The original version of this paper is published in:
Information--An International Interdisciplinary Journal, Vol.16, No.8(B), pp.5993-6006, 2013

A First Report on Electromagnetic and Power Analysis Attacks against a 28-nm FPGA Device

Yohei Hori*, Toshihiro Katashita*, Akihiko Sasaki* and Akashi Satoh**

**Research Institute for Secure Systems, National Institute of Advanced Industrial Science and Technology (AIST),*
Tsukuba Central 2, 1-1-1 Umezono, Tsukuba, Ibaraki 305-8568, Japan
E-mail:{hori.y,t-katashita,a-sasaki}@aist.go.jp

***Nanoelectronics Research Institute, National Institute of Advanced Industrial Science and Technology (AIST),*
Tsukuba Central 2, 1-1-1 Umezono, Tsukuba, Ibaraki 305-8568, Japan
E-mail:akashi.satoh@aist.go.jp

Abstract

Two types of side-channel attack (SCA)— electromagnetic analysis (EMA) and correlation power analysis (CPA)—are conducted on the latest 28-nm field-programmable gate array (FPGA) device. SCA exploits leakage of physical information, such as power consumption or electromagnetic (EM) radiation, from a cryptographic device to extract that device's secret key. Owing to remarkable advances in large-scale integration (LSI) technology factors such as reduced core voltages and use of on-chip capacitors, power analysis of cryptographic devices has become increasingly difficult; consequently, the threat of EMA to cryptographic devices has become the greater concern. To assess the feasibility of SCA against state-of-the-art LSI technology, we developed the Side-channel Attack Standard Evaluation Board (SASEBO)-GIII, which is equipped with Xilinx Inc.'s 28-nm Kintex-7 FPGA device. To demonstrate the suitability of SASEBO-GIII for SCA research, we performed EMA and CPA against advanced encryption standard (AES) circuits on the Kintex-7 FPGA and compared the results with those on the 65-nm Virtex-5 FPGA from our previous SASEBO-GII evaluation platform. EMA successfully extracted the entire secret key from the Kintex-7 FPGA on the SASEBO-GIII with fewer wave traces than were needed for the Virtex-5 FPGA on the SASEBO-GII; furthermore, EMA against Kintex-7 FPGA required fewer wave traces than did CPA against the same device. In this paper, we explain the features of SASEBO-GIII, provide experimental EMA and CPA results, and discuss the risk posed by EMA and CPA to leading-edge LSI technology.

Key Words: Side-channel attack (SCA), Side-channel Attack Standard Evaluation Board (SASEBO), Electromagnetic analysis (EMA), Correlation Power Analysis (CPA), Field-programmable gate array (FPGA)

1. Introduction

Cryptography has become an essential technology in information security (the practice of protecting the confidentiality, integrity, and availability of information). By convention, cryptographic algorithms are carefully evaluated in terms of computational complexity in order to ensure their security. Nevertheless, such algorithms can still be vulnerable when they are implemented on practical devices. Side-channel attacks (SCAs), or physically noninvasive attacks, are considered to be a serious threat to cryptographic devices. SCAs exploit the measurable phenomena of devices, such as power consumption, electromagnetic radiation, or operating times, to extract internal cryptographic keys [1]. Whereas invasive attacks require expensive setups that make physical contact with a device in order to extract internal signals, SCAs can be conducted using inexpensive, general instruments.

Following the introduction of differential power analysis (DPA) [2] to SCA research, several types of attacks have been reported so far including template attack [3], correlation power analysis (CPA) [4], mutual information analysis (MIA) [5], stochastic attack [6] and so on. Earlier studies focused mainly on variants of power analysis, which is considered easier to conduct than electromagnetic analysis (EMA) [7,8], even though it often requires a slight modification to a device's printed circuit board (PCB); for example, by setting up a point to monitor core voltage. However, electromagnetic (EM) radiation can easily be measured without any PCB modifications, and can even be measured at distance. Furthermore, monitoring device power consumption is becoming increasingly difficult owing to the shrinking of transistor process node sizes [9]. Because of process technology advances in features such as core voltage reduction, on-chip decoupling capacitors, and system-on-chip implementation, the signal-to-noise ratio (SNR) associated with SCAs has decreased. Consequently, EMA has become a greater threat than power analysis to cryptographic devices.

To test the feasibility of SCAs against state-of-the-art large-scale integration (LSI) technology, we developed a new experimental environment, the Side-channel Attack Standard Evaluation Board (SASEBO)-GIII [10], equipped with the latest 28-nm Kintex-7 field-programmable gate array (FPGA) device. We conducted correlation-based EMA (CEMA), a method similar to correlation power analysis, on the advanced encryption standard (AES) circuit of the Kintex-7 FPGA as well as on the AES circuit of the Virtex-5 FPGA device of our previous SASEBO-GII for comparison. A description of an earlier version of CEMA experiments on the 28-nm Kintex-7 can be found in [11]; for this study, we conducted further CPA experiments against the Kintex-7 in order to compare the effectiveness of EM and power side-channel analysis.

