SASEBO-GIII: A Hardware Security Evaluation Board Equipped with a 28-nm FPGA

Yohei Hori, Toshihiro Katashita, Akihiko Sasaki and Akashi Satoh
National Institute of Advanced Industrial Science and Technology (AIST)
1-1-1 Umezono, Tsukuba, Ibaraki 305-8568, Japan
Email: {hori.y,t-katashita,a-sasaki,akashi.satoh}@aist.go.jp

***Abstract*—The SASEBO-GIII board equipped with a 28-nm FPGA was developed for security evaluation against side-channel attacks (SCAs) and various other threats. SCAs are performed to extract a secret key inside a cryptographic module by analyzing its power consumption, electromagnetic radiation and other physical parameters. Since an increasing number of current consumer electronic devices provide hardware-accelerated cryptographic functionality for data encryption, device authentication, and so forth, SCAs are considered to be a serious problem in the electronics market. While previous SASEBO models mainly target SCA evaluation of a single cryptographic core, they are nevertheless insufficient for testing the security of integrated systems that consist of any combination of cryptographic, network, control and other modules. Providing high processing power with the latest Kintex-7 FPGA and considerable expandability with ANSI-standard FMC connectors, SASEBO-GIII is suitable for prototyping a wide variety of systems, such as home information appliances, content distribution systems and dynamic partial reconfiguration (DPR) systems, and offers a convenient environment for studying security issues in such integrated systems, for example, hardware trojans and counterfeit electronics. The configuration of the Kintex-7 FPGA is controlled by the other FPGA (Spartan-6), and therefore a user can verify the security of various types of device configuration processes, for example, DPR through ICAP or SelectMAP interfaces as well as though standard configuration interfaces such as BPI and JTAG. This paper presents the detailed architecture and features of SASEBO-GIII, and shows the results of an electromagnetic SCA attack against the standard AES block cipher implemented on the Kintex-7 FPGA.**

I. Introduction

With today's consumer electronics, users can enjoy a wide variety of multimedia content at home, including music, video, games and movies. In addition, most electronic devices can connect to the Internet to download entertainment content and software updates. However, digital content available online is always under threat of piracy and cyberattack as the content can be subject to eavesdropping, illicit copying and tampering when transferred over a network. Therefore, network-connected devices are constantly exposed to invasive attacks by persons with malicious intent. Thus, cryptographic modules are regarded as requisite components in recent consumer electronic devices for protecting both digital content and the devices themselves from such attacks.

After timing attacks [1] and differential power analysis (DPA) [2] were reported, side-channel attacks (SCAs) were recognized as a serious threat to the electronic industry. SCAs reveal secret data sequences (usually encryption keys) handled by cryptographic modules by exploiting information leakage through analyzing physical parameters such as the power consumption of the cryptographic module and electromagnetic radiation emitted by the module during operation [3], [4]. There have been reported several SCAs such as Correlation Power Analysis (CPA) [5], Mutual Information Analysis (MIA) [6], Template Attack [7] and other stochastic methods [8] so far. For example of SCA in the real world, Moradi et al. reported in 2011 that they successfully extracted the secret cipher key embedded in the commercial FPGA [9], [10]. In 2012, Skorobogatov and his coworker reported that a backdoor[1], which requires a secret key to activate, was found in a military grade FPGA [11], [12].

In such situations, the international standard ISO/IEC 19790 for cryptographic modules will soon be revised to include security evaluation criteria with respect to SCAs. Therefore, the ability to examine the resistance of electronic devices against SCAs is becoming increasingly important. However, until recently there was no common environment for testing devices against SCAs, and this problem of non-uniformity and unavailability of testing environments led us to develop SASEBO [13]. SASEBO is an acronym for Side-channel Attack Evaluation Board and also serves as a collective name for our evaluation boards developed so far. SASEBO-GIII is our latest SCA evaluation board, which is equipped with a 28-nm FPGA.

SASEBO-GIII is suitable for studying various security-related issues and technologies, including hardware trojans, physical unclonable functions (PUFs) and security-critical systems, such as dynamic partial reconfiguration (DPR) systems [14]. In DPR systems, one or several modules can be replaced with other modules dynamically while the rest of the circuit continues to operate. DPR technology is considered a promising approach to reducing the size, power consumption and operating cost of electronic products. However, since FPGAs can be (re)configured in the field by downloading configuration data, attackers can embed such hardware trojans into the configuration bitstream. The Kintex-7 [15][2] FPGA on SASEBO-GIII is connected to and controlled by a Spartan-6 [16] FPGA, and therefore SASEBO-GIII provides various (re)configuration interfaces, such as Internal Configuration Access Port (ICAP) and SelectMAP for testing the feasibility of DPR systems, as well as standard configuration interfaces such as JTAG and Byte Parallel Interface (BPI).

