Physical Security Testing Workshop, Sept. 26-29, 2005

TSRC and Side Channel Security Requirement

Tsutomu Matsumoto[†1] **Shinichi Kawamura**[†2] **Kouichi Fujisaki**[†3] **Naoya Torii**[†4]
Shuichi Ishida[†5] **Yukiyasu Tsunoo**[†6] **Minoru Saeki**[†7] **Atsuhiro Yamagishi**[†8]

†1-8) Tamper-resistance Standardization Research Committee (TSRC) of INSTAC member,
†1) Yokohama National Univ., †2, 3) Toshiba Corp., †4) Fujitsu Laboratories Ltd., †5) Hitachi, Ltd.,
†6) NEC Corp., †7) Mitsubishi Electric Corp., †8) Information-Technology Promotion Agency (IPA)
E-mail†1) tsutomu@mlab.jks.ynu.ac.jp, †2) shinichi2.kawamura@toshiba.co.jp

Abstract: This paper consists of two parts: First part deals with activities of TSRC. Second part is about TSRC comments on 140-3, which is primarily the same as the comments submitted to NIST last February, where we discussed that the forthcoming standards of cryptographic module should include the Side Channel Security Requirement (SCSR). Although SCSR may be described focusing on attack technique or countermeasure at the moment, it is important to develop and establish concrete *metrics* for the evaluation of tamper-resistance strength.

1. Introduction

Tamper-resistance Standardization Research Committee (TSRC) was established in 2003 in Information Technology Research and Standardization Center (INSTAC), which is a department of Japanese Standardization Association (JSA). The purpose of TSRC is to establish the foundations of secure implementation of information technologies from a point of view of standardization by carrying out the following study and research items:

1. Systematic study of various tampering techniques
2. Developing the method to describe requirements to tamper-resistance
3. Contributing to the international standardization with respect to tamper-resistance

It was in the year 2003 that Security Requirement for Cryptographic Modules became a New Work Item in ISO/IEC JTC1 SC27. This was one of the events that triggered TSRC to start. On the other hand, there were pressing domestic demands for secure implementation of cryptographic functions for government use as well as commercial use. With these backgrounds, TSRC has been focusing on technical study of future items for standardization. Its scope is a little different from that of the CRYPTREC cryptographic module committee, another activity in Japan, which is aiming at the creation of evaluation criteria and test requirements for cryptographic modules to prepare for a domestic CMVP compliant to the international standard.

TSRC is a three-year-term committee and its plan is as follows: it was established in September 2003 and decided its direction and started building platforms for experiments. In FY2004, it studied tamper-resistance deeply, based on theoretical and experimental analysis. It also discussed how to describe requirements to tamper-resistance. In FY2005, it is attempting to contribute to tamper-resistance standardization, including FIPS140 series.

This paper consists of two parts: First part deals with activities of TSRC. Second part is about TSRC comments on 140-3, which is primarily the same as the comments submitted to NIST last February, where we discuss that the forthcoming standards of cryptographic module should include the Side Channel Security Requirement (SCSR). Although SCSR may be described focusing on attack technique or countermeasure at the moment, it is important to develop and establish concrete measurement, which we call *metrics*, for the evaluation of tamper-resistance strength.

PART I: TSRC Activities

2. Systematic Study of Tamper-Resistance

At the early stage of our activities, we recognized the difficulties in handling the tamper-resistance issues due to the following points:

- Not all attack methods and protection methods can be discussed openly.
- Development of tamper-resistant technique requires a physical target module.
- A few literatures discussed evaluation methods of tamper-resistance.

This situation is quite different from that of the cryptographic algorithm research, where open discussion is common, no specific module is required, many criteria for evaluation have been discovered, and rigorous notion of security have been established. Systematic study of tamper-resistance is a challenge to overcome these difficulties.

Various invasive or non-invasive attacks have been proposed so far. Some of them are covered by the FIPS 140-2. However, we recognize that side channel attacks do not covered well in the current FIPS in spite of its threads, perhaps because it is relatively new attacks. In addition a lot of literatures describe side channel attacks. Therefore we decided to focus on the side channel attacks.

We have surveyed open literatures and categorize those attack methods. We also categorize those attacks with respect to the target algorithm. The resulting matrix is presented in the Appendix 1. The matrix is still to be maintained because there are blank cells. The ultimate goal of this work would be to make a comprehensive map or dictionary of side channel attacks.

This is our approach for the first point of the difficulties. As for second and third points, we have been trying other approaches described in Section 3 and 4, respectively.

3. Evaluation Platform

3.1. Specifications and Compliant Boards

As mentioned, development of tamper-resistant techniques requires a physical target module. Although many literatures reported experimental results, the specification of their target module is not necessarily clear and thus comparison of the results is difficult.

On the other hand, it is quite rare for a vendor to publish attack results against their own cryptographic module. Similarly, it is also rare for a researcher to report attack results against a cryptographic module of a specific vendor, because such reports would not be constructive.

In both cases, lack of standard platform seems to hinder the development of tamper-resistance technology. It will change the situation if there is a standard platform whose specification is publicly available and non-proprietary.

Table 1. INSTAC-8 Spec. Outline

CPC	Zilog Z80 (CMOS) 8MHz
Memory	256KB SRAM/32KB EEPROM
Peripheral IC	16bit Programmable Counter
Communication Port	RS232C
Clock	Built-in Crystal Oscillator
Supply Voltage	+5.0V
Board Size	18Cm * 15cm
Number of Layers	2
Board Material	FR-4 (Glass board material epoxy resin)

Table 2. INSTAC-32 Spec. Outline

CPC	Freescale MPC852T 100MHz (PowerPC)
Memory	8MB SDRAM, 512KB Flash Memory, 8MB Flash Memory*2
FPGA	Xilinx Virtex II XC2V1000-5FG456C (for Cryptographic Function), Xilinx Spartan II 100 (for I/O Controller)
Communication Port	10/100Base-TX Ethernet, RS232C
Clock	Built-in Crystal Oscillator
Supply Voltage	+3.3V
Board Size	30cm * 20cm
Number of Layers	6
Board Material	FR-4

Therefore, TSRC have designed specifications of evaluation platform, INSTAC-8 and INSTAC-32. It has developed evaluation platform boards compliant to the specifications. INSTAC-8 compliant board has 8-bit CPU, whereas INSTAC-32 board has 32-bit CPU and FPGA.

In order to collect fundamental data, we investigated whether the compliant platforms can be used to DPA experiments. We also evaluated validity of several countermeasures for DPA using the platforms.

After these self-evaluations, we have supplied them domestically upon request, in cooperation with IPA. Several results have been reported [302]-[306]. It seems that substantial results are starting to come out, so far in the academic area.

3.2. A Lesson form INSTAC-8 and -32

We summarize a lesson learned from INSTAC-8 and -32.

- Present specifications are not sufficient for making the different boards compliant to the spec. have the same property.
- Even if the same compliant board is used, it is not sufficient to obtain the same data. Standardization of experimental environment is also necessary.
- Stable supply route of the boards should be established.
- More flexible and easy-to-use user interface should be provided.
- Feedbacks from the users should be reflected to the latest version.

4. Toward Metrics Based Requirement

4.1. Three Approaches

According to second purpose of TSRC listed in the Introduction, we are searching for the method to describe requirements to tamper-resistance. We have categorized three approaches to describe the requirements:

1. Approach focusing on Attacks
2. Approach focusing on Countermeasure
3. Approach focusing on Metrics

Refer to Part II of this paper for the difference of these approaches.

1 and 2 are conventional approach, but even in these cases, it seems necessary to develop objective metrics that represent tamper-resistance. Thus, the metric based approach is not exclusive with other approaches, rather complementary. The problem is that there is no metrics specified to represent the side channel resistance, so far.

4.2. Metrics

To develop metrics based requirements, the following steps seem reasonable, not to say best or optimum.

First it is necessary to investigate as much side channel attacks as possible and to understand the attacks sufficiently. Then, categorize them appropriately and extract essential points of the attacks. To reduce the workload, we may consider specific algorithm for a while.

Secondly, it is necessary to determine physical quantity to measure such as timing, power consumption, electro magnetic radiation, sound, etc.

In addition, we have to specify conditions to assume for the measurement. They include parameter settings of a target module, environment around the module, method of measurement.

Most important thing is to specify how to process the measured quantity to evaluate the tamper-resistance. In general, since raw data tend to be noisy, it is important at the first stage to apply screening of significant data, alignment of data, filtering of data, and so on.

After that, auto- or cross-correlation of time variant data will be a good tool for timing analysis. It will be another typical tool to visualize correlation between measured data and certain reference signal. In fact, if the quantity is power consumption and the reference is intermediate data of encryption process, this is the differential power analysis itself.

We do not limit processing methods to those mentioned here. At the same time, we have to select or integrate the processing methods to reduce the testing cost.

Lastly, we needs judgment standard to determine the score of processed results. We also need a function to integrate plural of scores to a total score.

It is likely that explosion of steps will occur if every metric is checked. Sampling test method should be employed to reduce the cost. Optimization of total testing cost is another important issue.

4.3. White Box vs. Black Box

Another important point of argument we recognize is the white box evaluation versus black box evaluation. In the white box evaluation, an evaluator will access to any information concerning the implementation, such as source codes, circuit design, and so on. In addition, an evaluator may change various parameters such as key material, input data, etc. In this case, the evaluator will have the sufficient information about the implementation. In the black box evaluation, on the other hand, an evaluator will have the same level of information as the end user of the module.

It seems that white box evaluation is convenient for the evaluator in that it provide sufficient information. Black box evaluation seems better for the module vendor because vendor leaks minimum information about their module to the evaluator. Trade off of these two extreme cases should be considered to determine the appropriate gray box evaluation condition.

5. Conclusion of PART I

In this part, we have introduced TSRC activities, which include studying literatures about side channel attacks, development of evaluation platform, and the research on the description method of side channel security requirement. We have exchanged these ideas with several foreign organizations and have received valuable advice from them.

As mentioned in Section 2, the research of secure implementation is still premature compared with the research of cryptographic algorithm. There are a lot of things to do to establish the foundation of secure implementation of information technologies. Apparently, our work has not been finished yet. It is our pleasure if we have advices or comments which way to proceed.

