

Equivalent Circuit Modeling of Cryptographic Integrated Circuit for Information Security Design

Kengo Iokibe, *Member, IEEE*, Tetsuo Amano, Kaoru Okamoto, and Yoshitaka Toyota, *Member, IEEE*

Abstract—In this study, equivalent circuit modeling was examined to develop a method to evaluate cryptographic systems before fabrication. An equivalent circuit model of a cryptographic FPGA in which an advanced encryption standard (AES) algorithm had been implemented was determined from experimental measurements under the initial configuration of a power distribution network (PDN) of the FPGA. The model was implemented into a commercial analog circuit simulator, and power traces due to the simultaneous switching noise current were estimated under three different PDN configurations in which a decoupling circuit was inserted into the PDN as an on-board countermeasure. Estimated power traces were analyzed statistically by the correlation power analysis method to obtain correlation values, a major security index of AES. Variation of the correlation values with changes in decoupling configuration agreed with the corresponding experimental results. This means that the security of cryptographic devices against side-channel attacks can be evaluated by using the equivalent circuit model before fabrication.

Index Terms—Advanced encryption standard (AES), correlation power analysis (CPA), information leakage, power distribution network (PDN), side-channel analysis, simultaneous switching noise.

I. INTRODUCTION

RECENTLY, broadband networks have been growing worldwide as people exchange extremely large amounts of information globally. However, this trend means leakage and manipulation of information are becoming realistic threats to information security even in consumer products, such as smart cards, server computers, memory cards, and automated teller machines. Cryptographic technologies have been primarily used to protect the products from these threats, but they may not do so in the future.

Methods for attacking cryptographic devices, known as side-channel attacks, have been developed that can make the cryptographic technologies helpless. In 1999, Kocher *et al.* deciphered the secret key of a cryptographic device by analyzing traces of radio frequency (RF) power current that occurred when logic gates in the cryptographic integrated circuit (IC)

Manuscript received March 31, 2012; revised September 8, 2012; January 16, 2013; accepted February 10, 2013.

The authors are with the Graduate School of Natural and Science Technology, Okayama University, Okayama 700-8530, Japan (e-mail: iokibe@okayama-u.ac.jp; okamoto@dev.cne.okayama-u.ac.jp; toyota@okayama-u.ac.jp).

Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TEMC.2013.2250505

had switched [1]. They found that amplitude of the simultaneous switching noise (SSN) current was related to values of a switching register that temporarily stored intermediate values in a cryptographic process.

Side-channel attacks are cryptanalytic attacks by means of the SSN current from cryptographic ICs or electromagnetic emissions originating from the SSN current. The SSN current is generated as logic gates in a cryptographic IC switch simultaneously in an encryption process. Since variation of power current depends on the encryption process, the current contains secret cryptographic information that can be extracted by analyzing current profiles statistically [1]–[3]. An attacker observes the SSN current and/or electromagnetic (EM) radiation and acquires their waveforms, which are then analyzed for breaking the encryption. Thus, an important task in designing a cryptographic system to ensure security against side-channel attacks is to reduce the SSN current. In the field of electromagnetic compatibility (EMC), various techniques to reduce the SSN current and EM radiation have been developed and are potential countermeasures against the side-channel attacks.

Considering a design phase, designers have to evaluate their product with respect to security against the side-channel attacks after they have implemented countermeasures. The evaluation is usually based on actual attacks on their product or its prototype. If the results do not conform, the cryptographic system must be designed and built again. However, this process is very costly and should be avoided.

In this study, an equivalent circuit model of IC power circuits is examined for developing a method to evaluate cryptographic systems before fabrication. The equivalent circuit model, such as ICEM and LECCS, has been developed to predict the SSN current and/or electromagnetic emission of digital ICs for EMC design [4]–[8] and can also be utilized to estimate the SSN current of cryptographic ICs. If the equivalent circuit model of a cryptographic IC is obtained in the phases of designing and developing a cryptographic system, the designers can validate it with respect to the side-channel attacks before fabrication. Therefore, we will examine a method using the linear equivalent circuit model to estimate results of a side-channel attack on a commercial cryptographic device developed for the evaluation with respect to the side-channel attacks.

This paper is organized as follows. Section II reviews the SSN current from the point of view of the side-channel attacks, and Section III introduces the method that uses the equivalent circuit model. Section IV describes the device under tests and the encryption algorithm used in the experiments of this paper, and Section V determines model parameters on the basis of measurements of impedance and voltage bounce. In Section VI, voltage

variations due to the SSN current, the so-called “power traces,” are calculated in several decoupling configurations by using the equivalent circuit model, and obtained current waveforms are analyzed by the correlation power analysis (CPA) method. These simulated results are compared with experimental results to validate the method.

II. SIMULTANEOUS SWITCHING NOISE CURRENT AND SIDE-CHANNEL ANALYSIS ATTACKS

A. Side-Channel Analysis Attacks

Side-channel analysis is a method to reveal confidential information processed in a cryptographic device by using *side-channel information*. The side-channel information is carried with the SSN current of cryptographic ICs and EM radiation induced by the SSN current, not in the ciphertexts or electrical signals transmitting the ciphertexts. In the field of cryptographic engineering, the SSN current is called “power consumption” and its waveforms and voltage variations that are generated by the SSN current and observed in the power distribution networks (PDNs) are called “power traces.” Attackers observe the power traces and/or EM radiation and analyze their variation with changes in data values manipulated to obtain secret information.

