# A Fast Power Current Analysis Methodology using Capacitor Charging Model for Side Channel Attack Evaluation

Daisuke Fujimoto, Makoto Nagata
Graduate School of System Informatics , Kobe University
Email: fujimoto@cs26.scitec.kobe-u.ac.jp
nagata@cs.kobe-u.ac.jp

Toshihiro Katashita, Akihiko Sasaki,
Yohei Hori, Akashi Satoh
Research Center for Information Security,
National Institute of Advanced Industrial Science and Technology

***Abstract*—Fast power current analysis with capacitor charging model achieves 50x acceleration in derivation of more than 10,000 power current traces required for CPA, in comparison with conventional full transistor level analysis. Simulation based CPA clearly compared the strength of correlation among key bytes as well as the level of correlation among different types of AES modules. The accuracy of analysis of side channel attack is proven through remarkable consistency with silicon measurements of AES modules in a 65 nm CMOS technology.**

## I. Introduction

Side-channel attacks (SCAs) such as simple power analysis (SPA), differential power analysis (DPA), and correlation power analysis (CPA) are known to be quite powerful to break security of VLSI implementation of cryptographic algorithms. [1][2][3]. A secret key can be revealed by statistically analyzing simply captured power traces of a cryptographic LSI. Even using standard cipher algorithm whose logical security has been well evaluated, physical security of hardware implementation [4] against SCAs is hard to evaluate unless they are actually embodied in an IC chip.

In order to evaluate physical security of cryptographic LSIs against SAC in advance to their fabrication, this paper proposes a fast and high accurate power current simulation methodology using our original capacitance charging model extracted from post-layout data. The proposed method can be easily integrated to a design flow of VLSI systems, and it is applicable for any CMOS circuits. Therefore, physical security of various logical structures and countermeasures of cipher algorithms against various side channel attacks can be evaluated to choose appropriate hardware architecture before the LSI fabrication.

We developed a cryptographic LSI using a 65-nm CMOS standard library, and conducted CPAs on four types of AES circuits in the LSI. We also performed CPA using simulated power traces for the same AES circuits using our capacitance charging model extracted from the post layout data. Then the results were compared to demonstrate efficiency and accuracy of our methodology.

This paper is organized as follows. Section II briefly explains CPA on the AES circuit. Section III defines a power current simulation methodology of CMOS digital circuits, and then proposes a simulation flow of CPA on AES. The comparison of the CPA results between the simulation and the measurement will be discussed in Section IV. Finally, a brief conclusion will be given in Section V.

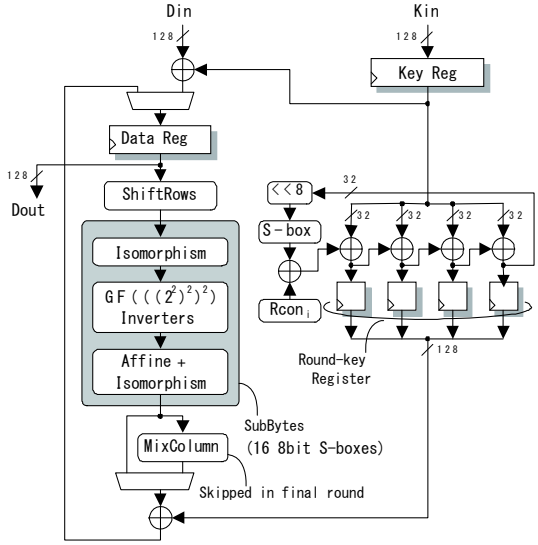



Fig. 1. Block diagram of AES cryptographic module

## II. Correlation power analysis (CPA)

Power consumption of a cryptographic module is considered linearly proportional to the number of transitions in a data register during the execution of a cipher algorithm. We have chosen Advanced Encryption Standard, AES, as a test vehicle of CPA simulation. Figure 1 shows a block diagram of AES encryption circuit.

