FPGA Prototyping of a Smart Card Platform for Evaluating Tamper Resistance of Cryptographic Circuits

Hiroyuki Kanbara
ASTEM RI
134 Chudoji Minamimachi
Shimogyo-ku Kyoto, 600-8813, Japan

Naoya Ito* Hinata Takebayashi
School of Science and Technology
Kwansei Gakuin University
2-1, Gakuen
Sanda, Hyogo, 669-1337, Japan

Muneyuki Takenae
College of Science and Engineering
Ritsumeikan University
1-1-1 Noji-Higashi
Kusatsu, Shiga 525-8577, Japan

Takashi Tsukamoto
IT Seculity Center
Information-technology Promotion Agency, Japan
Bunkyo Green Court Center Office
2-28-8 Honkomagome, Bunkyo-ku, 113-6591, Tokyo, Japan

Abstract— This article presents a smart card platform to evaluate tamper resistance of cryptographic circuits. Tamper resistance means difficulty of revealing sensitive information like cryptographic keys of a cryptographic device tampered with in order to make the device behave abnormally. Users of this platform can manipulate their own cryptographic circuits which are connected to a co-processor bus circuit and attempt to extract the key inside the circuit in non-invasive way called side-channel attacks. An RSA encryption/decryption Circuit, an AES encryption/decryption circuit and a random number generation circuit are designed as a reference and integrated with the platform. The platform with these circuits is implemented using Xilinx FPGA.

I. Introduction

Smart cards are widely used as cryptographic devices which provide authentication of users or store personal information. Symmetric encryption algorithm like the Data Encryption Standard (DES) or the Advanced Encryption Standard (AES) [1] is used to keep a secret of communication between a smart card and a card reader device. Asymmetric cryptography provides a mutual authentication between a smart card and a card reader or exchanges a common secret key safely. The most popular asymmetric one is the Rivest-Shamir-Adleman (RSA) algorithm [2]. Cryptographic circuits that implements the cryptographic algorithm and that store cryptographic keys are included in smart cards. If these cryptographic keys are extracted in an unauthorized way by an attacker, he/she can pretend to be someone else and get sensitive personal information.

Widely used cryptographic algorithms are verified by experts and considered to be secure in practice. If the number of bits of a secret key is long enough, it it almost impossible to find the secret key from pairs of plain texts and cipher texts within a reasonable amount of time and with a reasonable amount of computing power.

Execution time of encryption/decryption, power consumption or electromagnetic field of cryptographic devices are called as side-channel information [3]. Side-channel information can be gathered with a digital oscilloscope or a Personal Computer (PC). Side-channel attack is based on these information to break security of cryptographic devices and does not require expensive equipment. The secret key can be revealed by observing physical properties of the device.

Simple Power Analysis (SPA) and Differential Power Analysis (DPA) [4] were introduced by Kocher et al. in 1990s and are powerful side-channel attack methods. The basic idea of these attacks is to reveal the key of a cryptographic device by analyzing its power consumption. Side-channel attacks receives a large amount of attention because they are very powerful and they can be conducted easily. At Conference on Cryptographic Device and Embedded System (CHES), almost half of the presentations deals with side-channel attacks.

While methods of side-channel attacks have been developed, research of countermeasures has been in progress. Smart card platform for estimating efficiency of countermeasures for side-channel attacks evolved in future becomes more important.

SASEBO-W is a smart card reader board for testing and evaluating tamper resistance of smart cards [5]. MiM-ICC Card is a smart card board with an FPGA for prototyping smart card hardware [6]. Combination of these two boards works as a environment for side-channel attacks to cryptographic circuits. Still smart card hardware and software for controlling cryptographic circuits is needed for the evaluation.

*Naoya Ito is currently with Murata Manufacturing Co., Ltd.

