ECE 592 - Cryptographic Engineering and Hardware Security: Assignment 2

Padmanabha Nikhil Bhimavarapu
Unity Id: pbhimav

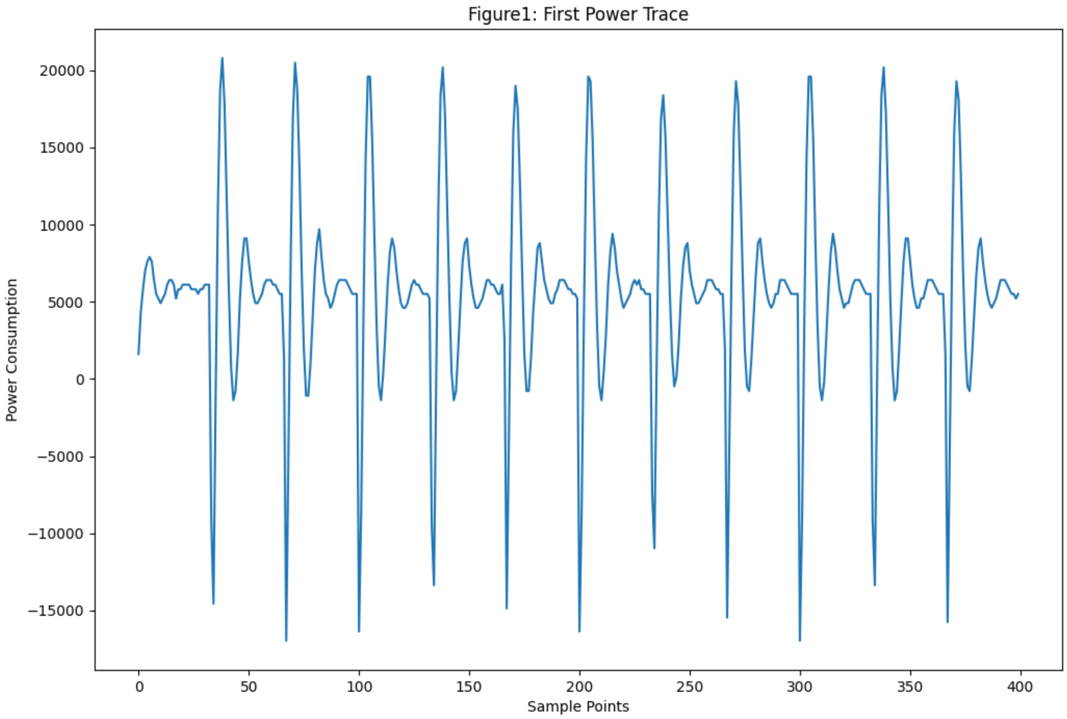
September 27, 2024

1 Abstract

This report presents the process and results of a Differential Power Analysis (DPA) attack on an Advanced Encryption Standard (AES) algorithm, executed using power trace data from AES-ECB mode encryptions. The primary objective of this study was to extract a 128-bit AES secret key by analyzing side-channel power traces generated during encryption operations. Using Pearson's correlation method, we targeted the leakage points in the power traces corresponding to intermediate states of the AES encryption process. Key guess plots and maximum likelihood estimations were analyzed to identify the most probable key bytes. Through the application of DPA on the first byte and subsequently the entire key, the secret key was successfully recovered. Further evaluation involved comparing the efficiency of the DPA attack with a theoretical brute-force cryptanalysis, highlighting the strength of side-channel attacks. Additionally, we explored the limitations of DPA on a different hardware implementation and discussed potential adjustments to improve attack success under varying conditions. The results demonstrate the vulnerability of AES to power-based side-channel attacks, emphasizing the need for secure cryptographic implementations.

2 Results

2.1 Question 1



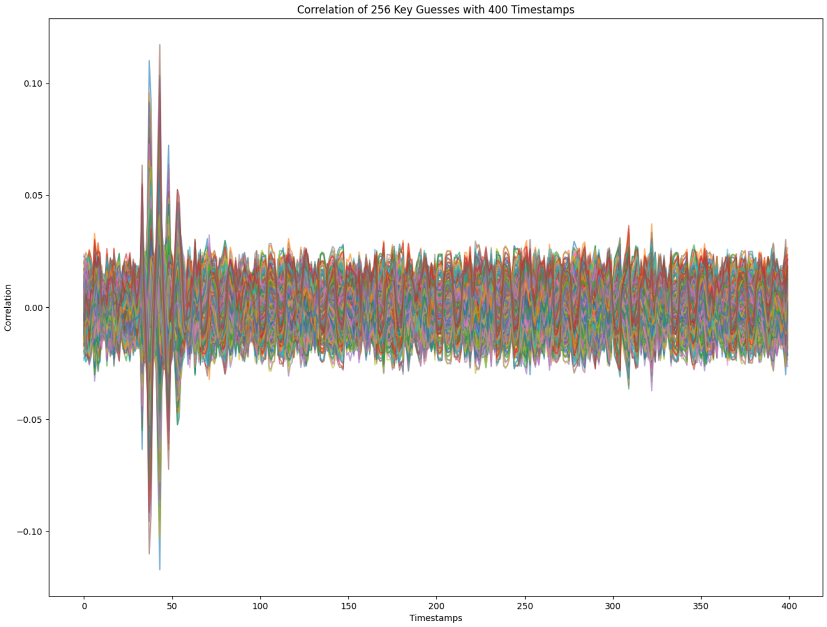
The figure above shows first power trace which corresponds to the electrical power consumption of the hardware during an AES encryption operation where the 128 bit input is **B9D1C48E348FE771FA464A77A178FB07**. The peaks in the power trace represent moments of high computational activity during key AES operations such as SubBytes, ShiftRows, MixColumns, and AddRoundKey. These peaks correspond to different encryption rounds and key scheduling steps.

