Development of Evaluation Environment for Physical Attacks against Embedded Devices

Toshihiro Katashita, Akihiko Sasaki, Yohei Hori
Research institute of secure systems, National institute of Advanced Industrial Science and Technology
Tsukuba, Japan

Mitsuru Shiozaki, Takeshi Fujino
Department of VLSI System Design, Ritsumeikan University
Kusatsu, Japan

Abstract—**We developed an experimental environment for testing side-channel attacks against cryptographic LSIs. A side-channel attack is one of the non-invasive physical attacks which exploit measurable physical leakage of the device such as power consumption and electromagnetic radiation. Our evaluation board is carefully designed to measure small fluctuation of power consumption of LSIs. To provide a uniform environment for side-channel testing of LSI, the design data of the developed PCB, control hardware and software are provided on our Web site.. In this paper, the architecture and functionality of the evaluation environment are described in detail, and the performance of the measurement quality and testability are demonstrated with an experimentation of side-channel attacks.**

Keywords-component; Physical attacks; side-channel attacks; evaluation environment; embedded devices; FPGA

I. INTRODUCTION

In the recent embedded devices, cryptography is a essential technology and its algorithm is theoretically evaluated in terms of computational security. However, there exists a different threat against cryptographic devices. Side-channel attack is one of the physical attacks that analyze measurable phenomena of devices such as power consumption and electro-magnetic radiation to extract the internal secret key [1]. In order to provide uniform evaluation environment, we developed SASEBO-RII board especially for measuring side-channel information of LSIs. The board was designed by simplifying the previous SASEBO-R (Side-channel Attack Standard Evaluation Board version R) [2] in order to improve measuring performance and customization flexibility.

In this paper, the details of the experimental environment and characteristics of SASEBO-RII are described. In addition, the measuring performance of the board is demonstrated with the results of the side-channel analysis experimentation.

II. SIDE-CHANNEL ATTACKS AND EXPERIMENTAL ENVIRONMENT

Physical attacks consist of invasive and non-invasive methods. An invasive attack is a powerful method which retrieves the secret usually by destroying a device and directly reading the information inside the device. However, quite expensive instruments and special technique are required to access the internal signals in the device. On the other hand, a non-invasive method exploits measurable physical information of the device or intentionally injects illegal signals to the device without breaking the device. . A side-channel attack is quite low cost attack practical with only fundamental instruments such as a digital oscilloscope and personal computer. Additionally, a side-channel attack leaves no trace of attack, and therefore is considered a significant threat in the consumer electronics.

After Kocher et al. introduced Differential Power Analysis (DPA) [3], lots of attack methods and experimental results have been reported with different environments by different research institutes. However, it is unfair or in the worst case meaningless to compare the experimental results from the different environments. In order to accelerate the research of side-channel attacks by providing a uniform experimental platform, AIST and Tohoku University have developed Side-channel Attack Standard Evaluation Boards (SASEBO)[2].

A. Experimental environment for cryptographic LSIs

In order to explore side-channel information leakage and evaluate countermeasure on practical LSIs, we developed a 65-nm cryptographic LSI and a new SASEBO-RII board. We also constructed an experimental environment as shown in Figure 1.

SASEBO-RII is designed to improve the measuring performance and customization flexibility. To simplify the board structure, the control logic is separately implemented on another board [4] and redundant measurement points are removed. The design data of the board will be provided in our Web site [5] and can be easily applied to other types of LSI

