DPA Attacks Simulator against Cryptography System on Algorithm Design Phase

Masaya Yoshikawa and Toshiya Asai

***Abstract*—When the encryption standard is incorporated into electronic devices as a security LSI, it is possible to estimate confidential information, such as cipher keys, by analyzing power consumption information that is leaked during the LSI's operation. Therefore, when an encryption algorithm is incorporated into hardware, it is important to evaluate the resistance against the attacks (tamper resistance) in the early stages of designing the algorithm. In this study, we proposes a new simulator to verify tamper resistance at the algorithm level. The proposed simulator realizes DPA simulation corresponding to multiple attack methods. Experimental results proved the validity of the proposed simulator.**

***Index Terms*— Differential Power Analysis, Cryptography system, Algorithm-level simulation, Information security, Tamper-resistance verification**

I. Introduction

ELECTRONIC devices handling confidential information such as IC cards are secured by encrypting data. The encryption standard, which has been widely diffused in recent years, is certified that its decryption is computationally impossible. However, it was recently reported that even if an encryption algorithm is theoretically secured, when the algorithm is incorporated into hardware, confidential information about the algorithm could be improperly specified using either power consumption or processing time when the hardware is operated. Such improper specifications are generally called side-channel attacks. In particular, differential power analysis (DPA)[1] is very risky, because it cracks security codes by statistically processing the difference in power consumption and can be easily attacked. Therefore, when an encryption algorithm is incorporated into hardware, it is important to evaluate the resistance against side-channel attacks (tamper resistance) in the early stages of designing the algorithm.

Several studies [2]-[5] have focused on tamper resistance at different design levels. For example, in a study on tamper resistance at the algorithm level, Sasaki et al.[2] reported that side-channel attacks could be performed by a simulator using a hamming weight power consumption model. In a study at the logic design level, Saeki et al.[3] developed a simulator in which electricity consumption was estimated using toggle frequencies. At the actual device level, many studies used SASEBO[6], which is a standard evaluation board. Several studies on architectures considered DPA resistance against encryption devices.

This study proposes a new simulator to verify tamper resistance at the algorithm level, which will be very important in the future. The proposed simulator realizes DPA simulation corresponding to multiple attack methods that have not been handled by already published simulators. By comparing the results obtained using an actual device, the validity of the proposed simulator is verified. The organization of this paper is as follows: Section 2 explains the principle of DPA and two kinds of attacks. Section 3 introduces the proposed simulator, and Section 4 reports the experimental results in comparison with the actual device. Finally, Section 5 summarizes and concludes the paper.

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

II. Principle of DPA attacks

DPA is one of the side-channel attacks in which analysis is statistically performed focusing on power consumption. The DPA uses the correlation between a specific bit (reference value) and power consumption during cipher processing. Actually, part of an unknown cipher key (partial key) is predicted, and a reference value is calculated from the prediction. Based on the reference value which is correlated with power consumption, power consumption waveforms are classified into two groups (A and B). In group A, power consumption waveforms, which are obtained when power consumption is low, are collected. In group B, power consumption waveforms which are obtained when power consumption is high, are collected. If the predicted cipher key is correct, the difference in power consumption will appear in the average power consumption waveforms of groups A and B. If the predicted cipher key is incorrect, the difference in power consumption will not appear because the classification is performed at random. By statistically processing a pair of the cipher text and power consumption, whether the predicted cipher key is correct can be analyzed. The DPA can be classified into two types: humming-weight DPA and humming-distance DPA.

A. Humming-weight DPA

In general complementary metal oxide semiconductor (CMOS) circuits, power consumption of nonlinear gates, such as AND and OR gates, differ according to their input and output values. In the humming-weight DPA, grouping is performed by using the power consumption as a reference value. The power consumption in CMOS circuits is classified into three types: power consumption due to switching, that due to pass-through current, and that due to leakage current.

In the humming-weight DPA, since the power consumption waveforms are statistically processed, power

ISBN: 978-988-19251-7-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

consumption due to the leakage current is not necessary to consider. Additionally, power consumption due to the switching and the pass-through current depend on the transition probability. The humming-weight DPA is detailed below using a two-input AND gate as an example. There are four input patterns of ([a, b] = [0, 0], [0, 1], [1, 0], and [1, 1]) before and after the transition. Therefore, the number of input patterns when the time is changed from t1 to t2 is 16 (4 x 4). Table 1 demonstrates the input patterns when input a1 before the transition is set at a specific bit (reference value).

