Intermediate Report

SPACES

Security evaluation of Physically Attacked Cryptoprocessors in Embedded Systems

Programme 2009/2010

This report was compiled for the ANR-JST Joint workshop which was held in Kobe, Japan in March 2012. This report summarised SPACES group research activity of first half research period.
本報告書は、2012 年 3 月に神戸で開催された領域内中間ワークショップのために編纂されました。研究グループの研究期間前半の活動内容をまとめたものです。

.

A IDENTIFICATION

Project acronym	SPACES
Project title	Security evaluation of physically attacked cryptoprocessors in embedded systems
Project coordinator (French side) (company/organization)	Jean-Luc Danger (Telecom ParisTech)
Project coordinator (Japanese side) (company/organization)	Naofumi Homma (Tohoku University)
Project start date Project end date	1 December 2010 30 November 2013
Competitiveness cluster labels and contacts (French side) (cluster, name and e-mail of contact)	
Project website if applicable	https://spaces.enst.fr/

Author of this report	
Title, first name, surname	Assoc. Prof. Naofumi Homma Prof. Jean-Luc Danger
Telephone	
E-mail	
Date of writing	10 February 2012
Period covered by activity report	From 1 December 2010 To 31 February 2012

B DELIVERABLES AND MILESTONES

No.	Designation	Nature*	Date of supply			Partners (underline the responsible partner)
			Initially planned	Re-scheduled	Delivered	
M1	Specifications of simulation engine and two-level power/EM models	Document (specification)	T0+6		T0+7	TP/LIP6/Morpho/ Tohoku/AIST/ Kobe
M2	Power/EM measurement Platform	System	T0+12		T0+12	TP/LIP6/Morpho/ Tohoku/AIST/ /UEC/Kobe
M3	Simulator kernel and Simulation models ver. 1	Document + code	T0+18			TP/LIP6/Morpho/ Tohoku/AIST/ Kobe
M4	Visualization of EM information leakage	Document	T0+30			TP/ Tohoku/UEC
M5	Simulator kernel and Simulation models ver. 12	Document (specification) + code	T0+36			TP/LIP6/Morpho/ Tohoku/AIST/ Kobe
D1	Web site of the project	Website	T0+3		T0+3	TP/Tohoku
D2	Cooperation agreement	Document	T0+12	T0	T0	TP/LIP6/Morpho/ Tohoku/AIST/ /UEC/Kobe
D3	Project reports	Document	T0+12,+24,+36	T0+15, +36		TP/LIP6/Morpho/ Tohoku/AIST/ /UEC/Kobe
D4	All the specifications, gathered in a unique document (then updated whenever necessary)	Document	T0+6		T0+7	TP/LIP6/Morpho/ Tohoku/AIST/ /UEC/Kobe

No.	Designation	Nature*	Date of supply			Partners (underline the responsible partner)
			Initially planned	Re-schedu led	Deliv-ered	
D5	D5.1 Simulation engine ver. 1 D5.2 Simulation engine ver. 2	Document + code	T0+18, T0+36,	T0+8	T0+8	LIP6/Morpho/ Kobe
D6	High-level symbolic models	Document + code	T0+36			TP/Morpho
D7	Low-level physical models	Document + code	T0+36			AIST/Kobe
D8	Reports on model validations	Document	T0+36			TP/Morpho/ AIST/Kobe
D9	D9.1: Power/EM measurement Platform D9.2: Analysis tools D9.3: Sets of power/EM traces and there analysis results	System + code + data	T0+12 T0+24 T0+36		T0+12	TP/ Tohoku/UEC/ AIST/Kobe
D10	D10.1: Reports on EM radiations at nearest field D10.2: Reports on EM radiations at far field	Document	T0+36 T0+36			TP/Tohoku

C PROGRESS REPORT

C.1 INITIAL OBJECTIVES OF THE PROJECT

This project aims to perform a comprehensive study of security evaluation methodologies on cryptographic modules against physical attacks such as side-channel attacks and fault-injection attacks. The main objective of this project to develop a novel evaluation platform based on both simulation and in-situ evaluations.

The first objective is to propose a novel simulation technology for evaluating the robustness of a cryptographic module (i.e., software or hardware) against side-channel attacks. A specific simulation engine is studied in order to collect the leakage of the sensitive information. The associated simulation models are also developed at two levels of abstraction: (i) high-level model where the circuit is like a black box, and (ii) low-level model based on post-layout circuit data. An effective extraction of physical parameters is proposed as a key technology to simulate a cryptographic module in the low-level model. This study would allow circuit designers to obtain accurate information of the robustness without fabricating the chips.

