Electromagnetic Information Leakage from Cryptographic Devices

Naofumi Homma, Yu-ichi Hayashi, and Takafumi Aoki
Graduate School of Information Sciences, Tohoku University
homma@aoki.ecei.tohoku.ac.jp, yu-ichi@m.tohoku.ac.jp, aoki@ecei.tohoku.ac.jp

***Abstract*—This paper presents an overview of electromagnetic information security on cryptographic devices. The research area includes theoretical studies on information propagation via electromagnetic (EM) fields; acquisition, measurement, and analysis techniques for information leakage from information and communication devices via EM fields; modeling and simulation techniques for evaluation of EM information leakage; countermeasures against attacks based on EM information leakage; and intentional EM interference (IEMI) and electrostatic discharge (ESD) threats related to information leakage. In this paper, we briefly explain the fundamentals of EM information security: typical mechanisms of information leakage via EM fields, possible countermeasures, and ongoing standardization efforts.**

***Index Terms*—system security, electromagnetic information leakage, hardware attacks, cryptographic devices**

I. Introduction

With the advancements of technology and the spread of electronic devices, as well as the rapid expansion of communication network infrastructure, information leakage and communication disruptions associated with telecommunication devices (equipment and systems) have a strong impact on social and economic activities, and security technology that can ensure the security and reliability of such devices is becoming increasingly important. One of the main reasons for information leakage is unintentional radiation of electromagnetic (EM) fields from communication devices. Such radiation, referred to as "EM information leakage", can even be in the form of weak EM fields emitted from devices that are compliant with existing public standards (e.g., for ergonomic design and radio-frequency interference). This issue requires us to regard EM radiation as "a signal containing information" and to pursue new security assessment and evaluation metrics.

In particular, research interest in compromising emanations from cryptographic devices (electric devices with cryptographic modules implemented in software or hardware) has increased substantially since Kocher et al. [1][2] demonstrated the possibility of revealing secret keys from high-frequency current fluctuations in cryptographic devices. Such attacks on cryptographic devices are currently referred to as side-channel attacks [3]. In cryptographic research, as in [4], EM emanation is considered to be one of the sources of side-channel information obtained from cryptographic devices, and attacks using EM emanations are known as EM analysis attacks [5]–[8]. Such EM information leakage from cryptographic devices has been openly discussed since the beginning of the 2000s. In recent years, many experimental studies have been reported in addition to theoretical studies. Moreover, it has been reported that intentional electromagnetic interference (IEMI) could also compromise the security of ICT devices. