Side-Channel Attack Standard Evaluation Board SASEBO-W for Smartcard Testing

Toshihiro Katashita [1], Yohei Hori [1], Hirofumi Sakane [1,2], Akashi Satoh [1]

1) National Institute of Advanced Industrial Science and Technology, Japan

2) National Institute of Standards and Technology, USA

Abstract**—Side-channel Attack Standard Evaluation BOards (SASEBOs) were developed as uniform evaluation platforms for research purposes. Cryptographic hardware, and control circuits for side-channel experimentation were also developed, and these platforms have been distributed to the government, the industry and academic research labs in order to facilitate research and development directed toward the establishment of an international standard for side-channel attacks. With standardization, testing environments are required to support security evaluation of side-channel attacks. In order to accelerate the adoption of the standard, we developed a new evaluation board named SASEBO-W for testing and evaluating smartcards, which are the most widespread cryptographic modules. The board supports ISO/IEC 7816-3 electrical interface smartcards and provides fine-grained control and trigger features with a control circuit implemented on an FPGA. A smartcard OS and cryptographic software for the ATMega 163 card were also developed. In this paper, the features of a variety of SASEBOs and side-channel attack tools are explained, and the analysis results for the power consumption and the electromagnetic radiation of a smartcard as obtained experimentally with SASEBO-W are presented.**

I. Introduction

Side-channel attacks constitute non-invasive physical attacks, which exploit measureable parameters of cryptographic devices to extract the internal key. A standard environment is needed for the purpose of comparing different attack algorithms and the efficiency of countermeasures [1]. Although the construction of a uniform testing environment is crucial for the formulation of international standards, it is difficult to standardize evaluation schemes proposed by different research institutions as each of them uses their own experimental equipment.

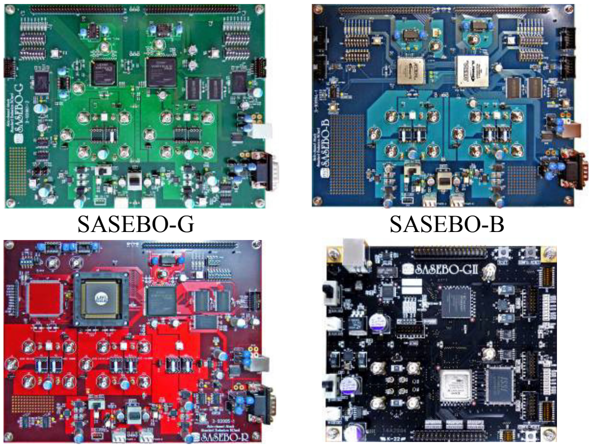
To contribute to these standardization efforts, we have developed Side-channel Attack Standard Evaluation BOards (SASEBOs), cryptographic circuits, IP macros and software, and have distributed them to over 100 government, industry and academic research laboratories. There are four types of SASEBO platforms, all of which use FPGAs and custom ASIC LSIs to implement experimental cryptographic circuits. Various side-channel attack experiments have been conducted by using the SASEBO platforms, and useful results were obtained.

With standardization, the testing environments are required to support security evaluation of side-channel attacks. To provide such support, we developed a new evaluation board, SASEBO-W, for testing smartcards, which are the most widespread cryptographic modules. This board supports ISO/IEC 7816-3 electrical interface smartcards and provides fine-grained measurement features with a control circuit implemented on FPGAs. We also developed a smartcard OS and cryptographic software for the ATMega 163 card as a target in side-channel attack experiments.

In this paper, the details of SASEBO and the new board are described, and their suitability as testing environments for side-channel attacks is demonstrated by performing a side-channel analysis experiment involving power consumption and electromagnetic (EM) radiation.

II. Side-channel Standard Evaluation Board

The four types of SASEBO platforms and LSIs are shown in Figs. 1 and 2, respectively. SASEBO-G and SASEBO-B employ Xilinx and Altera FPGAs (Field Programmable Gate Arrays), which provide user reconfigurability of circuit functions for implementation of cryptographic algorithms. The circuits for RSA and all the ISO/IEC 18033-3[2] standard block ciphers were designed to allow for side-channel attack experiments with various cryptographic algorithms. By using cryptographic modules, four types of LSIs were fabricated with 65-, 90- and 130-nm CMOS standard cell process. These LSIs can be mounted on a socket on SASEBO-R. Furthermore, SASEBO-GII is the successor of SASEBO-G and equips a cryptographic FPGA with a 4-fold higher logic capability. The usability of the board is further improved by a low-noise power supply system utilizing a USB port, as well as by its small size, which is about one-third that of SASEBO-G. The features of the boards and the LSIs are summarized in Tables 1 and 2, respectively.



SASEBO-G

SASEBO-B

SASEBO-R

SASEBO-GII

Figure 1: SASEBOs.

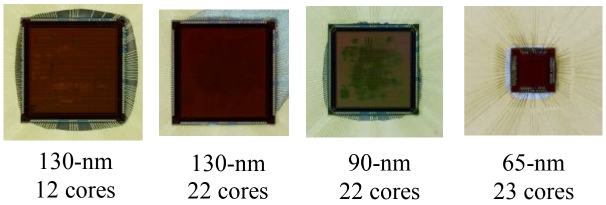


Figure 2: Cryptographic LSIs.