The final round of AES encryption is generally focused in the correlation power analysis (CPA) procedure [2][3]. MixColumns, that is a 32-bit word-oriented function, is skipped only at this round. Each 8-bit data block at the S-box boundary is independently processed.

An 8-bit value of k ($0 \leq k \leq 255$) is assumed for each sixteen 8-bit partial keys in the final round. Then, the Hamming distance, $H_k$ ($0 \leq H_k \leq 8$) of the data transition in each 8-bit register block at the 8-bit S-box boundary is calculated from the cipher text that is obtained at the output. A set of the Hamming distance among 256 potential key values is derived per each S-box.

On the other hand, $N$ power traces, $W_i(t)$ (0 ≤ i ≤ N-1) are measured with $N$ different cipher texts for the time duration of encryption procedures. This gives a chance to obtain a set of the Hamming distances of $H_{i,k}$ among 256 partial key candidates with respect to the $N$ traces.

The correlation coefficients, $corr_k(t)$, between $H_k$ and $W_i(t)$, are computed from (1), where $\overline{W(t)}$ and $\overline{H_k}$ are the average values of $W(t)$ and $H_k$, respectively. Finally, the 8-bit partial key with a particular value of $k$, that achieves the largest value of $corr_k(t)$, is considered as the secret key.

$$corr_k(t) = \frac{cov(W(t), H_k)}{\sqrt{var(W(t))}\sqrt{var(H_k)}} \quad (1)$$

$$cov(W(t), H_k) = \frac{1}{N}\sum_{i=1}^{N}(W_i(t) - \overline{W(t)})(H_{k,i} - \overline{H_k})$$

$$cov(W(t)) = \frac{1}{N}\sum_{i=1}^{N}(W_i(t) - \overline{W(t)})^2$$

$$cov(H_k) = \frac{1}{N}\sum_{i=1}^{N}(H_{k,i} - \overline{H_k})^2$$

## III. CPA Simulation Flow

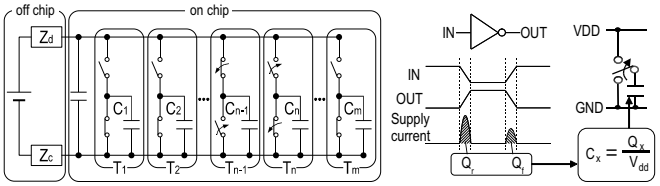
### A. Power current simulation of CMOS digital circuits

In general, CMOS digital circuits are composed of logical gate leaf cells and designed through a standard logic and physical synthesis flow. We assume that cryptographic modules also follow to them in realization with CMOS technologies, specifically for consumer products.

Power current simulation of a digital circuit needs to solve a full transistor level netlist or an equivalent circuit network that involves the same number of equivalent current source models as logical gate cells in a circuit. A current source in parallel with resistive-capacitive series shunts between Vdd and Vss is often used as a noise source model [5][6].

In contrast, we have proposed a time series divided parasitic capacitance (TSDPC) model shown in Fig. 2 [7], where a mass of logic gates that switch approximately within a narrow time frame is substituted by a single capacitor that is inserted between local Vdd and Vss and to be charged during that time frame. The size of capacitor is equal to the total parasitic capacitances to be charged during the corresponding time frame in a digital circuit.

Dynamic power supply current is simulated through successive charging of TSDPC models in this representation, as outlined in Fig. 2(a). The switched capacitor stages in a row are charged one by one at the corresponding timing of $T_1, T_2, ..., T_{n-1}, T_n, T_{n+1}$, ..., and $T_m$, respectively. When the capacitor $T_n$ is charged, the previously charged capacitor $T_{n-1}$ is discharged. This simplification drastically reduces the size of a circuit network to be solved by a circuit simulator and thus accelerate power current simulation. It is also noted that the equivalent circuit of Fig. 2 naturally represents voltage variation in power delivery and substrate networks, namely, power supply and substrate noises.