The authors have developed a smart card platform to evaluate tamper resistance of cryptographic circuits. This platform consists of an embedded CPU, a memory, a UART interface(IF) circuit, and a co-processor bus for controlling user designed cryptographic circuits. With this platform, user manipulates their cryptographic circuits and attempts to tamper with them. An RSA encryption/decryption Circuit, an AES encryption/decryption circuit, and a random number generation circuit are implemented and connected to the co-processor bus. The platform is written in Verilog-HDL and synthesized for mapping to Xilinx Spartan-6 FPGA device. Middleware based on ISO/IEC-7816 standard is developed for communicating with PC and manipulating the reference circuits.

II. Smart Card Platform for Evaluating Tamper Resistance

Users of the smart card platform attempt to attack to cryptographic circuits and exploit a secret key in a non-invasive way. Countermeasures against assumable side-channel attacks can be evaluated through experimental attack. Fig.1 shows block diagram of the platform. The smart card platform provides functions as follows.

- A user read or write contents of a memory via RS232C serial communication.
- An Embedded CPU executes a program in the memory.
- The CPU puts input data and receive output result calculated by user designed cryptographic circuits attached to a Co-processor Bus.

A. Embedded CPU

An Embedded CPU is a RISC processor with 5-stage pipeline [7]. C program for this CPU can be compiled with GNU C Compiler (GCC). The CPU interprets commands following ISO/IEC 7816 and transfer input data (ex. a secret key and a plain text) and output result (ex. a cipher text) to user cryptographic circuits connected to a Co-processor Bus circuit. Memory map is shown in Fig. 2. When CPU is turned on, value of a Program Counter of the CPU becomes 0x0028 0000 asynchronously. When an interrupt request is accepted or an exception is occurred in the CPU, the program counter jumps to an interrupt handler address : 0x0028 0080.

B. Co-processor Bus Circuit

User designed circuits for cryptographic or random number generation (RNG) can be attached to a Co-processor Bus Circuit in Fig.1. If a user tries to tamper a true random number generator or a physically unclonable

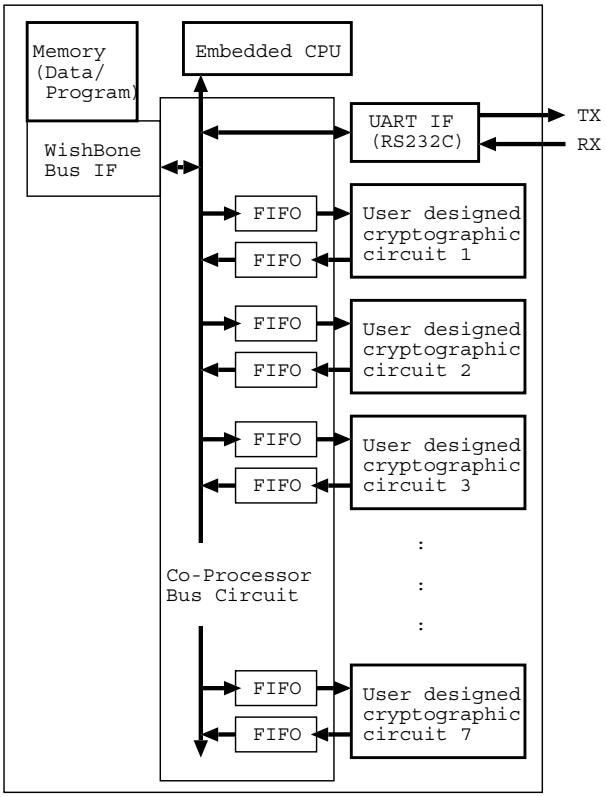

Fig. 1. Block diagram of the platform

function (PUF) circuit, ASIC implementation of this platform and these circuits will be used. Data input/output and execution of encryption/decryption of the attached circuits can be controlled via the Co-processor Bus Control Registers in Fig.2. User of the platform should add the Co-processor Bus interface functions to their own circuits. At most 7 circuits can be connected to the Bus.

C. UART IF

A UART IF circuit interprets original commands delivered from a PC with RS232C interface and reads/writes the memory and controls program execution by the CPU. Communication complying with ISO/IEC 7816 standard between the CPU and a PC is also carried out via the UART IF(RS232C).