Table 1: Basic features of four variants of SASEBO

	SASEBO -G	SASEBO -R	SASEBO -B	SASEBO -GII
Cipher device	Xilinx VirtexII pro 7	Custom LSI	Altera StratixII 15	Xilinx Virtex5 LX30/50
Control device	Xilinx VirtexII pro 30	<<	Altera StratixII 30	Xilinx Spartan 3A 400
Power supply	Two 3.3V DC supply lines	<<	<<	USB 5.0V DC power supply
Monitor point	Shunt resistors at Vcc, Vio and GND lines	<<	<<	Shunt resistors at Vcc and GND lines
Clock	24 MHz crystal	<<	<<	<<
Local bus	48-bit	<<	<<	38-bit
IF	USB RS-232	<<	<<	USB
EXT IF	64-bit pins	<<	<<	32-bit pins
Size	230 x 180 x 1.6 mm^3, 8 layers	<<	<<	120 x 140 x 1.6 mm^3, 8 layers

Table 2: Basic features of cryptographic LSIs

Generation	1st	2nd	3rd	4th
Technology	TSMC 130 nm	<<	TSMC 90 nm	e-shuttle 65 nm
Algorithms	AES, DES, MISTY1, Camellia, SEED, CAST and RSA	AES, 3DES, MISTY1, Camellia, SEED, CAST, ECC, and RSA	<<	AES, 3DES, MISTY1, Camellia, SEED, CAST, ECC, RSA, and CLEFIA
#Cores	13, AES (7cores)	22, AES (14 cores)	<<	23, AES (14 cores)
Package	QFP 160-pin	<<	<<	<<
Size	5.0 x 5.0 mm^2	<<	4.0 x 4.0 mm^2	2.1 x 2.1 mm^2
Voltage	1.2V	1.2V	1.0V	1.2V

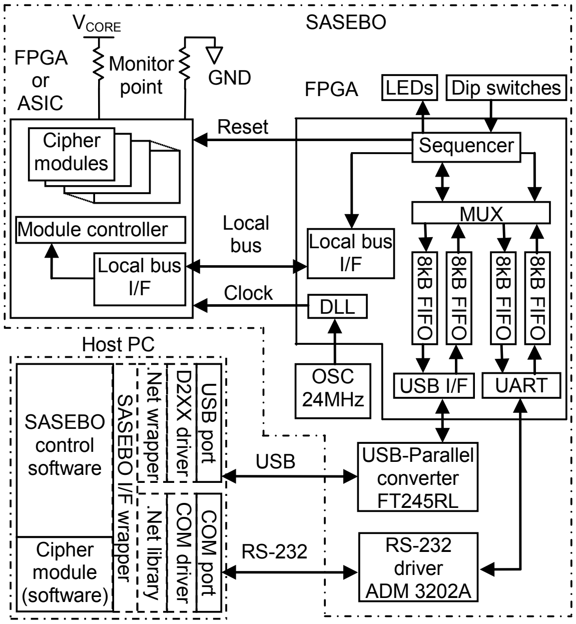
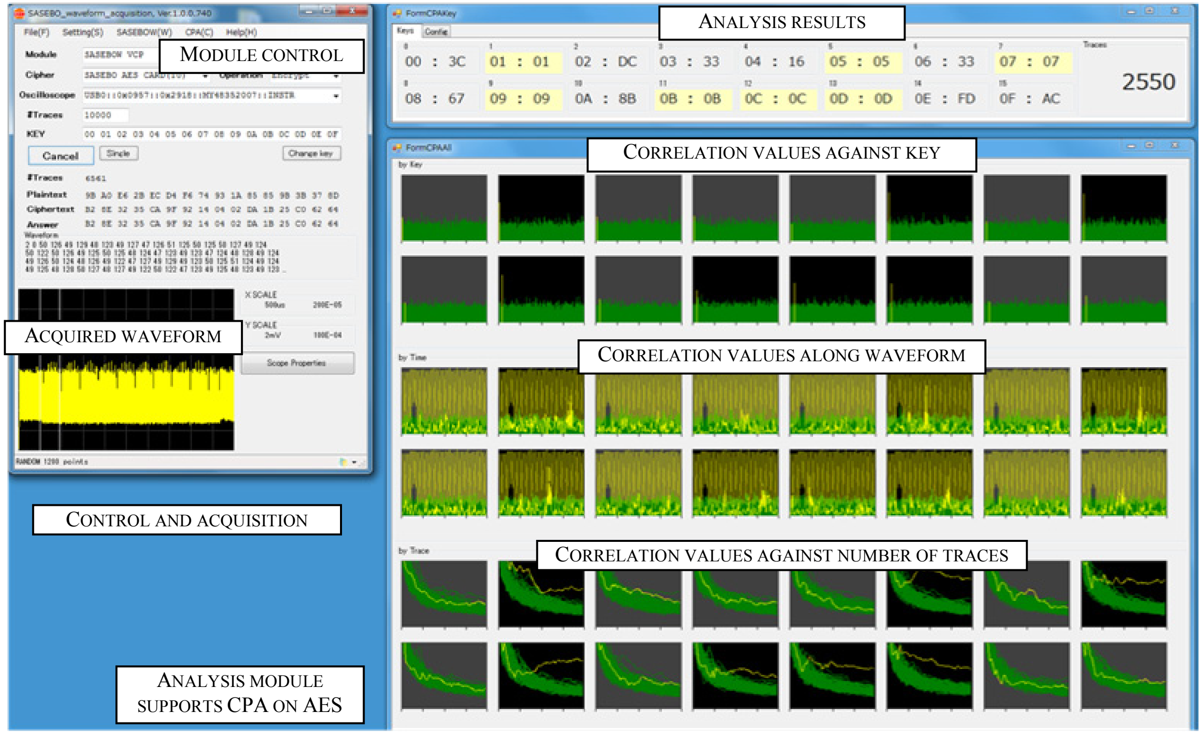


Figure 3: Block diagram of control HW/SW on SASEBO.