[1]Note that the term *backdoor* is NOT used for indicating a malicious interface in their context. The backdoor here means an interface or functionality which is *not officially documented*.

[2]The device to be implemented has not yet determined. The current prototype is equipped with Kintex-325T, but can be Kintex-7 160T (101,400 6-input LUTs).

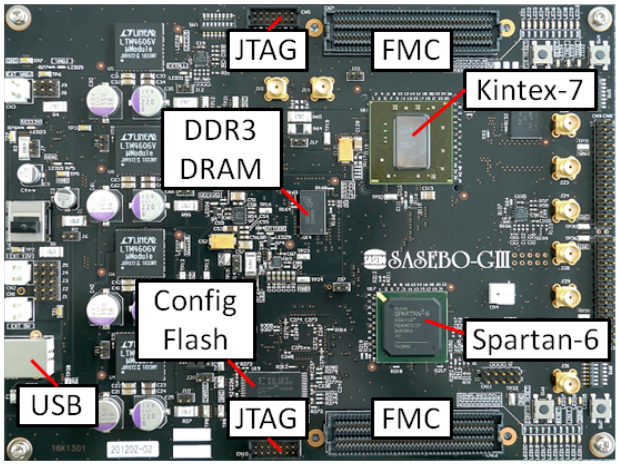

Fig. 1. Photograph of SASEBO-GIII.

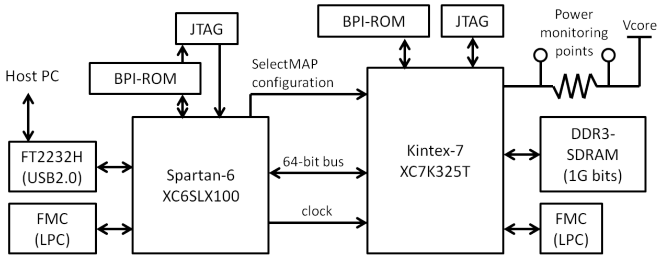

Fig. 2. Block diagram of SASEBO-GIII.

In this paper, the architecture and functionality of SASEBO-GIII are presented together with the results of an example SCA attack.

II. SASEBO-GIII

The main components and the block diagram of SASEBO-GIII are shown in Figs. 1 and 2, respectively, and a comparison of functionality between SASEBO-GIII and SASEBO-GII is summarized in Table I. Compared with the previous model SASEBO-GII, SASEBO-GIII is equipped with a Kintex-7 FPGA (a 10-fold increase in number of LUTs), USB 2.0 (a 40-fold increase in transfer speed) and 1 Gbit of DDR3-SDRAM (a 500-fold increase in memory capacity), providing sufficient hardware resources for system integration, multimedia data storage and DPR system implementation. Furthermore, one of the strongest advantages of SASEBO-III is its expandability through two standard FMC LPC connectors. Therefore, off-the-shelf boards with an FMC connector, for example, HDMI cards, Ethernet cards and camera boards, can be connected to SASEBO-GIII, enabling rapid prototyping of a wide variety of products. Therefore SASEBO-GIII is suitable for investigating the security of integrated systems as well as a cryptographic core. For example, SASEBO-GIII would be useful for implementing and testing Physical Unclonable Function (PUF) and its application [17], which is one of the hottest topics in the community of security research.

SASEBO-GIII provides high backward compatibility with previous models, such as SASEBO-G/-GII, and Verilog-HDL source code and control software [18], [19] designed for SASEBO-G/-GII can be used for SASEBO-GIII with only minor revision.

