Evaluation of On-chip Decoupling Capacitor's Effect on AES Cryptographic Circuit

Tsunato Nakai
Graduate School of Science and Technology, Ritsumeikan University
1-1-1 Nojihigashi, Kusatsu, Shiga, 525-8527, JAPAN
e-mail: ri0004pk@ed.ritsumei.ac.jp

Mitsuru Shiozaki
Research Organization of Science and Technology, Ritsumeikan University
1-1-1 Nojihigashi, Kusatsu, Shiga, 525-8527, JAPAN
e-mail: mshio@fc.ritsumei.ac.jp

Takaya Kubota
Research Organization of Science and Technology, Ritsumeikan University
1-1-1 Nojihigashi, Kusatsu, Shiga, 525-8527, JAPAN
e-mail: kubota-t@fc.ritsumei.ac.jp

Takeshi Fujino
Department of Science and Technology, Ritsumeikan University
1-1-1 Nojihigashi, Kusatsu, Shiga, 525-8527, JAPAN
e-mail: fujino@se.ritsumei.ac.jp

Abstract – Power Analysis (PA) attack and Electromagnetic Analysis (EMA) attack reveal a secret key on cryptographic circuits by measuring power variation and electromagnetic radiation during the cryptographic operations, respectively. Inserting decoupling capacitors reduces a PA leak; however, a resistance against EMA attack is not well-known. We fabricated Advanced Encryption Standard (AES) cryptographic chips with and without on-chip decoupling capacitors, and evaluated the resistance against PA and EMA attack. This paper presents that the on-chip decoupling capacitors make vulnerable to EMA attack using Hamming-weight model.

I. Introduction

Recently, the number of electronic devices with the cryptographic circuit such as IC cards has increased in an information-oriented society. On the other hand, side-channel attack, which reveals a secret key on cryptographic circuits by measuring consumed power and / or electromagnetic radiation variation during the cryptographic operations, is attracting more attentions. Differential Power Analysis (DPA) attack proposed by Kocher et al. in 1999 [1] and Correlation Power Analysis (CPA) attack proposed by Brier et al in 2004 [2] are well-known as the side-channel attack using the measured power variation, called Power Analysis (PA) attack [3]. Electromagnetic Analysis (EMA) attack proposed by Grandolfi et al. in 2001 [4] is the side-channel attack using the measured electromagnetic radiation. Both the PA and EMA leaks are caused by consumption current on cryptographic circuits. Therefore, it has been considered that the countermeasure against PA attack is also effective against EMA attack.

There is a study which reduces PA leaks by inserting decoupling capacitors into the printed board [5], but the effect on EMA leaks has never been unknown. Thus, this paper focuses on EMA attack using near-surface electromagnetic field, and investigates how on-chip decoupling capacitors have an influence on EMA attack. We fabricated advanced encryption standard (AES) cryptographic chips with and without on-chip decoupling capacitors. And, each resistance against PA and EMA attack is evaluated, and the attacking results are compared for the first time.

The paper is organized as follows. In section II, the fabricated chip, evaluation (attack) methods and experimental environments are described. Then, the results between AES chips with and without on-chip decupling capacitors are compared in section III. Section IV summarizes this paper.

II. Fabricated AES Chips and Experimental Environment

A. *Fabricated AES Cryptographic Chip*

Two AES chips were fabricated with a 0.18μm CMOS technology to investigate an effect of on-chip decoupling capacitors on PA and EMA attack. The layouts of these AES chips are identical except for on-chip decoupling capacitors. Fig. 1 shows a picture of the fabricated AES chip. The chip size is 2.5 mm x 2.5 mm. The chip includes two AES cryptographic circuits in which the SubBytes transformation circuit is implemented using a lookup table (AES-TBL) and composite field arithmetic (AES-CMP). The AES-CMP is smaller area, lower power and higher resistant against PA attack than the AES-TBL [6]. Fig. 2 shows the layout of the fabricated chip and you can find out where each encryption / decryption circuit is placed. The AES-TBL is placed at upper left of the chip. The AES-CMP is lower right of the chip. In particular, the encryption circuits (ENC), which are the attack targets in this paper, are placed at the corners of the chip. In the AES with on-chip decoupling capacitors, all filler cells used in Placement and Route are replaced with filler cells with decoupling capacitors. And, MOS capacitors are inserted along the power supply line on the chip. The total capacitance was 1 nF approximately.