Part II will deal with a proposal of Side Channel Security Requirement (SCSR).

PART II: Comments on FIPS140-3

6. Need of Side Channel Security Requirement (SCSR)

Side channel attacks such as power analysis, timing analysis have been discussed in many academic literatures. In addition, countermeasures against side channel attacks have already been implemented in some products, such as smart cards. Although side channel attacks are referred to in Section 4.11 of FIPS 140-2, where Mitigation of Other Attacks are dealt with, concrete security requirements for those attacks are not specified in FIPS 140-2. Therefore, the security requirements with respect to side channel attacks should be specified in the FIPS 140-3.

7. Methods to Describe SCSR

Three typical methods are identified to describe SCSR.

i. Approach Focusing on Attacks

In this approach, attack methods are explicitly specified and cryptographic modules are required to have resistance against these attacks. Statement in this approach may be exemplified by “Cryptographic module is required to be resistant to the timing attack.” An appropriate list of attacks is necessary to implement this approach.

ii. Approach Focusing on Countermeasure

In this approach, requirement is not described by the attack method, but by its countermeasures. For instance, “Cryptographic module is required to implement internal data masking” is a sample statement for this approach. Many requirements in FIPS140-2 are described in such a style.

iii. **Approach Focusing on Metrics**

Security requirement in this approach specifies the metrics and its target value to fulfill the security requirement. To define the metrics, additional conditions such as settings of test environment should be clarified.

We consider the approach focusing on metrics would be the best among three approaches if such metrics are established. It seems, however, premature to take this approach at this point except in a few cases where the metrics are well-defined and established.

It seems natural to describe SCSR based on "Approach Focusing on Attacks." On the other hand, it seems a little too restrictive to specify concrete countermeasure in the requirement because in that case, manufacturer will have little chance to choose a countermeasure from many candidate countermeasures.

Therefore, we conclude that it is desirable to describe SCSR basically focusing on attacks. We do not deny inclusion of countermeasures in the SCSR so long as the countermeasures are not too specific. We do not deny inclusion of well-established metrics for testing side channel security.

8. Security Levels and Cryptographic Boundary

8.1. Mapping Side Channel Attacks to Security Levels

The level mapping is considered based on two aspects, variation of the side channel attacks and availability of equipment used for the attacks.

We consider the timing analysis, the power analysis, the electromagnetic analysis, and the fault-based attacks as general side channel attacks.

The concrete classification is as follows:

Security level 1 requires nothing special with respect to side channel attacks.

Security level 2 requires resistance against basic side channel attacks, such as the timing analysis, and the attack equipment is inexpensive one. Attacker is assumed to have sufficient knowledge.

Security level 3 requires the resistance against timing analysis, power analysis, electromagnetic analysis, and casual fault-based attack, which we consider as general side channel attacks, and commercially available attack equipment is supposed. Attacker is assumed to be a proficient.

Security level 4 requires resistance against all known side channels attacks, with known equipments. Expert attacker is assumed.

8.2. On the Side Channel Attacks Based on Fault Induction

In the previous subsection, fault based attack is included in the requirement. Not all fault based attacks are considered to be a side channel attack. But fault induction technique is assumed in some side channel attacks and we think such attacks are to be handled in the side channel security requirement.

We classify that the level 3 requires the mechanisms against casual fault based attack, such as putting the glitch in the power supply line, and that the level 4 requires the mechanisms against fault based attack with advanced attack equipments.

8.3. Need for Application to All Embodiments

We think that the SCSR should apply all embodiments, that is, single-chip cryptographic modules, multiple-chip embedded cryptographic modules, and the multiple-chip standalone cryptographic modules. We have not found the necessity to treat these three embodiments separately with respect to side channel attacks.

8.4. About the Cryptographic Boundary

Difficulty to apply side channel attack sometimes depends on how we define the cryptographic boundary. For instance, let us consider a non-contact type smart card of which cryptographic module consists of a chip and antenna. If the antenna is not included within the cryptographic boundary, a power analysis is comparatively easy by measuring the current flows between the antenna and the chip. If the antenna is included within the cryptographic boundary, electromagnetic analysis may be necessary to attack the module.

It seems that the evaluation methods are different depending on the definition of the cryptographic boundary, that is, whether the cryptographic module includes the power circuit, or whether it includes the passive components as a part of module from the viewpoint of the side channel attack. It is thought that the definition of the cryptographic boundary of FIPS140-3 should clarify the definition in more detail so that a variety of cryptographic modules can be evaluated.

9. EFP/EFT as Countermeasure against Fault Based Attacks

This section describes additional requirements as countermeasure against fault based attacks which cause processing error temporally without accessing inside of cryptographic module's enclosure. There are requirements in EFP/EFT section for attacks changing temperature or voltage. For example, there is the following requirement for EFP.