D. WishBone Bus IF

The embedded CPU is connected with a WishBone Bus IF circuit to the memory. The Co-processor Bus IF circuit has a master interface of the WishBone Bus specification. Other memory module circuit with a slave interface of the WishBone Bus can be attached. The WishBone Bus IF circuit reads a memory following "Classic standard SINGLE READ Cycle" and writes a memory following "Classic standard SINGLE WRITE Cycle".

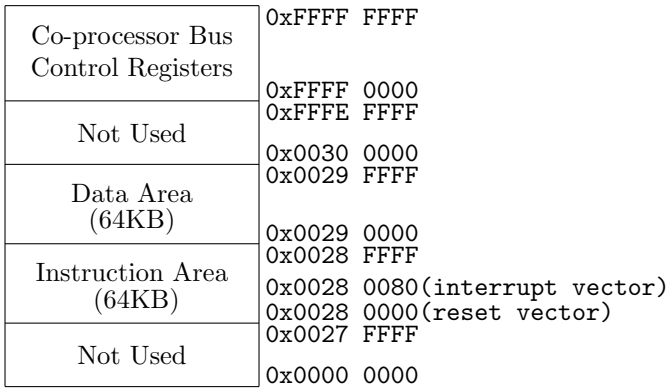

Fig. 2. Memory map

III. ISO/IEC 7816 Middleware

Communication middleware complying with ISO/IEC 7816 standard is developed for the platform to communicate with other device. This middleware can be compiled with GNU C Compiler. Compiled binary program is written to the memory of the platform through the UART IF circuit and executed by the CPU. The UART IF supports RS232C serial communication standard and its electrical interface does not meet ISO/IEC 7816-3 because the FPGA implementation of the platform communicates with a PC.

Application Protocol Data Unit (APDU) is transmitted by Transportation Data Protocol Unit (TPDU) defined in T=0 transmission protocol of ISO/IEC 7816-3. The T=0 protocol is a character-based transmission protocol and defined as a sequence of messages exchanged between a smart card and a card reader, as follows.

- A PC substituting a card reader sends a command to the smart card platform.
- The platform sends back a response message following the T=0 protocol definition.
- The command is constituted of a command header and a command data. The command header is composed of 5 bytes characters, CLA, INS, P1, P2 and P3. The CLA is a Class of Instruction byte and The INS is an instruction byte. The P1, P2 and P3 are parameter bytes.
- The response consists of response data and status bytes. The status bytes are 2 characters called SW1 and SW2. Maximum length of the command data is 255 bytes and of the response data is 256.

Fig.3 is an example of an APDU command which controls the random number generation circuit designed as a reference and attached to the Co-processor bus.

```
# Set length of generated random number:0x0C(12)
L "8040" -l "00 00 0C 00"
# Set seed value : 0x000a 414a
L "8045" -l "4a 41 0a 00"
# Invoke random number generation
L "8042"
# Read out all generated random number
L "804401" -r 1024
```

Fig. 3. APDU commands sample for controling the RNG circuit

IV. Reference Circuits Designed for the Platform

Cryptographic and a random number generation circuits for the co-processor bus are implemented for reference. Following is an outline of these circuits.

A. RSA Encryption/Decryption Circuit

An RSA encryption/decryption circuit for 2048 bit key length is designed with binary-synthesis compiler called ACAP [8]. The ACAP compiler synthesizes Verilog-HDL of the circuit from the binary code compiled with GCC. An RSA encryption/decryption program written in C is linked with simplified GNU Multi-Precision Library [9]. This circuit receives a public key, a secret key and a plain text and generates a cipher text.

B. AES Encryption/Decryption Circuit

An AES encryption/decryption circuit is designed manually. An algorithm for AES encryption/decryption is described in C and Verilog-HDL for the circuit is written by hand referencing to the C program. The embedded CPU of the platform generates a round key data from a common key and pushes the round key and a plain text to the AES circuit and invoke encryption.

C. Random Number Generator (RNG) Circuit

A random number generator (RNG) circuit is synthesized with the binary-synthesis compiler ACAP in the same way as the above mentioned RSA circuit. Pseudorandom numbers are generated from a random number seed following Mersenne twister algorithm [10].

