Nanyang Technological University
School of Computer Science and Engineering

CZ4055 Cyber Physical System Security

AY22/23 Semester 2

Correlation Power Analysis
Project Report

Group Name: A124 Lab

Group Members	**Matriculation Number**
Loh Zhi Heng	U2022581B
Liew Shaw Kee	U1922921D

Table of Contents

1. Introduction

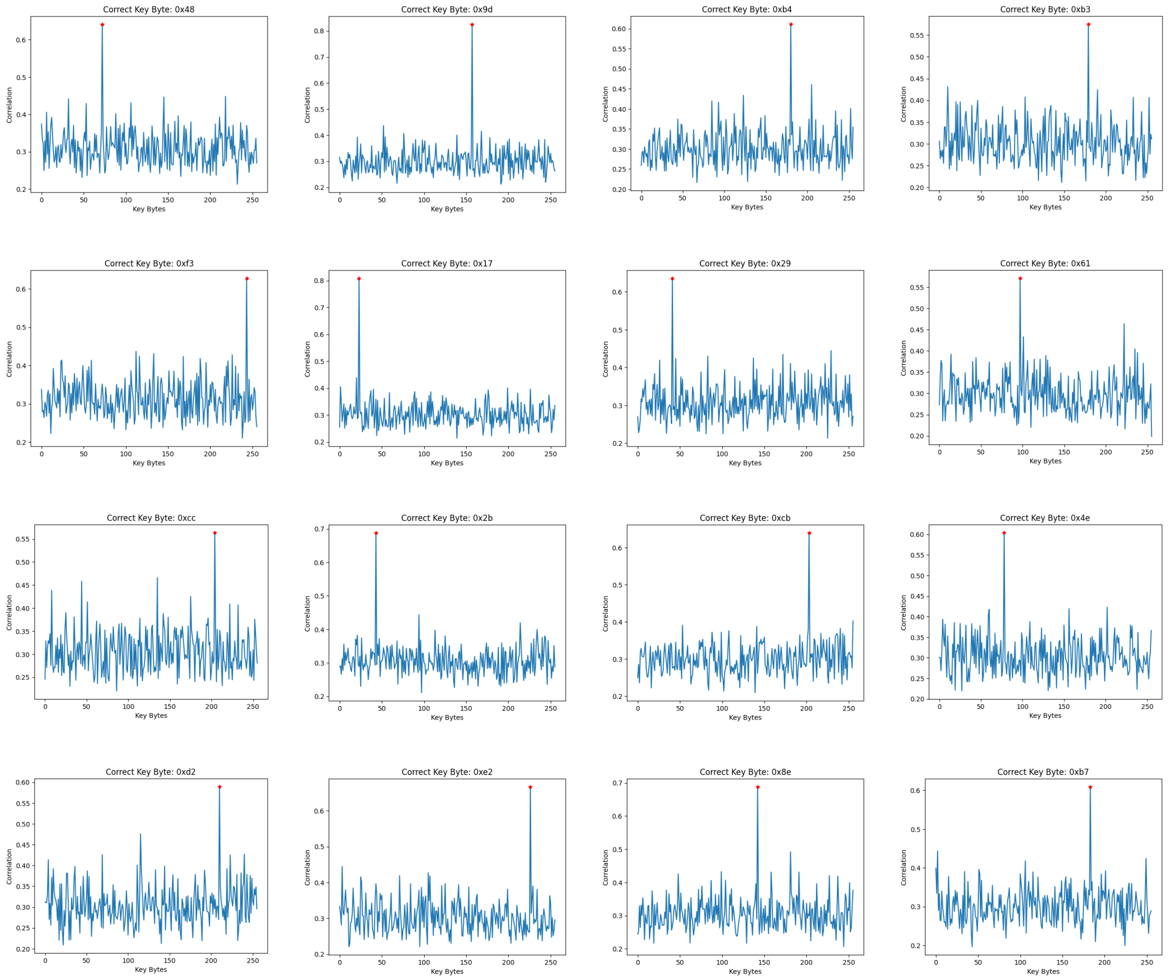
Correlation Power Analysis (CPA) is a type of side channel attack via power analysis whereby the attacker studies the power consumption of the cryptographic device to obtain the secret key that is stored inside the device. The attack requires the attacker to understand the model of the cryptographic device and the device's inputs or outputs, i.e. plaintexts and ciphertexts. The attack would use the model to guess intermediate values that are likely to occur in the computation of the cryptographic algorithm based on the known input and output values and also on the unknown secret key. They first compare the intermediate values to hypothetical power consumption values, then map the hypothetical power consumption to the device's real power consumption. To compare intermediate values to hypothetical power consumption values, standard power consumption models, such as the bit model, the Hamming Weight model, and the Hamming-distance model could be used [1]. These models are applicable if intermediate values that are stored in registers are attacked.

