Electrical Engineering in Japan, Vol. 186, No. 2, 2014
Translated from Denki Gakkai Ronbunshi, Vol. 131-C, No. 11, November 2011, pp. 1940–1949

Tamper Resistance Simulation on Algorithm Level Design

MASAYA YOSHIKAWA,[1,2] TOSHIYA ASAI,[1,2] MITSURU SHIOZAKI,[3,2] and TAKESHI FUJINO[3,2]
[1]Meijo University, Japan
[2]JST, CREST, Japan
[3]Ritsumeikan University, Japan

SUMMARY

Recently, side-channel attacks have become a serious problem. These attacks estimate the secret keys of cryptography circuits embedded in hardware. In particular, the most threatening side-channel attacks are differential power analysis and correlation power analysis, which use the correlation between information processing and power consumption, which are related to secret keys in cryptography circuits. Therefore, new measures are required to prevent confidential information in cryptography circuits from being leaked to side-channel information, such as power consumption. When designing preventive measures, resistance to side-channel attacks, for instance tamper resistance, must be evaluated. This study proposes a new simulation method by which tamper resistance can be verified in the algorithm and architecture design phases. Experimental results show the validity of the proposed simulation method. © 2013 Wiley Periodicals, Inc. Electr Eng Jpn, 186(2): 40–51, 2014; Published online in Wiley Online Library (wileyonlinelibrary.com). DOI 10.1002/eej.22342

Key words: side-channel attack; cryptography circuit; tamper resistance; algorithm level simulation.

1. Introduction

Systems that store financial information and personal information using LSIs have become widely used in society. Cryptography circuits are used in order to secure secret information in such LSIs, and the standard encryption used has been adequately verified as impossible to decode through brute-force attacks. However, in recent years, the problem of side-channel attacks, in which a secret key is guessed by using side-channel information such as the power consumption of a cryptography circuit in hardware or leaking electromagnetic fields, has arisen. In particular, differential power analysis (DPA) [1–4] and correlation power analysis (CPA) [5–7], which use the correlation between power consumption and information related to a secret key in a cryptography circuit, are particularly dangerous among the various side-channel attacks. As a result, countermeasures [4, 11] to prevent secret information in a cryptography circuit from leaking into side-channel information such as power consumption are required. Furthermore, evaluation of the resistance of such countermeasures to side-channel attacks, that is, tamper resistance, is important starting at the design stage [14]. Thus, we propose a new simulation method that can evaluate tamper resistance to a power analysis attack in the process of upstream design of LSIs with encryption processing in hardware, that is, in the algorithm and architecture design phase.

In general, algorithm-level simulation can be performed in a testing environment defined using HDL behavior descriptions and in C or some other programming language, and information in hardware is not taken into consideration. As a result, high-speed simulations are possible. The algorithm-level simulation discussed in this paper is assumed to be performed in the upstream stages of design to evaluate the robustness of countermeasures using, for instance, a random number mask, against power analysis attacks on a cryptography circuit using dedicated hardware. On the other hand, power consumption leaks, which are a factor in power analysis attacks, are dependent on information in hardware such as the load capacity and operating frequency. Thus, accurate simulation at the algorithm level is difficult. Consequently, there is a trade-off between processing speed and precision.

In the proposed simulation method, we give priority to the logical design of only the part of a circuit subject to attack based on power consumption and create a power consumption model. We overcome the problem of processing speed versus precision by allowing for repeated verifi-

cation by our model before RTL design. Thus, precise and fast simulation is performed in the early stages using a programming language. We verify the effectiveness of the proposed simulation method by several evaluation experiments using standard encryption.

2. Preliminary Considerations

2.1 Advanced Encryption Standard

The Advanced Encryption Standard (AES) is a shared key encryption method with a block length of 128 bits and a selectable key length of 128, 192, or 256 bits. The number of rounds is chosen on the basis of the key length, with 10 rounds for 128 bits, 12 rounds for 192 bits, and 14 rounds for 256 bits. AES encryption consists of four processing operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey. SubBytes is a nonlinear conversion, consisting of the inverse operation on a Galois field and affine transformation of the output. ShiftRows changes the order of 16 bytes of data within the block, and MixColumns performs multiplication on the Galois field for each 4 bytes in the block. AddRoundKey performs an XOR operation on the 16 bytes of data in the block and the 16 bytes of the round key. Figure 1 shows the processing flow in AES128. Below, AES in this paper refers to AES128.

2.2 Power analysis attack

Representative power analysis attacks include DPA and CPA. In DPA, a statistical analysis is performed on a particular bit (reference value) in encryption processing and power consumption. Specifically, a part (partial key) of an unknown encryption key is predicted and the reference value is calculated based on that prediction. Then, based on reference values correlated with the power consumption, the power consumption waveform is divided into two groups (group A and group B). For instance, if the reference value is the median value of 1 bit, then the waveform when the bit value is 0 is classified as group A, and the waveform when the bit value is 1 is classified as group B. If the assumed partial key is correct, then a difference appears in the average power consumption waveforms for group A and group B. Conversely, if the assumed partial key is incorrect, then the classification is performed at random and no difference in the power consumption appears. Thus, by processing pairs of encrypted text and power consumptions statistically, it is possible to analyze whether or not the predicted partial key is correct.

CPA is an attack in which it is assumed that there is a correlation between the Hamming distance and the power consumption when a given register undergoes a transition and the secret key is identified by finding the Pearson correlation coefficient between the Hamming distance and the power waveform. A CPA attack on AES encryption is generally performed by using output timing. In AES, the MixColumns processing is not performed in the final round, as shown in Fig. 1, and thus the median values of the encrypted text and the immediately previous round correspond in byte units. The partial key being used is also in byte units. The median value of the immediately previous round is calculated from the partial key, and the Hamming distance between this value and the encrypted text is found. The coefficient of correlation between the Hamming distance and the power waveform is found for 256 partial keys, and the one with the highest correlation coefficient is assumed to be the correct partial key.

2.3 Related research

Evaluations of tamper resistance to power analysis attacks can be broadly divided into verification using simulations and verification using real equipment. Considerable research has been performed on each.

