Tamper-Resistance Evaluation for Cryptographic Side Channel Leakage at Design Stage

Masaya Yoshikawa, and Toshiya Asai

***Abstract*---**Recently, problems with side-channel attacks have come to the surface. Therefore, the assumption of side-channel attacks and the establishment of countermeasures have become essential for the design and implementation of cryptograms. The present study proposes a method to evaluate the resistance of a circuit to side-channel attacks during the design stage of an LSI encryption processor. The proposed method evaluates the processor's vulnerability to side-channel attacks using information about the current consumption in each cell. Experiments show the validity of the proposed method.

***Keywords*---**Tamper resistance, Cryptographic circuit, Verification, Hardware security.

I. Introduction

POWER analysis attacks are typical side-channel attacks that obtain the observation waveform of the electricity consumed by an encryption device in every encryption process, statistically process the obtained waveform, and estimate a key value based on the correlation between the processed waveform and the internal secret key-related intermediate value. For example, in the advanced encryption standard (AES), for all possible values of a partial key (key for each byte) at the final round, the intermediate value at the final round is inversely calculated from a cipher. When a slight correlation between the obtained intermediate value and the observation waveform is relatively conspicuous, a partial key, which is used at this moment, is estimated to be the correct key. Many measures have been proposed to nullify power analysis attacks. As measures against side-channel attacks, the following two methods have been proposed: (1) disturbance of a correlation with side-channel information by performing an XOR operation for the encryption processing intermediate value using random numbers; and (2) adoption of a circuit structure that performs a complementary operation to offset information leakage to the side channel.

When developing an encryption processor with large-scale integration (LSI), investigators must sufficiently evaluate and determine whether the circuit containing measure against side-channel attacks (hereinafter referred to as a countermeasure circuit), which is to be used for the LSI, is thoroughly resistant to side-channel attacks. The present study proposes a method to evaluate the resistance of a circuit to side-channel attacks during the design stage of an LSI encryption processor. The proposed method evaluates the processor's vulnerability to side-channel attacks using information about the current consumption in each cell. In this way, the reason for the information leakage that causes the vulnerability can be investigated.

Masaya Yoshikawa and Toshiya Asai are with Department of Information Engineering, Meijo University, Nagoya, Japan.

II. Related Studies

The verification for side-channel attacks requires a lot of power consumption waveforms. These power consumption waveforms are generally obtained using commercial tools. In the case where power consumption waveforms are obtained by performing encryption processing for tens of thousands of times-hundreds of thousands of times, when a logic simulator is used, the accuracy of the obtained consumption waveforms is low. However, the use of the SPICE simulator with a high accuracy is not realistic from the viewpoint of the processing time.

III. Proposed Method

Figure 1 shows the procedures in the proposed method. First, Procedure 1 simulates the current consumption during encryption processing using the net list after the placement and the routing in the circuit that is to be verified. Here, the current consumption waveform of each cell is obtained using an event model simulation described in paper [7]. In this simulation, the current consumption waveform of each cell is generated using a method shown in Figure 2. Using this method, data on the current consumption waveforms of all the cells to be verified are prepared.

The data on the current consumption waveforms obtained in Procedure 1 are summarized in the form of a waveform matrix, as shown in Figure 3. In this matrix, encryption processing numbers 1-N are arranged in the row direction and the current consumption waveforms corresponding to all cells 1-M are arranged in the column direction. The current consumption waveforms that are to be attacked are contained in clock cycles. For example, when waveform data on 100 samples exist for each of 500 cells, a row contains data on 50000 samples.

Next, Procedure 2 performs clustering for the patterns of each row in the cell waveform matrix, as shown in Figure 3.

http://dx.doi.org/10.15242/IIE.E0514576

Figure 4 shows the clustering results obtained by assuming that the number of clusters is four. In the column direction, the waveforms are arranged in the same order as that shown in Figure 3.