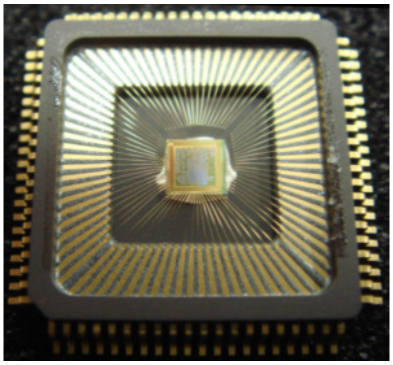


Fig. 1. The photograph of the fabricated AES chip

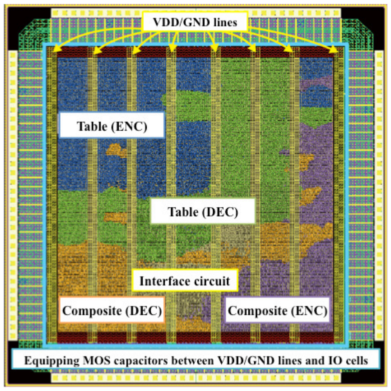
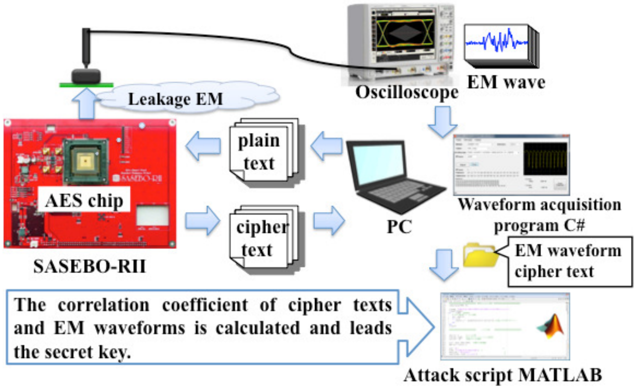


Fig. 2. Layout of the AES chip

B. *Attacking Method*

In this study, correlation power analysis (CPA) and correlation electromagnetic analysis (CEMA) attack are used to investigate an effect of on-chip decoupling capacitors. The CPA is an attacking method to exploit a secret key by analyzing the correlation coefficient between power variation and intermediate data during encryption operation. The CEMA is based on the correlation between electromagnetic radiation and intermediate data. In general, these two methods are more powerful attacking methods than the conventional DPA (Differential Power Analysis) and DEMA (Differential Electromagnetic Analysis). Fig. 3 shows an illustrated procedure of the CEMA attack. It is carried out as follows:

1. The AES cryptographic circuit accepts a plain text, and outputs a corresponding cipher text.
2. Electromagnetic (EM) field emanated from the AES circuit is measured by a magnetic-field probe, and an oscilloscope records the measured EM traces.
3. The correlation coefficient of cipher texts and EM waveforms is calculated and analyze the secret key.



The correlation coefficient of cipher texts and EM waveforms is calculated and leads the secret key.

Fig. 3. The procedure of CEMA attack

Fig. 4 shows the structure of the AES cryptographic circuit. The attacked round is the last (10th) round. The number of measured traces for attack is 10,000. The leak models using CPA and CEMA are the Hamming-Distance (HD) model and the Hamming-Weight (HW) model. They show the relationship between sensitive internal logical values and physical measurement. The HD model focuses on the logical transition of a register, and the HW model focuses on the logical bit value ("1" or "0") of the Sbox input (or output). These attacks are denoted as HD/HW-CPA, HD/HW-CEMA.