The other objective is to develop a prototype evaluation system based on a new SASEBO (Side-channel Attack Standard Evaluation Board) and custom ASICs plugged via daughter boards. The target devices that can be handled in this project are FPGA, ASIC and IC card implementations. A novel analysis technique is also studied in order to enhance the accuracy and robustness of the security evaluation. Moreover the mechanisms of electromagnetic (EM) information leakage and fault injection from/to cryptographic modules are understood by using a developed EM probing system. Effective countermeasures could be devised from both the better knowledge of the EM behaviour and the simulation and prototype evaluation.

C.2 WORK PERFORMED AND RESULTS ACHIEVED IN THE FIRST HALF PERIOD

The project consists of two work packages for security simulator (WP1) and evaluation system (WP2). The work and results of the three subtasks in each work package are described below.

WP1: Security simulation technology

T1.1 Simulator engine

Several modules have been defined and developed for constructing the simulation engine: (i) three parsers for the input netlists for SPICE, VHDL and Verilog, (ii) the file format called MVCD for the simulation patterns and the module related to read and produce the file, (iii) the scheduler, (iv) the functional abstractor that transforms a transistor netlist into a gate netlist for the low-level simulators, (v) the definition of the interconnection description simplified and merged with the gate's output for the low-level simulators, (vi) the netlist transformation module, and (vii) the first prototype of the engine including a simple timing evaluation model .

T1.2 High-level model

The high level modelling has been studied from both a top-down and a bottom-up approach. The top-level approach takes advantage of the stochastic model which allows to characterize a cryptographic implementation without detailed knowledge about the architecture of the device. The bottom up approach means that the characterization of the leakage starts at the gate level and go up to the higher level through the hierarchical layers. The specification of both approaches has been done jointly in order to go towards a convergence at the end of the project.

T1.3 Low-level model (+Test LSI vehicle)

Correlation power analysis is efficiently accomplished on cryptographic modules by simulation, with power waveforms simulated with original capacitor charging models. More than 50k waveforms derived by simulation were successfully correlated with a secret key. This proves that the proposed modelling technique well captures the low-level processes of information leakage through power noises. A test LSI vehicle embedding cryptographic modules was developed in a 65 nm CMOS technology, under Japan-France collaboration, to target in-depth understanding of physical processes of information leakage and better accuracy of modelling.

WP2: Evaluation system

T2.1 Side-channel evaluation platform

A side-channel measurement platform has been constructed by developing a new evaluation board named SASEBO-W. The related software and hardware (i.e., smartcard OS, control circuits and acquisition software) have also been developed. The SASEBO-W is designed for measuring cryptographic modules on an FPGA and smartcards. The board can also be extended to use design and operation test for custom ASICs.

T2.2 Analysis technique

Mutual information analysis (MIA) has been largely studied and compared. A new MIA approach based on high-order statistics has been proposed. It was also discovered that the behavior of cryptographic devices under an illegal operation was the key to revealing the nature of side-channel information including EM radiation. As a result, Fault Sensitivity Analysis (FSA) has been proposed as a universal and efficient side-channel distinguisher. Several methods have been implemented and tested to improve the side-channel attack efficiency: re-synchronization by moments, multi-resolution time-frequency analysis and wavelet transforms.

T2.3 Physical understanding

Radiation mechanisms behind EM attacks on cryptographic modules have been studied from the view point of Electromagnetic Compatibility (EMC). First, the EM scanning system has been constructed for the systematic and close measurement. Simple and differential EM attacks were then conducted on the developed evaluation platform and the EM radiation including significant information was investigated at a distance from cryptographic modules. In addition, the possibility of EM fault injection attack has been demonstrated by a series of experiments.

C.3 WORK FORECAST IN THE SECOND HALF PERIOD

The project is being smoothly conducted with close cooperation and the project milestones have been delivered as planned. In the second half period, the security simulation technology consisting of the simulation engine and the two models will be released in WP1 and the evaluation system and its related technologies (physical understanding, measurement tools, and analysis technique) will be developed. The detailed forecasts are as follows.

WP1: Security simulation technology

T1.1 Simulator engine

The simulation engine will evolve following two axes.

