A highly efficient power model for Correlation Power Analysis (CPA) of pipelined Advanced Encryption Standard (AES)

Ng, Jun-Sheng; Chen, Juncheng; Kyaw, Nay Aung; Lwin, Ne Kyaw Zwa; Ho, Weng-Geng;
Chong, Kwen-Siong; Gwee, Bah-Hwee

2020

Ng, J.-S., Chen, J., Kyaw, N. A., Lwin, N. K. Z., Ho, W.-G., Chong, K.-S., & Gwee, B.-H. (2020). A highly efficient power model for Correlation Power Analysis (CPA) of pipelined Advanced Encryption Standard (AES). Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS), 1-5. doi:10.1109/ISCAS45731.2020.9180778.

<https://hdl.handle.net/10356/146374>

© 2020 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at:
<https://doi.org/10.1109/ISCAS45731.2020.9180778>

Downloaded on 26 Apr 2023 13:04:54 SGT

A Highly Efficient Power Model for Correlation Power Analysis (CPA) of Pipelined Advanced Encryption Standard (AES)

Abstract— We evaluate the vulnerability of a pipelined Advanced Encryption Standard (AES) against Correlation Power Analysis (CPA) Side-Channel Attack (SCA). We identify that the registers in pipelined AES are most vulnerable against CPA SCA and propose a new power model targeting the switching activities of the registers. The proposed power model is constructed based on the Hamming Distance (HD) between the intermediate values stored in the registers in two consecutive clock cycles. Then, we analyze the vulnerability of pipelined AES under two scenarios. First, during regular pipeline operation where the device is performing AES pipeline operation. Second, in non-pipeline operation where we assume the adversaries can insert delay to the input of the device to increase the signal to noise ratio of the physical leakage information. The simulation results show that under regular pipelined operation, our proposed power model can reveal all the 16 key bytes in less than 4,900 traces, resulting in 4.7× more effective than the conventional power models. Under non-pipelined operation, our proposed power model requires only 590 traces to reveal all the 16 key bytes, which is 5.9× more effective than other power models.

Keywords— *Pipelined Advanced Encryption Standard (AES), Side-channel attack (SCA), Correlation Power Analysis (CPA)*

I. INTRODUCTION

In today's world, enormous amount of data are being generated and transmitted every second. According to IDC's white paper, the Global Datasphere will expand to 175 zettabytes in 2025 [1]. Hence, to protect the huge amount of data generation/transmission, effective cryptography algorithms are necessary. One of the most frequent used cryptography algorithms is the Advanced Encryption Standard (AES) [2]. It is the encryption standard established by the United States National Institute of Standards and Technology (NIST) as Federal Information Processing Standards Publications (FIPS PUBS) in 2001 [3].

AES is a symmetrical cryptography algorithm where the encrypts data of a fixed block length are 128 bits, 196 bits or 256 bits [4]. It encrypts data sequentially by going through different rounds of operations, depending on the length of the encryption key. For AES-128, the data is encrypted by going through 10 rounds of operations. Since the 10 rounds of operations are similar, hardware-implemented AES designs are usually designed in a serial structure where each round of operation takes 1 clock cycle to complete. However, to maximize the throughput, the pipelined AES is introduced. It increases the AES throughput for more than 10 times with the trade-off in terms of area [5]. Such kind of ultra-high-throughput AES is normally used for real-time encryption of

high-speed data communication and data encryption in the data storage center where the speed of encryption is critical.

Despite its secure features, AES remains vulnerable to Side-channel Attack (SCA) [6], [7]. SCA reveals the cryptography keys by correlating the intermediate data with the physical leakage of the device, such as power dissipation, electromagnetic, temperature, time, acoustic signals, etc. [8], [9]. In this paper, we particularly focus on Power Analysis Attack (PAA), which had been proven effective in revealing the cryptography key of AES [10]. Generally, there are 3 types of PAA, i.e. Simple Power Analysis (SPA), Differential Power Analysis (DPA) and Correlation Power Analysis Attack (CPA) [11]. Among these 3 types of attack, CPA is the most effective attack [12]. CPA exploits the secret keys of the AES by analyzing the correlation between the hypothetical power model and the power dissipation of the device, as illustrated in Figure 1. It had shown that CPA can reveal AES secret keys with only a few thousands of traces [13].

