Secure implementation of cryptographic modules

— Development of a standard evaluation environment for side channel attacks —

Akashi Satoh *, Toshihiro Katashita and Hirofumi Sakane

[Translation from *Synthesiology*, Vol.3, No.1, p.56-65 (2010)]

The use of cryptographic modules is rapidly expanding throughout the world. Because of this, it is necessary to standardize a security evaluation scheme and to establish a public evaluation and validation program for these modules. Side channel attacks, which extract secret information from the cryptographic module by analyzing power consumption and electromagnetic radiation, are attracting a lot of attention. Research activity on such attacks has intensified recently. However, it is difficult to compare evaluation schemes proposed by different researchers because of differences in the experimental platform or environment. This makes it difficult for other researchers to repeat and verify the results. Therefore, we have developed cryptographic hardware boards and analysis software to serve as a common, uniform evaluation platform for side channel attacks. We have distributed this platform to government, industry, and academic research labs throughout the world in order to facilitate the development of an international standard.

Keywords : Cryptographic module, cryptographic hardware, side channel attack, differential power analysis, fault injection attack, security evaluation scheme, SASEBO

1 Introduction

The fast expansion of the broadband network as well as the popularization of high-performance, rich-featured information appliances, IC cards, and RFID tags hasten the advent of a ubiquitous information society. On the other hand, the exchange of a vast amount of information in every aspect of our daily life raises security threats including eavesdropping and falsification of communication data to the surface. Cryptography is a fundamental technology indispensable to coping with such threats. With more and more use of the technology in consumer products, a number of active studies have been conducted not only on theoretical analysis for cryptographic algorithms but also on security assurance of implementation of practical devices such as cryptographic chips. In particular, many researchers have paid significant attention to physical attacks, which observe the measureable phenomena of operating devices such as power consumption, electro-magnetic radiation, and operating times and estimate the internal cryptographic key from the leaked information on the measurement results without invading or destructing the target device. This class of attacks is called side-channel attack since such attacks exploit the information on channels other than the intended input- or output-channels. Today, while the formulation of international security evaluation standards with regard to side-channel attacks is in progress, the efforts are confronting the following difficulties. First, there is no justification for us to oblige industrial parties such as IC card vendors to supply their cryptographic products for evaluation testing or to provide their proprietary information. Second, universities or other academic institutions may publish their experimental results, but third parties can hardly trace the results produced at the different experimental environments unique to each of them. Therefore, we have developed a standard experimental environment and published information about side-channel experiments in order to contribute to the standardization activities from the neutral standpoint of the National Institute of Advanced Industrial Science and Technology (AIST) as a pubic research institution. In addition, we are pursuing collaborations with domestic and overseas research institutions, private companies, and universities toward operations of security evaluation systems for cryptographic modules.

In this paper, we first present a comprehensive vision of these standardization activities and our role in them. Secondly, we explain our effort in developing a standard evaluation environment for side-channel attacks and demonstrate the current status of side-channel attacks through experiments with the environment. Thirdly, we introduce our vision for future research on fault-injection attacks and invasive attacks, which require higher techniques, and on system dependability and security assurance against accidental errors and faults in addition to attack-basis security issues.

2 Expanding application and security evaluation of cryptographic technology

2.1 Standardization of cryptographic algorithms

The invention of writing made non-oral information propagation and knowledge accumulation possible. Since then, humankind has devised various measures for preventing a third person from discovering the information or knowledge. Cryptographic technology is one of them.

Research Center for Information Security, AIST Akihabaradaibiru 1003, 1-18-13, Sotokanda, Chiyoda-ku, Tokyo 101-0021, Japan ＊E-mail : akashi.satoh@aist.go.jp

Original manuscript received November 30, 2009, Revisions received January 8, 2010, Accepted January 21, 2010

Cryptographic algorithms and cryptanalysis techniques made dramatic advances particularly in wartime. Cryptography seen in mystery novels and suspense films mostly uses a secret algorithm that only the involved parties know, so it seems to be a puzzle-solving game different from the one in information security. Third parties, however, can decipher such cryptography once they discover the algorithm or the secret of the puzzle.

On the contrary, in today's cryptography, the key of the secret lies in the cryptographic key. Even the same message is enciphered into different ciphertext by using a different key. Therefore, if a third party obtains one key, the communicators can keep the confidentiality of messages with another key. Likewise, the Enigma machine, a mechanical cipher machine the German army used during World War II, separates the initial device setting, treated as a cipher key, from the algorithm of the machine. However, since the algorithm still involves an important hint for cryptanalysis, secure management of not only the key but also the machine itself is essential.

After the war, bank businesses and governmental operations began using cryptography for securing information, motivated by DES (Data Encryption Standard)[1] that the National Institute of Standards and Technology (NIST) established as a U.S. Federal standard in 1977. Most of previous cryptographic schemes did not clearly separate the algorithms and keys like the Enigma machine. In addition, their algorithms were not willingly made public because of their specific purposes. In those regards, disclosing the algorithm of DES was epoch-making. In the same year, Rivest, Shamir, and Adleman at the Massachusetts Institute of Technology (MIT) devised the RSA[2] (named after the inventors' surnames) scheme, which is suitable for digital signatures as well as encryption. DES is categorized as *symmetric-key cryptography* since, with the DES algorithm, encryption and decryption both use the same key. On the other hand, RSA is classified into *public-key cryptography* as it uses an encryption key and a decryption key different from each other and making the encryption key public does not affect confidentiality.

