IEICE TRANS. COMMUN., VOL.E107–B, NO.12 DECEMBER 2024

INVITED PAPER *Special Section on Emerging Communication Technologies in Conjunction with Main Topics of ICETC 2023*

Identification of Dominant Side-Channel Information Leaking Mechanism Induced by Split Ground Planes

Kengo IOKIBE[†a)], ***Senior Member***, **Kohei SHIMODA**[††], **Masaki HIMURO**[†††b)], ***Student Members***, ***and*** **Yoshitaka TOYOTA**[†c)], ***Senior Member***

SUMMARY This study examines the threat of information leakage when digital ICs, which process sensitive information such as cryptographic operations and handling of personal and confidential information, are mounted on printed circuit boards with split ground (GND) planes. We modeled the mechanism of generating such information leakage and proposed a methodology to control it. It is known that the GND plane of a printed circuit board on which digital integrated circuits are mounted should be solid and undivided to ensure signal integrity, power integrity, and electromagnetic compatibility. However, in actual designs, printed circuit boards may have split GND planes to isolate analog and digital circuits, isolate high-voltage and low-voltage circuits, or integrate multi-function electronic control units. Such split GND planes can increase the risk of electromagnetic information leakage. We, therefore, investigated a side-channel attack standard evaluation board, SASEBO-G, which has been reported to leak cryptographic information superimposed on common-mode currents, known as one of the major causes of electromagnetic emanation. Our experimental results showed that the split GND planes were the dominant cause of common-mode (CM) information leakage. Next, we constructed an equivalent circuit model of the dominant leakage mechanism and confirmed that the behavior of side-channel information leakage superimposed in the simulated CM current was consistent with the measured results. We also confirmed that to mitigate side-channel information leakage in CM caused by the potential difference between the split GND planes, the impedance should be reduced in the information leakage band by connecting the GND planes with capacitors, and the like. In addition, the RF band coupling between cables should be weakened if the cables are connected to the split GND planes.

key words: *side-channel attack, cryptographic hardware, split ground, common mode, equivalent circuit, simulation*

1. Introduction

Security has become an essential function in all electronic systems, including IoT, automobiles, and control systems. Cryptographic functions are utilized as one of the security platforms, and the hardware that performs cryptographic operations is attracting increasing attention as a Root of Trust [1].

One known threat to such cryptographic hardware is the side-channel attack (SCA) [2]–[5]. SCAs observe the physical behavior of hardware during cryptographic operations and analyze it statistically [4] or through deep learning [5] to identify the secret key used in cryptographic operations. When attackers observe the voltage or current on the cryptographic hardware or the electromagnetic field near an integrated circuit (IC) where a cryptographic function is operated, they need to be close to the target. In other words, the attack surface will be very close to the cryptographic hardware.

On the other hand, when observing the common-mode (CM) current flowing through a cable connected to the cryptographic hardware or the electromagnetic field generated by the CM current, the attack surface extends away from the cryptographic hardware, and attackers can make their attack from outside the room or building where the attack target is located. In other words, side-channel information leakage superimposed on the CM current increases the risk of SCAs on cryptographic hardware, which accordingly increases the security threat.

Several studies examining SCAs on cryptographic hardware have focused on the CM current flowing through the power cable of the hardware [6]–[8]. These papers used a current probe to observe the CM current flowing through the power cable of the side-channel attack standard evaluation board (SASEBO-G)) [9], one of the most frequently utilized SCA standard evaluation boards. The observed current waveforms were analyzed by a side-channel analysis method to determine whether the attack succeeded or had the potential to succeed. SASEBO-G mounts two field programmable gate arrays (FPGAs) and separates the power distribution network for each, splitting the power and GND planes by slits. Electromagnetic compatibility (EMC) engineers know that a high-frequency voltage difference is generated between the split ground (GND) planes as digital ICs operate their functions. This voltage difference can excite the cables connected to the split GND planes and generate CM currents. A stable and solid GND plane is essential in an ideal printed circuit board (PCB) design for signal integrity (SI) and EMC [10], [11]. However, it is not uncommon for PCBs in actual products to be designed with split GND planes to separate noisy digital systems from sensitive analog systems or to isolate high-voltage circuits from low-voltage circuits. In automotive applications, there is also a trend toward integrating electronic control units (ECUs) with multiple functions to achieve increasingly complex functions and to reduce the

Manuscript received February 27, 2024.
Manuscript revised June 3, 2024.
Manuscript publicized August 22, 2024.

[†]Faculty of Environmental, Life, Natural Science and Technology, Okayama University, Okayama-shi, 700-8530 Japan.
[††]Graduate School of Natural Science and Technology, Okayama University, Okayama-shi, 700-8530 Japan.
[†††]Graduate School of Environmental, Life, Natural Science and Technology, Okayama University, Okayama-shi, 700-8530 Japan.
a) E-mail: iokibe@okayama-u.ac.jp
b) E-mail: pw9e5u6l@s.okayama-u.ac.jp
c) E-mail: toyota@okayama-u.ac.jp

DOI: 10.23919/transcom.2024CEI0010

number of ECUs and overall weight [12]. In such integrated ECUs, the circuitry can be split for each function, and the GND may also be split. The split GND plane of SASEBO-G can be used to simulate these splits.

The mechanism of side-channel information leakage from SASEBO-G superimposed on the CM current has not yet been clarified. In this paper, we therefore identify the dominant mechanism of CM side-channel information leakage in SASEBO-G. We also represent the leakage mechanism in an equivalent circuit model, propose a method to suppress side-channel information leakage caused by split GND planes, and show that the effect of the method can be predicted by using the equivalent circuit model. This simulation technique can predict the attack success rate when cryptographic hardware is subjected to an SCA. Predicting the attack success rate shows great promise because it can be utilized for security assessment at the system level and even at the product level.

