Correlation Power Analysis of AES-128

Jessica Liao, YSP Student, *Andover High School*
Faraz Iqbal, YSP Student, *Franklin High School*
Cheng Gongye, Ph.D. Candidate, *Northeastern University*
Professor Yunsi Fei, Electrical and Computer Engineering, *Northeastern University*

Northeastern University Center for STEM Education

Young Scholars Program

Northeastern University Khoury College of Computer Sciences

Jessica Liao, Andover High School

Jessica is passionate about music and the arts and has been involved with ballet and dance ever since she was young. She finds AI to be especially fascinating through its many medical applications, and is considering to major in CS or Chemistry.

Contact: jessica.jia.liao@gmail.com

Motivation

Modern cryptography protects our information used in daily life from online banking traffic to securing precious memory on the cloud. The designs of modern ciphers are open to the public. Only the key needs to be kept a secret to encrypt the data. However, if said key is leaked, every piece of information is compromised.

Correlation Power Analysis

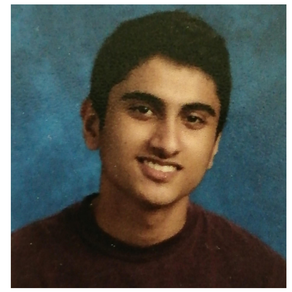
Obtain Power Traces from circuit (1) → Identify the Power model (2) → Identify Leakage Point (3) → Start CPA attack, byte by byte, with 256 possible keys per byte → Hamming Distance Model (2) → Pearson Correlation (4) → Plot the Results! Put all 16 keys together and the AES-128 key is recovered!

Each byte has 1/16th of the full AES-128 key, any of the 256 keys could be the right one.

Faraz Iqbal, Franklin High School

Faraz is interested in physics, calculus, and computer science and its real world applications in transport and travel. He aspires to start his own company or involved in a business revolving around the automobile industry.

Contact: faraz.norwood@gmail.com



1. Power Traces

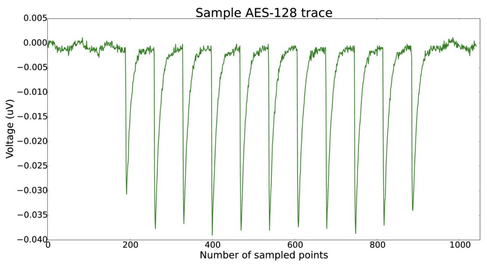


Figure 1. A sample of power traces measured at specific times

2. Hamming Distance Power Model

Input: Cipher Text Values and Key Guess Values

Hamming Weight
01011010
Results in:
4, or 00001000 in binary, as there are 4 ones.

Hamming Distance
Comparing (with XOR):
00001000 and 11010110
Results in:
11011110
The bit (the place for 0 or 1) will only be 1 (true) if the comparing bits in the same position are not the same value

Output: Presumed Power Consumption Value

3. Leakage Point

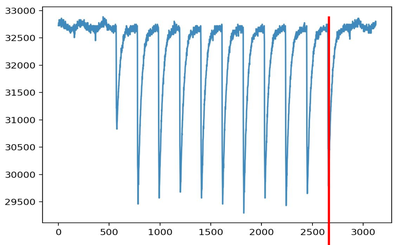


Figure 2. The leakage point, where the data relating to the key is the most obvious

4. Pearson Correlation

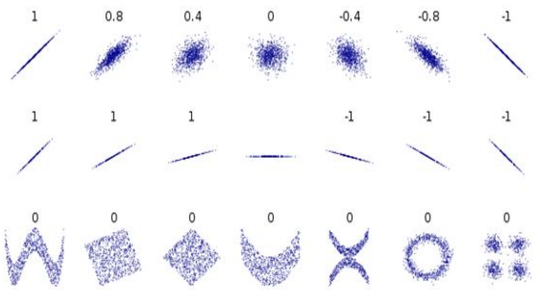


Figure 3. Pearson correlation values, the closer to a line the plotted points are, the more correlated and closer to 1 the points are

In CPA, Pearson Correlation compares the values between presumed and real power consumption, returning the correlation coefficient and placing them in an array in relation to the key guess.

Results

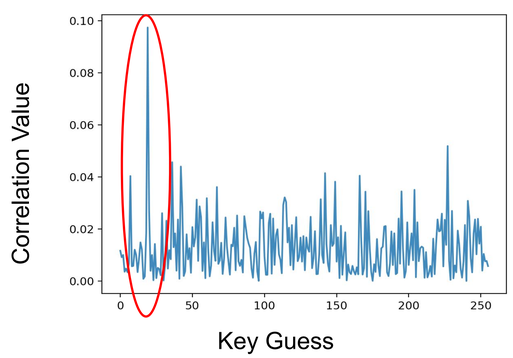


Figure 4. The true key of the first byte.

All 16 keys of the 16 bytes of the AES-128 encryption key were found. By putting together all 16 keys, the full AES-128 key can be recovered.

Slide Show QR Code

Conclusion

- CPA can be used to recover AES-128 keys
- The recovering of the AES-128 key for one byte can be extended to find all 16 bytes
- Improvement can be made by testing several different sets of power traces
- This can be used to test the security of a computer's hardware with this specific type of encryption algorithm
- The effect of AES-128 on computer hardware while running can be tested for different ways to mitigate the information being released

Acknowledgements

Department of Computer Engineering
Professor Yunsi Fei, Electrical and Computer Engineering, *Northeastern University*
Cheng Gongye, PhD Candidate, *Northeastern University*

Center for STEM Education
Nataasha Zaarour and Salima Amiji, *YSP Coordinators*
Claire Duggans, *Program Director*
Nicholas Fuchs, *Project Implementation Coordinator*

Young Scholar's Program at Northeastern University
Claire Duggan, Program Director

Image Source for Images at 2. Pearson Correlation and 1. Power Traces: Professor Yunsi Fei's Presentation on Power Analysis Attacks

More Detailed Poster (2nd slide):

This work was supported in part by the National Science Foundation under grants SaTC 1929300 and SaTC 1563697.