Vulnerability Evaluation Method Considering Power Supply Environment for Power Analysis Attacks

Masaya Yoshikawa and Toshiya Asai

***Abstract*—At present, encryption hardware handling confidential information of integrated circuit (IC) cards or the similar are widely available. Confidential information is protected by encryption algorithms, and its safety is computationally secured. However, the problem of power analysis attacks has been actualized. Power analysis attacks acquire confidential information based on information of power consumption leaked from cryptographic circuits that are embedded in hardware. Therefore, when designing cryptographic circuits, resistance against side-channel attacks must be evaluated. The present study proposes a method to verify the resistance including power supply environment. The present study also verifies the validity of the proposed method through several evaluation experiments.**

***Index Terms*—Vulnerability evaluation, Power analysis attack, Cryptographic circuit, Hardware security**

I. Introduction

Along with advancement of information-oriented society, encryption technology for securing safety has been diffused in our society. At present, encryption standards are generally used as encryptions. The safety of encryption standards is confirmed because their decryption is computationally difficult.

The resistance to attacks against encryption processing (tamper resistance) has been positively studied. Since information of keys can be estimated by collecting and statistically analysing secondary information (side-channel information) leaked during encryption hardware operation, such as power consumption and leaked electromagnetic waves, side-channel attacks are particularly risky[1], [2]. Regarding side-channel attacks, many analysis attack methods and countermeasures have been reported [3]-[7]. Power analysis attacks estimate keys using observation data of power consumption. Since power consumption can be easily observed, power analysis attacks are the most dangerous side-channel attacks.

The present study proposes a method to verify the resistance against power analysis attacks. In the proposed method, the operating environment of a substrate, on which large scale integration (LSI) is mounted, is taken into consideration. Using the proposed method, the accuracy of resistance verification can be improved and the safety of encryption hardware can be increased. The validity of the proposed method is verified through several evaluation experiments using the advanced encryption standard (AES), [8].

Manuscript received April 10, 2012; revised May 5, 2012.

The authors are with Meijo university, Japan (e-mail: dpa_cpa@yahoo.co.jp).

II. Proposed Analysis Method Considering Power Supply Noise

In an power consumption simulation of LSI, an ideal power supply without internal impedance is generally assumed. Therefore, the power supply voltage does not fluctuate and the electric current rapidly changes. Side-channel attacks use information, which is secondarily obtained during actual operation of an encryption processing circuit. In the information, various external elements other than LSI-related elements exist. The electric power of an actual device used for power analysis attacks can be obtained only after making LSI on an experimental basis. However, when models for elements of the power supply system on a substrate are created in the design process of LSI and when a simulation is performed together with design data of LSI, the electric power of an actual device can be estimated. To evaluate the final resistance against power analysis attacks, power supply system-related elements, which are observation-related elements, should be involved. An evaluation experiment using a common evaluation platform is considered useful. However, the resistance against power analysis attacks must be estimated using different platforms.

However, a tool to calculate power consumption waveforms used in the gate-level design process cannot satisfy these requests. A simulation to obtain many power waveforms using the simulation program with integrated circuit emphasis (SPICE) together with LSI and a substrate takes an extremely long time and infeasible. In the present study, a model for the power supply line system on a substrate is created, and observation power waveforms during actual operation are estimated within a realistic processing time based on the results of the power consumption simulation of LSI and those obtained using the power supply system-related model. Using the estimated power waveforms, the final attack resistance of an actual device is evaluated.

In the gate-level design process, when design of a substrate and selection of components proceed to some extent, the power supply system-related model for an actual device can be estimated. Fig. 1 shows the proposed method. For power consumption of LSI, power consumption waveforms corresponding to test vectors are to be obtained using a tool of electronic design automation (EDA) vendor.

Next, a power supply system-related model is created. Several methods to create the model exist. In the proposed method, the SPICE is executed using only the power supply system, an approximation model is created using the obtained voltage and current data. For this, SPICE models for components such as L and C in the power supply system must be prepared, and an approximation SPICE model for a substrate must be created after assuming the substrate's rough layout. The creation of the latter model requires certain know-how. Recently, along with the development of high-speed logic devices, verification environment including power planes has been improved. Therefore, the approximation SPICE model can be created in the improved verification environment.

