2022 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI) | 978-1-6654-0929-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/EMCSI39492.2022.9889445

SASIMI: Evaluation Board for EM Information Leakage from Large Scale Cryptographic Circuits

Daisuke Fujimoto, Youngwoo Kim, Yuichi Hayashi
Nara Institute of Science and Technology/JST CREST
Ikoma, Japan
{fujimoto,youngwoo,yu-ichi}@is.naist.jp

Naofumi Homma
Tohoku University/JST CREST
Sendai, Japan
naofumi.homma.c8@tohoku.ac.jp

Masanori Hashimoto, Takashi Sato
Kyoto University
Kyoto, Japan
{hashimoto,takashi}@i.kyoto-u.ac.jp

Jean-Luc Danger
Télécom Paris
Paris, France
jean-luc.danger@telecom-paristech.fr

***Abstract*— In this paper, we propose a common evaluation board(Side-channel Attack Standard IMplementation and evaluatIon board:SASIMI) for the threat of acquiring information leaked from electromagnetic(EM) noise generated by devices. To prevent this threat, it is necessary to implement circuits that do not leak secret information, like a secret key, via EM side-channel, and conduct actual measurement and evaluation environment, which makes it difficult for a third party to reproduce the results. However, since captured EM activity is affected by the surrounding EM noise, the evaluation results may vary depending on the evaluation environment.**

The proposed evaluation board can implement various cryptographic circuits. The IC must be capable of reconfiguring logic and implementing large-scale cryptographic blocks such as post quantum cryptography. To reduce the influence of environmental EM noise, an independent power supply network and measurement port are provided for the IC to be evaluated thus improving the measurement reproducibility.

In order to evaluate the performance of the SASIMI board, this paper proposes an index to evaluate the strength of the information of the secret key contained in the power supply noise. This index is to find the value of the resistance to be inserted into the power supply network of the prototype board. Measurement results show that the simple amplitude value of EM noise and the intensity of information leakage do not necessarily coincide.

***Index Terms*—Common platform, Information leakage, Measurement, Side-channel leakage**

I. Introduction

The problems caused by EM noise in many information devices have been much discussed [1], [2]. When an information device is operating, its current consumption generates electromagnetic (EM) noise. If the EM noise is radiated outside the equipment, it may affect other systems. EM noise generated by the equipment is strictly limited by standards such as FCC [3] and CISPR [4] to ensure that it does not affect other equipment. As a result, the maximum EM noise generated by the equipment is kept at a low level.

This work was supported by JST CREST Grant Number JPMJCR19K5, Japan.

On the other hand, obtaining the secret key from EM noise in cryptographic circuits is done focusing on the variation through processing rather than the peak amplitude [5]. A method to evaluate whether the secret key can be analyzed by statistically processing the variation over tens of thousands of operations is specified in ISO/IEC 19790 [6]. However, there is no standard for the method of measuring the EM noise that is the source of the key analysis. In addition to the EM noise generated by the analyzed device, other noises from external circuits and environmental noises affect the measurement. If the level of these external noises is high, the measurement accuracy of the signal to be evaluated will degrade, which may result in an underestimation of the information leakage.

In the evaluation of EM information leakage from cryptographic circuits, the Side-channel Attack Standard Evaluation BOard (SASEBO) and its successor, the Side-channel AttacK User Reference Architecture (SAKURA), have been proposed as standard evaluation boards [7], [8]. These boards are equipped with Field Programmable Gate Array (FPGA), and various cryptographic circuits can be implemented in the FPGA to evaluate the EM noise generated by its current consumption. However, in the design of the SASEBO, only a dedicated measurement port is provided in the power supply network, and its information acquisition quality has not been considered. In addition, for new ciphers, such as post quantum cryptography and advanced cryptography which requires more than 100 thousand of Look-up tables, the FPGA capacity on the above board is insufficient [9].

The first contribution of this paper is to propose a Side-channel Attack Standard IMplementation and evaluatIon (SASIMI) board as a common evaluation board with a larger capacity FPGA. In this type of FPGA, the EM noise that contains information will decrease compared to the EM noise that does not contain information due to the increase in circuit capacity. Furthermore, as the process shrinks, the dynamic noise generated by the circuitry decreases, reducing the accuracy of the measurement. To maximize the information acquisition from EM noise, it is necessary to design a power

supply that is suitable. In SASIMI, we design the power supply line by simulation at the board level and evaluate it by actual measurement.