2. Side-Channel Information Leakage Driven by Voltage Difference between Split GND Planes

In this section, we experimentally estimate the dominant mechanism of the CM side-channel information leakage generation from SASEBO-G and model it with equivalent circuits to prepare to simulate split GND planes inducing the leakage (presented later in Sect. 4).

2.1 Experimental Identification of Dominant CM Current Path

As shown in Fig. 1, SASEBO-G is equipped with two field programmable gate arrays (FPGAs), one for cryptographic operation and the other for control, which performs operations other than cryptographic operation. Each of the two FPGAs has a power distribution network (PDN) that supplies the DC bias voltage, and a power cable is connected to each PDN to deliver the DC bias from a DC power supply. Each PDN has its own GND plane; SASEBO-G has split GND planes isolated in radio frequencies (RF) with ferrite beads. In previous studies [6], [7], the CM current flowing through the power cable for the cryptographic FPGA, I_c, was observed, as shown in Fig. 2(a), and cryptographic keys were identified by side-channel analysis.

The CM current is a current that flows through multiple conductors in the same direction. Each power cable of SASEBO-G consists of two wires, 3.3 V and GND, and the CM current flows through these wires in the same direction. According to the circuit theory, the current forms a loop: in other words, I_c has a return path. In the SASEBO-G measurement system, the return path of the CM current can be the power cable for the control FPGA, labeled 'RP1' in Fig. 2(b), and the system GND, labeled 'RP2' in Fig. 2(c).

We observed I_c and other CM currents under the following four conditions to determine which return path is the dominant return path of I_c.

I. I_c and the CM current on RP1, under the conditions in Fig. 2 with the system GND installed (same conditions as in [6], [7])
II. CM current flowing in the same direction across all wires of the two power cables
III. I_c when the system GND has been removed
IV. I_c when the split GND planes have been short-circuited with lead wires

The observed CM currents were subjected to side-channel analysis to detect the side-channel information leakage in the common mode. The measurement equipment we used was the same as in Sect. 3 (described later). We utilized the correlation power analysis (CPA) [4] as the side-channel analysis method, and the information about the SCA scenario

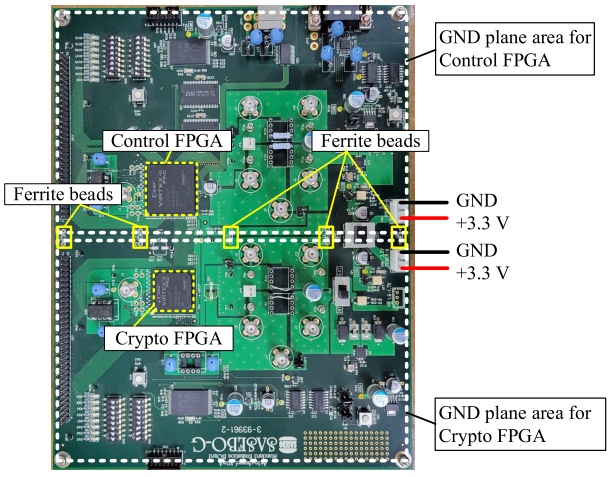
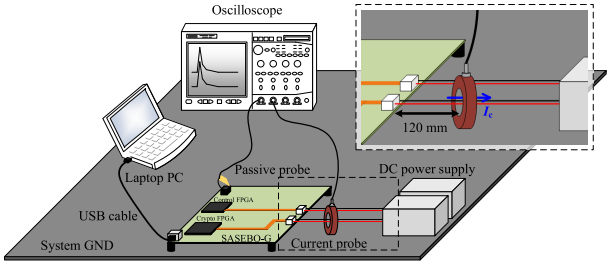
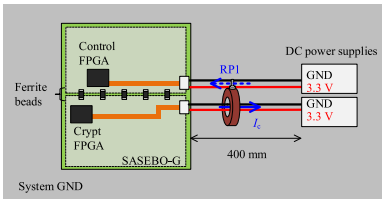


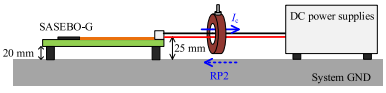
Fig. 1 SASEBO-G has split GND planes isolated in RF with ferrite beads.



(a) Overall bird's-eye view



(b) Top view of SASEBO-G and power supplies



(c) Side view of SASEBO-G and power supplies

Fig. 2 Measurement system for SCA utilizing CM current of SASEBO-G [6], [7].

examined here is also described in Sect. 3.

The acquired current probe output waveforms are shown in Fig. 3. These are probe output voltages and were not converted into a current. The graphs in (a) and (b) (Measurement I) show that the amplitudes of the CM currents flowing through the two cables are comparable. The magnitude of the correlation coefficients was also almost unchanged: the maximum values read (a) 0.48 and (b) 0.51 around 1.2 μs when the target operation in the cryptographic algorithm was executed.

In contrast, in Measurement II (Fig. 3(c)), the CM current flowing in the same direction across the two cables was significantly attenuated relative to the CM currents in Measurement I. The correlation coefficient was also considerably reduced. This result confirms that the dominant return path of the CM current flowing in the power cable for cryptographic FPGA was the power cable for the control FPGA.

Next, we compare Measurements I and III. When the system GND was removed, I_c was slightly increased. The profile of the correlation coefficient also showed a slight change, but its value remained large. From these results, we can confirm that the influence of the system GND was not significant as a return path for I_c.

Finally, the results in Measurement IV (Fig. 3(e)) show that when the split GND planes were short-circuited, the CM current barely flowed, and the correlation coefficient was significantly reduced. This result demonstrates that the potential difference between the GND planes significantly contributes to the CM side-channel information leakage.