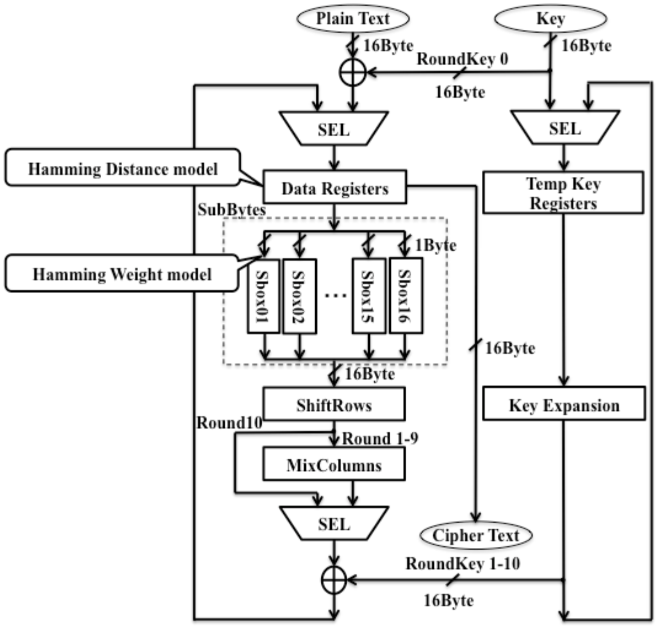


Fig. 4. AES cryptographic circuit structure

C. *Experimental Environment*

Fig. 5 shows the experiment environment. The AES chips were measured by mounting on SASEBO-RII [7]. The measured power traces are consumption current through 1Ω shunt resistance of GND line. Electromagnetic waveforms were measured by a horizontal magnetic-field probe placed on the chip surface, as shown in Fig. 5. A diameter of the horizontal magnetic-field probe is 550 µm. Probing position is determined by using the EMC (Electromagnetic Compatibility) scanner. The measured electromagnetic waveforms are amplified by a low noise amplifier with 50dB gain and 10-1000MHz bandwidth. The sampling rate and bandwidth of the oscilloscope are 20 GSa/s and 1 GHz, respectively. The experimental environment is summarized in TABLE I.

TABLE I
Experiment environment for attack evaluation

Oscilloscope	**Agilent DSO9104A**	
	Sampling Rate	**20GSa/s**
	Bandwidth	**1GHz**
PA Attack	**GND**	
EMA Attack	**EMC Scanner**	**WM7400**
	Magnetic-field Probe (HC020)	
	Coil	**Horizon**
	Resolution φ	**0.55mm**
	Amplifier (LNA-1050)	
	Bandwidth	**10-1000MHz**

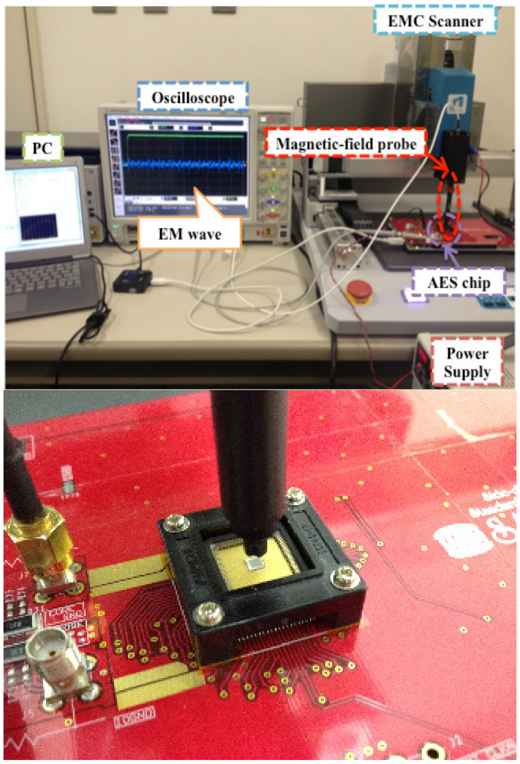


Fig. 5. Experimental environment of electromagnetic analysis attack

III. Experimental Results

A. Power Analysis Attack

The PA attack resistance of the AES cryptographic chips with / without on-chip decoupling capacitors is evaluated by using HD/HW-CPA attack. Figs. 6 and 7 show the measured power traces on the AES cryptographic circuit without and with on-chip decoupling capacitors, respectively. The Sbox of both the measured AES chips are implemented using composite field arithmetic. The power trace of the AES with on-chip decoupling capacitors revealed that the voltage spikes are eliminated compared to that of the AES without on-chip decoupling capacitors. Thus, the effect of on-chip decoupling capacitors on power waveforms is clearly observed.