We found that fewer wave traces were required by a CEMA in order to correctly extract the entire secret key from the SASEBO-GIII than were required for a SASEBO-GII; in addition, we discovered that a CEMA on the SASEBO-GIII required fewer wave traces than did a CPA. In this paper, the architecture and functionality of the SASEBO-GIII are described in detail, with the results of a CEMA and a CPA performed on this board presented and discussed.

2. Side-channel Attacks and Evaluation Platform

2.1 SASEBO Evaluation Platforms

Physical attacks are theoretical techniques used to extract secret keys from cryptographic devices. As shown in Figure 1, physical attack methods can be categorized into two main types: invasive attacks that require tampering with a device in order to directly monitor its internal signals, and noninvasive attacks that observe internal information from outside of the device using a measuring instrument. SCAs are particular types of noninvasive physical attack that exploit measurable physical leakage from a device, such as power consumption or EM radiation. The establishment of DPA revealed that SCAs can be a serious practical threat to cryptographic devices, and as a result, various research institutes have studied SCA methods and countermeasures; however, as these institutes typically used differing measuring apparatuses, it is difficult to make a fair comparison between their experimental results in order to arrive at meaningful conclusions. Therefore, in order to encourage SCA research under a uniform experimental platform, the National Institute of Advanced Industrial Science and Technology (AIST) and Tohoku University have jointly developed SASEBO.

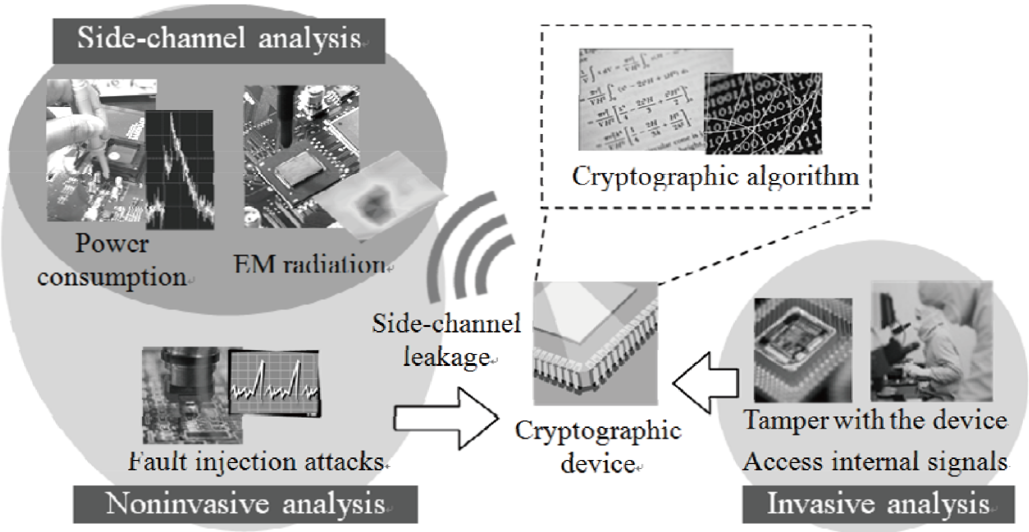

Figure 1. Classification of physical attacks against cryptographic devices

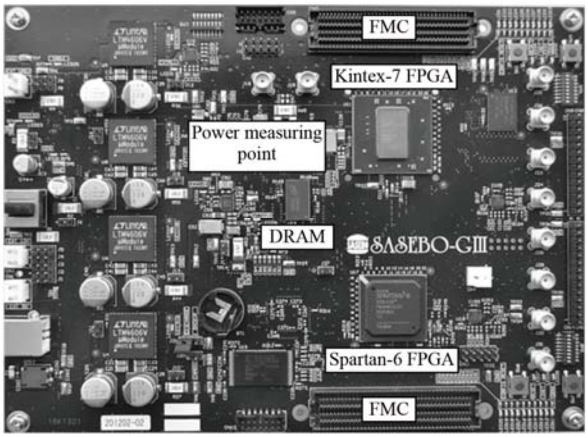

Figure 2. Main components of the SASEBO-GIII

2.2 SASEBO-GIII

Process technology advances have lowered device core voltages, resulting in a general reduction in power consumption of devices including FPGAs [12,13]. SCA is considered more difficult when the quantity of side-channel information is decreased through power consumption reductions. In actuality, fewer waveforms are required to analyze an AES circuit on a SASEBO-G with a 130-nm Virtex-II Pro FPGA device than on a SASEBO-GII with a 65-nm Virtex-5 FPGA. To measure physical information leakage from the latest FPGA and to investigate the feasibility of SCA against leading-edge LSI technology, we developed a new experimental platform, the SASEBO-GIII, which features a 28-nm process FPGA.

