Electromagnetic Side-channel Attack against 28-nm FPGA Device

Yohei Hori[1] ⋆, Toshihiro Katashita[1], Akihiko Sasaki[1], and Akashi Satoh[1]

1) National Institute of Advanced Industrial Science and Technology,
1-1-1 Umezono, Tsukuba, Ibaraki 305-8586, Japan

Abstract. Correlation-based electromagnetic analysis (CEMA), a type of side-channel attack (SCA), is conducted on the latest 28-nm field-programmable gate array (FPGA) device. SCA exploits physical information leakage from a cryptographic device such as power consumption and electromagnetic (EM) radiation to extract its secret key. The remarkable advance of large-scale integration (LSI) technology is such that power analysis of a cryptographic device is increasingly difficult due to reduced core voltages, on-chip capacitors, and so on. Consequently, the threat of EM analysis (EMA) has become the greater concern for cryptographic devices. To assess the feasibility of SCA against state-of-the-art LSI technology, we have developed the Side-channel Attack Standard Evaluation Board (SASEBO)-GIII equipped with Xilinx Inc.'s 28-nm Kintex-7 FPGA device. To demonstrate the suitability of SASEBO-GIII for SCA research, we performed CEMA on measured EM radiation emissions from the AES circuit of the Kintex-7 FPGA, and compared the results with those for EM radiation emissions from the 65-nm Virtex-5 FPGA on our previous SASEBO-GII evaluation platform. As a consequence, CEMA successfully extracted the entire secret key from the Kintex-7 FPGA on SASEBO-GIII with fewer wave traces than for the Virtex-5 FPGA on SASEBO-GII, showing that the noise reduction techniques utilized in SASEBO-GIII are highly effective for EMA. Notably, the results also indicated that the difficulty of EMA key extraction was dependent on the circuit structure rather than the key value. This paper explains the features of SASEBO-GIII, shows experimental CEMA results, and discusses the risk posed by EMA to leading-edge LSI technology.

Keywords: Side-channel attack (SCA), electromagnetic analysis (EMA), correlation-based EMA (CEMA), evaluation platform, field-programmable gate array (FPGA)

1 Introduction

Recently, cryptography has become an essential technology in information security, which protects the confidentiality, integrity, and availability of information. To ensure the security of cryptographic algorithms, by convention they are carefully evaluated in terms of computational complexity. Nevertheless, these algorithms can still be vulnerable when they are implemented on practical devices. Side-channel attacks (SCAs) are

⋆ This work is supported in part by the " Core Research for Evolutional Science and Technology (CREST) " project of the Japan Science and Technology Agency (JST).

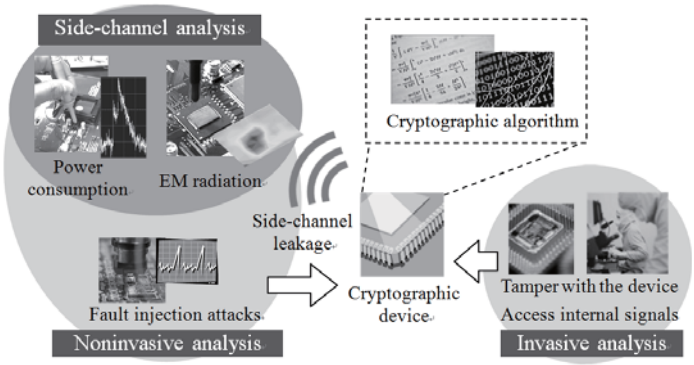

Fig. 1. Classification of physical attacks against cryptographic devices

noninvasive physical attacks, and are considered to be a serious threat to cryptographic devices. SCAs exploit the measurable phenomena of a device such as its power consumption, electromagnetic radiation, and operating times to extract its internal cryptographic key[1]. SCAs can be conducted by using inexpensive, general instruments, whereas invasive attacks require a more expensive setup that makes physical contact with the device to extract its internal signals.