2. Implementation

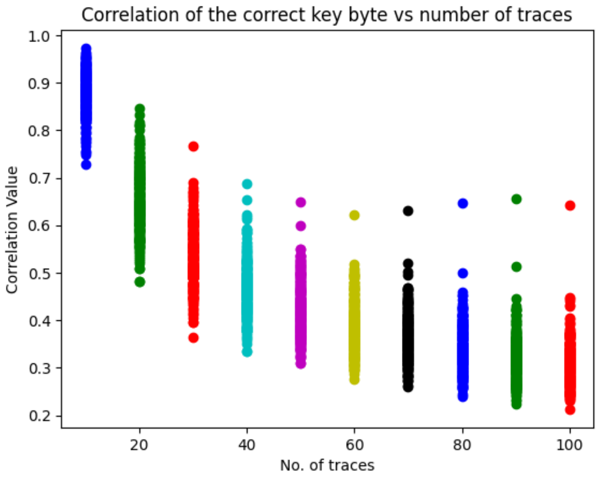
For our implementation of CPA, we need to uncover the secret key used in encryption of the plaintext using AES-128 algorithm. The intermediate value being exploited for this attack is the output of the SBOX which substitute the value of a given index with a fix value based onthe SBOX table of 256 values. By observing a device's behaviour over many operations with plaintexts as inputs or ciphertexts as outputs and making use of the Hamming Weight Power Model, we could retrieve the secret key one byte at a time. Hamming weight value is the number of bits switched between two values. The power consumption is directly proportional to the hamming weight value. Divide and Conquer strategy was used to retrieve the secret key one byte at time. For every possible value of each key byte, a hypothethical power consumption model is built. This was done by using Pearson's Correlation Coefficient to calculate the relation between the hypothetical power model and the actual power trace. Then, the hypothethical power model is compared with the real power consumption measurements for every key byte value. The model which best matches the real power consumption is the correct key byte. Thus, the entire secret key can be extracted after repeating 16 times to obtain all key byte. For more detail, refer to our code.

3. Results

For 100 traces, we plot the correlation of all possible key bytes, and identified the correct key byte. The correct byte has the highest correlation, which has a red dot in the figures.



For different numbers of traces, the correlation with the correct key byte for all 16 bytes is being plotted. The relationship between the correlation of the correct key byte and number of traces can be observed here. The number of traces range from 10 to 100, with intervals of 10. The correct key byte values have the highest overall correlation values.



4. Countermeasures against Power Analysis Attacks

Power analysis attacks exploit the correlation between the cryptographic devices' power consumption and the executed cryptographic algorithms' intermediate values. There are three main countermeasures that can be implemented at different levels i.e., software, hardware and cell levels, which aim at making the power consumption and the immediate values to be independent of one another [1]. To date, there are many papers which elaborated on the methods of protocol, hiding and masking. Gui et al. [2] focused on protocol. Studies by Kocher et. al. [3], Popp and Mangard [4], Mace et al. [5], Moore et al. [6] mentioned hiding scheme. Fahd et al. [7], Lee et al. [8], and Paschalis K. [9] focused on using masking. Soares et al. [10] presents an overview of countermeasures using both hiding and masking.

3.1 Protocol

In protocol, session keys are used to update secret keys during cryptographic operations, reducing the attackers' ability to gather information about each key and the number of traces. Hence making it harder for a power analysis attack to be performed. Although helpful in increasing the resiliency of the device to power analysis attacks, it is impractical to update secret keys frequently enough to prevent power analysis attacks.