The SASEBO-GIII’s main components are shown in Figure 2, and its characteristics are listed in Table 1, along with those of our previous SASEBO-GII board for comparison. The SASEBO-GIII is equipped with a Xilinx Kintex-7 XC7K325T FPGA for testing cryptographic modules and a Spartan-6 FPGA for implementing control logic; to reduce the price of the board, a Kintex-7 XC7K160T FPGA may be chosen instead.

It should be noted that the SASEBO-GIII is suitable for evaluating the security of integrated systems as well as serving as a sole cryptographic core. As the Kintex-7 XC7K325T FPGA has greater than 10 times the number of logic blocks (slices) than does the Virtex-5 XC5VLX30 FPGA on the SASEBO-GII, it can provide sufficient resources for implementing application logic. Additionally, as two connectors adhering to ANSI's FPGA Mezzanine Card (FMC) standard have been employed in order to enhance expandability, off-the-shelf FMC components such as video interface or Ethernet boards can be connected to a SASEBO-GIII. A 1-Gbit DDR3 DRAM memory mounted on the SASEBO-GIII—in place of the 2-Mbit SSRAM chip on the SASEBO-GII—allows for a wide variety of practical applications and offers ample space to store data such as video streams, network packets, and FPGA

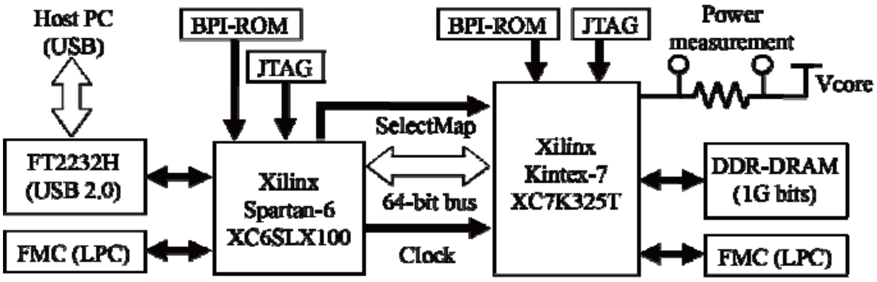

Figure 3. Block diagram of the SASEBO-GIII

configuration data. The USB 2.0 interface between the SASEBO-GIII and the host computer enables a data transfer rate 40 times faster than that of the USB 1.0 used with previous SASEBO boards.

As reported by Moradi and coworkers [14,15], the embedded cryptographic module of some FPGAs can be broken by means of power analysis. The SASEBO-GIII enables a user to evaluate the security of a vendor-provided cryptographic algorithm while exploring countermeasures to ensure that the module is secure. As can be seen from the block diagram for the SASEBO-GIII shown in Figure 3, the configuration interfaces of the Kintex-7 FPGA are connected to and controlled by the Spartan-6 FPGA. This architecture is useful for testing the security of the FPGA’s configuration procedure. The SASEBO-GIII also has an LR44 battery compartment, which was not mounted on previous SASEBO platforms, to supply power for battery-backed key storage. As a result, the Kintex-7 FPGA can be configured with an encrypted bitstream; however, it should be noted that its decryption key is embedded in its battery-backed flash memory.

In addition to the SASEBO-GIII's remarkable improvement over previous boards in terms of logic capacity, expandability, and configuration flexibility, it has high backward compatibility with these earlier platforms; in particular, the controls and cryptographic logic of previous boards can be implemented on the SASEBO-GIII with only minor revisions.

3. Experiments

To evaluate the advantageous performance and features of the SASEBO-GIII, we measured the EM radiation emitted from the AES circuit of the 28-nm Kintex-7 mounted on its board and conducted CEMA using the Hamming-distance model. For comparison, we also measured the core voltage of a Kintex-7 in order to conduct CPA. To isolate device process results, we also conducted the same experiment on the AES circuit of the 65-nm Virtex-5 FPGA on a SASEBO-GII, with the heat spreader of the Virtex-5 removed in order to effectively measure the EM radiation.