Since Kocher published his early work [9], many side-channel analyses have been developed [1], [2], [10], [11]. The following three types of analyzing method are now well known: The timing analysis [9], simple power analysis [1], and differential power analysis (DPA) [1]. We focus here on a sophisticated DPA method, the CPA [3] for the advanced encryption standard (AES), a common key cryptosystem standardized by the National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) in 2001 [12]. Another attacking method attracting the interest of many researchers is called the fault injection [13]: An active method in which excessive electrical or optical impulse is injected to the cryptographic device to cause a malfunction, similar to the direct power injection method [14]. However, this active method is not discussed here.

When a cryptographic IC processes an encryption algorithm, the SSN current occurs as logic gates in the encryption circuit switch. Temporal variation of the SSN current in magnitude depends on the data processed and/or operation performed [15]. Thus, if the magnitude of the SSN current was analyzed statistically, such information can be revealed. For attacks on AES, an attacker gathers the power traces with respect to an adequate number of plaintexts and analyzes the traces statistically by, for example, the CPA method.

B. Composition of Power Trace

A power trace is composed of voltage variations due to the SSN current and background noise and can be expressed as

$$\begin{aligned} v_m(t) &= u(t) * i_m(t) + v_n(t) \\ &= u(t) * \{k(t) * i_{IC}(t)\} + v_n(t) \end{aligned} \quad (1)$$

where i_{IC} represents the SSN current generated in a cryptographic IC, i_m the SSN current at the location where the current

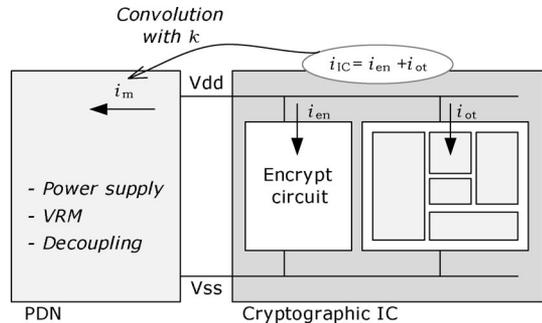


Fig. 1. Simultaneous switching noise currents.

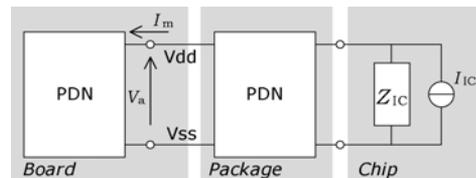


Fig. 2. Power distribution network.

is detected, k is the transmittance of the SSN current from the IC circuit to the detecting location, and u the system function of apparatus used to obtain the power trace. v_n represents the background noise. u is in the dimension of Ohm and depends on probe sensitivity and amplifier gain. Asterisks $*$ denote the convolution operator. As i_{IC} is divided into the two components of the encryption circuit and other circuits, i_{en} and i_{ot} as shown in Fig. 1, (1) becomes

$$v_m(t) = u(t) * [k(t) * \{i_{en}(t) + i_{ot}(t)\}] + v_n(t). \quad (2)$$

Since i_{en} involves confidential information but i_{ot} and v_n are independent of the encryption, decreasing the contribution of i_{en} to v_m makes the cryptographic devices more secure against the SCA attacks.

III. METHOD

Security of cryptographic devices installed in equipment is usually evaluated by analyzing the power traces. Acquisition of the power traces from experimental measurements takes enormous amounts of time and money, but both time and money can be saved if the power traces are estimated by calculation. The power traces can be estimated by means of analog circuit simulation using a linear equivalent circuit model that models the SSN current.

The SSN current occurs in digital IC circuits, leaks along the PDN, and is a major source of electromagnetic interference (EMI). There are two similar linear equivalent circuit models developed for predicting the SSN current: The linear equivalent circuit and current source (LECCS) model and ICEM model [4]. Both the LECCS and ICEM models have the same fundamental structure composed of impedance blocks and current sources, with which the equivalent circuit of a power network composed of a cryptographic IC and its PDN is expressed in Fig. 2. Z_{IC} is the driving point impedance of the IC at the V_{dd} - V_{ss} port. I_{IC} is the frequency-domain expression of i_{IC} . Throughout the paper,

variables written in upper and lower case denote those in the frequency-domain and those in the time-domain, respectively.

In LECCS modeling, a procedure determining the current source I_{IC} from measurements [7], [8] has been developed in accordance with

$$I_m = K I_{IC} \quad (3)$$

where I_m is the SSN current conducted along the PDN and K is a factor depending on Z_{IC} and all impedances on PDN. I_m is usually measured on a printed circuit board for the ease of probing, as shown in Fig. 2. When the current I_m and PDN impedances are obtained from experimental measurements, I_{IC} is calculated by (3). Furthermore, the probe sensitivity u and system noise v_m in (1) can be measured easily, so the power trace v_m is calculated by (1).