TABLE I
Example of the principle of hamming-weight DPA

a_1	b_1	a_2	b_2	c_1	c_2
0	0	0	0	0	0
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
1	0	0	0	0	0
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	0	1	0
1	1	1	1	1	0
1	1	1	1	1	1

The number of input patterns when a1 is '0' is 8. In these 8 patterns, the values of 2 patterns are transitioned. Therefore, the transition probability is 2/8 = 1/4. The number of input patterns when a1 is '1' is 8. In these 8 patterns, the values of 4 patterns are transited. Therefore, the transition probability is 4/8=1/2. Since the transition probability differs according to the specific input value a1, thus the value of a1 can be derived from the power consumption data. Consequently, if the secret key information is related to the value of a1, the secret key information is revealed by the statistical analysis of power consumption.

B. Humming-distance DPA

The hamming-Distance DPA is a method to predict secret key by judging whether the value of a register is transitioned. The cryptographic circuit using loop architecture can be attacked by this DPA. The resister data is updated by the output of combinational logic whose inputs are the previous resister data and the round key. The round key is calculated from the secret key, hence the secret key can be predicted by the round key. In the encryption sequence, the output value of a register Q_{final} at the final round can be obtained from the cipher text. The output value of a register Q_{final} at the final round is a known value which is obtained from the cipher text. The value of resister $Q_{final-1}$ at the pre-final round can be calculated from the presumed round key and Q_{final}. Therefore, the hamming-distance of Q_{final} and $Q_{final-1}$ are calculated by EXOR processing these values. The hamming-distance of the resister means the transition of output node, thus the power consumption with larger hamming-distance get larger. If the difference of power consumption between 'presumed' large hamming-distance (group A) and small hamming-distance (group B) appears, the presumed round key is correct.

III. Proposed Simulator

The proposed simulation method can cope with both hamming weight-type and hamming distance-type attacks. Using data encryption standard (DES)[7], two DPA simulation methods are explained. DES is a common key cryptography in which 64-bit plain texts are encrypted by a 56-bit key. In the encryption, a process including F function is repeated 16 times (rounds). Figure 1 shows processes at rounds 15 and 16 in DES encryption processing.

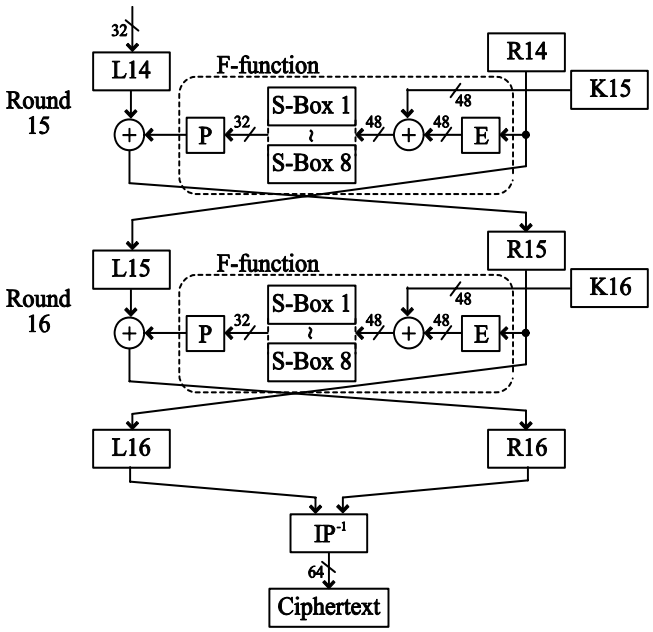

Fig.1 Rounds 15 and 16 in DES encryption processing

When DES is incorporated into hardware, the process is generally composed of F function for a round and loop architecture consisting of register groups. The substitution-box (S-Box) in F function is the section that performs nonlinear transformation and is the object of a DPA attack.

