Power Analysis Attack and Its Countermeasure for a Lightweight Block Cipher Simon

Masaya Yoshikawa and Yusuke Nozaki

Abstract This study proposes a power analysis attack and a countermeasure for a lightweight cipher Simon. Simon can be embedded in the smallest area among lightweight block ciphers. In the proposed power analysis method, an analysis based on conventional power analysis attacks is applied to Simon. In the proposed countermeasure, random masks are applied to data resisters. Experiments revealed the vulnerability of the normal implementation method and verified the validity of the proposed countermeasure.

Keywords Power analysis attack · Countermeasure · Lightweight block cipher · Simon

1 Introduction

In built-in apparatuses, the scale of a circuit is limited. Therefore, the development of a lightweight block cipher that can be embedded in a small-scale circuit has been highly anticipated. Simon [1] is a lightweight block cipher disclosed by the United States National Security Agency (NSA) [2], and in comparison to other typical lightweight ciphers [3,4,5], it can be embedded in a very small area [1].

The threat of side-channel attacks against circuits, in which a cipher whose safety is computationally secured has been embedded, is pointed out [6,7,8,9]. Side-channel attacks illegally obtain confidential information using physical information, such as power consumption and electromagnetic waves generated during encryption processing. In particular, since power analysis attacks [6], [7] using power consumption can easily analyze confidential information, they are considered to be the most dangerous types of attacks.

At present, many studies have reported on power analysis attacks against the advanced encryption standard (AES) [10], but few studies have reported on these attacks against lightweight ciphers. In particular, as far as we know, studies presenting measures to prevent power analysis attacks against Simon have not been published yet. The present study proposes a power analysis method against Simon,

M. Yoshikawa(✉) · Y. Nozaki
Department of Information Engineering, Meijo University, Nagoya, Japan
e-mail: dpa_cpa@yahoo.co.jp

S. Latifi (ed.), *Information Technology New Generations*,
Advances in Intelligent Systems and Computing 448,
DOI: 10.1007/978-3-319-32467-8_15

a lightweight block cipher, and it also proposes a countermeasure to prevent power analysis attacks. In the proposed power analysis method, an analysis based on conventional power analysis attacks is applied to Simon. In the proposed countermeasure, random masks are applied to data resisters. The present study also verifies the validity of the proposed power analysis method by performing an evaluation experiment using a field-programmable gate array (FPGA).

2 Preliminaries

2.1 Simon

Simon is a lightweight block cipher that has a Feistel structure. Its block length can be 32, 48, 64, 96, or 128 bits, and its key length can be 64, 72, 96, 128, 148, 196, or 256 bits. The number of rounds changes depending on the selected block length and key length.

When the intermediate value at the *r*th round is expressed as x^r, its left half is processed as x_L^r and its right half is processed as x_R^r, separately. By repeating the left rotation processing, the AND operation, and the XOR operation in a bit unit, encryption is performed. The intermediate value can be calculated using formula (1).

$$\begin{cases} x_L^{r+1} = \left(S^1\left(x_L^r\right) \& S^8\left(x_L^r\right)\right) \oplus x_R^r \oplus S^2\left(x_L^r\right) \oplus RK^r \\ x_R^{r+1} = x_L^r \end{cases} \tag{1}$$

In formula (1), S^1, S^8, and S^2 express the left rotation processing at 1, 8, and 2 bits, respectively; & expresses the AND operation; $\oplus$ expresses the XOR operation; and *RK* expresses a partial key generated form the key-scheduling section.

2.2 Power Analysis

Power analysis is a method that obtains confidential information using the power consumption that is generated during the operation of a cryptographic circuit. Differential power analysis (DPA) is a typical type of power analysis attack.

DPA consists of a hamming weight (HW)-type DPA and a hamming distance (HD)-type DPA. HW-type DPA uses the difference in power consumption that is generated due to the difference in the transition probability when certain input and output values (hamming weight) are noticed in the nonlinear element inside a cryptographic circuit. HD-type DPA assumes that a linear relationship exists between the intra-data resister hamming distance of data and the power consumption, and it uses this linear relationship.

In HW-type DPA, power consumption waveforms are divided into two groups based on whether the hamming weight with certain input and output values is 0 or 1. In HD-type DPA, power consumption waveforms are divided into two groups based on whether the hamming distance between the data resisters is larger or smaller than a predetermined value.

The hamming weight and the hamming distance are obtained using an already known cryptogram, and they are calculated using the predicted value of a partial key that is used during encryption processing. Subsequently, the difference in the average of each group is obtained. The predicted value of a key with the largest differential power value is estimated to be the correct key.

