High-Level Simulation for Side Channel Attacks

Masaya Yoshikawa and Toshiya Asai

Abstract— **Although an encryption algorithm is theoretically secured, by analyzing secondary information that is not directly related to the encryption algorithm—such as power consumption and electromagnetic waves that are generated during cipher processing—a secret key for an encryption device can be estimated in a short time. In particular, differential power analysis (DPA) is very risky, because it cracks security codes by statistically processing the difference in electricity consumption and can be easily attacked. Therefore, it is important to verify DPA in the early stage of designing an algorithm. This study proposes a new simulator that can evaluate the resistance of DPA at the algorithm design level.**

Index Terms—**Side-Channel Attack, Cryptography circuit, Mix-level simulation, Power consumption model, Tamper-resistance verification**

I. Introduction

RECENTLY, systems to store monetary and personal information using large scale integration (LSI), such as integrated circuit (IC) cards, have been widely diffused as social infrastructures. In LSI, cryptography circuits are used to protect confidential information, and the encryption standard used is theoretically secured. However, although an encryption algorithm is theoretically secured, by analyzing secondary information that is not directly related to the encryption algorithm—such as power consumption and electromagnetic waves that are generated during cipher processing—a secret key for an encryption device can be estimated in a short time. [1]-[21]

In particular, differential power analysis (DPA) [11]-[17] is very risky, because it cracks security codes by statistically processing the difference in electricity consumption and can be easily attacked. Therefore, it is important to verify DPA in the early stage of designing an algorithm. This study proposes a new simulator that can evaluate the resistance of DPA at the algorithm design level.

Moreover, experiments proved the validity of the proposed simulator.

II. Related studies

Regarding tamper-resistance simulation, several studies on different design phases have been reported. First, regarding tamper-resistance simulation at the algorithm design phase, a paper [3] noticed that the hamming weight of the medium value in a round of data encryption standard (DES) cryptogram reflected a bias of the transition probability due to nonlinearity of substitution-box (S-BOX). This result indicated that DPA simulation at the algorithm level could be performed using the hamming weight as a power consumption model. However, this simulation can not distinguish between hardware architectures.

Next, regarding the logic design phase, a paper [4] extracted the logic toggle information from the results of delay simulation. Then the paper simulated a CPA attack using the logic toggle information as power consumption model. Regarding studies on tamper-resistance verification of actual devices, such as field-programmable gate array (FPGA) and application-specific ICs (ASICs), papers [5],[6] reported a CPA evaluation according to the advanced encryption standard (AES) embedding method by using a side-channel attack standard evaluation board-R (SASEBO-R).

A tamper-resistance simulation method using a high-accuracy power consumption model at the algorithm level developed in the present study has not been reported to our knowledge.

III. Proposed simulation

In simulations of tamper resistance to side-channel attacks at the algorithm level, power consumption of all circuits need not be handled, but that of combinational circuits with nonlinearity, such as SubBytes transform circuits of AES, should be handled. In this study, to realize a high-accuracy and high-speed tamper-resistance simulation, a mixed-level method was devised in which a sophisticated power consumption model was introduced into a circuit block necessary for tamper-resistance verification. The verification environment was defined by the programming language employed into the other circuit parts.

A. Power consumption model

In general, power consumption of a complementary metal oxide semiconductor (CMOS) circuit is the sum of static and dynamic power consumption. However, in the power analysis attack, static power consumption is not necessary. Moreover, dynamic power consumption is in proportion to logic toggle frequency and load capacity. This study proposes a new power consumption model for power analysis attacks, taking into consideration the toggle frequency and load capacity. Using AES as a concrete example, the creation procedure of the power consumption model is explained below.

First, the logic is synthesized for a SubByte transform circuit with nonlinearity. From the net list of the synthesized results, the toggle frequency of each net is calculated. In the

This research was supported by Japan Science and Technology Agency (JST), Core Research for Evolutional Science and Technology (CREST). And this work also supported by VLSI Design and Education Center (VDEC), The University of Tokyo with the collaboration with Synopsys Corporation.

Masaya Yoshikawa and Toshiya Asai are with Department of Information engineering, Faculty of Science and Engineering, Meijo University, Nagoya, JAPAN. (corresponding author to provide e-mail: evolution_algorithm@ yahoo.co.jp).