3.2 Hiding

In hiding, noise is added to the observed signals during encryption to protect against power leakage collection. There are two types of hiding strategy, one is based upon random consumption, whereby power dissipation is different in each execution, and the other is uniform consumption whereby power consumed is uniform across executions [10]. The same intermediate results are being processed by both implementations with or without hiding countermeasures. As such, resiliency against power analysis attacks is based only on changing the power consumption characteristics of the cryptographic device's power.

3.3 Masking

In masking, the power that is needed to process intermediate values is largely independent of the actual intermediate values [10]. This is achieved by randomising the intermediate values. Usually, part of the input key and/or data words in a cryptographic primitive would be represented by two or more shares whereby the sum or the XOR of the shares are equal to the intended value of the word [9]. This significantly reduces the data dependency of the power consumption. An advantage of masking is that the device's power consumption characteristics do not need to be changed. However, masking is computationally intensive as it increases the number of computations executed.

3.4 Others

Apart from the above schemes, white-box modelling is also used against side channel attacks such as low-overhead generic circuit-level to prevent both electromagnetic (EM) and power side-channel attacks [11]. In elaboration, the crypto core is embedded with a signature suppression circuit, and routed locally within the lower-level metal layers. Hence, both power and EM side channel attack can be mitigated.

5. Conclusion

Even with an algorithm that computationally takes very long to crack such as AES, it is possible to crack them with a power analysis attack in a short time. Therefore, to enhance our data security, it is important to understand the various ways to implement power analysis attacks, and other side channel attacks so as to come up with countermeasures to protect against them.

6. References

[1] T. Popp, S. Mangard, and E. Oswald, "Power analysis attacks and countermeasures," IEEE Design &amp; Test of Computers, vol. 24, no. 99, p. x6, 2007.

[2] Y. Gui, S. M. Tamore, A. S. Siddiqui, and F. Saqib, "Key update countermeasure for correlation-based side-channel attacks," *Journal of Hardware and Systems Security*, vol. 4, no. 3, pp. 167–179, 2020.

[3] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. "Differential Power Analysis". In: CRYPTO'99. Ed. by Michael J. Wiener. Vol. 1666. LNCS. Springer, Heidelberg, Aug. 1999, pp. 388–397 (cit. on pp. 19, 24, 33).

[4] T. Popp and S. Mangard. "Masked Dual-Rail Pre-charge Logic: DPA- Resistance Without Routing Constraints". In: CHES 2005. Ed. by Josyula R. Rao and Berk Sunar. Vol. 3659. LNCS. Springer, Heidelberg, 2005, pp. 172–186 (cit. on p. 33).

[5] F. Mace, Francois-Xavier Standaert, I. Hassoune, Jean-Jacques Quisquater, and JeanDamien Legat. "A dynamic current mode logic to counteract power analysis". In: DCIS Conference on Design Of Circuits and Integrated Systems 11 (2004), pp. 186– 191 (cit. on p. 33).

[6] S.W. Moore, R.D. Mullins, P.A. Cunningham, R.J. Anderson, and G.S. Taylor. "Improving smart card security using self-timed circuits". In: ASYNC 211 (2002) (cit. on p. 33).

[7] S. Fahd, M. Afzal, H. Abbas, W. Iqbal, and S. Waheed, "Correlation Power Analysis of modes of encryption in AES and its countermeasures," Future Generation Computer Systems, vol. 83, pp. 496–509, 2018.

[8] J.-W. Lee, S.-C. Chung, H.-C. Chang, and C.-Y. Lee, "An efficient countermeasure against correlation power-analysis attacks with randomized montgomery operations for DF-ECC Processor," Cryptographic Hardware and Embedded Systems – CHES 2012, pp. 548–564, 2012.

[9] K. Paschalis, "Side channel attacks and countermeasures – Analysis of secure implementations" 2021. https://dione.lib.unipi.gr/xmlui/handle/unipi/13616.

[10] R. Soares, V. Lima, R. Lellis, P. Finkenauer Jr., and V. Camargo, "Hardware countermeasures against power analysis attacks: A survey from past to present," Journal of Integrated Circuits and Systems, vol. 16, no. 2, pp. 1–12, 2021.

[11] D. Das and S. Sen, "Electromagnetic and power side-channel analysis: Advanced attacks and low-overhead generic countermeasures through white-box approach," *Cryptography*, vol. 4, no. 4, p. 30, 2020.