Analysis on Equivalent Current Source of AES-128 Circuit for HD Power Model Verification

Kengo Iokibe, Kazuhiro Maeshima, Hiroto Kagotani
Yasuyuki Nogami, and Yoshitaka Toyota
Graduate School of Natural Science and Technology,
Okayama University
Okayama 700-8530, Japan
Email: iokibe@okayama-u.ac.jp

Tetsushi Watanabe
Industrial Technology Center of Okayama Prefecture
Okayama 701-1296, Japan
Email: watanabe@okakogi.jp

***Abstract*—We analyzed equivalent current source of cryptographic circuits implemented on a field programmable gate array (FPGA). The equivalent current source represented internal switching current behaviors in the cryptographic circuits during an Advanced Encryption Standard (AES) operation. In this work, the internal current was analyzed for extracting leakage functions and correlation coefficients from scatter diagrams of the Hamming Distance (HD) of AES intermediate values and the current magnitudes. The obtained leakage functions were confirmed a well-known assumption on the HD power model that magnitude of switching current due to transition of register states is proportional to HD of the register. The internal current was also investigated in terms of correlation with the HD model. Correlation coefficients increased as transforming the external power trace in the internal current because two types of noise were reduced by the transform; constant noise and overlap effect of successive rounds. The noise reduction inferred that the use of the internal current source would provide more precise verification of countermeasures.**

I. Introduction

It has become common today to digitize and exchange variety of information by modern sophisticated computers and the Internet, even sensitive information such as private and confidential information. Such situation is growing a threat of sensitive information being disclosed to third parties or public. To avoid the threat, sensitive information is often protected by modern cryptographies that generally require eavesdroppers tens of years for decryption even they use a super computer. Meanwhile, other threats are also rising in last two decades. A new cryptanalytic method was found in 1999 to decrypt a standardized encryption standard, data encryption standard (DES), by use of peripheral electric or electromagnetic variation caused by the switching noise of integrated circuits (ICs) [1]. The new method gave eavesdroppers capability to disclose a cryptographic secret key within an acceptable time, less than few hours. The new cryptanalytic method was named side-channel analysis and developed into more accomplished ones, such as the correlation power analysis (CPA)[2].

CPA uses a leakage function as a key clue as well as the switching noise. The leakage function is based on an assumption on relationship between the interesting encryption operation and the switching noise. The leakage function is called 'power model' since the switching noise was observed in terms of the power voltage fluctuation, or power bounce, on the power distribution network (PDN) of a cryptographic IC. One of the most popular power models is Hamming Distance (HD) model that generally assumes a linear relationship between the switching noise and the HD of intermediate values stored in a register memory tentatively. The assumption makes the HD model very simple and easy to apply to CPA, whereas it has been poorly confirmed because of difficulties in simulating the switching noise accurately with high-level circuit models and measuring the internal noise directly. Besides, there is a literature that arise a question on the linearity[3].

In this study, we investigate the linearity of the HD model in accordance with the internal switching noise. The internal switching noise is dynamic current that occurs as logic gates flip their states $0 \rightarrow 1$ or $1 \rightarrow 0$ then flows out of the IC. As the current flows out, it is conducted mainly along the power distribution network; consequently, it causes the power bounce and/or electromagnetic emanation. We have developed a method to identify the internal power current from on-board impedance and voltage bounce measurements[4]. By utilizing the method to a cryptographic IC, we identify the internal power current and extract power models.

II. Extraction of Leakage Function

In this study, we investigate the leakage function of CPA based on internal power current traces. The leakage function often employs an assumption that there is a linear relationship between magnitude of power current and the Hamming distance (HD) of intermediate values in the encryption operation[2]. The linear relationship was verified with a kind of digital circuit simulation or so-called power traces obtained outside of the targeted cryptographic IC. Such circuit simulation and power traces would not produce satisfactory verification because there is lack of information for accurate circuit simulations and also because external power traces involve effects of peripheral properties such as impedances of IC package and printed circuit board, and probe sensitivity. Those effects distort the external power traces. The internal power current is, on the contrary, so free from the peripheral properties that it is suitable for verification of the leakage function. Figure 1 illustrates the contrast between the internal power current and external power trace.

