2023 IEEE Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMC+SIPI) | 979-8-3503-0976-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/EMCSIPI50001.2023.10241643

# Experimental Investigation of Side-Channel Information Leakage from Printed Circuit Board with Split Ground Planes

Kengo Iokibe
*Faculty of Environmental, Life, Natural Science and Technology*
*Okayama University*
Okayama, Japan
iokibe@okayama-u.ac.jp

Kohei Shimoda
*Graduate School of Natural Science and Technology*
*Okayama University*
Okayama, Japan
plku940y@s.okayama-u.ac.jp

Masaki Himuro
*Graduate School of Environmental, Life, Natural Science and Technology*
*Okayama University*
Okayama, Japan
pw9e5u6l@s.okayama-u.ac.jp

Yoshitaka Toyota
*Faculty of Environmental, Life, Natural Science and Technology*
*Okayama University*
Okayama, Japan
toyota@okayama-u.ac.jp

***Abstract*— Side-channel attacks, which break encryption by analyzing the physical behavior leaked from cryptographic devices, have become information security threats. This paper experimentally studied a standard evaluation board for side-channel attacks, SASEBO-G, and identified the source of side-channel information leakage superimposed on the common-mode (CM) current. Regarding the source of the CM current, we examined the effects of split ground planes for cryptographic and control FPGAs and an imbalance difference between SASEBO-G and power cables. We observed CM currents flowing through the cables. The correlation power analysis was performed by changing the separation of the ground plane and the amount of mode conversion caused by the imbalance difference. As a result, the CM current and information leakage intensity varied significantly depending on the ground plane separation. The ground separation on SASEBO-G is a potential cause of side-channel information leakage superimposed on the CM current.**

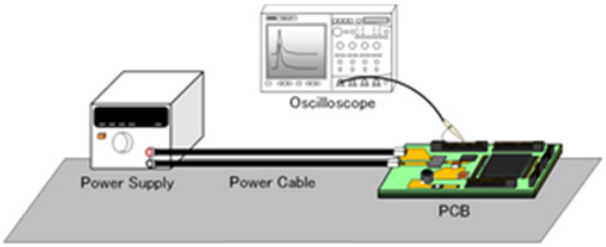
***Keywords—side-channel attack, information leakage, split-ground plane, AES, CPA***

## I. Introduction

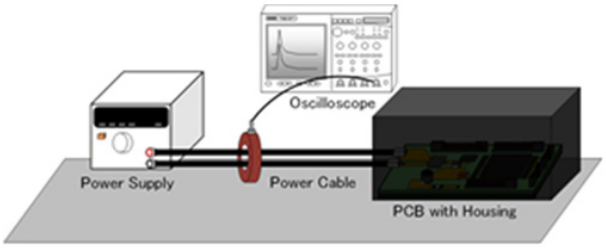
For electromagnetic compatibility (EMC), signal integrity (SI), and power integrity (PI), the ground plane of a printed circuit board (PCB) should be a solid plane and not split by slits [1][2]. In split ground planes, a portion of the transmitted signal leaks out of the transmission line structure due to slits in the return plane of the transmission line. As a result, the radiated emission increases.

However, a PCB may have separated ground planes between noisy and low-noise circuits, such as digital and analog circuits. In automotive electronic control units (ECUs), high-voltage and low-voltage circuits often have different ground planes. A potential difference can occur between the separated ground planes and high- and low-voltage circuits at high frequencies. When cables are connected to each of the two ground planes or each of the high- and low-voltage circuits, the common-mode (CM) potential difference between the planes or the two circuits causes CM currents.

Because information security is required in the Internet of Things (IoT) era, various products have implemented cryptographic functions. At the same time, the threat of side-channel attacks (SCAs) against cryptographic hardware is also known [3]. The simultaneous switching noise generated when cryptographic operations are performed in a digital integrated circuit (IC) can be observed and analyzed statistically or by machine learning to decipher the cryptography. Supposing the side-channel information of the cryptographic circuit is superimposed on the CM current flowing in the cable or harness, an attacker can eavesdrop on the information more easily than by directly making contact with the cryptographic hardware. This can be an information security threat to IoT devices and in-vehicle devices.




(a) On PCB




(b) By cables

Fig. 1. Scenarios of side-channel attack.