Figure 1: Illustration of CPA Attack

Most of the CPA analyses are based on standard AES design where at least 10 clock cycles are required for one complete encryption. To the best of our knowledge, there is no detailed study of CPA on AES with a pipelined design structure. Pipelined AES is implemented by pipelining 10 standard AES designs with registers inserted in between them. It prioritizes speed over area and power in order to achieve ultra-high throughput. We observed that the pipelined AES design generally does not come with SCA countermeasures with two main reasons. First, it is harder to attack pipelined AES due to its much lower Signal to Noise Ratio (SNR) physical leakage information for CPA. In a single clock cycle, 10 parallel AES encryption rounds occur concurrently. CPA will require much more traces to perform as the adversary may not be able to differentiate the power

dissipated in each encryption round. Second, the pipeline architecture imposes very high area overhead, implementing SCA countermeasures will further increase the area by $\sim 2\text{--}3\times$, which makes the cryptographic device very costly.

Hence, in this paper, the vulnerability of pipelined AES with low SNR value against SCA is evaluated. To effectively perform CPA attack on pipelined AES, a new power model is proposed. The proposed power model specifically targets on the register switching activities of the pipelined AES. It is constructed based on the Hamming Distance (HD) of the consecutive values stored by the registers. By performing CPA attack using the proposed power model, all the 128-bit keys can be revealed within 4,900 traces.

The remainder of this paper is organized as follows. The background knowledge of the pipelined AES and the CPA are discussed in Section II. The proposed power model is discussed in Section III. The CPA evaluation of the pipelined AES is reported in Section IV and finally the paper is concluded in Section V.

II. PIPELINED AES AND CORRELATION POWER ANALYSIS

A. Pipelined AES

There are a few pipelining techniques reported in [14] – [16] to maximize the throughput of AES algorithm. The reported techniques are capable to achieve throughput varies from $\sim 20\text{Gbps}$ to as high as 66.1Gbps . In this paper, we are investigating the CPA SCA on a basic pipelined AES without sub-pipelined architecture. The pipelined structure is implemented by increasing the number of AES cores to 10, i.e. equivalent to 10 rounds of standard AES design. Registers are inserted between the AES cores to make each of the cores a pipelining stage. The block diagram of the Standard AES and the pipelined AES are shown in Figures 2(a) and 2(b). The pipelined AES analyzed in this paper yielded throughput of 25.6Gbps , which is $\sim 10\times$ higher than standard AES.

B. Correlation Power Analysis(CPA)

CPA exploits the data dependency of a cryptographic device by analyzing a large number of power traces. It requires the construction of a hypothetical power model and assumes that this power model is correlated to the power dissipation of the device [17]. The power models are usually

built by using the Hamming Distance (HD) and Hamming Weight (HW) models.

The HD model assumes that the power dissipation of the device is proportional to the number of switching activities. It is based on the number of occurrences of 0-to-1 and 1-to-0 transitions during a specific period [18]. The number of flipping bits from A to B is denoted as $H(A \oplus B)$, and the HD model is expressed in (1) [19].

$$HD = aH(A \oplus B) + b \quad (1)$$

where a is the scalar gain while b is the constant which includes offset, time-dependent component and noise.

The HW model is similar to the HD model, by setting one of the intermediate values as zero. It assumes that the power dissipation of the device is proportional to the number of ‘1’ set in the processed data. The HW model is expressed in (2) [19].

$$HW = aH(A \oplus 0) + b \quad (2)$$

After the construction of the power model, the secret key of the cryptography device can be revealed by analyzing the linear correlation between the hypothetical power model and the actual power dissipation. Let k denotes the possible key candidature, t denotes time, the correlation coefficient of a key candidature at a particular moment, $r_{k,t}$, is expressed in (3) [12].

$$r_{k,t} = \frac{\sum_{i=1}^N (H_{i,k} - \bar{H}_k) \cdot (P_{i,t} - \bar{P}_t)}{\sqrt{\sum_{i=1}^N (H_{i,k} - \bar{H}_k)^2 \cdot \sum_{i=1}^N (P_{i,t} - \bar{P}_t)^2}} \quad (3)$$

where N is the number of power traces, H is the hypothetical power model and P is the actual power dissipation.

