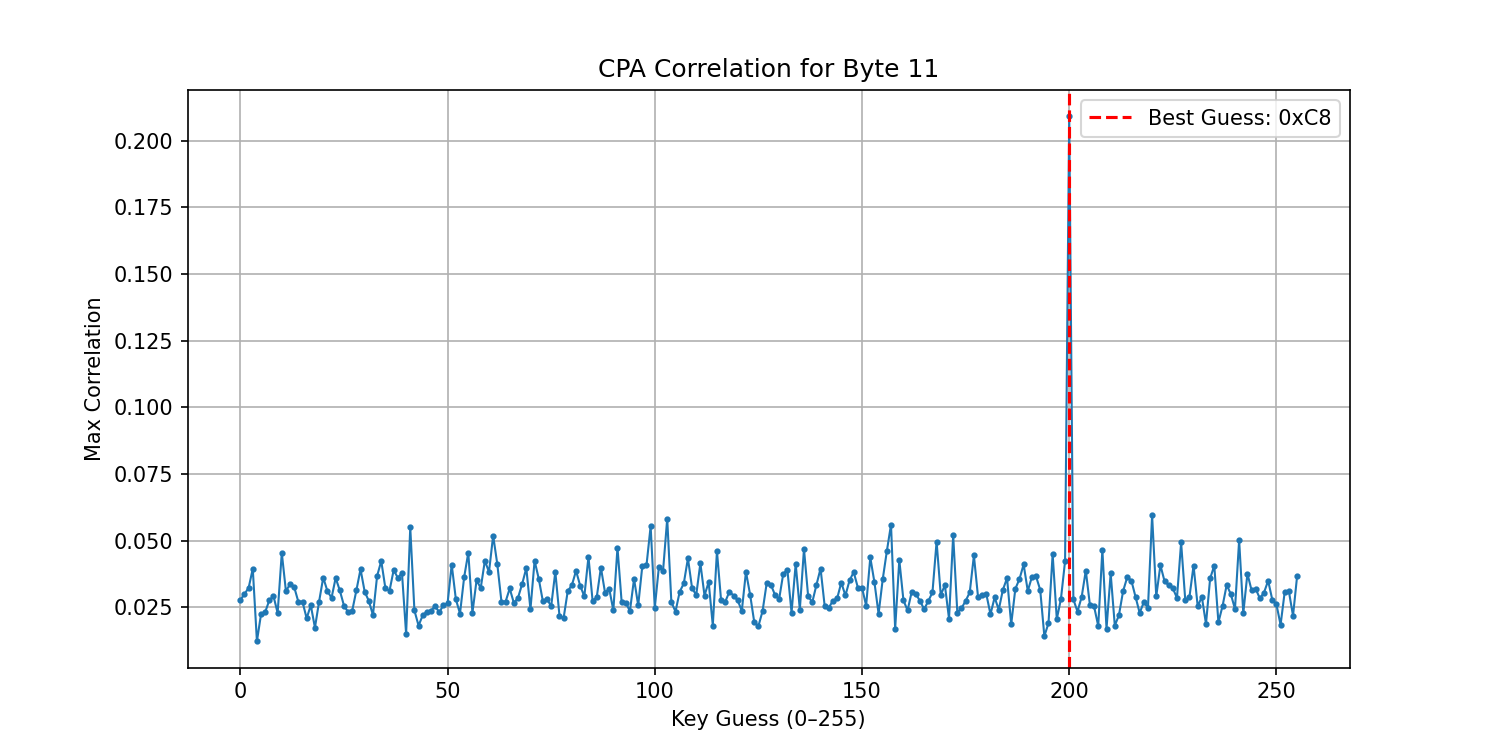
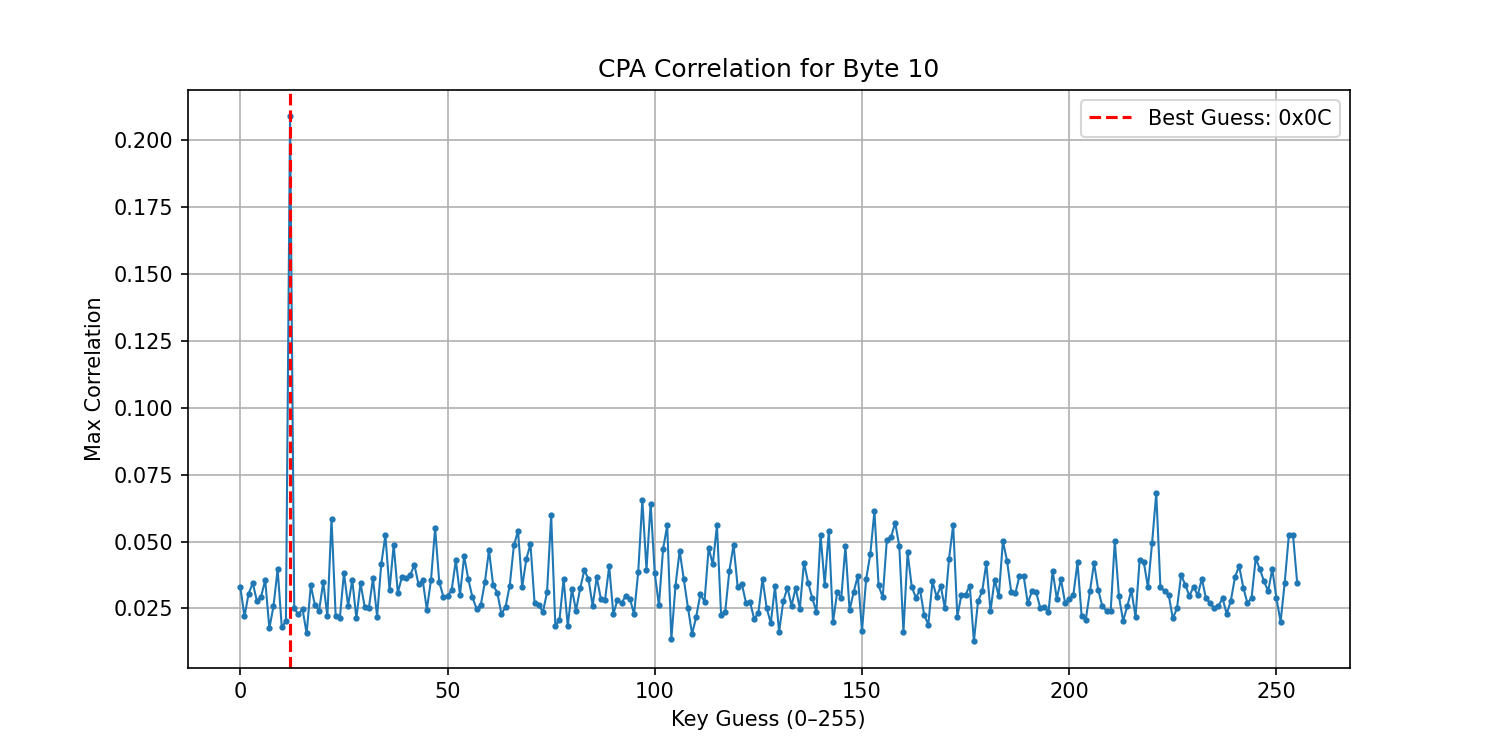
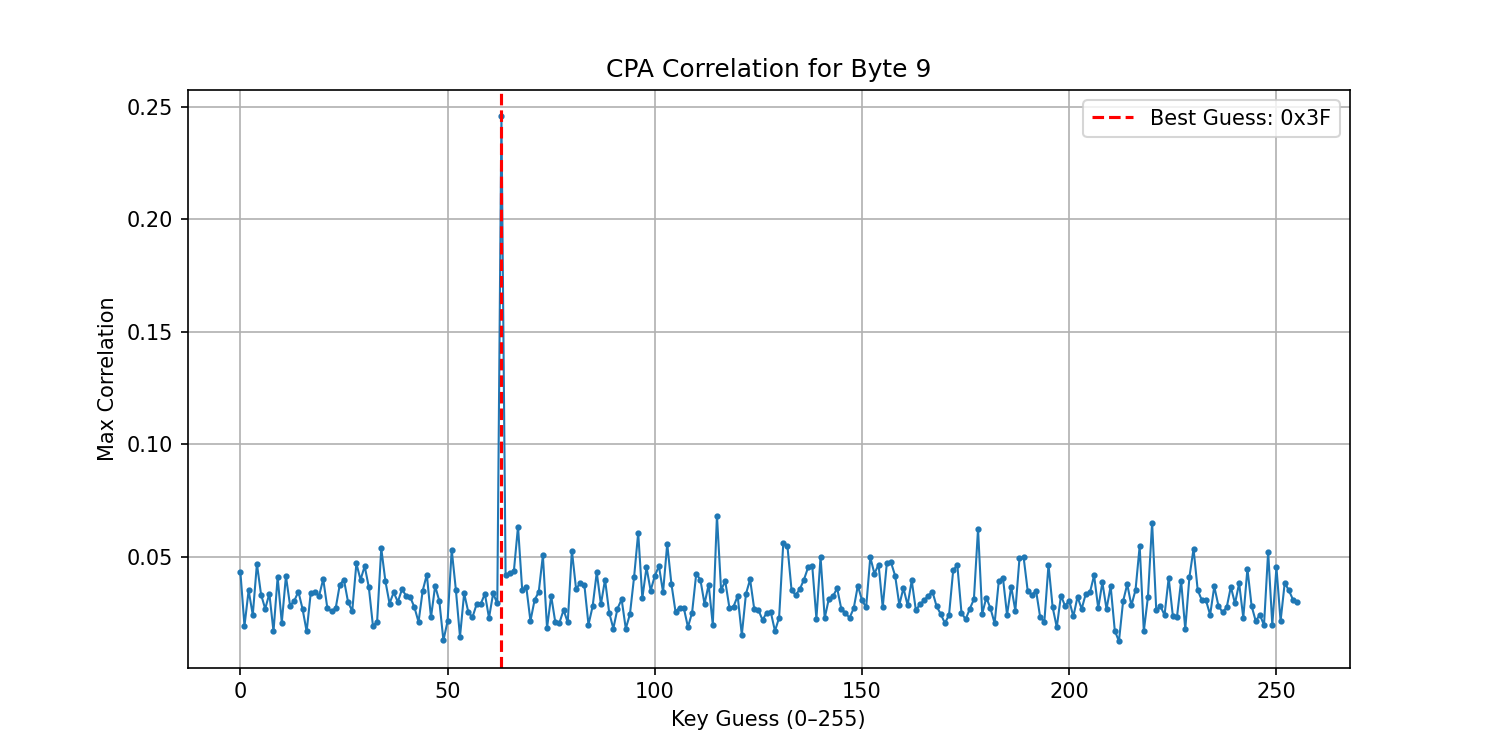
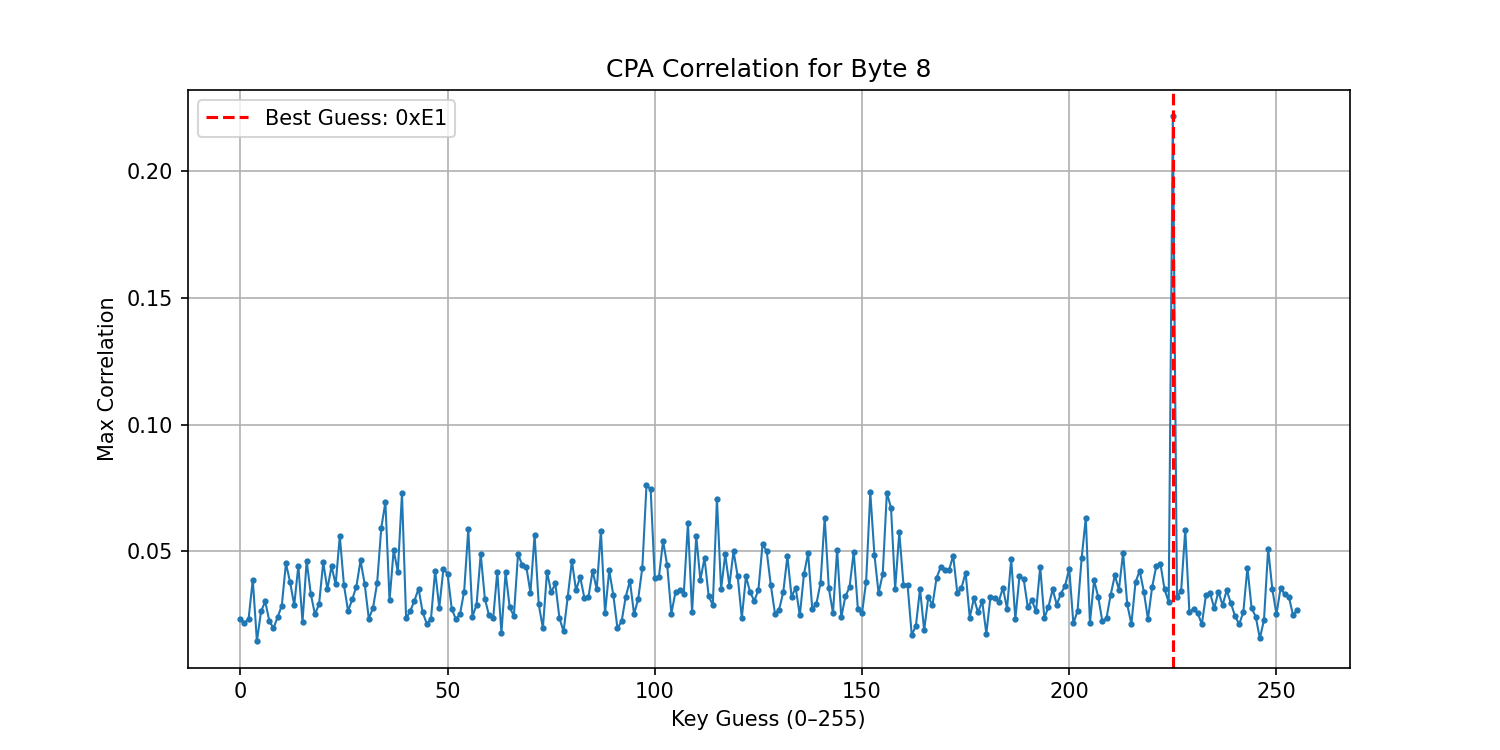
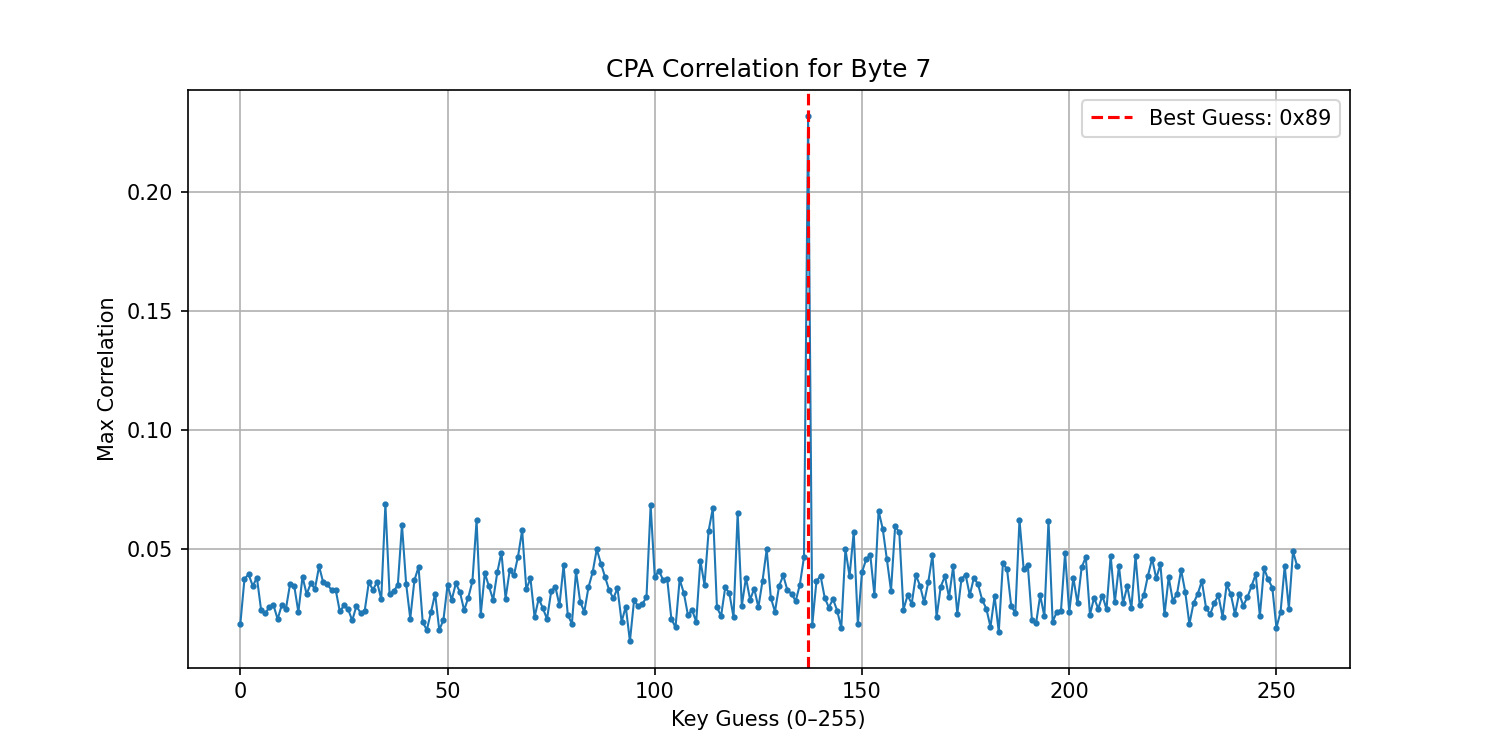
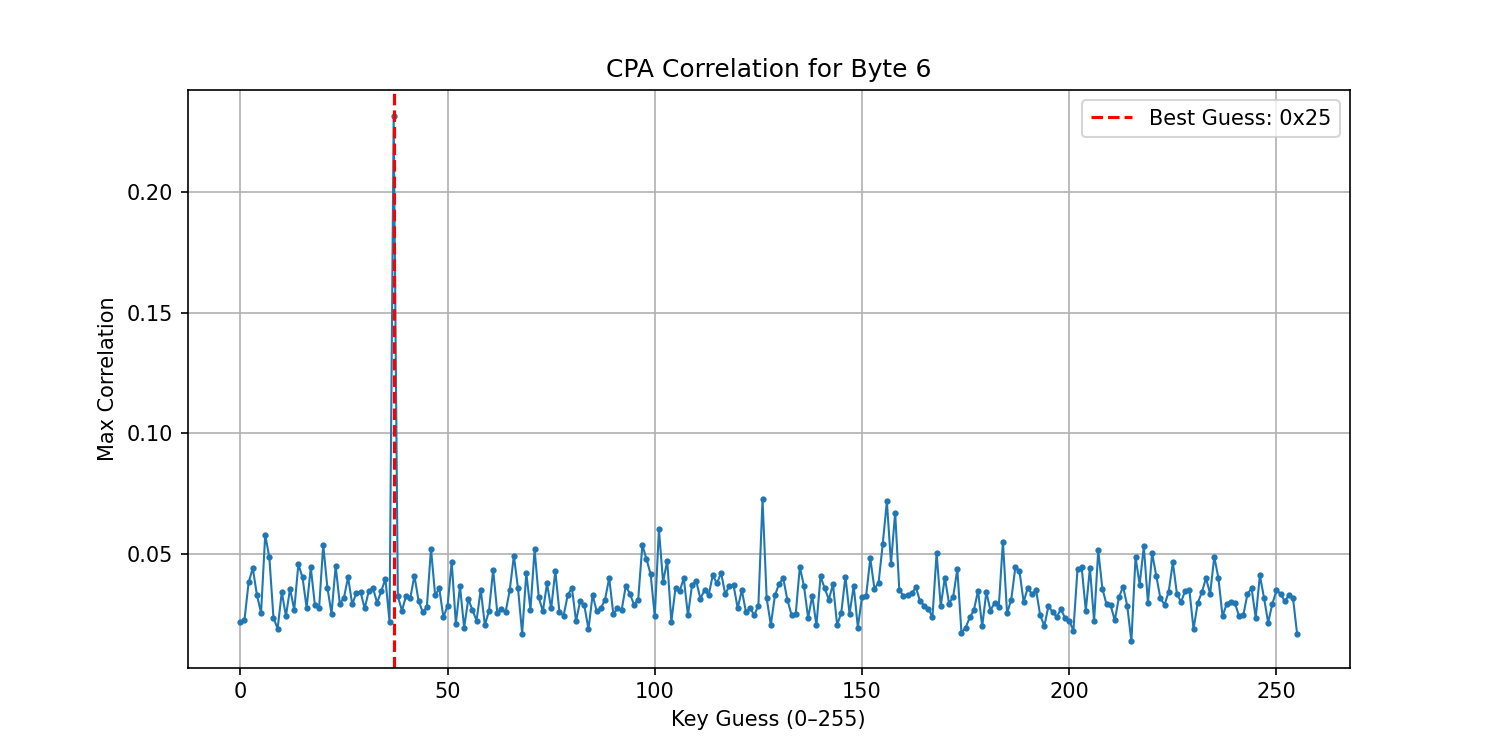
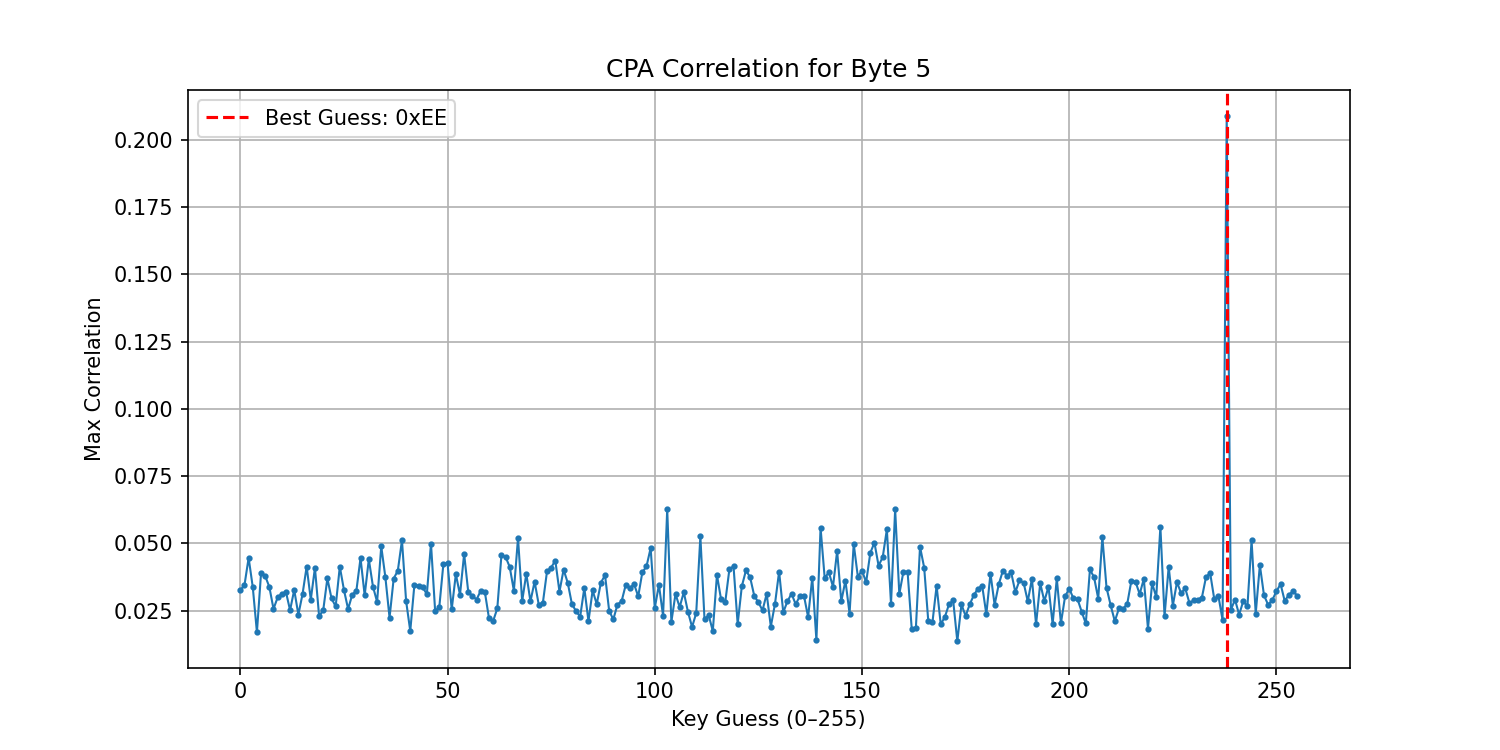
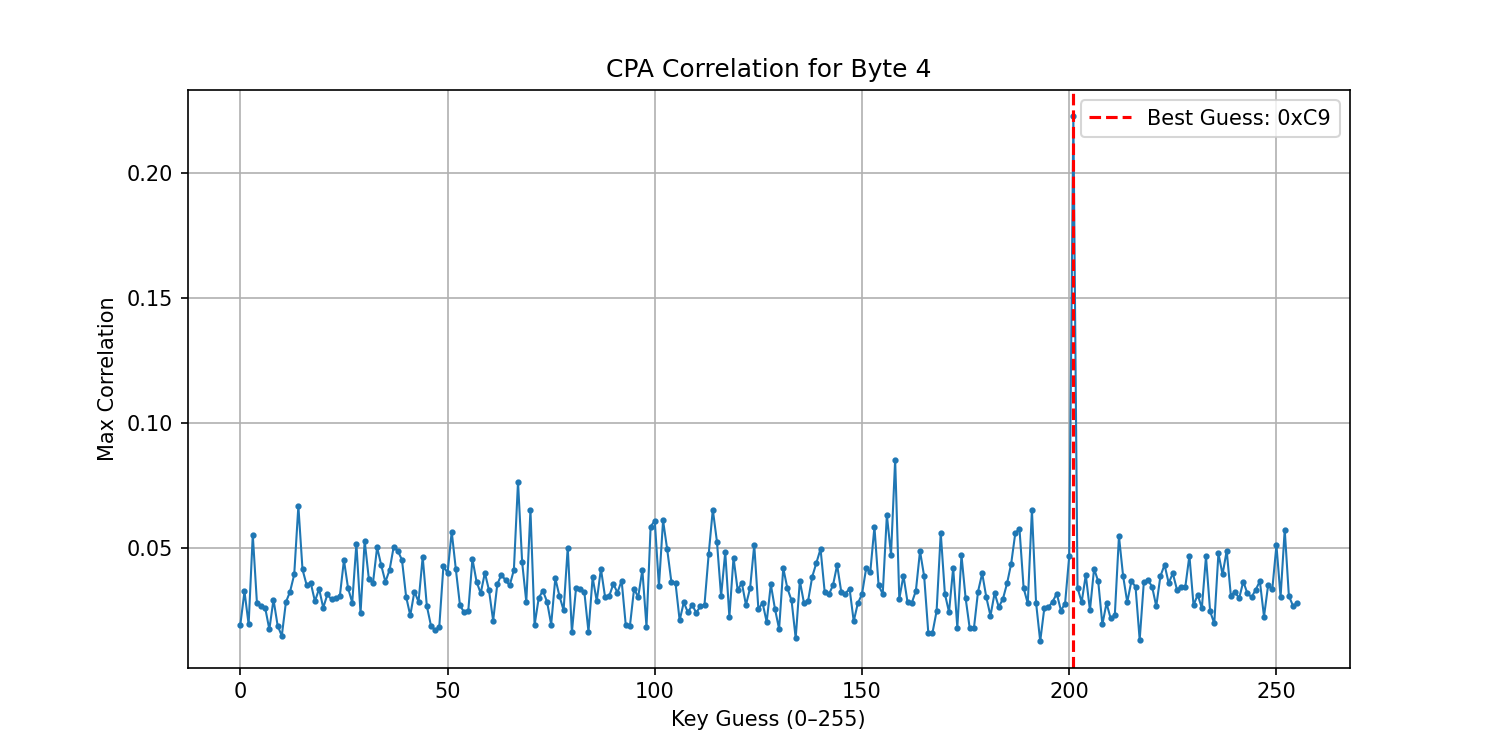