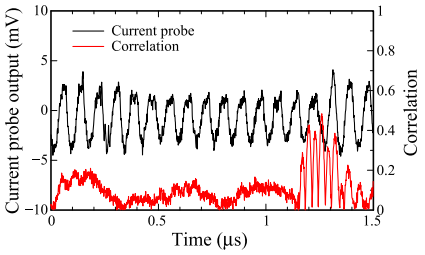
These observations indicate that the dominant return path of I_c was RP1 for SASEBO-G in the experimental setup in Fig. 2, where the contribution of RP2 to I_c was insignificant. Thus, the dominant CM current path was through the two power cables and was terminated by the DC power supplies. The potential difference between the split GND planes is what excited the path and generated the CM current.

2.2 Equivalent Circuit Modeling of CM Side-Channel Leakage

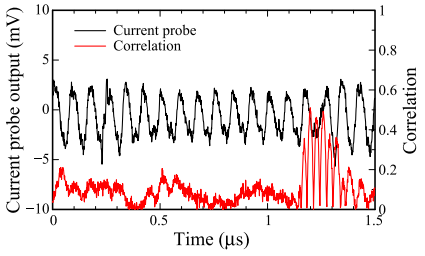
An equivalent circuit of the dominant CM current path in SASEBO-G is depicted in Fig. 4(a). V_s and Z_s represent a Thévenin's equivalent voltage source that generates the potential difference V_{gnds} between the GND planes. Z_{cable} represents the impedance of each of the power cables, and Z_{ps} represents the impedance of the DC power supply section.

The behavior of the CM current shown in Fig. 3 is qualitatively explained by this equivalent circuit. In the equivalent circuit, I_c flowing through the two Z_{cable}s have the same magnitude but an opposite phase. Therefore, the magnitude of the CM currents flowing through these cables changed only a little, as shown in Fig. 3(a) and (b). In contrast, the CM currents flowing through both cables attenuated significantly in Fig. 3(c) because they weakened each other. In Measurement II, as shown in Fig. 4(b), the output of the equivalent voltage source was short-circuited with trivial-impedance leads, $Z \ll 2Z_{cable} + Z_{ps}$, so that I_c was significantly reduced. The contribution of the system GND in Measurement IV is so tiny that this equivalent circuit includes no elements corresponding to the system GND.

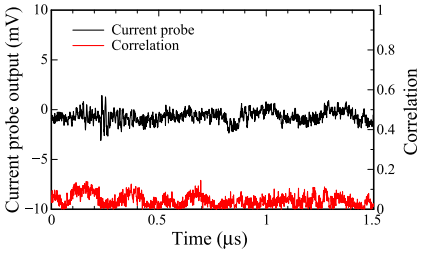
In Sect. 3, we identify all parameters of this equivalent circuit from measurements. In Sect. 4, we utilize the



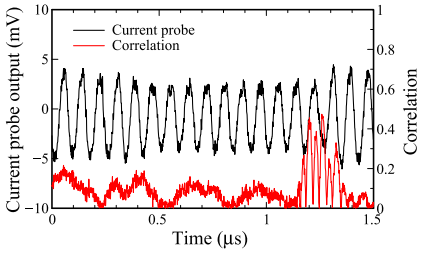
(a) I_c in Measurement I



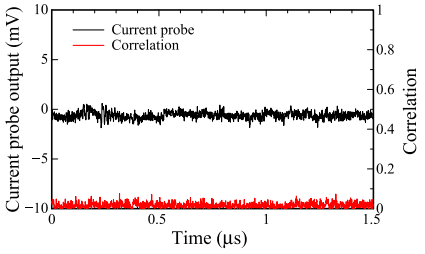
(b) CM current on RP1 in Measurement I



(c) CM current across both cables in Measurement II



(d) I_c in Measurement III



(e) I_c in Measurement IV

Fig. 3 CM current observations and corresponding correlation profiles in Measurements I–IV.

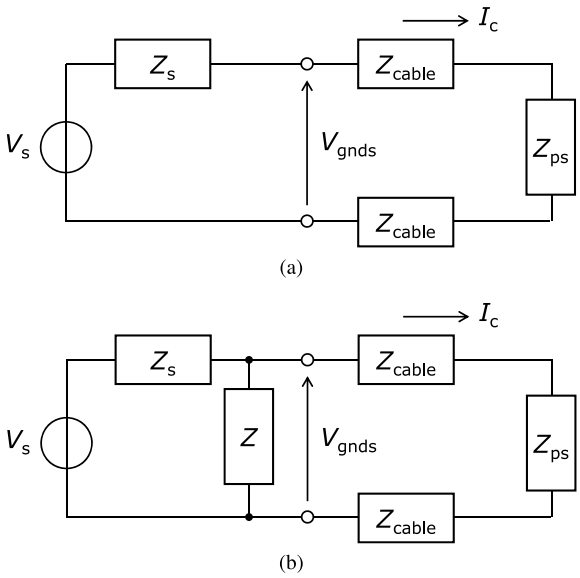


Fig. 4 Equivalent circuit model of dominant CM side-channel leakage path of SASEBO-G.

identified equivalent circuit to simulate the CM side-channel information leakage and determine the validity of the equivalent circuit model by comparing experimental results.

2.3 Expected Outcome of Modeling

Side-channel leakage can be simulated by modeling side-channel leakage mechanisms [13], [14]. Supposing an SCA scenario exploiting the CM current flowing through a cable connected to the cryptographic hardware, we can expect the CM side-channel leakage to be simulated by the equivalent circuit model, as in the previous works. Specifically, it can potentially estimate the success rates of SCAs against cryptographic hardware exploiting the CM current. System-level security assessments require quantitative evaluations of the success rates of assumed attacks on a component-by-component basis. The attack success rate prediction can thus be used in the security assessment of systems that incorporate cryptographic modules.