- After an evaluation period of the first prototype in terms of simulation speed, accuracy and features, a second prototype will be developed to fulfil the project's aims.
- The evaluation models (current and EM) will be integrated to the evaluation engine.

T1.2 High-level model

The main objective of this modelling task is to refine both approaches, i.e. top-level and bottom-up approaches, to converge toward a high level model. In particular, the top level modelling approach will investigate refinements of the stochastic approach, whereas the bottom-up approach will estimate leakage tables when going up to the upper level.

T1.3 Low-level model (+Test LSI vehicle)

The low-level modelling of digital cryptographic modules for more accurate simulation of power analysis attacks will be actualized with the integration of capacitor charging models by Kobe and precision gate switching and glitch timing extractors by LIP6. The test LSI vehicle developed through Japan-France collaboration will be examined in a variety of aspects of EM, SCA, and modelling. An integrated environment of the test LSI vehicle with SASEBO-W will also provide a reference platform of SCA analysis for custom cryptographic modules.

WP2: Evaluation system

T2.1 Side-channel evaluation platform

The side-channel platform (SASEBO-W shown in Fig. 1) and acquisition software developed in the first half are improved by adding side-channel analysis features and supporting a new test vehicle. The software refactoring will also be conducted to improve its scalability and maintenance performance.

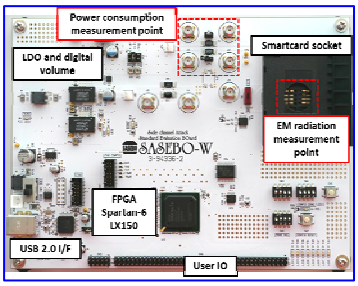

Fig. 1: SASEBO-W

T2.2 Analysis technique

Enhancement of FSA will be researched. Case studies on AES, ECC, and RSA hardware modules will be used for measuring the efficiency of FSA and its variance. When intermediate values collided in consecutive clock cycles, it is found that SCA information has a distinctive feature. FSA will also be studied in conjunction with MIA. The MIA will also be studied on protected implementations. The digital signal processing like signal resynchronisation and noise filtering will be carried out on real smartcard.

T2.3 Physical understanding

Radiation mechanisms behind EM attacks at a distance from cryptographic modules are studied continuously using the newly developed evaluation system and the test LSI vehicle. In the near measurement, the EM radiation including significant information is clarified as a distribution map. In the far measurement, the EM information leakage from attached cables is estimated in both theoretical and experimental manners under practical conditions. Based on the above understanding, leakage suppression techniques are investigated as countermeasures at the board-level.

C.4 DIFFICULTIES ENCOUNTERED AND SOLUTIONS

A huge earthquake happened in Japan at 11 March 2011, and it damaged Tohoku University heavily. As a result, an exchange-student plan to Tohoku was cancelled.

C.5 SIGNIFICANT EVENTS AND RESULTS

(a) New evaluation board (SASEBO-W):

A new evaluation board called SASEBO-W was successfully developed.

(b) Outreach activity at CHES 2011 exhibition booth:

Some demonstrations using SASEBO-W were performed at the SPACES project booth in a major conference on a cryptographic embedded system named CHES.

(c) Multinational joint papers and book chapter :

Multinational joint papers and book chapter were accepted and published at the following major conferences.

- L. Sauvage,S. Guilley, J-L Danger, N. Homma, Y. Hayashi, "Practical Results of EM Cartography on a FPGA-based RSA Hardware Implementation" EMC2011", Long Beach, August 2011
- O. Meynard, Y. Hayashi, N. Homma, S. Guilley, J-L Danger, "Identification of information leakage spots on a cryptographic device with an RSA processor", EMC2011, Long Beach, August 2011
- O. Meynard, D. Real, S. Guilley, J-L. Danger, and N. Homma, "Enhancement of Simple Electro-Magnetic Attacks by Pre-characterization in Frequency Domain and Demodulation Techniques," DATE2011, pp. 1004--1009, March, 2011.

One Book Chapter has been accepted for publication.

