The Switching Glitch Power Leakage Model

†Hongying Liu
† Graduate School of Information, Production and Systems, Waseda University, Kitakyushu, 8080135, Japan
Email: liuhongying@fuji.waseda.jp

††Guoyu Qian, †††Yukiyasu Tsunoo, †Satoshi Goto
††Sony LSI Design Inc., Yokohama, 2400005, Japan
†††Information and Media Processing Research Laboratories, NEC Corp., Kawasaki, 2118666, Japan
Email: qian_guoyu@ruri.waseda.jp, tsunoo@bl.jp.nec.com, goto@waseda.jp

***Abstract*—Power analysis attacks are based on analyzing the power consumption of the cryptographic devices while they perform the encryption operation. Correlation Power Analysis (CPA) attacks exploit the linear relation between the known power consumption and the predicted power consumption of cryptographic devices to recover keys. It has been one of the effective side channel attacks that threaten the security of CMOS circuits. However, few works consider the leakage of glitches at the logic gates. In this paper, we present a new power consumption model, namely Switching Glitch (SG) power leakage model, which not only considers the data dependent switching activities but also including glitch power consumptions in CMOS circuits. Additionally, from a theoretical point of view, we show how to estimate the glitch factor. The experiments against AES implementation validate the proposed model. Compared with CPA based on Hamming Distance model, the power traces of recovering keys have been decreased by as much as 28.9%.**

***Index Terms*—side channel attacks, correlation power analysis (CPA), glitches, AES, Hamming Distance.**

I. INTRODUCTION

Side channel attacks are any attacks that reveal the keys of cryptographic devices by exploiting its physical implementation information. Unlike the conventional cryptanalysis, it is not only based on the mathematical analysis but also observing and monitoring the running of encryption algorithms. It has posed a serious threat to the security of cryptographic devices. The power consumption, electromagnetic emission and timing information, as well as the variance of cache content of a cryptographic module might be investigated by adversaries to recover the keys. Power analysis attacks are based on analyzing the power consumption of the module while it performs the encryption operation. This kind of attack was introduced by Kocher [1]. After that, researchers pay much attention to such kind of side channel information. There are basically two sorts of power analysis attacks. Simple Power Analysis (SPA) attacks rely on detailed knowledge of the cryptographic algorithm being implemented and visual inspection of the power consumption curves, to extract cryptographic keys. Differential Power Analysis (DPA) attacks are more powerful based on SPA. It adds statistical techniques to separate signal from noise, and requires less detailed knowledge of the implementation of cryptographic algorithm. In 2004, aimed at improving Hamming Weight leakage model, Brier et al. [2] proposed the correlation power analysis (CPA) attack which uses the correlation factor between Hamming Distance and measured power to guess keys. Then Le et al. [3] enhanced the performance of CPA by restricting the normalization factor in the proposed Partitioning Power Analysis method. The key screening techniques [4] were used to reduce the key estimation time. Furthermore, in 2007, the Switching Distance model was suggested by Peeters et al [5]. They mounted the simulated attacks on an 8-bit PIC16F877 microprocessor against S-box output. All these challenge the implementation algorithms on cryptographic devices, such as Data Encryption Standard (DES) and so on.

Advanced Encryption Standard (AES), also named Rijndael, was published by the National Institute of Standards and Technology (NIST) of United States in 2001 [6]. It has become one of the most popular symmetrical encryption algorithms. AES is designed to be easy to implement on hardware and software, as well as in restricted environments and offer good defenses against various attack techniques. While plenty of research work are carried out on the security examination of AES. Mangard et al [7] implemented SPA against AES key expansions. The simulated measurements and real power measurements are both been used on ASIC implementation of DPA attack [8]. Additionally, abundant work is done on AES implementations with various countermeasures.

Glitch is the unnecessary signal transition due to the unbalanced path delays to the inputs of a logic gate. Glitch power can account for 20% to 70% of the dynamic switching power in CMOS circuits [9]. Raghunathan et al.[10] demonstrate that glitches form a significant component of the switching activity at signals in typical register-transfer level circuits. So it cannot be overlooked in the analysis of side channel information leakage. However, since glitch power dissipation strongly depends on both circuit topology and technology, there are limited publications about its analysis in side channel attacks.

doi:10.4304/jsw.6.9.1787-1794

The SPICE-based simulation of masked gates is shown by Mangard et al. [11]. They also point out that glitches in masked circuits pose the highest threat to masked hardware implementations [12]. And Saeki et al.[13] discussed the glitches in DPA-resistance of masked circuits. Suzuki et al.[14] propose Random Switching Logic (RSL) to suppress the propagation of glitches at the logic level .

In CPA, which is based on the widely used leakage models, such as Hamming Weight and Hamming Distance, glitch effects are not involved. In this paper, we propose a new model, named as Switching Glitch model, for CPA in general cases while taking into account of the glitch power consumption.

The remainder of this paper is organized as follows. Section Ⅱ describes the related background knowledge. Section Ⅲ presents the proposed model. Section Ⅳ shows the measurement setup. Section Ⅴ explains CPA experiments and results in detail. Section Ⅵ draws conclusions.