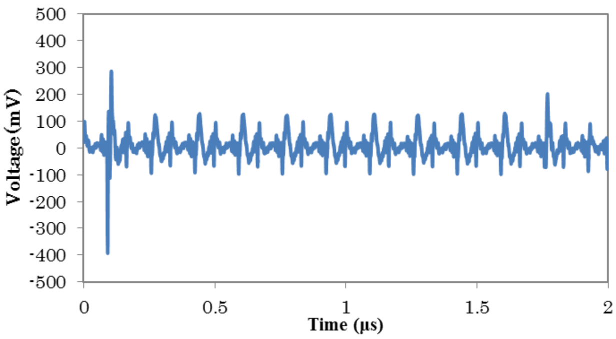


Fig. 6. A measured power trace of the AES cryptographic chip without on-chip decoupling capacitors

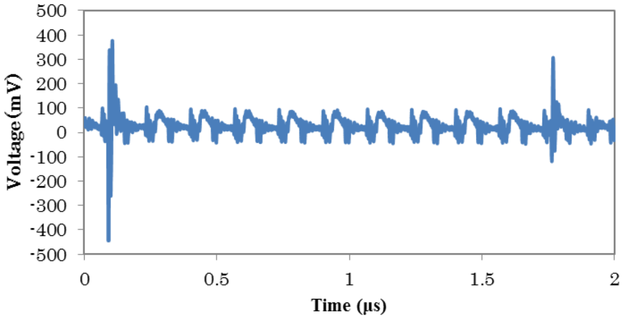


Fig. 7. A measured power trace of the AES cryptographic chip with on-chip decoupling capacitors

Figs. 8 and 9 show the relationship between the number of revealed key bytes (max 16 Bytes) and the number of the measured power traces. The less number of revealed keys even in more number of traces means that the circuit has higher resistance against HD/HW-CPA attack.

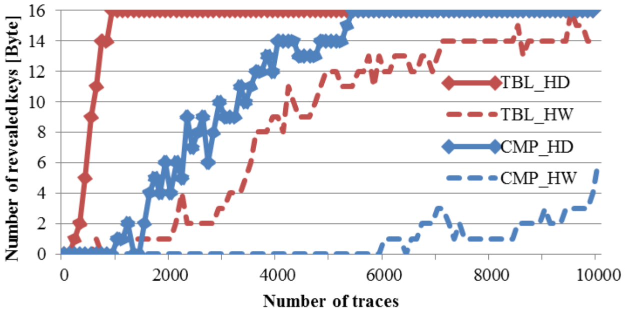


Fig. 8. Number of revealed keys on CPA against AES without on-chip decoupling capacitors

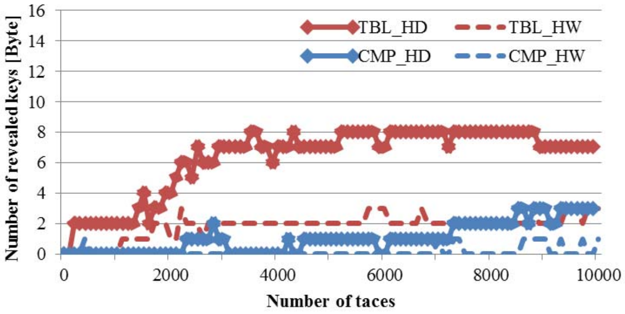


Fig. 9. Number of revealed keys on CPA against AES with on-chip decoupling capacitors

The results of the experiments are summarized as follows.

(1) The comparison of TBL (Red lines) vs. CMP (Blue lines)

The CMP circuit has higher resistance against both of HD and HW attack. It is probably because that the power consumption of CMP is less than that of TBL.

(2) The comparison of HD (Solid lines) vs. HW (Broken lines)

The HD-CPA attack is stronger than HW-CPA attack. It is that because the correlation between HD and power consumption is larger than that between HW and power consumption.

(3) The comparison of non-decoupled (Fig.8) and decoupled (Fig.9) chip

The reveal of keys require more traces in the case of the decoupled chip.

These results indicate that the on-chip decoupling capacitors enhance the resistance against PA attack because the voltage spike is averaged owing to the capacitor.