Table 1. Functional comparison of SASEBO-GIII and -GII

	SASEBO-GIII	SASEBO-GII
Board Size	250 × 200 mm^2, 8 layers	120 × 140 mm^2, 6 layers
Cryptographic Device	Kintex-7 325T, 28 nm, 1.0 V	Virtex-5 LX30/50, 65 nm, 1.0 V
Control Device	Spartan-6 LX45, 45 nm, 1.2 V	Spartan-3A 400, 90 nm, 1.2 V
Communication Interface	USB2.0 (480 Mbps)	USB1.0 (12 Mbps)
Expandability	2 × FMC (LPC)	2 × 34-bit header pins (24-bit for user pins)
External Memory	1-Gbit DDR3-SDRAM	2-Mbit SSRAM
FPGA Config. Interface	BPI, JTAG, ICAP, SelectMAP	SPI, JTAG, ICAP, SelectMAP
Monitoring Point	V_{core} line of Kintex-7	V_{core} and GND of Virtex-5

3.1 Experimental Setup

Figure 4 shows an overview of the experimental environment. The waveforms of the emitted EM radiation were acquired using a Langer LF-B 3 EM probe, a Miteq AU-3A-0150 amplifier (50 dB, 0.3–600 MHz), a fifth-order Bessel low-pass filter, and an Agilent DSO6104A oscilloscope. The EM probe was placed so that the peak voltage of the measured radiation waveform was maximized.

For the experiment, 50,000 waveforms were acquired for each of two cryptographic keys: key1 $\{00\ 01\ 02\ 03\ 04\ 05\ 06\ 07\ 08\ 09\ 0A\ 0B\ 0C\ 0D\ 0E\ 0F\}_{16}$, and key2 $\{2B\ 7E\ 15\ 16\ 28\ AE\ D2\ A6\ AB\ F7\ 15\ 88\ 09\ CF\ 4F\ 3C\}_{16}$. An S-Box transform of AES was implemented in the style of Composite Field.

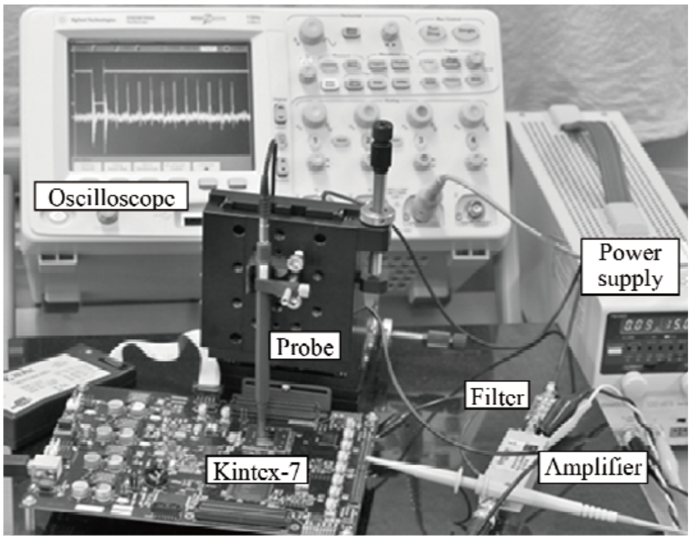

Figure 4. Overview of experimental environment

3.2 Experimental Results

Figure 5 shows examples of emitted EM radiation waveforms from the SASEBO-GIII and -GII. As the sampling interval used was 500 ns, a single waveform contains 10,000 values. Because the amplitude of the SASEBO-GIII's waveform is one fifth that of the GII, a lower noise environment and more expensive instruments with higher precision were required to measure the side-channel information from these state-of-the-art devices when evaluating physical vulnerability.