II. BACKGROUND

In this section, the necessary background about CPA attacks and leakage models are introduced.

A. CPA attacks

The process of conducting a CPA is as follows.

Step 1, selection. One specific intermediate point of the cryptographic device for an encryption algorithm is selected. This point must be a function of the known variable (e.g. the output of S-box) and secret keys K.

Step 2, measuring. The real power consumption of the cryptographic device is measured when it executes encryption algorithm. The digital oscilloscope can be a good candidate to acquire the power transformations. One such sampling data recorded during one round encryption is also called one power trace.

Step 3, assumption. An assumption is made about the power consumption with certain leakage model based on the selected function in Step 1. For example, the Hamming Weight or Hamming Distance is usually used to predict the power consumption of the specific point.

Step 4, computation. The correlation between the power assumption and the measured data is computed. The value which leads to the highest correlation coefficient corresponds to the correct key guess.

B. Leakage models

For an n-bit processor, in Hamming Weight model, it is assumed that the power consumption is proportional to the number of bits that are set in the processed data value, expressed in (1), where x_i is the value of (i+1)th bit of the processing data value X.

$$\mathrm{HW}(X) = \sum_{i=0}^{n-1} x_i \ , \ x_i \in \{0,1\} \qquad (1)$$

Based on the relation between the power consumption of static CMOS circuit and state changing process of the gate circuit, Brier et al. proposed the Hamming Distance model, in (2). X and X' are two consecutive intermediate values of a running algorithm during a target implementation. a denotes the scalar gain between the Hamming Distance and power consumption Y, b denotes the offsets, time dependent components and noise. It assumes that the power consumption Y is proportional to the transitions of the intermediate values not the value been processed.

$$Y = \mathrm{HD}(X, X') = a\ \mathrm{HW}(X \square X') + b \qquad (2)$$

$$Y = a\ E + b \qquad (3)$$

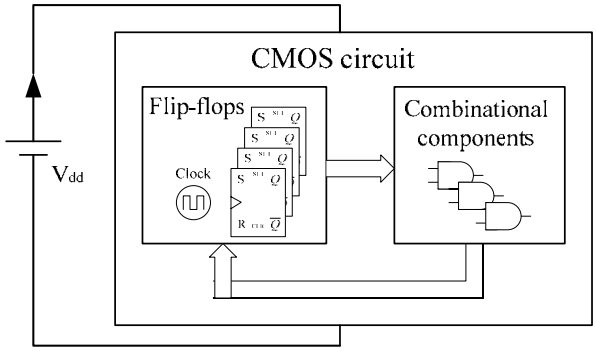


Figure 1. Simplified structure of CMOS circuit.

Our work follows the Hamming Distance model whereas considering a more accurate description to the data dependent power dissipation. Since there is a linear relationship between the power consumption Y of the cryptographic device and the assumed power consumption E, shown by (3), the more accurate the assumed power, the more legible this relation appears. The approach to calculate E will be presented in next section.

III. SG MODEL

The proposed switching glitch model is explained in detail after some preliminaries in this section.

A. Preliminaries

To simplify the problem, the following conditions are satisfied: the cryptographic device is built of CMOS logic gates and edge-triggered flip-flops, and is synchronous. The power supply and ground voltage are fixed on the chip. The simplified structure of a typical CMOS circuit is shown in Fig.1. During the clock ticking, the flip-flops and the combinational components together process the input signals to complete certain functions, such as encryption and so on. So the total power dissipation during this process should include both the flip-flops and combinational components.

The transition probability will be used to aid the analysis of power consumption. Its definition is as follows:

Transition probability [15] for a logic gate or flip-flop X: The average fraction of clock cycles in which the value of X at the end of the cycle is different from its initial value.

The power consumption of a circuit includes two parts: The dynamic power P_{dyn} and the static power P_{stat}. The latter is calculated by (4). V_{dd} is the voltage of the power supply. I_{leak} is the leakage current.

$$P_{stat} = V_{dd} I_{leak} \quad (4)$$

The dynamic power occurs when the logic gates or flip-flops perform output transitions. One type of this power comes from a short-circuit current. When a signal transition occurs at a gate output, both the pull-up and pull-down transistors can be conducting simultaneously for a short period of time. This causes the short-circuit power consumption P_{sc}. The average power of P_{sc} is expressed by (5). $P_{sc}(t)$ is the instantaneous short-circuit power consumed by one flip-flop or logic gate.

$$P_{sc} = \frac{1}{t}\int_0^t P_{sc}(t)dt \quad (5)$$

TABLE I.
POWER CONSUMPTION OF CMOS CIRCUIT

Dynamic	Switching activity	Flip-flop		$0.5V_{dd}^2 fC_x P(x)$
		Combinational components	Normal	$0.5V_{dd}^2 f\sum_{i=1}^{n} C_{xi}P(x_i)$
			glitch	$V_{dd}^2 fC_{av}N_{glch}$
	Short-circuit	$\frac{1}{t}\int_0^t P_{sc}(t)\,dt$		
Static	$V_{dd}\ I_{leak}$			