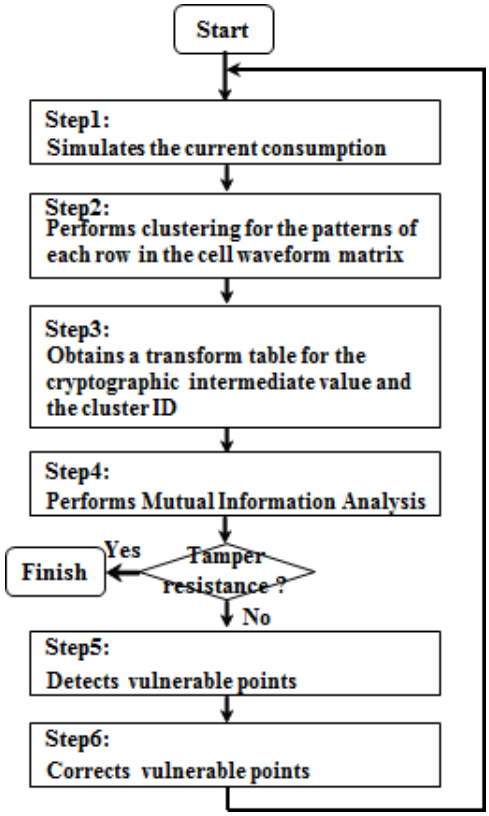

Fig. 1 Procedures in the proposed method

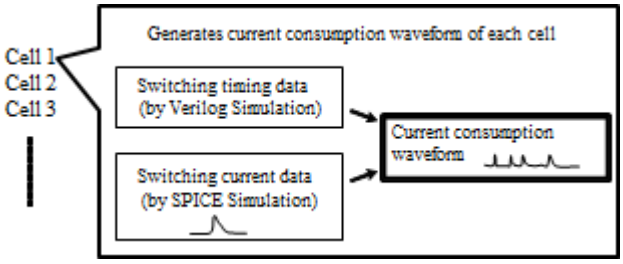

Fig. 2 Example of event model simulation

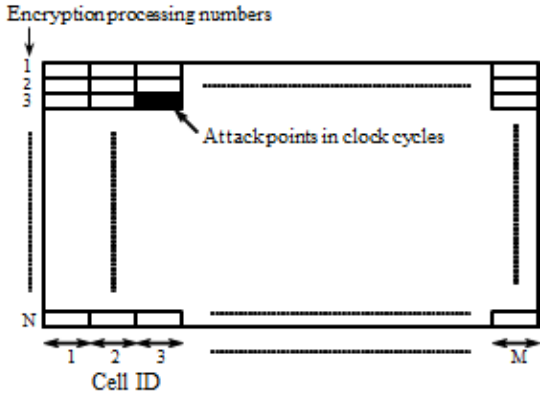

Fig. 3 Example of a waveform matrix

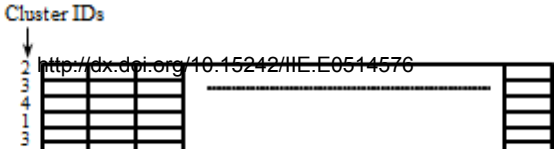

Fig. 4 Example of the clustering results obtained by assuming that the number of clusters is four

However, one of cluster IDs (1-4) is assigned to each row in the row direction. The clustering is processed while judging the similarity of the patterns of each row. Here, the clustering uses nonnegative matrix factorization (NMF). NMF is a clustering method that uses dimension reduction. When an observation data matrix is expressed as Y, a basis matrix is expressed as H, and a coefficient matrix is expressed as U, the NMF is expressed as the following approximate equation (Equation (1)).

$$Y \simeq HU \tag{1}$$

The transposed matrix of the cell waveform matrix in Figure 3 corresponds to Y. When the cell waveform matrix consists of m rows and n columns, Y consists of n rows and m columns. When the number of clusters is K, H is assumed to consist of n rows and K columns and U is assumed to consist of K rows and m columns. Of the K coefficients contained in each column of U, the row number of the largest coefficient is assumed to be a cluster ID.