With the introduction of differential power analysis (DPA) [2] to SCA research, early studies mainly focused on variants of power analysis. A power analysis is considered easier to conduct on a device than an electromagnetic analysis (EMA) even though it often requires a slight modification to the device's printed circuit board (PCB), for example, the setting up of a point to monitor the device's core voltage. However, electromagnetic (EM) radiation can be easily measured without any modification to a PCB, and can even be measured at distance. In addition, monitoring the power consumption of a device is becoming increasingly difficult due to the decrease of signal-to-noise ratio (SNR) brought about by core voltage reductions, on-chip decoupling capacitors, system-on-chip implementations, and so on. EMA has consequently become a greater threat than power analysis to cryptographic devices.

To test the feasibility of SCA against state-of-the-art large-scale integration (LSI) technology, we have developed a new experimental environment, the Side-channel Attack Standard Evaluation Board (SASEBO)-GIII [3], 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 [4], 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 on our previous SASEBO-GII for comparison. As a result, fewer wave traces were required for CEMA of SASEBO-GIII than of SASEBO-GII to correctly extract the entire secret key. In this paper, the architecture and functionality of SASEBO-GIII are described in detail, and the results of CEMA are presented and discussed.

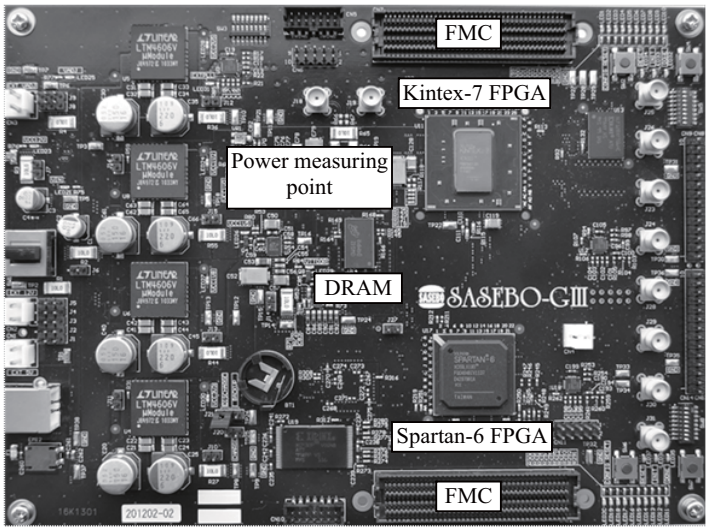

Fig. 2. Main components of SASEBO-GIII

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, attack methods can be categorized into two main types: invasive attacks that require tampering with the device to directly monitor its internal signals, and noninvasive attacks that observe internal information from outside of the device with a measuring instrument. In particular, SCAs are noninvasive physical attacks that exploit the measurable physical leakage of a device such as its power consumption and EM radiation. The establishment of DPA revealed that SCA is a serious practical threat to cryptographic devices. Since then, various research institutes have studied SCA methods and countermeasures; however, institutes typically use different apparatuses, so it is difficult to make a fair comparison between the experimental results and to arrive at a meaningful conclusion. To encourage SCA research under a uniform experimental platform, the National Institute of Advanced Industrial Science and Technology (AIST) and Tohoku University jointly developed SASEBO.

2.2 SASEBO-GIII

Process technology advances have lowered core voltages, and have thus reduced the power consumption of devices in general [5, 6]. Side-channel analysis 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 SASEBO-G with a 130-nm Virtex-II Pro FPGA device than on SASEBO-GII with a 65-nm Virtex-5 FPGA. To investigate the measurability of physical information

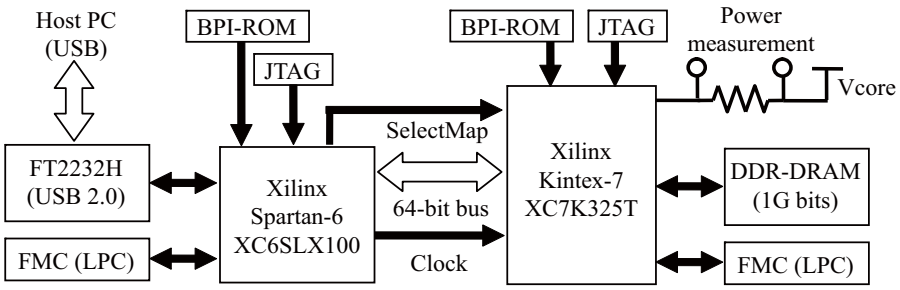

Fig. 3. Block diagram of SASEBO-GIII

leakage from the latest FPGA and the feasibility of SCA against leading-edge LSI technology, we have developed a new experimental platform, SASEBO-GIII, with a 28-nm process FPGA.