The other type of dynamic power is consumed by the transition activities of logic gates and flip-flops. For flip-flops, which are the main components of sequential elements of the circuit, the power of one flip-flop can be computed by (6). f denotes the clock frequency. C_x is the total capacitance at one flip-flop output. P(x) is the transition probabilities. In (7), P_{norm} expresses the power consumption of logic gates when they perform normal signal transitions to finish required logic functions. C_{xi} denotes the total capacitance at one gate. $P(x_i)$ is the transition probabilities. n is the total number of logic gates in the circuit. For logic gates, which constitute combinational elements of the circuit, besides the power of P_{norm}, glitch power P_{glch} may occur.

$$P_{flip} = 0.5V_{dd}^2 fC_x P(x) \quad (6)$$

$$P_{norm} = 0.5V_{dd}^2 f\sum_{i=1}^{n} C_{xi}P(x_i) \quad (7)$$

$$P_{glch} = V_{dd}^2 fC_{av}N_{glch} \quad (8)$$

Glitch, or hazard is the temporary states of the output of a combinational components because of the different arrival times of the input signals. Glitch power is a significant portion of the dynamic power consumption. On account of the indeterminate property, a probabilistic modeling is adopted to characterize the glitch power P_{glch}. The power dissipation due to input glitches [10, 11] is shown in (8). C_{av} is the average capacitance at logic gates. N_{glch} expresses the number of generated glitches within a circuit. The total power consumption of a CMOS circuit is summarized in TABLE Ⅰ.

B. The new leakage model

In power analysis, the data dependent and operation dependent power consumption are of the main interest of research. However, in general cases, operation dependent power consumption are more relied on specific cryptographic devices and it is totally black box for attackers, while the short-circuit and static power are negligible [18]. When the logic states change on the arrival of clock cycle, the intermediate value or cipher is stored in flip-flops, and the combinational components perform switching activities. During this period, glitches take place at some logic gates. The dissipated power which is related to data P_{data} is the sum of the power consumed by flip-flops and combinational components, shown as follows.

$$P_{data} = P_{flip} + P_{norm} + P_{glch} \quad (9)$$

For an encryption circuit, it is costly to compute the exact value of each part of P_{data} by the equation in 1. But quantitatively, from the equations in TABLE Ⅰ, we can conclude that the power consumption of flip-flops and combinational components is in a close magnitude. In other words, a number of flip-flops could consume similar power with the normal combinational components except the little difference of load capacitances. So we can simplify this proportional with some factors.

From a high level of perspective, the estimated energy E of encryption, namely SG model, is shown as follows.

$$E = E_{sf} + \beta \quad (10)$$

$$E_{sf} = N_{01} + \alpha N_{10} \quad (10.1)$$

E_{sf} denotes the power of normal switching activities of combinational gates and flip-flops. While glitch factor β describes the glitch power which is circuit and algorithm specific. For different chips and encryption data paths, the glitch factors vary a lot. N_{01} and N_{10} are the number of switches performed by the circuit from 0 to 1 and 1 to 0 respectively. α is switching factor, it characterizes the difference of such transitions. The existence of switching factor is based on the fact that these two kinds of transitions consume different power in normal switching activities. Our ways to estimate glitch factor β are as follows.

$$E_{sf} / \beta = P_{norm} / P_{glch} = 0.5V_{dd}^2 f\sum_{i=1}^{n} C_{xi}P(x_i) \Big/ V_{dd}^2 fC_{av}N_{glch} \quad (11)$$

Suppose that the total capacitance at each gate C_{xi} equals to C_{av}, and then the expression is simplified to (12).

$$E_{sf} / \beta = 0.5\sum_{i=1}^{n} P(x_i) \Big/ N_{glch} \quad (12)$$

For an encryption circuit, the value of $P(x_i)$ depends on the input data. Furthermore, if we know the relation between the number of generated glitches N_{glch} and the logic gates n, then β can be expressed by some expression of E_{sf}. In fact, because of the complexity of the design technologies and detailed processing techniques of CMOS circuits, it seems that this relation is unpredictable without CAD simulation tool. We will make a further reckon and verify it through experiments.

IV. MEASUREMENT SETUP

In this section, we describe the process of conducting CPA. As an example, our CPA is against AES implementations on SASEBO [19], which is provided by AIST and Tohoku University [20].

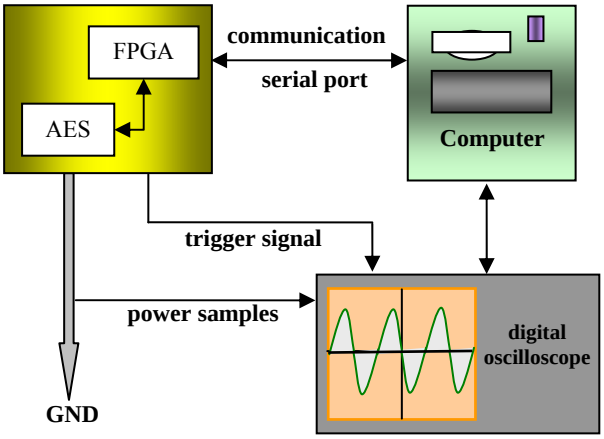


Figure 2. Experiment environment.

Firstly, we select one specific point for the attack. According to the architecture of the AES on ASIC, we choose the output of the final round of encryption function AddRoundKey as a target.

Figure 3. Power signals.

Secondly, the encryption process is measured. The experimental environment is shown in Fig.2.The computer randomly generates 128-bit plaintext in 10k groups, which are transmitted to the FPGA through RS-232 serial ports, and then upon receipt of the plaintext, the FPGA control the ASIC to implement AES encryption program. At the same time, the execution signal on ASIC triggers the digital oscilloscope to start sampling, and thus the oscilloscope obtains power signals through its probe, shown in Fig.3. The sampled data is transmitted to computer through LAN. After the encryption is finished, the cipher text is transmitted to computer. So we obtain 10k groups of plaintext, corresponding cipher text as well as 10k power traces Y. The power curves of 1, 50,1k and 10k for the final round are shown in Fig.4 respectively, where "PT" represents "Power Trace". They are almost overlapped.

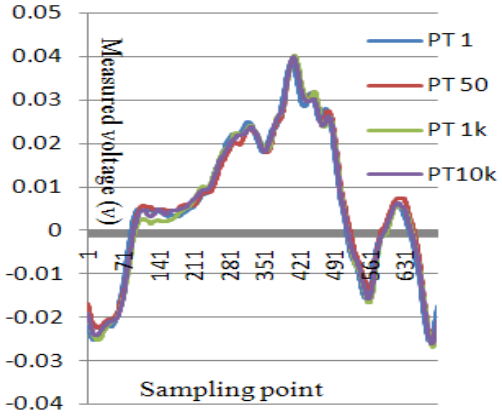


Figure 4. Sampling power curves.

Then we make estimation about the power consumption of the final round encryption. The cipher texts C are picked up to compute with guessed keys K by inverse-shift rows, inverse-sub bytes, C' are induced. Thus N_{01}' and N_{10}' can be calculated respectively. With our proposed model, we predict that the power consumption of final round encryption is $E_{est}= (N_{01}'+\alpha N_{10}')+\beta$. If α and β are determined, we could conduct this CPA continually to the last step.

$$\rho\,(\mathrm{Y}, \mathrm{E_{est}}) = \frac{Cov(Y, E_{est})}{\sqrt{Var(Y)}\sqrt{Var(E_{est})}} \qquad (13)$$

$$Cov\,(\mathrm{Y}, \mathrm{E_{est}}) = \frac{1}{n}\sum_{i=1}^{n}[Y_i - \overline{Y}][E_{est\,j} - \overline{E_{est}}] \qquad (14)$$

Finally, the correlation coefficient of the real power consumption Y and the predicted power consumption E_{est} is calculated according to (13) and (14). Since the predicted power consumption contains key guesses, when the correct key guess appears, the correlation coefficient is supposed to be largest.

ρ is the correlation coefficient between the power traces and estimated power consumption, Var is the mathematical Variance of Y and E_{est} respectively. $\overline{Y}$ and $\overline{E_{est}}$ are the average values of Y and E_{est} respectively. n denotes the nth point in power traces, 1=<i<=n , j denotes the j_{th} guess of keys.

V. EXPERIMENTS

In this section, we will further explain the SG model through experiments.

A. CPA without glitches

Notably, we focus on E_{sf} part of SG model, shown in (10.1). The aim of this analysis without considering the power consumption of glitches is to determine the switching factor α (in short, SF). With the acquired power trace curves, which is from the execution of AES with composite field S-box (In TABLE Ⅲ , AES1), we conducted CPA on a PC.

TABLE II.
NUMBER OF POWER TRACES TO RECOVER ALL THE KEY BYTES AT DIFFERENT SF

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Sacu
SF3.5	42	62	34	16	29	74	30	37	46	36	39	48	100	22	63	63	-132
SF3.0	42	61	34	16	29	74	30	35	41	35	28	49	90	21	51	50	-75
SF2.5	42	57	16	16	29	74	31	32	38	34	29	48	90	21	51	54	-53
SF2.0	42	54	34	11	31	55	32	35	37	33	22	48	41	21	50	50	13
SF1.8	42	52	17	11	31	55	32	35	38	34	22	48	41	22	50	50	29
SF1.7	43	51	15	11	29	58	36	35	33	34	21	51	40	21	50	48	35
SF1.6	35	51	16	15	31	56	40	24	32	32	28	48	41	21	50	47	42
SF1.5	35	51	16	15	31	56	40	24	28	32	28	47	38	20	50	47	51
SF1.3	35	54	16	15	28	75	55	31	31	29	38	58	38	15	49	28	14
SF1.1	35	65	16	15	46	76	55	21	26	35	23	64	37	15	49	28	3
SF0.9	38	70	15	20	46	93	67	21	38	39	31	66	40	25	50	28	-72
SF0.8	35	70	15	20	46	93	67	21	28	41	34	66	43	23	50	26	-66
HD	35	65	16	15	46	76	55	24	26	35	23	64	37	15	49	28	0