ISBN: 978-988-19251-2-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

proposed power consumption model, the correlation between the load capacity and the fan-out number in each net is used to estimate the dynamic power consumption. As shown in Table 1, regarding each input pattern for the SubBytes transform circuit, the result obtained by multiplying the toggle frequency of each net and the fan-out number is defined as the dynamic power consumption of the input.

TABLE I
ESTIMATION OF POWER CONSUMPTION

Input	Output	#Toggle	#Fan-out	Estimated Power
11001010	11001010	45	3	135
10001010	10101011	56	4	224
01111010	01001010	40	3	120
10001001	01000010	33	5	165
11001111	11011011	78	3	234
01000010	01101011	55	4	220

In this study, to achieve high-speed simulation, dynamic power consumption P is approximated by formula (1) as follows:

$$P = c_0*x_0 + c_1*x_1 + c_2*x_2 + c_3*x_3 + c_4*x_4 + \cdots\cdots + c_n*x_n \quad (1)$$

where x_1 and x_2 represent input and output patterns, and c_0 and c_1 represent coefficients. The coefficients in formula (1) are obtained by the multiple linear regression analysis using Table 1. Using the obtained coefficients, the electricity consumption model for the SubBytes transform circuit is created. Figure 1 shows the creation procedure of the power consumption model.

B. Procedure of simulation

Figure 2 shows the procedure of the simulation of the power analysis attack using the proposed power consumption model. In this figure, the function of the power consumption model expressed by formula (1) is built into the encryption program, the process of encryption is executed to N plain texts, and N cipher texts and N pieces of power consumption data are acquired.