SASEBO-GIII's main components are shown in Fig. 2 and its characteristics are listed in Table 1 along with those of our previous SASEBO-GII board for comparison. SASEBO-GIII is equipped with a Xilinx Kintex-7 XC7K325T FPGA for testing cryptographic modules and a Spartan-6 FPGA for implementing control logic.

Note that SASEBO-GIII is suitable for evaluating the security of integrated systems, as well as that of a sole cryptographic core. The Kintex-7 XC7K325T FPGA [1] has greater than 10-fold the logic blocks (slices) of the Virtex-5 XC5VLX30 FPGA on SASEBO-GII, and therefore provides sufficient resources for implementing application logic. Additionally, two connectors adhering to ANSI's FPGA Mezzanine Card (FMC) standard are employed to enhance expandability. Thus, various off-the-shelf FMC boards such as video interface and Ethernet boards can be connected to SASEBO-GIII. Whereas a 2 Mb SSRAM chip is mounted on SASEBO-GII, a 1 Gb DDR3 DRAM memory is mounted on SASEBO-GIII, which realizes a wide variety of practical applications and offers ample space to store video streams, network packets, FPGA configuration data, and so on. The interface between SAEBO-GIII and a host computer is USB 2.0, and the data transfer rate is 40 times faster than that of USB 1.0 on the previous SASEBO boards.

As reported by Moradi and coworkers [7, 8], the embedded cryptographic module of some FPGAs can be broken by power analysis. SASEBO-GIII enables a user to evaluate the security of a vendor-provided cryptographic algorithm and explore countermeasures to ensure that the module is secure. SASEBO-GIII's block diagram is shown in Fig. 3. The configuration interfaces of the Kintex-7 FPGA are connected to, and controlled by, the Spartan-6 FPGA. This architecture is useful to investigate the security of an FPGA's configuration procedure. SASEBO-GIII also has an LR44 battery compartment, which was not mounted on previous SASEBO platforms, to supply power for battery-backed key storage. Hence, the Kintex-7 FPGA can be configured with an encrypted bitstream; however, note that the decryption key is embedded in its battery-backed flash memory.

[1] The Kintex-7 XC7K160T FPGA may also be chosen to reduce the price of the board. The XC7K160T FPGA has greater than 5-fold the logic blocks of the XC5VLX30 FPGA.

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

	SASEBO-GIII	SASEBO-GII
Board Size	$250 \times 200\ mm^2$, 8 layers	$120 \times 140\ mm^2$, 6 layers
Cryptographic Device	Kintex-7 325T, 28nm, 1.0v	Virtex-5 LX30/LX50, 65 nm, 1.0v
Control Device	Spartan-6	Spartan-3A
Communication Interface	USB 2.0 and two FMCs (LPC)	USB 1.0 and two 32-bit header pins
Memory	1-Gbit DDR3-DRAM	2M-bit SSRAM
FPGA config. Interface	BPI, JTAG and Select Map	SPI, JTAG and SelectMap
Monitoring Point	V_{core} line of Kintex-7	V_{core} and GND of Virtex-5

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

3 Experiments

To demonstrate the performance of SASEBO-GIII and its advantageous features, we measure the EM radiation emitted from the AES circuit of the 28-nm Kintex-7 mounted on the board and conduct CEMA under the Hamming-distance model. The S-Box of AES is implemented in the style of Compsite Field. Figure 4 shows an overview of the experimental environment. The waveforms of the emitted EM radiation are acquired by 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 at a position where the peak voltage of the measured radiation waveform was maximal. To investigate the dependence of the results on the device's process, the same experiment was also conducted on the AES circuit of the 65-nm Virtex-5 FPGA on SASEBO-GII[2].