When the value of α is set to range from 0.8 to 3.5, the number of power traces used to recover all the 16- byte (128-bit) keys of AES is shown in TABLE Ⅱ. Some identical lines are omitted. For example, when SF is 1.4, the number of power traces is the same as SF1.3. Note that, all the numbers are in unit 100. For instance, when switching factor is 3.5, the first bytes of AES keys can be recovered at 4200 power traces.

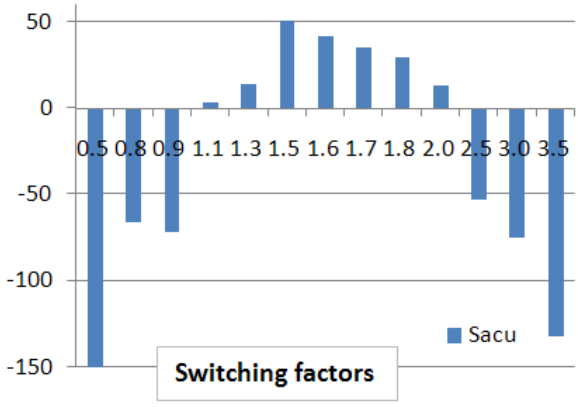


Figure 5. S_{acu} of different switching factors.

In order to find the optimal switching factor, the results of different SF-based analysis are compared with Hamming Distance (HD) model. At the last line of TABLE Ⅱ, the results of CPA using the same power curves with HD model are listed. To quantitatively explore which SF is better, we define "accumulation factor" S_{acu}, shown by (15). For switching factor N, the accumulative numbers of power traces of all the 16 bytes is the sum of the differences of each byte. It expresses the improved accumulative number of power traces compared with HD.

$$S_{acu}(N) = \sum_{i=1}^{16}(X_{HDi} - X_{Sfi}) \quad (15)$$

When S_{acu} is positive, that means the number of power traces is decreased. While the negative S_{acu} stands for an increase of power traces. For HD itself, this value is 0. So the larger this value is, the better the performance is improved. The last column of TABLE Ⅱ shows the S_{acu} of each SF. Fig.5 gives a more clear vision of S_{acu} at different SF. We can see that the S_{acu} is the largest when SF is 1.5. Therefore, for AES encryption on ASIC, when switching factor is set to 1.5, the 16-byte keys can be recovered with least power traces.

B. CPA with glitches

The purpose of the following experiments is to estimate the glitch factor β in SG model, thus further improve CPA performances. From (15), β can be expressed by (16).

$$\beta = E_{sf}\, N_{glch} / \; 0.5\sum_{i=1}^{n} P(x_i) \quad (16)$$

In our experiment, since the plaintext is randomized, the transition probability of the logic gates can be estimated with value 0.5. Then (17) is derived.

$$\beta = E_{sf}\; N_{glch} \; / 0.25 \; N_{gats} \quad (17)$$

N_{gats} denotes the number of logic gates in encryption circuit. For one byte input data, with switching factor α 1.5, E_{sf} is in 10 magnitude. Suppose that the average

generation rate of glitches at the logic gates is 0.1, and then β can be calculated from (17) at 1.0 magnitude.

However, in our experiment, different values of this glitch factor are attempted. We find that 1.0E-1 is the optimal value rather than the theoretical value 1.0. That is to say, when β is set at 1.0E-1, the number of power traces becomes least.

TABLE III.
AES CRYPTOGRAPHIC CIRCUITS ON ASIC

Name	Implementation	Gate No.	Area (μm^2)
AES1	Composite field S-box with encryption only	12059	61408
AES2	S-box with Look Up Table	20639	105097
AES3	Positive Prime Reed Muler (PPRM)based S-box using 1-stage AND-XOR logic.	61801	314702
AES4	PPRM-based S-box using 3-stage AND-XOR logic.	16541	84230

Since the value of switching factor α and glitch factor β are both computed, the CPA experiments with glitches are continued. We tested CPA against different AES hardware structures based on HD model and SG model on the same chip, which is named IC_a. The cryptographic core uses 0.13μm TSMC standard library of CMOS process technology. The detailed information of each AES is shown in TABLE Ⅲ. Throughout the experiments, the initial encryption 16-byte keys are set as hexadecimal numbers: 12 34 56 78 90 AB CD EF 12 34 56 78 90 AB CD EF. The final round encryption keys are: C3 BE 32 F4 60 A9 B3 4E F7 43 61 57 F2 B9 19 D8.