While cryptography had been considered equivalent to military technology and severely restricted to use and to import and export until the late 90's, the restrictions have gradually been relaxed since before or after 2000. Subsequently, more and more consumer products have begun using various cryptographic algorithms for different purposes. Meanwhile, the remarkable advancements in cryptanalysis techniques and computer's performance made the cryptographic strength of DES questionable. Thus, NIST called for stronger cryptographic algorithms for AES (Advanced Encryption Standard)[3] worldwide. Cryptographers and other specialists discussed the security issues and evaluated the performance of the implementations for AES algorithm proposals at three public standardization conferences[4]. Since NIST determined one as a new U.S. federal standard in 2001, several international standards have adopted AES.

The AES project triggered various evaluation and standardization works such as CRYPTREC (Cryptography Research and Evaluation Committees)[5] the security evaluation project for Japanese e-government recommended ciphers, the European Union's NESSIE project (New European Schemes for Signatures, Integrity and Encryption)[6], and ISO/IEC 18033[7]. Once it was thought that keeping the cryptographic algorithm secret provided attackers with fewer clues for cryptanalysis. However, there have been many incidents compromising proprietary algorithms that leaked through some channel or were reverse-engineered. Therefore, standard cryptographic algorithms such as AES are typically published so that many researchers and engineers can pursue various analyses for security verification of the algorithms throughout the world.

2.2 Security evaluation for cryptographic implementation

Enthusiastic security verification for standard cryptographic algorithms performed by a number of specialists ensures that there is little worry of a potential sudden exposure of a security flaw in the algorithm. Nevertheless, even with presumably secure algorithms, cryptographic key leakage may still occur due to a flaw in the software or hardware implementation of the algorithm. Unfortunately, it is hard for users to verify whether the implementation is secure or not. Thus, international standards were established for public institutes to perform security evaluation on security and cryptographic products for users' convenience, such as ISO/IEC 15408 (Common Criteria)[8][9] and ISO/IEC 19790[10].

ISO/IEC 15408 provides an evaluation framework for general information security products, including cryptographic modules, so that evaluators can verify the sound implementation of such products based on a Security Target (ST) determined by the developers. It also specifies Evaluation Assurance Level (EAL) in seven grades that express evaluation depths. The levels are roughly classified into two groups, which are EAL 1 to 4 for commercial use and EAL 5 to 7 for military and governmental secret agencies. Note that the EALs do not express the security strength of the product but indicate that the implementation of the security functions was properly conducted based on the specified ST. The security evaluation described in ISO/IEC 15408 mainly deals with logical functions, but physical security functions or hardware issues are not sufficiently mentioned. Under certain conditions, hardware security may be considered properly managed. However, this premise is not true when the attacker possesses the cryptographic hardware module such as a smart card. To address this issue,

the JIL (Joint Interpretation Library) Hardware Attacks Subgroup (JHAS), mainly consisting of European IC vendors, users, evaluation laboratories, and certification authorities, published a supporting document[11] that defines smart card physical security. Although the JIL has also accumulated the knowledge and technology about practical attacks and countermeasures on smart cards, it will not publish them.

ISO/IEC 19790, a modification of the U.S. Federal standard FIPS (Federal Information Processing Standard) 140-2[12], addresses security requirements for cryptographic modules comprising software, firmware or hardware in ten areas of different design and implementation aspects. The standardization of the testing items for the security requirements, based on the FIPS 140-2 DTR (Derived Test Requirements)[13], resulted in a separate document known as ISO/IEC 24579[14]. Cryptographic module testing under ISO/IEC 24579 judges the target module with the security levels specified in ISO/IEC 19790 ranging from 1 to 4 for each of the ten areas and eventually with the overall level indicating the minimum level across all the areas. Unlike ISO/IEC 15408, the level represents a security strength.

In Japan, Information-Technology Promotion Agency (IPA®) operates the following programs: JISEC (Japan Information Security Evaluation and Certification Scheme)[15] is based on ISO/IEC 15408. JCMVP® (Japan Cryptographic Module Validation Program)[16] is based on JIS X 19790 Security Requirements for Cryptographic Modules, which is equivalent to ISO/IEC 19790.

Since FIPS 140-2 was signed-off, more than eight years has passed, and side-channel attacks, which examine the internal activities of a cryptographic module to extract its secret key with various physical measures, have become a more and more serious threat. To reflect the changing cryptographic situation, in 2005, NIST began the process of transitioning from FIPS 140-2 to FIPS 140-3 and published the first public draft of FIPS 140-3[17] in July 2007. The revising process for ISO/IEC 19790 will proceed accordingly. In Japan, the Cryptographic Implementation Committee formed by the National Institute of Information and Communications Technology (NICT) and IPA, and the Side-channel Security Working Group under the committee are discussing security evaluation guidelines for implementations within CRYPTREC.

Side-channel attacks have drawn significant attention not only for standardization activities but also in academia, in which the international conferences on information security, hardware, or the like have held more and more sessions relevant to the attacks. In fact, technical papers on side-channel attacks account for a remarkable portion of the accepted papers in the Cryptographic Hardware and Embedded Systems (CHES)[18] workshop, which has a particularly high profile among such workshops.

3 Unification of hardware experimental environments and standardization of evaluation method

3.1 Research position

We are studying cryptographic hardware as one of the fundamental technologies that support the advancement of information network society. Our efforts include research on countermeasures and security evaluation methods against physical attacks, side-channel attacks in particular, as well as development of compact, high-speed and power-saving implementation technology in preparation for further expansion of the use of cryptographic hardware.