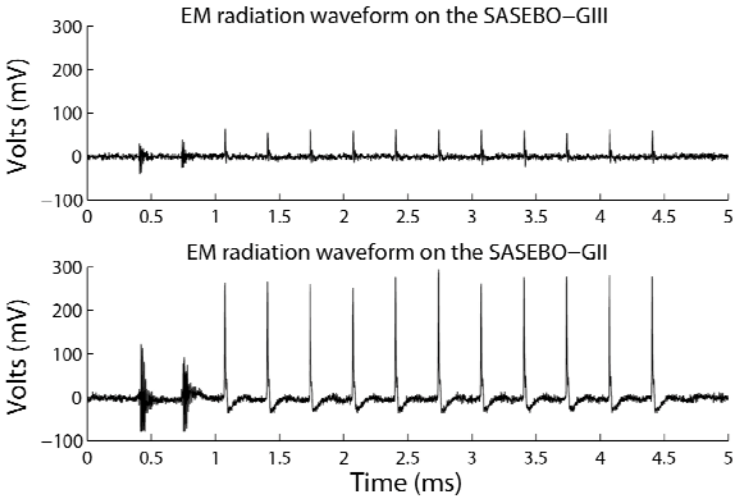

Figure 5. Example waveforms of emitted EM radiation for the SASEBO-GIII and -GII

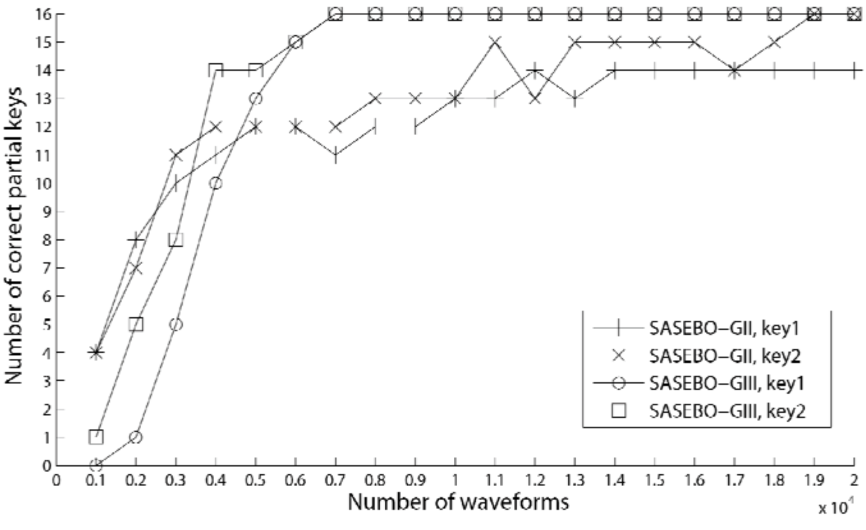

Figure 6. Number of correctly extracted subkey bytes in CEMA

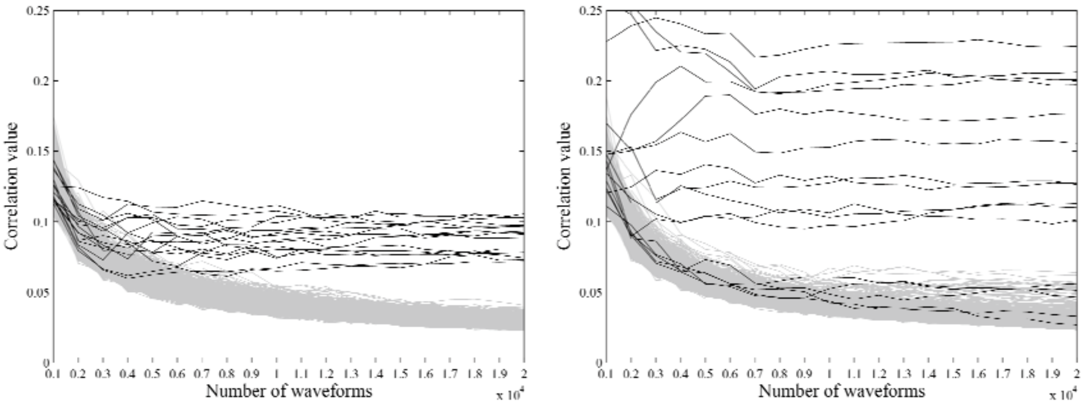

Figure 7. Correlation between key1 and EM traces for (left) SASEBO-GIII and (right) -GII

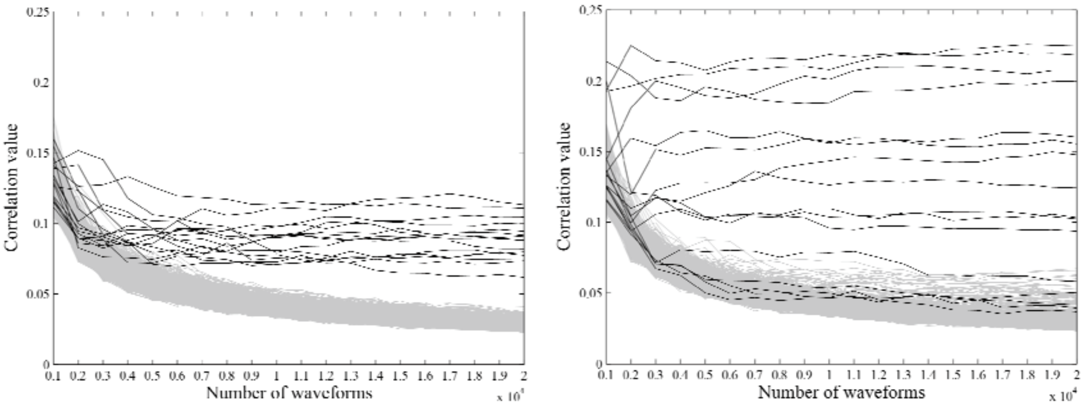

Figure 8. Correlation between key2 and EM traces for (left) SASEBO-GIII and (right) -GII

The results of key estimation by CEMA are shown in Figure 6. Contrary to our expectation that the device with smaller process geometry would require a greater number of wave traces, fewer waveforms were required to extract the entire 16-byte secret keys from the Kintex-7 FPGA on the SASEBO-GIII than from the Virtex-5 FPGA on the SASEBO-GII. Whereas key1 required 19,000 traces and key2 could not be completely extracted for SASEBO-GII, all bytes of key1 and key2 were correctly extracted in 7,000 traces for SASEBO-GIII. As illustrated in Fig. 6, the number of the extracted subkeys in SASEBO-GII is larger than that in SASEBO-GIII when the number of the wave traces is less than 4,000, however, the rest of the subkeys eventually requires more traces than SASEBO-GIII. It is still difficult to determine which of 28-nm and 65-nm FPGAs is easier to attack with EMA, but EMA is surely quite effective in 28-nm FPGA for key analysis. It remains as future work to conduct more experiments of CEMA and CPA for further investigation.