The boards are equipped with a USB interface and an RS-232 serial port for communication with a host computer. As illustrated in Fig. 3 the cryptographic modules, the controllers and the interface circuits were implemented in Verilog HDL, and the control software for operation check was developed in C#. The complete source code and all support documentation are available on our project website [3].

In order to implement the ability to measure the power consumption generated during cryptographic operations, shunt resistors are placed between the FPGAs and the V_{CORE}/GND lines of the boards. Decoupling capacitors are not mounted for the cryptographic FPGAs and the LSIs in order to allow for monitoring small fluctuations in the power consumption, whereas the power supply circuits of the control and cryptographic FPGAs are separated in order to suppress noise from the control circuits. The boards were distributed to over 100 government, industry and academic research laboratories as common experimental platforms. As a result, a number of studies have been reported in the area of side-channel attacks with SASEBO [6-9].

A tool for waveform acquisition and analysis for tracing power and electromagnetic waveforms and performing automatic analysis with CPA was also developed. The user interface is shown in Fig. 4. The software supports the AES cipher and all SASEBO variants, including SASEBO-W and our smartcard. The control and acquisition module is provided on our web site, and the analysis module is separated from the acquisition module to allow users to attach their own analysis modules. The analysis features are provided mainly for demonstration purposes.



Module SASEBOW VCP

Cipher SASEBO AES CARD(IO) Operation Encrypt

Oscilloscope USB0::0x0957::0x2918::MY48352007::INSTR

#Traces 10000

KEY 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

#Traces 6561

Plaintext 9B A0 E6 2B EC D4 F6 74 93 1A 85 65 9B 3B 37 8D

Ciphertext B2 8E 32 35 CA 9F 92 14 04 02 DA 1B 25 C0 42 64

Answer B2 8E 32 35 CA 9F 92 14 04 02 DA 1B 25 C0 42 64

Waveform

```
2 0 50 126 49 129 48 123 49 127 47 126 51 125 50 125 50 127 49 124
50 122 50 126 49 125 50 125 48 124 47 123 49 123 47 124 48 128 49 124
49 126 50 124 48 126 49 122 47 127 49 129 49 123 50 125 51 124 49 124
49 125 48 128 50 127 48 127 49 122 50 122 47 123 49 125 48 123 49 123 ..
```

X SCALE 500us 200E-05

Y SCALE 2mV 100E-04

RANDOM 1200 points

0	1	2	3	4	5	6	7	Traces
00 : 3C	01 : 01	02 : DC	03 : 33	04 : 16	05 : 05	06 : 33	07 : 07	2550
8	9	10	11	12	13	14	15	
08 : 67	09 : 09	0A : 8B	0B : 0B	0C : 0C	0D : 0D	0E : FD	0F : AC	

FIGURE 4: Side-channel attack evaluation software.

III. SASEBO-W

With increasing attention being paid to side-channel research and to the process of updating the standards, testing environment for consumer cryptographic devices is required. To support security evaluation of side-channel attacks, we developed a new board, SASEBO-W, for use in testing smartcards, which are the most widespread cryptographic modules. Figures 5 and 6 show the main components of SASEBO-W and a block diagram of its structure, respectively, and its basic features are summarized in Table 3. The board is equipped with an ID-1 format card socket, which provides support for ISO/IEC 7816-3 Class A, B and C contact cards [4]. The voltage of the power supply and the signals can be adjusted through a control FPGA in the range between 1.3 and 5.9 V in 256 steps. An alternative power supply is also available. Also, surface-mounted shunt resistors are soldered and SMA connectors are placed onto the V_{CC} and GND lines for measuring the power consumption. The top of the card connector is open to allow for EM measurements.

A Xilinx Spartan-6 LX150 FPGA is installed as a control device. It is connected to the smartcard signals and the digital volume of the voltage regulator. A USB interface (FTDI FT-2232H) supports RS-232 emulation, a bit bang mode and fast FIFO translation with a USB 2.0 high-speed interface. Power for operation of the board can be supplied through the USB connector. Various ways to access and control smartcards are available upon configuring the control device, and we also developed a UART direct access controller.

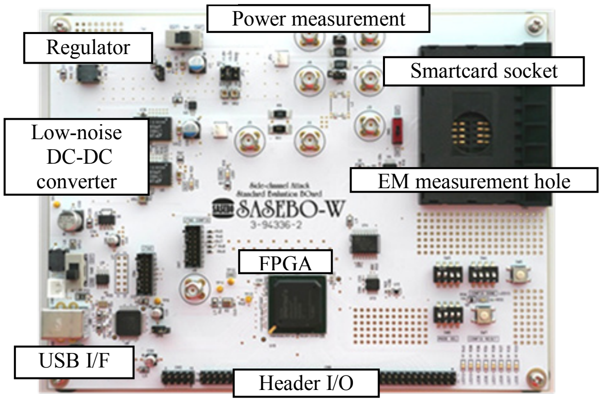


Figure 5: SASEBO-W platform.