If the temperature or voltage fall outside of the cryptographic module's normal operating range, the protection circuitry shall either (1) shutdown the

> *module to prevent further operation or (2) immediately zeroize all plaintext secret and private cryptographic keys and CSPs.*

This requirement may be considered as a countermeasure against fault based attacks with deliberate excursions outside the specified normal operating ranges of voltage and temperature. But there is no requirement in FIPS140-2 for clock signals out of normal operating range to synchronous circuit. The following shows a tentative additional EFP/EFT requirement with respect to clock signals.

> If clock signal outside of the cryptographic module's normal operating range is inputted, the protection circuitry shall (1) prevent the module from being affected by the signal, or (2) shutdown the module to prevent further operation, or (3) immediately zeroize all plaintext secret and private cryptographic keys and CSPs.

10. Table of Attacks and Cryptographic Algorithm

We surveyed papers about side channel attacks and summarized the result in a table, where a row corresponds to an attack method, and a column corresponds to a target algorithm (See Appendix 1). Note that not all papers are mapped in the table.

This table is supplied as background data for specification of security requirements based on "Approach Focusing on Attacks".

11. Tentative Description of Side Channel Security Requirements

The following is our tentative description of Side Channel Security Requirements (SCSR), whose necessity has been discussed in the first Section of Part II of this paper.

Table 3. Summary of Side Channel Security Requirement

	General Requirements for all Embodiments	Attacks
Security Level 1	Production-grade components	
Security Level 2	Mechanisms against basic side channel attacks and inexpensive attack equipment and sufficient knowledge.	Timing analysis
Security Level 3	Mechanisms against general side channel attacks and commercially available attack equipment and proficient's knowledge.	Power analysis Electromagnetic analysis Casual fault based attack
Security Level 4	Mechanisms against known side channel attacks and known attack equipment and expert's knowledge.	Fault based attack Known side channel attacks

X. Side Channel Security

A cryptographic module shall employ side channel security mechanisms in order to protect plaintext secret, private keys and CSPs against side channel attacks (including power analysis, electromagnetic analysis, timing analysis, and fault based attack) when it processes cryptographic operations.

Depending on the physical and logical side channel security mechanisms of a cryptographic module, unauthorized attempts to retrieve plaintext secret, private keys and CSPs will have a high probability of being failed.

Table summarizes requirements against the side channel attacks for each of the four security levels. Theses requirements at each security level enhance the requirements of the previous level.
The general side channel security requirements at each security level are applied all three distinct physical embodiments of a cryptographic module.

In general, Security Level 1 requires no mechanisms. Security level 2 requires the mechanisms against basic side channel attacks. These mechanisms resist attacks with inexpensive attack equipment and knowledge. Security level 3 adds requirements for mechanisms against general side channel attacks. These mechanisms resist attacks with general attack equipment and knowledge. Security level 4 adds requirements for the mechanisms against all known side channel attacks. These mechanisms resist attacks with known attack equipment and knowledge.

X.1 General Side Channel Security Requirements (SCSR)

The following requirements shall apply to all physical embodiments.

・Documentation shall specify the embodiment and the security level for which the side channel security mechanisms of a cryptographic module are implemented.

・Documentation shall specify the side channel security mechanisms of a cryptographic module.

・If a cryptographic module includes an interface which would be used for a side channel attack, the interface including a maintenance access interface shall be defined.

・ If a side channel security mechanism includes physical security mechanisms, documentation shall specify them.

SECURITY LEVEL 1

The following requirements shall apply to all cryptographic modules for Security Level 1.

・ The cryptographic module shall consist of production-grade components.

SECURITY LEVEL 2

In addition to the general requirements for Security Level 1, the following requirement shall apply to all cryptographic modules for Security Level 2.

・A probability to retrieve plaintext secret, private keys and CSPs shall have low when basic side channel attacks are applied with inexpensive attack equipment and sufficient knowledge.

・Basic side channel attacks shall includes timing analysis

SECURITY LEVEL 3

In addition to the general requirements for Security Levels 1 and 2, the following requirements shall apply to all cryptographic modules for Security Level 3.

・A probability to retrieve plaintext secret, private keys and CSPs shall have low when general side channel attacks are applied with commercially available attack equipment and proficient's knowledge.

・In addition to the general requirements for Security Levels 1 and 2, general side channel attacks shall include power analysis, electromagnetic analysis, and casual fault based attack.

SECURITY LEVEL 4

In addition to the general requirements for Security Levels 1, 2, and 3, the following requirement shall apply to all cryptographic modules for Security Level 4.

・A probability to retrieve plaintext secret, private keys and CSPs shall have low when all side channel attacks are applied with any presently available attack equipment and expert's knowledge.

X.2 Environmental Failure Protection/Testing

If clock signal outside of the cryptographic module's normal operating range is inputted, the protection circuitry shall (1) prevent the module from being affected by the signal, or (2) shutdown the module to prevent further operation, or (3) immediately zeroize all plaintext secret and private cryptographic keys and CSPs.

For Security Levels 1 and 2, a cryptographic module is not required to employ environmental failure protection (EFP) features or undergo environmental failure testing (EFT). At Security Level 3 and 4, a cryptographic module shall either employ environmental failure protection (EFP) features or undergo environmental failure testing (EFT).