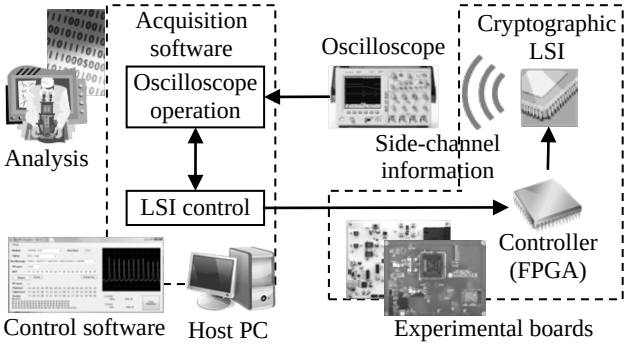

Figure 1. The experimental environment for side-channel attacks

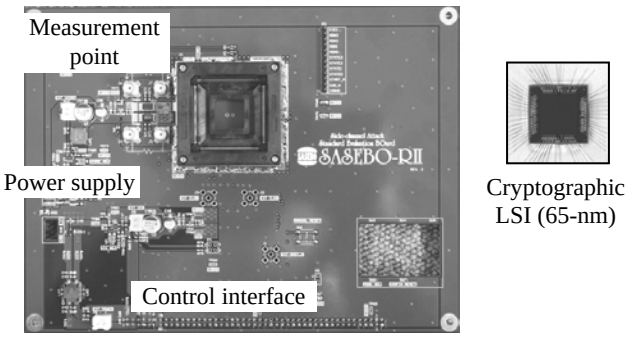

Figure 2. SASEBO-RII and the cryptographic LSI

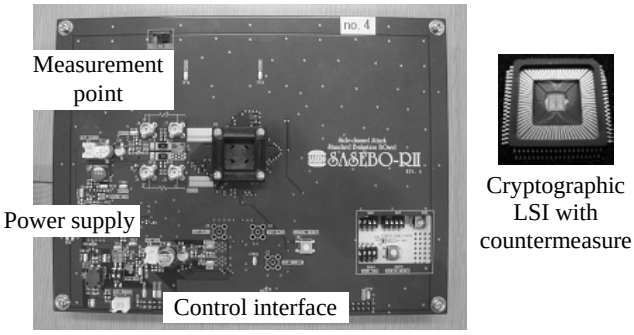

Figure 3. Customized SASEBO-RII and the countermeasure LSI

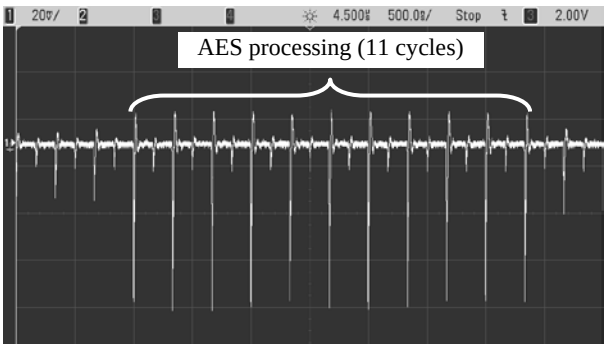

Figure 4. Waveform example of power consumption of the LSI

packages. Figure 3 shows the example use case of the SASEBO-RII design data. The board is developed by customizing the original design data to implement a different LSI socket. We needed such board since the ASICs with attack countermeasures were enclosed in the different packages.

III. EXPERIMENTATION OF SIDE-CHANNEL ANALYSIS

The power consumption of an AES [6] processing on a 65-nm cryptographic LSI was measured and analyzed by Correlation Power Analysis (CPA) [7]. The AES module was operated at 3 MHz and its voltage drops were measured with Agilent DSO 6104A at the resistor inserted on the Vcore line. The waveforms were amplified by Miteq AM-00110 (0.3-1,000 MHz, 28-dB) and processed using 5th-order Bessel low-pass filter (127MHz).

The example waveform is shown in Figure 4. The eleven peaks in the waveform show the voltage drop caused by the AES processing. Figure 5 shows the byte number of the secret sub-keys correctly extracted by CPA. The key length was 128 bits (16 bytes) in this experiment, and therefore the entire key was correctly analyzed by measuring the power consumption of the LSI. As a consequence, SASEBO-RII has advanced performance for measuring and analyzing a 65-nm LSI.

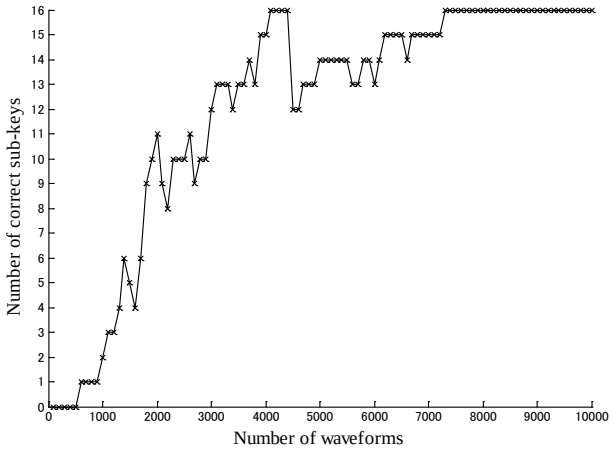

Figure 5. Result of CPA

IV. CONCLUTION

We developed an experimental environment for testing side-channel attack against cryptographic devices. The measuring performance of the environment is also demonstrated with preliminary experimentation of correlation power analysis. As the results show, the cryptographic key embedded in the LSI was successfully extracted by analyzing side-channel information by using the SASEBO-RII board.

As the future work, w will conduct side-channel attack experimentation to other LSIs, and to investigate the mechanism of the side-channel information leakage. We are also planning to analyze and evaluate the LSIs with various attack countermeasures.

REFERENCES

[1] S. Mangard, E. Oswald, and T. Popp: Power Analysis Attacks, Springer Science Business Media, LLC, ISBN 978-0-387-30857-9, 2007.

[2] A. Satoh, T. Katashita, H. Sakane: Secure implementation of cryptographic modules, Sysnthesiology Vol.3 No.1, pp.86-95,2010, http://www.aist.go.jp/aist_e/research_results/publications/synthesiology_e/vol3_no1/vol03_01_p86_p95.pdf

[3] P. C. Kocher, J. Jaffe, B. Jun : Differential Power Analysis, CRYPTO '99, LNCS 1666, pp.388-397, 1999.

[4] T. Katashita, Y. Hori, H. Sakane, A. Satoh: Side-Channel Attack Standard Evaluation Board SASEBO-W for Smartcard Testing, Non-Invasive Attack Testing Workshop (NIAT), 2011,
http://csrc.nist.gov/news_events/non-invasive-attack-testing-workshop/papers/10_Katashita.pdf.

[5] RISEC, AIST: Evaluation Environment for Side-channel Attacks, http://www.risec.aist.go.jp/project/sasebo/

[6] K. Elissa: Title of paper if known, unpublished. FIPS PUB 197, "Advanced Encryption Standard," 2001.
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[7] E. Brier, C. Clavier, and F. Olivier: Correlation Power Analysis with a Leakage Model, *CHES 2004*, LNCS 3156, pp. 16–29, 2004