Figure 5 presents example waveforms of the emitted EM radiation for SASEBO-GIII and -GII. The sampling interval here was 500 ns, and so a single waveform contains 10,000 values. The amplitude of SASEBO-GIII's waveform is one fifth that of -GII's waveform. A lower noise environment and more expensive instruments with higher precision are hence required to measure the side-channel information of state-of-the-art devices when evaluating physical vulnerability. In 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}$.

The results of key estimation by CEMA are shown in Figure 6. Contrary to our expectation that the device with a smaller process geometry would require a greater number of wave traces, CEMA required fewer waveforms to extract the entire 16-byte secret keys from the Kintex-7 FPGA on SASEBO-GIII than from the Virtex-5 FPGA on SASEBO-GII. All bytes of keys 1 and 2 were correctly extracted in 7,000 traces for

[2] The heat spreader of the Virtex-5 was removed to effectively measure the EM radiation.

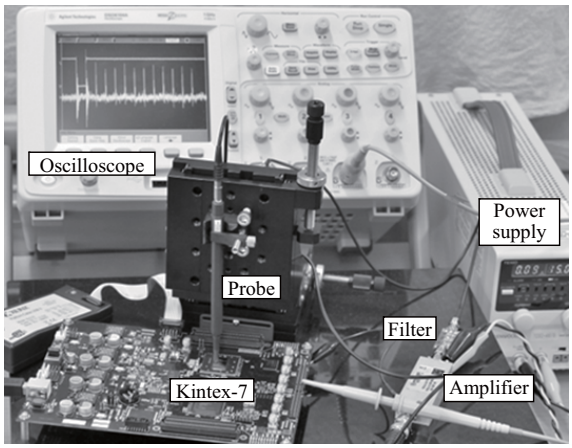

Fig. 4. Overview of experimental environment

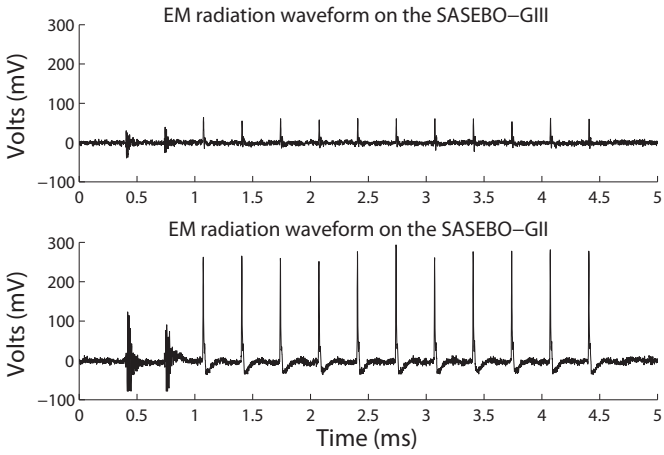

Fig. 5. Example waveforms of emitted EM radiation for SASEBO-GIII and -GII

SASEBO-GIII, whereas key 1 required 19,000 traces and key 2 could not be completely extracted for SASEBO-GII.

The correlation coefficients between intermediate subkey values and EM traces are shown in Figs. 7 (key1) and 8 (key2). The black and gray lines denote the correlations of the correct and incorrect subkeys, respectively. The trends of the correlation coefficients for SASEBO-GIII and -GII are clearly different. The average value of the correlation coefficient for SASEBO-GIII is smaller than that for SASEBO-GII, but the coefficients of all subkeys are similar for SASEBO-GIII, whereas those for SASEBO-GII are inconsistent. Notably, the incorrect extraction occurred for the 5th, 7th, 13th, and 15th byte of keys 1 and 2. The difficulty of EMA key extraction from cryptographic modules