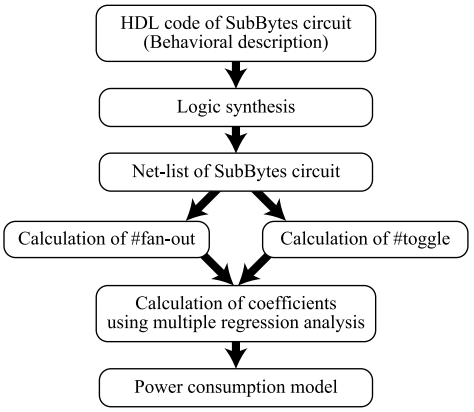

Fig.1 The creation procedure of the power consumption model

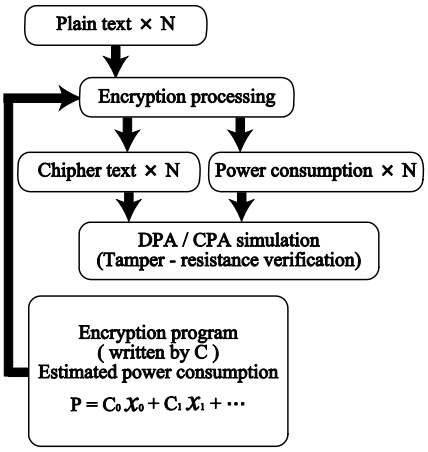

Fig.2 The creation procedure of the power consumption model

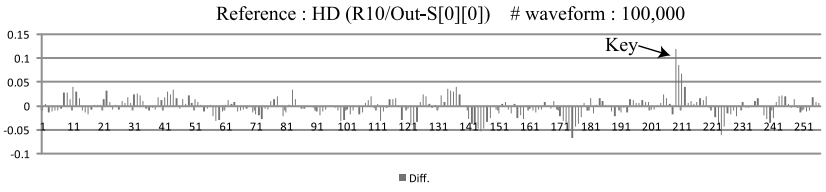

Fig.3 Result of DPA attack on algorithm level simulation

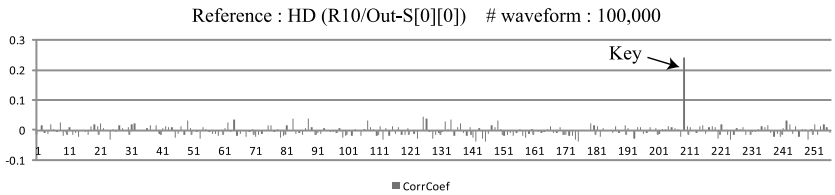

Fig.4 Result of CPA attack on algorithm level simulation

Here, only the power consumption data of the timing,

ISBN: 978-988-19251-2-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

IV. Evaluation experiments and discussion

A. Experimental conditions

To verify the validity of the proposed simulation method, several comparison experiments were performed under the following conditions: (1) as the platform of the experiments, CPU: Core 2 Duo 2 GHz, memory: 2 GB was used; (2) for logic synthesis in Figure 1, Design Compiler (Synopsys Inc., CA, USA) was used; (3) the tamper-resistance verification environment in Section 3.2 was written in the C language; (4) the encryption algorithm of the advanced encryption standard (AES) is to be verified; and (5) as the configuration methods for the device, truth table, PPRM3, and composite field methods were adopted.

B. Evaluation of the algorithm level simulation

First, we implemented the proposed simulation in order to evaluate tamper-resistance on algorithm level. Figures 3 and 4 show the simulation results. Figure 3 shows the result of the DPA attack and Figure 4 shows that of CPA attack. The proposed simulation method can achieve the both attacks as shown in Figures 3 and 4.

C. Comparisons of the power consumption models

Several comparison experiments were performed to verify the accuracy of the proposed power consumption model for the SubByte transform circuit. As the object to be compared, an power consumption model with hamming weight or hamming distance, which had been published, was used.

Figures 5,6,7, and 8 show the results of the comparison experiment. In each figure, the horizontal axis expresses the transition bit number of input terminals at 8 bits, and the vertical axis expresses the normalized power consumption value to compare power consumption.

The normalized power consumption value was obtained by dividing power consumption at each input and output in Table 1 by the average of power consumption peaks of all cycles during the simulation. As shown in Figure 5, in the power consumption model with hamming weight or hamming distance, since configuration methods of hardware cannot be considered, the truth table, PPRM3, and composite field methods all result in the same power consumption model. In the proposed power consumption model, high-accuracy estimation of power consumption could be realized, in which the difference in the configuration method of the device was reflected.

D. Comparisons of different architectures

Using the proposed power consumption model, an experimental CPA attack on the AES was performed, following the simulation procedure shown in Figure 2. The experimental results are shown in Figure 9, where the vertical axis expresses the number of specified keys and the horizontal axis expresses the number of required waveforms. Similar to the CPA results obtained when an actual device was used [7], the key was specified by a similar number of waveforms in the true table and PPRM3 methods, but that was specified by a larger number of waveforms in the composite field method as shown in Figure 9.