CRYPTREC is working for the revision of the E-Government Recommended Ciphers List scheduled for 2013. Involved with this, we are supporting CRYPTREC in their work on performance evaluation of hardware implementations of cryptographic algorithms and tamper resistance evaluation against side-channel attacks. In the development scheme for the current Recommended Ciphers List, security evaluations of theoretical aspects and performance evaluations of software implementations were performed for the proposed algorithms. While the software performance evaluations were carried out on the real processor platform specified by CRYPTREC, the hardware performance was not sufficiently evaluated and hardware implementations mainly provided by the proposers were merely presented as reference information. At that time, side-channel attacks had just emerged and were thus excluded from the evaluation elements. Thereafter, various attacking and protection schemes have been proposed and real platform evaluations with hardware have also been conducted. However, these changes have posed a problem such that third parties can hardly verify such evaluation results since each evaluator uses different experimental environments. In this regard, it may be possible to make a market-available cryptographic hardware product a common experimental platform for evaluators. However, evaluation results that may contain information about a serious vulnerability of such products should not be disclosed by third-party evaluators.

To address the construction of a common experimental environment for security evaluations for cryptographic hardware, we developed the Side-channel Attack Standard Evaluation Board (SASEBO)[19] in collaboration with Tohoku University within a project commissioned by the Ministry of Economy, Trade and Industry, and have promoted its utilization for domestic and foreign research bodies. We have also conducted various experiments ourselves with the SASEBO platform and actively published the information on newly developed countermeasures and evaluation techniques on it. The SASEBO has become available on the market through domestic circuit board vendors, intended for users such as universities and companies who plan to

engage in cryptographic hardware implementation or side-channel attack research. It is expected that this activity would further speed the promotion of side-channel attack research. At the same time, such an activity might be suspected of being an antisocial behavior encouraging malicious hackers. Comparing this situation with the case of security evaluation for cryptographic algorithms will lead to the answer to this question. The development of security evaluation schemes corresponds to that of attack schemes by a researcher of goodwill. The previous chapter demonstrated that making cryptographic algorithms open to the public for experts' third-party evaluations, rather than hiding them, will turn out to be an advantage. The same can be said for the security evaluations of cryptographic hardware implementations. In other words, through the evaluations done on the common experimental platform by many researchers, the evaluation framework efficiently determines the effective countermeasures and the effective evaluation (or attacking) techniques from various proposals, accumulating and utilizing the know-how of implementations and measurements. On that basis, we conduct the research activities with the goal of improving the security of information security products as well as contributing to constructing a dependable information network infrastructure, taking advantage of this knowledge.

3.2 Formulation of international standard specification and expansion toward security evaluation business

Toward the above-mentioned goals, as a public research institution, AIST addresses not only technological development but also various tasks as shown in Fig. 1 in cooperation with companies and related organizations domestic and overseas.

Firstly, AIST has sent a researcher to NIST to pursue collaboration works for contributions to international standardization of security evaluation schemes for side-channel attacks. While there is no question that the standardization activity by public research institutions of the U.S. and Japan is important for each of them individually, it was also important for AIST to demonstrate to NIST the advantages of working together. Therefore, we promoted our in-depth academic knowledge and advanced technology by showing a demonstration of an evaluation system prototype using the SASEBO as well as introducing AIST's activities in major related academic societies. In consequence, we took charge of the input for the description in the Physical Security – Non-Invasive Attacks section of the FIPS 140-3 second draft[20] published in December 2009. In addition, we have taken the lead in developing the evaluation testing technology for side-channel attacks.

Meanwhile, in Japan, to take advantage of the opportunity provided by the revisions of FIPS 140-3 and ISO/IEC 19790, CRYPTREC is advancing the discussion of the security evaluation guidelines for side-channel attacks. In the endeavor, AIST plays a central role and provides domestic companies and universities with a variety of technologies such as the SASEBO. Through information sharing in the CRYTPREC activity, AIST promotes not only gathering of domestic knowledge and the technological advancement but also improvement of the testing environment for a new evaluation system for cryptographic modules.

The aforementioned JHAS, in their ISO/IEC 15408 activity, is exchanging information on a variety of physical analysis methods including side-channel attacks targeting smart cards. However, they will not disclose details of such information because it contains proprietary information on their individual products. This may be considered as a way of assuring the security by hiding. However, remember that in our research activities for standardization of FIPS 140-3 or ISO/IEC 19790, disclosing the analysis results of individual products or implementation know-how is not our primary goal either. Our primary goal is to demonstrate the effectiveness and versatility of the attack methods and countermeasures through experiments on the common evaluation platform SASEBO and to formulate a security evaluation standard. In fact, even a JHAS member is not allowed to analyze a smart card of another member's without proper consent. In this respect, they are demanding a cryptographic LSI or an evaluation platform on which unrestricted analysis experiments for technology accumulation are allowed. Thus, we plan to be providing JHAS with the SASEBO technology through IPA, which is the contact point of JHAS in Japan.

Although ISO/IEC 19790 and ISO/IEC 15408 have different standardization directions, our analysis technology is applicable to the evaluation work under either one. It is difficult for cryptographic product vendors to disclose their know-how related to such analysis technology. At the same time, from the viewpoint of fairness, it is objectionable that the vendors whose products are evaluated lead the standardization of evaluation. Hence, it is significant in the standardization movements that AIST pursue the research

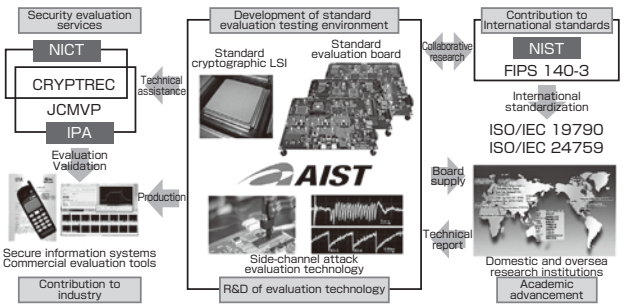


Fig. 1 Research activities for cryptographic module evaluation at AIST.

on security evaluation technology, cooperating with other organizations including NIST and CRYPTREC in its neutral position, listening to industry's voice.