The correlation coefficients between intermediate subkey values and EM traces are shown in Figures 7 (key1) and 8 (key2), with the black and gray lines denoting the correlations of the correct and incorrect subkeys, respectively. From this it can be seen that the correlation coefficient trends of the SASEBO-GIII and -GII are clearly different. The average value of the correlation coefficient for the SASEBO-GIII is smaller than that for the SASEBO-GII, but the coefficients of all subkeys for the SASEBO-GIII are similar to each other, whereas those for the SASEBO-GII are inconsistent: notably, incorrect extraction occurred for the 5th, 7th, 13th, and 15th byte of key1 and key2. The difficulty of EMA key extraction from cryptographic modules is thus related to the positions of the subkey bytes and the circuit structure, not to the key value.

To further investigate this relation, the SNRs of side-channel information [1] were calculated as shown in Figure 9, which gives maximal SNRs over 50,000 EM traces of each subkey. In addition to key1 and key2, key3 $\{00\ 00\ ...\ 00\}_{16}$ and key4 $\{FF\ FF...\ FF\}_{16}$ were tested. From the figure, it can be seen that bytes 5, 7, 13, and 15 of the keys on the SASEBO-GII clearly have a low SNR compared with the other subkeys. Furthermore, as key1 through key4 within the same AES structure have a similar SNR tendency, it can be deduced that the success of EMA depends on the AES hardware structure rather than on the key value.

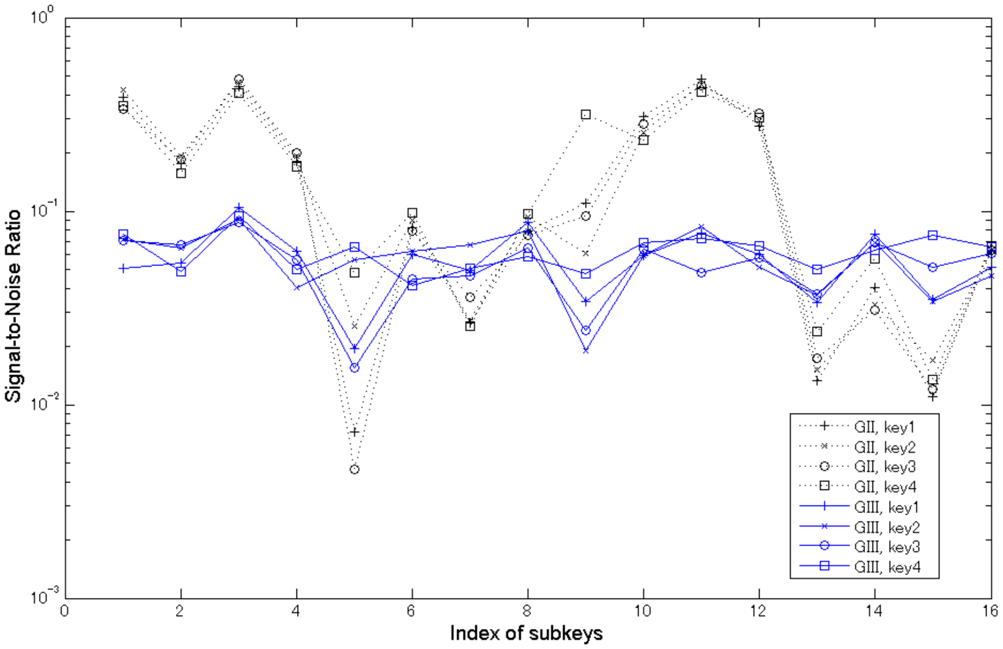

Figure 9. Maximal value of side-channel SNR for each subkey in CEMA

Given that all subkey bytes were successfully extracted from the Kintex-7 FPGA, it would seem that suitable implementation of a cryptographic circuit is device dependent. Therefore, the floor plan of a cryptographic circuit must be designed carefully to counteract SCAs; investigation of such floor plans is considered for future work.