It should be emphasized that the SASEBO-GIII and -GII are designed to support Dynamic Partial Reconfiguration (DPR) systems, also referred to as Run-Time Reconfiguration (RTR) systems, where a hardware module can be replaced with another while the rest of the circuit is still running. The configuration pins of the Kintex-7 FPGA are connected to and controlled by a Spartan-6 FPGA, allowing the user to test complete and partial reconfiguration of the chip through various interfaces. Figure 3 through 6 show the different types of (re)configuration of the Kintex-7 device supported in SASEBO-GIII. In Fig. 3, the configuration bitstream of the Kintex-7 FPGA is transferred from the host computer to the Spartan-6 FPGA, and the Kintex-7 is configured through the SelectMAP interface (= configuration pins) under the control of the user logic in Spartan-6. Through the SelectMAP interface, the Kintex-7 can be entirely or partially configured. In Fig. 4, the bitstream is transferred from the host computer to the BPI flash memory. In this case, the stored bitstream is effective after the device is restarted. In Fig. 5, the bitstream is transferred to the DPR control logic in the Kintex-7 and the Kintex-7 is self-reconfigured through the ICAP interface. In this case, only partial reconfiguration can be performed since the DPR control logic cannot reconfigure itself. As illustrated in Fig. 6, the device can be reconfigured without the control of the host computer. The device can directly download the bitstream from the network and self-reconfigure the device.

III. SCA Example

To investigate if an SCA is feasible in the case of a state-of-the-art 28-nm FPGA, we performed correlation-based electromagnetic analysis (CEMA) [5] of a 128-bit (16-byte) AES module implemented on the Kintex-7 FPGA.

No countermeasures were implemented in the AES module. In CEMA, an attacker guesses one byte of the 16-byte key and obtains the state transition of the encryption process on the basis of the guessed key. Here, the correlation between the measured EM radiation and the state transition (= Hamming distance) calculated from the correct key becomes significantly higher than that calculated from wrong keys.

The experimental environment is illustrated in Fig. 7. Electromagnetic (EM) radiation is measured by a Langer LF-B3 EM probe and amplified with Miteq AU-3A-0150 (0.3-1000 MHz, 28 dB). After passing through the 5th-order Bessel filter, the signal is measured using Agilent DSO6104A digital oscilloscope. The power to the SASEBO-GIII board is supplied through USB, and the external power source is used to supply power to the amplifier.

The upper graph in Fig. 8 shows an example of an EM trace obtained during a single 10-round encryption, and the lower graph shows the correlation between the EM traces and the correct key $\{00\ 01\ 02\ \ldots\ 0F\}_{16}$. Figure 9 shows the number of bytes of the key correctly guessed during the CEMA. The entire 16-byte key is successfully extracted from 6,000 traces, showing that SASEBO-GIII is a suitable platform for SCA evaluation of cryptographic systems. Further experiments of EM analysis using SASEBO-GIII can be found in [20].

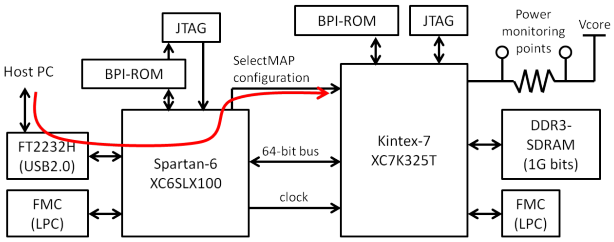

Fig. 3. Configuretion through SelectMAP interface.

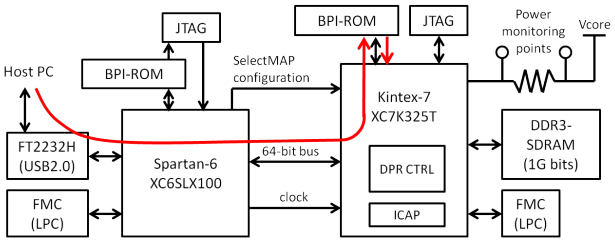

Fig. 4. Configuretion through BPI interface.

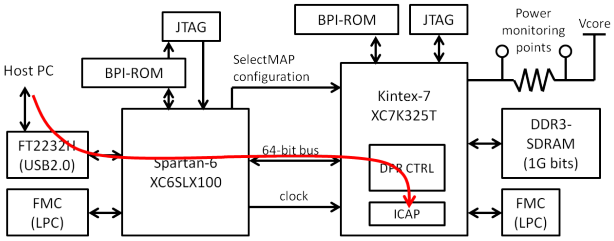

Fig. 5. Configuretion through ICAP interface.