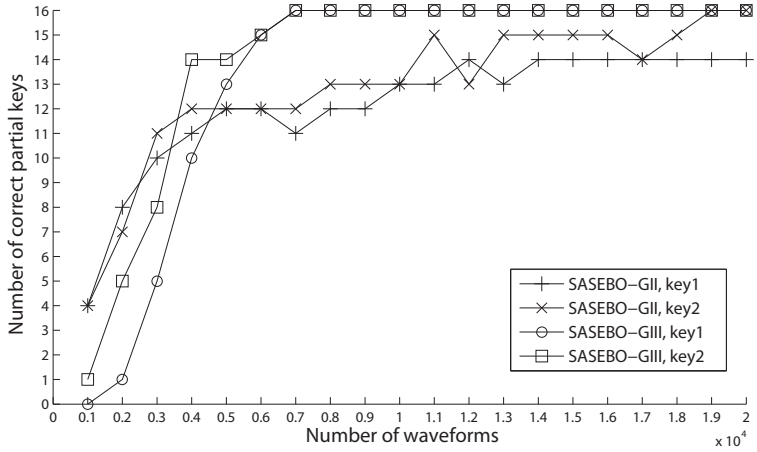

Fig. 6. Number of correctly extracted subkey bytes

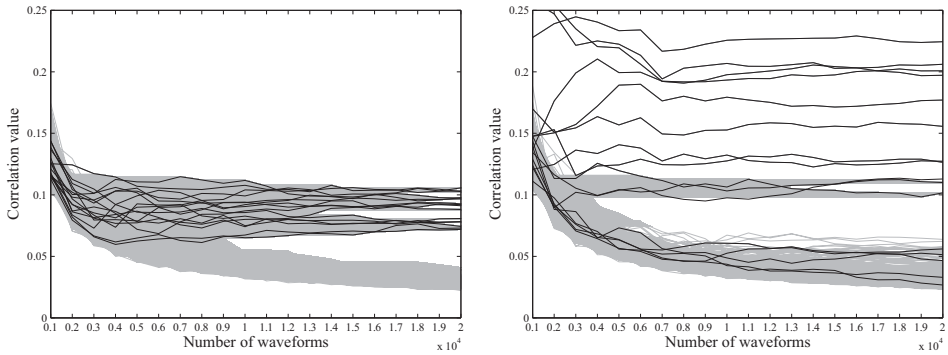

Fig. 7. Correlation between key 1 and EM traces for (left) SASEBO-GIII and (right) -GII.

is thus related to the positions of the subkey bytes and the circuit structure, not the key value.

To further investigate this relation, the SNRs of side-channel information [1] are calculated in Fig. 9, which shows the maximal SNR of each subkey over 50,000 EM traces. In addition to the key1 and 2, the key3 $\{00\ 00\ ...\ 00\}_{16}$ and key4 $\{FF\ FF\ ...\ FF\}_{16}$ are tested. We also implemented S-Box in the style of Positive Polar Reed-Muller (PPRM) whose results are illustrated as AES-PPRM in Fig. 9.

Bytes 5, 7, 13, and 15 of the keys on SASEBO-GII clearly have low SNR compared with the other subkeys. Additionally, the key1 through 4 in the same AES structure have the similar tendency of SNR. Hence, this figure also demonstrates that the success of EMA is reliant on the AES hardware structure rather than the key value.

Considering that all subkey bytes are successfully extracted from the Kintex-7 FPGA, suitable implementation of a cryptographic circuit is device dependent. We must there-

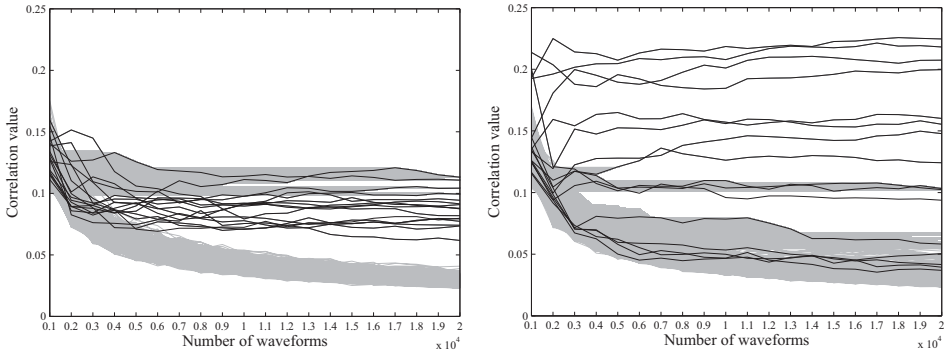

Fig. 8. Correlation between key 2 and EM traces for (left) SASEBO-GIII and (right) GII.