References:

Papers which appear in the Appendix 1

[2] R. Anderson and M. Kuhn, "Low Cost Attacks on Tamper Resistant Devices"----- Security Protocols, 5th International Workshop, 1997.

[3] H. Handschuh, P. Paillier, J. Stern, "Probing Attacks on Tamper-Resistant Devices",----- Proceedings of CHES '99.

[5] . Boneh, R. A. DeMillo, and R. J. Lipton, "A New Breed of Crypto Attack on Tamperproof Tokens Cracks Even the Strongest RSA Code", 1996.

[6] D. Boneh, R. A. DeMillo, R. J. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults",-----Advances in Cryptology: Proceedings of Eurocrypt '97.

[7] E. Biham, A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems"-----Advances in Cryptology: Proceedings of CRYPTO '97.

[8] M. Joye, J.-J. Quisquater, "Faulty RSA Encryption"----- UCL Report, 1997.

[9] Shiho Moriai, "Fault-Based Attack of Block Ciphers",----- Proceeding of SCIS '97.

[14] S.Chari, J.R.Rao, P.Rohatgi, "Template Attacks", CHES2002.

[16] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", CRYPTO '96.

[18] W. Schindler, "A Timing Attack against RSA with the Chinese Remainder Theorem",----- Proceedings of CHES '00.

[19] H. Handschuh and H. M. Heys, "A Timing Attack on RC5", SAC'98

[21] P. Kocher, J. Jaffe, B. Jun, "Introduction to Differential Power Analysis and Related Attacks", 1998.

[22] P. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis", CRYPTO '99.

[23] T. S. Messerges, E. A. Dabbish, R. H. Sloan, "Investigations of Power Analysis Attacks on Smartcards", USENIX Workshop on Smartcard Technology, 1999.

[25] S. Chari, C. Jutla, J. Rao, P. Rohatgi, "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards", Proceedings of the Second Advanced Encryption Standard Candidate Conference, 1999.

[26] . Chari, C. Jutla, J. Rao, P. Rohatgi, "Toward Sound Approaches to Counter Power Analysis Attacks" CRYPTO '99.

[27] L. Goubin, J. Patarin, "DES and Differential Power Analysis", CHES '99.

[30] J. S. Coron, L. Goubin, "On Boolean and Arithmetic Masking against Differential Power Analysis",----- Proceedings of CHES '00.

[33] J.Dj.Golic, C.Tymen, "Multiplicative Masking and Power Analysis of AES", CHES2002.

[37] C.D.Walter, "Sliding Windows Succumbs to Big Mac Attack", CHES'01.

[39] C. D. Walter and S. Thompson, "Distinguishing Exponent Digits by Observing Modular Subtractions", CT-RSA'01.

[40] M. Joye, J.-J. Quisquater, S.-M. Yen, and M. Yung, "Observability Analysis — Detecting When Improved Cryptosystems Fail —", CT-RSA'02.

[43] R. Novak, "SPA-Based Adaptive Chosen-Ciphertext Attack on RSA Implementation", PKC'02.

[44] W. Schindler, "Combined Timing and Power Attack", PKC'02.

[45] C.D.Walter, "Some Security of the MIST Randomizing Exponential Algorithm", CHES2002.

[47] B.den Boer, K.Lemke, G.Wiche, "A DPA Attack Against the Modular Reduction with a CRT Implementation of RSA", CHES2002.

[48] V.Klima, T.Rosa, “Further Results and Considerations on Side Channel Attacks on RSA”, CHES2002.

[49] C.Aumueller, P.Bier, W.Fischer, P.Hofreiter, J.P.Seifert, “Fault attacks on RSA with CRT :Concrete Results and Practical Counter measures”, CHES2002.

[50] J.-S. Coron, “Resistance Against Differential Power Analysis for Elliptic Curbe Cryptosystems”, CHES '99.

[51] M. A. Hasan, “Power Analysis Attacks and Algorithmic Approaches to their Countermeasures for Koblitz Curve Cryptosystems”, CHES '00.

[53] M.Joye and C.Tymen, “Protections against Differential Analysis for Elliptic Curve Cryptography: An Algebraic Approach”, CHES'01.

[56] K. Okeya and K. Sakurai, “Power Analysis Breaks Elliptic Curve Cryptosystems even Secure against the Timing Attack”, Indocrypt'00.

[60] E.Oswald, “Enhancing Simple Power-Analysis Attacks on Elliptic Curve Cryptosystems”, CHES2002.

[63] K.Itoh, T.Izu, “Address-bit Differential Power Analysis of Cryptographic Schemes OK-ECDH and OK-ECDSA”, CHES2002.

[76] Kazuhiko Minematsu, Yukiyasu Tsunoo, Etsuko Tsujihara, “An Analysis on Success Probability of Cache Attack”, SCIS2003.

[77] Kenji Ohkuma, Shinichi Kawamura, Hideo Shimizu, Hirofumi Muratani, “Key Inference in a Side-Channel Attack Based on Cache Miss”, SCIS2003.

[78] Toyohiro Tsurumaru,Yasuyuki Sakai, Toru Sorimachi, Mitsuru Matsui, “Timing Attacks on 64-bit Block Ciphers”, SCIS2003.