- O. Meynard, , S. Guilley, J-L Danger, Y. Hayashi, N. Homma, "Characterization of the Information Leakage of Cryptographic Devices by using EM Analysis", Intech publisher (to be published)

C.6 WORK SPECIFIC TO THE COMPANIES (WHERE APPLICABLE)

Company: Morpho

Company	Morpho
Author (name + e-mail address)	Thanh Ha LE, thanh-ha.le@morpho.com

In the framework of SPACES project, Morpho has been working on the following topics:

- **High-level simulator**: In the first time, a simulator based on simple power consumption model (Hamming weight, Hamming distance models) has been implemented and tested using acquisitions from SASEBO-GII board. In order to refine the power consumption model, the approach using the stochastic model has been chosen. It allows us to characterize a cryptographic implementation without detailed knowledge about the architecture of the device. As a smart-card provider, this approach corresponds to our context (no or very little information about the circuit) and our needs (evaluation of software countermeasures).
- **Signal processing techniques**: different studies on signal processing have been performed: synchronisation, wavelet, noise filtering. The obtained results help us to improve our analysis tools and competence.
- **Attacks and countermeasures**: we have been working on advanced side-channel analysis (for example Mutual Information Analysis) and countermeasures. Some results have been published and another is actually on submission. Some analysis methods are used now in our laboratory to evaluate our products.

During this period, we have worked with LIP6 and Telecom ParisTech on various topics (simulator, signal processing and attacks). We have also initialized a discussion with UEC about the combination of Mutual Information Analysis and Fault Analysis.

For the future works, beside the collaboration with French partners, we would like to reinforce

the common works with Japanese partners: fault analysis with UEC, signal processing with Tohoku, acquisitions & analysis on SASEBO board with AIST and multi-level simulator with University of Kobe.

C.7 CONSORTIUM MEETINGS (COLLABORATIVE PROJECTS)

Date	Place	Partners present	Subject of the meeting
18 May 2010	Tohoku (Tokyo office)	Tohoku/AIST/UEC/Kobe	Japanese partners kick-off meeting
24 Sep 2010	Télécom ParisTech	All	Kick-off plenary meeting
07 Dec 2010	Conf call	TPT/Tohoku	Coordinator meeting for consortium agreement
29 Dec 2010	Conf call	Tohoku/AIST/UEC/Kobe	Japanese partners meeting for progress report
22 Feb 2011	Télécom ParisTech	TPT/Tohoku	Coordinator meeting for progress report
01 Mar 2011	Télécom ParisTech	TPT/LIP6/Morpho	French partners meeting for progress report
07 Mar 2011	Tohoku	Tohoku/UEC/Kobe	Japanese partners meeting for progress report
17 May 2011	Tohoku (Tokyo office)	Tohoku/AIST/UEC/Kobe	Japanese partners meeting for progress report
26 May 2011	Télécom ParisTech	TPT/LIP6/Morpho/ Tohoku	Tohoku/ French partners meeting for progress report
07 June 2011	Télécom ParisTech	TPT/LIP6/Morpho	French partners meeting for progress report
06 July 2011	Conf call	TPT/LIP6 Tohoku/Kobe	Meeting for test LSI vehicle
28 July 2011	Tohoku (Tokyo office)	Tohoku/AIST/UEC/Kobe	Japanese partners meeting for progress report
29-30 Aug 2011	LIP6	TPT/LIP6 Kobe	Meeting for progress report on WP1
06 Sep 2011	Télécom ParisTech	TPT/LIP6/Morpho	French partners meeting for progress report
03 Oct 2011	Kobe	All	Plenary meeting
12 Dec 2011	Télécom ParisTech	TPT/LIP6/Morpho	French partners meeting for progress report
12 Dec 2011	Kobe	Tohoku/UEC/Kobe	Japanese partners meeting for progress report
21-22 Dec 2011	Télécom ParisTech	TPT/LIP6/Morpho Tohoku/UEC/Kobe	Plenary meeting + Test LSI vehicle meeting
05 Jan 2012	Conf call	TPT/Tohoku/Kobe	Meeting for test LSI vehicle

C.8 FREE COMMENTS

Comments from the French/Japanese coordinators (PIs)

A strong collaboration has been created between Japanese and French partners. Regular meetings, either plenary or work package meetings allowed all the partners to work in perfect consistency. The first part of the project has already produced many common results, as joint publications, use of the SASEBO boards, common exhibition Booth at CHES workshop. This is the evidence of the motivation and interaction the partners share within the SPACES project.