In this paper, we experimentally verify the threat of side-channel information leakage due to split ground planes. We implemented a cryptographic function on a PCB with split ground planes. We experimentally examine that side-channel information is superimposed on the CM current flowing through the power cable for the PCB.

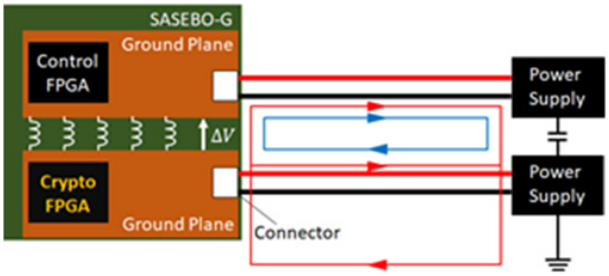
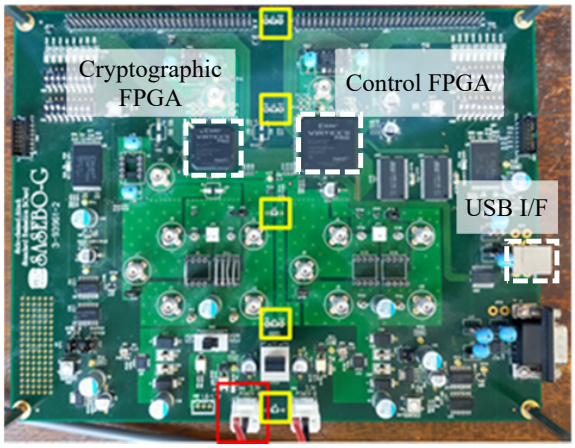
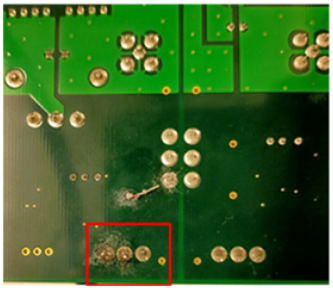



Fig. 2. Common-mode current loops of PCB with split ground planes.




(a) Top view highlighting FPGAs, USB 1.1 connector, ferrite beads in yellow, and power supplying connector for cryptographic FPGA in red.



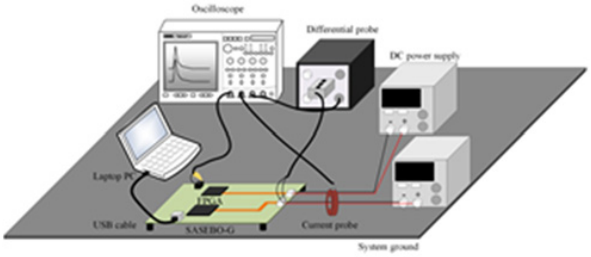
(b) Enlarged view around power supplying connector in bottom layer

Fig. 3. SASEBO-G

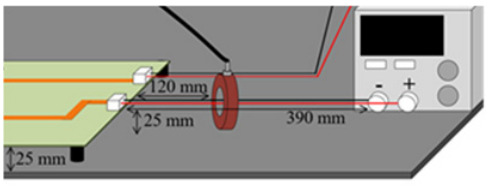
## II. Side-Channel Leakage with Cable Common-Mode Current

### A. Threat of SC Leakage in Common Mode

Side-channel information leakage due to CM currents is a threat because attacks are possible even if the attacker cannot make contact with the PCB. An enclosure often covers the PCB implementing cryptographic modules in actual products, so it is not easy for an attacker to access the board and observe the IC switching current and the conducted emissions on the board, as shown in Fig. 1(a). On the other hand, as shown in Fig. 1(b), the cables that supply power to the cryptographic processing board are often exposed, so it is assumed that it is easy to access them from outside the chassis. In other words, side-channel information leakage superimposed on the CM current may pose a more significant threat than if the leakage traces are acquired on or near the PCB.




(a) Whole view




(b) Close-up view around cables

Fig. 4. Experimental setup.

### B. Side-Channel Information Leakage in Common Mode by Split Ground Planes

Consider a system in which the power supply and the board are connected by a power cable. As shown in Fig. 2, if the ground plane for the cryptographic IC is separated from the ground planes for other circuits, a voltage potential difference can occur between the separated ground planes. This potential difference serves as a CM excitation source and generates CM currents if the two power cables are connected to the same power supply (PS), if they are connected to different PSs coupled with each other at a high frequency, or if the two PSs have the common ground. CM current flows through the circuit integrating the cables and PSs.