III. PROPOSED POWER MODEL

By using HD and HW models, various power models can be built based on different targeted intermediate values. For AES algorithm, conventional power models are targeting the input or output points of the SBox where the information of the secret keys leaks. To describe the power models, we denotes Hamming Distance between x and y as $HD(x,y)$, Hamming Weight of x as $HW(x)$, SubByte of input x as $SB(x)$, inverse SubByte of input x as $ISB(x)$, plaintext as PT , ciphertext as CT and key candidature as KEY .

Figure 2: Block diagrams of (a) standard AES and (b) pipelined AES

Table I summaries various power models that attack a hardware-implemented AES based on different intermediate values. These power models can be used to reveal the secret key of different kinds of serial AES experimentally. In the pipelined AES, different rounds of AES operations are executed together due to its pipelining nature. This leads to a significant reduction in SNR in attacking the targeted key bytes. The CPA attacks on pipelined AES is exploiting the 8-bits of information from 1,280-bits of switching activities, with the 10 AES cores contributes to 128-bit each. Neglecting the electronic noise, the SNR of the CPA on pipelined AES can be estimated as $8/1280$ which is equivalent to 0.00625 [12]. Hence, to improve the effectiveness in attacking pipelined AES, two methods are proposed.

TABLE I: LIST OF POWER MODELS BASED ON DIFFERENT INTERMEDIATE VALUES

Scheme	Power Model	Attack
HWF1	$HW(PT \oplus KEY)^+$	Logic state pattern of SBox Input
HWF2	$HW(SB(PT \oplus KEY))^+$	Logic state pattern SBox Output
HDF1	$HD(SB(PT \oplus KEY), PT)^+$	Switching pattern between plaintext and SBox Output
HDF2	$HD(SB(PT \oplus KEY), PT \oplus KEY)^+$	Switching pattern between SBox Input and Output
HWL1	$HW(CT \oplus KEY)^*$	Logic state pattern SBox Output
HWL2	$HW(ISB(CT \oplus KEY))^*$	Logic state pattern SBox Input
HDL1	$HD(ISB(CT \oplus KEY), SR(CT))^*$	Switching pattern between ciphertext and SBox Input

⁺ SCA on the first round of AES operations

^{*} SCA on the last round of AES operations

First, we do not alter the input of AES and attack the pipelined AES while it performs 10 rounds of operations simultaneously. In order to perform CPA attack efficiently, the power dissipation waveform of pipelined AES is analyzed. Figure 3 shows the power dissipation waveform of the pipelined AES. From the figure, the peaks can be observed in every 2.5ns. This corresponds to the rising and falling edge of the clock cycle. They are the power dissipated by the registers when latching in and latching out new data. Those peaks are the Physical Leakage Information (PLI) exploited by CPA to reveal the secret keys. Hence, the registers in pipelined AES are identified as the weak point for the adversaries to launch a CPA attack.

Figure 3: Power Dissipation Waveform of Pipelined AES.

Thus, we propose a new power model targeted on the registers of pipelined AES. In the pipelined AES, intermediate values stored by registers are no longer the

intermediate values of a plaintext between consecutive rounds of operations. Instead, the registers are storing the intermediate values of the same round of operation, but for different input plaintext. Hence, the conventional HD power models attacking the switching activities between ciphertext and SBox Input are no longer able to reveal the keys, because they are not the consecutive intermediate values stored in the registers. Thus, we construct a power model for the last round attack, targeting on the last registers of the pipelined AES by using the intermediate values from the consecutive output of pipelined AES. We denote CT_i as the i^{th} output of AES, then CT_{i+1} is the next output of AES. Our proposed power model is described as:

$$P = HD(ISB(CT_i \oplus KEY), ISB(CT_{i+1} \oplus KEY)) \quad (4)$$

The targeted intermediate values of the new proposed power model are illustrated in Figure 4. v indicates the intermediate values with respect to each ciphertext.

Figure 4: Illustration of the targeted intermediate values that are used to construct the proposed power model

For the second method, we assume that the adversaries can manipulate the input of pipelined AES to increase the SNR. Since 10 rounds of operations are executed simultaneously in one clock cycle, we can remove the pipeline properties of the device by delaying the arrival time of the AES input. If the input is delayed by 10 clock cycles, there is only one round of operation performed in each clock cycle, and there is in effect no pipeline operation. Under this non-pipeline operation, the power dissipation signal of the pipelined AES is similar to the signal of the standard AES design. Since there are only 128-bits of switching activities in one clock cycle, the SNR of CPA attack can be estimated as $8/128$ which is equivalent to 0.0625. Consequently, the SNR is increased by 10 times, which makes the CPA attack on pipelined AES design much more effective.