D PROJECT VALORIZATION AND IMPACT SINCE BEGINNING

D.1 PUBLICATIONS AND COMMUNICATIONS

<Joint> Multinational Joint Papers, etc

List of the Multinational publications (resulting from jointly conducted work)		
International	Peer-reviewed journals	1. 2.
	Books or chapters in books	1. Meynard, S. Guilley, J-L Danger, Y. Hayashi, N. Homma, "Characterization of the Information Leakage of Cryptographic Devices by using EM Analysis," Intech publisher (to be published)
	Communications (conferences)	1. L. Sauvage, S. Guilley, J-L Danger, N. Homma, Y. Hayashi, "Practical Results of EM Cartography on a FPGA-based RSA Hardware Implementation," EMC2011, pp. 768-772, Liong Beach, August 2011 2. O. Meynard, Y. Hayashi, N. Homma, S. Guilley, J-L Danger, "Identification of information leakage spots on a cryptographic device with an RSA processor," EMC2011, pp. 773-778, Long Beach, August 2011 3. O. Meynard, D. Real, S. Guilley, J-L. Danger, and N. Homma, "Enhancement of Simple Electro-Magnetic Attacks by Pre-characterization in Frequency Domain and Demodulation Techniques," DATE2011, pp. 1004-1009, March, 2011.
France	Peer-reviewed journals	1.
	Books or chapters in books	1.
	Communications (conferences)	1.
Japanese	Peer-reviewed journals	
	Books or chapters in books	
	Communications (conferences)	
Outreach initiatives	Popularization articles	1.
	Popularization conferences	1.
	Others	1. Demonstration at CHES 2011 exhibition booth, Sep., 2011.

<French side> Single partner Papers, etc

List of single-partner publications (involving a single partner)		
International	Peer-reviewed journals	1. 2.
	Books or chapters in books	1. 2.
	Communications (conferences)	1. N. Debande, Y. Souissi, S. Guilley, J-L. Danger, M. Nassar, Thanh-Ha Le, "Re-synchronization by Moments*: an efficient solution to align Side-Channel traces," WIFS2011, Foz de Iguacu, Brazil, Dec., 2011. 2. N. Debande, Y. Souissi, A.E. Aabid, S. Guilley, J-L.Danger, "A Multiresolution Time-Frequency Analysis Based Side Channel Attacks", Poster Session of WIFS2011, Dec., 2011. 3. H. Chabanne, G. Cohen, J-Pierre Flori, A. Patey, "Non-Malleable Codes from the Wire-Tap Channel," ITW2011, Oct., 2011. 4. Y Souissi, M.A. Elaabid, N. Debande, S.Guilley, J-L. Danger; "Novel Applications of Wavelet Transforms based Side-Channel Analysis," NIAT2011, Sep., 2011. 5. N.Debande, T-H. Le, M. Berthier; "An overview of Mutual Information Analysis," Poster Session of CHES 2011, Sep., 2011. 6. S. Guilley, O. Meynard, M. Nassar, G.Duc, P. Hoogvorst, M.A. Elaabid, S. Bhasin, Y. Souissi, N. Debande, L. Sauvage, J-L. Danger, "Vade Mecum on Side Channel Attacks and Countermeasures for the Designer and Evaluator," DTIS2011, April 2011. 7. S. Wang, T-H. Le, M. Berthier, "When CPA and MIA go hand in hand," COSADE 2011, Feb., 2011. 8. J. Bringer, H. Chabanne, T-H Le, "Protecting AES Against Side-Channel Analysis Using Wire-Tap Codes," (Under submission) 9. Y. Souissi, S. Mekki, N. Debande, S.Guilley, J-L. Danger, "On the

		optimality of Correlation Power Analysis," WISTP'12 (Under submission) 10. H. Chabanne, G. Cohen, A. Patey, "Secure Network Coding and Non-Malleable Codes: Protection against Linear Tampering," (Under submission) 11. L. Sauvage, S. Guilley, J-L Danger, Y. Hayashi, N. Homma, "A Fault Model for Conducted Intentional ElectroMagnetic Interferences," EMC 2012 (Under submission)
France	**Peer-reviewed journals**	1. 2.
	Books or chapters in books	1. 2.
	Communications (conferences)	1. 2.
Outreach initiatives	**Popularization articles**	1. 2.
	Popularization conferences	1. 2.
	Others	1. 2.