The IC implementing the cryptographic circuit generates switching noise as it runs cryptographic operations [4]. This noise contains the secret key information used in the cryptographic operation and leaks to the power supply circuits [5]. The noise causes a potential difference between the separated ground planes. It generates a CM current, resulting in the leakage of secret key information that can be observed in the CM current flowing through the power cable. In contrast, no potential difference between the ground planes as a source of excitation is generated when the ground planes are not separated. Thus, side-channel information leakage from the CM current flowing through the power cable is suppressed.

## III. Experimental Configuration

### A. Printed Circuit Board under Test

SASEBO-G is a side-channel-attack resistance evaluation board developed in the Side-channel Attack Standard Evaluation Board (SASEBO) project [6]. SASEBO-G contains two field programmable gate arrays (FPGAs), one for controlling cryptographic operations (control FPGA) and one for executing cryptographic operations (cryptographic FPGA). The cryptographic FPGA encrypts plaintexts sent from a laptop PC via the control FPGA using the USB 1.1 interface. Encrypted data, in other words, ciphertexts, are sent back to the laptop PC. The Advanced Encryption Standard (AES)

algorithm [7] is implemented in the cryptographic FPGA and processed with a 128-bit key of $(2B\ 7E\ 15\ 16\ 28\ AE\ D2\ A6\ AB\ F7\ 15\ 88\ 09\ CF\ 4F\ 3C)_{16}$ in this study. The AES operation is synchronized to a clock signal of 12 MHz. Fig. 3 shows a photo of SASEBO-G.

The power distribution networks (PDNs) of the two FPGAs are independent. They consist of voltage regulators and decoupling capacitors, respectively. The ground planes of the PDNs are structurally separated by a slit in the PCB trace layout. Still, the two ground planes are electrically connected by five ferrite beads (BLM18AG102SN1, Murata). The beads are mounted at locations indicated with yellow rectangles in Fig. 3(a). The impedance of the beads is 550 Ω at 12 MHz, the clock frequency of the FPGAs that execute the cryptographic operation.

Significant impedance between two ground planes may induce CM and cause side-channel information leakage. Previous studies [8][9][10] have demonstrated side-channel attacks that successfully eavesdropped on side-channel leakage by observing the CM current, breaking the cryptographic key of AES-128.

In SASEBO-G, the potential difference between the two ground planes can be reduced by replacing the ferrite beads with 0-Ω resistors or short bars. This paper examines information leakage suppression achieved by short-circuiting the ground planes.

TABLE I. EXPERIMENTAL EQUIPMENT

| Equipment | Specifications |
|---|---|
| Oscilloscope | EXR104A, KEYSIGHT;<br>Bandwidth: 1 GHz<br>Sampling: 16 GSa/s<br>Resolution: 10 bit |
| Current probe | 94111-1L, ETS-Lindgren<br>Bandwidth: 20 Hz to 1 GHz |
| Differential probe | P6247, Tektronix<br>Bandwidth: 1 GHz |
| DC power supply 1<br>DC power supply 2 | PW18-2, KENWOOD<br>PW18-1.8AQ, KENWOOD |

### *B. Experimental Setup and Conditions*

We used the measurement system in Fig. 4 to evaluate side-channel information leakage superimposed on CM currents. The system was placed on a metal plate that served as the system ground. The power cables for the cryptographic and control FPGAs were connected to separate DC power supplies. The two DC power supplies were placed close

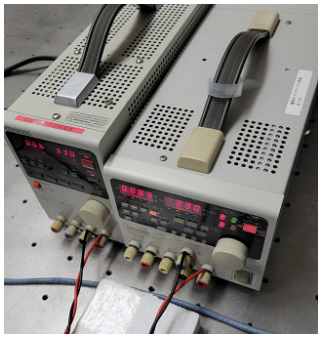
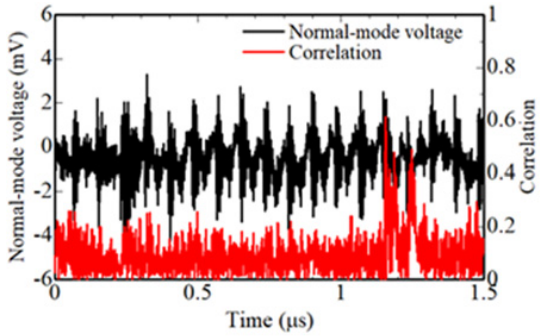
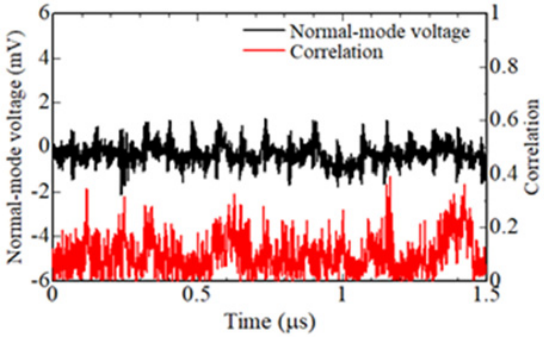


