Success Rate Model for Fully AES-128 in Correlation Power Analysis

Ali Akbar Pammu*, Kwen-Siong Chong, Ne Kyaw Zwa Lwin, Weng-Geng Ho, Nan Liu and Bah-Hwee Gwee
School of Electrical and Electronic Engineering
Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798
Email: *ali1@e.ntu.edu.sg

Abstract — **We propose a Success Rate (SR) estimation model for Correlation Power Analysis (CPA) attack on AES-128 encrypted devices. The SR is a ratio between the number of successful attacks to obtain secret key and the total number of attacks. There are two key features in the proposed model. First, we derive the Second Order Standard Deviation (SOSD) of the processed data to analyze their switching activities during encryption processes, to identify the Least Difficult Sub-Key (LDSK - the easiest revealable sub-key) and Most Difficult Sub-Key (MDSK – the hardest revealable sub-key). Second, we apply the Error Function Model (EFM) by using LDSK and MDSK to estimate the SR with respect to the number of power traces required to reveal the secret key. Our proposed SR estimation model is evaluated based on a Sukura-X encryption board and shows that our proposed SOSD requires only 1,000 processed data to determine the LDSK and MDSK. Based on the EFM of the LDSK and MDSK, it shows that 10% - 94% of SR requires 1,220 – 3,550 power traces respectively to reveal all the 16 sub-keys. We demonstrate the accuracy of our proposed SR estimation model by benchmarking against the two reporting techniques to evaluate 1-byte of key and show that the accuracy of our technique is 96% whereas other reported techniques are only 21% and 49%.**

Keywords — **Correlation Power Analysis, AES-128, Success Rate, Hiding Countermeasure, Second Order Standard Deviation, Error Function Model.**

I. Introduction

To date, most of the electronic communication devices are connected via internet. Shopping of goods, watching of videos and banking transactions can easily be done online. However, digital information available online is highly vulnerable against cyber-attack. Unauthorized party may intercept the unprotected data and retrieve the confidential information. Hence, effective encryption algorithms are required to protect the data from unauthorized party. Encryption algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), triple-DES (3-DES), Rivest Shamir Adleman (RSA) and Elliptic Curve Cryptography (ECC) typically encrypt the data (plaintext) into a form of encrypted data (ciphertext) and decrypt it to the original data upon receipt as to protect the data.

A new physical-attack approach which is known as Side Channel Attack (SCA) [1] has been reported to successfully extract the secret key of the encryption algorithm by analyzing the physical parameters such as power dissipation [2], electromagnetic interference [3] and timing [4] of electronic devices. Power analysis is the most common SCA where it analyzes the power dissipation profile to extract the secret key. Simple Power Analysis (SPA), Differential Power Analysis (DPA) and Correlation Power Analysis (CPA) are three types of SCA power analyses.

AES-128 algorithm, which processes 128-bit key size, requires 10 rounds of operations to encrypt the plaintext into ciphertext. The 10 rounds of operations makes AES-128 highly effective when compared to other encryption algorithms such as DES, 3-DES, RSA and ECC. However, due to the leaking of physical parameters correlate with intermediate data, the AES-128 may still be vulnerable against SCA, particularly against the CPA attack, as depicted in Fig. 1.

In Fig. 1, the power dissipated ($P = V_{DD} \cdot I_{DD}$) during the encryption process, which transforms the plaintext and the secret key into ciphertext through the AES-128 encrypted device, is measured and recorded. The power traces of the power dissipation, and the respective power model of the ciphertext based on the Hamming Distance (HD) are used for the CPA attack to reveal the secret key.

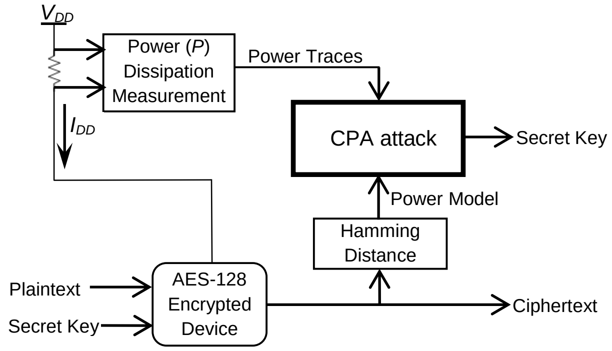


Fig. 1: CPA based Side Channel Attack on AES-128

In order to protect devices against CPA attack, two types of countermeasures, Masking and Hiding, have been developed [1]. The basic idea of masking is to randomize the intermediate data values during the execution of encryption algorithm at the algorithm level, while hiding is to break the dependency of the processed intermediate data and their correlated power dissipation [2].