The internal power current is extracted from an external power trace as an equivalent current source[4]. The equivalent

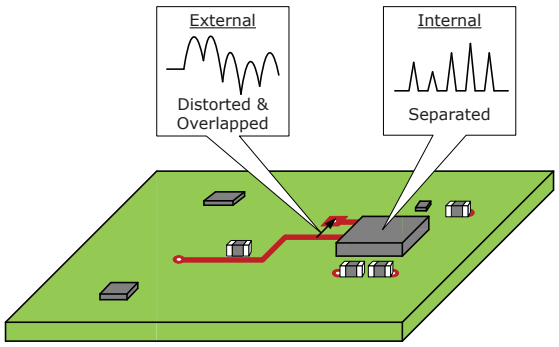


Fig. 1. Internal and external power traces

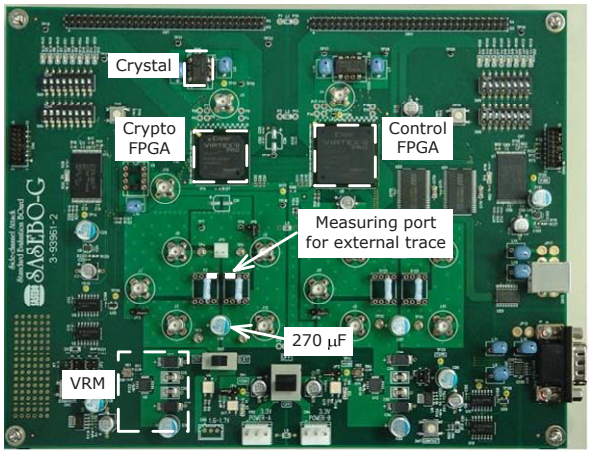


Fig. 2. SASEBO-G

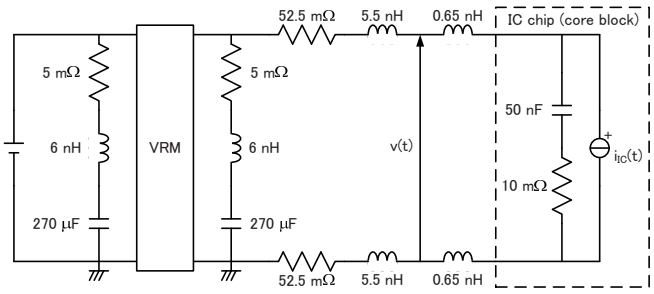


Fig. 3. Equivalent circuit of PDN for the core circuit of the cryptographic FPGA

current source represents dynamic switching current occurring inside the cryptographic IC during an execution of the encryption operation. The equivalent current source has been confirmed that its profile has good correlation with the encryption operation both in the time- and frequency-domain[4]. Furthermore, it produced estimation of the external power trace in outstanding accuracy[5]. These facts confirmed that the equivalent current source represented the internal power current accurately.

The relationship between HD and the internal power current will be figured in this study. Firstly, we identify the internal current source of an AES[6] circuit by the method shown in the literatures [4] and [5]. Secondly, the peak value of the internal current is plotted as a function of the HD for every AES round. Finally, regression formulas are determined as the leakage function by the least squares approximation on the HD vs. current peak value plots.

III. Cryptographic Module Under Test

A commercial printed circuit board developed for evaluating cryptographic devices, SASEBO-G[7], was used in this study. It has two FPGAs on it as shown in Fig. 2: one for operating encryption processes and the other for controlling the encryption operation. In the cryptographic FPGA, an AES-128 circuit was implemented on its core block. The core circuit was supplied with a 1.5 V DC bias through the PDN mainly composed of a voltage regulator module (VRM) and a decoupling capacitor. Detailed circuitry composition of the PDN is drawn with an equivalent circuit in Fig. 3 involving parasitic components as well as impedances of the VRM and decoupling capacitor. The equivalent circuit has a current source. It represents the internal power current of the AES-128 circuit.

In the following experiments, the cryptographic FPGA processed a standardized encryption algorithm, Advanced Encryption Standard (AES)[6], with a 128-bit key of $(2B\ 7E\ 15\ 16\ 28\ AE\ D2\ A6\ AB\ F7\ 15\ 88\ 09\ CF\ 4F\ 3C)_{16}$. The AES-128 encryption process was composed of 10 round-operations as well as a pre-operation including preparation of subkeys used in the round operations. Each operation began synchronized to the clock signal of 24 MHz that was supplied from the crystal oscillator mounted by the cryptographic FPGA, see Fig. 2.