TABLE IV.
COMPARISON OF CPA ON IC_A

Name	Glitch Factor	HD (K)	SG Without Glitch (K)	Reduction Rate (%)	SG With Glitch (K)	Reduction Rate (%)
AES1	0.1	7.6	5.6	26.3	5.4	28.9
AES2	0.09	3.5	3.1	11.4	2.9	17.1
AES3	0.09	3.2	2.9	9.3	2.8	12.5
AES4	0.2	4.9	4.0	18.4	3.8	22.4

TABLE V.
COMPARISON OF CPA ON IC_B

Name	Glitch Factor	HD (K)	SG Without Glitch (K)	Reduction Rate (%)	SG With Glitch (K)	Reduction Rate (%)
AES1	0.1	6.1	5.1	16.4	4.6	24.5
AES2	0.09	3.0	2.7	10.0	2.6	14.4
AES3	0.09	2.3	2.1	8.7	2.0	13.0
AES4	0.2	3.4	2.9	14.7	2.7	20.6

In TABLE Ⅳ, we list the glitch factor and the least number of power traces used to recover 16-byte keys by HD model and SG model respectively as well as the power trace reduction rate, where K denotes 1000. For example, the first line of TABLEⅣ means: For AES1 implementation on IC_a, the HD-based CPA uses 7.6k power traces to recover16-byte keys. The SG-based CPA without glitches can recover these keys at 5.6k power traces. And the power traces have been reduced by 26.3% compared with HD-based CPA. While the SG model with glitches can recover these keys with 5.4k power traces. And the power traces have been reduced by 28.9%. For different AES implementations, the glitch factors vary. But they are almost in the same magnitude about 1.0E-1. Notably, the reduction rates of power trace also differ a lot.

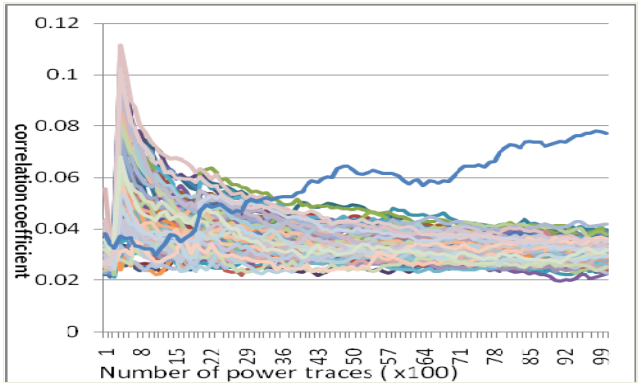


Figure 6. The correlation coefficient of recovering the 13th key.

The correlation coefficient ρ of recovering all the key bytes are calculated from (13). In Fig.6, the computation process of 13th byte key "F2" is exemplified. The largest correlation coefficient peaks at the guess value of F2. In Fig.7, the correct key appears clearly from 10k power traces.

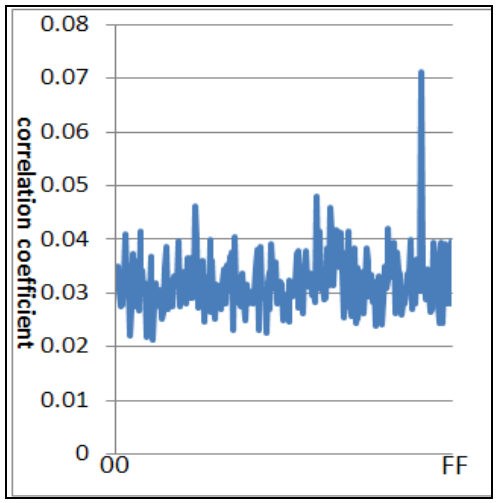


Figure 7. The appearing of correlation coefficient for correct key.

The successful rates [21] of HD-based and SG-based CPA against AES1 are illustrated in Fig.8. Successful rates express the number of power traces when all the keys can be recovered. With HD model, 100% appears at 7.6k power traces, which is circled in the Fig. But with the proposed SG model, 100% appears at 5.4k power traces, which means the power traces of recovering keys have been decreased by 28.9%.

To verify the SG model, the same experiments are repeated on another chip, namely IC_b, which is produced with the same technology. The results are listed in TABLE Ⅴ. The same glitch factor is used for each AES implementation. Surprisingly, the SG with glitches can further cut the number of power traces from 5.1k to 4.6k, which means the glitch power leakage leads to a reduction rate of 8.1%, namely (24.5-16.4) %. That is much than expected. The greatest reduction rate of power trace is 24.5%, which occurs at CPA against AES1. The successful rates are also compared with HD-based CPA in Fig.9.With HD model, 100% appears at 6.1k power traces, which is circled in the Fig. But with SG model, 100% appears at 4.6k power traces. The power traces of recovering keys have been reduced by 24.5%.

