Experimental Results on INSTAC-8 Compliant Board

Yukiyasu Tsunoo[†1], Toru Hisakado[†2], Etsuko Tsujihara[†3], Tsutomu Matsumoto[†4], Shinichi Kawamura[†5], Kouichi Fujisaki[†6]

†1,4,5,6) JSA/INSTAC/TSRC[#], †1,2) NEC Corporation, †3) Y.D.K.Co.,Ltd.,
†4) Yokohama National University, †5,6) TOSHIBA Corporation

†1) NEC Corporation,
1753, Shimonumabe, Nakahara-ku, Kawasaki, Kanagawa 211-8666, Japan,
tsunoo@BL.jp.nec.com
†4) Yokohama National University, Graduate School of Environment and Information Sciences,
79-7 Tokiwadai, Hodogaya, Yokohama 240-8501, Japan
tsutomu@mlab.jks.ynu.ac.jp

Abstract This paper presents the results of three kinds of side-channel attacks, experimentally made against software-implemented ciphers on INSTAC-8 Compliant Board. INSTAC-8 is the standard evaluation platform, newly designed by the Information Technology Research and Standardization Center (INSTAC; a division of Japan Standards Association), to test Side-channel attack against the software-implemented ciphers. Three side-channel attacks referred above are Differential Power Analysis (DPA), Electro Magnetic Analysis (EMA), and Simple Power Analysis (SPA).

The first experiment, where DPA was applied on DES cipher, was conducted by the designers of INSTAC-8, in order to check the board if it works as intended [10][12]. The second experiment, where EMA was made on mini-cipher, that is, a lookup of substitution box after key addition, was carried out and was reported in TECHNICAL REPORT OF IEICE by Takahashi et al. [9]. The third one, where SPA was made against A5/1 cipher, was performed by Tsunoo et al. in May 2005[11].

A5/1 is a stream cipher used as an encryption standard in the GSM (Global System for Mobile Communications). Our attack method works on the assumption that an attacker can obtain move frequency, a kind of side-channel information, that is, the number of linear feedback shift registers which are clocked at each time. Our attack is a SPA, which uses the changes in LFSR move frequency to determine the internal state of A5/1 with the average computation cost of $2^{26.84}$. In other words, our attack deduces the internal state of software-implemented A5/1, if we could know the timing that key stream bits are output.

[#] TSRC: Tamper-resistance Standardization Research Committee
INSTAC: Information Technology Research and Standardization Center
JSA: Japanese Standardization Association

1. Introduction

Side-channel cryptanalysis is known as an attack technique against the cipher module implemented on smart-cards and something like that. This attack uses the information leaked off during cipher module operation, including operation time, power consumption, electromagnetic waves, in order to derive the secret information.

In 1996, Kocher [5] proposed Timing Attack, which derives key information from the variation in cipher processing time. In 1998, Kocher, Jaffe, Jun [6] proposed Power Analysis, which derives key information from the variation in power consumption of cipher processing unit. They applied their attack against DES implemented on smartcard, to verify the efficacy of their attack.

Power Analysis is subdivided into Simple Power Analysis (SPA) and Differential Power Analysis (DPA). To derive key information, SPA uses power consumption data obtained from one encryption, while DPA uses the statistical data about power consumption based on many encryptions.

Generally, it is said that DPA is stronger than that for SPA. DPA can be applied, even if power consumption is not measured very accurately, since DPA uses more information.

Besides Power Analysis (A technique to estimate confidential information by observing power consumption) such as DPA and SPA, Side Channel Attacks include Fault-based Analysis (A technique to derive internal confidential information using the difference between normal output and faulty output caused artificially), and Timing Analysis (A technique to estimate confidential information by analyzing processing time).

Recently, more and more side-channel attacks have been presented at conferences including Workshop on Cryptographic Hardware and Embedded Systems (CHES). However, practical attack techniques were dependent on cipher algorithm, way to implement cipher, and so on. Thus, researchers needed the open platform, to which they can make an attack more freely, to make comparison of data or to verify the results of experiment.

With the goal of systematic understanding of tampering techniques, JSA/INSTAC/Tamper-resistance Standardization Research Committee established the specifications for the standard evaluation platform. INSTAC-8, which we use for our experiment, is the compliant board equipped to 8-bit CPU, based on the specifications. By March 2005, 3 experiments carried on INSTAC-8; 1) DPA was applied on DES cipher, to check the effectiveness of the attack and to make countermeasures to the DPA. 2) EMA was made on mini-cipher, a block cipher, by Takahashi et al. 3) At Symposium on Cryptography and Information Security (SCIS) held in January 2005, Tsunoo et al. presented the results of SPA and timing attack made against A5/1 cipher in computer simulation.

This paper reports the results of the attack presented at SCIS and performed on INSTAC-8. This attack is a SPA, since it works well, if we can deduce the timing that software instructions are executed, using only one kind of data obtained through measuring the power consumption data.

This paper is organized as follows. Section 2 outlines INSTAC-8 that we used for our experiment. Section 3 describes 3 experiments carried out using INSTAC-8. We conclude this paper in section 4.

2. Overview of INSTAC-8

Various side-channel attacks have been presented at conferences. However, there is no common evaluation measure for those attacks, and it is difficult to measure their threatening level and to verify the effectiveness of countermeasures. It seems that some firms are conducting research and development of anti-tampering techniques, but duty of researchers to keep their secret know-how to themselves prevents free and active exchange of their ideas. Although the threatening level of side-channel attack should be evaluated, considering its feasibility, there is no measure for evaluating those attacks. Thus, no standard platform for evaluating them was established. To cope this problem, JSA/INSTAC/Tamper-resistance Standardization Research Committee established the specifications for the standard evaluation platform. Based on the specifications, INSTAC-8 is designed. So far, the results of some experiments carried on INSTAC-8 have been announced. Judging from those results, the specifications that INSTAC established serves as useful measure to evaluate side-channel attacks and

countermeasures to them.

To meet with the purpose of collecting basic data, INSTAC-8 is designed as a compliant board equipped to 8-bit CPU. INSTAC-8 has RAM as working area, ROM to store programs, and RS232C port for communicate beside CPU, so that it can measure the power consumption while instructions of 8-bit CPU are being executed, and it can verify the effectiveness of Differential Power Analysis (DPA).

Since measuring the variation in voltage is the matter of top priority for the compliant board, power source line and ground line of INSTAC-8 compliant board are designed so that resistor can be connected to either or both of them. The board features the design that allows users to measure only changes voltage during the operation of CPU. Also, INSTAC-8 board has RS232C port as an outside interface. Thus, loading communication program into ROM of INSTAC-8 allows us to download the programs stored in our personal computers into RAM on the board, or allows our personal computers to read RAM on the board. INSTAC-8 employs LSI (MSM82C53) that has 3 16-bit wide programmable counters, as a programmable counter. With input/output instruction, CPU has access to the board, and this makes it possible to use counter output as a trigger of oscilloscope. Clock signal oscillator is specified to be implemented on the board, using 8-pin DIP socket. This is done, considering various frequencies of clock generator used as clock, or modification of frequencies with the change of oscillator. On the board, a 28 pin DIP type ROM socket is equipped, so that ROM to store programs can be changed.

3. Three Experimental Results on INSTAC-8

INSTAC-8 is the specifications of evaluation platform equipped to 8-bit CPU. It was made to meet with the purpose of collecting basic data about side-channel attacks against software-implemented ciphers. This section describes the experimental results of Differential Power Analysis made by designers of INSTAC-8 against DES, and attacks other than DPA, namely, EMA and SPA on the ciphers other than DES.