The equivalent circuit model was developed for predicting the EM radiation caused by the SSN current, so voltages detected with probes were converted into the dimension of current. However, when making side-channel attacks, especially power analysis attacks, attackers are interested in whether their detected traces contain secret information but not interested in their dimension. They, therefore, usually analyze the voltage traces without a conversion of dimension. Since the PDN is passive, the voltage V_a , the frequency-domain expression of a power trace, is obviously related to I_{IC} by a similar expression to (3), as

$$V_a = Z_K I_{IC} \quad (4)$$

where Z_K is the transfer impedance from the port across Z_{IC} to the port where V_a is measured, which depends on Z_{IC} and the PDN impedances. The time-domain expression of V_a corresponds to the first term, $u(t) * i_m(t)$, of (1).

Considering, for example, a scene designing a PDN to enhance cryptographic device security, designers are able to calculate Z_K easily by using an analog circuit simulator, and power traces v_m are obtained when the PDN has been changed. Thus, designers can evaluate their design before experimenting with a prototype, and they will make the prototype after their design is confirmed to be sufficiently secure.

IV. DEVICE UNDER TEST AND TARGET ENCRYPTION ALGORITHM

A commercial printed circuit board developed for evaluating cryptographic devices, SASEBO-G, was used here as the target cryptographic device. SASEBO-G is a side-channel attack evaluation board developed by the Research Center for Information Security of the National Institute of Advanced Industrial Science and Technology and Tohoku University [16]. SASEBO-G has two field-programmable gate array (FPGA) ICs on it as shown in Fig. 3: One is for operating encryption processes and the other for controlling the encryption operation. Circuitry composition of the PDN of the encryption FPGA is drawn in Fig. 4(a). Between the cryptographic FPGA and the voltage regulator module (VRM), only an electrolytic capacitor is mounted as a decoupling capacitor, named C_{dc2} here, and a single pair of pads for a chip decoupling capacitor is prepared

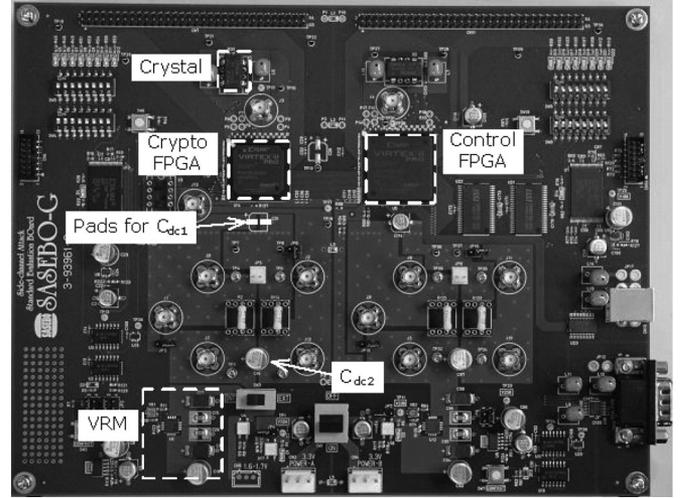


Fig. 3. Top view of SASEBO-G.

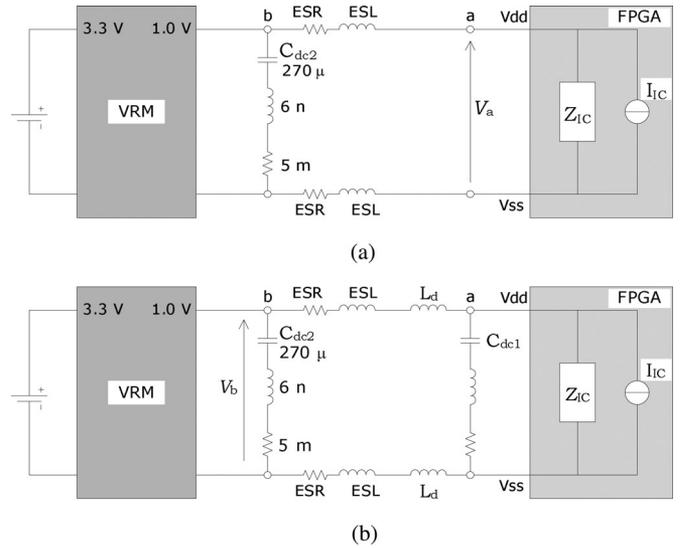


Fig. 4. PDN of cryptographic FPGA. (a) Standard composition and used for modeling. (b) For validation.

near the FPGA. In this study, a 2012 sized chip capacitor of 10 nF is mounted on the pads, as C_{dc1} .

In the following experiments, the AES algorithm was processed in the cryptographic FPGA 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, a 1000-plaintext set was used that contained two 500-plaintext-sets: one gave the HD of the tenth round as two and the other gave it as 124. Plaintexts in the 1000-plaintext set were arranged to take the two HD values in turn. Such large changes in HD provide a strong correlation in CPA, and this allows designers to judge with a small number of power traces whether their products may potentially leak. The AES-128 encryption process was composed of ten round-operations as well as a preoperation including preparation of subkeys used in the round operations, as shown in Fig. 5. Each operation began synchronized to the clock signal of 24 MHz that was supplied from the crystal oscillator mounted near the cryptographic FPGA, see Fig. 3.