In addition, knowledge of the SCA countermeasure design can be obtained from the equivalent circuit model. Identifying model parameters that contribute significantly to side-channel information leakage makes it possible to narrow down the areas to focus on in the countermeasure design. In addition, as explained in the previous section, it is also possible to analyze the behavior of the CM side-channel leakage based on the equivalent circuit model.

3. Model Identification

3.1 Experimental Configuration

This section describes the experimental system for SCAs exploiting the CM currents generated by SASEBO-G during the cryptographic operation. The configuration of the experimental system is shown in Fig. 2. SASEBO-G was placed on the system GND with 20-mm plastic spacers. The two SASEBO-G FPGAs were each supplied with the DC bias voltage of 3.3 V using a 400-mm power cable from a DC power supply. The power cables were routed 25 mm above the system GND. A laptop PC was connected to SASEBO-G via a USB cable.

Table 1 Experimental equipment for SCA.

Equipment	Model and specifications
Oscilloscope	EXR104A, Keysight Technologies
Current probe	94111-1L, ETS-Lindgren 20 Hz to 1 GHz
Differential probe	P6247, Tektronix 1 GHz
Passive probe	N2894A, Keysight Technologies
DC power supply	PW18-2, KENWOOD PW18-1.8AQ, KENWOOD

A clamp-type current probe detected the CM current flowing through the power cable. The current probe was located 120 mm from SASEBO-G. The side channel leakage waveform on SASEBO-G was measured in the floating condition using a differential probe. A passive probe detected the trigger signal. Table 1 lists the specifications of the measurement equipment.

3.2 Side-Channel Attack Scenario

We used CPA as the side-channel analysis method in this study. The cryptographic algorithm to be attacked was the advanced encryption standard (AES) [15] with the key length of 128 bits, which was implemented on the cryptographic FPGA encrypting plaintexts at the 12-MHz clock. The target round of AES-128 was the final (10th) round. Hamming distance (HD) between the outputs of the 9th and final rounds was utilized as the leakage model. The secret key of AES was set to 0x2B7E151628AED2A6ABF7158809CF4F3C.

We chose 2000 plaintexts with HDs alternating 36 and 124 and obtained leaked waveforms during encryption operations. Although random plaintexts are utilized in actual SCAs, we opted for the chosen plaintexts here to observe the variation of the leakage waveform and spectrum with the condition of the information leakage path. This is because the leakage increases when using the chosen plaintexts, making observing the variation in leakage strength easier. To obtain the leakage waveform in synchronization with the encryption process, a pulse signal synchronized with the start of the encryption process was output from the cryptographic FPGA to a GPIO port and utilized as the trigger signal.

3.3 Identification of Model Parameters

The equivalent circuit model parameters V_s, Z_s, Z_{cable}, and Z_{ps} were identified by measurement. Z_{ps} was identified for the three configurations shown in Fig. 5, which were later used to verify the identified model parameters in Sect. 4: CLOSE, where two DC power supplies were positioned

Table 2 Experimental equipment for model identification.

Equipment	Model and specifications
Vector network analyzer	EXR104A, KEYSIGHT
Test fixture	16092A, Agilent Technologies

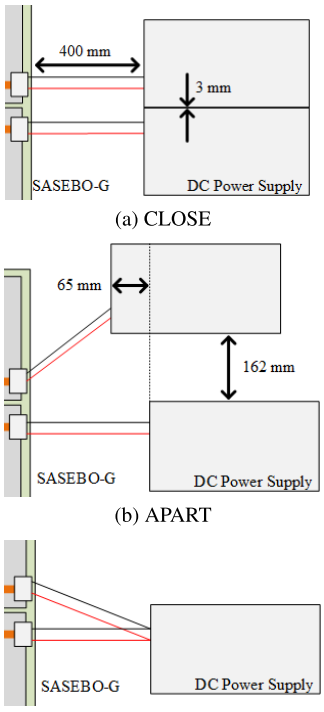


Fig. 5 Placement of DC power supply and connection of power cables.

close together; APART, where they were positioned 162 mm apart; and CONNECTED, where one DC power supply was utilized with two power cables short-circuited at the DC power supply. First, the three impedances were measured using a vector network analyzer (VNA). From the frequency response of the measured impedances, the equivalent circuit was identified below 100 MHz. Since the side-channel leakage of SASEBO-G is contained around the clock frequency driving the FPGA and in the lower frequency band, the upper-frequency limit of the equivalent circuit was set to 100 MHz. The measured impedance includes the effect of lead wires connecting the circuit under test to the VNA. Therefore, the equivalent series inductance (ESL) of the lead wires was removed from the identified equivalent circuit, and the equivalent circuits of Z_s, Z_{cable}, and Z_{ps} were identified.

Z_{cable} was determined by measuring the composite impedance of two power cables and dividing it equally. Lead wires were utilized to connect the EUT to the test fixture. To de-embed the impedance of the lead wire, we also measured the impedance of the lead wire only. The measured impedances are shown in Fig. 6(a). The combined inductance of the power cable and lead wires was 800 nH, while the inductance of the lead wires alone was 200 nH. On the basis of this result, we set the inductance of one power cable to 300 nH. Similarly, the resistive component was identified