In verification by simulations, methods using various power consumption models based on design processes have been proposed. First, to simulate power analysis attacks with the Hamming weight or Hamming distance taken as the power consumption, Ref. 2 focuses on the fact that the Hamming weight of the median value in hardware DES reflects the bias in the transition probability due to the nonlinearity of the SubBytes conversion, and demonstrates the possibility of algorithm-level DPA simulation with the Hamming weight as an estimated power level. For hardware-level AES, Ref. 21 performs DPA simulations with the Hamming distance taken as the power consumption model, and compares the results with the performance of

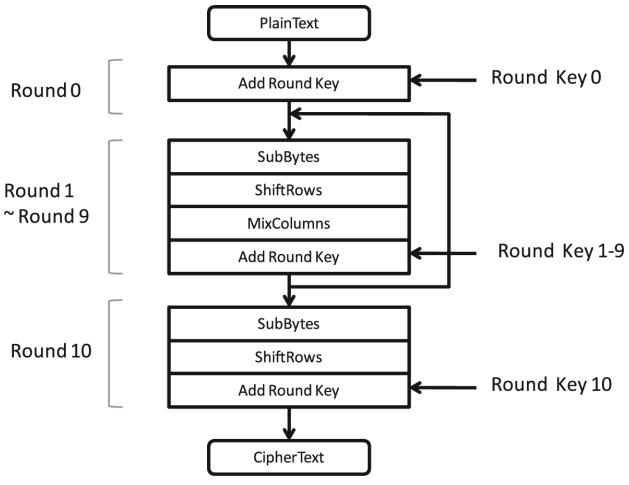

Fig. 1. Procedure for AES encoding.

DPA on a real device. Further, in Refs. 25 and 26, verification is performed on AES using a power consumption model based on the Hamming weight and Hamming distance. In these methods that perform simulations of power analysis attacks with the Hamming weight and the Hamming distance as the estimated power level, verification of the success of the attack is possible during the initial design phase.

Methods that perform simulations of power analysis attacks using toggling information at the gate level as the estimated power level have been proposed for verification in the theoretical design phase. In Ref. 8, the effectiveness of a method that incorporates a PLI for extracting signal transition information in a Verilog simulator, and uses the extracted toggle information as power consumption information for a DPA simulation on DES, is described. Reference 6 also reports a CPA simulation against AES using the same information for the power consumption. In Ref. 18, a method of cycle-based simulation taking account of both toggling information and glitches is proposed.

At the transistor level using SPICE, there are reports of verification [20] in a subcircuit that includes S-Box KASUMI encryption, verification [22] of a circuit with DPA countermeasures based on the WDDL method, verification [23] in an ASIC with DPA countermeasures implemented using random numbers, and verification [24] in the circuit design of custom command sets for encryption processes.

In verification using real equipment, research using SASEBO [9] has been plentiful [10]. Reference 7 reports the CPA evaluation of AES implementations using SASEBO-R. Reference 12 uses SASEBO-R in a similar manner and shows that an attack using the correlation between power consumption and the values of both the Hamming weight and the Hamming distance may be effective, depending on the form of implementation of the SubBytes conversion in AES. Reference 15 reports that several SubBytes conversion circuits account for a large percentage of total power consumption in AES overall. Reference 17 describes countermeasures against a power analysis attack using differences in the power consumption characteristics of several SubBytes conversion circuits.

Reference 16 presents research results for a model of resistance to side-channel attacks. Reference 19 describes a simulation platform for power analysis that takes advantage of commercially available tools.

Thus, when designing encryption hardware, it is important both to verify tamper resistance and to establish the quality of device security by performing simulations. In particular, verification of tamper resistance during the initial phase of design is important from the standpoint of increasing design efficiency and reducing costs. Thus, in the present research we propose an accurate and rapid verification method for verifying tamper resistance in the early design process.

3. The Proposed Simulation Method

In a simulation of tamper resistance against a side-channel attack at the algorithm level in a cryptography circuit using dedicated hardware, it is not necessary to consider the power consumption in the entire circuit: it is the power consumption in the circuits with nonlinearity such as the AES SubBytes conversion that is important. In typical verification of a power analysis attack, thousands to tens of thousands of rounds of encryption must be performed, and power consumption information must be acquired. Acquiring this kind of power consumption information, for instance using a SPICE simulation, is not practical in terms of processing time.

Thus, in the present research we introduce a detailed power consumption model of only the circuit blocks necessary for tamper resistance verification in order to achieve accurate and rapid simulation of tamper resistance during the early design phase. For the other parts of the circuit we introduce a mixed-level simulation method using a verification environment defined in a programming language.

3.1 Power consumption model

In general the power consumption in a CMOS circuit is the sum of the static power consumption and the dynamic power consumption. However, in the power analysis attack described in Section 2.2, the static power consumption need not be taken into consideration because differences are being calculated. Furthermore, the dynamic power consumption can be found in clock units, as shown in Fig. 2, based on a circuit simulation.

Here, t_1 and t_2 are the sampling times in each clock cycle, and $i_1(t_1)$, $o_1(t_1)$, and $\mathrm{P}(t_1)$ are the input state, output state, and power consumption at sampling time t_1. Thus, the dynamic power consumption can be considered as a function of the input and output states. In the present research, for verification in the early design stage we use a general linear iterative model, taking account of verification accuracy, verification speed, and verification cost. Specifically, the power consumption P is approximated as follows:

$$\mathrm{P} = c_0 + c_1 x_1 + c_2 x_2 + \cdots + c_k x_k \qquad (1)$$

t_1: $[i_1(t_1), i_2(t_1), \cdots, i_n(t_1), o_1(t_1), o_2(t_1), \cdots, o_m(t_1), \mathrm{P}(t_1)]$
t_2: $[i_1(t_2), i_2(t_2), \cdots, i_n(t_2), o_1(t_2), o_2(t_2), \cdots, o_m(t_2), \mathrm{P}(t_2)]$
t_3: $\cdots$

Fig. 2. Power consumption in each clock cycle.

Here x_1, x_2, and x_k are the input and output information, and c_0, c_1, and c_k are coefficients. In this investigation the power consumption model is created by the procedure shown in Fig. 3, based on Eq. (1). The procedure for creating a specific power consumption model is illustrated in Fig. 3 for the example of AES.