Success Rates (SR) have been used as the figure of merit to evaluate the effectiveness of countermeasure techniques and it is defined as the ratio between the number of successful attacks to obtain the secret key and the total number of attacks. The first reported SR estimation technique which is based on Fisher-transformation [8] to determine the correlation coefficient difference of the two sub-keys. This reported technique assumed that the incorrect sub-keys are completely uncorrelated to the intermediate data and thus may not be accurate in evaluating the countermeasure technique. This assumption may not be practical as the incorrect sub-keys could still have correlations to the intermediate data. An improvement to this technique based on Cumulative Distribution Function (CDF) was presented in [6]. The idea is to compare the correct and incorrect sub-keys by means of multivariate normal distribution and the result is used to calculate the SR based on the CDF. This SR estimation technique [6] assumed the power dissipation measurement is noise free which may not be practical. Furthermore, even if same value of sub-key is used, the SR is different due to random bit-transitions of the power model [6]. Another method [5] implemented using the Rank Correction model to minimize the search space of the possible correct keys. By means of a small number of power traces, the first half of the sub-keys which have higher correlation coefficient is selected and the second half is discarded. For instance, by means of 100 power traces, the first 128 sub-keys based on their correlation coefficients are selected out of the total of 256 sub-keys. The selected 128 sub-keys are further evaluated with a higher number of power traces to reveal the correct sub-key. However, it is possible that the correct sub-key could be in the discarded pool as it exhibits low correlation coefficient in the early stage of power traces analysis.

In this paper, we propose a Success Rate (SR) estimation model for Correlation Power Analysis (CPA) attack on AES-128 implementation. The proposed technique exploits three key features of the SR. First, we derive the Second Order Standard Deviation (SOSD) of the intermediate data to analytically identify the Least Difficult Sub-Key (LDSK) and Most Difficult Sub-Key (MDSK). Second, our proposed technique can estimate the SR with respect to the number of power traces required to reveal the secret key based on its Error Function Model (EFM). Third, we introduce different noise levels to estimate different SRs, hence establishing a means to evaluate the countermeasure of hiding the power leakage against CPA attack. We demonstrate the accuracy of our proposed SR estimation technique by benchmarking against the reporting techniques to evaluate 1-byte of key and show that the accuracy of our technique is 96% whereas other reported techniques are only 21% and 49%. Furthermore, the accuracy level for the SR of 16 sub-keys is 94% based on measurement result which is not shown in any reported counterpart.

This paper is organized as follows. Section II presents the Correlation Power Analysis (CPA) of the AES-128 implementation. Section III presents the proposed SOSD based SR estimation model of AES-128. Section IV presents the measurement results and finally, conclusions are drawn in Section V.

II. CPA Attack on AES-128 implementation

CPA is the most prevalent type of power analysis attack against encrypted devices [7] based on the power leakage model. An attacker exploits the correlation between the power dissipated by the device and the intermediate data (power model) generated during the encryption process. In the AES-128 encryption process, there are 10 rounds of operations and at the last round consists of three operations such as S-Box, ShiftRow and AddRoundKey (XOR). As depicted in Fig. 2, the HD of the input (output of round 9) and the output (ciphertext) of the last round (round 10) is obtained to generate the power model. The correlation coefficient based on the correlation between the power model and the power traces can then be determined.