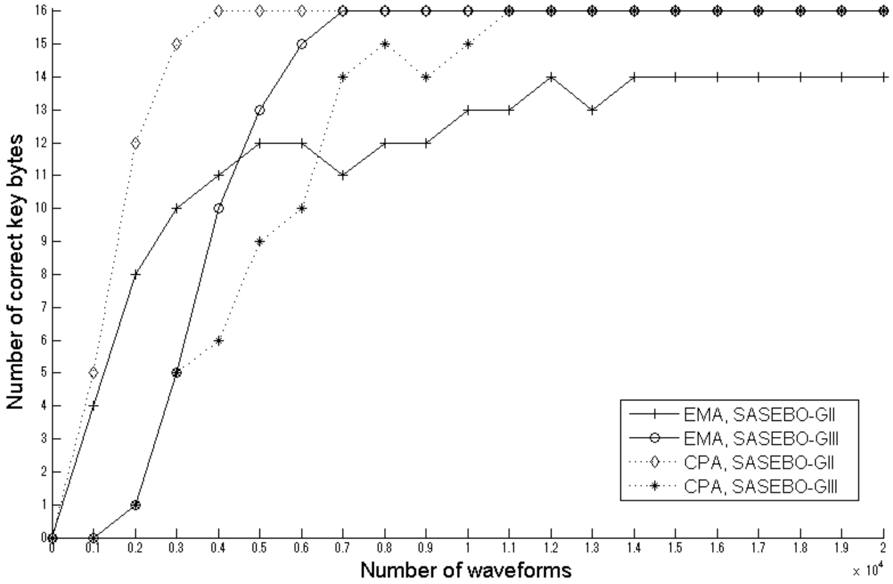

Figure 10. Number of correctly extracted subkey bytes in CEMA and CPA

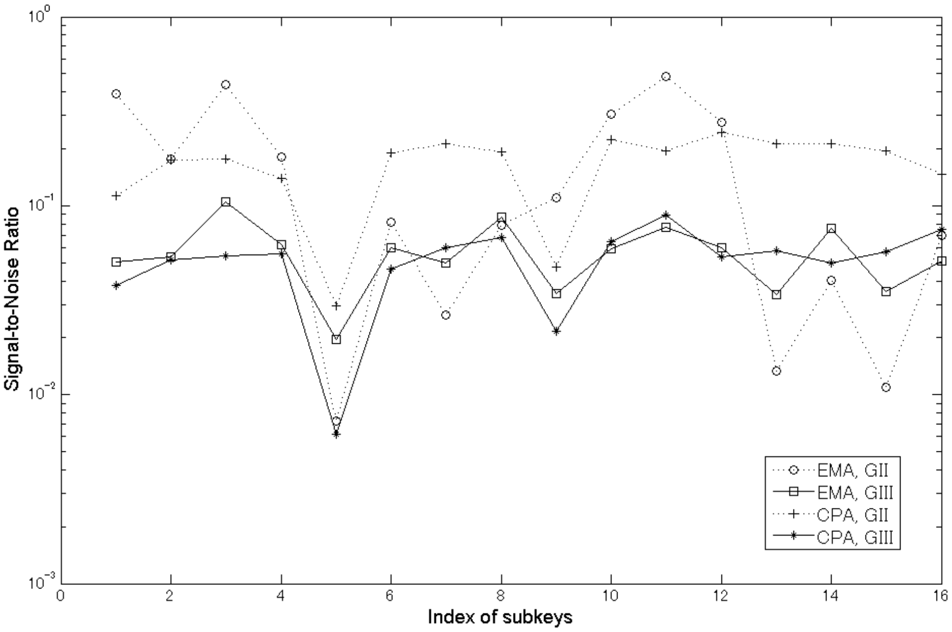

Fig. 11. Maximal value of side-channel SNR for each subkey in CEMA and CPA

Figure 10 shows the experimental results of EMA and CPA against the SASEBO-GIII and -GII. Notably, EMA against the 28-nm Kintex-7 on the SASEBO-GIII required fewer wave traces than did EMA against the 65-nm Virtex-5 on the SASEBO-GII; conversely, CPA against the Kintex-7 required more wave traces than did CPA against Virtex-5. Moreover, EMA required fewer traces than did CPA against the Kintex-7, and EMA required more traces than did CPA against Virtex-5.

Figure 11 shows the comparison of SNRs of EM and power information in SASEBO-GIII and -GII under the key1. Comparing EM and power information, EM has higher SNRs in 10 bytes out of 16 in SASEBO-GIII, while in SASEBO-GII EM has higher SNRs in 7 out of 16 bytes.

These results indicate that, in small process nodes of semiconductors such as the 28-nm FPGA, the EM side-channel is more informative and exploitable for key analysis than is the power side-channel, as the power channel can become noisier under smaller process nodes. The increase in power channel noise is likely caused by the reduction in the exploitable part of power consumption with decreasing process size: although the total power consumption of the chip decreases, electric noise on the board caused by the power source, clock, and other sources remains constant. On the other hand, the exploitable part of the EM channel also decreases, but to a lesser degree than in the power channel, perhaps owing to the high localization of EM radiation. It should be noted that while CPA measures the entire power consumption of the chip, including noise sources, EMA can measure the EM emitted from a small area of interest on the chip by using an EM probe of high spatial resolution. However, further experiments using EMA and CPA remain to be done in order to find clearer reasons for these results.