(a) (b)

Fig. 2. TSDPC modeling for power current simulation of CMOS digital circuits. (a) Equivalent circuit expression by capacitance charging model and (b) derivation of capacitance of standard logic cell

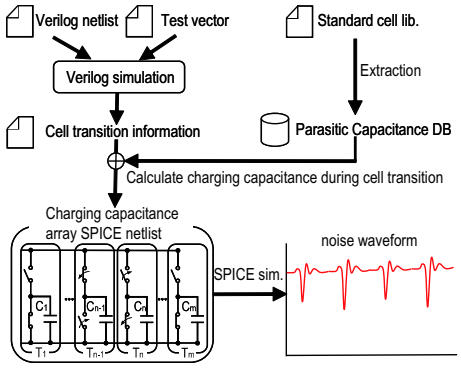



Fig. 3. TSDPC modeling of cryptographic core

TSDPC model can be generalized for any CMOS digital circuit [8]. The total energy of $C_{load}$ * $Vdd^2$ is drawn from a power source when a logic gate cell toggles, where $C_{load}$ is a total load capacitance of the cell. The size of $C_{load}$ is characterized for every cell in a digital circuit, as shown in Fig. 2(b). The extraction of $C_{load}$ is detailed in Ref. 7. A single capacitor, $T_n$, is then determined as the sum of $C_{load}$ according to toggle records of each time frame. The number of capacitor stages of TSDPC model can increase to capture long-time noise waveforms for frequency-component analysis.

### B. Power current simulation of cryptographic module

power supply current of a cryptographic module can also be captured by the TSDPC models. Since the capacitance is calculated from gate-level operation of cryptographic processing, as shown in Fig. 3, the simulated power current is considered to naturally involve information of ciphers. Since the logical activity of a digital circuit varies with operands, TSDPC models of a cryptographic module need to be updated whenever binary codes are altered with regard to plain texts and secret keys.

A cryptographic module is embedded in a silicon chip and typically assembled on an FR-4 board. Power and ground

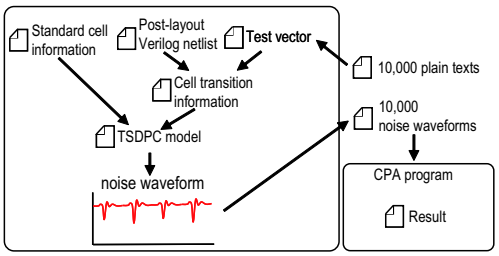



Fig. 4. Simulation based CPA flow of post-layout cryptographic core

traces hence include impedance parasitic to a power delivery network (PDN). This brings about filtering or enhancement of frequency components of power current. The impedance network of PDN can be extracted by a full wave simulator and connected in series to TSDPC models, as defined as "off chip Zd" in Fig. 2(a).

### C. Correlation power analysis using power current simulation

Correlation of power and cipher is a source of vulnerability against side channel attack. When specific clock cycles of cryptographic processing are designated for such as an update of cipher codes, power supply current of that duration can be used for correlation power analysis (CPA).

The final round of AES processing, discussed in Sect. II, is located at the 10th clock cycles from the beginning of the processing. Figure 4 depicts the flow of CPA against AES. Power current waveforms in the 10th clock cycle are acquired by simulation or by measurements and then correlated with the Hamming distance of the date register, according to (1). The highest possible value is statistically determined for each of 16 bytes of the secret key.

In order to accomplish CPA flow by simulation, TSDPC models of 10 clock cycles are prepared for an AES hardware module with a set of 128 bit plain texts and a 128 bit secret key. Since the number of plain texts reaches as many as 10,000 for succeeding the attack, high efficiency of power current simulation is strongly demanded.