B. *Electromagnetic Analysis Attack*

In the measurement, a horizontal magnetic-field probe is placed in the center of the chip and moved as close as possible on the chip surface. Figs. 10 and 11 show the measured electromagnetic traces of the AES with and without on-chip decoupling capacitors, respectively. The Sbox of both the measured AES chips are implemented using composite field arithmetic. The electromagnetic trace of the AES with on-chip decoupling capacitors was slightly greater than that of the AES without on-chip decoupling capacitors. On the contrary to the power traces, the on-chip decoupling capacitors are ineffective to decrease the spike of the electromagnetic traces.

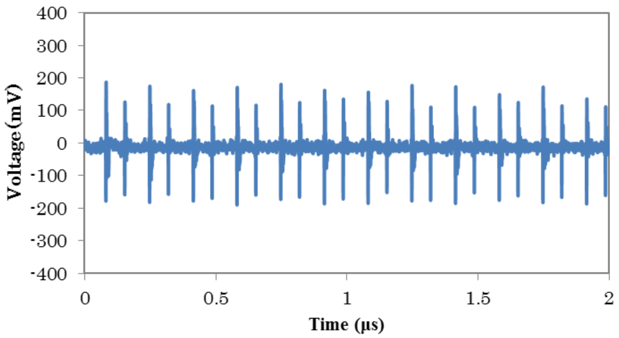


Fig. 10. Measured electromagnetic trace of the AES-CMP cryptographic chip without on-chip decoupling capacitors

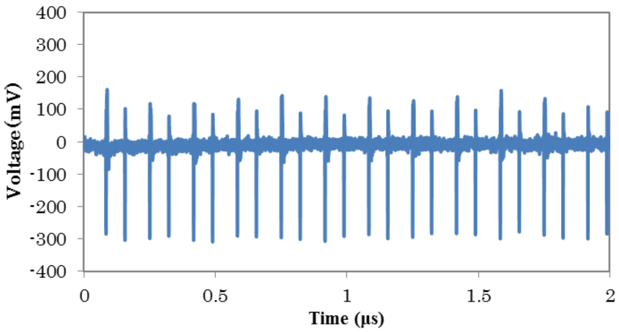


Fig. 11. Measured electromagnetic trace of the AES-CMP cryptographic chip with on-chip decoupling capacitors

Figs. 12 and 13 show the relationship between the number of revealed key bytes and the number of the measured electromagnetic traces. The results of the experiments are summarized as follows.

(1) The results of AES without decoupling capacitors (Fig.12)

The reveal of keys require more traces in the case of the EMA attack compared to the PA attack. The dependency of TBL/CMP and HD/HW is the same as the PA attack.

(2) The results of AES with decoupling capacitors (Fig.13)

These experimental results greatly differ from the case in the PA attack. Apparently, the attack is efficiency increased in the case of decoupled chip, especially, in the case of applying HW-CEMA.

These experimental results indicate that the on-chip decoupling capacitor is ineffective as the countermeasure against the EMA attack.

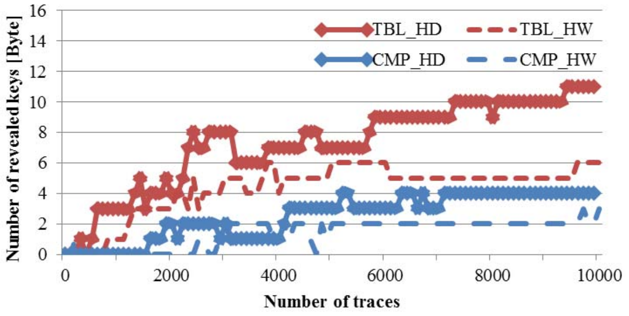


Fig. 12. Number of revealed keys on CEMA against AES without on-chip decoupling capacitors

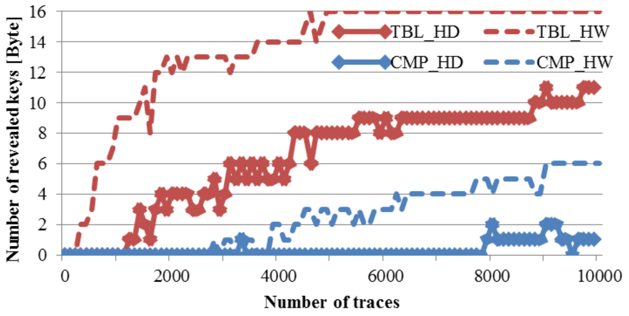


Fig. 13. Number of revealed keys on CEMA against AES with on-chip decoupling capacitors