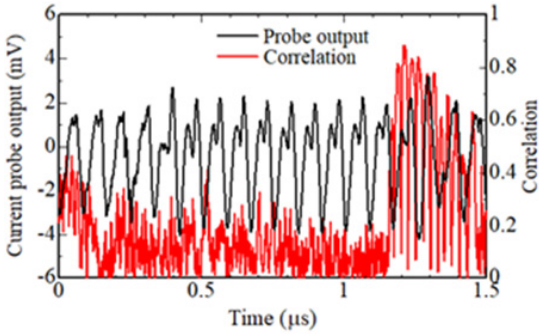
Fig. 5. Two DC power supplies placed close together.



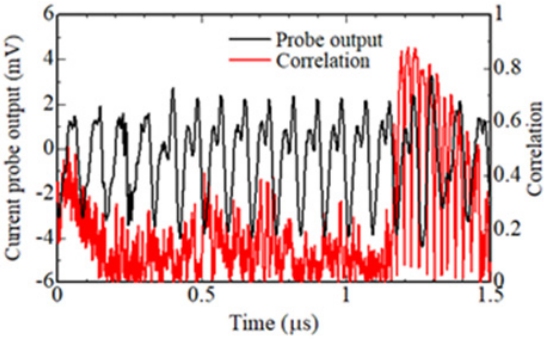

(a) DM voltage without capacitors




(b) DM voltage with capacitors

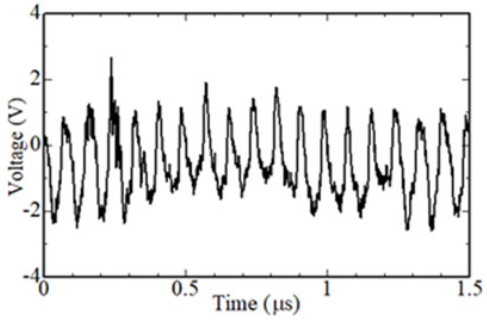



(c) CM current without capacitors

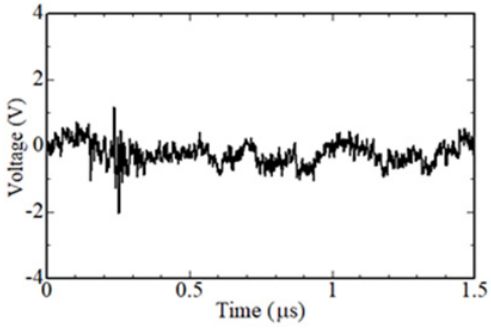



(d) CM current with capacitors

Fig. 6. Side-channel traces and correlation profiles measured with and without capacitor installed at connector.

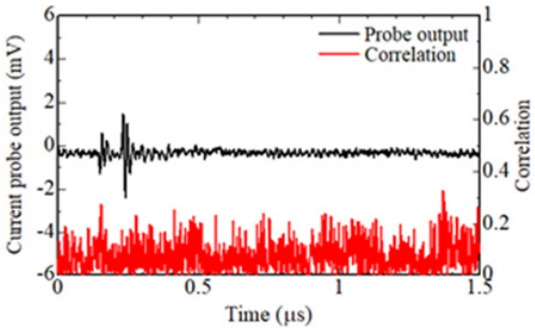



(a) Split with ferrite beads

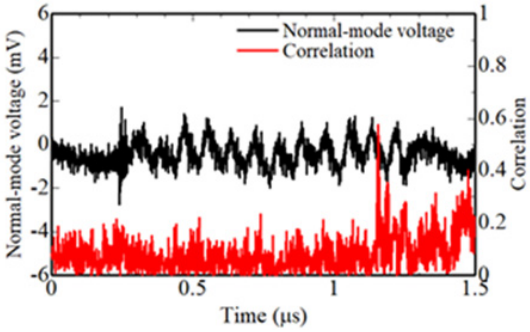



(b) Short-circuited

Fig. 7. Measured voltage difference between separated ground planes.