First, as shown in Fig. 3(1), logic synthesis of a nonlinear circuit (SubBytes conversion) is performed and the results of the synthesis are converted to a SPICE model. Then, as shown in Fig. 3(2), a circuit simulation is performed using a test vector, and the peak value of the power consumption in each clock cycle is extracted.

Next, as shown in Fig. 3(3), the relationship between the extracted power consumption level and the input/output for the test vector used is found. In the present research, two methods of calculating this relationship are introduced: (a) a method using information on the input/output transitions and (b) a method using the values of the input/output signal. The power consumption model obtained by method (a) is referred to as a Hamming distance (HD) model, and an attack that uses this model is called an HD attack. The power consumption model found by method (b) is referred to as a Hamming weight (HW) model, and an attack using this model is called an HW attack.

Table 1 gives the relationships for the HD model. In Table 1, i_1 to i_8 and o_1 to o_8 indicate whether or not there is a transition between the respective input signal and output signal, and pwr denotes the power level based on the simulation. Using the correspondences in the table, the

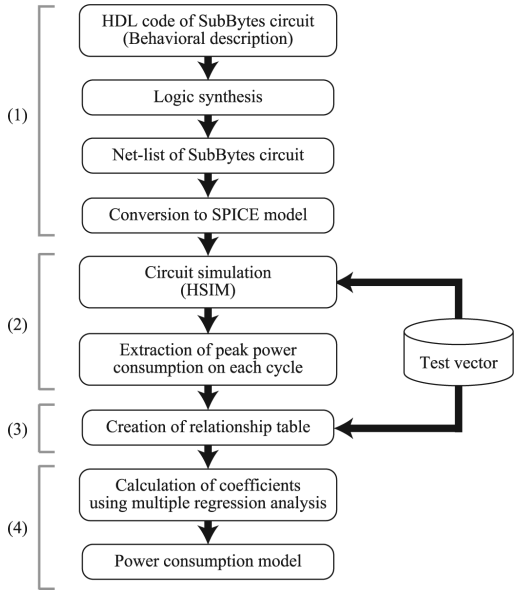

Fig. 3. Procedure for creating power consumption model.

Table 1. Relationship table for power consumption model

i_1	i_2	$\cdots$	i_8	o_1	$\cdots$	o_8	pwr
1	0	$\cdots$	1	0	$\cdots$	0	12.511
0	1	$\cdots$	1	0	$\cdots$	0	8.493
1	1	$\cdots$	0	1	$\cdots$	1	10.226
1	1	$\cdots$	1	0	$\cdots$	0	9.809
				$\vdots$			
0	0	$\cdots$	1	0	$\cdots$	0	11.523

coefficients in Eq. (1) are calculated by multiple regression analysis, as shown in Fig. 3(4). A general model that includes not only the input signal but also the output signal is used in order to obtain the various correspondences. Therefore, the power consumption equation for the HD model is written as

$$\mathrm{P} = c_0 + ci_1 ti_1 + \cdots + ci_8 ti_8 + co_1 to_1 + \cdots + co_8 to_8 \quad (2)$$

Here ti_1 to ti_8 and to_1 to to_8 indicate whether there is a transition in the input bit/output bit in the SubBytes conversion, and c_0, ci_1 to ci_s, and co_1 to co_8 are the coefficients found by multiple regression analysis. Using these coefficients, we create the power consumption model for SubBytes conversion.

For the HW model, the relationship between the value of each bit in the input and output and the power consumption is used. Thus, the power consumption equation for the HW model is

$$\mathrm{P} = c_0 + ci_1 vi_1 + \cdots + ci_8 vi_8 + co_1 vo_1 + \cdots + co_8 vo_8 \quad (3)$$

vi_1 to vi_8 and vo_1 to vo_8 are the values of the input and output bits for the SubBytes conversion, and c_0, ci_1 to ci_8, and co_1 to co_8 are the coefficients found by multiple regression analysis. As in the HD model, we use these coefficients to create the power consumption model for the SubBytes conversion.

3.2 Power analysis attack methods

The methods of simulating a power analysis attack using the proposed approach are illustrated in Fig. 4, taking a CPA attack against AES as an example. Figure 4 shows the final round of AES.

First, an HD attack is possible for a loop architecture configuration in which each round runs in one clock cycle.

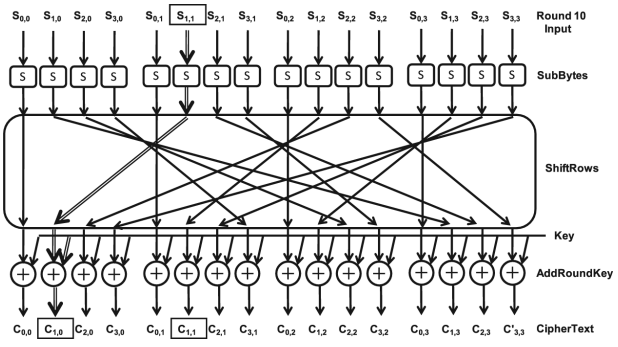

Fig. 4. Example of AES encoding in final round.

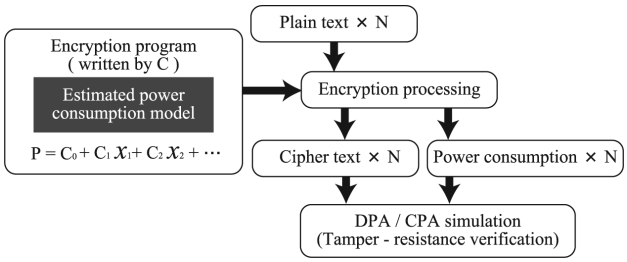

Fig. 5. Procedure for simulation of power analysis attack.

Considering the $C_{1,1}$ byte transition in the encrypted text, its Hamming distance (*Hd*) is

$$Hd(S_{1,1},\, C_{1,1}) = Hw(S_{1,1} \oplus C_{1,1}) \qquad (4)$$

where *Hw* is the Hamming weight. $S_{1,1}$ is the value of the $C_{1,1}$ register one cycle earlier, assuming a loop architecture configuration. The bytes are exchanged by ShiftRows when predicting the value of $S_{1,1}$ from the encrypted text, and thus the value of $C_{1,0}$ in the encrypted text is used:

$$Hd(S_{1,1}, C_{1,1}) = Hw(S^{-1}(C_{1,0} \oplus K_{1,0}) \oplus C_{1,1}) \qquad (5)$$

Here $K_{1,0}$ is the partial key corresponding to $C_{1,0}$. S^{-1} is the inverse conversion in SubBytes, and is the same for the other bytes. Two hundred fifty-six trials are performed against the partial key, the coefficients of correlation between the expected $Hd(S_{1,1}, C_{1,1})$ and the power consumption data are calculated, and the coefficient with the largest value is assumed to indicate the real key. The same holds for the other bytes.