## IV. Experimental results

### A. Test chip

A variety of AES hardware modules with different realization of AES cryptographic algorithm is actually fabricated on a test chip of Fig. 5 with a 65 nm CMOS technology. The resistance of AES modules against CPA is evaluated in this paper, comparing four different types of S-box (Fig. 1) that are listed in Tab. 1. They are named as "Composite S-box," "PPRM3 S-box," "Table S-box," and "PPRM1 S-box, " given in the order of the number of logic gate instances.

### B. Power current measurements

Power current measurements are supported by SASEBO board [9] of Fig. 6(a) and performed on the test chip with the experimental setup of Fig. 6(b). Power current flowing through power pin (Vdd) of the test chip is terminated through an 1-ohm resistor on SASEBO board, and voltage waveforms across

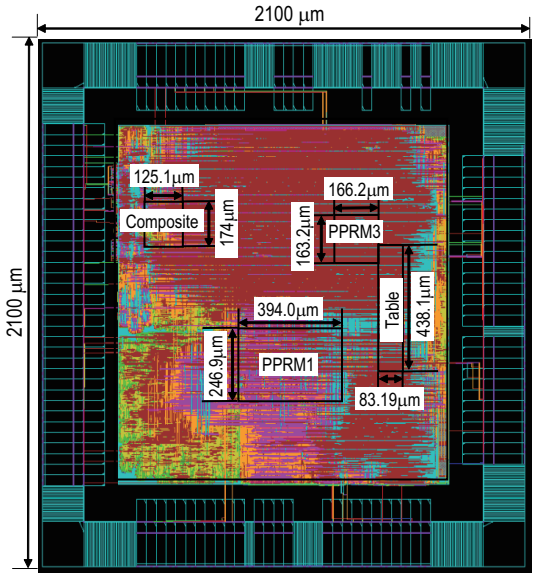



Fig. 5. 65 nm CMOS chip layout floorplan including AES modules with different S-box realization

TABLE I
Implementation of AES cryptographic modules with different S-box realization

| S-box | Silicon area[$\mu m^2$] | # of gates |
|---|---|---|
| Compsite | 21,852 | 53,417 |
| PPRM1 | 27,110 | 66,249 |
| Table | 36,470 | 84,512 |
| PPRM3 | 97,306 | 235,389 |

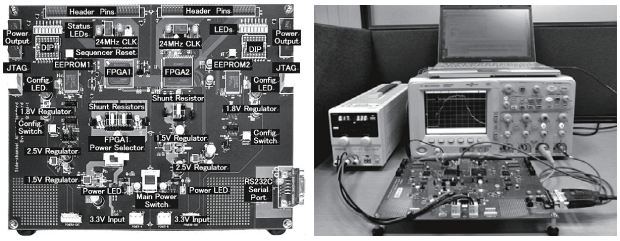
the resistor are acquired by an oscilloscope. Power current waveforms for more than 10,000 plain texts by SASEBO measurement are prepared for comparison of CPA analysis with TSDPC simulation.

### C. Power current simulation

Power current simulation uses TSDPC modeling, defined for the duration of AES operation with a given plain text and secret key. The time resolution of 100 ps (= $T_{n+1}$ - $T_n$) is chosen among capacitor stages of the TSDPC model. The entire equivalent circuit including on-chip TSDPC models and off-chip PDN impedance models is simulated with a SPICE simulator. TSDPC models are individually created for every AES modules and more than 10,000 plain texts.

Figure 7 compares power current waveforms of TSDPC simulation and SASEBO measurement. The waveforms involve a single clock cycle for latching a plain text and subsequent 10 clock cycles for AES cryptographic processing. A cipher is output at the 11th clock cycle, immediately after the final round of AES computation. Magnified power current waveforms during the final round are also shown.

Both waveforms clearly exhibit peak drops in the beginning of every clock period. This is naturally due to power current consumption by logical operation of gate elements in an AES module, that are concentrated right after the rise edge of clock




(a) (b)

Fig. 6. (a) SASEBO test board for side-channel attack experiments and (b) experimental setup.