3 Proposed Method

3.1 Analytical Method Using Correction Processing

In the first step of this proposed approach, a basic power analysis method is explained in which HW-type DPA is applied to Simon. As shown in Fig. 1, the hamming weight of input value *A* of the AND operation is actually used.

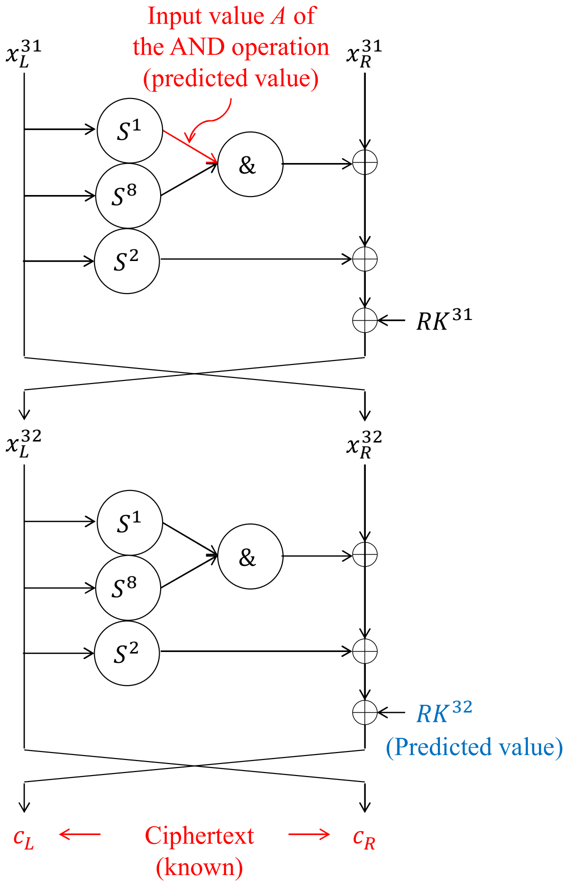


Fig. 1 Attack point

The input value A of the AND operation can be calculated using formula (2).

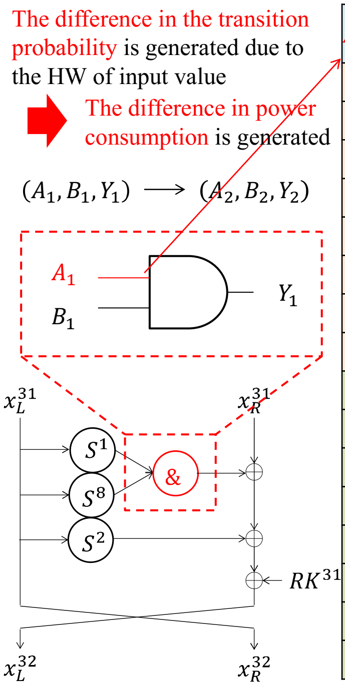
$$A = S^1\left(x_R^{32}\right) \tag{2}$$

In formula (2), x_R^{32} can be calculated as the already-known cryptogram c_R and the predicted value RK^{32} of a partial key. This calculation is expressed as formula (3).

$$x_R^{32} = \left(S^1(c_R)\,\&\,S^8(c_R)\right) \oplus c_L \oplus S^2(c_R) \oplus RK^{32} \tag{3}$$

The difference in the transition probability generated in the AND operation of Simon is explained in Fig. 2, which shows the true table of input and output values when a two-input AND gate is used. When the input value of certain time 1 (A_1) is 0, the transition probability of output Y is 1/4. When input value A_1 is 1, the transition probability of output Y is 1/2. Therefore, the difference in the transition probability is generated due to the hamming weight of input value A_1.

In the analysis, power consumption waveforms are divided into two groups based on whether the hamming weight of input value A is 0 or 1. The difference in the average of the power consumption waveforms in each group is obtained, the differential power value is calculated, and the predicted value of a key with the largest differential power value is estimated to be the correct key.