In an HW attack, the input in the final round is used. Prediction of the Hamming weight of $S_{1,1}$ in the input data of the final round is performed as follows:

$$Hw(S_{1,1}) = Hw(S^{-1}(C_{1,0} \oplus K_{1,0})) \qquad (6)$$

using $C_{1,0}$ in the encrypted text. Two hundred fifty-six trials are performed against the partial key, the coefficients of correlation between the expected $Hw(S_{1,1})$ and the power consumption data are calculated, and the coefficient with the highest correlation is assumed to indicate the real key. The same holds for the other bytes.

3.3 Simulation procedure

Figure 5 shows the proposed procedure for simulation of a power analysis attack using the power consumption model. In Fig. 5, a function representing power consumption model (2) or (3) is incorporated into the encryption processing program, encryption is performed on N instances of plain text, and the cipher text × N and the power data × N are acquired. In this process, the difference from real equipment is that the value on the time axis is a single value. That is, the power data used in the simulation consist only of data on the timing of the target of the attack.

Thus, in the proposed simulation, we use the combination of the cipher text and the estimated power value to simulate a power analysis attack similar to that using real equipment.

4. Evaluation Experiments

4.1 Overview of the experiments

In order to verify the effectiveness of the proposed simulation method, we performed several comparison experiments. A Core2 Duo CPU running at 2 GHz with 2 GB of memory was used as the experimental platform, and Design Compiler by Synopsys was employed for the logical synthesis in Fig. 3. NC-Verilog by Cadence was used for the logical simulation, and HSIM by Synopsys for the circuit simulation. In Design Compiler and HSIM, the 0.18-µm rule standard cell library was utilized. We used a side-channel attack reference evaluation board (SASEBO-GII) [9] created by the National Institute of Advanced Industrial Science and Technology in Japan as the FPGA board. As the oscilloscope, we employed an Agilent Technologies DSO1022A.

The simulation environment for verifying tamper resistance in Section 3.3 was written in the C language. The AES encryption algorithm was used for verification, and four methods, the truth table method, the PPRM1 method, the PPRM3 method, and the composite field method, were used as the architectures for the SubBytes conversion. The truth table method is a method that uses a truth table of 256 bytes; PPRM1 [15] is a method described using a one-stage positive polarity Reed Muller (PPRM) expansion; the PPRM3 method [15] is a method described using a three-stage PPRM expansion; and the composite field method

[15] is a method that performs inverse calculations using the composite field GF(((2^2)^2)^2).

4.2 Evaluation of the power consumption model

We performed comparisons in order to verify the accuracy of the power consumption model in the SubBytes conversion circuit. A previously published power consumption model [2] was used for comparison purposes. In this power consumption model, the Hamming weight, the number of "1" bits in the bit string, is used as the power consumption. Because the correlation of the HD model tends to be stronger than that of the HW model, we decided to use the characteristics of the HW model, with its tendency to lower correlation, in order to evaluate the accuracy approximately. Figures 6 to 14 show the results of the comparison. In the figures, the horizontal axis represents the 8-bit Hamming weight of the input terminal. The vertical axis shows the power consumption level, normalized to allow comparison. This normalized power consumption is obtained by dividing the power consumption during input and output in Fig. 2 by the average peak power consumption for the entire cycle.

Figure 6 shows the characteristics obtained when using the previously published power consumption model. In the simulation using the power consumption model of Ref. 2 with the Hamming weight as the power consumption, the architecture of the SubBytes conversion cannot be taken into consideration. Thus, it is the same power consumption model regardless of whether the truth table method, the PPRM1 method, the PPRM3 method, or the composite field method is used.

Figures 7 to 14 show the characteristics of the proposed power consumption model. To allow comparison with the conventional model, which uses the Hamming weight, in the experiments the proposed method also uses the HW model.

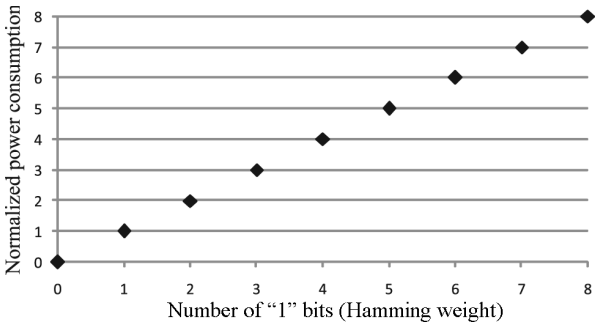

Fig. 6. Results of conventional power consumption model.

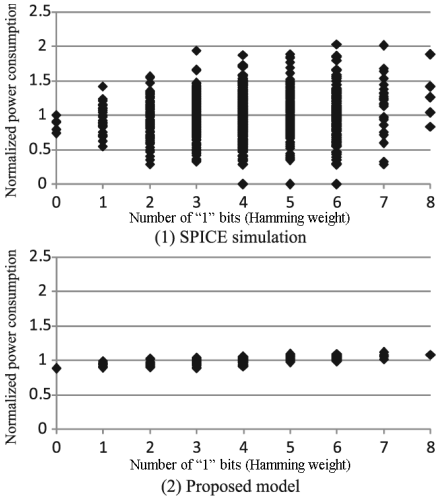

Fig. 7. Results of proposed HW power consumption model with truth table using Test 1.

Figures 7 to 10 show comparisons with a SPICE simulation in which 1000 data elements (referred to as Test 1) were utilized to create a power consumption model for the four architectures for SubBytes conversion. Figures 11 to 14 show the results of comparison with the SPICE simulation for a different set of 1000 data elements from that used in Test 1 (referred to as Test 2). The correspondence in each figure is explained using the truth table method (Figs. 7 and 11) as an example.