C. *The Dependence of the Probing Position*

To investigate the dependence of the probing position, electromagnetic traces were measured at four positions shown in Fig.14. The position (A) is just above AES-TBL, and the position (B) is just above AES-CMP. The position (C) is above a bonding wire for power supply which is close to AES-TBL circuit. The position (D) is above a bonding wire for power supply which is close to of AES-CMP circuit.

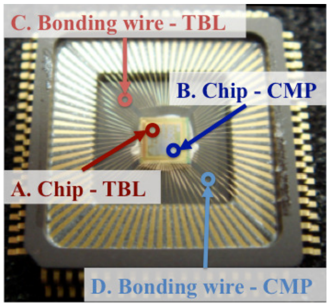


Fig. 14. The photograph of magnetic-field probing positions

Fig. 15 shows the CEMA resistance of the AES cryptographic circuits without on-chip decoupling capacitors at the position (A). Since the magnetic-field probe is close to AES-TBL, CEMA attacks reveal more key bytes of AES-TBL in contrast with the result in Fig.12. Fig.16 shows the CEMA resistance of the AES cryptographic circuit with on-chip decoupling capacitors at the position (A). The resistance against HW-CEMA becomes low by inserting the on-chip decoupling capacitors just like the results in Fig.13. In addition, the HD-CEMA attack was also effective in these experimentations. This is beacuse that the magnetic-field probe was able to obtain more transition information of the data registers (HD information), because the magnetic-field probe is closely placed to the resister.

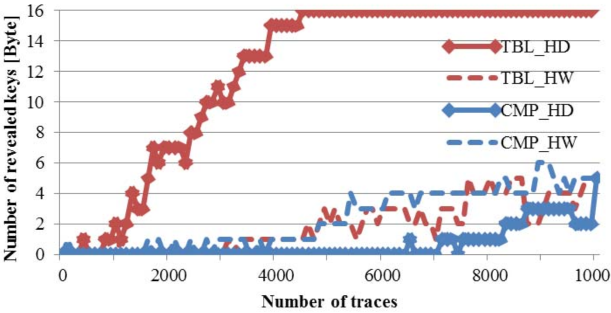


Fig. 15. Number of revealed keys on CEMA without on-chip decupling capacitors at Position (A) (above AES-TBL circuit)

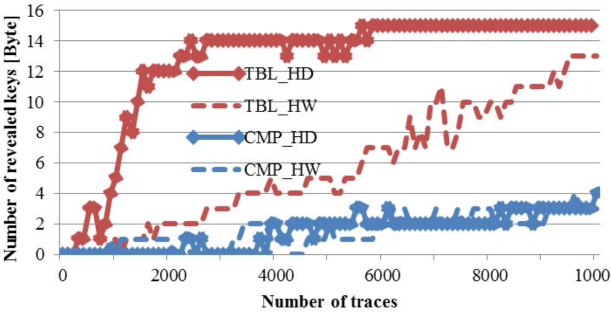


Fig. 16. Number of revealed keys on CEMA with on-chip decoupling capacitors at Position (A) (above AES-TBL circuit)

The attack efficiency to the AES-CMP is decreased at position (A), because AES-CMP circuit is located far from the magnetic-field probe. Adversely, the attack efficiency to the AES-CMP is increased at the position (B). These results suggest that the distance between the position of a magnetic-field probe and attack target circuit is very important on EMA attack.

Figs. 17 and 18 show the CEMA resistance of the AES cryptographic circuits with and without on-chip decoupling capacitors at the position (C), respectively. Only HD-CEMA on the AES-TBL was powerful and the implementation of the on-chip decoupling capacitors enhanced the resistance against HD-CEMA. These tendencies have some resemblance to the result of the PA attack in Figs. 8 and 9. At the position (D), AES-CMP was vulnerable to the HD-CEMA. These results suggest that the CEMA above the bonding wire resembles to the results of CPA, from two points of view: one is that the HD attack is stronger than the HW attack, and the other is that the decopling capacitor is effective as the countermeasure against the attack.