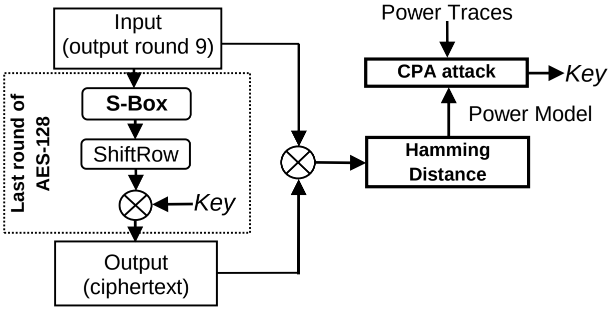


Fig. 2: CPA attack is based on HD power model of the last round AES

The CPA attack is a byte-based power analysis attack. Each byte of key (sub-key) is estimated by means of 256 possible values (1 byte = 8 bits and possibility is $2^8 = 256$), hence the correct sub-key is one of the 256 sub-key candidates. The CPA attack is performed by analyzing the correlation coefficient ($r_{i,j,t}$) of two variables, power model ($X_{i,j,m}$) and power traces ($Y_{t,m}$), for i = 1, …, 16 sub-keys, j = 1, …,256 sub-key candidates, t = 1, …, 400 sampling points, as described in Equation (1) as follows:

$$r_{i,j,t} = \frac{\sum_{m=1}^{n}(X_{i,j,m}-\bar{X}_{i,j})(Y_{t,m}-\bar{Y}_t)}{\sqrt{\sum_{m=1}^{n}(X_{i,j,m}-\bar{X}_{i,j})^2}\cdot\sqrt{\sum_{m=1}^{n}(Y_{t,m}-\bar{Y}_t)^2}} \qquad (1)$$

The correct sub-key, i, corresponds to the highest $r_{i,j,t}$ at particular sub-key candidate, j, and sampling point of power traces, t. For instance, in attacking the first sub-key (i =1), with 1000 power traces (n = 1000), the highest correlation coefficient ($r_{i,j,t}$ = 0.9) occurs at sampling point 61 (t = 61) for sub-key candidate 45 (j = 45), thus the correct first sub-key is 45.

It is worthwhile to note in Equation (1) that the sub-key, i, and sub-key candidate, j, from power model, $X_{i,j,m}$ are independent of the power traces, $Y_{t,m}$, and the evaluation of i and j of $X_{i,j,m}$ can be done independently of $Y_{t,m}$ to obtain the LDSK and MDSK. In short, our proposed technique can obtain the LDSK and MDSK analytically, thus without the need of power measurement.

The MDSK can then be used to estimate the required number of power traces to reveal all the 16 sub-keys. The number of power traces which is obtained based on MDSK value will be verified experimentally and the measurement results will be shown in Section IV.

III. Proposed SOSD based SR estimation model

The power model can be based on HD or Hamming Weight. The HD is used in our proposed technique as HD power model measure the bit-transitions of two registers (input and output of last round) in FPGA implementation, thus leaking more information and easier to evaluate our proposed technique. The HD power model is the statistical based prediction of power dissipation at the last round of AES-128 implementation. The LDSK and MDSK can then be obtained from the average value (μ) and variance of the intermediate data from the HD power model of each sub-key.

There are four steps to determine the LDSK and MDSK. Step 1, the distribution of the bit-transition, HD, of the each sub-key candidate is determined. Step 2, 256 standard deviations of bit-transition for each sub-key are calculated. Step 3, 16 sub-key SOSDs, ($\dot{\sigma}_1,\ \dot{\sigma}_2, \dots,\ \dot{\sigma}_{16}$), each based on the distribution of the 256 standard deviations are obtained. Step 4, the minimum and maximum of 16 sub-key SOSDs are obtained as the value of the MDSK and LDSK respectively.

In the Step 1, the 8 possible bit-transitions are measured for each sub-key candidate, since the employed register is 8-bit basis. The distribution of the bit-transition probability can be used to analytically estimate the power model of the processed intermediate data. For instance, the higher value of the distribution implies that the higher power dissipated during the operation. In the Step 2, the Standard Deviation (σ) of the bit-transition is determined as to identify the distribution of bit-transition thus, there are 256 standard deviations obtained for one sub-key. In the Step 3, SOSD ($\dot{\sigma}$) is determined based on 256 standard deviations for each sub-keys, as shown in (3) and hence there are 16 sub-key SOSDs. In the Step 4, LDSK and MDSK are obtained based on 16 sub-key SOSDs, ($\dot{\sigma}_1,\ \dot{\sigma}_2, \dots,\ \dot{\sigma}_{16}$) as shown in (4) and (5) respectively.