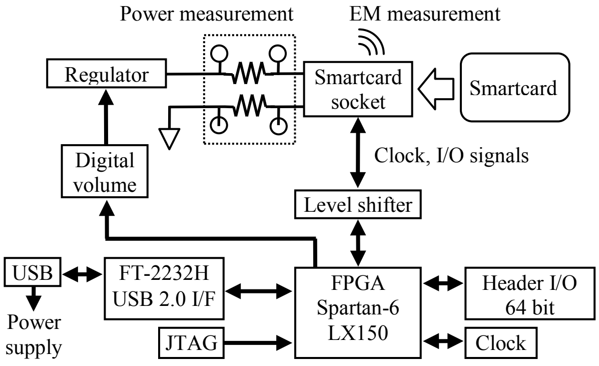


Figure 6: Block diagram of SASEBO-W.

Table 3: Basic features of SASEBO-W

Card support	ID-1 format card socket ISO/IEC 7816-3 contact card 1.3 to 5.9V supply voltage (up to 4.5V with USB power)
Control device	Xilinx Spartan-6 LX150 FPGA
Power supply	USB 5.0V DC power supply External power supply supported
Monitor points	Shunt resistors at Vcc and GND lines
Clock	Clock variable through a PLL and DCM on the control device External clock supported
I/F	USB External 64-bit pin
Size	200 x 150 x 1.6 mm3, FR-4, four layers

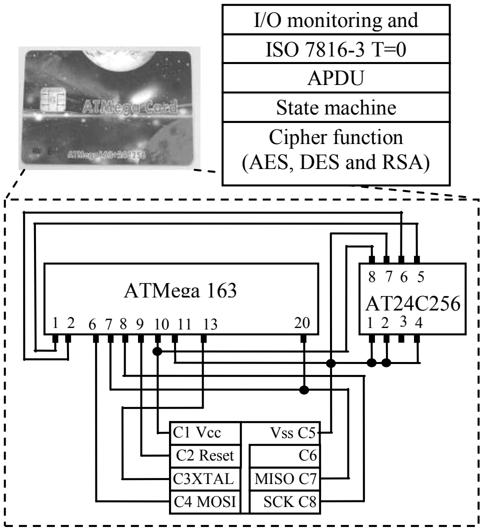


Figure 7: ATMega 163 card and smartcard OS.

The logic resources of the FPGA are 4-fold higher in comparison with Virtex-5 LX30 on SASEBO-GII. In spite of its simplicity, SASEBO-W provides high compatibility with SASEBO-GII, and the source code and control software designed for SASEBO-GII can be reused for SASEBO-W by emulating the control and cryptographic devices on the FPGA.

In addition to SASEBO-W, we developed a smartcard OS and cryptographic software on a processor card as a target of side-channel attacks for research purposes. Figure 7 shows the architecture of the card and the smartcard OS. The processor card features an Atmel ATMega 163 microcontroller with an 8-bit architecture and 1 KB of data and instruction memory. There are eight contact pads on the card, of which AUX1 and AUX2 are accessible in software for interacting with trigger signals, status indicators and so forth. The OS supports the ISO/IEC 7816-3 T=0 transmission protocol and control of the AES, DES and RSA cryptographic functions with APDU commands.

IV. Experimentation

In this section, the power consumption and electromagnetic radiation during AES processing on the smartcard were measured, and the waveforms were analyzed in order to demonstrate the suitability of SASEBO-W for use in experiments on side-channel attacks.

The smartcard operates at 3.57 MHz and supports the AES function, which is shown as pseudocode in Fig. 8. In the experiment, the power consumption and the EM radiation of the entire AES processing sequence on the card were captured by using an Agilent DSO6104A oscilloscope at a sampling rate of 10 MSa/s for a duration of 5 µs. Thus, a waveform of one AES processing sequence included 50,000 sampling points. In order to visualize the round functions of AES on the smartcard, 30 and 100 NOP operations were inserted into each round function and block, respectively. The signal of the power consumption was amplified with a Miteq 0.3-1000 MHz 28 dB AM-2A-000110 amplifier. The electromagnetic radiation was measured by using a single-loop probe with a diameter of 1.6 mm and amplified with a Miteq 0.3-600 MHz 60dB AU-1667 amplifier. The amplified signal was refined with a 3.79 MHz fifth-order Bessel low-pass filter. The measurement environment for the power consumption is shown in Fig. 9.

```
aes_128() {
  SET_PORT_HIGH; // Enable trigger
  add_round_key();
  for (i=0; i<9; i++) {
    sub_byte();
    shift_rows();
    mix_columns();
    key_expansion();
    add_round_key();
  }
  sub_byte();
  shift_rows();
  key_expansion();
  add_round_key();
  SET_PORT_LOW; // Disable trigger
}
```

Figure 8: Pseudocode of AES function.

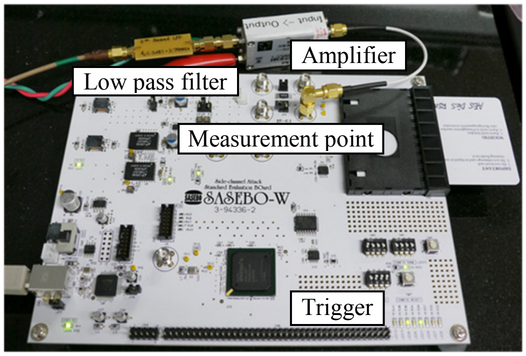


Figure 9: Measurement environment for power trace.

