Side-Channel Leakage Evaluation of Multi-Chip Cryptographic Modules

Kazuki Monta
Graduate School of Science, Technology and Innovation
Kobe University
Kobe, Japan
monta@cs26.scitec.kobe-u.ac.jp

Takumi Matsumaru
Graduate School of Science, Technology and Innovation
Kobe University
Kobe, Japan
takumi.matsumaru@cs26.scitec.kobe-u.ac.jp

Takaaki Okidono
SCU Co., Ltd
Tokyo, Japan
okidono@cs26.scitec.kobe-u.ac.jp

Takuji Miki
Graduate School of Science, Technology and Innovation
Kobe University
Kobe, Japan
miki@cs26.scitec.kobe-u.ac.jp

Makoto Nagata
Graduate School of Science, Technology and Innovation
Kobe University
Kobe, Japan
nagata@cs.kobe-u.ac.jp

***Abstract*— 2.5D and 3D packaging are methodologies that include multiple integrated circuit (IC) chips. They deliver enhanced performance, lower latency and power performance. Cryptography hardware modules are vulnerable to side-channel (SC) attacks. In this paper, we focus on the security level of multi-chip modules. Electromagnetic (EM) noise from multi-chip module demonstrators with crypto module is captured and evaluated for SC leakage. And also, we introduce an SC leakage mitigation methodology applicable for 3D integrated circuits.**

Keywords—Cryptographic engine, electromagnetic (EM) noise, side channel leakage, 3D CMOS chip stacks, Si substrate backside.

I. INTRODUCTION

These days, there are various requirements for integrated circuit (IC) devices, such as high performance, low power consumption and small area. 2.5D and 3D packaging technology is drawing attention as a technology that meets these demands. In 2.5D packaging, multiple chips are placed horizontally and are connected through an interposer. On the other hand, in 3D packaging, chips are stacked vertically and connected using Through-Silicon Vias (TSVs).

Cryptographic hardware modules are vulnerable to side-channel (SC) attacks. Differential Power Analysis (DPA) and Correlation Power Analysis (CPA) exploit the physical information of a device, such as power consumption, to disclose secret information [1][2]. In these attacks, SC leakage model is assumed and the relationship between SC leakage model and physical information is analyzed. The number of bit changes in a data register which is called Hamming distance is an example of SC leakage model.

In this paper, we investigate a security level of multi-chip modules. 3D silicon demonstrator and 2.5D silicon demonstrator were experimentally fabricated. Each demonstrator integrates cryptographic engines. Electromagnetic (EM) waveforms during crypto processing were captured and evaluated for SC leakage. And in the end of this paper, we introduce an SC leakage mitigation methodology, which can be used for Security 3D chip stacking. This methodology should be used in collaboration with countermeasure design techniques of cryptographic circuits and algorithms.

II. SCA EVALUATION OF MULTI-CHIP MODULE

A. Si demonatrator and evaluation setup

The prototype IC chip was developed in 0.13 um CMOS technology. The chip is composed of a cryptographic module based on elliptic curve cryptography. We have developed 2.5D and 3D packaging demonstrators with prototype IC chips. Four IC chips are placed horizontally, flipped down and assembled on a plastic interposer in the 2.5D demonstrator. In the 3D demonstrator, four chips are stacked vertically, connected using TSV, placed faceup and assembled on a plastic interposer.

An EM probe senses EM radiations from demonstrators as shown in Fig. 1. The EM wave is amplified and then captured by an oscilloscope. EM waves are measured at power supply terminals on printed circuit board (PCB), as the point #1 and the point #A, and are measured above the chip, as the point #2 and the point #B. Captured waveforms are evaluated for SC leakage.

A known SC analysis methodology, called test vector leakage assessment (TVLA), is used in SC leakage evaluation. TVLA uses Welch's t-test to determine if two sets of measured waveforms are significantly different[3]. Measured EM waveforms are divided into two sets based on a digital internal value in cryptographic function. A t-value over 4.5 means a significant difference between two sets. If there is a significant difference in two sets divided based on a digital value in the cryptographic function, the difference can be used by SC attackers to disclose secret information. In this paper, t-test is executed based on the digital value in Chip1.

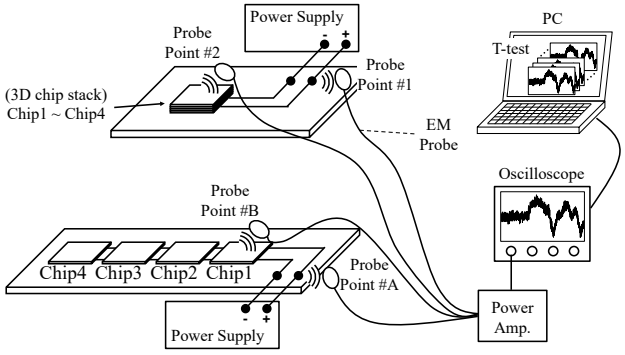

Fig. 1. Experimental setup.

B. Evalustion results

First, EM emission was measured at power supply terminals on PCB, as the point #1 and the point #A in Fig. 1, and evaluated for SC leakage. Fig. 2 shows the results of SC leakage evaluation with changing the number of chips that operate cryptography function in parallel. The highest SC leakage is observed for one chip operation in both 2.5D demonstrator and 3D demonstrator. This result can be explained by the fact that power delivery network (PDN) is shared by four chips in both 2.5D and 3D demonstrator and signal-to-noise ratio (SNR) of an evaluated chip's noise is higher in single-chip operation than in multi-chip operations because of the noise addition in the PDN. Multi-chip operation's SC leakage suppression effect is larger in 3D demonstrator than in 2D demonstrator.