TABLE I. Experimental Equipment

Instruments	Model, Manufacture, Specifications
Cryptographic Module	SASEBO-G, Toppan Printing
FPGAs	Virtex-II Pro xc2vp7 for encryption Virtex-II Pro xc2vp30 for control
Clock Freq.	24 MHz
DC Power Supply	PW16-5DP, KENWOOD
Volts	3.3 V
Current limit	1 A
Oscilloscope	54845A, Agilent Technologies
Bandwidth	1.5 GHz
Sampling	1 GS/s
Passive Probe	1161A, Agilent Technologies
Bandwidth	500 MHz
Controlling PC	Vostro1710, DELL
CPU	Celelon 550 2.0 GHz
RAM	2.0 GB

TABLE II. Cryptographic Algorithm

Item	Parameters
Algorithm:	AES-128
Secret Key	2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C
Plaintext	Incremented from 0 to 999

IV. Results

In this section, we identify the internal power current and look into it for investigating the HD model with respect to linearity.

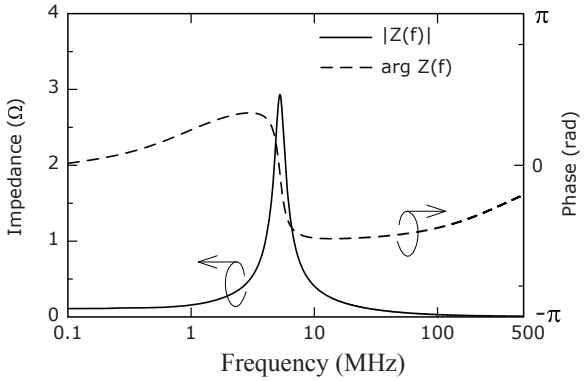


Fig. 4. Transfer impedance

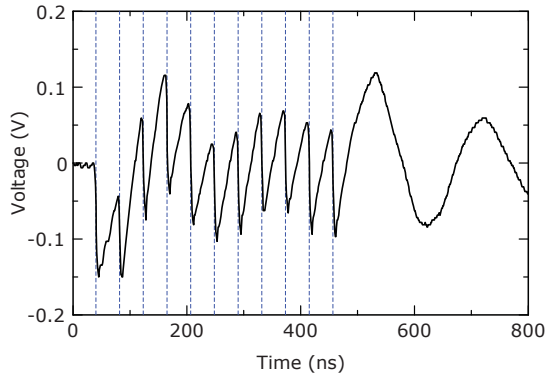
A. Identification of Internal Power Current

Waveforms of the internal power current were obtained for all the 1000 plaintexts. Firstly, external power traces were measured as $v(t)$ in Fig. 3 for all the plaintexts. Secondly, the frequency-domain expression of $v(t)$ was transformed into that of the internal power current $i_{\mathrm{IC}}(t)$ by multiplying the transfer impedance Z_{k} from $i_{\mathrm{IC}}(t)$ to $v(t)$. The transfer impedance was calculated with the equivalent circuit by a analog circuit simulator, AWG Microwave Office. as plotted in Fig. 4. As well as $v(t)$, an example of obtained internal current sources i_{IC} are shown in Fig. 5.

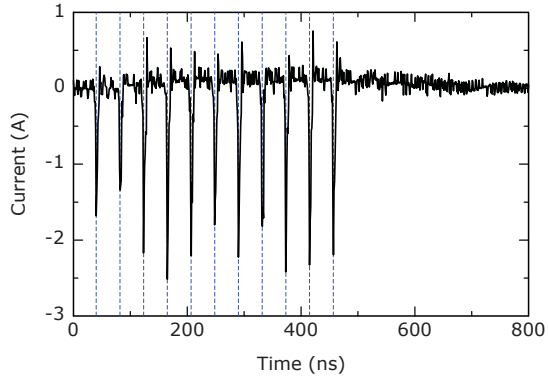
In the identified waveforms of internal power current, we found separated current peaks generated by round operations of AES-128. The current waveform was composed of 11 separated sharp peaks with a period of 41.7 ns, corresponding to the clock frequency, as shown in Fig. 5(b). In contrast, 11 successive peaks in the external power trace were not separated in Fig. 5(a). The separation of current means that the current pulse of a round is not affected from other rounds, whereas round pulses in $v(t)$ overlapped and started at different voltage levels. Such overlap in $v(t)$ had been already described in [8] which also noted that a low clock frequency led to separate voltage peaks in the power trace. These two peak separations in i_{IC} and $v(t)$ are looks similar. They are, however, different in a sense of network theory. Each peak in i_{IC} represents the temporal variation of internal power current of the round not involving effects of Z_{k}, whereas that in $v(t)$ affected by Z_{k} even if peaks are sufficiently separated.