Figures 10 and 11 show the respective waveforms of the power consumption and the EM radiation, and a magnified view of a portion of the power consumption waveform is shown in Fig. 12. The round operations are clearly visible in the figures, and the two waveforms are similar in shape. However, it must be noted that the scale of the EM radiation waveform is ten times larger than that of the power consumption waveform, and the magnification ratio of the amplifier used for the EM trace is considerably larger than that for the power trace. By using the abovementioned amplifiers and filters, the waveforms were captured clearly and aligned precisely by using the AUX1 signal of the card as a trigger.

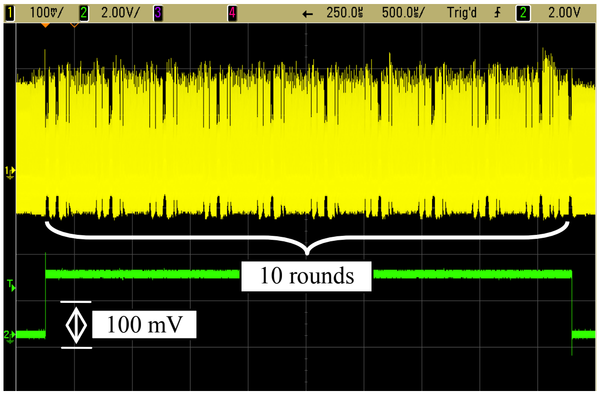


Figure 10: Waveform of power consumption trace.

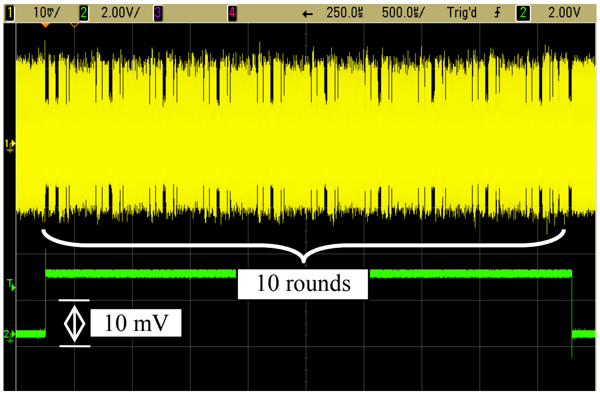


Figure 11: Waveform of EM radiation.

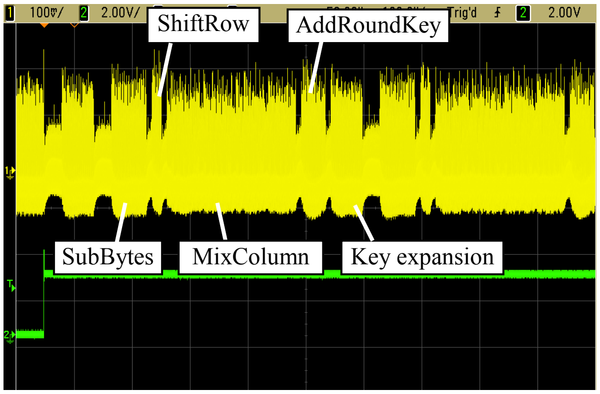


Figure 12: Magnified view of the power consumption waveform.

500 waveforms for the power consumption and the EM radiation were collected with two cryptographic keys, namely key-1 $\{2B\ 7E\ 15\ 16\ 28\ AE\ D2\ A6\ AB\ F7\ 15\ 88\ 09\ CF\ 4F\ 3C\}_{16}$ and key-2 $\{00\ 01\ 02\ 03\ 04\ 05\ 06\ 07\ 08\ 09\ 0A\ 0B\ 0C\ 0D\ 0E\ 0F\}_{16}$, and the collected waveforms were analyzed by using Correlation Power Analysis (CPA) [5]. The hypothetical power consumption H_{ij} of the CPA was set to the Hamming weight of the SubBytes output.

$$H_{i,j} = HW(S(pt_i \oplus k_j)) \qquad (1)$$

The correlation coefficients $corr_k(t)$ between H_k and $W_i(t)$ were calculated for all k and t according to Eq. 2, where $\overline{W(t)}$ and $\overline{H_k}$ are the average values of $W_i(t)$ and $H_{k,i}$, respectively. The 8-bit partial key k with the largest absolute value $corr_k(t)$ was estimated as the secret key. Figure 13 shows the number of partial keys that were estimated correctly by CPA from the power and EM waveforms. As a result, the secret key was extracted from only 150 power consumption waveforms. All sixteen partial keys were also estimated correctly with 500 EM radiation waveforms. There was no clear difference between the keys, in other words, the hypothetical model indicates a linear relation with the internal power consumption instead of the cipher keys.

This result also shows that SASEBO-W and the smartcard used in this demonstration are highly suitable for side-channel attack experiments.

$$\begin{aligned}
corr_k(t) &= \frac{cov(W(t), H_k)}{\sqrt{var(W(t))}\sqrt{var(H_k)}} \\
cov(W(t), H_k) &= \frac{1}{N}\sum_{i=1}^{N}(W_i(t) - \overline{W(t)})(H_{k,i} - \overline{H_k}) \\
var(W(t)) &= \frac{1}{N}\sum_{i=1}^{N}(W_i(t) - \overline{W(t)})^2 \\
var(H_k) &= \frac{1}{N}\sum_{i=1}^{N}(H_{k,i} - \overline{H_k})^2 \qquad (2)
\end{aligned}$$