In hamming weight-type DPA, 6 bits (an estimation key), which is related to the S-Box to be attacked, are predicted in 48 bits of K16, a secret key of round 16. Figure 2 shows the relationship between the S-Box and the estimation key. In R14 (L15), which is the input of F function at round 15, when a node correlating with the estimation key is '0,' electricity consumption is defined as group 0. When the node is '1,' electricity consumption is defined as group 1. By using these groupings, the secret key can be analyzed. Similar to hamming weight-type DPA, 6 bits are predicted as the estimation key in hamming distance-type DPA. Here, the output of a delay flip-flop (DFF) (R) is noticed, and grouping is performed to determine whether a node to be noticed is transited between one round before the final round and the final round (R 14 and R 15 in Figure 1). By using this grouping, the secret key can be analyzed.

ISBN: 978-988-19251-7-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

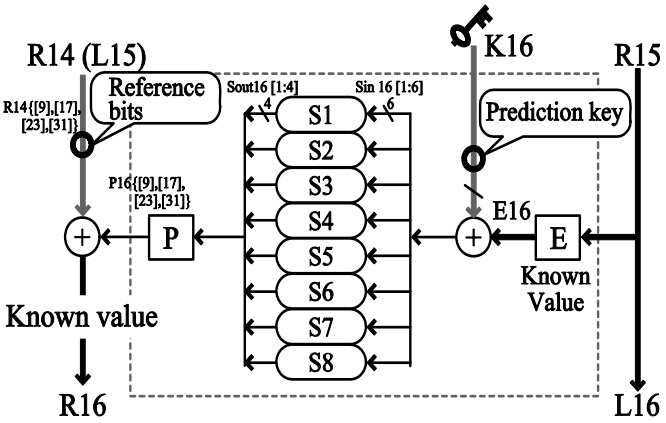

Fig.2 Relationship between S-Box and the estimation key

In DPA using an actual device, power consumption can be measured using an oscilloscope. In simulation at the algorithm level, actual power consumption values cannot be used. Therefore, in the proposed simulator, power consumption estimations corresponding to hamming weight-type or hamming distance-type DPA are used. In hamming weight-type DPA, the number '1' in the sequence of data expressions in the algorithm, which corresponds to the bit string including reference values, is defined as power consumption. In hamming distance-type DPA, the transition bit number in the sequence of data expressions is defined as power consumption.

Figure 3 shows the actual procedure of the simulation of the power analysis attack in the proposed simulator. In Figure 3, the process of encryption is executed to N plain texts; N cryptograms and N pieces of electricity consumption data are acquired. Here, only the electricity consumption data of the timing that is to be attacked is used. Thus, using a pair of cryptograms and electricity consumption estimation, the simulation of a power analysis attack is performed, which is similar to the case of an actual device.

IV. Experiments and Discussion

A. Experiment Outline

To verify the validity of the proposed simulator, several evaluation experiments were performed.

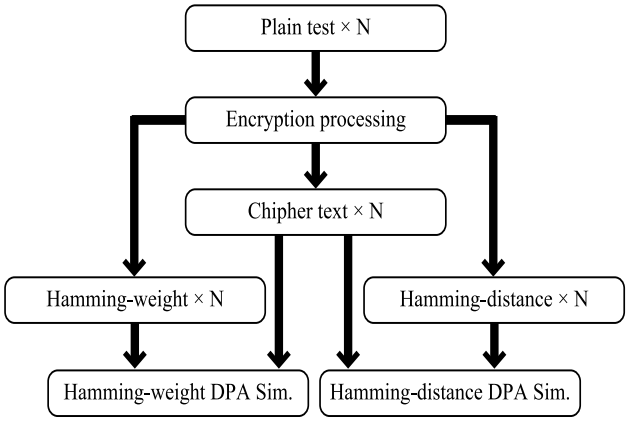

Fig.3 Procedure of software simulation for DPA attacks

In comparison experiments with an actual device, SASEBO-GII[6], a board for evaluating side-channel attacks, was used. Figure 4 shows an experimental environment using SASEBO-GII.

Since SASEBO-GII is a field programmable gate array (FPGA) board, in order to realize the DPA characteristics that are the same as those of typical application-specific integrated circuits (ASICs), each theory of the cryptography circuit was changed to the primitive gate and assigned to each look-up table (LUT).