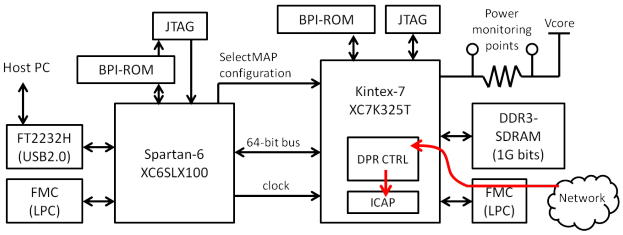

Fig. 6. Configuretion directly from the network through ICAP.

TABLE I
COMPARISON OF SASEBO-GIII AND SASEBO-GII

		SASEBO-GIII	SASEBO-GII
Cryptographic Device	FPGA	Kintex-7 325T (subject to change)	Virtex-5 LX30/50
	Process node	28-nm	65-nm
	Core voltage	1.0 V	1.0 V
	H/W resource	203,800 6-input LUTs	19,200/28,800 6-input LUTs
Control Device	FPGA	Spartan-6 LX45	Spartan-3A400
	Process node	45-nm	90-nm
	Core voltage	1.2 V	1.2 V
	H/W resource	27,288 6-input LUTs	7,168 4-input LUTs
Board Size		$250 \times 200\ mm^2$, 8 layers	$120 \times 140\ mm^2$, 6 layers
Communication Interface		USB 2.0 (480 Mbps)	USB 1.0 (12 Mbps)
Memory		1-Gbit DDR3-DRAM	2-Mbit SSRAM
FPGA Configuration Interface		BPI, JTAG, ICAP and SelectMAP	SPI, JTAG, ICAP and SelectMAP
Expandability		Two FMC connectors	Two 34-bit header pins (24-bit for user pins)
Monitoring Point		V_{core} line of Kintex-7	V_{core} and GND of Virtex-5

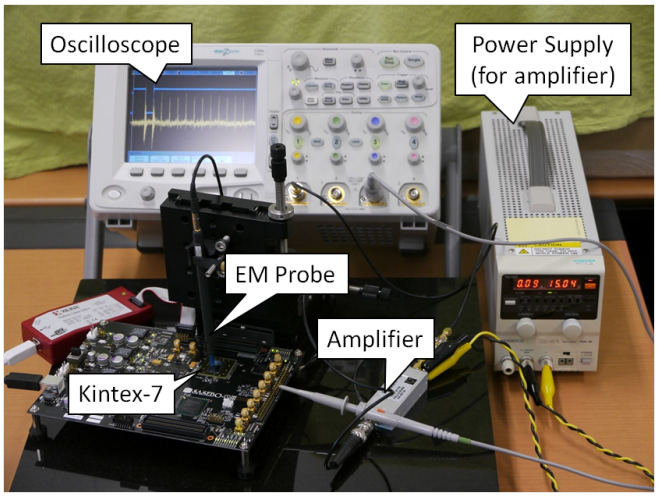

Fig. 7. The experimental environment for EM analsys.

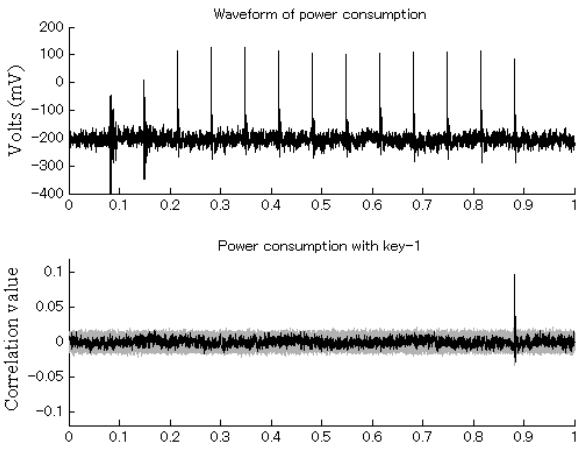

Fig. 8. Power traces and their correlation to the correct key.