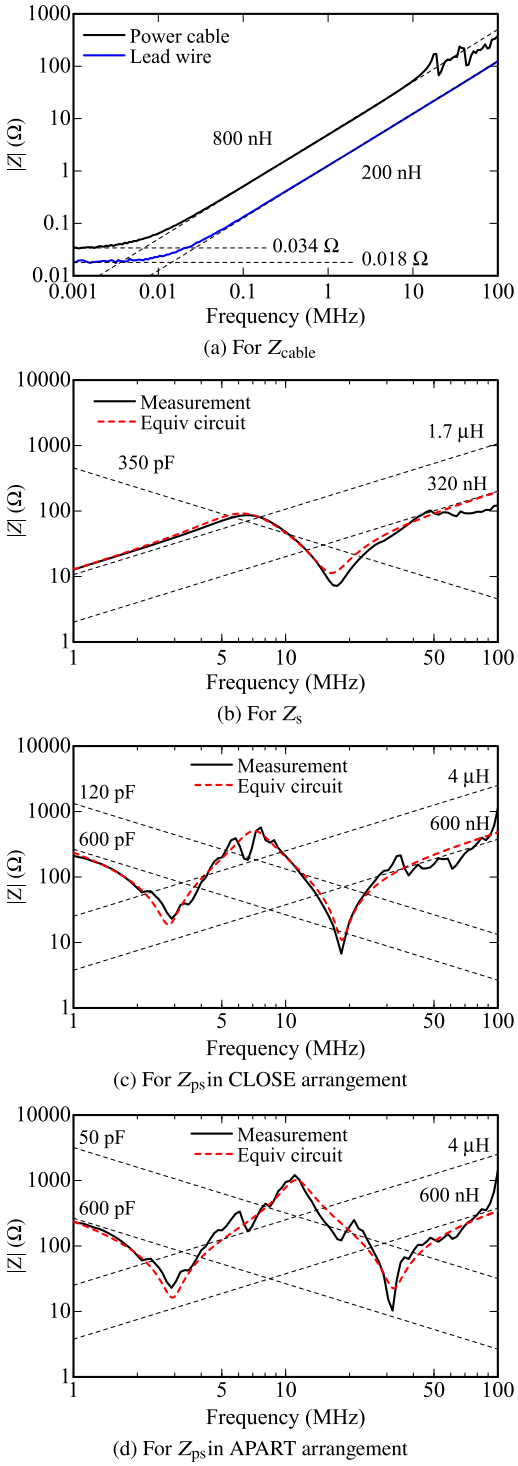
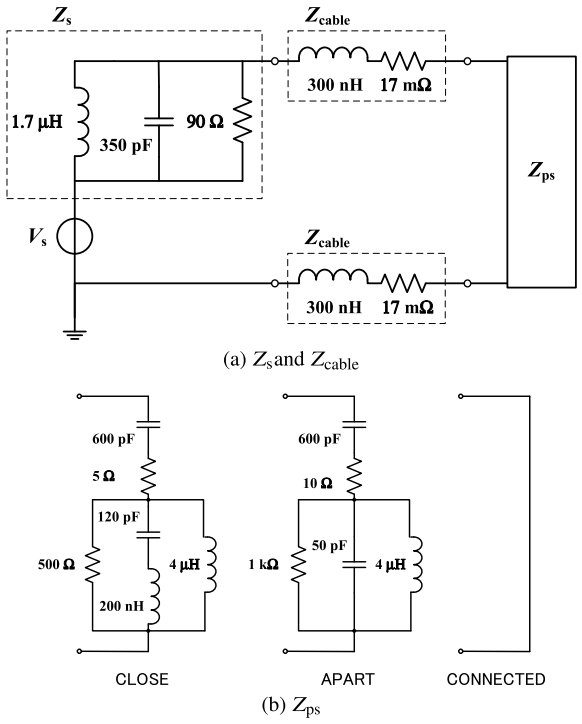


Fig. 6 Measured impedances to identify Z_{cable}, Z_{ps}, and Z_s.

as 17 mΩ.

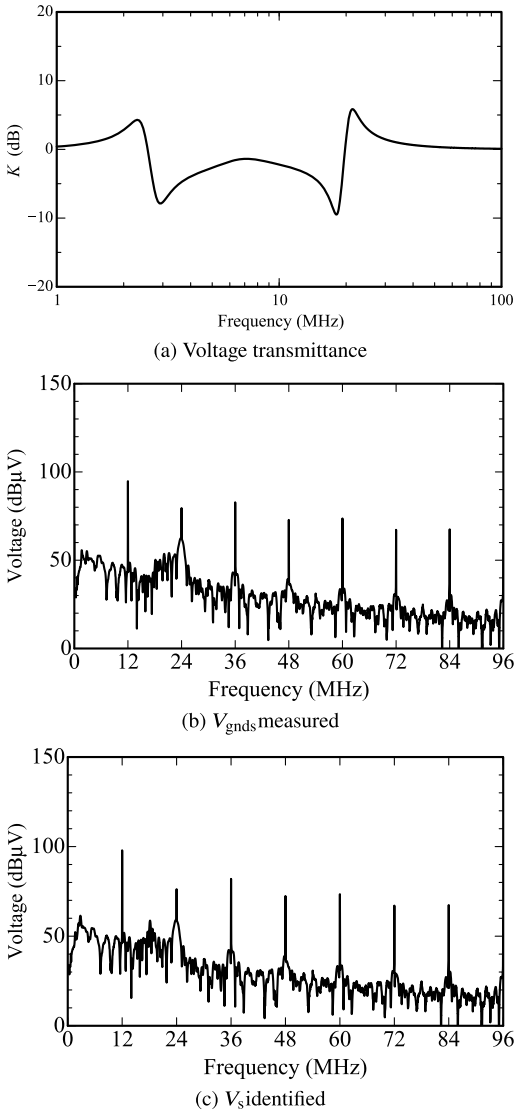
Z_s was measured under non-powered conditions with SASEBO-G connected to the VNA via lead wires. The obtained impedance is shown in Fig. 6(b). The graph shows the parallel circuit of 1.7 μH, 350 pF, and 90 Ω along with a series connection of 320 nH, where 320 nH is the ESL of the lead wires. Therefore, Z_s is represented by the RLC parallel



(a) Z_s and Z_{cable}

(b) Z_{ps}

Fig. 7 Identified impedances of the equivalent circuit.