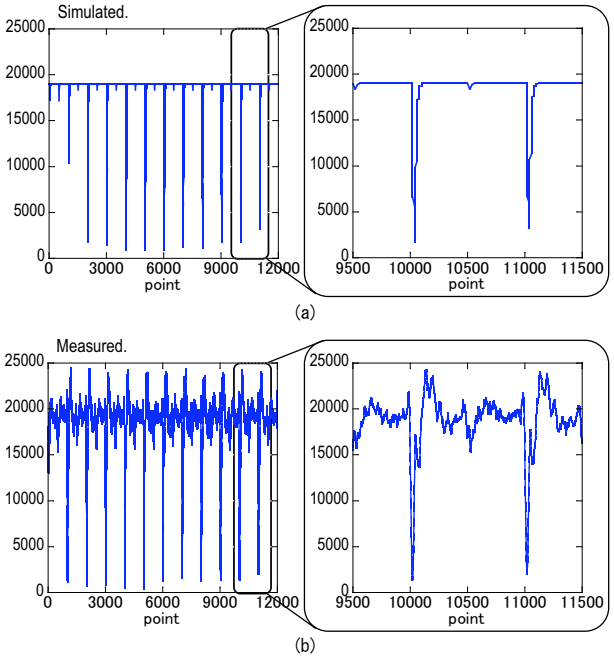



Fig. 7. Comparison of power supply current by (a) TSDPC simulation and (b) SASEBO measurements (voltage generated on 1 ohm termination resistor). Magnified plots are also shown)

signal, Fclk. The major difference between simulation and measurements is found in the shape of peak waveforms, those results from the filtering effect by off-chip PDN impedances. The simulation model of Fig. 2 includes a simplified PDN with lumped inductance (L), resistance (R), and capacitance (C), assuming a typical wire bonded assembly. On the other hand, the measurements involve distributed impedances parasitic to wirings within a chip, multiple bond wires and lead frames in a package, and traces and decoupling elements on the SASEBO board. It is indeed of interest that the observed difference in peak waveforms will not impact CPA results, since the correlation of peak heights with the Hamming distance is essential.

Cost of simulation is summarized in Tab. 2. Power current simulation is obviously accelerated for approximately 50x by

TABLE II
COST OF SIMULATION

| Simulation model | S-box realization | | | |
|---|---|---|---|---|
| | Composite | PPRM3 | Table | PPRM1 |
| Full Tr. netlist* | 1288 s | 1076 s | 938 s | 5734 s |
| TSDPC model** | 21 s | 22 s | 20 s | 130 s |
| Acceleration | 61.3 x | 44.1 x | 48.9 x | 46.9 x |

Simulated by *HSIM, **HSPICE.

using TSDPC models, in comparison with the case when a full transistor level netlist of an AES module is simulated even with a fast SPICE simulator. It is noted that simulation of CPA is infeasible with the full transistor netlist, where more than 10,000 power current traces are required.

The difference will further extend when parasitic wiring capacitances are involved in the transistor level netlist. TSDPC model already incorporates their effect on delay and power in the model creation procedure, since standard delay format (SDF) is annotated in the gate level simulation.

## V. CPA SIMULATION AND MEASUREMENTS

The correlation of power current with the Hamming distance is calculated for each of 256 possible values in a key byte according to (1), and the evolution of correlation is evaluated with the number of power current traces. Figure 8 compares simulation and measurement performed in “Composite S-box” version of AES module. It is obviously shown that the black bold line, showing the correlation value of the 0th byte of a secret key with the correct number, becomes isolated from the other candidates when the number of traces used for correlation becomes larger than 2000.

Similar analyses were performed on the other types of AES modules, as plotted in Figs. 9, 10, and 11. Key bytes are clearly identified for every AES modules, and more interestingly, “PPRM1 S-box” and “Table S-box” versions leak secret keys faster than the others.