In operation of an evaluation system, every participating testing laboratory is required to produce the same evaluation results if they use the same target cryptographic module. In order to ensure uniform evaluation environments and analysis skills, we plan to conduct a skill test for the testing laboratories with the SASEBO implementing a cryptographic circuit. We are also developing an analysis tool for the testing laboratories, who would then demand a training program using the board or the tool. To develop and operate such a training program will require much money and human resources, but it is difficult to keep acquiring public funds for it. Note not only that the entire society obviously benefits from the improvement of the cryptographic products security, but also that cryptographic product vendors and the testing laboratories running a security evaluation business benefit from this security evaluation movement. Therefore, we should take advantage of the vitality of corporations for the realization of higher security and the advancement of the evaluation systems. To realize this, we have brought the SASEBO to market through a few Japanese circuit board vendors toward popularization of the evaluation and countermeasure technologies. We are also planning to expand the distribution channel overseas. There are two companies in Europe and one in the U.S. which run smart card evaluation tool businesses. The negotiations we had with each of the three companies resulted in having all their tool products support the SASEBO. In addition, discussions are in progress to offer their evaluation tools and training programs to the testing laboratories with the analysis scheme AIST is developing. As a public research institution, AIST will control the fundamental subjects such as the standardization of evaluation method and the development of analysis technology with other organizations including CRYPTREC and NIST and pursue further cooperation with domestic and overseas companies toward more efficient operation of the system.

4 Practical side-channel attacks

4.1 Various physical analysis attacks against cryptographic modules

Physical analysis attack methods against cryptographic modules are classified roughly into *invasive attacks* and *non-invasive attacks* as shown in Fig. 2. Invasive attacks require expensive equipment and sophisticated technical skills to depackage the LSI, which is the core part of a cryptographic module, and to analyze its insides directly. In contrast, side-channel attacks[21][22], proposed by Kocher *et al.*, are non-invasive attacks, which do not make modifications to the modules. They exploit the internal activity information leaked through side-channels in the form of power consumption waveforms, electromagnetic waves, or timing of the operating LSI that are different from the normal I/O channels. Side-channel attacks only require relatively cheap equipment such as an oscilloscope and a personal computer to acquire and analyze the information, but they are a remarkably strong attack method. While side-channel attacks, which observe the operating states of the LSI from outside, are classified as a passive attack method, fault-injection attacks, which inject noise into the power line or clock signal to induce false operations on the LSI and analyze its response, are classified as a more sophisticated attack. It is necessary to carry out the standardization of security evaluation schemes for fault-injection attacks, following that of side-channel attacks.

4.2 Side-channel attack standard evaluation board (SASEBO)

To construct a security evaluation standard platform, we have developed the SASEBO boards and the cryptographic LSIs shown in Fig. 3 and Fig. 4, respectively. The SASEBO-G and SASEBO-B employ Xilinx® and Altera® FPGAs (Field Programmable Gate Arrays), respectively, which offer users reconfigurability of circuit functions for cryptographic algorithm implementation on different device architectures. To enable various side-channel attack experiments on these boards, we have designed the circuits of all the ISO/IEC 18033-3 standard block ciphers and the RSA scheme, the public-key cipher standard, and published the source codes of those on our partner's web site[23]. These boards offer not only hardware experiments, but also cryptographic software evaluation experiments with the Xilinx® FPGA's embedded processor or a processor macro. The cryptographic LSIs shown in Fig. 4 were fabricated in a 90-nm and a 130-nm CMOS standard cell process and have the published cryptographic circuits. These LSIs are designed to be mounted on the SASEBO-R. The SASEBO-GII, the latest SASEBO board, is equipped with a Xilinx® FPGA, and has a four to seven times larger logic capacity than SASEBO-G, while achieving a significant reduction of the board area to one third the size with a much higher density. It also features the cutting-edge partial-reconfigurability for uses other than side-channel attack experiments so that research on even higher level hardware security systems is possible.

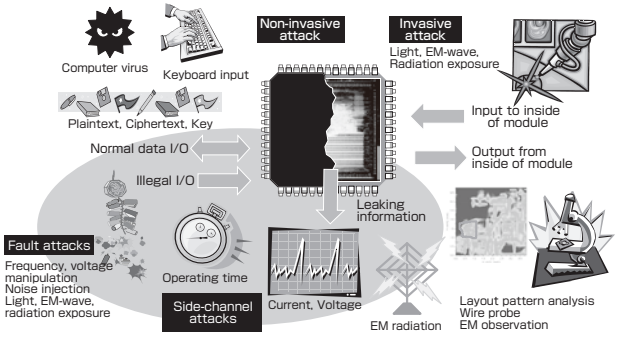


Fig. 2 Various physical attacks against cryptographic modules.

Meanwhile, the initial version of SASEBO board obtained the first JCMVP® certification[24] for a hardware module. As a secure implementation example, all of its design information and source codes are available to the public on the SASEBO web site. By the same token, we will attempt to obtain a JCMVP® certification for the SASEBO-GII.

4.3 Simple power analysis on an RSA cipher circuit

This section presents a practical side-channel attack example with the RSA scheme implemented on the SASEBO's FPGA and LSI and the experimental results from Simple Power Analysis (SPA), which extracts the cryptographic key directly from the power traces (namely, the waveform of power consumption).