The second contribution of this paper is to propose a method to evaluate the information leakage from EM noise. Specifically, we propose an index for separating EM noise which includes information leakage from cryptographic circuits from environmental noise. Then, we evaluate the method on a prototype board using this index.

This paper is organized as follows. In Section 2, we propose a common evaluation board, and describe the index for evaluating the information leakage from EM noise. In Section 3, we present the prototype board called SASIMI and evaluate the effect of the impedance change on the power supply network using the proposed index.

II. Common Evaluation Board for EM Information Leakage from Cryptographic Circuit

In this section, we propose a common board for the evaluation of information leakage through EM noise from cryptographic circuits. The performance evaluation index of signal acquisition of the evaluation board is described.

A. Requirement for Common Evaluation Board

In the cryptographic circuit, the ciphertext is output by processing according to the input data and the secret key. In this process, the current corresponding to the processing is consumed. Therefore, the information of the secret key is included in the current consumption. In the analysis method called power analysis attack, changing the input data, and observing the current consumption allows statistical processing retrieve the secret key [5]. Therefore, the accuracy of the power activity traces impacts the efficiency of the analysis.

The current consumption of the cryptographic circuit is observed as EM noise on the board. Since the EM noise varies depending on the transfer function of the board, it is necessary to control the transfer function for an accurate evaluation. To achieve this, it is necessary to mount ICs that can implement many cryptographic algorithms. Therefore, it is preferable to use FPGAs to make the logic reconfigurable, similar to SAKURA. In addition, as the demand for cryptographic circuits that require a large circuit area, such as post quantum cryptography, is increasing, it is essential to increase the capacity of FPGAs.

In a common evaluation board, it is necessary to be able to acquire EM noise with good reproducibility even if the evaluator is different. In the actual evaluation of cryptographic devices, the mainstream method is to place an EM probe directly above the cryptographic circuit to acquire the EM noise. However, in the method using EM probes, the accuracy of the acquisition varies greatly depending on the positional relationship with the cryptographic circuit, making fair evaluation among different evaluators difficult. Therefore, the evaluation board needs to have a dedicated port on the power supply network to measure the EM noise generated by the current consumption of the cryptographic circuit.

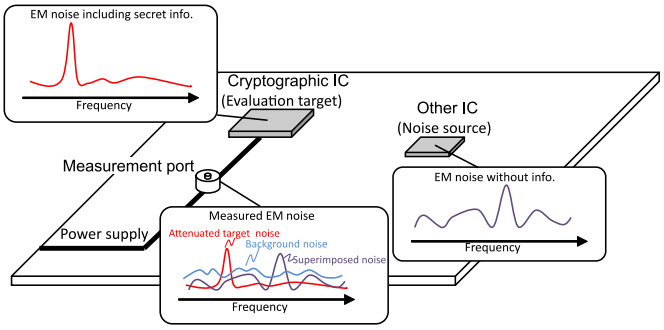

Fig. 1. Image of background noise and noise from other ICs superimposed on the acquisition of EM noise containing secret information from an cryptographic IC.

For secret key analysis, it is important to keep a high quality of acquiring EM noise generated by changes in the internal operation of the cryptographic circuit. Unfortunately the EM noise generated by the cryptographic circuit can be attenuated when it reaches the measurement port. Moreover, EM noise generated by other ICs mounted on the same board and environment noise are superimposed (Fig. 1). Therefore, the evaluation board needs to be designed such that the EM noise including the leaked information from the cryptographic circuit reaches the measurement port with a small attenuation rate and the influence of other ICs and environment noise is mitigated.

In order to design an evaluation board that satisfies these requirements, it is necessary to maximize the strength of the leakage information contained in the EM noise generated by the cryptographic circuit. For this purpose, it is necessary to have an index to evaluate the strength of the leakage information contained in the EM noise generated by the cryptographic circuit from the measured EM noise.