Next, Procedure 3 obtains a transform table for the cryptographic intermediate value and the cluster ID based on the clustering results. When the cryptographic intermediate value is expressed as DI, the cluster ID is expressed as NC, and a transform function is expressed as FC; consequently, Equation (2) is obtained.

$$N_C = F_C(D_I) \tag{2}$$

Using this FC, Procedure 4 performs a mutual information analysis (MIA)[1]. Here, since the relationship between the cluster ID and the current consumption is investigated, MIA is used instead of correlation power analysis (CPA), which is used to investigate linear correlation. Kernel density estimation is used to obtain the current consumption distribution in MIA. When vulnerability exists in a circuit, the keys can be estimated using MIA. Using the above-mentioned evaluation method for power analysis attacks, vulnerability can be evaluated using operation information about all the cells that comprise the verification circuit.

http://dx.doi.org/10.15242/IIE.E0514576

Figure 5 shows an example that is obtained in such a way that, after clustering, the average of all the waveforms contained in the same cluster ID is obtained, and the obtained average waveform is compared among the clusters. In this example, four average waveforms corresponding to four clusters are plotted. The dispersion among the clusters increases in the second half of the average waveform. In this second half, vulnerability may be high. In the case of a countermeasure circuit using random masks, the state transition of random numbers may cause the dispersion. Therefore, to accurately evaluate vulnerability, an attack simulation is used.

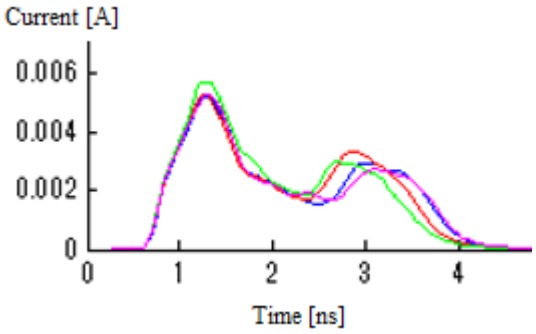

Fig. 5 Example of the average of all the waveforms contained in the same cluster ID

IV. Experiments and Discussion

A. Experimental conditions

The validity of the proposed method was verified using a verification module. Figure 6 shows a verification module used for the AES-embedded SubBytes transform circuit. For evaluation experiments, a countermeasure circuit using each of the various methods is incorporated into the SubBytes transform section. For the module, logic synthesis was applied and the placement and the routing were performed using a 0.18 um complementary metal oxide semiconductor (CMOS) standard cell library. Using the generated net list and delay information, the evaluation experiment was performed following the procedures shown in Figure 1.

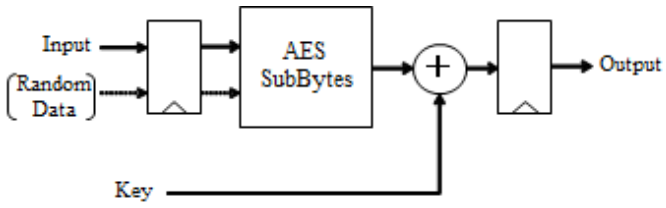

Fig. 6 Verification module

B. Evaluation of vulnerability

As the countermeasure circuit, each of following methods were used and evaluated: masked-AND operation (MAO)[2], threshold implementation (TI)[3], wave dynamic differential logic (WDDL)[4], and masked dual-rail pre-charge logic (MDPL)[5]. Figures 9-12 show the results obtained by performing MIA against each of these methods. The number of waveforms used for the attack was 20,000. For clustering, another 2,000 waveforms were used.

In each of these figures, the horizontal axis represents the elapsed time in an attack cycle and the vertical axis represents the identification ratio of vulnerability to MIA. The identification ratio was defined as the value obtained by dividing mutual information about the correct key by the standard deviation of mutual information about all incorrect keys. These methods were more vulnerable to MIA as the identification ratio was larger; i.e., the key could be obtained using a smaller number of waveforms. Since the key estimation succeeded above the dotted line in these figures, the dotted line can be the standard for vulnerability.