The difference in the transition probability is generated due to the HW of input value

The difference in power consumption is generated

A_1	B_1	A_2	B_2	Y_1	Y_2	Transition	probability
0	0	0	0	0	0	×	1/4
0	0	0	1	0	0	×	
0	0	1	0	0	0	×	
0	0	1	1	0	1	✓	
0	1	0	0	0	0	×	
0	1	0	1	0	0	×	
0	1	1	0	0	0	×	
0	1	1	1	0	1	✓	difference
1	0	0	0	0	0	×	1/2
1	0	0	1	0	0	×	
1	0	1	0	0	0	×	
1	0	1	1	0	1	✓	
1	1	0	0	1	0	✓	
1	1	0	1	1	0	✓	
1	1	1	0	1	0	✓	
1	1	1	1	1	1	×	

Fig. 2 Example of the transition probability generated in the AND operation of Simon

Next, a method to apply HD-type DPA is explained. In the proposed power analysis method, the hamming distance of the right half of the intermediate value is used. As shown in Fig. 3, when the final round is targeted, the hamming distance between cryptogram c_R and intermediate value x_R^{32} is used, which is calculated using the cryptogram, the predicted value of a partial key, and formula (3).

In the proposed power analysis method, the hamming distance is used one bit by one bit, and a partial key is predicted one bit by one bit. Therefore, to estimate a 16-bit partial key, the computational complexity becomes 2^1 x 16 = 32 ways. To analyze a 64-bit partial key, the computational complexity becomes 32 x 4 = 128 ways.

Finally, correction processing is explained. As shown in Fig. 4, the voltage value is slightly shifted in the amplitude direction due to measurement errors in the power consumption waveforms that are obtained using an oscilloscope. Because a lightweight cipher consumes little power, measurement errors have a significant effect on it. Therefore, before applying the proposed power analysis method, the obtained power consumption waveforms are processed so that the effect of the measurement errors can be minimized.

In this correction processing, the average of the voltage values in a region where no voltage variation occur, as shown in Fig. 4, is obtained in each power consumption waveform. Subsequently, all of the sample points of each power consumption waveform are shifted so that the obtained average in each power consumption waveform is the same. This is the correction processing.

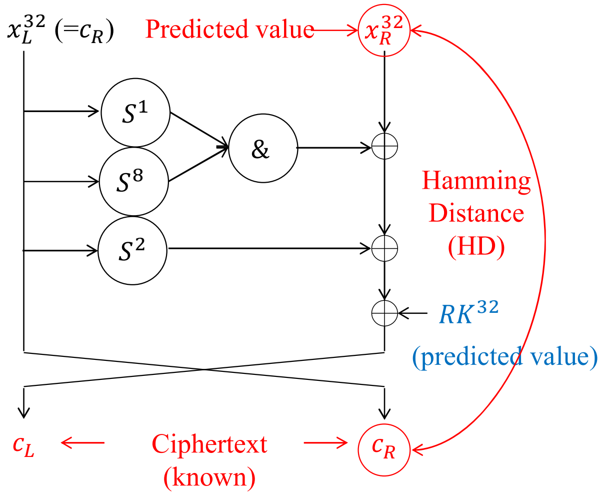


Fig. 3 Example of the hamming distance between cryptogram c_R and intermediate value x_R^{32}

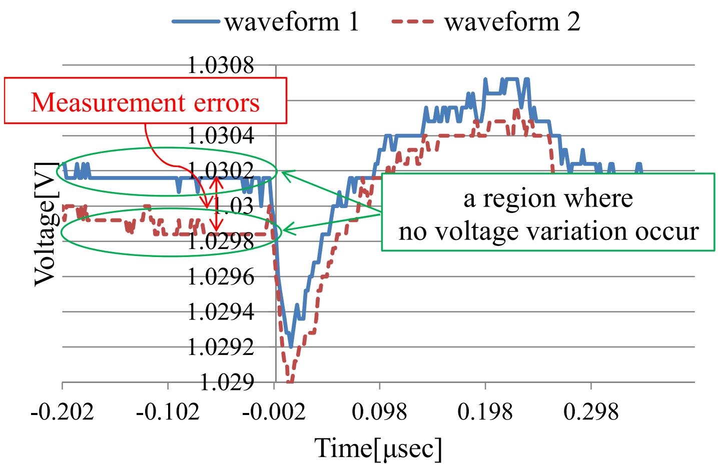


Fig. 4 Example of measurement errors

3.2 Method to Prevent Power Analysis Attacks using Random Masks

In power analysis attacks, the linear correlation between the hamming distance and power consumption is used. The hamming distance is the data transition between data resisters. The proposed method to prevent power analysis attacks pays attention to this linear correlation and ensures tamper resistance by eliminating this linear correlation.

As shown in Fig. 5, mask processing (i.e., the XOR operation) is actually performed for the data resisters used for side-channel attacks. By performing mask processing using random numbers, the values stored in the data resisters differ from the normal intermediate values. Thus, the linear correlation between the hamming distance and power consumption can be eliminated. For the values called out from the data resisters, unmask processing is performed using the same random numbers.