[79] Kazumaru Aoki, Go Yamamoto, Hiroki Ueda, Shiho Moriai, “Cache attacks on 128-bit block ciphers”, SCIS2003.

[80] Yukiyasu Tsunoo, Hiroyasu Kubo, Maki Shigeri, Etsuko Tsujihara, Hiroshi Miyauchi, “Timing Attack on AES Using Cache Delay in S-boxes”, SCIS2003.

[81] Teruo Saito, Yukiyasu Tsunoo, Tomoyasu Suzaki, Hiroshi Miyauchi, “Timing Attack on DES Using Cache Delay in S-boxes”, SCIS2003.

[82] Yukiyasu Tsunoo, Takeshi Kawabata, Etsuko Tsujihara, Kazuhiko Minematsu, Hiroshi Miyauchi, “Timing Attack on KASUMI Using Cache Delay in S-boxes”, SCIS2003.

[83] Yukiyasu Tsunoo, Tomoyasu Suzaki, Teruo Saito, Takeshi Kawabata, Hiroshi Miyauchi, “Timing Attack on KASUMI Using Cache Delay in S-boxes”, SCIS2003.

[84] Yukiyasu Tsunoo, Maki Shigeri, Etsuko Tsujihara, Hiroshi Miyauchi, “Timing Attack on SC2000”, SCIS2003.

[85] Takeshi Kawabata, Yukiyasu Tsunoo, Teruo Saito, Etsuko Tsujihara, Hiroshi Miyauchi, “Timing Attack on Hierocrypt-L1/-3”, SCIS2003.

[86] Kazumaro Aoki, Soichi Furuya, Shiho Moriai, “A timing attack using time difference of multiplications against a CIPHERUNICORN-A implementation”, SCIS2003.

[88] Tetsutaro Kobayashi, Fumitaka Hoshino, Hideki Imai, “Attack on Implementations of Elliptic Curve Cryptosystems”, SCIS2003.

[91] Yasuyuki Sakai, Kouichi Sakurai, “On the Side Channel Attacks Against a Parallel Algorithm of the Exponentiation”, SCIS2003.

[92] Hideyuki Miyake, Yuuki Tomoeda, Atsuhi Shimbo, Shinichi Kawamura, “New timing attack against RSA implementation with Montgomery multiplication”, SCIS2003.

[95] Masanobu Koicke, Shinichi Kawamura, Tsutomu Matsumoto, “Shide-Channel Attacks on RSA Implementation in RNS Representation and Their Countermeasures”, SCIS2003.

[101] Dakshi Agrawal, Josyula R. Rao, and Pankaj Rohatgi, “Multi-channel Attacks”, CHES2003.

[102] Siddika Berna Ors, Elisabeth Oswald, and Bart Preneel, “Power-Analysis Attacks on an FPGA - First Experimental Results”, CHES2003.

[103] Yukiyasu Tsunoo, Teruo Saito, Tomoyasu Suzaki, Maki Shigeri, and Hiroshi Miyauchi, “Cryptanalysis of DES Implemented on Computers with Cache”, CHES2003.

[104] Gilles Piret and Jean-Jacques Quisquater, “A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD”, CHES2003.

[105] Pierre-Alain Fouque, Gwnaelle Martinet, and Guillaume Poupard, “Attacking Unbalanced RSA-CRT Using SPA”, CHES2003.

[107] Nigel P. Smart, “An Analysis of Goubin's Refined Power Analysis Attack”, CHES2003.

[108] Julien Cathalo, Francois Koeune, and Jean-Jacques Quisquater, “A New Type of Timing Attack: Application to GPS”, CHES2003.

[201] Eric Brier, Christophe Clavier, and Francis Olivier, “Correlation Power Analysis with a Leakage Model”, CHES2004.

[202] Francois-Xavier Standaert, Siddika Berna Ors, and Bart Preneel, “Power Analysis of an FPGA Implementation of Rijndael: Is Pipelining a DPA Countermeasure?”, CHES2004.

[203] Kai Schramm, Gregor Leander, Patrick Felke, and Christof Paar, “A Collision-Attack on AES Combining Side Channel- and Differential-Attack”, CHES2004.

[205] Colin D. Walter, “Simple Power Analysis of Unified Code for ECC Double and Add”, CHES2004.

[206] Kerstin Lemke, Kai Schramm, and Christof Paar, “DPA on n-Bit Sized Boolean and Arithmetic Operations and Its Application to IDEA, RC6, and the HMAC-Construction”, CHES2004.

[207] Jonathan J. Hoch and Adi Shamir, “Fault Analysis of Stream Ciphers”, CHES2004.

[208] Ludger Hemme, “A Differential Fault Attack Against Early Rounds of (Triple-)DES”, CHES2004.

[301] Sebastien Kunz-Jacques, Frederic Muller, and Frederic Valette “The Davies-Murphy Power Analysis”, ASIACRYPT2004.

Papers which do not appear in the Appendix 1.

[1] R. Anderson, M. Kuhn, “Tamper Resistance a Cautionary Note”-----2nd USENIX Workshop on Electronic Commerce, 1996

[4] O. Kommerling, M. Kuhn, “Design Principles for Tamper-Resistant Smartcard Processors”,-----USENIX Workshop on Smartcard Technology, 1999.