(a) Voltage transmittance

(b) V_{gnds} measured

(c) V_s identified

Fig. 8 Identification of V_s.

circuit excluding the lead wires.

To identify Z_{ps}, the driving point impedance was measured for the CLOSE and APART conditions, looking from the power connector of SASEBO-G to the DC power supply side. The magnitudes of the measured impedances are shown in Fig. 6(c) and (d). These measured impedances include Z_{cable}. On the basis of the capacitive, inductive, and resistive values obtained by curve fitting, we identified the equivalent circuits for Z_{ps} in CLOSE, APART, and CONNECTED, as shown in Fig. 7(b). In the CONNECTED condition, the power cable is short-circuited at the DC power supply, so the equivalent circuit of Z_{ps} is assumed to be a short circuit.

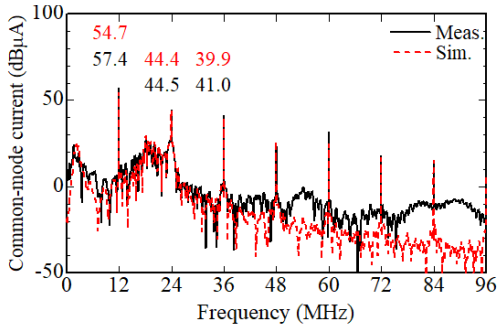
Finally, V_s was identified. Since the equivalent circuit impedance elements in Fig. 4 were identified, the ratio between V_s and V_{gnds} was also determined as shown in Fig. 8(a). Therefore, V_{gnds} was measured in the CLOSE power supply arrangement, and V_s was calculated. V_s was identified for all 2000 chosen plaintexts. Figure 8(b) shows V_{gnds} measured during the encryption process of the first plaintext, and (c) shows the corresponding identified V_s. A spectrum with sharp peaks at the clock frequency of 12 MHz and its harmonics was obtained.

4. Simulation of Side-Channel Leakage in Common Mode

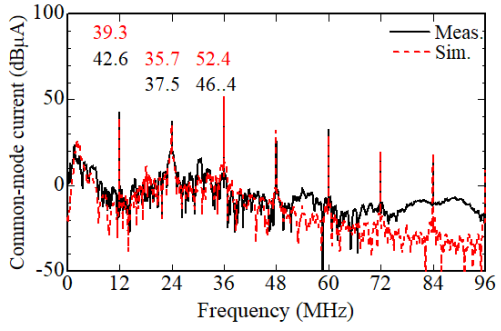
To determine whether the dominant source of side-channel information leakage superimposed on the CM current in SASEBO-G is the potential difference between the split GND planes, we utilize the equivalent circuit model to predict the change in leakage intensity when the impedance of the dominant CM current path is changed.

First, we predicted the CM current under the CLOSE condition. I_c was calculated by the equivalent circuit model and compared with the measured I_c to confirm the accuracy of the equivalent circuit model. The calculated I_c is shown in Fig. 9(a). The simulation results are shown as red dashed lines, and the measured current spectrum as black lines. The transfer admittance from V_s to I_c calculated from the equivalent circuit is shown in Fig. 10. The current values are noted at the clock frequency and the second and third harmonics in the graphs in Fig. 9 since the side-channel information leaked among this frequency range (as discussed later in Fig. 11). The simulation results were consistent with the measured results by up to 3 dB in the side-channel information leakage bandwidth.

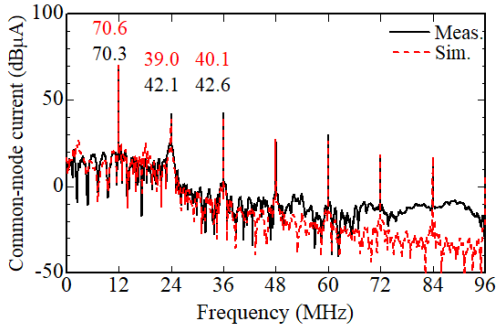
Next, we simulated the CM currents for the APART and CONNECTED conditions. Figure 9(b) and (c) show



(a) CLOSE



(b) APART



(c) CONNECTED

Fig. 9 Simulations of I_c.

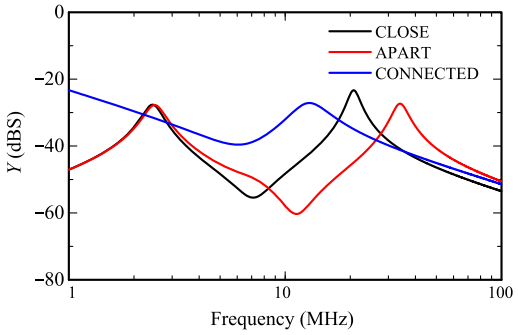
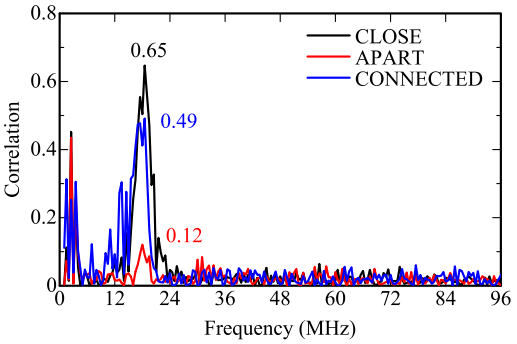


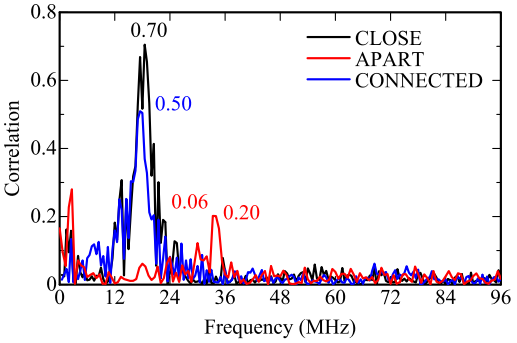
Fig. 10 Transfer admittances.

that they agreed with the corresponding measurements with a maximum difference of 4 dB.