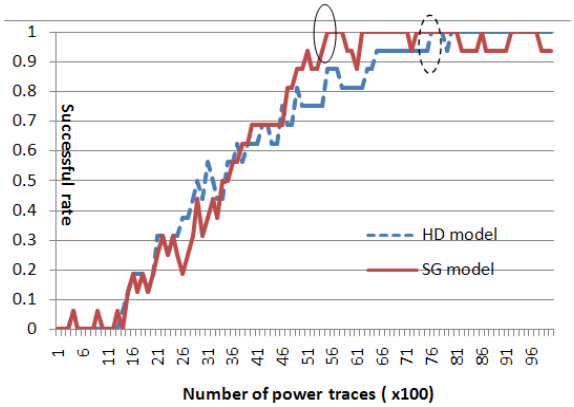


Figure 8. The successful rates of CPA against AES1on IC_a.

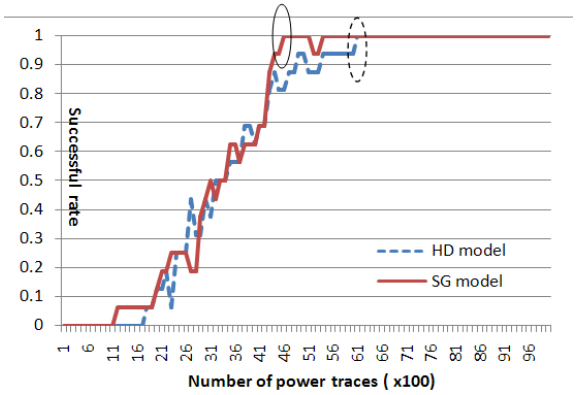


Figure 9. The successful rates of CPA against AES1on IC_b.

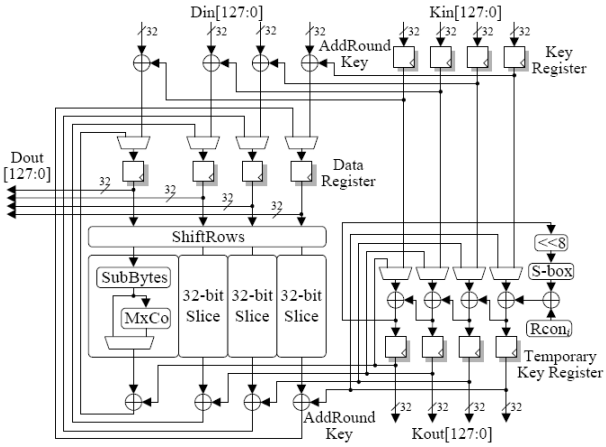
From results of TABLE Ⅳ and TABLE Ⅴ, the glitch effects contribute a lot to CPA. The power traces are reduced because that a more accurate model which including the power consumption of glitches is built.

Ⅵ. Conclusions

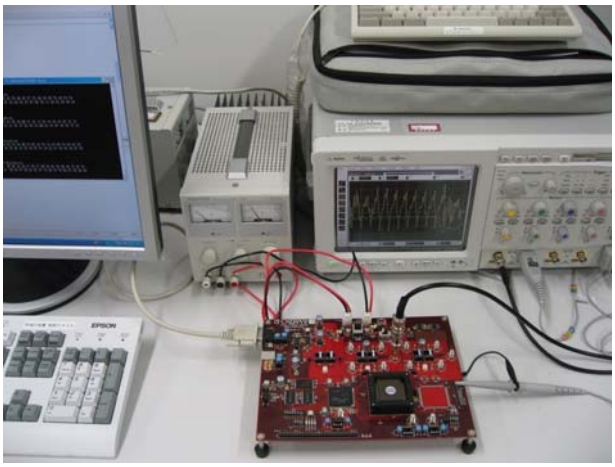
In this paper, a new power consumption model, namely Switching Glitch model, is proposed, which characterizes the power consumption of cryptographic devices more accurately. The distinguishing of two different dynamic switching activities and the power consumption of glitches are both included. Compared with CPA based on Hamming Distance model, it can reduce the number of power traces by as much as 28.9%. However the switching factor and glitch factor are experimentally represented from AES implementation on ASIC after theoretical derivations. Theoretically, these two factors can be applied to other CPA not confined to against AES and ASIC chip.

Appendix

A. AES hardware implementation on ASIC



B. CPA experiment environment



Acknowledgment

This work was supported by “Global COE program” of MEXT and CREST of JST in Japan.

References

[1] P. Kocher, J. Jaffe and B. Jun, “Differential Power Analysis”, proceedings of CRYPTO ’99, LNCS 1666, Springer, pp. 388-397, 1999.

[2] E. Brier, C. Clavier, and F. Olivier, “Correlation Power Analysis with a Leakage Model”, proceedings of CHES 2004, LNCS 3156, pp. 16-29, 2004,.

[3] T. Le, J. Clédière, C. Canovas, et al, “A proposition for correlation power analysis enhancement”, LNCS 4249, pp.174, 2006.

[4] T. Katashita, A. Satoh, T. Sugawara, et al, “Enhanced Correlation Power Analysis Using Key Screening Technique”, proceedings of Reconfigurable Computing and FPGAs (ReConFig '08), pp. 403-408, Dec. 3-5, 2008.