[10] P. Paillier, “Evaluating Differential Fault Analysis of Unknown Cryptosystems”, PKC'99.

[11] S.-M. Yen, S. Kim, S. Lim, and S. Moon, “RSA Speedup with Residue Number System Immune against Hardware Fault Cryptanalysis”, ICISC'01.

[12] S.Skorobogatov and R.Anderson, “Optical fault induction attacks”, CHES2002.

[13] E.Trichina, D.De Seta, L.Germani, “Simplified Adaptive Multiplicative Masking for AES and its Securized Implementation”, CHES2002.

[15] S.Agrawal, B.Archambeault, J.R.Rao, P.Rohatgi, “The EM side-channel(s)”, CHES2002.

[17] J.-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestre, J.-J. Quisquater, J.-L. Willems, “A Practical Implementation of the Timing Attack”, UCL Report, 1998.

[20] K. Okeya, H. Kurumatani, and K. Sakurai, “Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications”, PKC'00.

[24] E. Biham, A. Shamir, “Power Analysis of the Key Scheduling of the AES Candidates”,-----Proceedings of the Second Advanced Encryption Standard Candidate Conference,1999.

[28] M.Akkar and C.Giraud, "An Implementation of DES and AES, Secure against Some Attacks", CHES'01.
[29] Thomas S.Messerges, "Securing the AES Finialists Against Power Analysis Attacks", Fast Software Encryption, FSE 2000, pp.150-164.FSE2000.
[31] L.Goubin, "A Sound Method for Switching between Boolean and Arithmetic Masking", CHES'01.
[32] K. Itoh, M. Takenaka, and N. Torii, "DPA Countermeasure Based on the Masking Method", ICISC'01.
[34] T. S. Messerges, E. A. Dabbish, R. H. Sloan, "Power Analysis Attacks of Modular Exponentiation in Smartcards", CHES '99.
[35] G. Hachez and J.-J. Quisquater, "Montgomery Exponentiation with no Final Subtractions: Improved Results", CHES'00.
[36] C.Clavier and M.Joye, "Universal exponentiation Algorithm: A First Step towards Provable SPA-Resgistance", CHES'01.
[38] S.-M. Yen, S. Kim, S. Lim, and S. Moon, "A Countermeasure against One Physical Cryptanalysis May Benefit Another Attack", ICISC'01.
[41] C. D. Walter, "Precise Bounds for Montgomery Modular Multiplication and Some Potentially Insecure RSA Moduli", CT-RSA'02.
[42] C. D. Walter, "MIST: An Efficient, Randomized Exponentiation Algorithm for Resisting Power Analysis", CT-RSA'02.
[46] K.Itoh, J.Yajima, M.Takenaka, N.Torii, "DPA Countermeasure by improving the Window Method", CHES2002.
[52] E.Oswald and M.Aigner, "Randomized Addition-Subtraction Chains as a Countermeasure against Power Attacks", CHES'01.
[54] P.-Y.Liardet and N.P.Smart, "Preventing SPA/DPA in ECC Systems Using the Jacobi Form", CHES'01.
[55] M.Joye and J.-J.Qusiquater, "Hessian Elliptic Curves and Slide-Channel Attacks", CHES'01.
[57] K. Okeya, K. Miyazaki, and K. Sakurai, "A Fast Scalar Multiplication Method with Randomized Projective Coordinates on a Montgomery-Form Elliptic Curve Secure against Side Channel Attacks", ICISC'01.
[58] T. Izu and T. Takagi, "A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks", PKC'02.
[59] E. Brier and Marc Joye, "Weierstra Elliptic Curves and Side-Channel Attacks", PKC'02.
[61] E.Trichina, A.Bellezza, "Implementation of Elliptic Curve Cryptography with Built-in Counter Measures against Side Channel Attacks", CHES2002.
[62] C.Gebotys, R.Gebotys, "Secure Elliptic Curve Implementations: An Analysis of Resistance to Power-Attacks in a DSP Processor", CHES2002.
[64] M.Ciet, J-J.Quisquater, F.Sica, "Preventing Differential Analysis in GLV Elliptic Curve Scalar Multiplication", CHES2002.
[65] J.C.Ha, S.J.Moon, "Randomized Signed-Scalar Multiplication of ECC to Resist Power Attacks", CHES2002.
[66] R. Mayer-Sommer, "Smartly Analyzing the Simplicity and the Power of Simple Power Analysis on Smartcards"----- Proceedings of CHES '00.
[67] P. N. Fahn, "IPA: A New Class of Power Attacks"----- Proceedings of CHES.
[68] T. S. Messerges, "Using Second-Order Power Analysis to Attack DPA Resistant Software"----- Proceedings of CHES '00.
[69] "Electromagnetic Attacks", CHES01.
[70] M.-L. Akkar, R. Bevan, P. Dischamp, and D. Moyart, "Power Analysis, What Is Now Possible...", Asiacrypt 2000.
[71] S.Agrawal, B.Archambeault, J.R.Rao, P.Rohatgi, "The EM side-channel(s)", CHES2002.
[72] Shamir, "Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies"----- Proceedings of CHES '00.
[73] C. Clavier, J. S. Coron, N. Dabbous, "Differential Power Analysis in the Presence of Hardware Countermeasure"----- Proceedings of CHES '00.
[74] E.Brier, H.Handschuh, and C.Tymen, "Fast Primitives for Internal Data Scrambling in Tamper Resistant Hardware", CHES'01.
[75] D.May, H.L.Muller, and N.P.Smart, "Random Register Renaming to Foil DPA", CHES'01.
[87] Yukiyasu Tsunoo, Tomoyasu Suzaki, Hiroyasu Kubo, Etsuko Tsujihara, Hiroshi Miyauchi, "Timing Attack on CIPHERUNICORN-A Using Cache Delay in S-boxes", SCIS2003.
[89] Katsuyuki Okeya, Kouichi Sakurai, "On Assumptions of Implementational Attacks and Their Practicality", SCIS2003.
[90] Tetsuya Izu, Takeshi Koshiba, Tsuyoshi Takagi, "Provable Security against Side Channel Attacks", SCIS2003.
[93] Tetsuya Izu, Kouichi Itoh, Masahiko Takenaka, Naoya Torii, "Comparison of Side-channel Countermeasures for Protecting Elliptic Curve Cryptography", SCIS2003.
[94] Tetsuya Izu, Kouichi Itoh, Masahiko Takenaka, "A Practical Countermeasure Against Address-bit DPA", SCIS2003.
[96] David Naccache, Michael Tunstall, "How to Explain Side-Channel Leakage to Your Kids", CHES'00.
[97] Steve H.Weingart, "Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses", CHES'00.
[106] Pierre-Alain Fouque and Frederic Valette, "The Doubling Attack - Why Upwards Is Better than Downwards", CHES2003.
[204] Herve Ledig, Frederic Muller, and Frederic Valette, "Enhancing Collision Attacks", CHES2004.
[209] J. Waddle and D. Wagner, "Towards Efficient Second-Order Power Analysis", CHES2004.
[302] K.Fujisaki, Y.Tomoeda, H.Miyake, Y.Komano, A.Shimbo, K.Kawamura, "Development of DPA evaluation platform for 8 bit processor", ISEC2004-55,2005.
[303] K. Fujisaki, H. Shimzu, A. Shimbo, "Development of DPA evaluation platform for 32 bit processor", ISEC2005-19,2005.
[304] Y. Takahashi, T. Fukunaga, T. Fukunaga,T. Fukunaga, "Side channel attacks against block cipher implementaion on CPU", ISEC2004-114,2004.
[305] H. Miyake, H. Nozaki, H. Shimizu, A. Shimbo, "A method of PA-evaluation based on the property of S-BOXes", SCIS2005, 2005.
[306] Y.Tsunoo, T. Hisakado, E.Tsujihara, T. Matsumoto, S. Kawamura, K. Fujisaki, "Experimental Results on INSTAC-8 Compliant Board", To appear in this workshop.