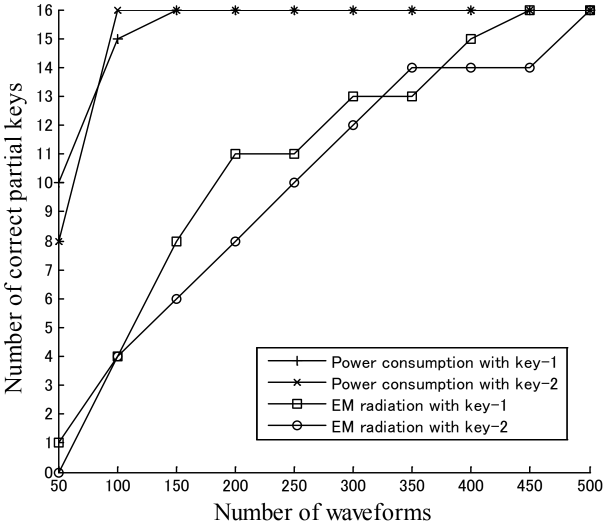


Figure 13: Number of correct partial keys versus number of power trace waveforms.

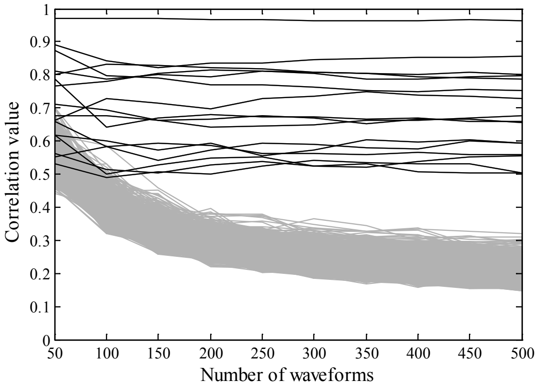


Figure 14: Correlation values of power waveforms with key-1.

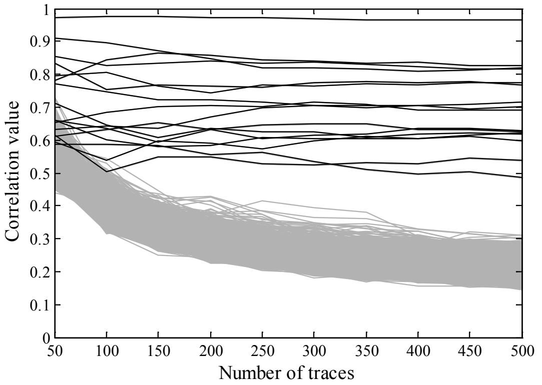


Figure 15: Correlation values of power waveforms with key-2.

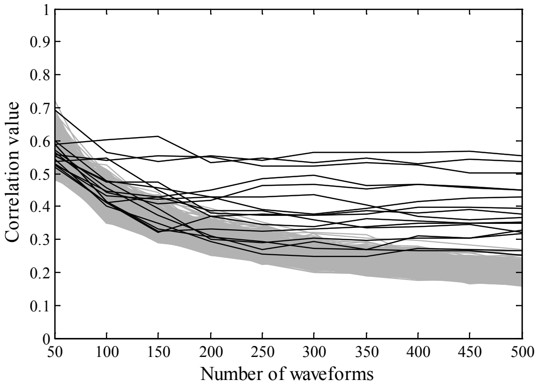


Figure 16: Correlation values of EM waveforms with key-1.

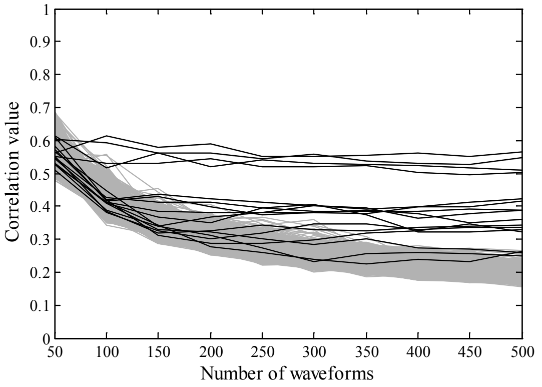


Figure 17: Correlation values of EM waveforms with key-2.

Figures 14 and 15 show the absolute correlation values between power trace waveforms and key-1 and key-2, respectively. The figures present 16 overlaid graphs corresponding to the partial keys. The values of the 16 correct keys are drawn with black lines, while the values of the wrong keys are given in gray. As clear from the graphs, the correlation values corresponding to correct keys are consistently higher. This result demonstrates the ease with which side-channel analysis of power consumption for smartcards can be implemented on SASEBO-W. Furthermore, the correlation values obtained in the EM radiation analysis are shown in Figures 16 and 17. The values of the correct keys decrease by around 0.3 points in comparison with those obtained from the power consumption waveforms, while the values of the wrong keys remain at about the same level. It is inferred from these results that the signal levels of the waveforms are similar in Figs. 9 and 10, however, the linear relationship between the EM radiation and power model is less applicable than that of the power consumption. There was also no obvious difference between the results obtained with the two keys.

Figure 18 shows the power consumption waveforms at the beginning of the AES function, where the correlation values from the power consumption and the EM radiation are plotted with the two keys at the corresponding period. The graph indicates the linear relationship between the power model and the measured waveforms for the SubBytes output and the MixColumn operation. The highest peak is observed in the MixColumn function, although according to the Hamming weight model it is expected to correspond to the output value of the SubBytes function since the S-box is implemented as a look-up table. Generally, the table is stored in an instruction ROM, and the load instruction shows high power consumption at the data bus. The difference in power consumption between instructions will be examined in future works. The correlation for the EM radiation is shown for the same period as that for the power consumption.