These results indicate that the secret key of AES module might potentially be disclosed only with a feasible number

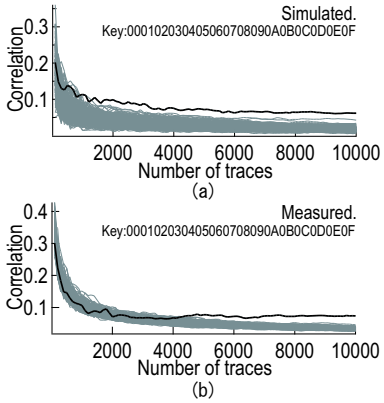



Fig. 8. Correlation values of each key candidate that are evolved along with the number of traces. black bold line shows case with correct key. (a) Simulation and (b) measurements are compared for AES module with “Composite S-box”

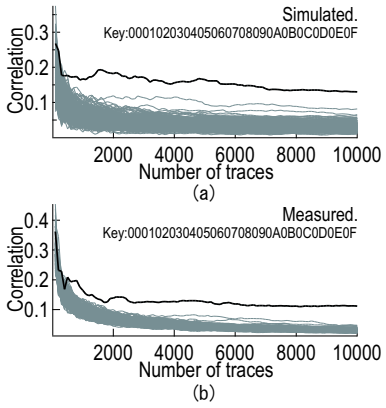



Fig. 9. Correlation values of each key candidate that are evolved along with the number of traces. black bold line shows case with correct key. (a) Simulation and (b) measurements are compared for AES module with "PPRM3 S-box"

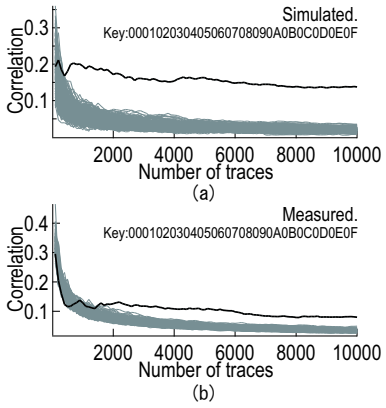



Fig. 10. Correlation values of each key candidate that are evolved along with the number of traces. black bold line shows case with correct key. (a) Simulation and (b) measurements are compared for AES module with "Table S-box"

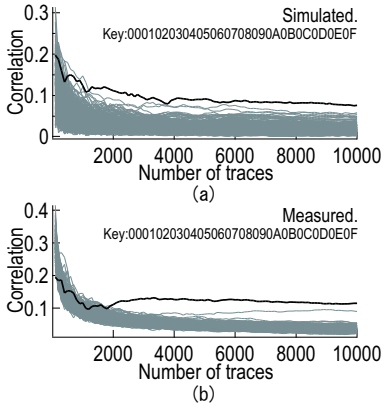



Fig. 11. Correlation values of each key candidate that are evolved along with the number of traces. black bold line shows case with correct key. (a) Simulation and (b) measurements are compared for AES module with "PPRM1 S-box"

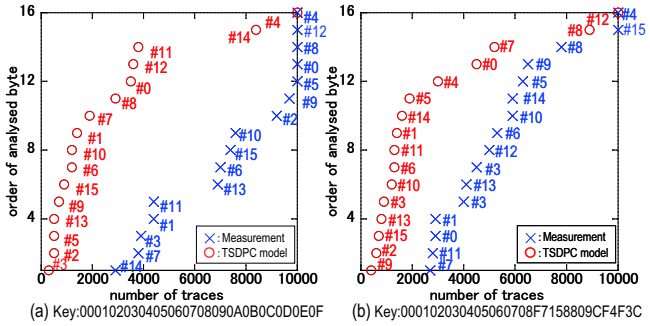



Fig. 12. CPA against AES module with "composite S-box". Number of traces needed for achieving complete power correlation per each byte unit of a correct key. Simulation and measurements are compared for test cases with different correct keys