Figure 7 shows the results of MIA against MAO. In this figure, two types of MAO, MAO (HD) and MAO (CL), are plotted. MAO (HD) represents the results obtained by performing MIA using the hamming distance of the intermediate value. MAO (CL) represents the results obtained by performing MIA after obtaining Equation (2) from the clustering results, as mentioned in Chapter 3. Although the keys could not be estimated in MAO (HD), the keys could be estimated above the dotted line in MAO (CL).

Figure 8 shows the results of MIA against TI. Similar to MAO, the keys could not be estimated in TI (HD), but they could be estimated in TI (CL).

Figure 9 shows the results of MIA against WDDL. WDDL (HW) represents the results obtained by performing MIA using the hamming weight. As shown in this figure, the keys could be estimated in WDDL (HW). Therefore, WDDL was vulnerable. The range on the time axis, in which the keys could be estimated, was larger in WDDL (CL) than it was in WDDL (HW). Therefore, WDDL (CL) is more vulnerable than WDDL (HW).

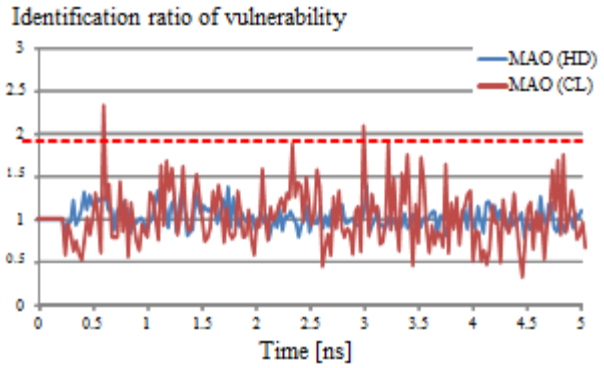

Fig. 7 Results of MIA against MAO

Figure 10 shows the results of MIA against MDPL. The results obtained using MDPL were similar to those obtained using WDDL. Compared to MDPL (HW), MDPL (CL) was more vulnerable.

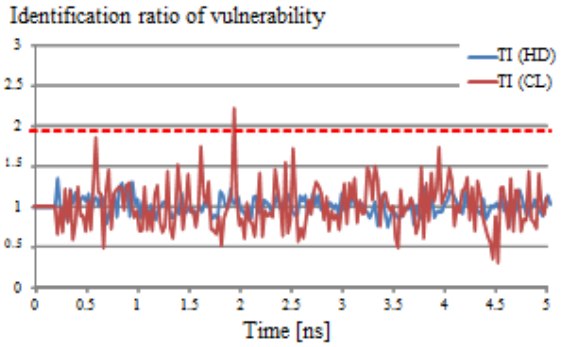

Fig. 8 Results of MIA against TI

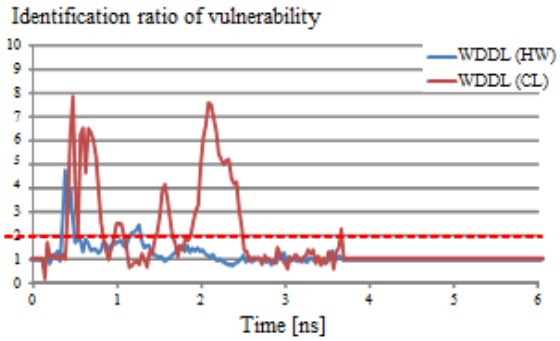

Fig. 9 Results of MIA against WDDL

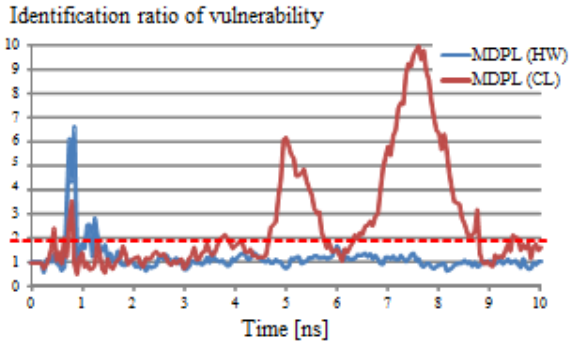

Fig. 10 Results of MIA against MDPL

Thus, the attack using the proposed method could use causes of vulnerability, which could not be found by the attacks using the hamming distance and weight.