To match the periods of peaks with the instructions of the MixColumn function, the correlation values of 16 partial keys were plotted together with a waveform as shown in Figs. 20 and 21. The pseudocode for the MixColumn function is shown in Fig. 19. In this function, the 16-byte state is processed sequentially in 4-byte groups in the order of 0, 5, 10, 15, 4, 9, 14, 3, 8, 13, 2, 7, 12, 1, 6 and 11, and the correlation values are plotted in this order. The peaks of the 4-byte groups {0, 5, 10, 15}, {4, 9, 14, 3}, {8, 13, 2, 7} and {12, 1, 6, 11} show similar patterns and processing sequence, which confirms that the Hamming weight model of the S-box output corresponds to the MixColumn function.

V. Conclusion

SASEBO was developed as a standard platform for side-channel attack research, and we recently developed a new standard board, SASEBO-W, for conducting side-channel attack experiments on smartcards. An experimental smartcard OS was also developed for research purposes.

In this paper, the details of the SASEBO platform are presented, and side-channel attack experimentation with SASEBO-W and a smartcard is demonstrated. The waveforms of the power consumption and EM radiation traces were observed clearly, and a strong correlation between the model and the waveforms was obtained through side-channel analysis. The existence of a linear relationship between the model and the waveforms was also demonstrated, which affirms the suitability of SASEBO-W for side-channel attack experiments on contact smartcards.

In future works, we plan to perform similar analyses with other cryptographic algorithms, such as DES and RSA. We also plan to investigate the relationship between instructions and power consumption with SASEBO-W.

VI. ACKNOWLEDGEMENTS

The development of SASEBO was supported by METI (Ministry of Economy, Trade and Industry, Japan). SASEBO-W and the presented smartcard software were developed as part of a project of JST.

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

[2] ISO/IEC 18033-3:2005, “Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers,” 2005.

[3] “Side-channel Attack Standard Evaluation BOard (SASEBO),” AIST. http://staff.aist.go.jp/akashi.satoh/SASEBO/en/index.html

[4] Wolfgang Rankl and Wolfgang Effing, “Smart Card Handbook 3rd edition,” John Wiley & Sons, ISBN: 0-470-85668-8.

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

[6] Cryptography Research, Inc. “Protecting FPGAs from Power Analysis,” Cryptography Research Whitepaper, Vertion 1.0, April 20, 2010.

[7] Amir Moradi, Oliver Mischke, and Thomas Eisenbarth, “Correlation-Enhanced Power Analysis Collision Attack,” CHES2010, pp.125, 2010.

[8] L. Batina, J. Hogenboom, N. Mentens, J. Moelans and J. Vliegen, "Side-channel evaluation of FPGA implementations of binary Edwards curves", ICECS, special session Cryptographic Hardware & Embedded Systems, Dec. 12-15, 2010.

[9] Kazuyuki Kobayashi, Jun Ikegami, Shin'ichiro Matsuo, Kazuo Sakiyama and Kazuo Ohta, "Evaluation of Hardware Performance for the SHA-3 Candidates Using SASEBO-GII," Cryptology ePrint Archive, Report 2010/010, 2010.

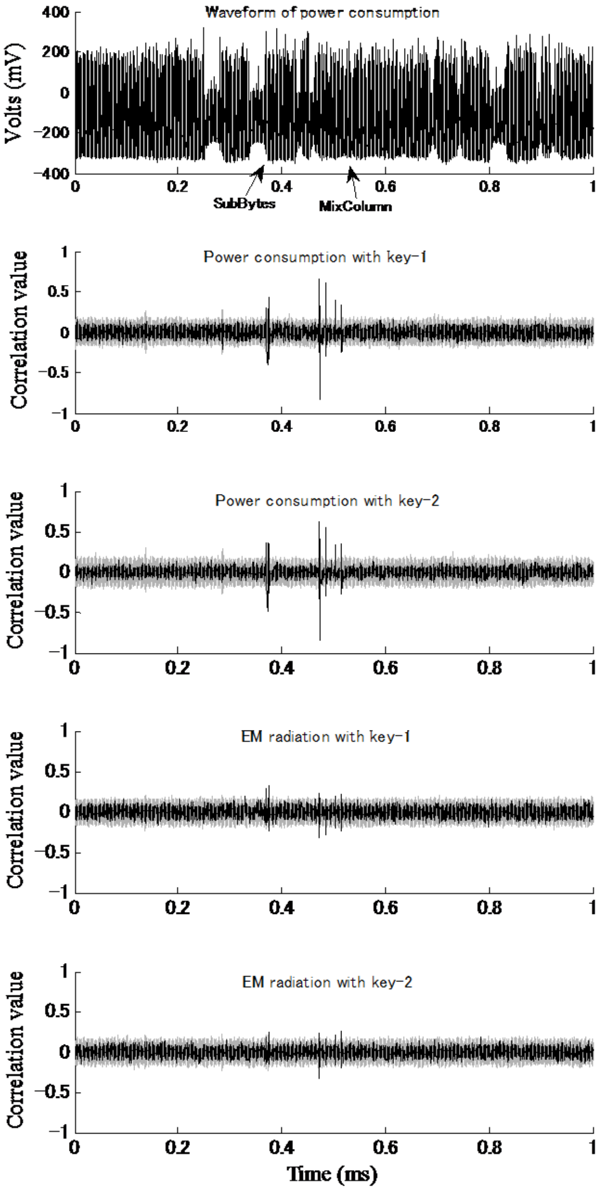


Figure 18: Correlation values against time.

```
mix_columns() {
  for (col = 0; col < 4; col++) {
    mix_column(col);
  }
}

mix_column(col){
  for (row = 0; row < 4; row++) {
    t[row] = st[row, col];
  }
  tt = t[0] ^ t[1] ^ t[2] ^ t[3];

  for (row = 0; row < 4; row++) {
    st[row, col] ^= mul2(t[0] ^ t[1]) ^ tt;
  }
}
```

Figure 19: Pseudocode of MixColumn function.