Thus, mask processing is performed immediately before data are stored in the data resisters, and unmask processing is performed immediately after data are read out from the data resisters. Consequently, the correlation between the intra-data register hamming distance and power consumption can be eliminated and correct encryption results can be obtained.

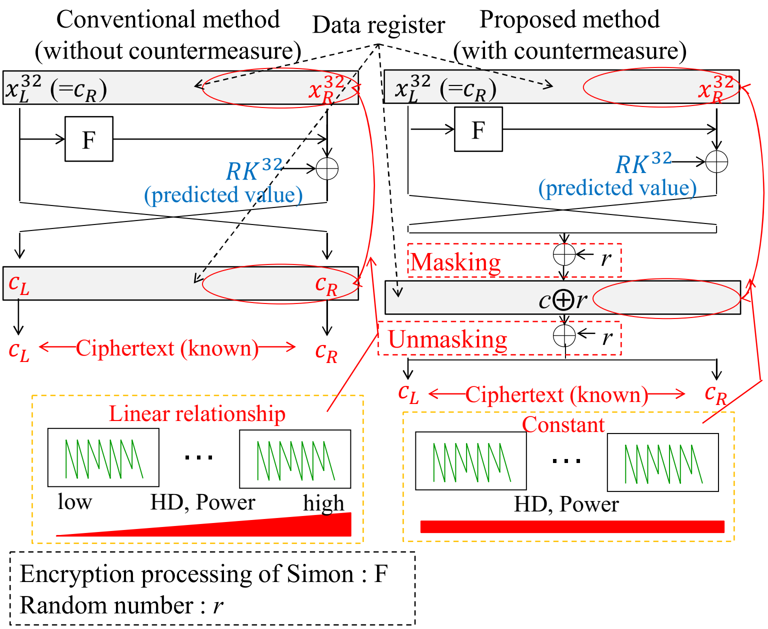


Fig. 5 Mask processing

4 Evaluation Experiments

In the evaluation experiment, Simon with a 32-bit block length and a 64-key length was embedded in an FPGA. Table 1 and Fig. 6 show the experimental environment. Under this experimental environment, encryption processing of Simon was performed 50,000 times, and 50,000 cryptograms and power consumption waveforms were obtained. In the evaluation experiment, a 16-bit partial key RK^{32} at the final round (1-bit partial keys are expressed as RK_1^{32}, RK_2^{32}, and RK_{16}^{32}) was analyzed.

Table 1 Experimental conditions

Encryption algorithm	Simon
Block size [bit]	32
Key size [bit]	64
Evaluation board	SASEBO-GII
FPGA	Virtex-5 XC5VLX30
Implementation tool	Xilinx ISE Design Suite 14.1
Oscilloscope	Agilent DSO1024A
Sampling rate [Gsa/sec]	2
Power supply	USB power supply from PC

Table 2 shows the analytical results obtained using 50,000 waveforms by applying HW-type DPA to Simon. As shown, not all of the partial keys could be analyzed. However, of the 16-bit partial keys, 12-bit partial keys could be analyzed. Therefore, HW-type DPA is effective for Simon. It is considered that when the number of waveforms used for the analysis is increased, the remaining partial key can be analyzed.

Next, the conventional method in Fig. 7 shows the analytical results obtained using 20,000 waveforms by applying HD-type DPA to Simon. The horizontal axis represents the number of waveforms used and the vertical axis represents the number of correct keys, which is expressed by the number of bits of each successfully analyzed partial key. In this experiment, since partial key RK^{32} at the final round was analyzed, the number of the correct keys is 16 [bits], at the maximum. As shown, all of the partial keys could be analyzed using 6,000 waveforms. Therefore, the proposed power analysis method was demonstrated to be effective.

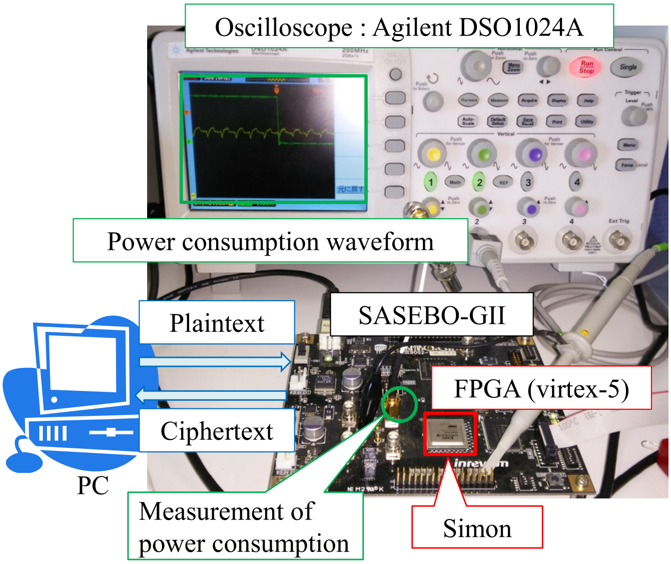

Oscilloscope : Agilent DSO1024A
Power consumption waveform
Plaintext
SASEBO-GII
FPGA (virtex-5)
Ciphertext
PC
Measurement of power consumption
Simon