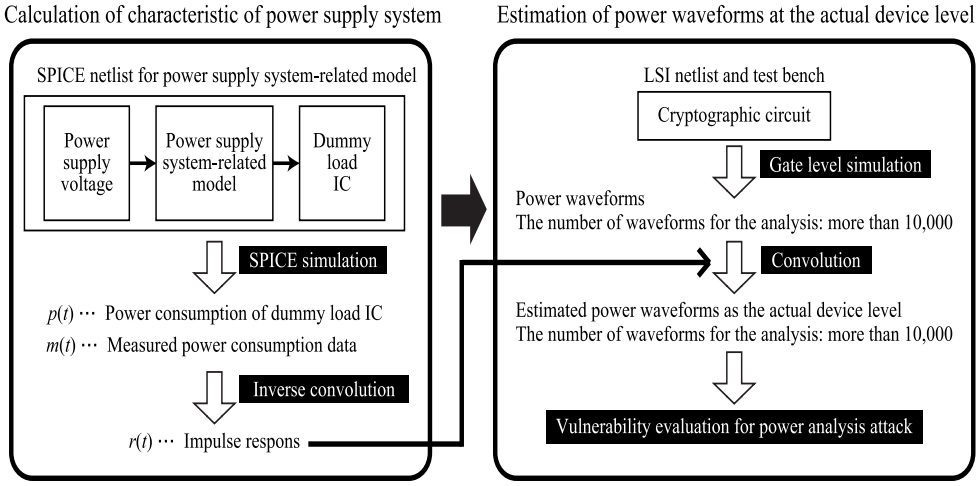

Fig. 1. Proposed analysis method

In the proposed method, a dummy load integrated circuit (IC) is connected instead of encryption LSI to be analysed. For this, a SPICE model for the dummy load IC is prepared. In the proposed method, a standard logic IC is used, by which the SPICE model is available. Models for power supply components and a substrate are created from an ideal power supply. Using the created models, the SPICE netlist for the dummy load IC is created to perform a simulation. The simulation will be satisfied if only one event to generate load fluctuation is involved. Therefore, the processing time required for the simulation is short.

In the simulation, a point to measure the electric power for power analysis attacks in an actual device is predetermined, and data of voltage or current at the point are output simultaneously. After obtaining estimated observation data of power consumption of the dummy load IC and those at the point, the relationship between these two sets of data is calculated.

III. Evaluation Experiment

A. Experiment Outline

The validity of the proposed method was verified by performing several comparison experiments. In the experiments, an AES encryption processing chip with 0.18 um and its design data were used.

To simulate power consumption waveforms, VCS and PrimeTime-PX (Synopsys, Inc., USA) were used. To simulate the power supply system-related model, HSPICE produced by the same company was used. To perform power analysis attacks and correlation analysis, a machine with specifications (CPU: Xeon W3565 3.2 GHz and Memory: 8 GB) was used.

B. Results

An evaluation experiment using estimated power waveforms in a substrate was performed. A dummy load IC (inverter 74HC04) was used instead of encryption LSI, and the response of the substrate was obtained. SPICE models for components in the power supply system (similar components were used in the experiment) were prepared. As a model for the substrate, a simple SPICE model which can be calculated using an electromagnetic field simulator (Sonnet; Sonnet Software Inc., USA) was used. A SPICE simulation of the power supply system was performed using the dummy load IC, and response waveforms of the power supply system were obtained following the procedure described in Section 2.

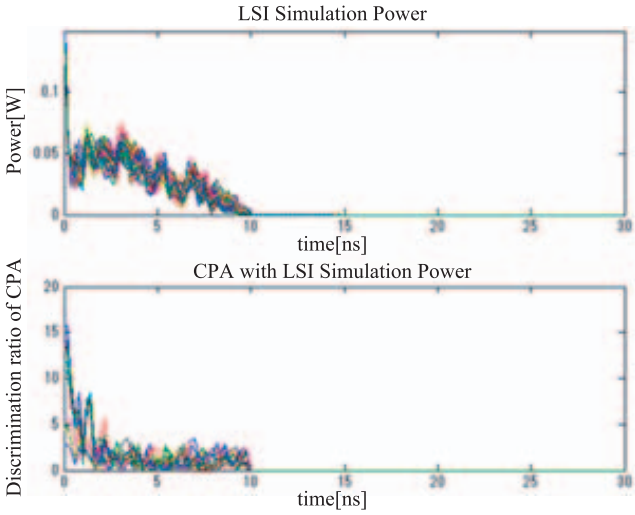

Fig. 2. Simulated power consumption of LSI (the upper part) and the discrimination ratio of CPA (the lower part)

In order to verify the validity of the obtained response waveforms, the obtained estimated power detection waveforms were compared with waveforms actually measured in the experiment, which was obtained by measuring the inter-terminal voltage of current detection resistance in the situation where the dummy load IC was

used instead of encryption LSI. Consequently, the former waveforms were similar to the latter waveforms although a slight error was observed. The accuracy of the comparison was particularly affected by the accuracy of the substrate modeling. Thus, the estimated power consumption waveforms for the encryption LSI on the board were calculated using the power supply system-related model and the simulation power waveforms.

Fig. 2-4 shows the results obtained using the conflation method. Fig. 2 shows the simulated power consumption (the upper part) and the discrimination ratio of CPA (the lower part) obtained using the waveforms. When the CPA discrimination ratio is above three, the possibility of attack success can be considered great.