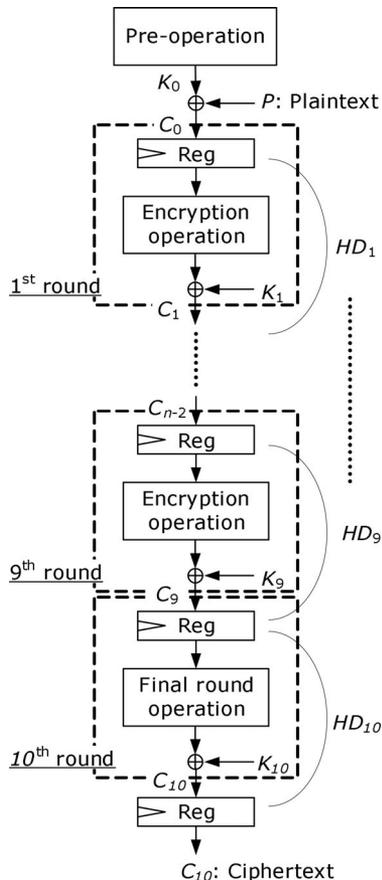


Fig. 5. Flowchart of AES-128 encryption.

As the method for side-channel attack, the correlation power analysis [3], which is known as the most powerful method for AES, was used in this study. The final (tenth) round of the AES-128 encryption was set to be the target round of CPA. In CPA, attackers focus on the variation of SSN current in magnitude with a change in plaintext. The change in plaintext changes the Hamming distance (HD) of register values between the target round and the previous round. The HD is the number of register gates that shift the states, so the SSN current is large when HD is large. In contrast, the SSN current is small when HD is small. HD also depends on the secret key, which can, therefore, be revealed by investigating the correlation between the current variation and HD variation. The variations of HD for all the possible secret keys are calculated in advance as a “power model” in CPA.

V. DETERMINATION OF MODEL PARAMETERS

The equivalent circuit model of the cryptographic FPGA consists of impedance between V_{dd} and V_{ss} terminals Z_{IC} and a current source I_{IC} parallel to the impedance. The impedance was determined from an S-parameter measurement at the port of V_{dd} and V_{ss} terminals, and the current source from a measurement of V_a according to (4). The factor Z_K was calculated by an analog circuit simulation using the linear equivalent circuit of the PDN for the encryption circuit in the cryptographic FPGA.

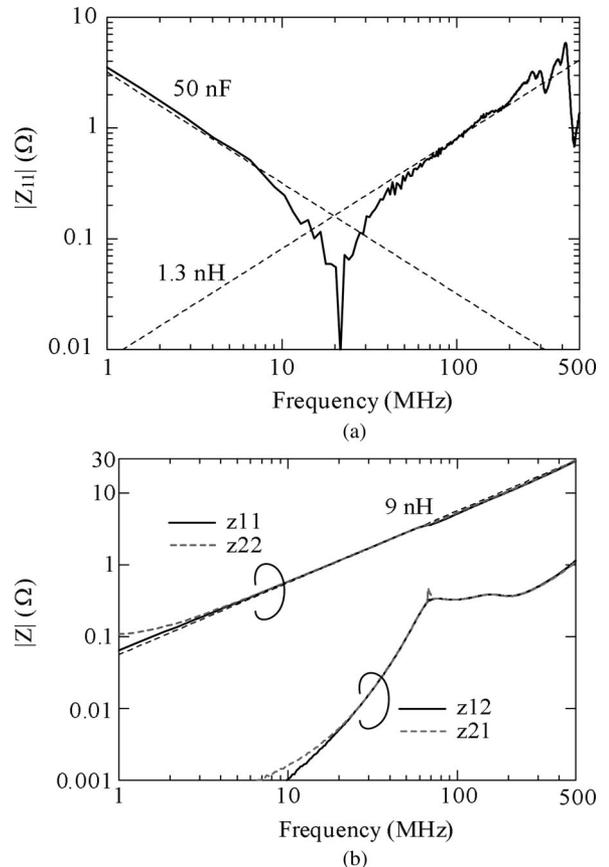


Fig. 6. Measured impedances. (a) Cryptographic FPGA. (b) Voltage regulator module.

Impedances of the VRM, decoupling capacitors, and decoupling inductors were obtained from measurements.

A. Impedances

The FPGA impedance Z_{IC} was measured at the pads for a decoupling capacitor C_{dc1} by using a microprobe (FPC-SG-1250, Cascade Microtech) and a vector network analyzer (E5071, Agilent Technologies). All 1Ω resistor and short bar, which might have been mounted in the default configuration on socket connectors, were removed and C_{dc1} was not mounted on the pads during the measurement, that is, the FPGA was disconnected with the PDN and not biased. Obtained S parameters converted into the driving point impedance at the measurement port, as shown in Fig. 6(a), found the impedance composed of a capacitance of 50 nF and an inductance of 1.3 nH. The measured impedance surely involves impedances of power and ground traces and vias between the pads and FPGA. They were difficult to de-embed from the measured impedance because the detailed layout information of the commercial board had not been released and because a bare board had not been obtained. Consequently, Z_{IC} was given with the measured impedance.