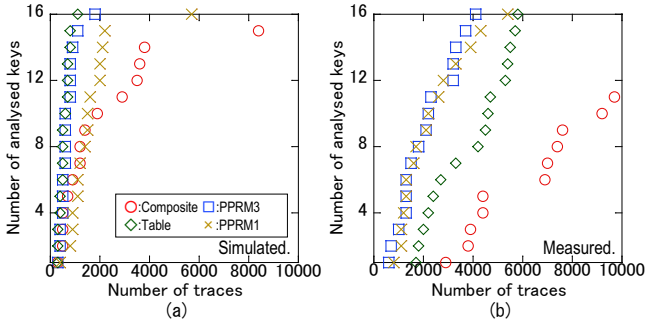



Fig. 13. CPA against AES modules with different S-box realization. Number of traces needed for achieving complete power correlation per each byte unit of a correct key. (a) Simulation and (b) measurements are compared among "composite S-box", "pprm1 S-box", "pprm3 S-box", and "table S-box."

of power current traces. Since this trend of correlation is outstandingly matched among simulation and measurement, the TSDPC modeling approach is considered quite powerful for the simulation-based post-layout verification of SCA resistance of cryptographic modules in standard CMOS digital realization.

The speed of correlation is visualized in Fig. 12, where the number of power current traces needed for each key bytes of "Composite S-box" version of AES is plotted. TSDPC simulation exhibits the higher speed compared to SASEBO measurements, without depending on the bit codes of a secret key. Figure 13 also compares the speed of correlation among different S-box realization of AES modules. "Composite S-box" version experiences the slowest correlation and some key bytes are not resolved with up to 10,000 traces, while "Table S-box" exhibits the fastest disclosure of all key bytes. It is thus considered the highest resistance against SCA is provided by "Composite S-box" among these four particular AES modules, while the highest vulnerability is given by "Table S-box."

There are physical mechanisms that weaken or conceal the correlation. The highest rank of correlation among 256 possible values in each key byte is plotted against the number of traces, shown in Fig. 14. The trend is differently seen for the specific 8th key byte that is not resolved even with 10,000

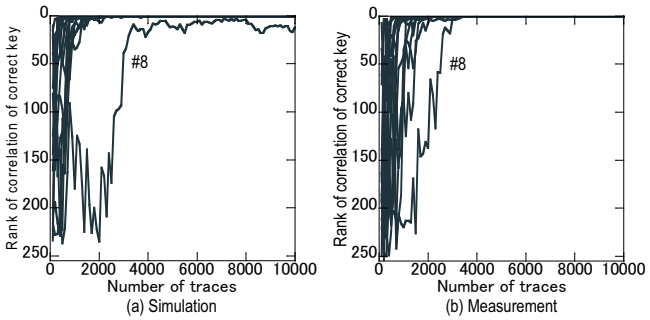



Fig. 14. Rank of correlation of each key bytes as a function of number of traces

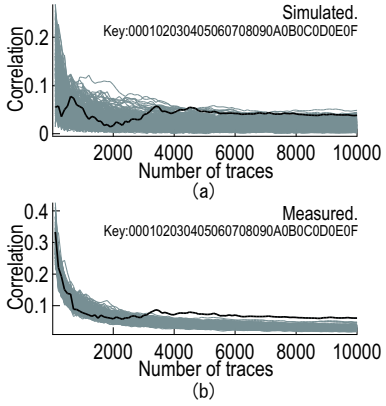



Fig. 15. Correlation values of each key candidate that are evolved along with the number of traces, in the case where correct key are in obscurity of correlation. (a) Simulation and (b) measurements

traces. The correlation plot of this particular key byte is shown in Fig. 15, where the correlation of the correct key value does not become apparent. TSDPC simulation accurately captures this trend, and more importantly, CPA of the key bytes that was resolved exhibits a faster trend of correlation in simulation, compared with measurement. Therefore, simulation based CPA with TSDPC models provides a practical opportunity of exploration in the design space toward the higher resistance of a cryptographic module.