Second, we measured EM waveforms at the point above the chip, as the point #2 and the point #B in Fig. 1, and measured waveforms were evaluated for SC leakage with changing the number of operating chips. The results are shown in Fig. 3. In the result of the 3D demonstrator, one chip operation has the highest leakage. Since the four chips in 3D packaging are vertically aligned inside the stack with the same footprint, EM radiation from multiple chips adds up at the point above the chip stacking in multi-chip operation. As a result, the SNR of the noise of an evaluated chip and SC leakage in multi-chip operation is lower in multi-chip operation than in single-chip operation. On the other hand, in the result of 2.5D demonstrator, a multi-chip operation's SC leakage suppression effect can not be seen. This is because EM radiation from different chips are not added in 2.5D structure and on-chip PDNs of different chips are not strongly coupled.

In these evaluations, multi-chip operation's SC leakage suppression effect is confirmed except for the evaluation at the point above the chip in 2.5D demonstrator. We explained that SNR reduction of the noise from an evaluated IC chip causes this SC leakage suppression effect. And also, from the results, it can be observed that significant differences in SC leakage level can be seen only between 1 chip operation and 2 chips operation. From these results, we conclude that multi-chip cryptography module operation has an SC leakage suppression to a certain level. However, this effect itself cannot be a perfect countermeasure against SC leakage.

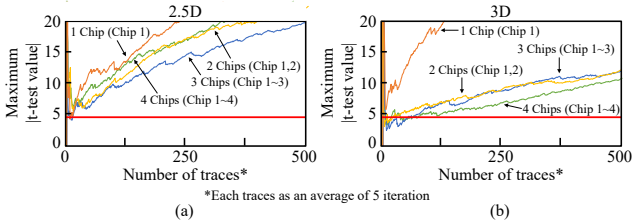

Fig. 2. T-test results for SC leakage evaluation at the power supply terminal on PCB. (a) 2.5D probe point #A and (b) 3D probe point #1

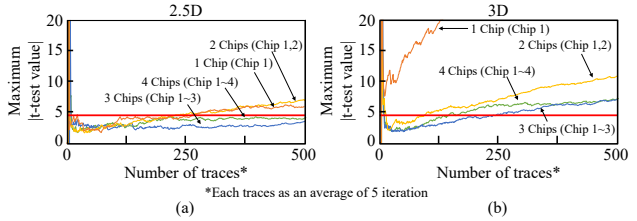

Fig. 3. T-test results for SC leakage evaluation at the point above the chip. (a) 2.5D probe point #B and (b) 3D probe point #2

III. Secure 3D CMOS Chip Stacks with Backside Buried Metal

In [4], the authors proposed an SC leakage mitigation methodology that is applicable for 3D integrated circuits. The methodology uses a vast and vacant space of a Si substrate backside for "passive elements to be integrated". The space is used for backside buried metal (BBM) as shown in fig. 4 and its power noise suppression effect and side channel leakage mitigation effect are evaluated in the paper. 14x increase in the number of EM traces for a significant difference is achieved with the methodology. 3D CMOS PDN using BBM wirings can be technical options toward high computation performance and strong attack resiliency.

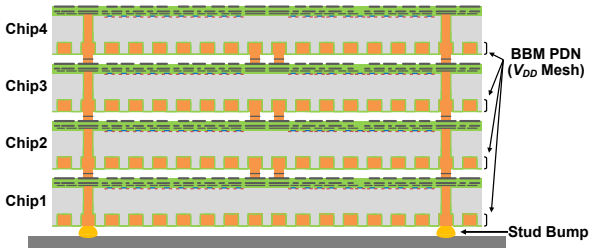

Fig. 4. 3-D stacking structure with BBM PDN

IV. Conclusion

SC attack is a threat to cryptographic hardware. In this paper, we evaluated SC leakage from multi-chip cryptographic modules using 3D silicon demonstrator and 2.5D silicon demonstrator. The results show that multi-chip cryptography module operation has an SC leakage suppression to a certain level. And also, we introduced an SC leakage mitigation methodology that is applicable for 3D integrated circuits. To achieve high SC leakage resiliency, SC leakage suppression effect of multi-chip operation and the introduced methodology should be used in collaboration with countermeasure circuit design techniques and countermeasure cryptographic algorithms. As the future work, we plan to make a simulation methodology for evaluating SC leakage from multi-chip cryptographic modules using a power current simulation of a chip and a field solver. With the simulation, we can provide deeper insight into multi-chip cryptographic module's SC leakage.

Acknowledgment

This work has been supported by JSPS KAKENHI Grant No. JP22H04999.

References

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

[2] E. Brier et al., "Correlation Power Analysis with a Leakage Model," In CHES 2004, volume 3156 of LNCS, pages 16–29. Springer, August 2004.

[3] J. Cooper et al., "Test Vector Leakage Assessment (TVLA) methodology in practice," International Cryptographic Module Conference, 2013.

[4] K. Monta et al., "3-D CMOS Chip Stacking for Security ICs Featuring Backside Buried Metal Power Delivery Networks With Distributed Capacitance," in IEEE Transactions on Electron Devices, vol. 68, no. 4, pp. 2077-2082, April 2021.