The impedance of VRM was also measured using another printed board copying the VRM circuit of SASEBO-G utilizing the same regulator module IC and the same chip capacitors and chip resistors in quantity and size. Measured Z parameters

TABLE I
EQUIPMENT USED IN MEASUREMENTS

Impedance measurement	
Vector Network analyzer	E5071A, Agilent Technologies
Freq. range	300 kHz–2 GHz for FPGA 30 kHz–500 MHz for VRM
No. of Points	1601
No. of Averaging	16
IFBW	70 kHz for FPGA 10 kHz for VRM
Microprobe	FPC-SG-1250, Cascade Microtech
V_m measurement	
Digital oscilloscope	54845A, Agilent Technologies
Bandwidth	1.5 GHz
Sampling rate	4 GSa/s
Coupling	AC
Passive probe	1161A, Agilent Technologies
Bandwidth	500 MHz

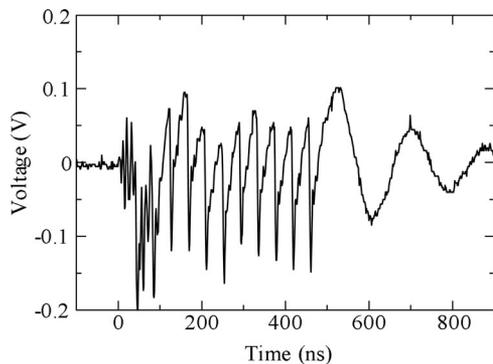


Fig. 7. measured waveform of V_a for a plaintext.

are plotted in Fig. 6(b). The driving point impedances are obviously dominated by inductance, the amount of which was found as 9 nH. This inductance was coincident to the equivalent series inductance (ESL) of the stabilizing capacitors installed on the VRM output side. The transfer impedances were smaller than 1Ω up to 500 MHz, that is, the two ports of VRM were isolated sufficiently. The equivalent circuit of VRM was, therefore, expressed with an inductance of 9 nH.

On top of that, the parasitic impedance of C_{dc2} was obtained by measuring the electrolytic capacitor alone. The resultant ESL and ESR are written in the schematic in Fig. 4(a). Impedances of power and ground traces and vias will be neglected since the detailed layout information was not gained as mentioned above.

B. Current Source

According to (4), the current source of the equivalent circuit model can be calculated from V_a and Z_K . First, V_a was measured at Port a in the PDN configuration of Fig. 4(a) with a digital oscilloscope and a passive probe. The PDN configuration is a nondecoupling configuration in which the nodes a and b were shunt with short-bars that had their ESLs and ESRs taken into account. Specifications of experimental equipment are listed in Table I. Waveforms of V_a were obtained for all the plaintexts, and an example of the waveforms is drawn in Fig. 7. The time origin corresponds to the beginning of the AES-128 encryption process, since the waveform acquisitions were synchronized to

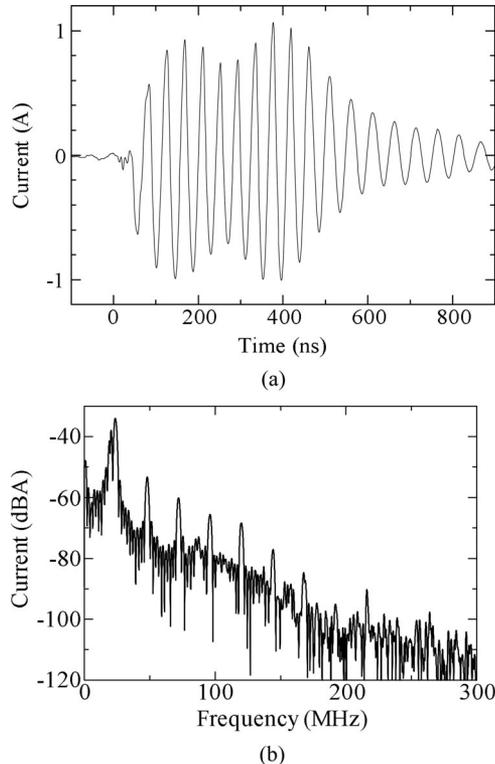


Fig. 8. Current source calculated from V_a in Fig. 7. (a) i_{IC} in time-domain. (b) I_{IC} in frequency-domain.

the trigger pulse that occurred in the cryptographic FPGA when the encryption process began. The voltage started fluctuating at the time origin and 11 periodic sharp peaks appeared. The last peak is seen around $t = 460$ ns corresponding to 11 periods of the 24 MHz clock. The AES-128 algorithm is composed of 11 successive operations: a key-schedule and ten round-operations. These successive operations were synchronized to the 24 MHz clock and had to spend 458 ns, which is consistent with the measured waveform.

Next the system constant Z_K was calculated by simulating the linear equivalent circuit of the PDN on a commercial circuit simulator, AWR Microwave Office, using the impedances determined in Section V-A. By substituting Z_K and V_a , the current sources I_{IC} were obtained for all the 1000 plaintexts. The current source corresponding to the V_a in Fig. 7 is indicated in Fig. 8: in the (a) time-domain and (b) frequency-domain. In the time-domain, the SSN current rises at $t = 40$ ns corresponding to the period of the clock and attenuates after 11 periodic oscillations. In the frequency-domain, harmonics of the clock rate of 24 MHz were observed. These results seemed to be reasonable as a current source of the cryptographic FPGA.

