A Novel Smart Card Development Platform for Evaluating Physical Attacks and PUFs

Toshihiro Katashita, Akihiko Sasaki, Yohei Hori
Research Institute of Secure Systems, National institute of Advanced Industrial Science and Technology,
Tsukuba, Japan

Abstract—**Smart cards are widely used in our life, and they handle sensitive information. The cryptographic modules on smart cards must be updated to support new algorithms and countermeasures against new threats. In this study, we designed a smart card board with an FPGA in order to develop and evaluate embedded circuits for smart cards. A smart card reader board for side-channel attack experimentation was developed in our previous study. By combining these boards and software, we constructed a platform to develop embedded hardware, software, and applications with smart cards for countermeasures against physical attacks and physical unclonable functions. The details of the platform are described in this paper, and side-channel attack experiments demonstrate that a cryptographic key was extracted from electromagnetic radiation on the smart card board, while a countermeasure with regulators and capacitors prevented attacks that exploit power consumption.**

Keywords-component; smart card; development platform; physical attacks; physical unclonable functions; embedded devices; FPGA

I. Introduction

Smart cards are widely used and handle authentication information, personal data, and so on. Therefore, cryptography is a fundamental technology for smart cards, and it is necessary to update its algorithms and architecture in order to support renewed algorithms and counter new attacks. Prototyping of embedded hardware on smart cards is required to evaluate new architecture, applications, and so on. However, a hardware development environment for smart cards does not exist, but processor-embedded smart card evaluation kits for software design are available.

In order to accelerate the development of embedded hardware for smart cards, we have developed an FPGA board with dimensions close to ISO/IEC 7816-2 standards. The Spartan-6 LX45 FPGA has adequate logic resources to implement processor IPs, cryptographic modules, physical unclonable functions (PUFs), and interface circuits. By employing the smart card reader board SASEBO-W [1] and designing the essential control software, we additionally construct a smart card development platform.

In this paper, the details of the environment and characteristics of the smart card FPGA board are described. Preliminary experimentation with side-channel attacks demonstrates that electromagnetic (EM) radiation analysis is a threat, while a regulator circuit suppresses the leakage of the internal information on the FPGA device.

II. Smart Card Development Platform

Figure 1 shows the smart card board. The board is equipped with a 45-nm Spartan-6 LX45 FPGA and a power supply circuit. The dimensions of the PCB are 86.0 mm by 54.0 mm. The PCB is 0.8 mm in thickness, and thin devices are mounted on half plane of the back side in order to fit to card sockets. Contact pads are located on both sides of the board. The detailed specifications are listed in Table 1.

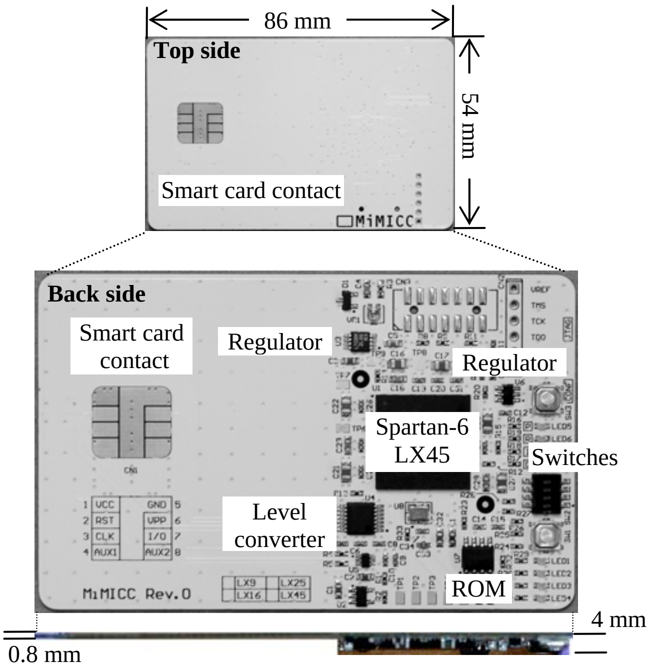

Figure 1. Experimental smart card board

Table 1. Specifications of the smart card development board

	Smart card development board
Device	Xilinx Spartan-6 LX45 FPGA
Configuration	SPI ROM, JTAG header pad
Power supply	Single 3.0–5.0 V supply through smart card interface
Size	$86.0 \times 54.0 \times 0.8$ mm^3, 4 layers Maximum height is approximately 4.0 mm

Clock	Smart card interface and internal 24 MHz
Interface	Smart card interface on both sides of the board Signal voltage is adjusted by a level converter

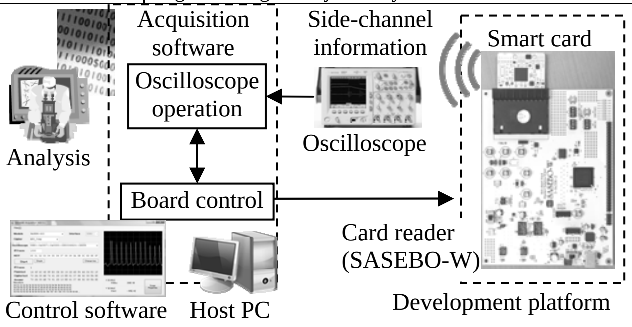

Figure 2. Experimental environment for side-channel attacks

Figure 2 shows an experimental environment for side-channel attacks [2] by using our smart card development platform. The SASEBO-W board is used as a smart card reader, and it has measuring functions for power consumption and EM radiation of smart cards.