B. Index of Strength Information Leakage through EM noise

The EM noise obtained from the board includes the signal component V_{signal} derived from the operation of the cryptographic circuit and other noise components V_{noise}. The ratio of these components $\frac{V_{signal}}{V_{noise}}$ is the signal to noise ratio [10]. However, the level of the signal of the leakage information contained in the EM noise is not easy to separate because the acquired signal is contaminated with the background noise and other signals.

Therefore, in order to estimate the level of the signal of the leaked information contained in the EM noise, we focus on the maximum switching (Max. Hamming Distance: HD) and the minimum switching (Min. HD) of the values that vary depending on the target process of the target cryptographic circuit. Since the switching affects the current consumption, the difference between the amplitude value V_{highHD} and V_{lowHD} represents the range of current consumption information that can be leaked from the cryptographic circuit(Fig. 2). Therefore, the SNR of the maximum difference (SNR_{diff}) is the leakage index define in Equation (1)

$$Index = SNR_{diff} = \frac{V_{highHD} - V_{lowHD}}{V_{noise}} \quad (1)$$

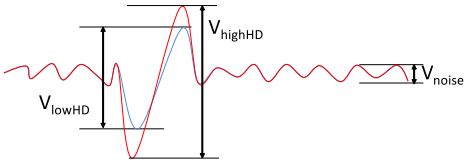

Fig. 2. Signal to noise ratio definition for evaluating leakage from cryptographic circuit using HD variance.

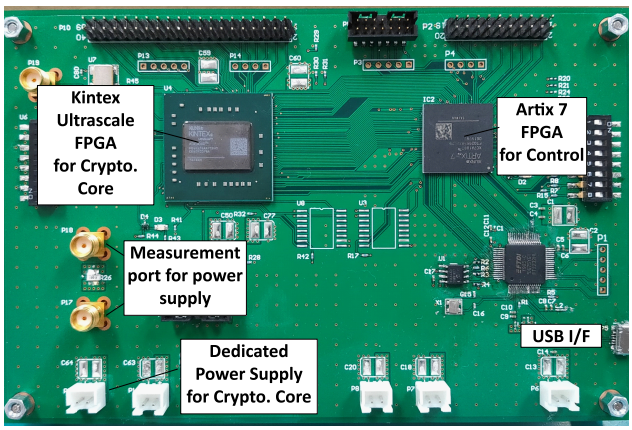

Fig. 3. Prototype board photo.

III. Prototype Evaluation Result

In this section, we show a prototype of a common evaluation board and evaluation using the proposed index.

A. Prototype Board and Measurement set-up

The photo of the prototype board we designed is shown in Fig. 3. The IC (Crypt. Core) for implementing the cryptographic circuit is a Xilinx Kintex Ultrascale XCKU040. The circuit capacity comparison with SASEBO and SAKURA are shown in Table I, which shows that the circuit capacity is more than three times larger than that of the largest SAKURA-X and enough for implementing large-scale QPC shown in [9].

A block diagram of the measurement environment for EM noise from the cryptographic circuit using the prototype board is shown in Fig. 4. 128-bit Advanced Encryption Standard (AES) was selected as the cryptographic algorithm. The power supply of the Crypto. core is connected to the oscilloscope via the SMA port on P18 to observe the voltage fluctuation on the power supply line caused by the current consumption. In

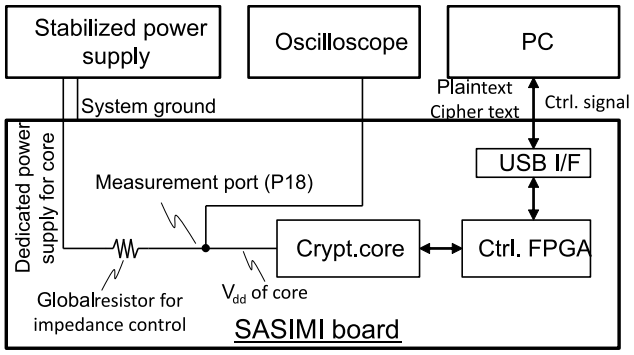

Fig. 4. Block diagram of measurement set-up.