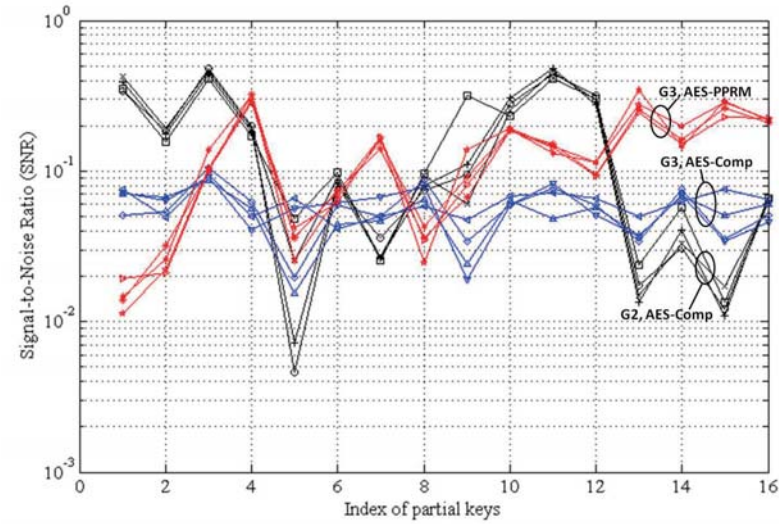

Fig. 9. Maximal value of side-channel SNR for each subkey

fore design the floorplan of a cryptographic circuit carefully to counteract SCAs. Investigation of such floorplans is considered future work.

4 Conclusion

We have developed a new SCA experimental board, SASEBO-GIII, with a leading-edge 28-nm Kintex-7 FPGA device. We conducted CEMA on measured EM radiation emissions from the AES circuit of the Kintex-7 FPGA, and also on those from the 65-nm Virtex-5 FPGA for comparison. The results showed that SASEBO-GIII has enhanced performance for observing side-channel information, although the measured voltage of SASEBO-GIII decreased to one fifth that of SASEBO-GII.

Contrary to our expectation, CEMA of the FPGA with smaller process geometry on SASEBO-GIII required fewer waveforms for successful key extraction than CEMA of the FPGA on SASEBO-GII did, verifying that SASEBO-GIII is suitable for SCA research purposes. Notably, subkeys at specific positions were difficult to extract for both keys tested, indicating that the difficulty of EMA key extraction was dependent on the structure of the cryptographic circuit rather than on the key value.

Future work of this study includes investigating the relation between SCA difficulties and circuit structure, implementing other cryptographic algorithms, and conducting various attacks against these algorithms such as differential EMA and mutual information-based attacks.

Acknowledgment

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., Popp, T.: Power Analysis Attacks. Springer-Verlag (2007)
2. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: CRYPTO’99. (1999) 388–397
3. Akashi, S., Toshihiro, K., Sakane, H.: Secure implementation of cryptographic modules—development of a standard evaluation environment for side channel attacks. Synthesiology **3**(1) (2010) 56–65
4. Brier, E., Clavier, C., Olivier, F.: Correlation Power Analysis with a Leakage Model. In: CHES 2004. (2004) 16–29
5. Klein, M.: Power Consumption at 40 and 45 nm. Xilinx, Inc. (2009)
6. Hussein, J., Klein, M., Hart, M.: Lowering Power at 28 nm with Xilinx 7 Series FPGAs (WP389). Xilinx, Inc. (2012)
7. Moradi, A., Barenghi, A., Kasper, T., Parr, C.: On the vulnerability of FPGA bitstream encryption against power analysis attacks—extracting keys from Xilinx Virtex-II FPGAs. Cryptology ePrint Archive (2011)
8. Moradi, A., Kasper, M., Paar, C.: On the portability of side-channel attacks –an analysis of the Xilinx Virtex 4 and Virtex 5 bitstream encryption mechanism. Cryptology ePrint Archive (2011)