$$\sigma_{i,j} = [\sigma_{i,1}, \sigma_{i,2}, \dots\dots\ \sigma_{i,256}\ ] \tag{2}$$

Based on the result obtained from (2), the SOSD in (3) is calculated as follows:

$$\dot{\sigma}_i = \sqrt{\frac{1}{n-1}\sum_{n=1}^{j}(\sigma_{i,n} - \bar{\sigma}_{i,n})^2} \tag{3}$$

The LDSK and MDSK values are determined by using (4) and (5) respectively.

$$\dot{\sigma}_{LDSK} = Max[\dot{\sigma}_1, \dot{\sigma}_2, \dots\dots\ \dot{\sigma}_{16}\ ] \tag{4}$$

$$\dot{\sigma}_{MDSK} = Min[\dot{\sigma}_1, \dot{\sigma}_2, \dots\dots\ \dot{\sigma}_{16}\ ] \tag{5}$$

The MDSK could be identified from the distribution value of the bit-transition. If 256 sub-key candidates in particular sub-key are relatively close to each other, then every sub-key candidates are competing to be the highest in correlation coefficient value. Therefore, this byte requires more data to determine the correct sub-key of 256 sub-key candidates. The smallest the difference between the standard deviation of the bit-transition value, the more difficult is the attack. Whereas the LDSK is obtained based on the largest difference between the standard deviation of the bit-transition value. The LDSK and MDSK can then be obtained by means of the SOSDs of each sub-key (one byte).

IV. Experimental Results

The experiment is conducted based on the Sakura-X board [3], to measure the power dissipation exclusively for the AES-128 implementation. The values of the 16 sub-keys are selected for the AES-128 algorithm in hexadecimal = (15, AE, A2, 3C, 07, 91, 3D, 38, 9F, 99, 2E, 95, AE, 50, 59, 88). The results of the calculated SOSD is shown in Table I. The LDSK is the sub-key 9 while the MDSK is the sub-key 14.

The SOSD value of MDSK $\dot{\sigma}_{MDSK}$, which is equal to 2.657, is used for the SR calculation. The mean value, (μ_{th} = 367.54), is calculated based on the HD value for theoretical SR determination and SNR value of 52.07dB (μ_{ex} = 401.55) for experimental analysis of power dissipation measurement. Fig. 3 depicts the SR value of sub-key 14 resulting in the range of 2,800 to 3,700 power traces for both data measurement (based on HD power model) and measurement result (based on SNR measurement). The number of power traces for SNR measurement is approximately 1.4%, ((3,550-3,500)/3,550 = 0.014), higher than the data measurement for the same SR value due to low noise in the measurement of the power traces.

Table I
The SOSD value for each sub-key (16 sub-keys)

Sub-key	SOSD	
1	**5.840**	
2	**2.898**	
3	**2.787**	
4	**2.691**	
5	**6.136**	
6	**2.878**	
7	**2.723**	
8	**2.877**	
9	**6.274**	**LDSK**
10	**3.035**	
11	**2.826**	
12	**2.673**	
13	**5.965**	
14	**2.657**	**MDSK**
15	**2.919**	
16	**2.707**	

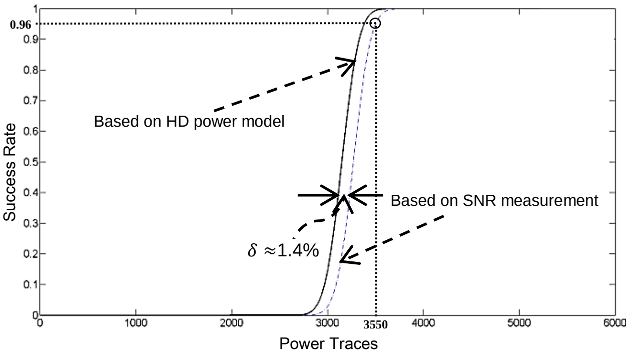
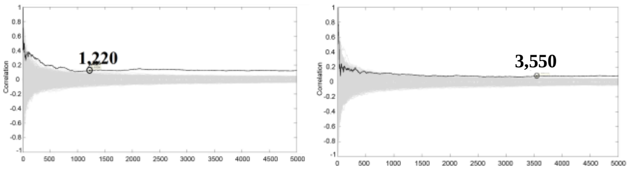