TABLE I
Comparison of FPGA Capacity of Side-channel Evaluation Board

Board name	FPGA	#Slices	#DSPs
SASIMI(this work)	XCKU040 + XC7A100T	641 k	2160
SAKURA-X	XC7K160T + XC6LX45	205 k	658
SAKURA-G	XC6SLX75 + XC6SLX9	83 k	148
SASEBO-W	XC6SLX150	147 k	160

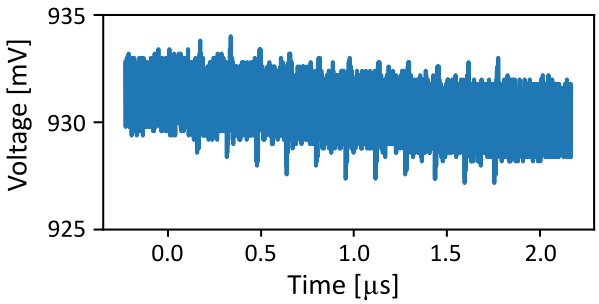

Fig. 5. Time-domain EM noise waveform with decoupling capacitor.

addition, the power supply of the Crypto. Core is connected to a stabilized power supply through a resistor (R26).

The plaintext is sent from the PC to the Crypto Core through the USB Interface, and the encryption result is sent back to the PC. We input data with low and high current consumption in the process under attack in 25 different ways, respectively, and measure their power consumption. In the case of data with low current consumption, only 8 bits out of 128 bits are changed during the processing of the attack target of AES (low HD). For the data with high current consumption, 120 bits out of 128 bits are changed during the processing of the AES attack target round (high HD). From this difference, it is possible to see the difference in switching current of 112 bits, and to estimate the range of the signal part in the EM noise.

On the back side of the board where the FPGA is mounted,12 capacitors of 0.01nF are mounted on the core power supply of the FPGA. When the board is modified by an attacker, the decoupling capacitors may be removed. Since the amplitude of EM noise increases when decoupling capacitors are removed, the most severe condition is expected.

The resistance values of the resistors inserted into the power distribution network (PDN) are 0.001, 0.1, 0.5, 1, 2, 3, and 4 ohms. 5 ohms or more is not suitable for evaluation because the voltage drop is too large to drive the FPGA.

B. Experimental Result

The time waveform of EM noise acquired using the prototype board is shown in Fig. 5. The peaks on the 10 spikes are EM noise generated by the operation of the AES. The level of background noise is high, indicating that the SNR is low in this condition.

To verify the effect of removing the decoupling capacitors, the time waveforms of the EM noise with and without all the decoupling capacitors are compared in Fig. 6. To confirm the change, an enlarged view near the last round which is the attack point is shown. From this result, we can see that

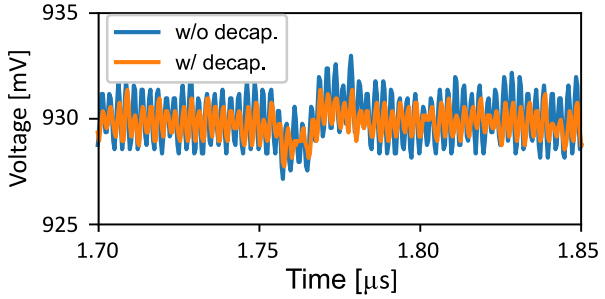

Fig. 6. Change in time domain waveform of EM noise due to removal of decoupling capacitor

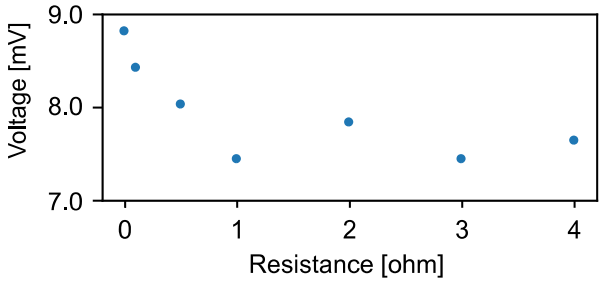

Fig. 7. Change in the amplitude value of EM noise generated by the AES that varies with the change in resistance value of the resistor inserted in the PDN.

the amplitude of the EM noise generated by the current consumption of the AES is increased by removing the decoupling capacitor. On the other hand, the amplitude of the background noise, which is not caused by the operation of the AES, also increases. At this time, SNR_{diff} was 0.30 with the decoupling capacitor and 0.35 without it. This indicates that the increase in amplitude by removing the decoupling capacitor exceeds the background noise and is expected to improve the accuracy of information acquisition in the evaluation.