Fig. 6 Experimental environment

Table 2 Analytical results (50,000 waveforms by applying HW-type DPA)

	Success	Failure
Key	RK_1^{32} , RK_3^{32} , RK_4^{32} , RK_5^{32} RK_5^{32} , RK_6^{32} , RK_7^{32} , RK_{10}^{32} , RK_{11}^{32} , RK_{12}^{32} , RK_{13}^{32} , RK_{14}^{32} , RK_{16}^{32}	RK_2^{32} , RK_8^{32} , RK_9^{32} , RK_{15}^{32}

Finally, power analysis attacks were performed against Simon. In one of the experiments, the proposed method to prevent those attacks was embedded in Simon, and in the other experiment, no countermeasures were taken. When the proposed method to prevent power analysis attacks was embedded, only eight partial keys were successfully analyzed, although 20,000 waveforms were used. Because all of the partial keys consisted of 16 bits, these results are the same as the results obtained by predicting the value one bit by one bit, randomly. Therefore, the proposed method to prevent power analysis attacks is considered to be resistant to power analysis attacks.

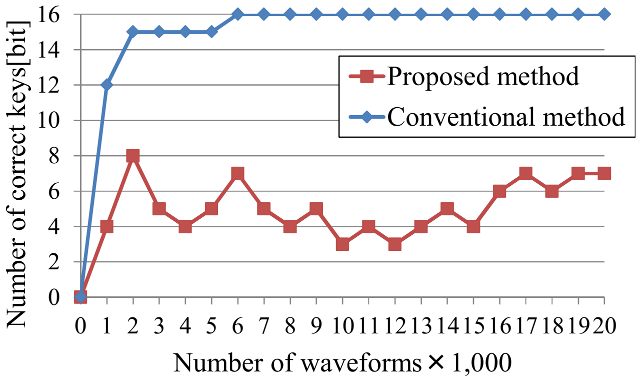


Fig. 7 Comparison results of countermeasure and normal implementation

5 Conclusion

The present study presented two types of power analysis attacks against Simon and proposed a method to prevent those attacks. The evaluation experiment using an FPGA revealed that the proposed power analysis method could attack Simon. Moreover, the proposed method to prevent power analysis attacks was resistant to power analysis attacks. In the future, we will examine whether the proposed method to prevent power analysis attacks is effective against electromagnetic analysis attacks by performing an experiment.

References

1. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptography ePrint Archive, Report 2013/404 (2013) http://eprint.iacr.org/
2. National Security Agency. https://www.nsa.gov/

3. Bogdanav, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B, Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Proceedings of 9th International Workshop Cryptographic Hardware and Embedded Systems (CHES 2007). LNCS, vol. 4727, pp. 450−466. Springer (2007)
4. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T.: Piccolo: an ultra-lightweight blockcipher. In: Proceedings of 13th International Workshop Cryptographic Hardware and Embedded Systems (CHES 2011). LNCS, vol. 6917, pp. 342−357. Springer (2011)
5. Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E.: TWINE: a lightweight, versatile blockcipher. In: Proceedings of ECRYPT Workshop on Lightweight Cryptography (LC11), pp. 146−149 (2011)
6. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Proceedings of International Cryptology Conference (CRYPTO 1999). LNCS, vol. 1666, pp. 388−397 (1999)
7. Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. In: Proceedings of 6th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004). LNCS, vol. 3156, pp. 16−29. Springer (2004)
8. Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic analysis: concrete results. In: Proceedings of 3rd International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2001). LNCS, vol. 2162, pp. 251−261. Springer (2001)
9. Meynard, O., Guilley, S., Danger, J.-L., Sauvage, L.: Far correlation-based EMA with a precharacterized leakage model. In: Proceedings of Design, Automation and Test in Europe (DATE 2010), pp. 977−980 (2010)
10. Federal Information Processing Standards (FIPS) Publication 197: Advanced Encryption Standard (AES), U. S. Department of Commerce/National Institute of Standard and Technology (2001)