Fig. 3 shows estimated power consumption and the CPA results. Figure 4 shows a power wave measured using the encryption LSI on the board and the CPA results. The LSI power consumption shown in Figure 2 is steep, and the shape of which differs from that of the estimated power consumption shown in Figure 3 and that of the measured power shown in Figure 4. As shown in the CPA results, although the attack using the LSI power was extremely weak at a certain time, the weak period was short. As shown in Fig. 3 and 4, in the power consumption at the substrate level, the leak of power consumption (confidential information) was temporally extended and its peak was low.

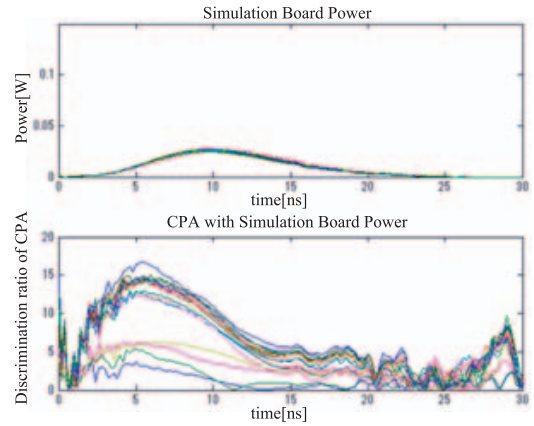

Fig. 3. Estimated power consumption and the CPA results.

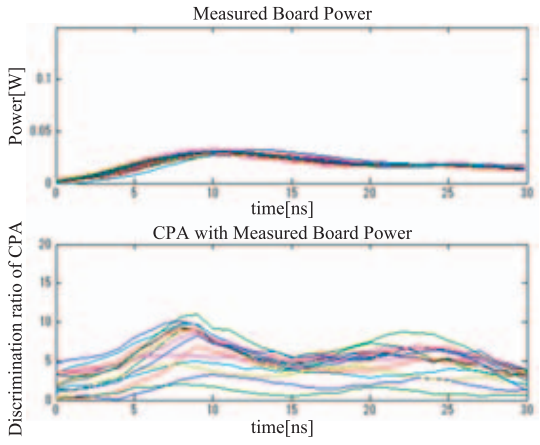

Fig. 4. Power consumption measured using the encryption LSI on the board and the CPA results

When an attackable leak exists, the weak period is prolonged. Therefore, observation becomes easy in some cases. Since power consumption waveforms at the substrate level were affected by other noises, the key estimation was more difficult for the attack using the estimated power consumption shown in Figure 3 than for the attack using the measured power consumption shown in Fig. 4.

As mentioned above, the examination of power consumption waveforms including the power supply system enabled actual verification of the safety against power analysis attacks. The simulation results of LSI power consumption revealed that the processing time required for estimating the power of a substrate was approximately 30 seconds for 30000 waveforms used in the experiment. Even though the time required for preparatory works including model creations is taken into consideration, the proposed method is sufficiently useful.

IV. Conclusion

The present study proposed a method to improve the evaluation accuracy in the resistance verification against power analysis attacks in the gate-level design process of LSI. In the proposed method, power consumption at the actual device level was estimated in the design process. Therefore, the weakness against power analysis attacks could be evaluated at both LSI and actual device levels. Experiments using an AES encryption processing chip verified that the final resistance could be estimated within a short period of time.

In the future, we will improve the accuracy of power supply system-related models, realize high-speed acquisition of power consumption waveforms, and apply the proposed method to electromagnetic analysis attacks.

Acknowledgements

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

References

[1] P. C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Proc. of International Cryptology Conference'99*, pp.388-397, 1999.

[2] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," in *Proc. of Cryptographic Hardware and Embedded Systems 2004*, pp.16-29，2004.

[3] E. Trichina, "Combinational Logic Design for AES SubByte Transformation on Masked Data," *Cryptology ePrint Archive*, pp.2003-236, 2003.

[4] K. Kojima, K. Okuyama, K Iwai, M. Shiozaki, M. Yoshikawa, and T. Fujino, "LSI Implementation Method of DES Cryptographic Circuit Utilizing Domino-RSL Gate Resistant to DPA Attack," in *Proc. of the 16th Workshop on Synthesis And System Integration of Mixed Information Technologies*, pp.169-201, 2010.

[5] H. Shimizu, "A Countermeasure against Side Channel Attack using Mask Logic Elements," *IEICE Technical Report*, vol. 104, no. 315, ISEC2004-69, pp.15-20, 2004.

[6] S. Nikova, C. Rechberger, and V. Rijmen, "Threshold Implementations against Side-Channel Attacks and Glitches," in *Proc .of ICICS2006, LNCS4307,* pp.529-545, 2006.

[7] Z. Chen and P. Schaumont, "Early Feedback on Side-Channel Risks with Accelerated Toggle-Counting," in *Proc. of IEEE Workshop on Hardware Oriented Security and Trust*, pp.90-95, 2009.

[8] NIST, "Advanced Encryption Standard (AES)," FIPS PUB 197, http://csrc.nist.gov/publications/fips/index.html