VI. VALIDATION

To validate it, the linear equivalent circuit model was applied to predict effects of the PDN decoupling in making cryptographic devices more secure.

TABLE II
DECOUPLING CONFIGURATIONS

Configuration	C_{dc1} (nF)	L_d (nH)
#1	0	0
#2	10	0
#3	0	100

A. Simulation of Power Traces

Power traces were simulated at the port b as V_b for the validation, see Fig. 4(b). The alternative expression of (4) for V_b is given as

$$V_b = Z'_K I_{IC} \quad (5)$$

where Z'_K represents the transfer impedance from the port across Z_{IC} to Port b . The PDN was decoupled by a decoupling capacitor C_{dc1} and decoupling inductors L_d . In the simulation of the power traces, V_b was calculated in accordance with (5), in three decoupling configurations (#1, #2, and #3) as listed in Table II. Configuration #1 is the same configuration for modeling, where no decoupling capacitors or decoupling inductors were used. Configuration #2 used a decoupling capacitor of 10 nF installed at Port a by mounting a chip capacitor on the pads indicating in the photo of SASEBO-G in Fig. 3. In Configuration #3, decoupling inductors of 100 nH were inserted along the power trace and ground trace. The transfer impedance Z'_K was calculated for the three configurations taking the ESL and ESR of the decoupling capacitor C_{dc1} into account. Amounts of ESL and ESR were determined from an impedance measurement of the capacitor as 1.3 nH and 0.01 Ω , respectively.

The background noise was given as a white noise with a variance. The noise variance was given from measurements with the experimental equipment. A noise trace v_n with the variance was generated numerically and added to v_b , the time-domain expression of V_b , and finally v_m was obtained for each plaintext. The given v_n did not contain the noise occurred in the cryptographic FPGA during the encryption operation. The variance of the noise in the FPGA varies in time during the operation and is, in general, difficult to predict. However, the current source I_{IC} involved the noise occurring during the operation since it was involved in the measured power bounce V_a from which I_{IC} was calculated.

Power traces v_m simulated are depicted in Fig. 9, overwritten on measured traces. Approximate profiles of the simulated and measured traces agree in terms of amplitude and periodic fluctuation in Configurations #1 and #2. In Configuration #3, the simulated trace hid the periodic fluctuation behind the noise as the measured profile did.

B. Correlation Power Analysis

The simulated power traces were analyzed by the CPA method with the correct key, and correlation between v_m and the power model was obtained as shown in Fig. 10(a). The correlation profiles peaked around 458 ns, when the final round finished. The peak correlation values were 0.99 for Configuration #1, 0.98 for #2, and 0.56 for #3. The CPA method was also applied for measured power traces. Peak correlation values were found

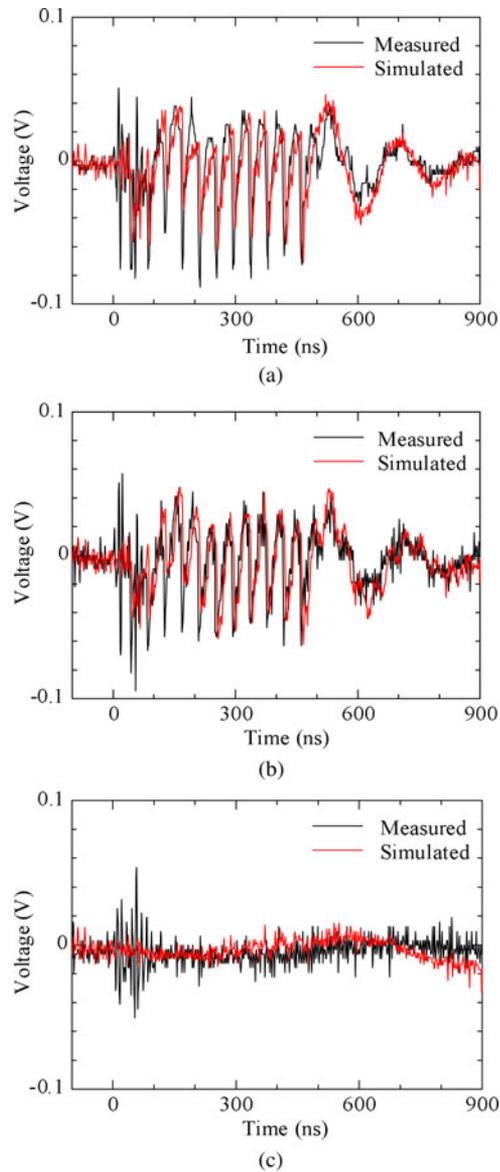


Fig. 9. Power traces simulated in red lines and measured in black. (a) Configuration #1. (b) Configuration #2. (c) Configuration #3.

to be 1.00 for Configuration #1, 0.98 for #2, and 0.51 for #3, see Fig. 10(b). The peak values of simulated power traces were found to agree well with those of measured ones.