<Japanese side> Single partner Papers, etc

List of single-partner publications (involving a single partner)		
International	**Peer-reviewed journals**	1. Miroslav Knežević, Kazuyuki Kobayashi, Jun Ikegami, Shin'ichiro Matsuo, Akashi Satoh, Ünal Kocabaş, Junfeng Fan, Toshihiro Katashita, Takeshi Sugawara, Kazuo Sakiyama, Ingrid Verbauwhede, Kazuo Ohta, Naofumi Homma, and Takafumi Aoki, "Fair and Consistent Hardware Evaluation of Fourteen Round Two SHA-3 Candidates," IEEE Trans. VLSI Syst., 13 pages, (to be published). 2. Yang Li, Kazuo Ohta, and Kazuo Sakiyama, "New Fault-Based Side-Channel Attack using Fault Sensitivity," IEEE Trans. Inf. Forensic Secur., Vol.7, No.1, pp.88-97, Feb., 2012. 3. Naofumi Homma, Kazuya Saito, and Takafumi Aoki, "A Formal Approach to Designing Cryptographic Processors Based on GF(2^m) Arithmetic Circuits," IEEE Trans. Inf. Forensic Secur., Vol. 7, No. 1, pp. 3-13, Feb., 2012. 4. Sho Endo, Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, Akashi Satoh, "A configurable on-chip glitchy-clock generator for fault injection experiments," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol. E95-A, No. 1, pp. 263-266, Jan., 2012. 5. Yang Li, Kazuo Ohta, and Kazuo Sakiyama, "Toward Effective Countermeasures against An Improved Fault Sensitivity Analysis," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.A95-A, No.1, pp.234-241, Jan., 2012. 6. Sho Endo, Naofumi Homma, Takeshi Sugawara, Takafumi Aoki and Akashi, "An On-chip Glitchy-clock Generator for Testing Fault Injection Attacks," Journal of Cryptographic Engineering, Vol. 1, No. 4, pp. 265-270, Dec., 2011. 7. Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, and Akashi Satoh, "High-performance Architecture for Concurrent Error Detection for AES Processors," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol. E94-A, No.10, pp. 1971-1980, Oct., 2011. 8. Atsushi Miyamoto, Naofumi Homma, Takafumi Aoki, and Akashi Satoh, "Systematic design of RSA processors based on high-radix Montgomery multipliers," IEEE Trans. VLSI Syst., Vol. 19, No. 7, pp. 1136-1146, July 2011.
	Books or chapters in books	
	Communications (conferences)	1. Yu-ichi Hayashi, Shigeto Gomisawa, Yang Li, Naofumi Homma, Kazuo Sakiyama, Takafumi Aoki, and Kazuo Ohta, "Intentional Electromagnetic Interference for Fault Analysis on AES Block Cipher IC," EMCCOMPO2011, pp.235-240, Nov., 2011. 2. Amir Moradi, Oliver Mischke, Christof Paar, Yang Li, Kazuo Ohta, Kazuo Sakiyama, "On the Power of Fault Sensitivity Analysis and Collision Side-Channel Attack in a Combined Setting," CHES2011, LNCS 6917, Springer-Verlag, pp.292-311, Sep., 2011. 3. Hikaru Sakamoto, Yang Li, Kazuo Ohta, and Kazuo Sakiyama, "Fault Sensitivity Analysis against Elliptic Curve Cryptosystems,"