Appendix 1

			Target Ciphers																												
			Symmetric Ciphers																				Asymmetric Ciphers			Digital Signature	Elliptic Curve		Authentication		
			DES	Triple-DES	AES	MISTY	Camellia	KASUMI	CIPHERUNICORN-A	CIPHERUNICORN-E	Hierocrypt-L1	Hierocrypt-3	SC2000	KHAZAD	IDEA	RC6	RC5	RC4	Lili-128	SOBER-t32	Feistel type	HMAC-Construction	RSA	Diffie-Hellman	Binary Exponential Asymmetric Ciphers	DSS	Elliptic Curve Cryptosystem	EC-DSA	Fiat-Shamir Scheme	Schnorr Scheme	GPS identification scheme
			FIPS 46-3	FIPS81	FIPS 197																		FIPS186-2	FIPS186-2		FIPS186-2	FIPS186-2	FIPS186-2			
category of attacks	Invasive Attack	Invasive Analysis	[2]																		[3]		[2]		[3]						
	Fault Attack	Fault Analysis	[7] [208]	[208]	[104]									[104]			[9]	[207]	[207]	[207]			[5] [6] [8] [40] [49]						[6]	[6]	
	Timing Attack	Timing Attack							[86]								[19]						[16] [18] [37] [39] [44] [48] [91] [92] [95]	[16]		[16]	[53] [88]				[108]
		Cache Attack	[77] [81] [103]	[78]	[80]	[76]	[83]	[82]		[78]	[78] [85]	[79] [85]	[79] [84]																		
	Power Analysis	Simple Power Analysis	[21] [22] [301]		[25]																		[43] [44] [47] [48] [105]				[51] [53] [60] [102] [205]				
		Differential Power Analysis	[21] [22] [23] [27]		[25] [26] [30] [33] [202]										[206]	[206]						[206]	[27] [37] [45] [95]				[50] [51] [53] [56] [63] [107]	[63]			
		correlation power analysis	[201]		[201]																										
	Hybrids	Multi-channel Attack	[101]																												
		collision attack			[203]																										
		Template Attacks	[14]															[14]													