Figure 7(1) presents the results of a SPICE simulation on the data (Test 1) used to create the proposed power consumption model, and Fig.7(2) shows a plot of the power

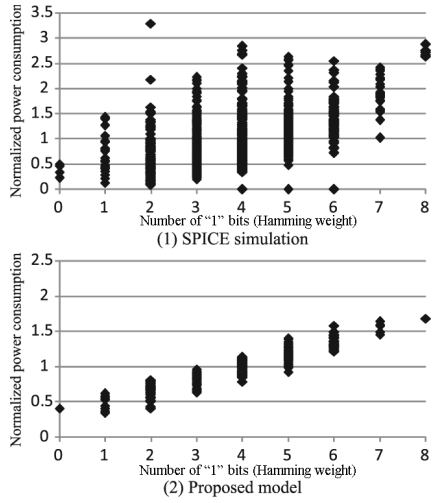

Fig. 8. Results of proposed HW power consumption model with PPRM1 using Test 1.

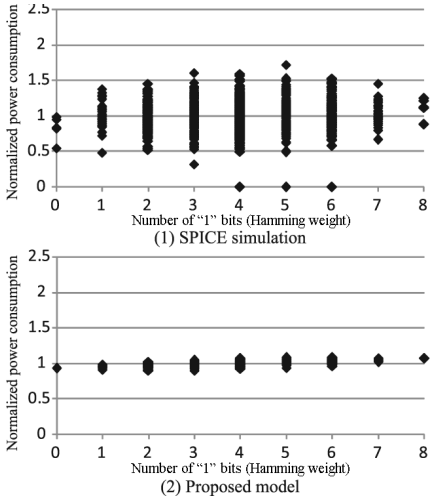

Fig. 9. Results of proposed HW power consumption model with PPRM3 using Test 1.

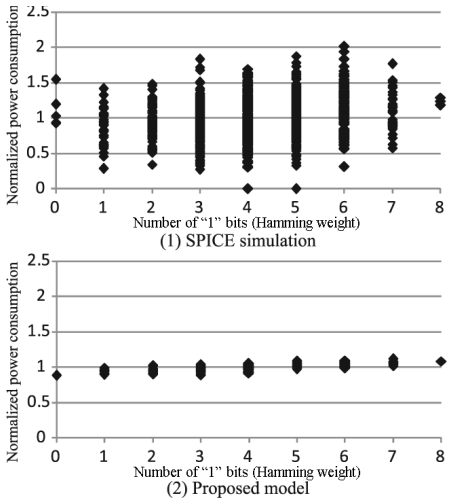

Fig. 11. Results of proposed HW power consumption model with truth table using Test 2.

consumption using Test 1 as input in the proposed power consumption model. Specifically, Fig. 7(2), presenting the results for the proposed method, shows that if the merits of Fig. 7(1), representing the SPICE simulation, are captured, the prediction accuracy of the multiple regression analysis used in the proposed power consumption model is high. Figure 11(1) gives the results of a SPICE simulation for the separate data (Test 2), and Fig. 11(2) shows a plot of the power consumption when using Test 2 as input for the proposed power consumption model.

Thus, in the experiment using data with no relation to the creation of the proposed power consumption model,

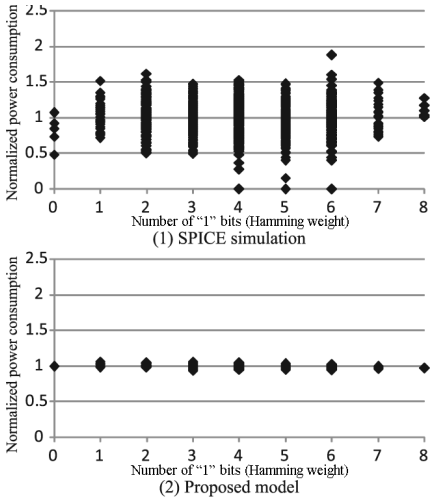

Fig. 10. Results of proposed HW power consumption model with composite field using Test 1.

if Fig. 11(2), the results for the proposed method, can capture the characteristics of Fig. 11(1), representing the results of the SPICE simulation, then the proposed power consumption model can be considered very precise.

First, in the comparative experiments using the truth table method, the PPRM1 method, and the PPRM3 method with Test 1, as shown in Figs. 7 to 9, it can be seen that there is a correlation between the results of the proposed power consumption model and the SPICE simulation. In the PPRM1 method in particular, the increase in power consumption is clearly proportional to the Hamming weight. This confirms that the proposed power consumption model using multiple regression analysis is effective.

In the comparative experiments using Test 2 shown in Figs. 11 to 13 there is likewise a correlation with the SPICE simulation, as in the case of the comparative experiments using Test 1.

Thus, in the truth table method, the PPRM1 method, and the PPRM3 method, by introducing the proposed power consumption model into the SubBytes conversion circuit, the target of the power analysis attack, an estimate of power consumption differences in the architecture of the SubBytes conversion can be obtained.

On the other hand, for the composite field test, as shown in Figs. 10 and 14, the characteristics of the proposed power consumption model and the SPICE simulation differ slightly in some places. In the proposed power consumption model, a tendency to a small slope (difference) in the power consumption versus the Hamming weight can be represented, as in the case of the SPICE simulation. However, when the Hamming weight is 0 or 8 the characteristics are the reverse of those in the SPICE simulation. Cases in which the Hamming weight is 0 or 8 are relatively few, and

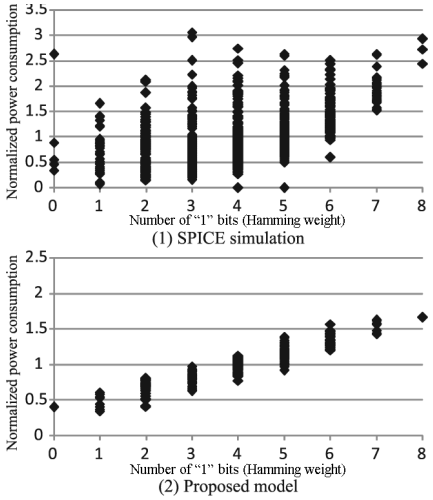

Fig. 12. Results of proposed HW power consumption model with PPRM1 using Test 1.