Fig. 3: Success Rate vs power traces of sub-key 14, MDSK

The correlation coefficient with respect to the number of power traces is depicted in Figs. 4(a) and 4(b) for the LDSK and MDSK respectively. The sub-key 14 (MDSK) requires a minimum of 3,550 power traces to reveal the correct sub-key as depicted in Fig. 4(b). Based on the SNR measurement in Fig. 3, the SR value at 3,550 power traces is 96% and it is relatively high SR value. This also implies that the required power traces to reveal all the 16 sub-keys is 3550. In Fig. 4(b), the difference of correlation coeficient between correct and wrong key is relatively small. This is due to the SOSD ($\dot{\sigma}_{MDSK}$ = 2.657) of sub-byte 14 is low when compared with other sub-keys. The correlation coefficients of the sub-key candidates in sub-key 14 are close to each other and hence difficult to distinguish. Thus, it requires more power traces to clearly identify the correct sub-key.



(a) (b)

Fig. 4: Correlation vs number of traces (a) LDSK, sub-key 9 (b) MDSK, sub-key 14

The minimum number of power traces to reveal at least one of the 16 sub-keys can be determined by LDSK value. The sub-key 9 which is the highest SOSD of LDSK ($\dot{\sigma}_{LDSK}$= 6.274) requires 1,220 power traces to reveal the correct sub-key 9, as depicted in Fig. 4(a). In contrast with sub-key 14, the correlation coefficients of sub-key candidates in sub-key 9 are highly distributed. Hence, the correct sub-key is easily distinguished with a small number of power traces.

The SR value of the 16 sub-keys which is calculated based on the EFM with LDSK and MDSK (e.g. μ, $\dot{\sigma}_{LDSK}$ and $\dot{\sigma}_{MDSK}$) is depicted in Fig. 5. The number of power traces at SR 10% and 94% is 1,220 and 3,550 respectively.

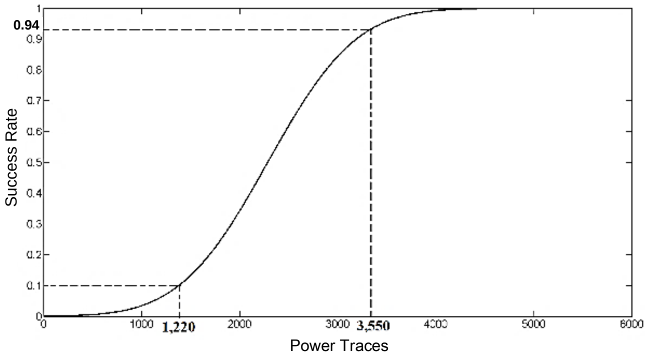


Fig. 5: SR for the 16 sub-keys based on CPA attack of AES-128

The comparison of our proposed SR model with the reported techniques is tabulated in TABLE II. Instead of obtaining the 16 sub-keys which needs more computational resources, our proposed SR estimation technique requires only MDSK to estimate the required number of power traces of the full 16 sub-keys. This has significantly improved the accuracy of the estimated number of the power traces on the CPA attack for the 16 sub-keys of AES-128 implementation. It is worthwhile to note that our proposed technique can be applied to estimate the SR of the CPA attack in different noise conditions.