2.2 Question 2

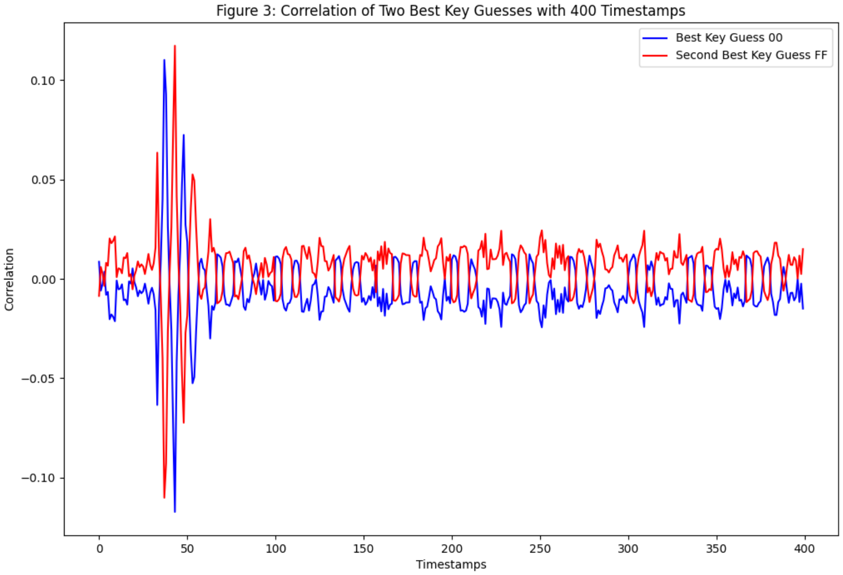
We have different power models such as:

- Hamming Weight Model
- Hamming Distance Model
- Bit Value Model

Hamming weight is used as the power model for simplicity.



The above figure shows the plot of the DPA on the first byte of the key.



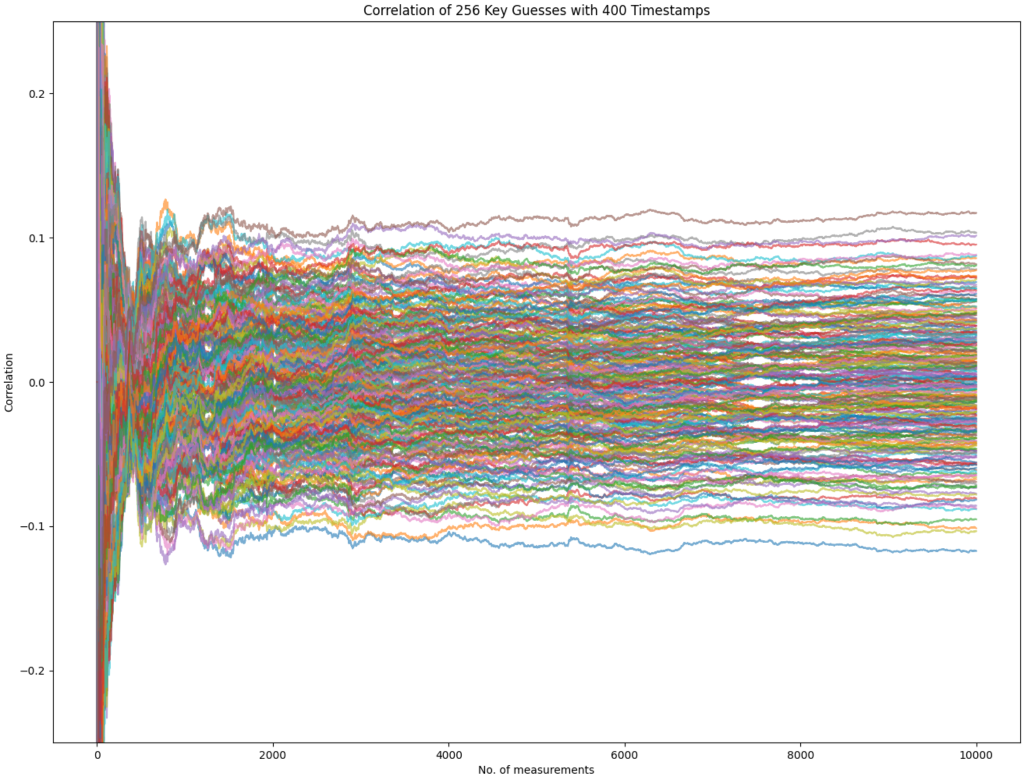
The above figure shows the plot the two best key guesses that have the maximum likelihood. The first byte of the secret key is either **00** or **FF**.