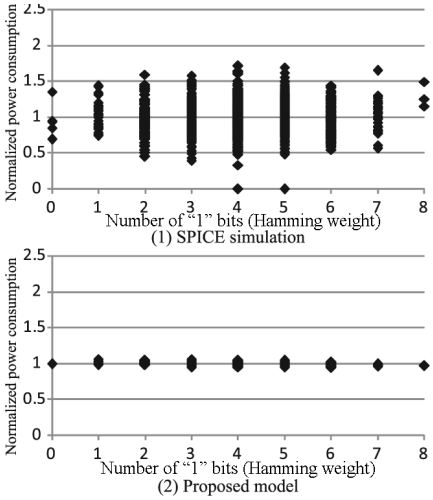

Fig. 14. Results of proposed HW power consumption model with composite field using Test 2.

approximation error can easily occur. In particular, because this slope is small in the composite field method, we might consider that the inverse slope occurs.

In order to investigate the relationship between the amount of data used and the approximation error, we performed a comparison experiment using the data of Test 1 (data count = 1000), and also Test 1a with an additional 4000 data elements (data count = 5000). Figure 15(1) shows a plot with expansion of the vertical axis of Fig. 10 (data count = 1000), and Fig. 15(2) gives the experimental results obtained with Test 1a (data count = 5000).

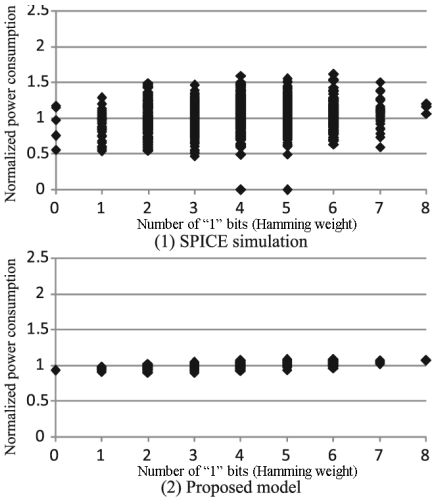

Fig. 13. Results of proposed HW power consumption model with PPRM3 using Test 2.

Comparison of Figs. 15(1) and (2) shows that the characteristics of the proposed power consumption model are improved even when the Hamming weight is 0 or 8, that is, the characteristics of the results of the SPICE simulation are better approximated. On the other hand, in a preliminary experiment using 300 data, cases in which the Hamming weight was 0 or 8 were very few. Thus, in order to capture the resistance trends of each SubBytes conversion architecture, a data count of about 1000 is required.

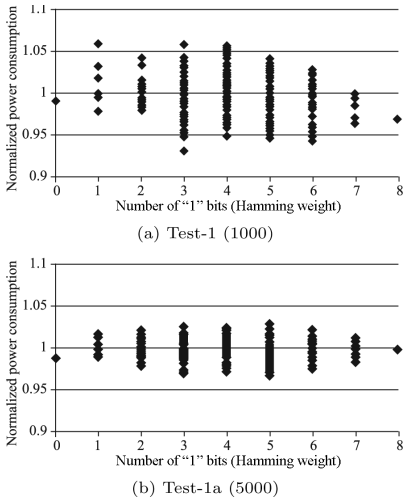

Fig. 15. Results of proposed HW power consumption model with composite field using Test 1 and Test 1a.

4.3 Evaluation of power analysis attacks

Next, we performed a CPA experiment on AES in accordance with the simulation procedure shown in Fig. 6, using the proposed power consumption model. First, for comparison with the previously published power model, we performed an experiment using an HW attack. Figures 16 and 17 show the results of the experiment. In both figures, the vertical axis represents the number of revealed keys, and the horizontal axis represents the number of waveforms required. In a simulation using the conventional power model [2], identical experimental results were obtained for all SubBytes conversion architectures, as shown in Fig. 16.

In the proposed method, the PPRM1 approach readily succeeded in all key attacks, just as in the attack results [7] using real equipment (dedicated encryption LSI), as shown in Fig. 17. In the composite field method, the attacks on the keys failed. Thus, under the proposed method, we were able to simulate whether a CPA attack succeeded depending on differences in the SubBytes conversion architectures based on the PPRM1 method and the composite field method.

However, in the proposed method, all of the keys were identified by the PPRM3 method and the truth table method, and while some keys were identified in the PPRM3 method using real equipment, in the truth table method the attack did not succeed. Improvement of the accuracy of the PPRM3 method and the truth table method in an HW attack constitutes a topic for the future.

Next, we performed an experiment using an HD attack. A comparison of the HW and HD attacks shows that the latter is a more powerful attack method. Figure 18 shows the results of the experiment. The vertical and horizontal axes in Fig. 18 are the same as in Figs. 16 and 17. In this attack too, Fig. 18 shows that the composite field method requires more waveforms for key identification than the truth table method, the PPRM1 method, or the PPRM3 method, just as in the results of CPA using real equipment [7].

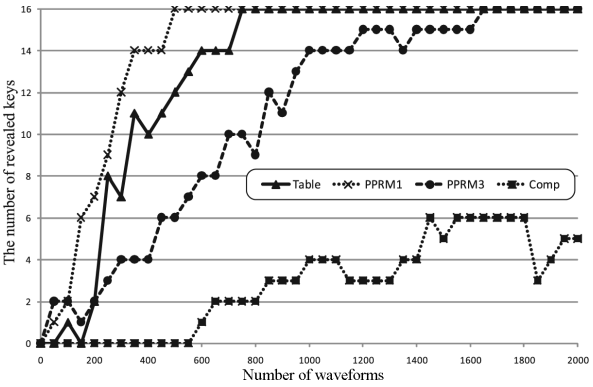

Fig. 17. Results of HW attack for each architecture using the proposed consumption model.

Thus, in the proposed simulation method, it is possible to verify tamper resistance with the differences in the SubBytes conversion architecture taken into account, and to verify tamper resistance under various attack methods, both of which are impossible in conventional simulation methods using the Hamming weight as an estimate of the power level.