B. Extraction of Leakage Function

A leakage function was extracted from the 1,000 identified waveforms of internal power current. In every current waveform, the peak value in every round was plotted as a function of HD. Since the AES-128 operation used a fixed secret key and known plaintexts, HD was also known for all rounds and for all the plaintexts. Such 2D plots were made for all rounds, as shown in Fig. 6(a), where 10 plot sets of all the 10 rounds were superposed. Every plot set produced a linear regression equation, dashed lines, by means of the least square approximation. Corresponding plots and regression equations were also obtained from $v(t)$, as shown in Fig. 6(b). Table III lists regression coefficients for all rounds, where a and b are the gradient and intercept of the regression equations, respectively.



(a) Measured external power trace $v(t)$



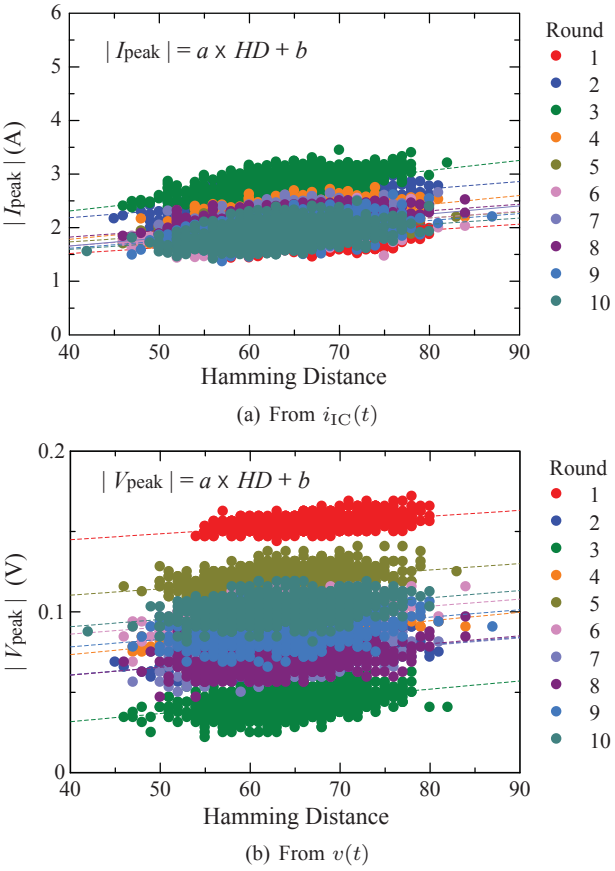
(b) Calculated $i_{\mathrm{IC}}(t)$ representing internal power current

Fig. 5. Identification of internal power current

r represents the correlation coefficient between the regression equation and their original plots. Suffixes i and v represents $i_{\mathrm{IC}}(t)$ and $v(t)$, respectively. The ranges of HD varied with round as the incrementing plaintext set was used; from 54 to 80 for the 1st round (red) and from 46 to 82 for 3rd round (green) for instance.

The use of the internal power current improved leakage functions in two aspects. The first one is the reduction of constant noise. The scatter plots in Fig. 6(b) vertically ranged widely from 5 to 55 V and they rather low overlapped each other. On the contrary, all scatter plots in Fig. 6(a) overlapped highly except for the first round. This high overlap means that the internal current is almost free from the constant noise independent with the cryptographic operation. The other is the reduction of previous round effects. As a characteristic of the AES algorithm, the algorithm provides no correlation between behavior of power current in previous rounds and HD of the interesting round. This means that the power current occurred in previous rounds reduces correlation coefficients in the interesting round. In other words, the correlation coefficients increase with the internal power current because of its separation of round current. As listed in TABLE III and also illustrated in Fig. 7, correlation coefficients, actually, enlarged with $i_{\mathrm{IC}}(t)$ except for the 1st and last (10th) rounds. The identification of internal power current, thus, can allow us to verify the leakage function with high reliability.