3.1. Example of DPA against Block Cipher DES

Designers of INSTAC-8 performed DPA against DES, to demonstrate the usefulness of the compliant board. They also provided 2 countermeasures to DPA, and verified the effectiveness of those countermeasures. They chose DES, to apply DPA, taking account of the performance of 8-bit CPU (Z80) equipped to the evaluation platform. When considering the performance of Z80, using only software to compute the secret key of public-key cipher is inappropriate. Thus, DPA was not applied on the algorithm of public key ciphers on INSTAC-8.

DPA was made experimentally on the DES that had not taken countermeasures to DPA. To determine the most significant bit output from the left side of the 15th round of DES, DPA was performed, to reveal the relational values between the reference values of key candidates and the changes in voltage. Based on the relational values, they determined the key candidates strongly related to the changes in voltage. When DPA was made on 32 bits output from the left side of the 15th round of DES, there was correlation between all of them and the changes in voltage.

Two tested countermeasures against DPA are the ones proposed by Goubin et al. and by Akkar et al. DPA was made experimentally against the DES program that had taken countermeasure of Goubin et al, to verify the effectiveness of those countermeasures. It was shown that attackers cannot obtain the key candidate strongly related to the changes in voltage. In other words, there was no relation ship between the reference values and the changes in voltage. For the DES that takes countermeasure of Akkar et al, no key candidate strongly related to the changes in voltage was detected, to show that there was no relation ship between the reference values and the changes in voltage.

3.2. Example of EMA against Block Cipher "Mini Cipher Model"

Takahashi et al. applied EMA against "Mini Cipher Model". Power consumption is generally measured as the value for a whole unit. But values for electromagnetic waves may provide much more information

about the unit, depending on the measuring points. Thus, they assume EMA is more threatening. Although the designers of INSTAC-8 reported that there is no strong relation between the electromagnetic wave forms and the humming weight on data values, i.e. the number of "1"s, Takahashi et al. showed that EMA can deduce the humming weight for mini cipher model.

"Mini Cipher Model" XORs plaintexts with key and lookup S-box (Substitution table) to output ciphertexts. It is the minimum cipher module using S-boxes, and used widely as a component function for most block ciphers, including DES and AES. They placed antenna they made with a lead wire around the CPU of INSTAC-8, and obtained the information on electromagnetic waves, using oscilloscope. Then, they found the linear correlation between the humming weight on key value of Mini Cipher and the electromagnetic wave forms, through paying attention to the unit which XORs input with key and forwards the data as input to S-box.

Based on computer simulation they performed, they concluded that their attack breaks mini-cipher at the success probability of 90% and 65%, if they have 2 kinds of measured data and only one kind of measured data, respectively.

Kocher, Jaffe, Jun [6] showed that DPA using differentials of electromagnetic wave forms detects the extended key on the last round of DES, if attackers uses 2 or more kinds of measured data. This is true to the case that the details of cipher implementation are unknown.

There are attacks that directly derive the secret information from one kind of measured data, if "the details of cipher implementation are unknown." SPA is one of those attacks. If attackers obtain more specific information about cipher implementation by means of changing the value of secret key, performing measurement on 2 or more units, or so, SPA becomes stronger than DPA. Takahashi et al. call such information on cipher implementation that strengthens attacks "implementation information", and they studied the efficient way to obtain implementation information. They showed that EMA deduces the humming weight of key, by providing implementation information as a template previously and comparing the measured data at time of attack with the template. They also warn that providing freely programmable platform with cipher module may lead to the leakage of implementation information, that could be hints for stronger attack.

3.3. Example of SPA against Stream Cipher A5/1

Many of stream ciphers generate keystream independently from plaintext, and use the plaintext XORed with keystream as a ciphertext. Thus, it is difficult to apply the attacks like the one made on DES, which encrypt a plenty of plaintexts using the same key, and measure the power consumption at that time. Our cryptanalysis on A5/1 determined the internal state of the cipher, by using the fact that candidates for input to clock-control unit are narrowed down, if attackers determines the number of clocked LFSRs at each time during the keystream generation of A5/1. Our attack is conditional to obtaining the number of clocked LFSRs at each time from the side-channel information.

A5/1 is the stream cipher used in the GSM (Global System for Mobile Communication) standard for cellular phone in Europe. A5/1 consists of 3 LFSRs, R1, R2, and R3, and a clock-control unit, which controls the clock of LFSR. It operates, taking 64-bit key and the frame number, that is 22-bit open parameter, as input data. Attacks against A5/1 other than ours have been proposed.

In 1997, Golic[4] proposed Time-memory Trade off attack, which uses the fact that LFSR size of A5/1 is small. In 2000, Biryukov, Shamir, and Wagner [1] presented an improved Time-memory Trade off attack. It recovers the secret key only in a few seconds to a few minute, though it requires previously computed data of about 150 to 300GB. Ekdahl and Johansson [3] proposed Correlation Attack, which uses the fact that the non-linear part of A5/1 depends only on the clock-control unit. Zenner[8] evaluated attacks, based on clock-control guessing attack, i.e. the linear consistency test (LCT) that uses keystreams Zenner also proposed the attack, which determines the internal state of A5/1, by means of detecting clock-controls that do not contradict keystreams. Lano, Mentens, Preneel, and Verbauwhede[7] proposed the DPA that uses the information on the power consumption of frames, taking account of the fact that stream ciphers like A5/1 frequently perform resynchronization using the same secret key and different frame numbers. However, its effectiveness has not evaluated in detail nor verified yet.

Our attack is conditional to the followings

1. The attacker observes a frame of keystream.
2. The attacker knows the frame number of the frame that he or she observed. The attacker need not change the frame number; any frame number will do.
3. Using the time t when a frame of keystream is generated, the attacker determines the number of clocked LFSRs. However, he or she cannot know which 2 LFSRs of 3 LFSRs of A5/1 are clocked, even if he or she knows that 2 LFSRs were clocked.

The number of LFSRs clocked at each time under the condition 3 described above is referred to as move information, hereafter, and it is assumed that move information is obtained from the side-channel information. In experiment on INSTAC-8, the move information at each time is detected from the electromagnetic wave forms during keystream generation. For the first, candidates for 3 register values that are taken to clock-control unit as input data are listed, using move information. Then, LFSRs are clocked, using one of those 3 candidates in accordance with the output from clock-control unit. By repeating this process for some times, keystream can be computed. Then, compare the computed keystream with observed keysteam. Discard the register value candidate whose internal state contradicts the keystream, and try other candidates. If all register values of 3 LFSRs are determined, then check to see if move information matches the keystream, which is computed, based on the internal state of the candidate. If contradiction is found, then discard the candidate. The candidate without contradiction holds the right internal state. If the internal state is determined, the secret key can be recovered.

We applied this SPA technique experimentally against A5/1, using INSTAC-8 compliant platform, to verify the effectiveness of the technique in the real world. In other words, we checked to see if the move information described in condition 3 can be obtained from side-channel information. We measured the changes in the voltage waves during the operation of A5/1 implemented on INSTAC-8, and we found characteristic wave form pattern among them, which allows determining the processing time of Clock operation at each time. Through comparison of width of wave patterns, each of which is based on its corresponding move information, we made sure that the width of wave form corresponding with move information=2 is different from that corresponding with move information=3. Previously performed emulation shows that interval between waves is average of 3.4ms and 4.2ms, if move=2 and 3, respectively. We also verified that correct move information can be obtained, by using this findings on wave interval.

This attack can determine the internal state of cipher with an average of $2^{26.84}$ steps of computation, if attackers obtain the move information at each time t in the course of A5/1 operation. The attack could deduce the secret key in 13.2 minutes in average, when the attack is performed, using a computer (Pentium 4, 2.0GHz)

4. Conclusion

This paper outlines INSTAC-8 established by JSR/INSTAC/TSRC and refers to 3 kinds of attacks, DPA proposed by Fujisaki et al. who are designers of INSTAC-8, EMA proposed by Takahashi et al., and SPA we proposed, which were applied against DES, Mini cipher, and A5/1, respectively. The results of these experiments indicate the usefulness of INSTAC-8 Compliant Board in evaluating side-channel attacks and countermeasures to them.