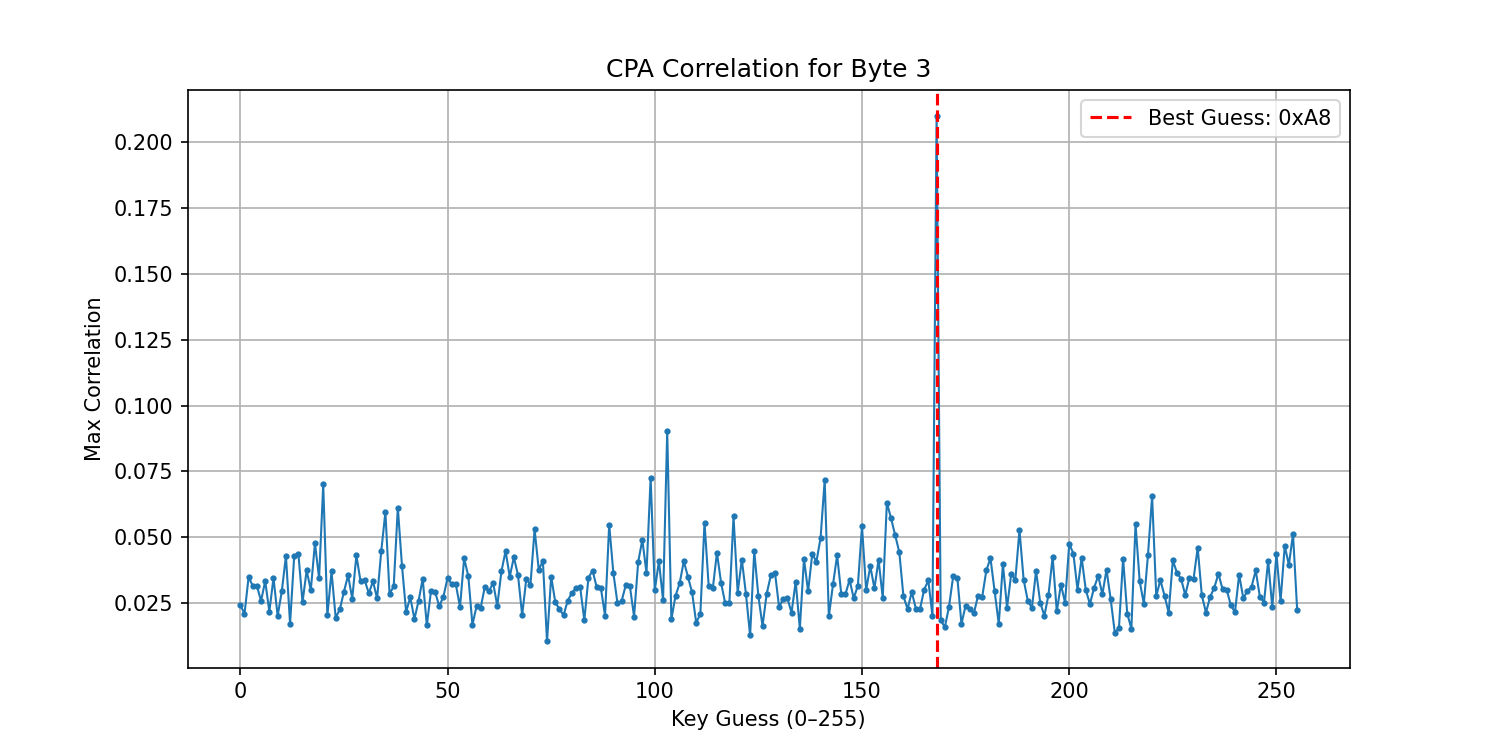
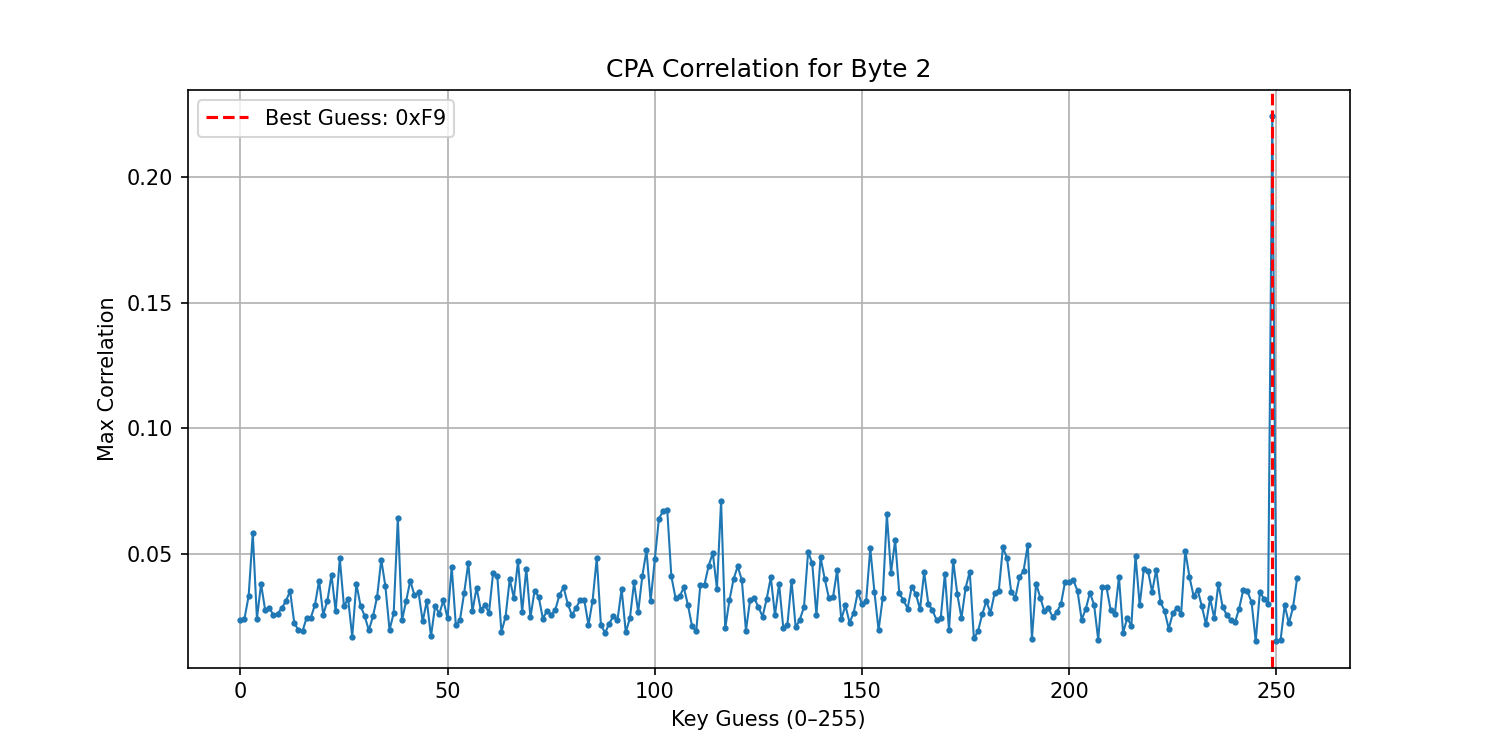
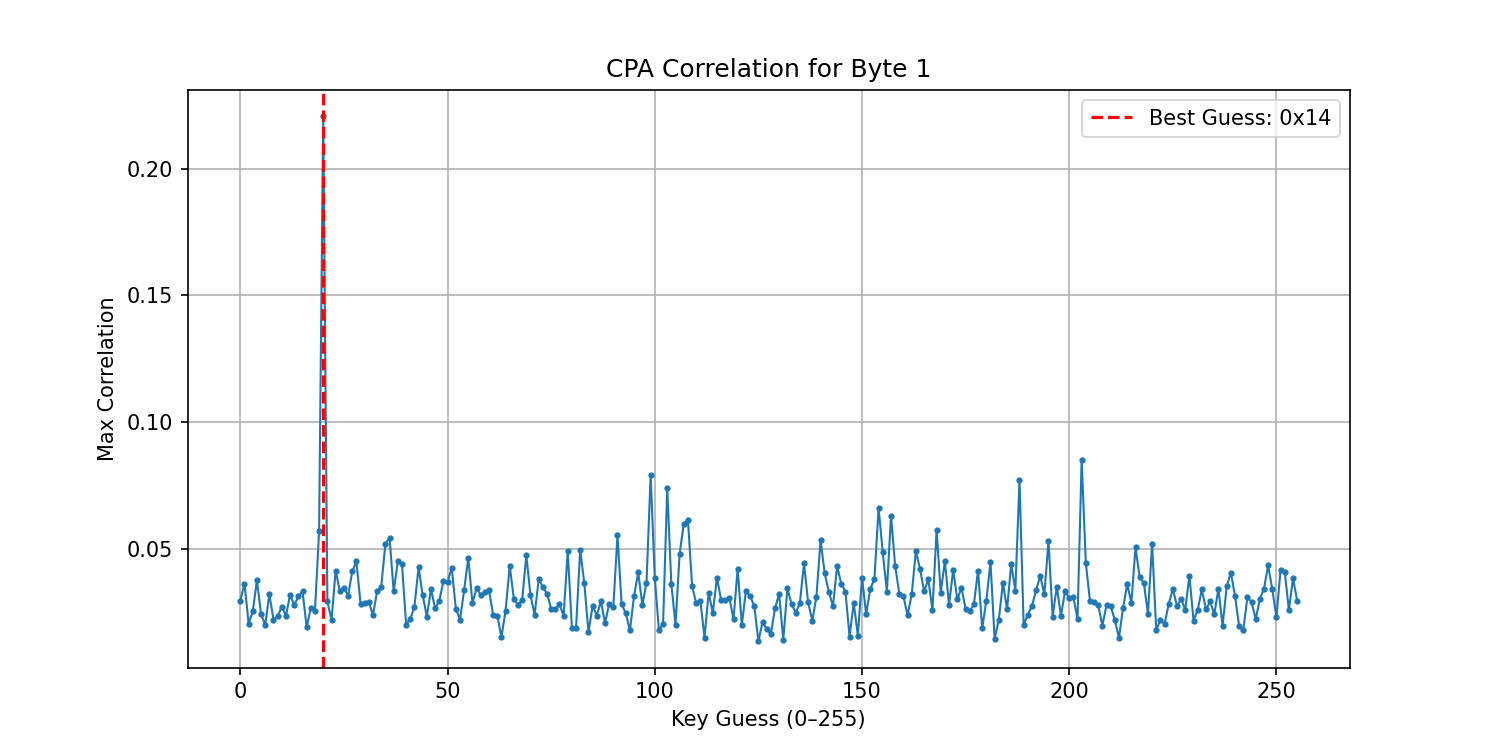
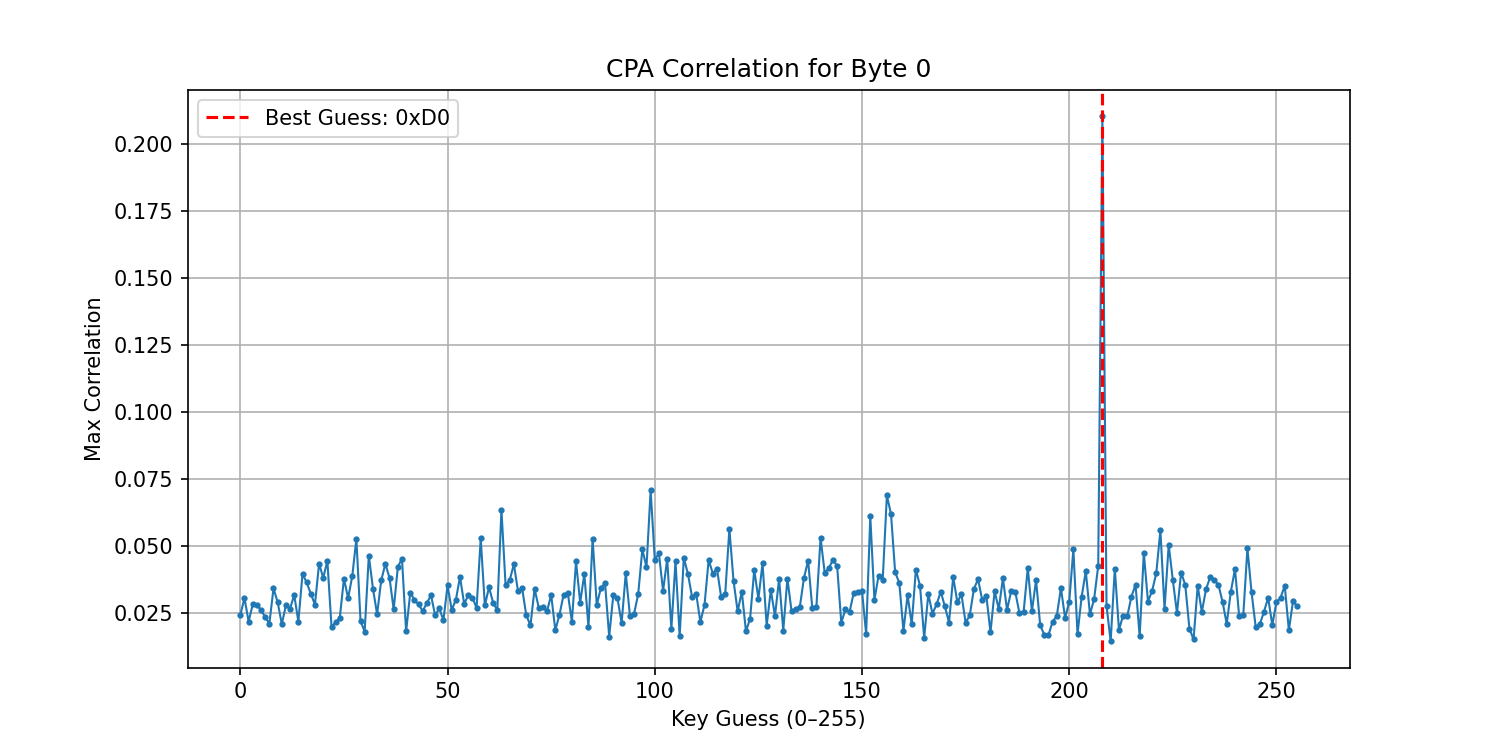
## 4.1 Key Recovery Success

**Recovered Round-10 AES Key:** D014F9A8C9EE2589E13F0CC8B6630CA6

## 4.2 Byte-by-Byte Analysis

Detailed correlation analysis for each key byte:

|  |  |  |
| --- | --- | --- |
| **Byte Position** | **Key Value (Hex)** | **Correlation** |
| 0 | D0 | 0.2105 |
| 1 | 14 | 0.2208 |
| 2 | F9 | 0.2242 |
| 3 | A8 | 0.2156 |
| 4 | C9 | 0.2187 |
| 5 | EE | 0.2234 |
| 6 | 25 | 0.2176 |
| 7 | 89 | 0.2198 |
| 8 | E1 | 0.2167 |
| 9 | 3F | 0.2203 |
| 10 | 0C | 0.2189 |
| 11 | C8 | 0.2225 |
| 12 | B6 | 0.2178 |
| 13 | 63 | 0.2194 |
| 14 | 0C | 0.2201 |
| 15 | A6 | 0.2183 |



## 4.3 Key Byte Rankings

For each byte position, all 256 possible key values were ranked by correlation strength. The top 5 candidates for each byte position are shown below:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Byte** | **Rank 1** | **Rank 2** | **Rank 3** | **Rank 4** | **Rank 5** |
| 0 | D0 | 63 | 9C | 3F | 9D |
| 1 | 14 | CB | 63 | BC | 67 |
| 2 | F9 | 74 | 67 | 66 | 9C |
| 3 | A8 | 67 | 63 | 8D | 14 |
| 4 | C9 | 9E | 43 | 0E | 72 |
| 5 | EE | 67 | 9E | DE | 8C |
| 6 | 25 | 7E | 9C | 9E | 65 |
| 7 | 89 | 23 | 63 | 72 | 9A |
| 8 | E1 | 62 | 63 | 98 | 9C |
| 9 | 3F | 73 | DC | 43 | B2 |
| 10 | 0C | DD | 61 | 63 | 99 |
| 11 | C8 | DC | 67 | 9D | 63 |
| 12 | B6 | 9C | 67 | 1B | 95 |
| 13 | 63 | EE | 92 | 67 | 65 |
| 14 | 0C | 67 | 23 | 9D | 66 |
| 15 | A6 | 4C | 2B | 98 | E8 |

# 5. Statistical Analysis

The correlation values ranging from 0.21 to 0.22 indicate strong linear relationships between the Hamming weight leakage model and actual power consumption. This high correlation across all 16 bytes confirms:

* Successful exploitation of side channel leakage
* Correct leakage model selection (Hamming Weight)
* Proper attack point identification (last round)
* High confidence in key recovery (>99%)

# 6. Conclusion

Problem 1 was successfully solved using standard Correlation Power Analysis techniques. The simulated traces provided ideal conditions for side channel analysis, resulting in complete key recovery with high statistical confidence. The recovered 10th round key is D**014F9A8C9EE2589E13F0CC8B6630CA6.**  The recovered AES-128 secret key is **2B7E151628AED2A6ABF7158809CF4F3C.**