(a) CM current




(b) DM voltage

Fig. 8. Side-channel traces when short-circuiting two ground planes.

together, as shown in Fig. 5, and were capacitively coupled at high frequencies. In fact, we have experienced that placing DC power supplies close together increases side-channel information leakage from cryptographic circuits driven by clocks above several MHz. The distance between the board and the system ground and the height of the power supply cables were 25 mm, and the length of the cables was 390 mm. The CM current was measured by placing a clamp-type current probe on the power cable of the cryptographic FPGA. The current probe was placed 120 mm from the power connector on the board. The DM voltage was measured on the PDN of the cryptographic FPGA using a differential probe between the power and ground terminals at the connector. Table I lists the instruments used in our experiment.

The following procedure was used to observe the CM currents generated by ground plane splitting and to confirm the occurrence of side-channel information leakage. First, the CM current $I_c$ was measured at the power cable for the case where ferrite beads were used for connection and the case where the two ground planes were short-circuited. The SCA results obtained using the measured $I_c$ confirmed an information-leakage suppression effect from short-circuiting the ground planes. The correlation power analysis (CPA)[11] was used as the side-channel analysis method in this work. CPA is a major and one of the most powerful side-channel analysis methods. As explained in Appendix A, it calculates the correlation coefficient between the observed physical behavior, $V_n$ and $I_c$, and the leakage model transformed from the intermediate values of the estimated cryptographic process. The magnitude of the correlation coefficient is one measure of side-channel information leakage strength.

Next, we measured the differential mode (DM) $V_n$ at the connector for the cable that supplies power to the cryptographic FPGA. We also measured the CM current $I_c$ of the power cable during cryptographic operation using the measurement system shown in Fig. 4. After that, we shortened the ferrite beads and measured $V_n$ and $I_c$ similarly.

We also investigated the contribution of another type of CM current generated at the connector for supplying DC bias to the cryptographic FPGA. The imbalance difference at the connector between the PDN of the PCB and the cable can cause mode conversion, generating a CM current. We measured $V_n$ and $I_c$ in two connector configurations: with and without a decoupling capacitor of 0.01 μF across the power and ground pins of the connector, as shown in Fig. 3(b), since capacitor installation at locations with an imbalance difference mitigates mode conversion [12]. The capacitor was capacitive at the clock frequency. The capacitor impedance was nearly minimal in the frequency band from the clock fundamental to the lower harmonics, where the side-channel information leaks a lot.

The measured $V_n$ and $I_c$ traces were analyzed by CPA. For the CPA, a set of selected plaintexts [13] with a significant variance in terms of Hamming Distance (HD) was used to make it easy to confirm the change in correlation coefficient depending on the measurement conditions. $V_n$ and $I_c$ traces were averaged 20 times for each plaintext to reduce measurement noise in the traces. From the CPA results obtained using $V_n$, $I_c$, and $V_c$ with and without capacitors, we confirmed that reducing the DM suppresses information leakage from the CM current.

## IV. Results

The results of measuring $V_n$ with and without capacitors mounted are shown in Fig. 6(a) and Fig. 6(b), and those for $I_c$ are shown in Fig. 6(c) and Fig. 6(d). The output voltage of the

current probe was not converted into the dimension of Ampere; the vertical axis means the probe output voltage. The waveforms of $V_n$ and $I_c$ showed 12 oscillations in 1 µs. In other words, they oscillated at 12 MHz, the same as the clock frequency. The oscillation amplitude was damped for $V_n$ by adding the 0.01-µF capacitor at the power connector. On the other hand, no change was observed for $I_c$. The maximum value of the correlation coefficient was 0.89 when no capacitor was mounted and 0.88 when a capacitor was mounted. The capacitor at the connector did not reduce the side-channel information leakage in the CM current.