Our cryptanalysis of A5/1 determines the internal state of LFSRs, using the correlation between the number of clocked LFSRs at each time t and input data to clock-control unit. This attack is conditional to that attackers can determine how many LFSRs are clocked at each time t, during keystream generation. It is assumed that this kind of information is obtained from the side-channel information. However, any kind of side-channel information will work. With less than 1 frame of data, or to be specific, with 47-bit data in average and the number of LFSRs clocked at that time, our attack can determined the secret key of A5/1, in average of $2^{26.84}$ steps of computations. When using the computer (Pentium 4, 2.0GHz), our attack deduced the key in 13.2 minutes in average.

To verify the effectiveness of our cryptanalysis, we implemented A5/1 on INSTAC-8 standard evaluation platform and measured the power consumption. Through measuring power consumption data we found the characteristic power wave form pattern that allows us to determine the number of LFSRs

clocked at each time t. By using this information, we also ascertained that we can deduce the key of A5/1.

References:

[1] Biryukov, A., Shamir, A., and Wagner, D. Real Time Cryptanalysis of A5/1 on a PC. Fast Software Encryption (FSE 2000) (New York, NY, USA, April 2000), B. Schneier, Ed., vol. 1978 of Lecture Notes in Computer Science, pp. 1-18.

[2] Briceno, M., Goldberg, I., andWagner, D. A Pedagogical Implementation of A5/1. http://www.scard.org, May 1995.

[3] Ekdahl, P., and Johansson, T. Another Attack on A5/1. IEEE Transactions on Information Theory(June 2001).

[4] Goli´c, J. Cryptanalysis of Alleged A5 Stream Cipher. Advances in Cryptology - EUROCRYPT '97 (Konstanz, Germany, May 1997), W. Fumy, Ed., vol. 1233 of Lecture Notes in Computer Science, Springer-Verlag, pp. 239-255.

[5] Kocher, P. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. Advances in Cryptology - CRYPTO '96 (Santa Barbara, California, USA, August 1996), N. Koblitz, Ed., vol. 1109 of Lecture Notes in Computer Science, Springer-Verlag, pp. 104-113.

[6] Kocher, P., Jaffe, J., and Jun, B. Differential Power Analysis. Advances in Cryptology - CRYPTO'99 (Santa Barbara, California, USA, August 1999), M. Wiener, Ed., vol. 1666 of Lecture Notes in Computer Science, Springer-Verlag, pp. 388-397.

[7] Lano, J., Mentens, N., Preneel, B., and Verbauwhede, I. Power Analysis of Synchronous Stream Ciphers with Resynchronization Mechanism. The State of the Art of Stream Ciphers (SASC2004) (2004), pp. 327-333.

[8] Zenner, E. On the Efficiency of the Clock Control Guessing Attack. ICISC (2003), P. J. Lee and C. H. Lim, Eds., vol. 2587 of Lecture Notes in Computer Science, Springer, pp. 200-212.

[9] Yoshio Takahashi, E., Fukunaga T., Otsuka H. and Kanda M. Side-channel Attack on Block Cipher Implemented on CPU Board. TECHNICAL REPORT OF IEICE, vol. 104, no. 731, ISEC2004-114, pp. 49-54, 2005-3.

[10] Fujisaki H., Miyake H., Komano Y., Shinbo A., Kawamura S. and Tomoeda Y. Development and Examination of platform implemented on 8-bit CPU to evaluate Electric Magnetic Analysis. TECHNICAL REPORT OF IEICE, vol. 104, No. 200, ISEC2004-41-66, pp.99-102, 2004

[11] Tsunoo Y. Hisakado T. Tsujihara E. and Isshiki T. Side-Channel Cryptanalysis on A5/1. To appear.

[12] Matsumoto T. et al. TSRC and Side Channel Security Requirement. The proceeding of Physical Security Testing Workshop, Sep. 26-29, 2005