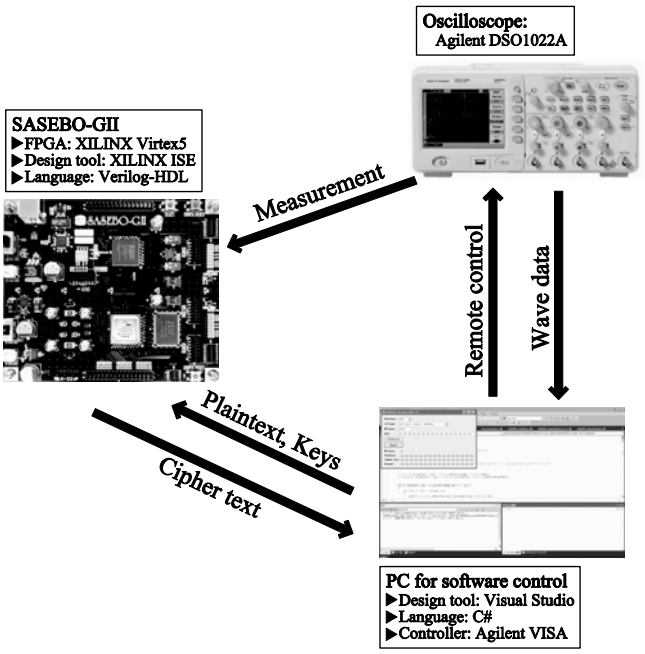

Fig.4 DPA environment when an actual device was used

B. Comparison with a DPA Actual Device

Experiments to evaluate two DPA attack methods (hamming weight-type attack and hamming distance-type attack) were performed. Figures 5 and 6 show the experimental results.

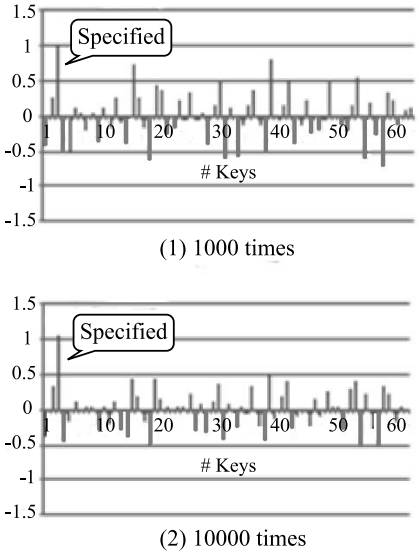

Fig.5 Simulation results of a hamming weight-type attack obtained using the proposed simulator

ISBN: 978-988-19251-7-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

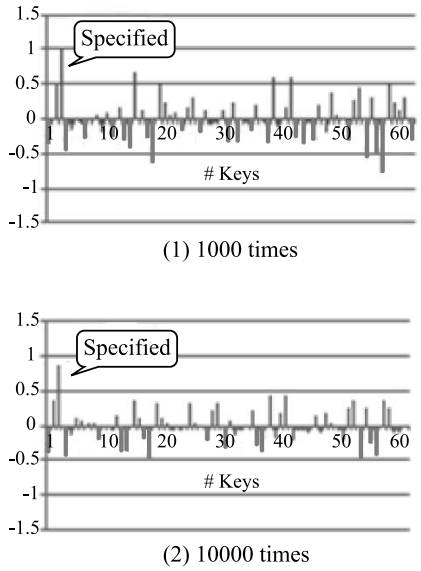

Fig.6 Simulation results of a hamming distance-type attack obtained using the proposed simulator

As shown in these figures, similar to the results obtained using an actual device, the accuracy of key estimation became higher as an increase in the number of electricity consumption waveforms in both attack methods. Thus, the proposed simulator could realize not only simulation of a hamming weight-type attack but also that of a hamming distance-type attack.