IV. CPA EVALUATION OF PIPELINED AES

The side-channel attack evaluation of the pipelined AES design is conducted by precise simulation in Synopsys Prime Time static timing analysis tool, based on @65nm CMOS process library cells. The supply voltage is at 1.2V and the clock frequency is set at 200MHz. The simulated power dissipation signal is resampled with a sampling period of 400ps to emulate the sampling period of an oscilloscope. 30,000 traces are generated under non-pipeline operation while 100,000 traces are generated under regular pipeline operation. The power traces simulated in the two scenarios are shown in Figure 5. From the figure, we can observe that in non-pipeline operation, the device dissipates lesser power because there is only one active round of encryption operation in each clock cycle. This increases the SNR and causes the variance of power dissipation of the targeted round more obvious.

Figure 5: Simulated power traces based on (a) regular pipeline operation and (b) input-delayed method

The simulated power traces are attacked using different power models discussed in Section III and the minimum number of traces required to reveal all 16 key bytes are tabulated in Table II. The results have shown that if the adversaries can delay the input of pipelined AES, most of the conventional power models can reveal all the 16 key bytes within 30,000 traces. However, if we allow the pipelined AES to perform regularly, the first-round attack requires $6.6\times$ more traces while the last-round attack is unable to reveal any key with 100,000 traces. Nevertheless, in both cases, our proposed power model outperformed all the power models. In CPA attack under non-pipelined operation, our proposed power model requires $4.7\times$ lesser power traces than other power models. While all the power models in the last round attack are unable to reveal the key under regular pipeline operation, our proposed power model is able to reveal all the key bytes with only 4,900 traces which is $4.7\times$ more effective than the first round attack by HWF2 (next best candidate). This implies that our proposed power model is highly correlated to the power dissipation profile of pipelined AES and can perform CPA attack on pipelined AES effectively.

TABLE II: RESULTS OF CPA ATTACKS BASED ON DIFFERENT POWER MODEL

Scheme	No. of traces	
	Regular pipeline operation	Input-delayed method
HWF1	No key <100,000 traces	No key <100,000 traces
HWF2	23,000	3,500
HDF1	No key <100,000 traces	No key <100,000 traces
HDF2	No key <100,000 traces	No key <100,000 traces
HWL1	No key <100,000 traces	12,000
HWL2	No key <100,000 traces	16,000
HDL1	No key <100,000 traces	No key <100,000 traces
Proposed	4,900	590

Figures 6(a), (b) and (c) depict the graphs of correlation coefficient versus the number of traces for HWL1, HWL2 and our proposed power model under regular pipeline operation. The red (solid) line represents the correlation coefficient of the correct key while the gray lines are the correlation coefficient of other key candidatures. The graphs

show that the proposed power model has a distinguishable correlation from $\sim 5,000$ traces onwards. This shows that the proposed power model predicts the power dissipation of pipelined AES accurately and hence significantly increases the efficiency of CPA attack.

Figure 6: Correlation Coefficient vs Number of Traces (a) Power Model HWL1 (b) Power Model HWL2 (c) Proposed Power Model

V. CONCLUSION

A new power model for side-channel attack evaluation of pipelined AES is proposed and evaluated. The proposed power model targeted the switching activities of the registers and can reveal all the 16 key bytes with $>4,900$ traces under regular pipeline operation, which is $4.7\times$ more effective than conventional power models. Under non-pipeline operation, the proposed power model reveals all the key bytes in less than 590 traces, which is $5.9\times$ more effective compared to other power models. Hence, it is concluded that despite its lower SNR in CPA attack, pipelined AES can be very vulnerable to SCA. Countermeasures need to be implemented such that the encrypted information is secured against the adversaries.

ACKNOWLEDGMENT

This research work was in part supported by Singapore National Research Foundation (NRF) under ‘‘SOCure’’ grant NRF2018NCR-NCR002-0001. The authors thank NRF for the kind support in funding this research.