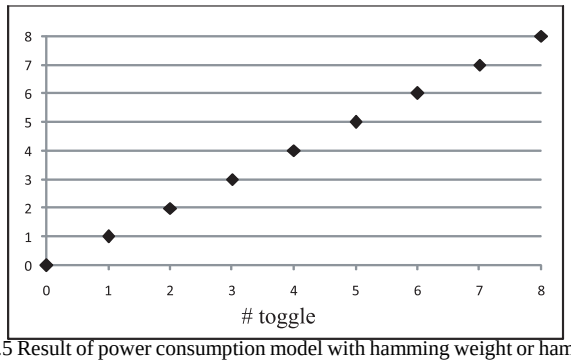

Fig.5 Result of power consumption model with hamming weight or hamming distance

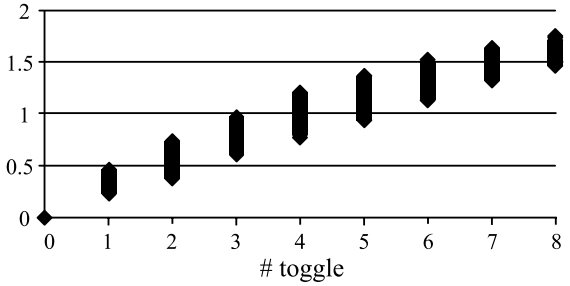

Fig.6 Result of power consumption model with truth table

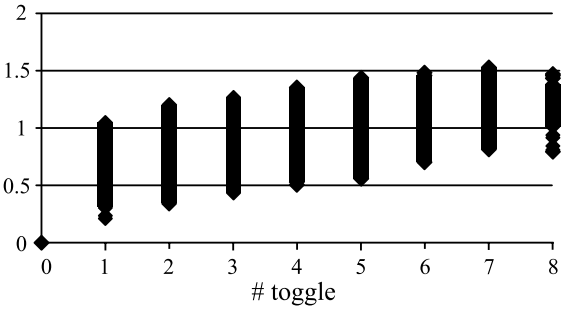

Fig.7 Result of power consumption model with PPRM3

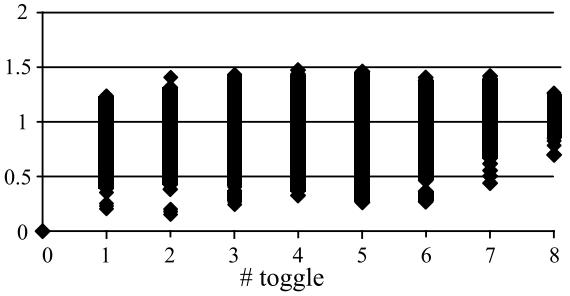

Fig.8 Result of power consumption model with composite field

ISBN: 978-988-19251-2-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Thus, the proposed simulation method could verify tamper resistance using the difference in the configuration method of a device, which could not be verified by the simulation method using hamming weight [2] or hamming distance as the power consumption model.

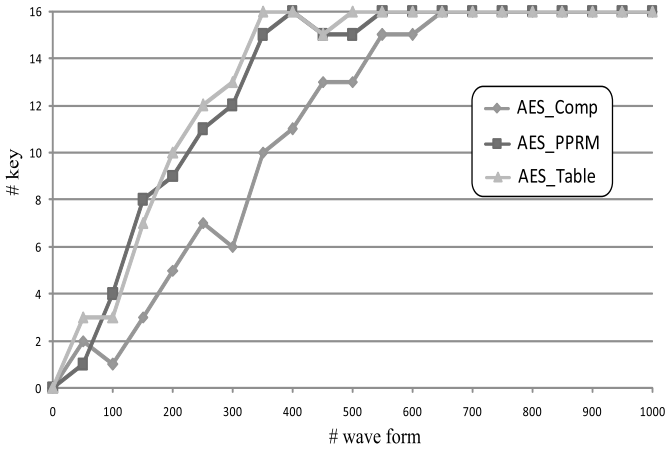

Fig.9 Result of CPA attacks for difference architecture

Table 2 compares the actual measurements of the processing time required for power consumption waveform acquisition with those required for the simulation in this experiment. In Table 2, the processing time required for power consumption information on 10,000 waveforms is shown, and N represents the number of samples in the clock cycle. The processing time required for the waveform acquisition was shorter in the proposed simulation method than in the experiment using an actual device.

TABLE II
PROCESSING TIME

	# N	Proposed Simulation	FPGA borad
Waveform acquisition	1	6 [sec]	80 [min]
	10	7 [sec]	
		35 [min]	36 [min]

V. CONCLUSION

This study proposed a new simulation method by which tamper resistance to an encryption device could be verified at the algorithm level. In the proposed simulation method, a sophisticated power consumption model was only introduced into a circuit block with nonlinearity, which is the target of side-channel attack. The verification environment defined by programming language was used in the other parts. Using this simulation method with mixed-level, high-accuracy and high-speed simulation could be realized. Using the encryption algorithm of AES, three device configuration methods of truth table, PPRM3, and composite field methods were evaluated.

In the future, we will compare the results obtained in this study with those obtained by power analysis attacks such as DPA and CPA by using ASIC. Moreover, we will investigate interconnection delays at algorithm level.