The correlation coefficients in Fig. 10(a) are much better than general values obtained by CPA. These large values were due to the use of the special set of plaintext described in Section IV. Fig. 11 shows the correlation to the number of traces plotted with both the correct and wrong key hypotheses. The horizontal axis indicates the number of traces analyzed, and the vertical the peak correlation value in a correlation trace such as traces plotted in Fig. 10. The correct key (black) is clearly distinguished from wrong keys (gray) in all the decoupling configurations. The simulated results in the left column agree with the measured ones in the right just as the simulated traces did in Figs. 9 and 10.

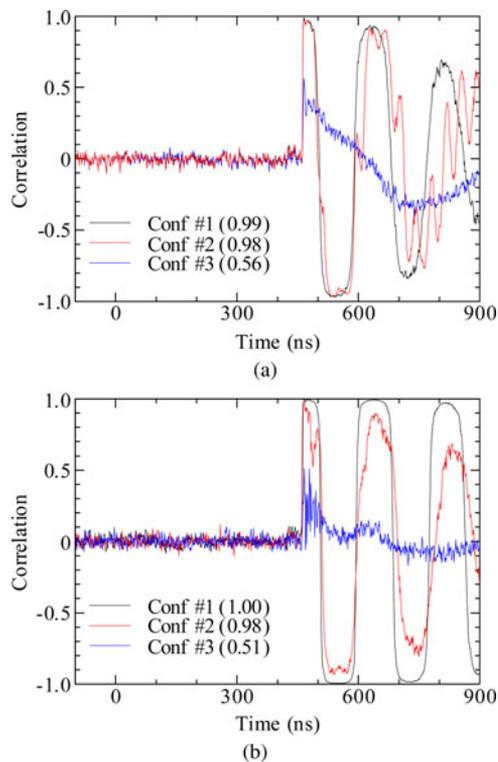


Fig. 10. Results of CPA in the correct key hypotheses. (a) Simulated. (b) Measured.

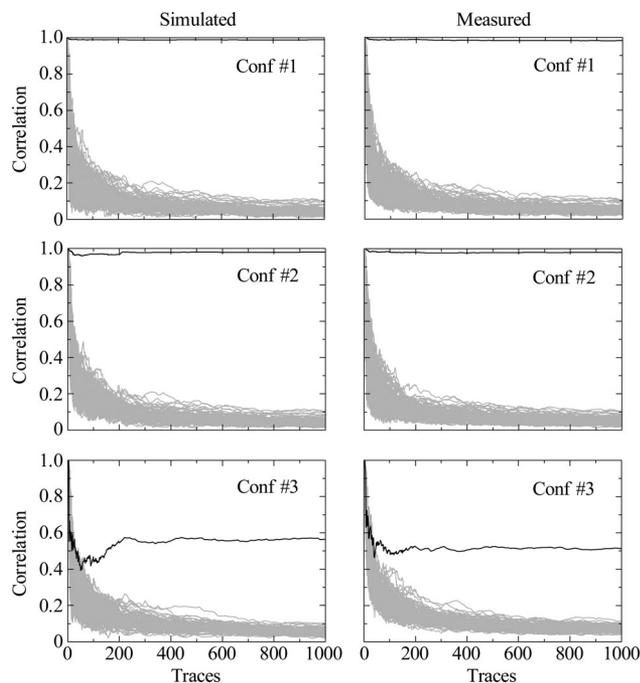


Fig. 11. Correlation coefficients versus the number of analyzed traces plots for the correct (black) and wrong (gray) key hypotheses. Those from simulated and measured power traces are in the left and right columns, respectively.

The agreement between the simulated and measured CPA results indicates that the equivalent circuit model provided accurate calculations of the SSN current that varies with input

data, and that it is, therefore, applicable to predict how secure the cryptographic device is.

VII. CONCLUSION

A method was proposed for designing cryptographic devices secure against the side-channel attacks before fabrication. The method is based on analog circuit simulations with an equivalent circuit that models SSN current of a cryptographic FPGA and can easily be introduced into the existing design procedure of printed circuit boards. Parameters of the equivalent circuit model including impedances and current sources were determined from measurements. A commercial cryptographic printed circuit board, SASEBO-G, a side-channel attack standard evaluation board, was used for modeling and validation. SASEBO-G involving a cryptographic FPGA in which an advanced encryption standard (AES) algorithm had been processed with a set of plaintext. The equivalent circuit model was analyzed with a commercial analog circuit simulator in different decoupling configurations to obtain power traces, which are temporal waveforms of voltage variations caused by the SSN current. The obtained power traces were analyzed by the CPA method, and then the simulated power traces and the power model correlated for all the decoupling configurations. The correlation coefficients of simulated power traces closely agreed with those of measured ones. The correlation coefficients of CPA were, thus, estimated successfully by means of analog circuit simulation with the equivalent circuit model.

The results indicated that security of cryptographic devices against side-channel attacks can be predicted by the equivalent circuit model without actual attacks against a prototype or final product. This leads us to expect a significant reduction in cost for developing cryptographic devices.

ACKNOWLEDGMENT

The authors would like to thank Strategic Information and Communications R&D Promotion Programme (SCOPE) from the Ministry of Internal Affairs and Communications (MIC).