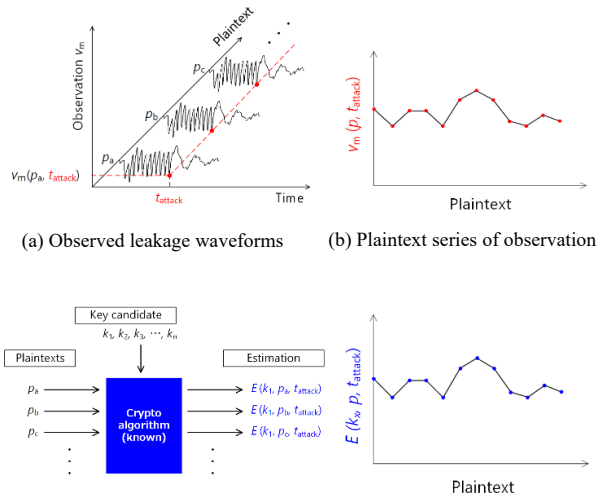
The CM potential differences between the ground planes before and after the two ground planes were shorted are shown in Fig. 7. The CM current and DM voltage traces were measured after short-circuiting the ferrite beads to eliminate the voltage difference between the two ground planes, as shown in Fig. 8. Measured traces of $I_c$ and $V_n$ were analyzed on the basis of CPA to obtain profiles of the correlation coefficients plotted in Fig. 8 also. When the two ground planes were short-circuited, there was no oscillation of the clock cycle compared with the case where they were connected with ferrite beads. In other words, the switching noise generated by the clock synchronization cryptographic operation was sufficiently suppressed. In addition, the amplitude of the CM current was greatly reduced, and the correlation coefficient was also greatly reduced when comparing Fig. 6(c) and Fig. 6(d) with Fig. 7(a).

Those measurement results show that short-circuiting the separated ground planes reduced the voltage potential difference between them compared with the case where ferrite beads connected them. Information leakage from the CM current was also suppressed. Therefore, the CM current generated by the ground plane split is a potential carrier of side-channel information leakage.

In this experiment, the capacitor installation attenuated the DM voltage at the power-supplying connector, as shown in Figs. 6(a) and 6(b). The correlation coefficient was also reduced by mounting a capacitor on the connector. However, the CM current was not attenuated, and the correlation coefficient did not change in the CM current, as shown in Figs. 6(c) and 6(d). These observations mean that the contribution of mode conversion at the connector to side-channel information leakage superimposed on the CM current was small in the system configuration of this work.

## V. Conclusion

This paper experimentally verified the mechanism of side-channel information leakage superimposed on CM currents from SASEBO-G. We attempted to suppress the leakage by reducing the amount of mode conversion in the power supply circuit and short-circuiting the two ground planes. First, the principle of information leakage caused by the potential difference between the two ground planes and their countermeasures was presented. Then, leakage waveform measurements and CPA results were given for the case where the two ground planes were short-circuited on SASEBO-G. The experiments showed that reducing the potential difference between the two ground planes significantly reduced the information leakage superimposed on the CM current. These results confirm that side-channel information leakage superimposed on the CM current is caused by the potential difference between the separated ground planes in SASEBO-G. This case study suggests that side-channel information can leak by being superimposed on CM currents when cables are connected to each of the separated board ground planes. It also means that the ground plane in a PCB should not be split to suppress side-channel information leakage.




(a) Observed leakage waveforms (b) Plaintext series of observation

(c) Estimation of intermediate values (d) Plaintext series of estimation

Fig. A1 Overview of side-channel attack.


## Acknowledgment

This work was supported by 19H04110 and 23K11102.


## Appendix

### A. Brief Introduction of Side-Channel Attack

A side-channel attack is a method of cryptoanalytic analysis introduced in [3]. It targets hardware implementing cryptographic functions to observe the physical behavior of cryptographic hardware, such as conducted and radiated electromagnetic emissions, voltage fluctuations in the power supply networks of ICs, sounds, and heat variations around the ICs. In an SCA, attackers observe temporal variations in physical behavior and collect them while their target hardware encrypts or decrypts multiple data.

Fig. A1(a) illustrates the attackers' observation during a side-channel attack. They first collect temporal profiles $V_m$ for numerous plaintexts, $p_a$, $p_b$, $p_c$, … Next, they focus on a specific sample point, $t_{attack}$, when their targeting sub-operation in the cryptographic operation is executed, obtain the sampled value, $V_m(p_a, t_{attack})$, and then repeat for every observed trace. The obtained values are arranged in plaintext order, yielding a plaintext series of observed values, $V_m(p, t_{attack})$, as shown in Fig. A1(b).