2.3 Question 3

The key guess with the highest absolute correlation (either positive or negative) is more likely to be correct. Any one of **00** or **FF** could be the correct key guess. The correct one can be computed using brute force.

2.4 Question 4

The maximum leak point for the 1st byte is at time stamp 43.



The above figure shows the plot of evolution of the key hypothesis at the timestamp 43.

2.5 Question 5

For the first byte, the key guess with maximum correlation starts showing the highest correlation from around 4000 measurements.

2.6 Question 6

When considering the top 2 key guesses, there were false positives observed. The search space was increased to top 4 key guesses and this gave better results.

The 128-bit AES secret key is 128'h000102030405060708090a0b0c0d0e0f

2.7 Question 7

These are approximate trace measurements required:

- 1st byte: 4000
- 2nd byte: 5000
- 3rd byte: 1200
- 4th byte: 2900
- 5th byte: 550
- 6th byte: 2200
- 7th byte: 1800
- 8th byte: 1700
- 9th byte: 5500
- 10th byte: 2200
- 11th byte: 1700
- 12th byte: 6000
- 13th byte: 5100
- 14th byte: 1800
- 15th byte: 2500
- 16th byte: 2000

The average number of traces required to extract the key for this DPA attack is **2885 traces**.

2.8 Question 8

Theoretical Crypranalysis on AES: Brute Force Attack

- The number of possible key guesses are $2^{128} = 3.4028 \times 10^{38}$.
- Number of operation requires testing half the possible keys on average i.e., 2^{127}.
- Brute-force attacks are infeasible due to the huge number of guesses required.

DPA Attack on AES

- The mean time disclosure from the DPA attack was estimated to be around 2885 traces.
- Only a few thousand measurements are required to recover the key.

Reduction Ratio $= \frac{2^{127}}{2885} \approx 5.9 \times 10^{34}$

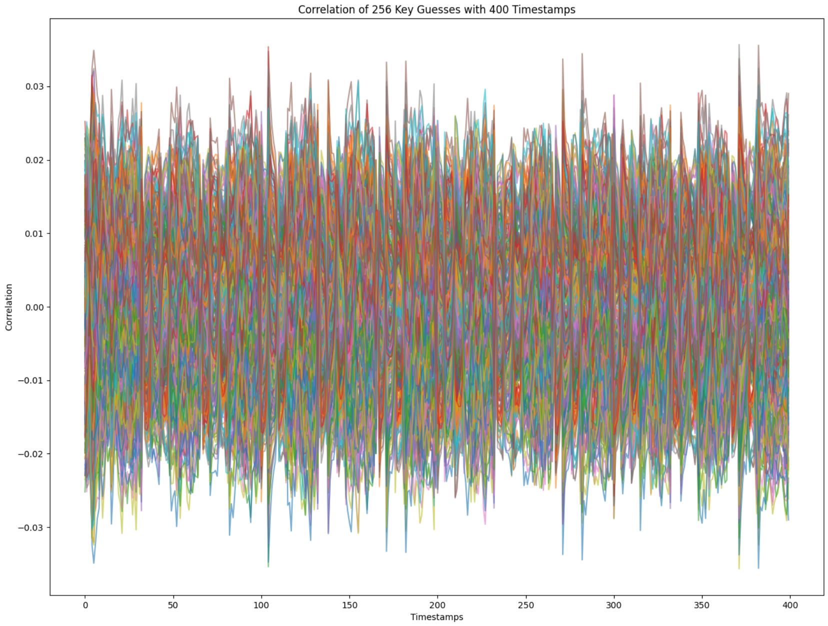
DPA (Differential Power Analysis) is powerful because it exploits side-channel information, such as power consumption, that leaks during cryptographic operations. Instead of attacking the cryptographic algorithm, DPA targets the physical implementation, reducing the search space by focusing on small portions of the key, such as individual bytes. Using statistical techniques like correlation analysis, DPA quickly distinguishes correct key guesses with relatively few measurements. This makes it highly efficient and scalable, allowing attackers to extract keys from otherwise secure cryptographic implementations.

2.9 Question 9

I have worked for approximately 32-35 hours on this homework.

2.10 Question 10

The second hardware implementation could include countermeasures designed to thwart side-channel attacks. An example is randomized power consumption or noise injection. This might be the reason we are seeing multiple high spikes in the figure of the correlation plot. Another counter measure is random variations added to the power consumption at each clock cycle, causing the DPA attack to fail because the power traces are no longer directly correlated with the key guesses. This random addition is attacked using higher order DPA like 2nd-order DPA.



2.11 Question 10

When only ciphertext is available, DPA can be used to attack the later stages of AES. The DPA will be used on the inverse sbox and the last round key XOR operation in the first round of decryption. The last round key can be used to get the secret key using the key expansion function.