The results of CPA with simulated I_c are shown in Fig. 11(a). Here, we calculated Pearson's correlation coefficients between I_c and the leakage model by assuming the correct secret key, as our focus is the change in leakage intensity. The correlation between the current and the leakage model was calculated for each frequency. The frequency distribution of the correlation coefficients represents the variation of leakage intensity with frequency. Focusing on the band around 18 MHz, where the correlation coefficient was highest, the highest correlation coefficient of 0.65 was obtained when the two DC power supplies were placed CLOSE together, followed by a correlation coefficient of 0.49 when the power cables were CONNECTED at the power supply. When the two power sources were placed APART, the correlation coefficient decreased significantly to about 0.1. The correlation coefficients and trends among those three conditions were consistent with the measurements, as shown in Fig. 11(b).



(a) Simulated



(b) Measured

Fig. 11 Correlation coefficients.

The change in leakage intensity in Fig. 11 depends on the transfer admittance from the leakage source to the CM current. Fig. 12 examines the relationship between the correlation coefficient and the transfer admittance below 36 MHz. Z_{ps} was zero for CONNECTED, but the transfer admittance was less significant for CONNECTED than CLOSE at 18.5 MHz. Therefore, the correlation coefficient of CLOSE is greater than that of CONNECTED. The transfer admittance was reduced by 14 dB from CONNECTED to APART, significantly decreasing the correlation coefficient to 0.12. As these results are consistent with the measurement results, we can safely say that the equivalent circuit represents the behavior of side-channel information leakage in the common mode. These results also indicate that reducing transfer admittance in the CM current path is an essential measure to

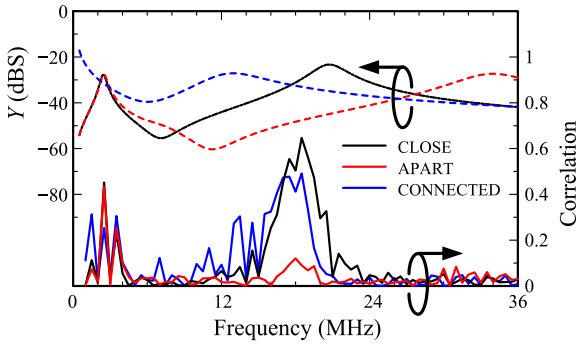


Fig. 12 Correlation coefficients and transfer admittance below 36 MHz.

suppress information leakage in the common mode.

The frequency distribution of the correlation coefficients also contained discrepancies between the simulation and measurement: specifically below 5 MHz, the correlation coefficient in the simulation was more significant than that in the measurement. This difference is presumably due to the low sensitivity of the current probe at low frequencies; in fact, the sensitivity of the current probe we used dropped sharply below 10 MHz. On the other hand, the differential probe used in the V_s identification of the equivalent circuit model has constant sensitivity at low frequencies. Therefore, peripheral noise affected the measured CM currents more in the low-frequency band than in other bands, resulting in differences from the simulation results.

Around 30 MHz, the correlation was about 0.2 in the measurement in the APART condition, but it was small (less than 0.1) in the simulation. These differences suggest the presence of CM currents that return to the system GND. The same occurrence was pointed out in Sect. 2 when comparing the results of Measurements I and III. The modest CM current is estimated to contain side-channel information around 30 MHz. It increased its contribution to the correlation coefficient as the dominant one decayed.

5. Discussion

On the basis of the results in Sects. 2 and 4, we were able to identify the dominant mechanism of side-channel information leakage superimposed on the CM current generated by SASEBO-G. The excitation source was the potential difference between the split GND planes. It excited the two cables connected to the printed circuit board and the circuitry connected to their ends, generating the CM current. We further showed that information leakage in this dominant CM can be suppressed by reducing the potential difference between the GND planes and the transfer admittance of the CM current path.

Although these results are from a case study by SASEBO-G, similar side-channel information leakage can occur in other systems, as mentioned in the Introduction. For example, printed circuit boards with connected cables can have split GND planes for digital and analog circuits. An automobile-integrated ECU may incorporate printed circuit boards separated by function, and harnesses are connected to each. In such a system, if splits of the GND plane are unavoidable, it is crucial to connect the split GND planes with low impedance in the side-channel information leakage band using capacitors and the like and to weaken the coupling of the connected cables and the circuits connected to them.

6. Conclusion

In this work, we identified the dominant leakage mechanism for the cryptographic module SASEBO-G, which has been reported to leak side-channel information in the common mode. First, we measured CM currents by changing the electrical connections of the split GND planes of SASEBO-G and the placement of the system GND and estimated the dominant CM current paths. An equivalent circuit of the estimated dominant CM current path was constructed, and impedance measurements identified its circuit parameters. The side-channel information leakage strength was simulated with the equivalent circuits for two CM current path transfer admittances. The simulation results were consistent with the measured results, and we identified the dominant information leakage mechanism as the potential difference between the split GND planes, which excites the cable connected to the printed circuit board and the circuit beyond it.

We also touched on the fact that side-channel information leakage by the same leakage mechanism can also occur in other systems with split GND planes. We clarified the threat of information leakage superimposed on CM currents in such systems and suggested countermeasures to mitigate it. In particular, it is crucial to connect the split GND planes with low impedance in the information leakage band by, for example, capacitors and to weaken the coupling of multiple cables and harnesses connected to the printed circuit board in the information leakage band.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number 23K11102.