C. Experiments using an Anti-DPA Circuit

Next, evaluation experiments were conducted using a circuit in which measures against DPA had been taken. As the object, the transformed masking method (TMM)[8], a typical method against DPA, was used. This method against DPA conceals the correlation between the secret key and electricity consumption by using a mask consisting of random numbers for encryption processing. Figures 7 and 8 show the results obtained using hamming weight-type DPA. Figure 7 shows the results when an actual device was used. Figure 8 shows the results when the proposed simulator was used. As shown in these figures, the method against DPA is useful for a hamming weight-type attack in an actual device and the proposed simulator. Regarding this attack, results similar to those obtained using an actual device could be obtained using a conventional method reported in a paper[2].

Figures 9 and 10 show the results obtained using hamming distance-type DPA, which cannot be handled by conventional methods. Figure 9 shows the results when an actual device was used. Figure 10 shows the results when the proposed simulator was used. It was reported that for this attack method, measures against DPA by TMM using a mask consisting of random numbers were useless, and, as a result, the attack succeeded. As shown in Figure 10, similar to an actual device, the attack succeeded when the proposed simulator was used. Thus, similar to an actual device, the operation of a circuit, in which measures against DPA had been taken, could be simulated in the proposed simulator at the algorithm level.

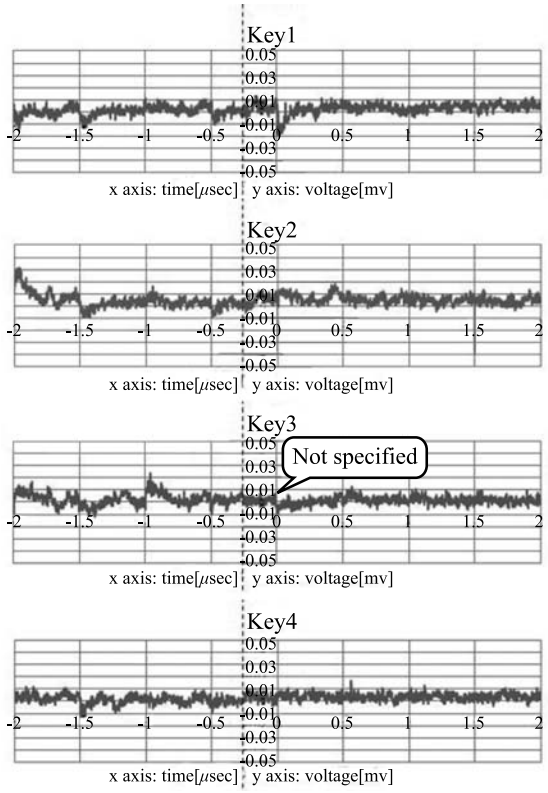

Fig.7 Results of a hamming weight-type attack against an anti-DPA circuit in an actual device

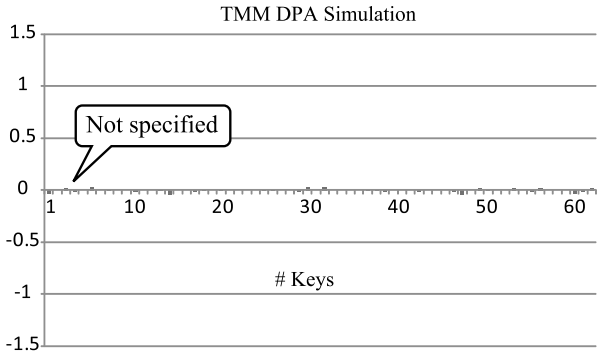

Fig.8 Results of a hamming weight-type attack against an anti-DPA circuit in the proposed simulator

V. CONCLUSION

This study proposed a new software simulator to realize tamper resistance verification at the algorithm level. The proposed simulator could perform DPA simulation corresponding to multiple attack methods that could not be handled by already published simulators. Similar to an actual device, the operation of a circuit in which measures against DPA had been taken could be simulated in the proposed simulator at the algorithm level. By performing DPA simulation at the algorithm level, vulnerability due to the architecture in the cryptography and peripheral circuits can be found in the early stages of designing an algorithm. Consequently, tamper resistance can be improved, and the time required for developing the algorithm can be shortened. Our future task will be DPA simulation, in which signal transmission delay is considered.