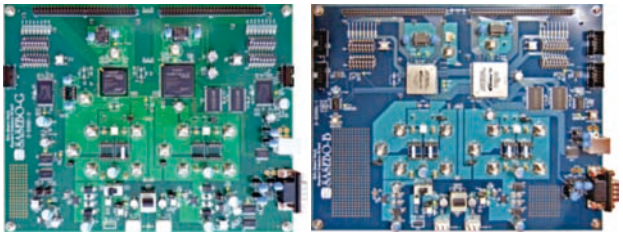
The modular exponentiation operations expressed in Eq. (1) and Eq. (2) define the RSA scheme encryption and its inversion as the decryption, respectively. The plaintext x, the data before encryption in Eq. (1), will be encrypted with e and n, both of which form the public key, into the ciphertext y, while in Eq. (2) the ciphertext y will be decrypted with the secret key (a.k.a. private key) d into the plaintext x. In these computations, 1,024-bit or longer precision integers are typically used for every variable except e so that it can be computationally difficult to obtain the secret key from the public key, while still theoretically possible.

$$\text{Encryption} : y = x^e \bmod n \quad (1)$$
$$\text{Decryption} : x = y^d \bmod n \quad (2)$$

The modular exponentiation operation in the RSA scheme is realized by iterating modular multiplication and modular squaring operations, reflecting the bit pattern of the exponent e or d. SPA attempts to acquire the secret key d by examining the computation times of each operation[21] or the differences in the power traces of each operation. Figure 5 represents an example of the left binary method, which begins the bit-wise test for the exponent d=25=$11001_{(2)}$ from the left end. As the result of each test, a bit '0' involves a modular squaring operation, whereas a bit '1' invokes both modular squaring and multiplication ($\times x$) operations. If one can distinguish between the power traces of every squaring (S) and multiplication (M), the result represents the secret key directly.

However, the difference between squaring and multiplication is not necessarily observable for the intermediate value derived from the input data differing every time. In this regard, some attack methods that enhance the difference of the operations on the power trace by manipulating input data have been studied. Figure 6 depicts parts of the power traces measured for the running RSA circuits on the 130-nm cryptographic LSI (represented as ASIC in the figure) and on the FPGA mounted on the SASEBO-R and SASEBO-G, respectively. It is difficult to distinguish between the power traces of multiplication and squaring on either circuit for random input data. However, by providing the input with the particular value x=2^{-1024} that is effective for the attack against the 1,024-bit Montgomery multiplication algorithm adopted in the circuits, the results show the clear distinction between multiplication (M) and squaring (S).

(a) SASEBO-G (b) SASEBO-B



(c) SASEBO-R (d) SASEBO-GII

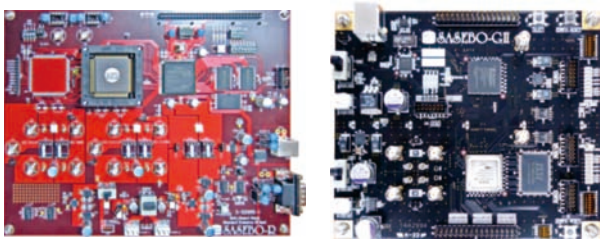


Fig. 3 SASEBO Board.

(a) 90-nm Version (b) 130-nm Version

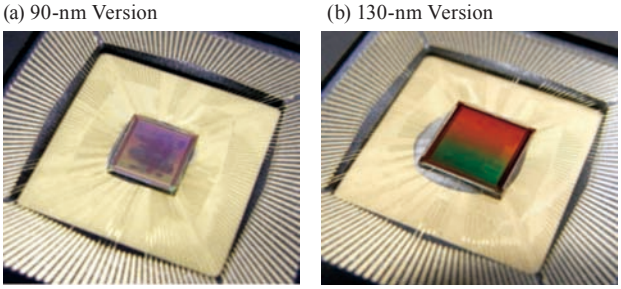


Fig. 4 Cryptographic LSI.

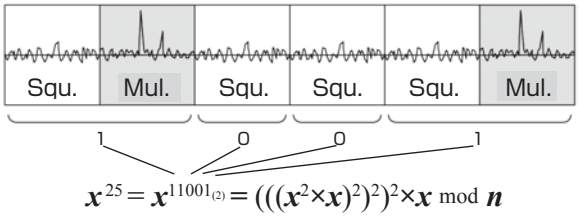


Fig. 5 SPA against RSA implemented with the left binary method.

(a) ASIC (b) FPGA

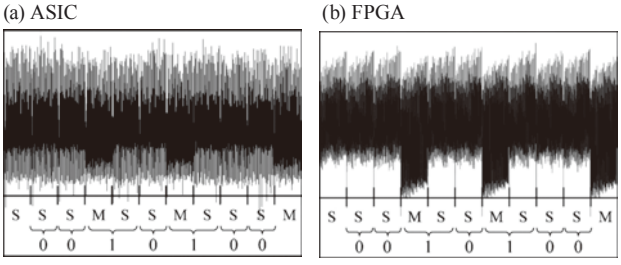


Fig. 6 SPA against RSA implemented on SASEBO-R and SASEBO-G (x=2^{-1024}).

The simplest and most basic SPA countermeasure for the RSA scheme is to insert a dummy multiplication operation after the squaring operation of every '0' appearing in the secret-key bit pattern. However, some other attack methods with input-data manipulation techniques, which can determine such a dummy multiplication, have been proposed. We are exploring the effectiveness of various attack methods and countermeasures through experiments with the SASEBO, and also attempting to find and develop new attack methods and countermeasures.

4.4 Differential power analysis on an AES cipher circuit

This section explains the AES algorithm, which is the standard symmetric-key cipher that is most widely used today, and demonstrates the Differential Power Analysis (DPA)[22] attack, which processes a multitude of power traces.