[5] E. Peeters, F. X. Standaert, and J.J.Quisquater, "Power and electromagnetic analysis: Improved model, consequences and comparisons", Integration, the VLSI Journal, Elsevier, vol.40, issue 1, pp.52-60, 2007.
[6] National Institute of Standards and Technology (NIST) of U.S. Department of Commerce, "FIPS 197: Advanced Encryption Standard", Nov.2001.
[7] S. Mangard, "A simple power analysis attack on implementation of the AES expansion", proc. of Information Security and Cryptology (ICISC) 2002, LNCS 2587, pp.343-358, 2002.
[8] S.B.Ors, F. Gurkaynak, E. Oswald, et al, "Power-Analysis Attack on an ASIC AES implementation", proceedings of ITCC 2004, Las Vegas, April 5-7, 2004.
[9] Y. Lu, and V.D. Agrawal, "CMOS Leakage and Glitch Minimization for Power-Performance Tradeoff", Journal of Low Power Electronics, vol.2 (no.3), pp.1-10, 2006.
[10] A.Raghunathan, S.Dey, and N.K. Jha, "High-level macro-modeling and estimation techniques for switching activity and power consumption", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol.11, NO.4, pp.538-557, 2003.
[11] S.Mangard, T.Popp, and B. M. Gammel, "Side-channel Leakage of Masked CMOS Gates", LNCS 3376, Springer, pp.351-365, 2005.
[12] S.Mangard and K.Schramm, "Pinpointing the side-channel leakage of masked AES hardware implementations", LNCS 4249, pp.76-90, 2006.
[13] M.Saeki, D.Suzuki, and T.Ichikawa, "Leakage analysis of DPA Countermeasures at the Logic Level", IEICE transactions on fundamentals of electronics, communications and computer sciences, Vol.E90-A, No.1, pp.169-178, 2007.
[14] D.Suzuki, M.Saeki, and T.Ichikawa," Random Switching Logic: A New Countermeasure against DPA and Second-Order DPA at the Logic Level", IEICE transactions on fundamentals of electronics, communications and computer sciences,Vol.E90-A No.1, pp.160-168,2007.
[15] F.N.Najm, "Power estimation techniques for integrated circuits", proceedings of the International Conference on Computer-Aided Design; California, United States, pp.492-499, 1995.
[16] X. Liu and M.C. Papaefthymiou,"A statistical model of input glitch propagation and its application in power macromodeling", journal of Power,Volume:10, pp.10.
[17] X. Liu and M. C. Papaefthymiou, "Incorporation of input glitches into power macromodeling", Proceedings of IEEE International Symposium on Circuits and Systems, May 2002.
[18] S.Chari, C.S. Jutla, and J. R. Rao et al,"Towards sound approaches to counteract power analysis attacks", LNCS 1666, pp. 398-412,1999.
[19] Research Center for Information Security (RCIS) of AIST,"Side-channel Attack Standard Evaluation Board(SASEBO)".http://www.rcis.aist.go.jp/special/SASEBO/index-en.html
[20] Computer Structures Laboratory of Tohoku University, "Cryptographic Hardware Project". http://www.aoki.ecei.tohoku.ac.jp/crypto
[21] G.Qian, Y.Zhou, Y.Xing, et al, "A Weighted Statistical Analysis of DPA Attack on an ASIC AES Implementation", proceedings of IEEE 8th International Conference on ASIC (ASICON 2009), Changsha, China, October 20-23, 2009.

Hongying Liu was born in ShaanXi, China, in 1983. She received the B.S. and M.S. degrees in Computer Science and Technology from Xi'An University of Technology, China, in 2002 and 2006, respectively. She participated in several major projects when pursued her M.S degree, such as National High Technology Research and Development Program of China ("863" Program) etc. Currently, she is a Ph.D candidate in Graduate school of Information, Production and Systems, Waseda University. Her major research interests include information security, RFID systems, etc.

Guoyu Qian received the B.E. degree in computer science from Beijing Institute of Technology, China in 2007 and M.S. degree in electronics engineering from Graduate School of Information, Production and Systems, Waseda University, Japan in 2009. His research interests include information security, cryptanalysis and LSI design.

Yukiyasu Tsunoo received his B.E. degree from Waseda University in 1982, M.S. degree from JAIST, and Dr.Eng. from Chuo University. He joined NEC Software Hokuriku, Ltd. in 1985. He is now a Research Fellow of NEC Information and Media Processing Research Laboratories. He is engaged in the design of common key ciphers and the study of evaluation techniques. Dr. Tsunoo is a member of the Expert Commission of Information Security Research, The Institute of Electronics, Information and Communication Engineers, the Information Processing Society of Japan, the Japan Society for Security Management and the Atomic Energy Society of Japan.

Satoshi Goto was born in 1945, in Hiroshima, Japan. He received the B.E. and M.E. degree in Electronics and Communication Engineering from Waseda University in 1968 and 1970, respectively. He also received the Dr. of Engineering from the same university in 1981. He is IEEE fellow, member of Academy Engineering Society of Japan and professor of Waseda University. His research interests include LSI system and Multimedia System.