In the above-mentioned evaluation, the number of clusters was set at two for MAO and TI and at four for WDDL and MDPL. The number of clusters cannot be judged only by the number of approximation errors during the clustering, and compatibility with MIA should be considered. Therefore, several numbers of clusters must be tested. The present study tested eight clusters. However, no effective attacks were achieved when a large number of clusters were used.

Regarding these four methods, clustering was performed for waveform patterns of the entire horizontal axes in Figures 7-10. When the waveform section used for clustering is narrowed down to a certain time range, the causes of vulnerability due to the characteristics of the waveform in the time range can be extracted.

Therefore, the obtained attack results differ from those obtained by performing clustering for a wide time range. Figure 11 shows the results of MIA obtained when the clustering section was set near 1 [ns] for MDPL (CL) in Figure 10. Thus, the obtained results were closer to MDPL (HW) in Figure 10 than to MDPL (CL) in Figure 10. Consequently, the causes of vulnerability differ according to the differences in the clustering section.

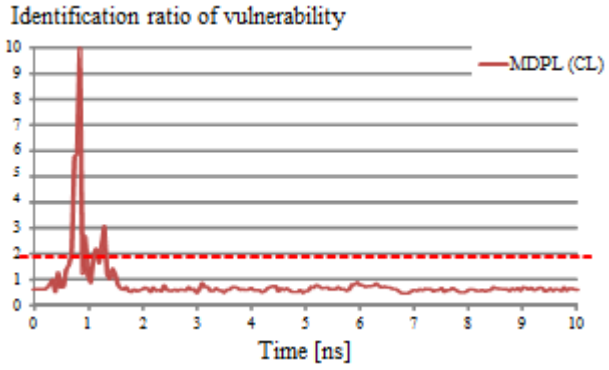

Fig. 11 Results of MIA obtained when the clustering section was set near 1 [ns] for MDPL (CL)

V. Conclusion

The present study evaluated the vulnerability of encryption processing with LSI against power analysis attacks using information about the current consumption of each cell, and proposed a method that could investigate not only the success or failure of the attacks but also the causes of vulnerability.

The present study also confirmed the validity of the proposed method by performing experiments in which a standard cell library and a verification module for an AES-embedded SubBytes transform circuit were used. Using the proposed method in the design stage of an encryption processing circuit, problems with vulnerability against side-channel attacks can be detected in the early stage and amendment can be repeatedly performed within a short period of time.

In the future, we will develop the circuit amendment method and improve the evaluation platforms.

Acknowledgment

This study was supported by Japan Science and Technology Agency (JST), Core Research for Evolutional Science and Technology (CREST).

References

[1] B.Gierlichs, L.Batina, P.Tuyls, B.Preneel, "Mutual Information Analysis", Proc. of CHES 2008, pp.426-442, 2008.

[2] E.Trichina, "Combinational Logic Design For AES SubByte Transformation On Masked Data" , Cryptology ePrint Archive, pp.2003-236, 2003.

[3] S.Nikova,C.Rechberger,and and V.Rijmen, "Threshold Implementations Against Side-Channel Attacks and Glitches", Proc .of ICICS2006, LNCS4307, pp.529-545, 2006.
[4] K.Tiri,I,Verbauwhede, "A Logic level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation", Proc. of Design, Automation and Test in Europe2004, pp246-251, 2004.
[5] T.Pop, S.Mangard, "Masked Dual-Rail Pre-charge Logic:DPA-Resistance Without Routing Constraints", Proc .of Cryptographic Hardware and Embedded Systems 2005, LNCS3659, pp.172-186, 2005.
[6] T.Asai, M.Yoshikawa, "Efficient Acquisition Of The Side-Channel Information Using Event Model Simulation Methods". Proc .of the 30th Symposium on Cryptography and Information Security, 1E1-1, 2013.