ISBN: 978-988-19251-7-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

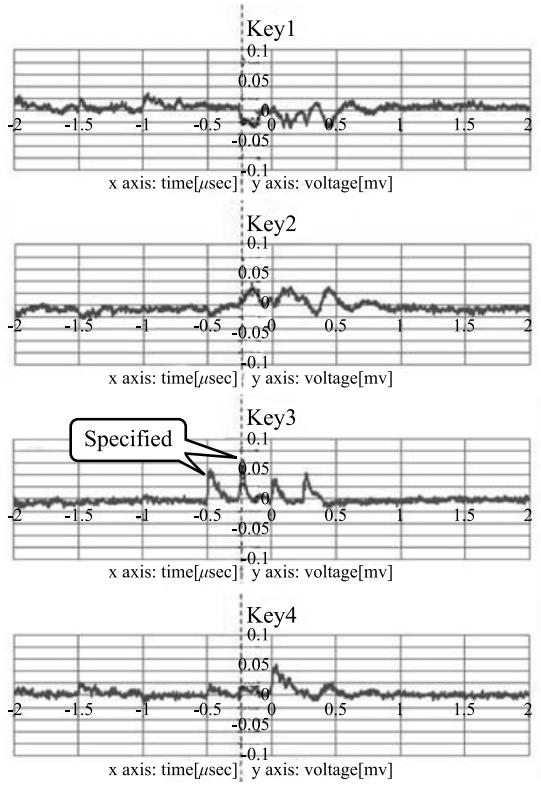

Fig.9 Results of a hamming distance-type attack against an anti-DPA circuit in an actual device

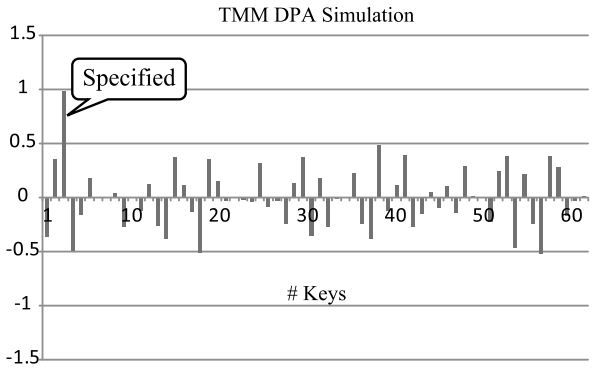

Fig.10 Results of a hamming distance-type attack against an anti-DPA circuit in the proposed simulator

ACKNOWLEDGMENT

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

REFERENCES

[1] P.C.Kocher, J.Jaffe, B.Jun, "Differential Power Analysis", Proc. of International Cryptology Conference'99, pp.388--397, 1999.
[2] A.Sasaki, K.Abe, "Algorithm Level Evaluation of DPA Resistivity against Cryptosystems", IEEJ Transactions on Electronics, Information and Systems, Vol.126, No.10, pp1221--1228, 2006.
[3] M.Saeki, D.Suzuki, T.Ichikawa, "Construction of DPA Leakage Model and Evaluation by Logic Simulation", Technical report of IEICE. ISEC 104(200), 111-118, 2004-07-14, 2004.
[4] A.Miyamoto, N.Homma, T.Aoki, A.Satoh, "An Experimental Comparison of Power Analysis Attacks against RSA Processors on ASIC and FPGA", Proc. of 14th Workshop on Synthesis And System Integration of Mixed Information technologies, pp.58-63, 2009.
[5] K.Kojima, K.Okuyama, K.Iwai, M.Shiozaki, M.Yoshikawa, T.Fujino, "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, pp.169-201, 2010.
[6] Side-channel Attack Standard Evaluation Board (SASEBO) Webpage, http://www.rcis.aist.go.jp/
[7] NIST:Data Encryption Standard, Federal Information Processing Standard (FIPS), Publication 46, 1997.
[8] M.L.Akkar, C.Giraud, "An Implementation of DES and AES, Secure against Some Attacks", Proc. of Workshop on Cryptographic Hardware and Embedded Systems, pp.309-318, 2001.Paul C.Kocher, Joshua Jaffe, Benjamin Jun, “Differential Power Analysis”, Proc. of CRYPTO '99, pp.388-397 1999

ISBN: 978-988-19251-7-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)