REFERENCES

- [1] P. C. Kocher, J. M. Jaffe, and B. C. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO* (Lecture Notes Computer Science, 1666), M. Wiener, Ed. New York, NY, USA: Springer-Verlag, 1999, pp. 388–397.
- [2] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks*. New York, NY, USA: Springer-Verlag, 2007.
- [3] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proc. Cryptographic Hardware and Embedded Systems*, 2004, pp. 16–29.
- [4] S. D. Dhia, M. Ramdani, and E. Sicard, *Electromagnetic Compatibility of Integrated Circuits*. New York, NY, USA: Springer-Verlag, 2006.
- [5] Y. Fukumoto, Y. Takahata, O. Wada, Y. Toyota, T. Miyashita, and R. Koga, "Power current model of LSI/IC containing equivalent internal impedance for EMI analysis of digital circuits," *IEICE Trans. Commun.*, vol. E84-B, no. 11, pp. 3041–3049, Nov. 2001.
- [6] Y. Fukumoto, O. Shibata, K. Takayama, T. Kinoshita, Z. L. Wang, Y. Toyota, O. Wada, and R. Koga, "Radiated emission analysis of power bus noise by using a power current model of an LSI," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, Aug. 2002, vol. 2, pp. 1037–1042.
- [7] K. Nakamura, T. Toyota, O. Wada, R. Koga, and N. Kagawa, "EMC macro-model (LECCS-core) for multiple power-supply pin LSI," in *Proc. 2004 Int. Symp. Electromagn. Compat.*, pp. 493–496.

- [8] K. Iokibe, R. Higashi, T. Tsuda, K. Ichikawa, K. Nakamura, Y. Toyota, and R. Koga, "Modeling of microcontroller with multiple power supply pins for conducted EMI simulations," in *Proc. 2008 Electr. Des. Adv. Packag. Syst. Symp.*, Dec., pp. 135–138.
- [9] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Advances in Cryptology—CRYPTO* (ser. Lecture Notes Computer Science 1109), N. Koblitz, Ed., Springer-Verlag, 1996, pp. 104–113.
- [10] M. Joye, "Basics of side-channel analysis," in *Cryptographic Engineering*, Ç. K. Koç, Ed. New York, NY, USA: Springer-Verlag, no. 13, 2009.
- [11] P. Rohatgi, "Improved techniques for side-channel analysis," in *Cryptographic Engineering*, Ç. K. Koç, Ed. New York, NY, USA: Springer-Verlag, no. 14, 2009.
- [12] *Advanced Encryption Standard (AES)*, NIST FIPS publication 197, Nov. 2001.
- [13] Y. Hayashi, N. Homma, T. Sugawara, T. Mizuki, T. Aoki, and H. Sone, "Non-invasive EMI-based fault injection attack against cryptographic modules," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, Aug. 2011, pp. 763–767.
- [14] IEC, "Integrated circuits - Measurement of electromagnetic immunity, 150 kHz to 1 GHz - Part 3: Bulk current injection (BCI) method," IEC 62132-3 ed1.0, Sep. 2007. Available: http://webstore.iec.ch/webstore/webstore.nsf/Artnum_PK/38377
- [15] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks*. New York, NY, USA: Springer-Verlag, 2007, pp. 27–60.
- [16] Morita Tech and AIST, "Side-channel attack standard evaluation board (SASEBO)." (2007). [Online]. Available: <http://www.morita-tech.co.jp/SASEBO/en/>



Kengo Iokibe (M'06) received the B.S., M.S., and Ph.D. degrees in electrical and electronic engineering from Okayama University, Okayama, Japan, in 1997, 1999, and 2005, respectively.

He was a Research Associate in the Department of Communication Network Engineering, Okayama University, from 2000 to 2002. He is currently an Assistant Professor in the Department of Information and Communication Systems, Graduate School of Natural Science and Technology, Okayama University, where he focuses on security against side-

channel analysis attack on cryptographic devices, the design of the power distribution network of integrated circuits for power integrity, signal integrity and EMC, and EMC modeling of power converter circuits.

Dr. Iokibe is a member of the Institute of Electronics, Information and Communication Engineers and the Japan Institute of Electronics Packaging.



Tetsuo Amano received the B.S. degree in communication and network engineering from Okayama University, Okayama, Japan, in 2011, where he is currently working toward the M.S. degree in electronic and information systems engineering.

His research interests include the design methodology for security of cryptographic devices against side-channel analysis attack.

Mr. Amano is a student member of the Institute of Electronics, Information and Communication Engineers.



Kaoru Okamoto received the B.S. degree in communication and network engineering from Okayama University, Okayama, Japan, in 2012 where he is currently working toward the M.S. degree in electronic and information systems engineering.

His research interests include the modeling of cryptographic circuits for security estimates against side-channel analysis attack.

Mr. Okamoto is a student member of the Institute of Electronics, Information and Communication Engineers.



Yoshitaka Toyota (M'04) 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 at Georgia Tech as an Overseas Research Scholar of the Ministry of Education, Culture, Sports, Science and Technology (MEXT) of Japan. He is currently an Associate

Professor of the Graduate School of Natural Science and Technology, Okayama University, Okayama, Japan. His recent research interests include EMC design for high-speed digital systems.

Dr. Toyota is a member of the Institute of Electronics, Information and Communication Engineers, the Japan Institute of Electronics Packaging, and the Japan Society of Applied Physics.