4. Conclusions

We have developed a new SCA experimental board, the SASEBO-GIII, featuring a leading-edge 28-nm Kintex-7 FPGA device. As a comparison, we conducted CEMA on measured EM radiation emissions from both the AES circuits of the Kintex-7 FPGA as well as on 65-nm Virtex-5 FPGA. To study the exploitability of EM and power side-channels under different process nodes, we conducted CPA on the Kintex-7 and Virtex-5. The results of our analysis show that the SASEBO-GIII performed better at observing side-channel information even though its measured voltage was one fifth that of SASEBO-GII.

Contrary to our expectations, fewer waveforms for successful key extraction were required by a CEMA of the 28-nm Kintex-7 on the SASEBO-GIII than were required for the 65-nm Virtex-5 on the SASEBO-GII; this result verifies that the SASEBO-GIII is suitable for SCA research purposes. Furthermore, CEMA of the Kintex-7 required fewer waveforms than did CPA of the same device. Together, these results indicate that using the EM side-channel could be more informative and exploitable for key analysis as semiconductor process nodes advance. In addition, subkeys at specific positions were difficult to extract for both of the keys tested, indicating that the difficulty of EMA key extraction is dependent on the structure of the cryptographic circuit rather than on the key value.

Future work remains in using CPA and EMA to investigate the effectiveness of power and EM side-channels for SCA. Other potential directions of research include investigating the relation between SCA difficulties and circuit structure, implementing additional cryptographic algorithms, and conducting various attacks against these algorithms, such as template attack, mutual information-based attack and other stochastic attacks.

Acknowledgments

Part of this work was conducted under the “Core Research for Evolutional Science and Technology (CREST)” funded by the Japan Science and Technology Agency (JST).

References

[1] Mangard, S., Oswald, E., and Popp, T., *Power Analysis Attacks,* Springer-Verlag (2007).

[2] Kocher, P., Jaffe, J., and Jun, B., Differential Power Analysis. *Proc. CRYPTO '99* (1999), 388-397.

[3] Chari, S., Rao, J. R., and Rohatgi, P., Template Attacks, *Proc. CHES 2002* (2002), 51-62.

[4] Brier, E., Clavier, C., and Olivier, F., Correlation Power Analysis with a Leakage Model. *Proc. CHES '04* (2004), 16-29.

[5] Gierlichs, B., Batina, L., Tuyls, P., and Preneel, B., Mutual Information Analysis, *Proc. CHES* 2008 (2008), 426-442.

[6] Lemke-Rust, K., Models and Algorithms for Physical Cryptanalysis, Ph.D. dissertation, Ruhr-Universität Bochum (2007)

[7] Quisquater, J. J. and Samyde, D., Electromagnetic Analysis (EMA): Measures and Countermeasures for Smart Card, *Proc. e-Smart 2001* (2001), 200-210.

[8] Gandolfi, K., Mourtel, C., and Olivier, F., Electromagnetic Analysis: Concrete Results, *Proc. CHES 2001* (2001), 251-261.

[9] International Technology Roadmap for Semiconductors (ITRS), Process Integration, Devices, and Structures, 2011 Edition (2011).

[10] Akashi, S., Katashita, T., and Sakane, H., Secure Implementation of Cryptographic Modules---Development of a Standard Evaluation Environment for Side Channel Attacks. *Synthesiology,* 3(1) (2004), 56-65.

[11] Hori, Y., Katashita, T., Sasaki, A. and Satoh, A., Electromagnetic Analysis against 28-nm FPGA Device, *Pre-Proc. WISA2012* (2012).

[12] Klein, M., Power Consumption at 40 and 45 nm, Xilinx Inc., (2009).

[13] Hussein, J., Klein, M., and Hart, M., Lowering Power at 28 nm with Xilinx 7 Series FPGAs (WP389), Xilinx, Inc., (2012).

[14] Moradi, A., Barenghi, A., Kasper, T., and Parr, C., On the Vulnerability of FPGA Bitstream Encryption against Power Analysis Attacks---Extracting Keys from Xilinx Virtex-II FPGAs, *Cryptology ePrint Archive* (2011).

[15] Moradi, A., Kasper, M., and Paar, C., On the Probability of Side-Channel Attacks---An Analysis of the Xilinx Virtex 4 and Virtex 5 Bitstream Encryption Mechanism, *Cryptology ePrint Archives* (2011).

*Corresponding author: Yohei Hori, Ph.D.
Research Institute for Secure Systems (RISEC),
National Institute of Advanced Industrial Science and Technology (AIST),
Tsukuba Central 2, 1-1-1 Umezono, Tsukuba, Ibaraki 305-8568, Japan
E-mail: hori.y@aist.go.jp