Next, we show the change in the amount of information leakage depending on the resistance value of the resistor inserted in the power supply network. First, the amplitude of the EM noise from the AES, which varies with the resistance value, is shown in Fig. 7. The same plaintext is used for all the resistance values to perform the measurement. The results show that the amplitude of the EM noise tends to be larger for smaller resistance values. This observation is reasonable since the EM noise is determined by the amount of current, instead of voltage. Therefore, it is expected that a smaller resistance value is more advantageous for evaluating information leakage in the conventional index.

Next, SNR_{diff}, which varies with resistance, is shown in Fig. 8. This result shows that SNR_{diff} does not correspond to the change in amplitude, and is maximum at 0.5 ohms. This is because there is a difference between the frequency of the background noise of the FPGA and the frequency of the EM noise generated by the AES, and the change in the transfer function due to the change in the impedance of the PDN may have caused the difference in SNR. In order to generalize this result, it is necessary to generalize the EM noise caused by the cryptographic circuit to be evaluated.

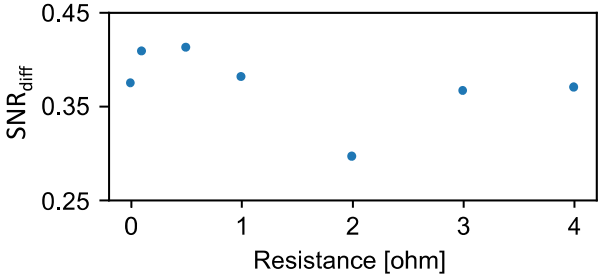

Fig. 8. Change in SNR_{diff} of EM noise generated by the AES that varies with the change in resistance value of the resistor inserted in the PDN.

IV. Conclusion

In this paper, we proposed a common evaluation environment against the threat of acquiring information leaked from EM noise generated by cryptographic circuits. The accuracy of obtaining key information contained in EM noise is affected by ambient EM noise and environmental noise. In order to implement and evaluate various cryptographic circuits on the same board, we have developed a common evaluation board equipped with an FPGA that can reconfigure the logic. We have shown that the evaluation board proposed in this paper is capable of supporting large-scale cryptographic schemes such as post quantum cryptography.

Since it is difficult to evaluate the strength of information leakage through EM noise by amplitude, we proposed an index of leakage strength based on the characteristics of the operation of the cryptographic circuit. Using the proposed index, we evaluated the strength of information leakage by changing the resistance value inserted in the power network of the prototype board. We showed that the amplitude of the EM noise does not necessarily lead to the strength of the information leakage.

References

[1] C. R. Paul, “Introduction to Electromagnetic Compatibility,” Wiley Series in Microwave and Optical Engineering, Wiley-Interscience, 2006.
[2] H.W. Ott, “Electromagnetic Compatibility Engineering,” Wiley, 2009.
[3] Federal Communications Commission,“FCC Part 15 Subpart B”
[4] CISPR, “CISPR 22 Radiated and Conducted EMI Limits”
[5] E. Brier, C. Clavier, F. Olivier, “Correlation Power Analysis with a Lekage Model,” in CHES 2004, LNCS 3156, pp. 16-29, 2004.
[6] ISO/IEC 19790, “Information technology - Security techniques - Security requirements for cryptographic modules”
[7] AIST, “SASEBO:Side-Channel Standard Evaluation BOard,” https://satoh.cs.uec.ac.jp/SASEBO/en/
[8] UEC, “SAKURA:Side-channel AttacK User Reference Architecture,” https://satoh.cs.uec.ac.jp/SAKURA/
[9] F. Turan, S. S. Roy and I. Verbauwhede, “HEAWS: An Accelerator for Homomorphic Encryption on the Amazon AWS FPGA,” in IEEE Transactions on Computers, vol. 69, no. 8, pp. 1185-1196, 2020.
[10] S. Mangard, E. Oswald, T. Popp,“Power Analysis Attacks: Revealing the Secrets of Smart Cards,” 2007.