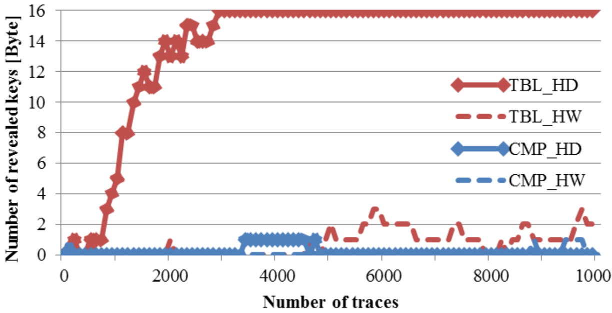


Fig. 17. Number of revealed keys on CEMA without on-chip decoupling capacitors at Position (C) (above bonding wire near AES-TBL)

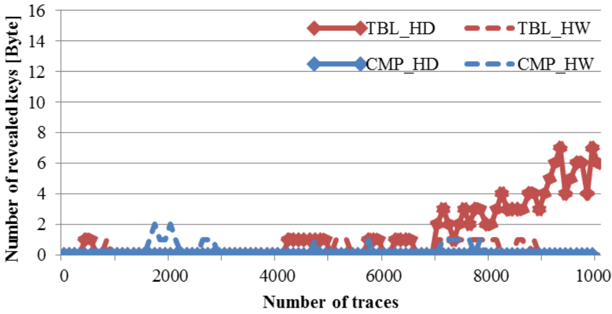


Fig. 18. Number of revealed keys on CEMA with on-chip decoupling capacitors at Position (C) (above bonding wire near AES-TBL)

IV. Summary and Conclusions

In order to investigate the effect of on-chip decoupling capacitors against PA/EMA attack, we carried out CPA and CEMA attack to the AES cryptographic circuits with and without on-chip decoupling capacitors, and compared each other. In addition, the effect of placement of the magnetic-field probe is also investigated, since EMA attack depends greatly on probing position. The below is obtained by the experimental results in this paper.

- As a countermeasure against PA attack, the on-chip decoupling capacitor increases the required number of traces for revealing keys, but the attack is successful
- On PA attack, the attack using HD model is more efficient than the attack using HW model whether decoupling capacitors are implemented or not.
- The on-chip decoupling capacitor increases an EM leak on the surface of the chip, especially the attacks using HW model becomes effective.
- EMA attack strongly depends on the measurement position. The probe positioning just over the target circuit is effective on the attack based on both HD and HW model. The attack results above the bonding wire of power supply resemble the results of PA attack.

This paper clarified the several characteristics of EMA attack, which is different from PA attack. We have already developed the AES circuit which is resistant to PA attack; however, this study suggests that the countermeasure against PA attack is not always sufficient against EMA attack. In the future, we will continue to the research about an EM leak, and propose a better countermeasure against both PA and EMA attack.

Acknowledgements

This research was supported by JST, CREST. The chip implementation was supported by VLSI Design and Education Center (VDEC), the University of Tokyo in collaboration with Rohm, Co., Ltd.

References

[1] P. Kocher, “Differential Power Analysis,” *Crypto’99*, pp. 388-397, 1999.

[2] E. Brier, “Correlation Power Analysis with a Leakage Model,” *CHES 2004*, Vol.3156, pp.135-152, 2004.

[3] S. Mangard, “Power Analysis Attacks –Revealing the Secrets of Smart Cards,” Springer, 2010.

[4] K. Gandolfi, “Electromagnetic Analysis Concrete Result,” *CHES2001*, Vol.2162, pp.251-261, 2001.

[5] T. Katashita, “Experimentation of Decoupling Capacitance Effects of CPA,” *SCIS2009*, 2009 (in Japanese).

[6] K. Kawamura, “Tamper resistance of implementation methods of AES against CPA,” *FIT2009*, Vol.8, pp.147-148, 2009 (in Japanese).

[7] “Side-cannel Attack Standard Evaluation Board,” http://staff.aist.go.jp/akashi.satoh/SASEBO/ja/index.html