AES encrypts a 128-bit data block with a 128-, 192- or 256-bit key. Figure 7 illustrates the encryption algorithm with a 128-bit key. The 128-bit data is arranged into a 4 × 4 array of bytes to be processed in 10 rounds, each of which forms a round function and consists of four transforms: SubBytes, ShiftRows, MixColumns, and AddRoundKey, except for the last round excluding MixCoulumns. The 128-bit secret key will be transformed iteratively by a simple key scheduler into the 10 × 128 bits round keys to be provided to each round. Each of the round keys is used for the exclusive logical OR (XOR) with the corresponding data block in the AddRoundKey function. SubBytes is a collection of 16 S-boxes where the byte-wise non-linear transform for each byte of the 4 × 4 array is performed individually. In ShiftRows, the cyclic shift for each row of the 4 × 4 array is performed individually. MixColumns consists of 4 of the 4-byte linear transforms for each column.

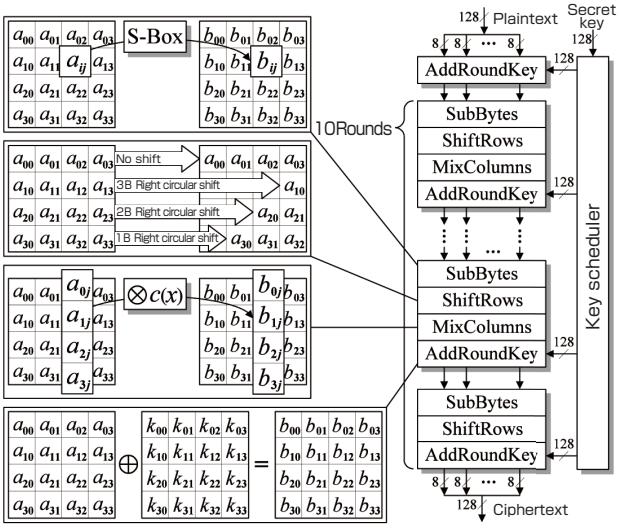


Fig. 7 The AES encryption algorithm.

A typical circuit implementation of AES employs a loop architecture that iteratively uses one round function for 10 times. Figure 8 shows the power traces measured for the AES circuits implemented on the cryptographic LSI and FPGA mounted on the SASEBO-R and SASEBO-G, respectively, indicating the saw-teeth shaped peeks corresponding to each round. Unlike an SPA case on the RSA scheme where the secret-key bit sequence reads on the power trace as a form of geometric pattern, the key cannot be extracted in that way for AES because all the 128 key bits are XORed in a moment and the difference contributed by each bit on the power trace is too small to read. By contrast, DPA is the key extraction scheme that applies a statistical technique to thousands of or tens of thousands of power traces. It builds a set of power models each based on a different partial key estimation, examines the correlation between each model and the power traces acquired for different input data, and determines the most probable partial key corresponding to the power model that indicates the highest correlation with the measured data. Since SubBytes is a byte-oriented transform, ShiftRows has shift operations along with the byte boundaries, and AddRoundKey is a bit-wise XOR, an individual operation at every byte will be performed at the last round, which skips MixColumns. Therefore, the 128-bit key can be analyzed at every byte. Because an eight-bit value has possible 256 combinations from 0 to 255, the estimation for an eight-bit partial key requires one to build and to examine as few as 256 power models. Accordingly, for the whole 128-bit key, only 16 individual analyses have to be done. During the analysis for an 8-bit part of the key, the power consumption component based on the operations for the other 120 bits behaves as noise. Note that, however, since a cryptographic circuit is considered to be a sort of random number generator, the power consumption of the unrelated part will be uncorrelated with the part being analyzed. That is, the influence of random noise components can be reduced by a statistical process on a number of power traces.

Figure 9 is a screen shot of the power analysis attack evaluation tool for AES circuits we developed. This instance is performing the CPA (Correlation Power Analysis)[25], focusing on the intermediate value register, with the power model based on the hypothesis that the power consumption will be proportional to the number of transitioning bits (Hamming distance) at the last round. The lower half of the

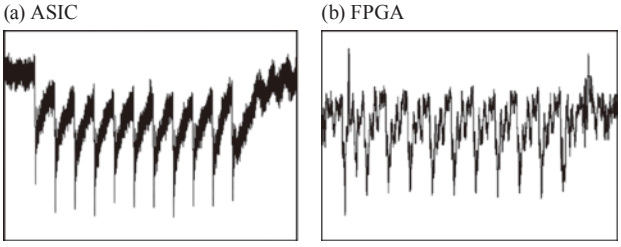


Fig. 8 Power traces for AES circuit.

figure shows the 16 partial key bytes represented as 16 boxes each with 256 vertical lines displayed in the box. The height of each line indicates the strength of the correlation between each model based on the partial key hypothesis ranging from 0 to 255 and the actual power consumption of the AES circuit. The tool determines the partial key hypothesis that indicates the highest correlation among the 256 candidates as the right partial key in each box. For a circuit without a countermeasure, it can extract the entire correct key in only a few minutes even with a cheap oscilloscope of around 200,000 yen to capture up to several thousands of power traces and with a low-end personal computer of as cheap as a few tens of thousands of yen.

As well as CPA, many other attack methods against AES have been emerging. In addition, more and more countermeasures have been proposed, too. We are pursuing verification of the effectiveness of those and have begun implementing them on our evaluation tool.

4.5 Development of more sophisticated attack methods and formulation of new evaluation guidelines

Along with the advancement of LSI analysis technology, research on security evaluation schemes for active attacks such as fault-injection attacks and invasive attacks is becoming more and more important. Examples of fault-injection attacks include, for an AES circuit with the loop architecture, the technique that induces a false operation in the circuit to pull out an intermediate value processed before the last round, and the technique that investigates how the error caused at a specified round propagates to the output. However, there is no guarantee of successful fault injection convenient for analysis. Even with a high success rate of triggering, the types of errors to be induced greatly depend on the circuit implementation. Furthermore, to publish experimental results, it is important that the cryptographic module can be attacked freely. Consequently, to conduct research on fault-injection attacks, use of a common experimental platform with a real cryptographic hardware module such as the SASEBO is necessary.