REFERENCES

- [1] D. Reinsel, J. Gantz and J. Rydning, "The Digitization of the World From End to Core," IDC, Nov 2018.
- [2] J. Lim, W.-G. Ho, K.-S. Chong and B.-H. Gwee, "DPA-resistant QDI dual-rail AES S-Box based on power-balanced weak-conditioned half-buffer," in 2017 *IEEE International Symposium on Circuits and Systems (ISCAS)*, Baltimore, MD, USA, 2017.
- [3] National Institute of Standards and Technology (NIST), "Announcing the ADVANCED ENCRYPTION STANDARD (AES)," Nov 2001.
- [4] L. Wu, X. Wang, X. Zhao, Y. Cheng, D. Su and A. Chen, "AES design improvement towards information safety," in 2016 *IEEE International Symposium on Circuits and Systems (ISCAS)*, Montreal, QC, Canada, 2016.
- [5] D. Kotturi, S.-M. Yoo and J. Blizzard, "AES crypto chip utilizing high-speed parallel pipelined architecture," in 2005 *IEEE International Symposium on Circuits and Systems*, Kobe, Japan, 2005.
- [6] J. Dofe, J. Frey and Q. Yu, "Hardware security assurance in emerging IoT applications," in 2016 *IEEE International Symposium on Circuits and Systems (ISCAS)*, Montreal, QC, Canada, 2016.
- [7] P.-C. Liu, H.-C. Chang and C.-Y. Lee, "A True Random-Based Differential Power Analysis Countermeasure Circuit for an AES Engine," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 59, no. 2, pp. 103 - 107, 2012.
- [8] A. A. Pammu, K.-S. Chong, K. Z. N. Lwin and B.-H. Gwee, "High Secured Low Power Multiplexer-LUT Based AES S-Box Implementation," in 2016 *International Conference on Information Systems Engineering (ICISE)*, Los Angeles, CA, USA, 2016.
- [9] B. Ege, K. Papagiannopoulos, L. Batina and S. Picek, "Improving DPA resistance of S-boxes: How far can we go?," in 2015 *IEEE International Symposium on Circuits and Systems (ISCAS)*, Lisbon, Portugal, 2015.
- [10] P. Kocher, J. Jaffe, B. Jun and P. Rohatgi, "Introduction to differential power analysis," *Journal of Cryptographic Engineering*, vol. 1, no. 1, pp. 5-27, 2011.
- [11] A. A. Pammu, K.-S. Chong and B.-H. Gwee, "Highly secured state-shift local clock circuit to countermeasure against side channel attack," in 2017 *IEEE International Symposium on Circuits and Systems (ISCAS)*, Baltimore, MD, USA, 2017.
- [12] S. Mangard, O. Elisabeth and T. Popp, *Power Analysis Revealing the Secret of Smart Cards*, Springer, 2007.
- [13] N. Benhadjyoussef, H. Mestiri, M. Machhout and R. Tourki, "Implementation of CPA analysis against AES design on FPGA," in 2012 *International Conference on Communications and Information Technology (ICCIT)*, Hammamet, 2012.
- [14] A. Hodjat and I. Verbauwhede, "A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA," in 12th *Annual IEEE Symposium on Field-Programmable Custom Computing Machines*, Napa, CA, USA, 2004.
- [15] K. Rahimunnisa, P. Karthigaikumar, N. Anitha Christy, S. Suresh Kumar and J. Jayakumar, "PSP: Parallel sub-pipelined architecture for high throughput AES on FPGA and ASIC," *Central European Journal of Computer Science*, vol. 3, no. 4, pp. 173-186, 2013.
- [16] Q. Liu, Z. Xu and Y. Yuan, "A 66.1 Gbps Single-pipeline AES on FPGA," in 2013 *International Conference on Field-Programmable Technology (FPT)*, Kyoto, 2013.
- [17] M. Alioto, L. Giancane, G. Scotti and A. Trifiletti, "Leakage Power Analysis Attacks: A Novel Class of Attacks to Nanometer Cryptographic Circuits," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 57, no. 2, pp. 355 - 367, 2010.
- [18] A. A. Pammu, W.-G. Ho, N. K. Z. Lwin, K.-S. Chong and B.-H. Gwee, "A High Throughput and Secure Authentication-Encryption AES-CCM Algorithm on Asynchronous Multicore Processor," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 1023 - 1036, 2018.
- [19] E. Brier, C. Clavier and F. Olivier, "Correlation Power Analysis with a Leakage Model," in *Cryptographic Hardware and Embedded Systems - CHES 2004*, Springer, Berlin, Heidelberg, 2004, pp. 16-29.