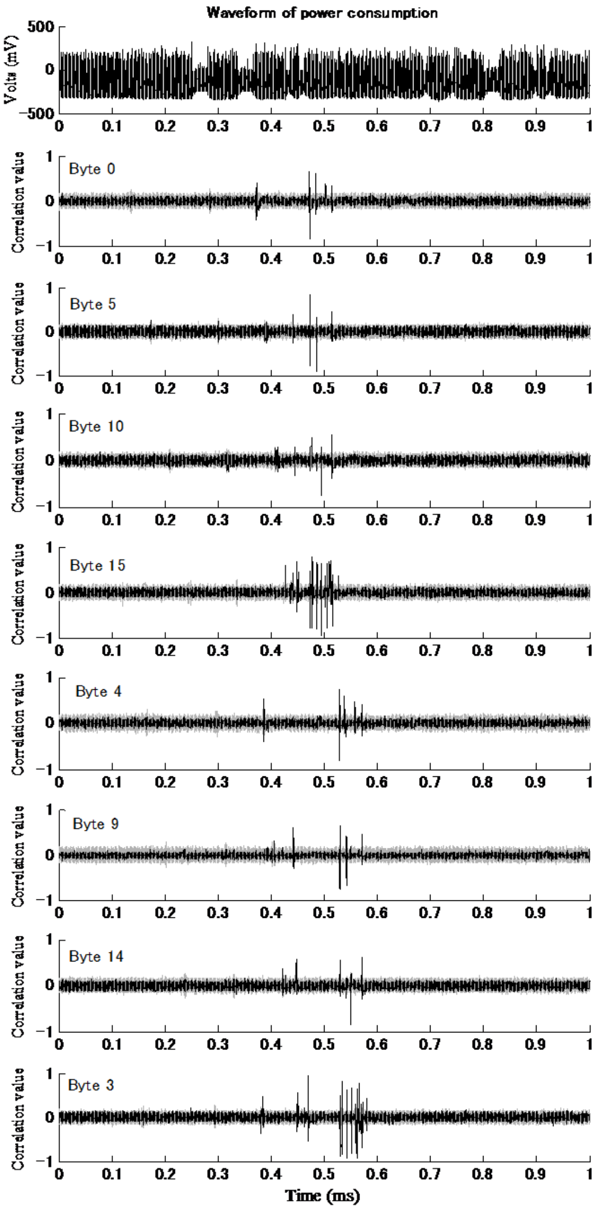


Figure 20: Correlation values plotted against time in matching the peaks to the MixColumn function.

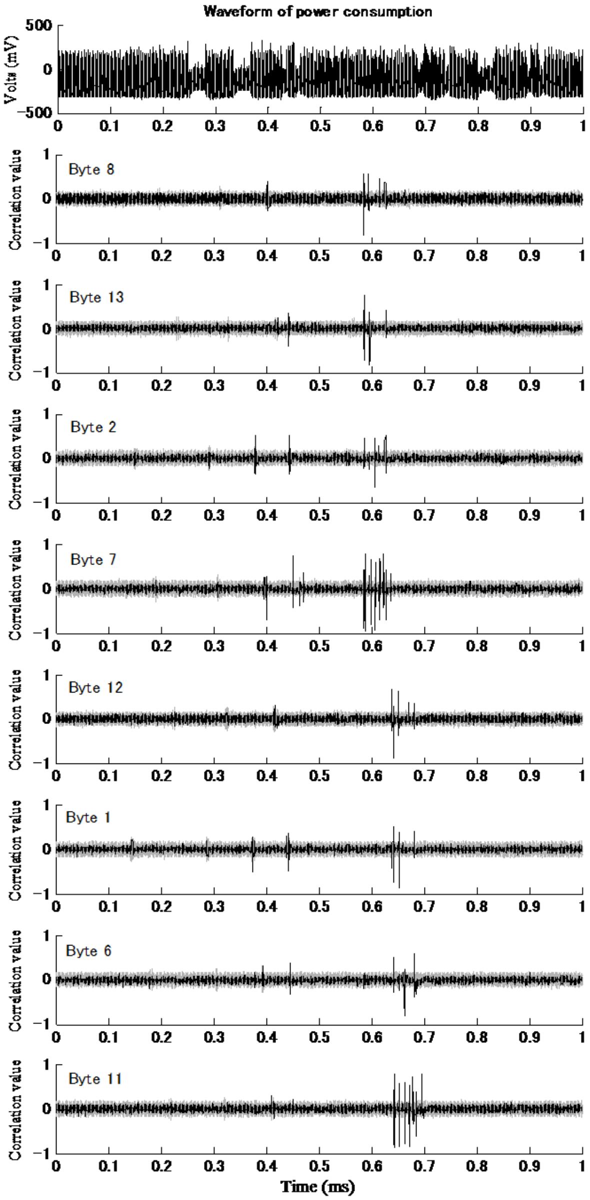


Figure 21: Correlation values plotted against time in matching the peaks to the MixColumn function.