V. Environment for Evaluating Tamper Resistance

Fig.4 shows an environment to evaluate tamper-resistance of cryptographic circuits integrated to the platform from side-channel attacks. User of the platform attaches their own cryptographic circuits to the co-processor

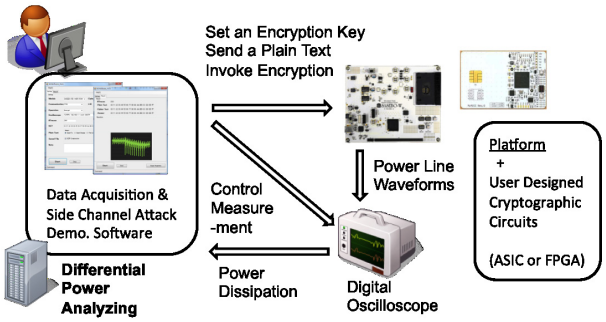

Fig. 4. Experimental environment for side-channel attacks

bus and implements them with ASIC or FPGA. The attached cryptographic circuit is controlled by the embedded cpu executing the ISO/IEC 7816 middleware and interpreting a command sent by the PC. Also a PC software specialized for the DPA attacks is constructed. The software provides functions as follows.

- Send a secret key and plain texts to the cryptographic circuit of the platform
- Invoke encryption or decryption
- Control a digital oscilloscope and measure power consumption variation of the platform
- Exploit a secret key automatically from the power consumption data

VI. Design Result

The smart card platform integrated with the RSA encryption/decryption, the AES encryption/decryption, and the random number generation (RNG) circuit is synthesized with Xilinx ISE 14.1 and mapped to a Xilinx Spartan-6 LX150 device on SASEBO-W board in Fig.5. TABLE I summarizes the synthesized result of the platform with the RSA, the AES, and the RNG circuits. The RSA, the AES, and the RNG circuits are tested using APDU commands sent from a PC and operate normally. If a user attempts to implement this platform to a Spartan-6 LX45 device on MiMICC Card, only the AES and RNG circuits should be included to the platform because of the limitation of maximum circuit scale to be mapped.

VII. Conclusion

A smart card platform for evaluating tamper resistance of cryptographic circuits is constructed. Users of the platform integrated with their own cryptographic circuits attempt to extract the key inside the circuits and evaluate

TABLE I
FPGA Mapping Result

	Slices	FFs	LUTs	Delay[ns]
Platform(with RSA,AES and RNG circuit)	11,614	11,927	31,510	21.9

countermeasures against side-channel attacks. The platform including an RSA encryption/decryption circuit, an AES encryption/decryption circuit and a random number generation circuit is implemented using Xilinx FPGA and tested. In future, performing side-channel attacks with this platform not only to the AES/RSA circuits for reference But also to cryptographic circuits designed by others is planned.

Acknowledgements

We would like to thank to all the people who contributed, especially Mr. Takayuki Nakatani who was with Ritsumeikan University, Mr. Masaharu Yano who was with Kyoto University and Mr. Shimpei Tamura who was with Kwansei Gakuin University for their former contribution. This work has been made possible by appropriate assistance by Information-technology Promotion Agency, Japan(IPA).

References

[1] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES) FIPS Publication 197," http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, Nov. 2001.

[2] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* 21.2, pp. 120-126, 1978.

[3] S. Mangard, E. Oswald, and T. Popp, "Power Analysis Attacks - Revealing the Secrets of Smart Card," Springer Science Business Media, LLC, ISBN 978-0-387-30857-9, 2007.

[4] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," CRYPTO 1999, Lecture Notes in Computer Science, vol.1666, pp.388-397, 1999.

[5] 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.

[6] T. Katashita, S. Akihiko, and Y. Hori, "A Novel Smart Card Development Platform for Evaluating Physical Attacks and PUFs, " *2013 IEEE 2nd Global Conference on Consumer Electronics (GCCE)*, 2013.