The HD leakage function seemed to have linearity. As far as looking into both graphs in Fig. 6, all rounds had the trends



(a) From $i_{\mathrm{IC}}(t)$

(b) From $v(t)$

Fig. 6. Extraction of leakage function

TABLE III. REGRESSION COEFFICIENTS

Round	a_i (mA)	b_i (A)	r_i (%)	a_v (V)	b_v (V)	r_v (%)
1	8.6	0.84	36	0.12	41	47
2	11	1.4	48	0.15	12	42
3	17	1.4	50	0.16	2.7	41
4	15	1.0	47	0.17	16	43
5	11	1.3	46	0.13	29	33
6	13	1.2	44	0.14	21	36
7	16	1.1	42	0.15	13	37
8	13	1.4	47	0.16	12	38
9	14	1.2	44	0.15	18	36
10	13	1.3	36	0.14	22	38

of linear relationship between the power current and HD. The linearity, actually, has been investigated in a limited range of HD between 45 and 85 and might lose its credibility with far small or far large HDs. Even so, such far small and large HDs seldom happen. The linearity on the leakage function is, therefore, a reasonable and efficient assumption for CPA.

V. CONCLUSION

Regarding the correlation power analysis (CPA) on cryptographic devices, a leakage function was investigated with waveforms of internal power current. The leakage function of an AES-128 circuit was extracted from the internal current waveforms instead of the external power traces. The internal power current was identified based on on-board measurements. It had been confirmed to represents the behavior of dynamic

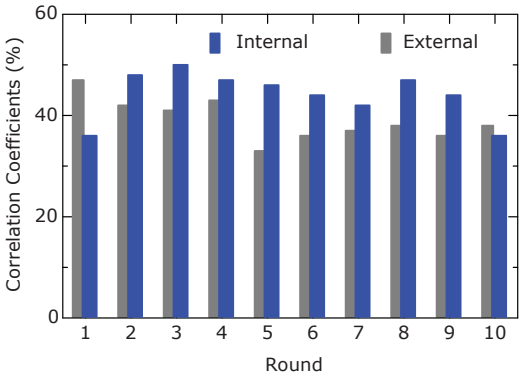


Fig. 7. Changes in correlation coefficient

switching current occurring during the AES-128 operation implemented on an FPGA very well. With such internal power current, leakage functions were extracted as a linear function of Hamming Distance (HD) for all AES-128 rounds. Extracted leakage functions indicated linearity in a range of HD between 45 and 85. We also found that investigating the leakage function based on the internal power current made an advantage in two aspects: reduction of constant noise and that of previous round effects. Those noise reductions can allow to verify the leakage function with high reliability.

ACKNOWLEDGMENTS

The authors would like to thank the Strategic Information and Communications R&D Promotion Programme (SCOPE) from the Ministry of Internal Affairs and Communications (MIC) for its financial support. They would also like to acknowledge Ms. Kana Shimizu and Mr. Nobuhiro Tai for their generous contribution to this work.

REFERENCES

[1] P. C. Kocher, J. M. Jaffe, and B. C. Jun, "Differential power analysis," in *Advances in Cryptology – CRYPTO ' 99*, ser. LNCS, M. Wiener, Ed. Springer-Verlag, 1999, vol. 1666, pp. 388–397.

[2] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," *CHES 2004*, pp. 16–29, 2004.

[3] D. Kamel, M. Renauld, D. Flandre, and F.-X. Standaert, "Understanding the limitations and improving the relevance of spice simulations in side-channel security evaluations," in *PROOFS 2013 (Security Proofs for Embedded Systems)*, Santa-Barbara, California, August 2013, pp. 69–82.

[4] K. Iokibe, T. Amano, K. Okamoto, and T. Watanabe, "Improvement of linear equivalent circuit model to identify simultaneous switching noise current in cryptographic integrated circuits," *International Symposium on Electromagnetic Compatibility 2011*, pp. 834–839, August 2013.

[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.*, 2013 (to be published).

[6] *Advanced encryption standard (AES)*, NIST FIPS publication 197, Nov. 2001.

[7] AIST. Side-channel attack standard evaluation board (sasebo). [Online]. Available: http://staff.aist.go.jp/akashi.satoh/SASEBO/en/index.html

[8] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks —Revealing The Secrets of Smart Cards—*. New York: Springer, 2007, ch. 3, pp. 27–60.