		FDTC2011, pp.11-20, Sep., 2011. 4. Toshihiro Katashita, Yohei Hori, Hirofumi Sakane, Akashi Satoh, "Side-Channel Attack Standard Evaluation Board SASEBO-W for Smartcard Testing," NIAT2011, NIST, Sep., 2011. 5. Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, and Hideaki Sone, "Non-invasive Trigger-free Fault Injection Method Based on Intentional Electromagnetic Interference," NIAT2011,NIST, pp. 15-19, Sep., 2011. 6. Taishi Ikematsu, Yu-ichi Hayashi, Takaaki Mizuki, Naofumi Homma, Takafumi Aoki, and Hideaki Sone, "Suppression of Information Leakage from Electronic Devices Based on SNR," EMC2011, pp. 920-924, Aug., 2011. 7. Yu-ichi Hayashi, Naofumi Homma, Takeshi Sugawara, Takaaki Mizuki, Takafumi Aoki, and Hideaki Sone, "Non-Invasive EMI-Based Fault Injection Attack against Cryptographic Modules," EMC2011, pp. 763-767, Aug., 2011. 8. Li Yang, Kazuo Ohta, and Kazuo Sakiyama, "Revisit Fault Sensitivity Analysis on WDDL-AES," HOST2011, pp.148-153, Jun., 2011. 9. Daisuke Fujimoto, Makoto Nagata, Toshihiro Katashita, Akihiko Sasaki, Yohei Hori, Akashi Satoh, "A Fast Power Current Analysis Methodology Using Capacitor Charging Model for Side Channel Attack Evaluation," HOST 2011, pp. 87-92, Jun., 2011 10. Toshihiro Katashita, "SASEBO for smartcards," 1st Korea-Japan R&D Collaboration Day in South Korea, May 2011. 11. Sho Endo, Naofumi Homma, Takeshi Sugawara, Takafumi Aoki, and Akashi Satoh, "An On-Chip Glitchy-Clock Generator and its Application to Safe-Error Attack," COSADE 2011, pp. 175–182, Feb., 2011. 12. Yang Li, Kazuo Sakiyama, Shigeto Gomisawa, Toshinori Fukunaga, Junko Takahashi, and Kazuo Ohta, "Fault Sensitive Analysis," CHES2010, LNCS 6225, Springer-Verlag, pp. 320-334, Aug., 2010. 13. Daisuke Nakatsu, Li Yang, Kazuo Sakiyama, and Kazuo Ohta, "Combination of SW Countermeasure and CPU Modification on FPGA against Power Analysis," WISA2010, LNCS 6513, Springer-Verlag, pp.258-272, Aug., 2010. 14. Masahiro Yamaguchi, Hideki Toriduka, Shoichi Kobayashi, Takeshi Sugawara, Naofumi Homma, Akashi Satoh, and Takafumi Aoki, "Development of an on-chip micro shielded-loop probe to evaluate performance of magnetic film to protect a cryptographic LSI from electromagnetic analysis," EMC2010, pp. 103-108, Jul., 2010. 15. Yu-ichi Hayashi, Takeshi Sugawara, Yoshiki Kayano, Naofumi Homma, Takaaki Mizuki, Akashi Satoh, Takafumi Aoki, Shigeki Minegishi, Hideaki Sone, Hiroshi Inoue, "Information Leakage from Cryptographic Hardware via Common-Mode Current," EMC2010, pp. 109-114, Jul., 2010. 16. Akashi Satoh, Toshihiro Katashita, Takeshi Sugawara, Takafumi Aoki and Naofumi Homma, "Hardware Implementations of Hash Function Luffa," HOST2010, Jun., 2010.
Japanese	**Peer-reviewed journals**	1. Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, "Recent Research Trends in Side Channel Attack on Cryptographic Modules and its Countermeasure ," IEEJ Trans. Fundam. Material., Vol. 132, No. 1, pp. 9-12, Jan., 2012. 2. Toshihiro Katashita, Akashi Satoh, Takeshi Sugawara, Naofumi Homma, and Takafumi Aoki, "Hardware Implementations of Hash Function Luffa," IPSJ Journal, Vol.52, No.12, pp. 3755-3765, Dec., 2011. (Recommended paper) 3. Yuichi Baba, Atsushi Miyamoto, Naofumi Homma, Takafumi Aoki and Akashi Satoh, "Design and Evaluation of RSA Processor Generation System," IPSJ Journal, Vol. 51, No. 9, pp. 1847-1858, Sep., 2010. (Recommended paper)
	Books or chapters in books	
	Communications (conferences)	1. Yuichi Hayashi, Takaaki Mizuki, Naofumi Homma, Hideaki Sone, Takafumi Aoki, "An efficient cartography for acquisition of side-channel information on a cryptographic device," SCIS2012, 3C2-1, Feb., 2012. 2. Yang Li, Kazuo Ohta, Kazuo Sakiyama, "Sensitive-Data Dependency of Faulty Behavior and Its Application," SCIS2012, 3C1-3E, Feb., 2012. 3. Daisuke Fujimoto, Makoto Nagata, Toshihiro Katashita, Akihiko Sasaki, Yohei Hori, Akashi Satoh, "A Fast Power Current Analysis Methodology using Capacitor Charging Model for Side Channel