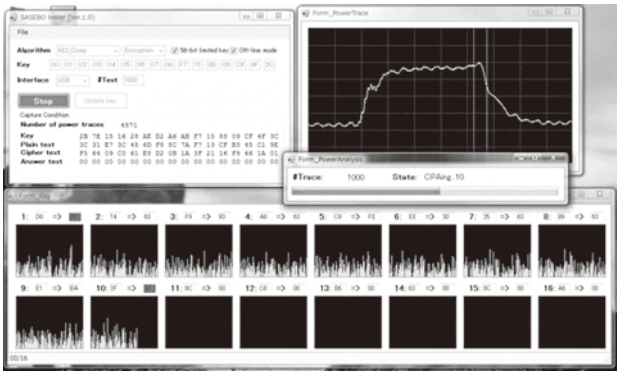


Fig. 9 AES circuit evaluation tool.

Invasive attacks are capable of observing not only the information buried in the total power consumption of an LSI, but also a local signal in the cryptographic circuit with such an LSI measuring system as shown in Fig. 10. However, such an existing system is not designed for an attacking purpose. Therefore, it is necessary to develop a system suitable to observe leaking information and sophisticated measurement technologies. We have seen that the quality of power traces and electromagnetic waveforms significantly influences the analysis results also in side-channel attack cases. Thus, we are also working on the development of new measurement technologies and the standardization of measurement environment.

Further, it is important not only to publish experimental results of successes or failures for each attack, but also to provide such security guidelines as criteria for designing tamper-resistant cryptographic modules against side-channel attacks through such experiments. This will require analysis of the mechanism of information leakage and in turn construct models that explain it qualitatively and quantitatively.

In developing cryptographic modules, perfect security is not necessarily required; rather, the implementer must consider the balance between the cost to implement countermeasures and the value of the protection. Conversely, from the attackers' point of view, the attacking costs should be worth the benefits. Even for standard cryptographic algorithms such as AES and RSA, brute force attacks would compromise them. Practical limitations of time and cost, however, do not allow successful searching in the entire key space. Thus, we will also be considering how to perform the security evaluation for cryptographic module implementations in the attacking cost aspect.

5 Conclusion

In this paper, we have discussed security evaluation for cryptographic module implementations, focusing on the side-channel attacks, and AIST's efforts toward the formulation of international standards and their significance. With the

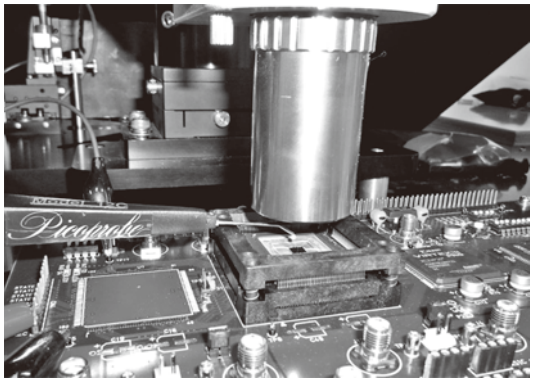


Fig. 10 Invasive attack on the cryptographic LSI on SASEBO-R.

cryptographic circuits implemented on the SASEBO boards developed as part of constructing a standard experimental platform, we showed that power analysis attacks successfully compromise such implementations, if they lack proper countermeasures, even with inexpensive measurement instruments, suggesting that urgent action is required. We also pointed out that it is necessary to immediately begin developing proper countermeasures and evaluation methods even for attacks requiring higher skills such as fault-injection attacks and invasive attacks.

Research on information security subjects including cryptography aim to construct protection measures against attackers with malicious intent. At the same time, as information systems are becoming more and more complex, the development of technology that prevents damage from incidental errors or faults is also in great demand. For example, although software bugs can be fixed on the running system even over the network, hardware bugs or faults not only require the system to halt, but also may take much time, in the case of a remote site, to be treated. To address this problem, the dynamic partial reconfiguration technology of FPGA, which enables altering a part of the logic circuit with the system operating, is offering a promising solution. The SASEBO-GII, the latest in the series, is equipped with functions that make possible research and development of dynamic partial reconfiguration, and has already begun driving research on applications of online circuit reconfiguration. Once it becomes possible to exchange hardware configuration information through the network, new threats including potential theft and falsification of such information, and hardware viruses involving a system failure may emerge. Therefore, these future pressing issues will also need to be addressed.

Our ultimate goal is to construct a *dependable information system* where highly-improved security and reliability of the entire hardware system are achieved following the fulfillment of the research on cryptographic hardware security. Toward this goal, we will pursue the research and development of the new hardware technology that will be in demand in the future.

References

[1] NIST, *Data Encryption Standard (DES)*, FIPS Publication, 46-3 (1999).
http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[2] R. L. Rivest, A. Shamir and L. Adleman: A method for obtaining digital signatures and public key cryptosystems, *Comm. ACM*, 21 (2), 120-126 (1978).

[3] NIST, *Advanced Encryption Standard (AES)*, FIPS Publication, 197 (2001).
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[4] NIST, AES home page
http://csrc.nist.gov/encryption/aes

[5] CRYPTREC (Cryptography Research and Evaluation Committees)
http://www.cryptrec.go.jp/english/index.html

[6] NESSIE (New European Scheme for Signatures, Integrity and Encryption)
https://www.cosic.esat.kuleuven.ac.be/nessie

[7] ISO/IEC 18033-1/-2/-3/-4, "Information technology – Security techniques – Encryption algorithms" Part 1: General / Part 2: Asymmetric ciphers / Part 3: Block ciphers / Part 4: Stream ciphers.

[8] ISO/IEC 15408-1/-2/-3, "Information technology – Security techniques – Evaluation criteria for IT security" Part 1: Introduction and general model / Part 2: Security functional requirements / Part 3: Security assurance requirements.