TABLE II
COMPARISON OF THE PROPOSED SR AND REPORTED ESTIMATION MODEL BASED ON CPA ATTACK OF AES-128 IMPLEMENTATION

SR model	**Reported techniques**			**Proposed SR estimation model**
	[8]*	[9]+	[3]#	
SR for 16 sub-keys	1	1	3	16
Power Model (HD)	1-bit	1-bit	1-bit	8-bit
Sub-keys required	16 (all)	16 (all)	16 (all)	1 (MDSK)
Accuracy	~21.3%	~49.7%	NA	96%

*Fisher-transformation estimation model
+ CDF estimation model
#Trial-and error method is employed at different power traces

V. CONCLUSIONS

We have proposed the SR for the 16 sub-keys of AES-128 implementation based on the CPA attack. We have derived the SOSD of the power model to analytically identify the LDSK and MDSK. Based on the MDSK analysis, the minimum number of power traces required to reveal the secrete key has been analytically estimated. Our proposed technique can determine the SR with respect to the number of power traces to reveal the full 16 sub-keys and verify it using SNR ratio of the power dissipation measurement based on the EFM. In addition, our proposed technique can estimate the SR with respect to different noise levels to effectively evaluate the Hiding countermeasure against CPA attack. We have demonstrated the accuracy of our proposed SR estimation technique by benchmarking against the reporting techniques to evaluate 1-byte of key (one sub-key) and showed that the accuracy of our technique is 96% whereas other reported techniques are only 21% and 49%. Furthermore, the accuracy level for the SR of 16 sub-keys is 94% based on measurement result which is not shown in any reported counterpart.

ACKNOWLEDGMENT

This research work was supported by Agency for Science, Technology and Research, Singapore, under SERC 2013 Public Sector Research Funding, Grant No: SERC1321202098. The authors thank A*STAR for the kind support in funding this research.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Advances in Cryptology — CRYPTO' 99*. vol. 1666, M. Wiener, Ed., ed: Springer Berlin Heidelberg, 1999, pp. 388-397.

[2] K-S. Chong, K. Z. L. Ne, W-G. Ho, L. Nan, A.Akbar, B-H. Gwee and J. S. Chang, "Counteracting differential power analysis: Hiding encrypted data from circuit cells," *International Conference on Electron Devices and Solid-State Circuits (EDSSC), IEEE,* 2015, pp. 297-300.

[3] Y. Hori, T. Katashita, A. Sasaki, and A. Satoh, "SASEBO-GIII: A hardware security evaluation board equipped with a 28-nm FPGA," in *1st Global Conference on Consumer Electronics (GCCE), IEEE*, 2012, pp. 657-660.

[4] C. Arnaud and P.-A. Fouque, "Timing Attack against Protected RSA-CRT Implementation Used in PolarSSL," in *Topics in Cryptology – CT-RSA 2013*. vol. 7779, E. Dawson, Ed., ed: Springer Berlin Heidelberg, 2013, pp. 18-33.

[5] M. Nassar, Y. Souissi, S. Guilley, and J.-L. Danger, ""Rank Correction": A New Side-Channel Approach for Secret Key Recovery," in *Security Aspects in Information Technology*. vol. 7011, M. Joye, D. Mukhopadhyay, and M. Tunstall, Eds., ed: Springer Berlin Heidelberg, 2011, pp. 128-143.

[6] O. X. Standaert, E. Peeters, G. Rouvroy, and J. J. Quisquater, "An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays," *Proceedings of the IEEE*, vol. 94, pp. 383-394, 2006.

[7] Z. Martinasek, V. Clupek, and T. Krisztina, "General scheme of differential power analysis," *36th International Conference on Telecommunications and Signal Processing (TSP), IEEE,* 2013, pp. 358-362.

[8] S. Mangard, "Hardware Countermeasures against DPA – A Statistical Analysis of Their Effectiveness," in *Topics in Cryptology – CT-RSA 2004*. vol. 2964, T. Okamoto, Ed., ed: Springer Berlin Heidelberg, 2004, pp. 222-235.

[9] A. Thillard, E. Prouff, and T. Roche, "Success through Confidence: Evaluating the Effectiveness of a Side-Channel Attack," in *Cryptographic Hardware and Embedded Systems - CHES 2013*. vol. 8086, G. Bertoni and J.-S. Coron, Eds., ed: Springer Berlin Heidelberg, 2013, pp. 21-36.

[10] W. Jun, S. Yiyu, and C. Minsu, "Measurement and Evaluation of Power Analysis Attacks on Asynchronous S-Box," *IEEE Transactions on Instrumentation and Measurement,* , vol. 61, pp. 2765-2775, 2012.