We can conclude from those experimental results that TSDPC simulation involves necessary information of power current components that exhibit high correlation with logical activities of AES cryptographic processing. The proposed analog simulation of power supply current includes the interaction with impedance networks parasitic to PDN, although the expression of PDN is much simplified for the purpose of pursuing the adaptability to CPA in the present paper. In future, PDN models will be connected in detail for more accurate wave shapes of power current traces, that will elucidate the mechanisms behind the observed slow correlation in measurements. This possibility of simulation in TSDPC modeling is a major advantage over logical power consumption analysis that is used in a digital design flow.

## VI. Conclusion

Correlation power analysis (CPA) becomes feasible with the proposed fast power current analysis with a unique capacitor charging modeling, namely, TSDPC modeling technology. The derivation of power supply current traces reaches 50x acceleration in comparison with conventional full transistor level analysis, that enables to simulate more than 10,000 traces per design of a cryptographic module typically required for CPA.

The accuracy of power current analysis is high enough to reveal in-depth correlation processes of CPA among different hardware implementation of cryptographic algorithms. A variety aspects of CPA such as the evolution of correlation coefficients with the number of power current traces, the speed of correlation for key bytes as well as for different logical realization, and the obscurity of correlation due to physical processes, are quantitatively evaluated and shown to be well consistent with measurements performed on AES modules in a 65 nm CMOS technology.

The proposed technique will be pursued to establish the design flow of cryptographic hardware toward high resiliency against side channel attack.

## Acknowledgment

This research is partly supported by Strategic International Cooperative Program (Joint Research Type), Japan Science and Technology Agency (JST).

## References

[1] P. Kocher, et al , “Differential power Analysis,” in CRYPTO 1999, LNCS 1666, pp. 388-397, 1999.
[2] E. Brier, et al., “Correlation Power Analysis with a Lekage Model,” in CHES 2004, LNCS 3156, pp. 16-29, 2004.
[3] S. Mangard, et al., “Power Analsysis Attacks,” Springer Science Business Media, LLC, 978-0-387-30857-9, 2007.
[4] D. Hwang, K. Tiri, A. Hodjat, B-C. Lai, S. Yang, P. Schaumount, I. Verbauwhede, “AES-Based Security Coprocessor IC in 0.18-um CMOS With Resistance to Differential Power Analysis Side-Channel Attacks,” IEEE J. Solid-State Circuits, vol. 41, no. 4, pp. 781-791, Apr. 2006.
[5] H. Tsujikawa, K. Shimazaki, S. Hirano, M. Ohki, T. Yoneda, H. Benno, “A Design Methodology for Low EMI-Noise Microprocessor with Accurate Estimation-Reduction-Verification,” in Proc. CICC 2002, pp. 299-302, 2002.
[6] M. Badaroglu, G. Van der Plas, P. Wembacq, S. Donnay, G. G. E. Gielen, H. J. De Man, “SWAN: High-Level Simulation Methodology for Digital Substrate Noise Generation,” IEEE Trans. VLSI Systems, vol. 14, no. 1, pp. 23-33, Jan. 2006.
[7] M. Nagata, J. Nagai, K. Hijikata, T. Morie, A. Iwata, “Physical Design Guides for Substrate Noise Reduction in CMOS Digital Circuits,” IEEE J. Solid-State Circuits, vol. 36, no. 3, pp. 539-549, Mar. 2001.
[8] T. Matsuno, D. Kosaka, M. Nagata, “Modeling of power noise generation in standard-cell based CMOS digital circuits,” IEICE Trans. Fundamentals, vol. E-93A, no. 2, pp.820-826, Feb. 2009.
[9] “Side-channel Attack Standard Evaluation BOard (SASEBO),” RCIS, AIST, Japan. http://www.rcis.aist.go.jp/special/SASEBO/index-en.html.