		Attack Evaluation," SCIS2012, 1C2-6, Jan., 2012. 4. Taishi Ikematsu, Yu-ichi Hayashi, Takaaki Mizuki, Naofumi Homma, Hideaki Sone, Takafumi Aoki, "A prediction method of information acquisition on electromagnetic information leakage," EMCJ, EMC-11-32, Dec., 2011. 5. Haruki Shimada, Yuichi Hayashi, Takaaki Mizuki, Naofumi Homma, Hideaki Sone, Takafumi Aoki, "Fundamental study on investigation of relationship between the intensity of EM radiation and that of EM information leakage on a cryptographic device," EMCJ, EMC-11-23, Oct., 2011. 6. Yuichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, "Study on Intentional Electromagnetic Interference against Cryptographic Modules," 2011IEICE Society Conf., B-4-58, Sep., 2011. 7. Toshihiro Katashita, Yohei Hori, Akashi Satoh, "Development of a side-channel standard evaluation board for IC cards," DICOMO2011, pp. 1301-1307, Jul., 2011. 8. Yuichi Hayashi, Takeshi Sugawara, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, "Fundamental Study on Fault Injection Analysis to Cryptographic Module Using Intentional Electromagnetic Interference," EMCJ, EMC-11-17, Jun., 2011. 9. Yuichi Hayashi, Taishi Ikematsu, Takaaki Mizuki, Naofumi Homma, Takafumi Aoki, Hideaki Sone, "Evaluation of information availability from electronic devices on the basis of SNR," EMCJ, EMC-11-002, Mar., 2011. 10. Hikaru Sakamoto, Yang Li, Kazuo Ohta, Kazuo Sakiyama, "Fault Sensitivity Analysis against Elliptic Curve Cryptosystems," SCIS2011, 3D3-2, Jan., 2011. 11. Kazuya Matsuda, Yutaka Kawai, Kazuo Sakiyama, Kazuo Ohta, "Key-Private Identity-Based Proxy Re-Encryption," SCIS2011, 3F3-6, Jan., 2011. 12. Toshihiro Katashita, Yohei Hori, Akashi Satoh, "Preliminary evaluation of a side-channel standard evaluation board for IC cards," SCIS 2011, 1D1-1, Jan., 2011. 13. Sho Endo, Naofumi Homma, Takeshi Sugawara, Takafumi Aoki, Akashi Satoh, "Power Analysis Attack with Fault Injection on Modular Exponentiation Algorithms," SCIS2011, 1D2-5, Jan., 2011. 14. Yuichi Hayashi, Takeshi Sugawara, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, "Fault Injection Attack Using Electromagnetic Field through Power Cables," SCIS2011, 3D3-4, Jan., 2011. 15. Toshihiro Katashita, Akashi Satoh, "Hardware Evaluation of Luffa on FPGA," CSS2010, 1B2, Oct., 2010. 16. Toshihiro Katashita, Akashi Satoh, Makoto Nagata, Daisuke Fujimoto, "Side-channel analysis by noise simulation of device power supply," DICOMO2011, Jul., 2010.
Outreach initiatives	**Popularization articles**	1. Yang Li, Daisuke Nakatsu, Qi Li, Kazuo Ohta, and Kazuo Sakiyama, "Clockwise Collision Analysis – Overlooked Side-Channel Leakage Inside Your Measurements," Cryptology ePrint Archive, Report 2011/579, 2011.
	Popularization conferences	
	Others	1. Kazuo Sakiyama, "A New Fault Analysis Attack (joint work with Yang Li and Kazuo Ohta)," 2010 Japan-Taiwan Joint Research Symposium on Cryptography and Next IT-society, Nov., 2010. (Invited talk) 2. Naofumi Homma, "Electromagnetic Information Leakage for Side-Channel Analysis of Cryptographic Modules," IEEE International Symposium on Electromagnetic Compatibility, July 2010. (Invited talk)

D.2 OTHER VALORIZATION FACTORS

List of factors. Indicate the titles, years and comments	
International patents obtained	1. 2.
International patents pending	1. 2.
French National patents obtained	1. 2.
Japanese National patents obtained	3.
French National patents pending	1. 2.
Japanese National patents pending	3.
Operating licences (obtained / transferred)	1. 2.
Company creations or spin-offs	1. 2.
New collaborative projects	1. 2.
Scientific symposiums	1. 2.
Others (specify)	1. Provide measurement platform as a standard environment. (http://staff.aist.go.jp/akashi.satoh/SASEBO/en/board/sasebo-w.html) 2. Licensing production and distribution of SASEBO-W boards with MORITA TECH CO.,LTD. and TOPPAN CO., LTD. (http://www.morita-tech.co.jp/security_system.html) 3. SASEBO-W is supported by a smartcard testing product. (Riscure INSPECTOR, http://www.riscure.com/pdf/Inspector_brochure_screen.pdf)