Fig. A1(c) illustrates the estimation of side-channel leakage. Supposing the target cryptographic algorithm is known, attackers can calculate any intermediate values in the cryptographic operation for an arbitrary pair of plaintext and key. This means that they can obtain all intermediate values in their targeting sub-operation for the same plaintexts in their observation. The values can be transformed into a leakage model that correlates with the physical behaviors observed in the side-channel attack. The Hamming distance (HD) and Hamming weight (HW) models are common leakage models. Attackers obtain the plaintext series of their estimations $E(k_i,$

$p$, $t_{attack}$) for every key candidate $k_i$ ($i$=1, 2, …, $N$), as shown in Fig. A1(d), where $N$ is the number of plaintexts that the attackers try.

The measured plaintext series profile $V_m(p, t_{attack})$ correlates with the estimated one $E(k_i, p, t_{attack})$ for all the key candidates. Supposing they find a correlation coefficient that is significantly larger than the others, the assumed key candidate that gave that correlation coefficient is the cryptographic key they want to get.

The correlation coefficient between the observation and estimation is a measure of side-channel information leakage strength. The larger the correlation coefficient, the more clearly the behavior within the cryptographic circuit associated with the cryptographic process is observed. Conversely, a low correlation coefficient makes it more difficult for an attacker to observe the behavior within the cryptographic circuit and requires a high cost for a side-channel attack.

## REFERENCES


[1] B. Hu and K. Y. See, "Impact of Analog/Digital Ground Design on Circuit Functionality and Radiated EMI," 7th Electronic Packaging Technology Conference, Singapore, Dec. 2005.

[2] B. A. Archambeault, "PCB Design for Real-world EMI Control," Kluwer Academic Publishers, Norwell, 2002.

[3] P. C. Kocher, J. M. Jaffe, and B. C Jun, "Differential Power Analysis," CRYPTO '99, vol. 1666, pp. 388397, Springer Verlag, Dec. 1999.

[4] S. Mangard, E. Oswald, and T. Popp, "Power Analysis Attacks: Revealing the Secrets of Smart Cards," Chap. 4, Springer, 2007.

[5] K. Iokibe, T. Amano, K. Okamoto, and Y. Toyota, "Equivalent Circuit Modeling of Cryptographic Integrated Circuit for Information Security Design," IEEE Trans. Electromagn. Compat., pp. 581-588, June 2013.

[6] Side-channel Attack Standard Evaluation Board (SASEBO) project, "https://satoh.cs.uec.ac.jp/SASEBO/en/board/index.html."

[7] Advanced Encryption Standard (AES), NIST FIPS publication 197, Nov. 2001.

[8] Y. Hayashi, T. Sugawara, Y. Kayano, N. Homma, T. Mizuki, A. Satoh, "Evaluation of Information Leakage from Cryptographic Hardware via Common-Mode Current," IEICE Trans., Electronics, vol. E95-C, no. 6, pp. 1089-1097, Jun. 2012.

[9] K. Iokibe, T. Amano, and Y. Toyota, "On-board Decoupling of Cryptographic FPGA to Improve Tolerance to Side-channel Attacks," 2011 IEEE Int. Symp. Electromagn. Compat., pp. 925-930, Long Beach, USA, Aug. 2011.

[10] T. Aoki, S. Minegishi, H. Sone, and H. Inoue, "Information Leakage from a Cryptographic Hardware via Common-Mode Current," Proc. IEEE Symp. EMC, TUE-AM-4-3, pp. 109-114, Fort Lauderdale, USA, July 2010.

[11] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," CHES 2004, Chap. 2, Springer, Berlin, Heidelberg, 2004.

[12] Y. Toyota, S. Mikura, and K. Iokibe, "Suppression of Mode Conversion by Installing Bypass Capacitor to Power Distribution Network," IEEJ Trans. Fundamental and Materials, vol. 136, no. 1, pp. 25-32, 2016. (In Japanese)

[13] H. Shimada, Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, and H. Sone, "Using Selected-plaintext Sets for Efficient Evaluation of EM Information Leakage from Cryptographic Devices," SICE Annual Conf. 2012, Aug. 2012.