IV. CONCLUSION

This paper presented the latest SCA evaluation board SASEBO-GIII equipped with the state-of-the-art 28-nm Kintex-7 FPGA. SASEBO-GIII provides a common experimental environment for investigating the security of various cryptographic systems against SCAs and other security issues. The Kintex-7 FPGA on the board can be (re)configured through several configuration interfaces, and thus SASEBO-GIII is useful for testing the feasibility and effectiveness of different types of reconfigurable systems, such as DPR systems. In the CEMA experiment conducted in this study,

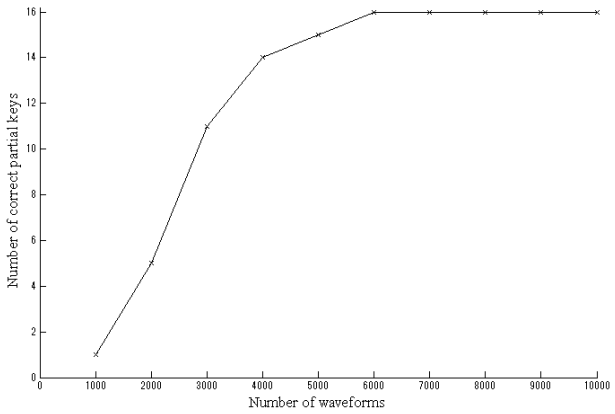

Fig. 9. Number of bytes of the correct key extracted by CEMA.

an AES module implemented without any countermeasures on the Kintex-7 FPGA resulted in extraction of the secret key from only 6,000 EM traces, demonstrating that SASEBO-GIII is useful for investigating the security of various consumer electronic devices.

ACKNOWLEDGEMENT

Part of this work was supported by the "Core Research for Evolutional Science and Technology (CREST)" funded by the Japan Science and Technology Agency (JST).

REFERENCES

[1] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems," in *CRYPTO'96*, 1996, pp. 104–113.
[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *CRYPTO'99*, 1999, pp. 388–397.
[3] J. J. Quisquater and D. Samyde, "Electromagnetic analysis (EMA): Measures and countermeasures for smart card," in *e-Smart'01*, vol. LNCS 2140, 2001, pp. 200–210.
[4] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *CHES'01*, vol. LNCS 2162, 2001, pp. 251–261.
[5] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," in *CHES 2004*, 2004, pp. 16–29.
[6] B. Gierlichs, L. Batina, and P. Tuyls, "Mutual information analysis," in *CHES2008*, 2008.
[7] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *CHES 2002*. Springer, 2003, pp. 51–62.
[8] K. Lemke-Rust, "Models and algorithms for physical cryptanalysis," Ph.D. dissertation, Ruhr-Universität Bochum, 2007.
[9] A. Moradi, A. Barenghi, T. Kasper, and C. Parr, "On the vulnerability of FPGA bitstream encryption against power analysis attacks—extracting keys from Xilinx Virtex-II FPGAs," Cryptology ePrint Archive, 2011.
[10] A. Moradi, M. Kasper, and C. Paar, "On the portability of side-channel attacks –an analysis of the Xilinx Virtex 4 and Virtex 5 bitstream encryption mechanism," Cryptology ePrint Archive, 2011.
[11] S. Skorobogatov and C. Woods, "In the blink of an eye : There goes your AES key (DRAFT of 28 May 2012)," IACR Cryptology ePrint Archive, 2012.
[12] ——, "Breakthrough silicon scanning discovers backdoor in military chip (DRAFT of 05 March 2012)," 2012. [Online]. Available: http://www.cl.cam.ac.uk/.../Silicon_scan_draft.pdf
[13] A. Satoh, T. Katashita, and H. Sakane, "Secure implementation of cryptographic modules—development of a standard evaluation environment for side channel attacks," *Synthesiology*, vol. 3, no. 1, pp. 56–65, 2010.
[14] *Partial Reconfiguration User Guide (UG702)*, Xilinx, Inc., 2010.
[15] *7 Series FPGAs Overview (DS180)*, Xilinx, Inc., 2012.
[16] *Spartan-6 Family Overview (DS160)*, Xilinx, Inc., 2011.
[17] Y. Hori, T. Katashita, and A. Satoh, "Tackling the security issues of FPGA partial reconfiguration with physical unclonable functions," in *ERSA 2012*, 2012, (to appear).
[18] "Side-channel attack standard evaluation board (SASEBO)," http://www.morita-tech.co.jp/SASEBO/ja/index.html, Morita Tech. Co., Ltd. SASEBO Web Site.
[19] "Cryptographic hardware project," http://www.aoki.ecei.tohoku.ac.jp/crypto/, aoki Lab., Tohoku University.
[20] Y. Hori, T. Katashita, A. Sasaki, and A. Satoh, "Electromagnetic side-channel attack against 28-nm FPGA device," in *Pre-proceedings of WISA*, 2012, (to appear).