[7] G. Kane, "mips RISC Architecture," Prentice-Hall, 1988.

[8] N. Ishiura, Hiroyuki Kanbara, and Hiroyuki Tomiyama, "ACAP: Binary Synthesizer Based on MIPS Object Codes," *in Proc. International Technical Conference on Circuit/Systems Computers and Communications (ITC-CSCC 2014)*, pp. 725728, July 2014.

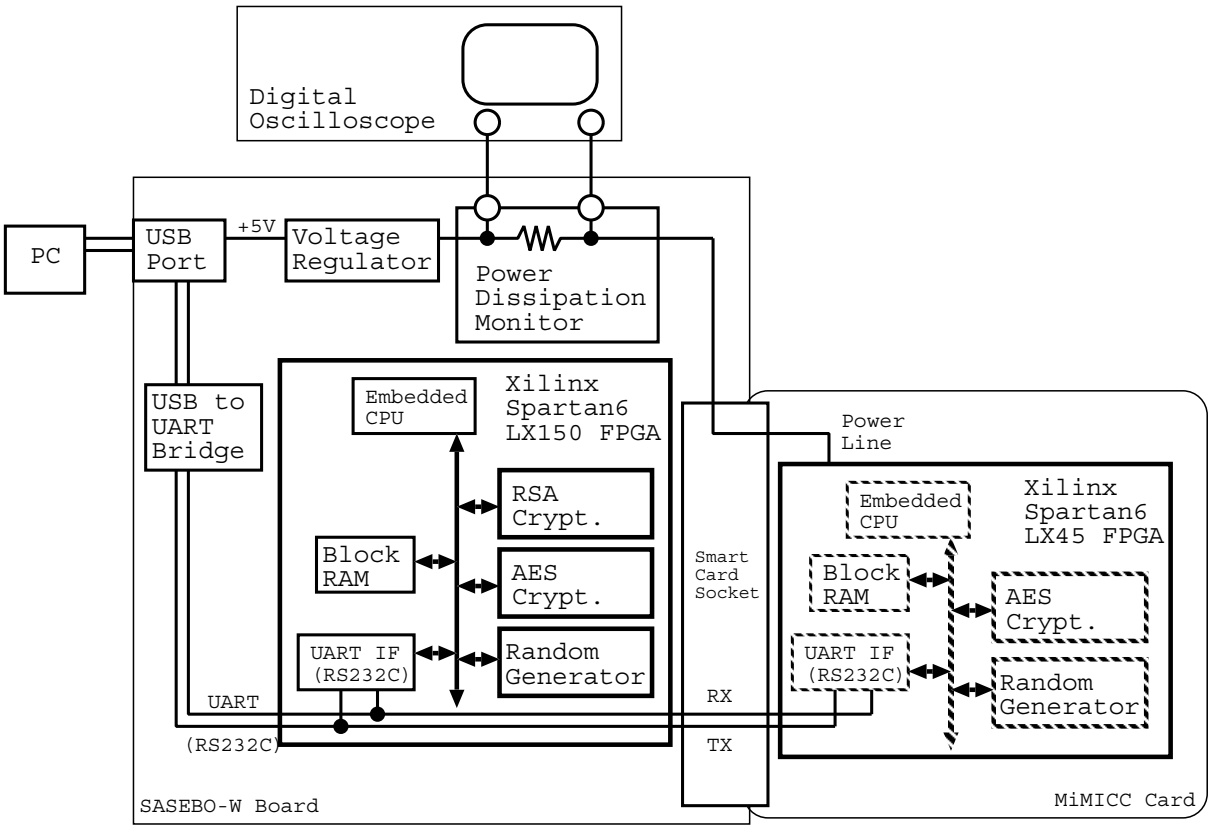

Fig. 5. Platform implementation environment

[9] http://gmplib.org/ (accessed 2015-07-01).

[10] M. Matsumoto and T. Nishimura, "Mersenne twister: A 623-dimensionally equidistributed uniform pseudorandom number generator, " *ACM Trans. on Modeling and Computer Simulations*, 1998.