4.4 Evaluation of countermeasure circuits

Section 4.3 gave an evaluation of power analysis attacks against typical circuit architectures. In this section, we describe an evaluation of a circuit that employs power analysis countermeasures. Random switching logic (RSL) [13] is a representative method for countermeasures. RSL achieves resistance to a power analysis attack by breaking the correlation between power consumption and encryption

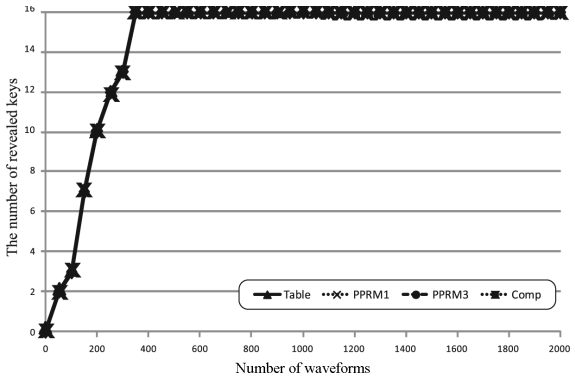

Fig. 16. Results of HW attack for each architecture using the conventional power consumption model.

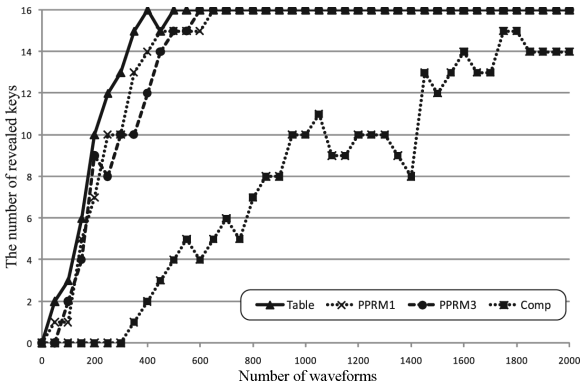

Fig. 18. Results of HD attack for each architecture using the proposed consumption model.

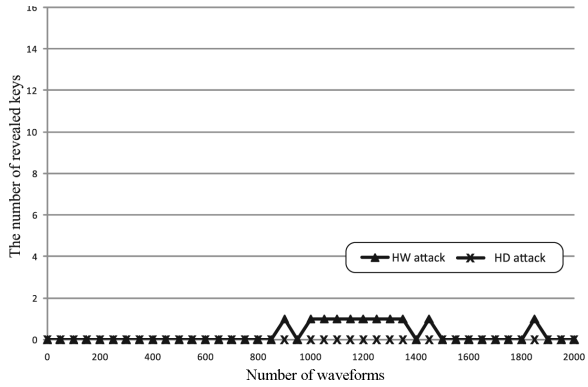

Fig. 19. Simulation results for RSL circuit.

processing by means of logic switching with random numbers (a random number mask). We performed two attack experiments, using an HW attack and an HD attack, against RSL. Figure 19 shows the results of the experiments. As in the experimental results for an ASIC in Ref. 7, Fig. 19 shows that neither power analysis attack could be performed against RSL. Thus, the proposed method achieves accurate simulation at the algorithm level even for a circuit such as RSL that employs countermeasures against a power analysis attack.

4.5 Evaluation of processing time

In order to evaluate the processing time, we compared the time required to acquire the power consumption information and the time required for simulation. Table 2 gives the measured values. "Waveforms" in Table 2 denotes the time required to acquire the power consumption information for 10,000 waveforms. "CPA Sim." denotes the processing time in a CPA simulation using 10,000 waveforms. As can be seen from Table 2, in the proposed simulation method, rapid processing is achieved when acquiring the power consumption information in the early design phase. A similar processing time was obtained for the CPA simulation because it was performed using a similar procedure to that for real equipment.

Table 2. Comparison of processing time

	Level	Waveforms	CPA Sim.
Proposed Sim.	Algorithm	6sec	35min
Timing Sim.	Logic	11min	36min
SPICE Sim.	Physical	131h	36min
FPGA board	Actual device	80min	36min

5. Conclusions

We have proposed a new simulation method capable of verifying the tamper resistance of encryption devices at the algorithm level. In the proposed simulation method, we introduce an accurate power consumption model for only circuit blocks with nonlinear characteristics that are targeted in a side-channel attack. We use a verification environment defined in a programming language for all other parts. By using this mixed-level simulation method, we were able to achieve fast and accurate simulations. We used AES encryption and performed evaluation experiments not only on four SubBytes conversion architectures, the ordinary truth table method, the PPRM1 method, the PPRM3 method, and the composite field method, but also on a circuit with countermeasures against a power analysis attack. An experimental evaluation of CPA against AES was also performed. In the proposed simulation method, the encryption algorithm can be readily changed to DES or another encryption algorithm.

Future topics of research include improving the accuracy of the PPRM3 method and the truth table method in an HW attack. We also plan to perform an analysis of fault utilization attacks.

REFERENCES

1. Kocher PC, Jaffe J, Jun B. Differential power analysis. Proc of the International Cryptography Conference '99, p 388–397.
2. Sasaki A, Abe K. Algorithm level evaluation of DPA resistivity against cryptosystems. IEEJ Trans EIS 2006;126:1221–1228. (in Japanese)
3. Miyamoto A, Homma N, Aoki T, Satoh A. An experimental comparison of power analysis attacks against RSA processors on ASIC and FPGA. Proc of 14th Workshop on Synthesis and Systems Integration of Mixed Information Technologies, p 53–63, 2009.
4. Kojima K, Okuyama K, Iwai K, Shiozaki M, Yoshikawa M, Fujino T. LSI implementation method of DES cryptographic circuit utilizing domino-RSL gate resistant to DPA attack. Proc of the 16th Workshop on Synthesis and System Integration of Mixed Information Technologies, p 169–201, 2010.
5. Brier E, Clavier C, Olivier F. Correlation power analysis with a leakage model. Proc of Cryptographic Hardware and Embedded Systems 2004, p 16–19.
6. Yamakoshi K, Yamagishi A. Estimation of CPA attack for AES using simulation method. IEICE Tech Rep, ISEC, Vol. 109, No. 42, p 13–20, 2009-05-15. (in Japanese)
7. Kawamura K, Iwai K, Kurokawa T. Tamper resistance of implementation methods of AES against