III. Side-Channel Analysis Experiments

The power consumption and EM radiation of an Advanced Encryption Standard (AES) implementation was measured during processing on the smart card board. The measured waveforms were analyzed by correlation power analysis (CPA) [3]. The power waves were measured with the SASEBO-W smart card reader. The EM radiation waves were traced on the top of the FPGA devices by a Langer LF-B3 probe and were amplified by a Miteq AM-00110 amplifier (0.3–1000 MHz, 28 dB). Each waveform was captured at a 20 GSa/s sampling rate with an Agilent DSO9104A oscilloscope. Example waveforms are shown in Figure 3. The power waveform exhibits the same peaks at each clock cycle owing to the regulator and capacitors on the smart card board. In contrast, 11 peaks in the EM radiation waveform reveal AES processing.

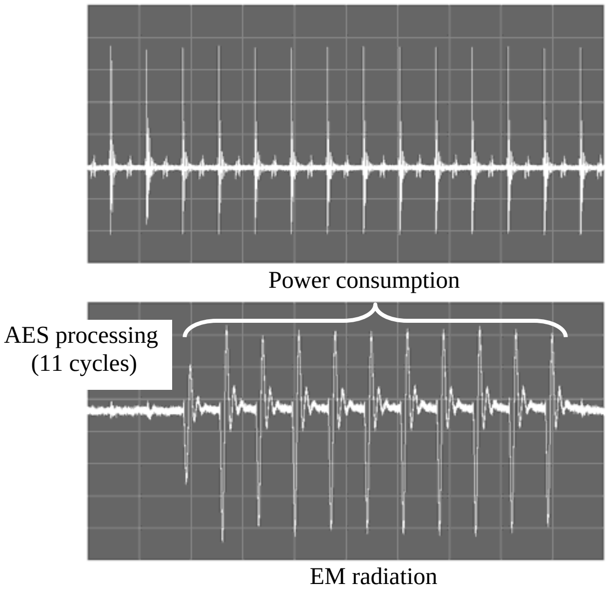

Figure 3. Example power consumption and EM radiation waveforms

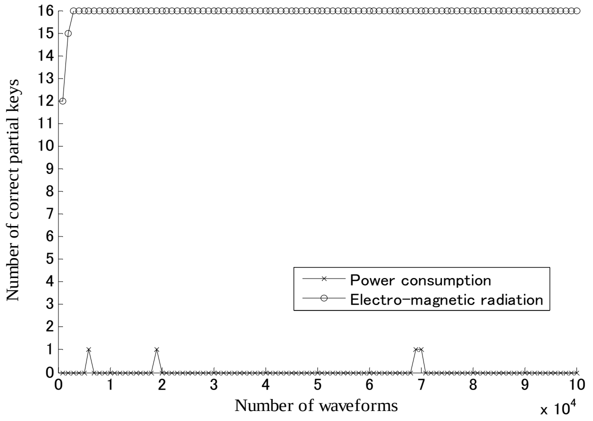

Figure 4. CPA results

Figure 4 shows the number of extracted partial AES keys by CPA. In the analysis, a 128-bit (16-byte) key is separated to one byte, and each partial key is analyzed independently. When the number of correct keys reaches 16 bytes in Figure 4, the cryptographic key is successfully extracted. This result illustrates that hiding the power consumption of AES processing by regulators and a capacitor works well as a countermeasure against CPA. However, a small amount of EM radiation from the device leaks the internal information. Hence, the key is analyzed correctly with 3,000 waveforms, while no partial key is extracted by 100,000 waveforms of power consumption. In the experiments, good results against CPA are obtained by hiding the power consumption. We plan to investigate the efficiency of the power supply circuit with various other analysis methods.

IV. Conclusion

In this paper, we detail a smart card development board and platform, and preliminary experiments demonstrate the evaluation of side-channel attacks by measuring the power consumption and EM radiation. In the future, we plan to conduct experiments with various analyses and to investigate side-channel information leakage. We will also conduct experiments with PUF circuits on our platform.

Acknowledgment

This study was conducted as part of a Core Research for Evolutional Science and Technology (CREST) project funded by the Japan Science and Technology Agency (JST).

References

[1] T. Katashita, Y. Hori, H. Sakane, and A. Satoh: Side-Channel Attack Standard Evaluation Board SASEBO-W for Smartcard Testing, Non-Invasive Attack Testing Workshop (NIAT), 2011,

http://csrc.nist.gov/news_events/non-invasive-attack-testing-workshop/papers/10_Katashita.pdf.

[2] S. Mangard, E. Oswald, and T. Popp: Power Analysis Attacks, Springer Science Business Media, LLC, ISBN 978-0-387-30857-9, 2007.

[3] E. Brier, C. Clavier, and F. Olivier: Correlation Power Analysis with a Leakage Model, *CHES 2004*, LNCS 3156, pp. 16–29, 2004.