REFERENCES

[1] Paul C.Kocher, Joshua Jaffe, and Benjamin Jun, "Differential Power Analysis", Proc. of CRYPTO '99, pp.388-397 1999
[2] Eric Brier, Christophe Clavier, and Francis Olivier, "Correlation Power Analysis with a Leakage Model", Proc. of CHES 2004, pp.16-29, 2004.
[3] A.Sasaki and K.Abe, "Algorithm Level Evaluation of DPA Resistivity against Cryptosystems", IEEJ Trans. on Electronics, Information and Systems, pp.1221-1228, 2006.
[4] D.Suzuki, M.Saeki, and K.Shimizu, "Evaluation of Side-Channel Resistance for Block Cipher Architecture", Proc. of Symposium on Cryptography and Information Security, SCIS2010, 1A1-1, 1A1-2, 2010.
[5] D.Yamamoto, T.Ochiai, K.Itoh, M.Takenaka, N.Torii, D.Uchida, T.Nagai, and S.Wakana, "Hybrid Correlation Power Analysis", Proc. of Symposium on Cryptography and Information Security, SCIS2010, 3B1-2, 2010.
[6] K.Yamakoshi and A.Yamagishi, "Estimation of CPA attack for AES using Simuation method", IEICE Technical Report, ISEC2009-3, pp.13-20, 2009.
[7] K.Kawamura, K.Iwai, and T.Kurokawa, "Tamper resistance of implementation method od AES against CPA", Proc. Forum on Imformation Technology 2009, vol.4, pp.147-148, 2009.
[8] N.Kamoun, L.Bossuet, A.Ghazel, "Experimental implementation of DPA attacks on AES design with Flash-based FPGA technology", Proc. of Systems, Signals and Devices (SSD'09), pp.23-26, 2009.
[9] J.Huang, Y.Zhou, J.Liu, "Measuring the effectiveness of DPA attacks - from the perspective of distinguishers' statistical characteristics", Proc. of 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), Vol.4, pp.161-168, 2010.
[10] J.F.Jin; E.H.Lu; X.W.Gao, "Resistance DPA of RSA on Smartcard", Proc. of Fifth International Conference on Information Assurance and Security, Vol.2, pp.406-409, 2009.
[11] J.Quan, G.Bai, "A DPA-Resistant Digit-Parallel Modular Multiplier over GF (2m)", Proc. of Sixth International Conference on Information Technology: New Generations (ITNG), pp.53-57, 2009.
[12] Y.Wang, L.M.Douglas, "A robust algorithm for DPA-resistant ECC", Proc. of 12th International Symposium on Integrated Circuits, pp.667-670, 2009.
[13] N.Kamoun, L.Bossuet, A.Ghazel, "Correlated power noise generator as a low cost DPA countermeasures to secure hardware AES cipher", Proc. of 3rd International Conference on Signals, Circuits and Systems (SCS), pp.1-6, 2009
[14] X.Zheng, Y.Zhang, B.Peng, "Design and Implementation of a DPA Resistant AES Coprocessor", Proc. of 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '08), pp.1-4, 2008.
[15] K.J.Lin, S.C.Fang, S.H.Yang, C.C.Lo, "Overcoming Glitches and Dissipation Timing Skews in Design of DPA-Resistant Cryptographic Hardware", Proc. of Design, Automation & Test in Europe Conference & Exhibition (DATE'07), pp.1-6, 2007.
[16] N.Kamoun, L.Bossuet, A.Ghazel, "RAM-FPGA implementation of masked S-Box based DPA countermeasure for AES", Proc. of 3rd International Design and Test Workshop, pp.74-77, 2008.
[17] Y.Wang, J.Leiwo, T.Srikanthan, L.Jianwen, "An Efficient Algorithm for DPA-resistent RSA", Proc. of IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), pp.1659-1662, 2006.
[18] H.Li, K.Wu, B.Peng, Y.Zhang, X.Zheng, F.Yu, "Enhanced Correlation Power Analysis Attack on Smart Card", Proc. of The 9th International Conference for Young Computer Scientists, pp.2143-2148, 2008.
[19] Z.Zhaoxia, Z.Xuecheng, L.Zhenglin, C.Yicheng, "Security Analysis and Optimization of AES S-Boxes Against CPA Attack in Wireless Sensor Network", Proc. of International Conference on Wireless Communications, Networking and Mobile Computing, (WiCOM '07), pp.2608-2612, 2007.
[20] K.Wu, H.Li, B.Peng, F.Yu, "Correlation Power Analysis Attack against Synchronous Stream Ciphers", Proc. of The 9th International Conference for Young Computer Scientists, pp.2067-2072, 2008.
[21] T.H.Le, J.Clediere, C.Serviere, J.L.Lacoume, "Noise Reduction in Side Channel Attack Using Fourth-Order Cumulant", IEEE Transactions on Information Forensics and Security, Vol.2, No.4, pp.710-720, 2007.

ISBN: 978-988-19251-2-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)