CPA. Proc of Forum on Information Technology, Vol. 4, p 147–148, 2009. (in Japanese)
8. Saeki M, Suzuki D, Ichikawa T. Construction of DPA leakage model and evaluation by logic simulation. IEICE Tech Rep, ISEC, Vol. 104, No. 200, p 111–118, 2004-07-14. (in Japanese)
9. Side-channel Attack Standard Evaluation Board (SASEBO) web page, http://www.rcis.aist.go.jp/.
10. Cryptographic Hardware Project web page, http://www.aoki.ecei.tohoku.ac.jp/crypto/web/cores.html.
11. Sasaki M, Iwai K, Kurokawa T. A design of AES S-BOX circuit for DPA countermeasure. IEICE Tech Rep, Vol. 106, No. 394, p 1–6, 2006-1123. (in Japanese)
12. Yamamoto D, Ochiai T, Itoh K, Takenaka M, Torii N, Uchida D, Nagai T, Wakana S. Hybrid correlation power analysis. Proc of Symposium on Cryptography and Information Security, 3B1-2, 2010. (in Japanese)
13. Suzuki D, Saeki M, Simizu K, Satoh A. A design methodology for a DPA-resistant cryptographic LSI with RSL techniques. Proc of Cryptographic Hardware and Embedded Systems (CHES 2009), Lecture Notes in Computer Science, p 189–204.
14. Katashita T, Satoh A, Nagata M, Fujimoto D, Kikuchi K, Nakagawa H, Aoyagi M. DPA characteristic measurement for board level simulation of side-channel analysis. Proc of Symposium on Cryptography and Information Security, 4B2-1, 2010. (in Japanese)
15. Morioka S, Satoh A. A logic design methodology of low-power AES cryptographic circuits. Trans IPSJ 2003;44:1321–1328. (in Japanese)
16. Kawamura S, Koike M, Shiba M, Sano F, Nozaki H. A digital model for assessing side-channel attack resilience. Proc of Symposium on Cryptography and Information Security, p 519–524, 2001. (in Japanese)
17. Zheng Z, Zou X, Liu Z, Chen Y. Security analysis and optimization of AES S-Boxes against CPA attack in wireless sensor network. Proc of Wireless Communications, Networking, and Mobile Computing, p 2608–2612, 2007.
18. Chen Z, Shaumont P. Early feedback on side-channel risks and accelerated toggle-counting. Proc of IEEE Workshop on Hardware Oriented Security and Trust, p 90–95, 2009.
19. Bai X, Wang Y, Wang Y, Hu X. A power analysis attack software simulation platform design and its applications. Proc of the International Conference on Computer Engineering and Technology, Vol. 6, p 479–482, 2010.
20. Regazzoni F, Badel S, Eisenbarth T, Grobschadl J, Poschmann A, Toprak Z, Macchetti M, Pozzi L, Parr C, Leblebici Y, Ienne P. A simulation-based methodology for evaluating the DPA-resistance of cryptographic functional units with application to CMOS and MCML technologies. Proc of IEEE 2nd International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulations, p 209–214, 2007.
21. Börs S, Gürkaynak FK, Oswald E, Preneel B. Power-analysis attack on an ASIC AES implementation. Proc of IEEE International Conference Information Technology: Coding and Computing, p 546–552, 2004.
22. Tiri K, Verbauwhede I. A VLSI design flow for secure side-channel attack resistant ICs. Proc of Design, Automation and Test in Europe Conference, p 58–63, 2005.
23. Bucci M, Guglielmo M, Luzzi R, Trifiletti A. A power consumption randomization countermeasure for DPA-resistant cryptographic processors. Proc of 15th International Workshop Power and Timing Modeling, Optimization and Simulation, p 481–490, 2004.
24. Regazzoni F, Cevrero A, Standaert FX, Badel S, Kluter T, Brisk P, Leblebici Y, Ienne P. A design flow and evaluation framework for DPA-resistant instruction set extensions. Proc of Cryptographic Hardware and Embedded Systems, p 205–219, 2009.
25. Bucci M, Luzzi R, Menichelli F, Menicocci R, Olivieri M, Trifiletti A. Testing power-analysis attack susceptibility in register transfer level designs. IET Information Security 2007, Vol. 1, No. 3, p 128–133.
26. Menichelli F, Menicocci R, Olivieri M, Trifiletti A. High level side channel attack modeling and simulation for security-critical systems-on-chips. IEEE Trans Dependable and Secure Computing 2008;5:164–176.

AUTHORS (from left to right)




Masaya Yoshikawa (member) completed the doctoral program at the Graduate School of Engineering of Ritsumeikan University in 2001. After becoming a lecturer and subsequently an instructor in the First Department of Engineering of the same university, he was appointed an associate professor on the Faculty of Engineering of Meijo University in 2007. He became a CREST researcher in 2009. He is engaged in research on LSI design and design automation technology. He received an ISCIE Industrial Technology Award, a CAINE 2010 Best Paper Award, a FIT 2003 Best Paper Award, and a Third LSI IP Design Award for Development Scholarship. He holds a D.Eng. degree, and is a member of IPSJ, IEICE, ISCIE, the Japan Society for Fuzzy Theory and Intelligent Informatics, and IEEE.

Toshiya Asai (nonmember) received a bachelor's degree from the Department of Electrical Engineering of Tohoku University in 1984 and joined Sony, where he worked on the design of video equipment for the broadcasting industry. In 2010 he became a CREST researcher at Meijo University, where he is engaged in research on tamper-resistant LSI design. He is a member of IEEE.

Mitsuru Shiozaki (nonmember) completed the doctoral program in physics at the Graduate School of Engineering of Hiroshima University in 2006. He became a CREST researcher in 2010, investigating tamper-resistant LSI design. He holds a D.Eng. degree, and is a member of IEICE and IEEE.

Takeshi Fujino (nonmember) received a bachelor's degree from the Department of Electronic Engineering of the University of Kyoto in 1984, completed the M.E. program in 1986, and joined Mitsubishi Electric, where he was engaged in research on semiconductor micromachining technology and memory circuit design. He received a Chemical Technology Prize from the Kinki Chemical Society in 1995. In 2003 he was appointed a professor on the Faculty of Engineering of Ritsumeikan University, where he is engaged in research on application-specific LSI and programmable LSI. He received a 2008 LSI IP Design Award Research Grant. In 2009 he became a JST/CREST researcher, investigating tamper-resistant LSIs. He holds a D.Eng. degree (University of Kyoto, 1995), and is a member of IEICE, IPSJ, JSAP, and IEEE.