References

[1] L. Chen, J. Franklin, and A. Regenscheid, “Guidelines on hardware rooted security in mobile devices,” Technical Report, National Institute of Standards and Technology, 2012.
[2] P.C. Kocher, “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems,” Advances in Cryptology – CRYPTO’96, N. Koblitz, ed., LNCS, vol.1109, pp.104–113, Springer-Verlag, 1996.
[3] P.C. Kocher, J.M. Jaffe, and B.C. Jun, “Differential power analysis,” Advances in Cryptology — CRYPTO’99, M. Wiener, ed., LNCS, vol.1666, pp.388–397, Springer-Verlag, 1999.
[4] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model,” CHES 2004, pp.16–29, 2004.
[5] B. Timon, “Non-profiled deep learning-based side-channel attacks,” IACR Trans. Cryptographic Hardware and Embedded Systems, pp.107–131, 2019.
[6] Y. Hayashi, T. Sugawara, Y. Kayano, N. Homma, T. Mizuki, A. Satoh,

T. Aoki, S. Minegishi, H. Sone, and H. Inoue, "Information leakage from cryptographic hardware via common-mode current," 2010 IEEE International Symposium on Electromagnetic Compatibility, pp.109–114, 2010.

[7] K. Iokibe, T. Amano, and Y. Toyota, "On-board decoupling of cryptographic FPGA to improve tolerance to side-channel attacks," 2011 IEEE International Symposium on Electromagnetic Compatibility, pp.925–930, 2011.

[8] Y.i. Hayashi, K. Ohmura, T. Mizuki, and H. Sone, "Influence of PCB and attached line of hardware on electromagnetic (EM) information leakage," IEEJ Trans. Fundamentals and Materials, vol.132, no.2, pp.173–179, 2012. DOI: 10.1541/ieejfms.132.173

[9] AIST, "Side-channel attack standard evaluation board (SASEBO)," http://staff.aist.go.jp/akashi.satoh/SASEBO/en/index.html

[10] E.B. Joffe and K.S. Lock, Grounds for Grounding — A Handbook from Circuits to Systems, 2nd ed., ch. 13, pp.697–1000, Wiley, Hoboken, 2023.

[11] H.Y. Shim, J. Kim, and J.G. Yook, "Modeling of ESD and EMI problems in split multi-layer power distribution network," 2003 IEEE Symposium on Electromagnetic Compatibility, Symposium Record (Cat. no.03CH37446), vol.1, pp.48–51, 2003.

[12] S.S.A. Naqvi, H. Jamil, N. Iqbal, S. Khan, M.A. Khan, F. Qayyum, and D.H. Kim, "Evolving electric mobility energy efficiency: In-depth analysis of integrated electronic control unit development in electric vehicles," IEEE Access, vol.12, pp.15957–15983, 2024.

[13] K. Iokibe, T. Amano, K. Okamoto, and Y. Toyota, "Equivalent circuit modeling of cryptographic integrated circuit for information security design," IEEE Trans. Electromagn. Compat., vol.55, no.3, pp.581–588, 2013.

[14] M. Himuro, K. Iokibe, and Y. Toyota, "Triangular pulse-based ic switching current model using multiple regression analysis for fast side-channel attack prediction," IEEE Trans. Electromagn. Compat., vol.66, no.1, pp.49–60, 2024.

[15] NIST, "Advanced encryption standard (AES)," FIPS publication 197, National Institute of Standards and Technology, Nov. 2001.

Kengo Iokibe received the B.S. and M.S., degrees in electrical and electronic engineering and the Ph.D. degree in science and technology for intelligence from Okayama University, Okayama, Japan, in 1997, 1999, and 2005, respectively. From 2005 to 2023, he was an Assistant Professor with Okayama University, where he is currently an Associate Professor. His recent research interests include information security against side-channel attacks on cryptographic circuits, designing power distribution networks to achieve power integrity, signal integrity and EMC, and EMC modeling of power converters. He is a Senior Member of the Institute of Electronics, Information and Communication Engineers (IEICE) and a Member of the Institute of Electrical Engineers of Japan (IEEJ), and the Japan Institute of Electronics Packaging (JIEP).

Kohei Shimoda received the B.S. degree in electrical and communication engineering and M.S. degree in electronic and information systems engineering in 2022 and 2024, respectively, from Okayama University, Okayama, Japan, where he is currentlyworking as a system engineer. His research interests include electromagnetic information leakage from cryptographic modules.

Masaki Himuro received the B.S. degree in electrical and communication engineering and M.S. degree in electronic and information systems engineering in 2021 and 2023, respectively, from Okayama University, Okayama, Japan, where he is currentlyworking toward the Ph.D. degree in information and communication systems. His research interests include electromagnetic information leakage from cryptographic modules. He is a Graduate Student Member of the Institute of Electrical and Electronics Engineer.

Yoshitaka Toyota received the B.S. and M.S. degrees in electrical and electronic engineering from Okayama University, Okayama, Japan, in 1991 and 1993, respectively, and the Ph.D. degree in electronic engineering from Kyoto University, Kyoto, Japan, in 1996. From 1996 to 1998, he was with Yokogawa Electric Company Ltd., and in 2005, he worked with Georgia Tech as an Overseas Research Scholar of the Ministry of Education, Culture, Sports, Science and Technology (MEXT) of Japan. He is currently a Professor of Institute of Academic and Research with Okayama University. His recentresearch interests include EMC design for electrical and electronic equipment and systems. He is a Senior Member of the Institute of Electronics, Information and Communication Engineers (IEICE) and a Member of the Japan Institute of Electronics Packaging (JIEP), the Japan Society of Applied Physics (JSAP), and the Institute of Electrical Engineers of Japan (IEEJ).