[9] Common Criteria – Common Criteria portal
http://www.commoncriteriaportal.org/

[10] ISO/IEC 19790:2006, "Information technology – Security techniques – Security requirements for cryptographic modules."

[11] Common Criteria Supporting Document: *Mandatory Technical Document – Application of Attack Potential to Smartcards*, 2.7 (1), (2009).
http://www.commoncriteriaportal.org/files/supdocs/CCDB-2009-03-001.pdf

[12] NIST, *Security Requirements for Cryptographic Modules*, FIPS Publication 140-2 (2001).
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[13] NIST, *Derived Test Requirements for FIPS* 140-2, Security Requirements for Cryptographic Modules (Draft), (2004).

[14] ISO/IEC 24759:2008, "Information technology – Security techniques – Security requirements for cryptographic modules."

[15] IPA, Japan Information Technology Security Evaluation and Certification Scheme (JISEC).
http://www.ipa.go.jp/security/jisec/jisec_e/index.html

[16] IPA, Japan Cryptographic Module Validation Program (JCMVP).
http://www.ipa.go.jp/security/english/jcmvp.html

[17] NIST, *Security Requirements for Cryptographic Modules*, FIPS Publication 140-3 (Draft), (2007).
http://csrc.nist.gov/publications/fips/fips140-3/fips1403Draft.pdf

[18] CHES (Cryptographic Hardware and Embedded Systems)
http://www.iacr.org/workshops/ches/

[19] AIST, Side-channel Attack Standard Evaluation Board (SASEBO).
http://www.rcis.aist.go.jp/special/SASEBO/index-en.html

[20] NIST, *DRAFT Security Requirements for Cryptographic Modules* (Revised Draft), (2009).
http://csrc.nist.gov/publications/drafts/fips140-3/revised-draft-fips140-3_PDF-zip_document-annexA-to-annexG.zip

[21] P. Kocher: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, *CRYPTO'96*, LNCS1109, 104-113 (1996).
http://www.cryptography.com/public/pdf/TimingAttacks.pdf

[22] P. Kocher, J. Jaffe and B. Jun: Differential Power Analysis, *CRYPTO'99*, LNCS1666, 388-397 (1999).
http://www.cryptography.com/public/pdf/DPA.pdf

[23] Aoki Laboratory, Tohoku University, Cryptographic Hardware Project.
http://www.aoki.ecei.tohoku.ac.jp/crypto/

[24] Tohoku University & AIST, Cryptographic Hardware Project, SASEBO-AES Cryptographic FPGA Board, Cryptographic Module Validation List, Cert. # F0003.
http://www.ipa.go.jp/security/jcmvp/jcmvp_e/val.html#F0003

[25] E. Brier, C. Clavier and F. Olivier: Correlation Power Analysis with a Leakage Model, *CHES 2004*, LNCS3156, 135-152 (2004).

Authors

Akashi Satoh

Received B.S. and M.S. degrees in electrical engineering from Waseda University, Tokyo, in 1987 and 1989, respectively. In 1989, joined IBM Research, Tokyo Research Laboratory, and was involved in the research and development of digital and analog VLSI circuits. Received a Ph.D. in electrical engineering from Waseda University, Tokyo in 1999. In 2007, joined the National Institute of Advanced Industrial Science and Technology, Research Center for Information Security. Current research interests include algorithms and architectures for data security and high-performance VLSI implementations. In this paper, managed the entire research project and also developed cryptographic hardware.

Toshihiro Katashita

Completed the doctoral program in Graduate School of Systems and Information Engineering, University of Tsukuba in 2006. In 2006, joined the National Institute of Advanced Industrial Science and Technology as a fixed-term researcher. In 2008, joined AIST as a tenure-track researcher. Involved in research projects on high-performance computation circuit design and on hardware security. In this paper, engaged in development of cryptographic software and hardware, and experiments of side-channel attacks.

Hirofumi Sakane

Completed the master's program in electronic engineering at the Graduate School of Electro-Communication, University of Electro-Communications in 1992. Subsequently joined Electrotechnical Laboratory. Initially studied parallel computer architecture. A senior researcher at AIST since 2001. Completed the doctoral program in information network at the Graduate School of Information Systems, University of Electro-Communications in 2001. Doctor of engineering. Currently works on safeness of implementations of cryptographic algorithms. In this paper, was engaged in standardization of security requirements for cryptographic modules in collaboration with NIST.

Discussions with Reviewers

1 Synthesiological descrption

Comment (Hideyuki Nakashima, Future University Hakodate)

Although the description of the synthesiological aspect of this research is rather weak, the paper is well written as a tutorial of the side-channel attack in cryptography, which is not necessarily widely perceived.

Comment (Masaaki Mochimaru, Digital Human Research Center, AIST)

The article is clearly written for non-specialists. The ideas of encryption, security evaluation, side-channel attack, and historical background, which are necessary items to understand this article, are well written. Note that this journal is about "synthesiology" as titled, intending to inform readers of synthesiological points of the authors' work. By following this concept more closely, and making such points clearer, the authors can make the article more informative of "the approaches and 'synthesiology' of the work" even to readers in different fields.

I think that how the AIST's action involved the stakeholders and synthesized them to achieve the goal would be central to "synthesiology". The authors might want to revise the article by elaborating how they changed the stakeholders and changed society to connect them to the goal.

Answer (Akashi Satoh)

We changed the last half of chapter 3 into "3.2 Formulation of international standard specification and expansion toward security evaluation business", wrote up a large part about AIST's activity in the section, and made the collaborations shown in Fig. 1 more obvious. The description of "Side-channel attack standard evaluation board (SASEBO)" was moved to section 4.2.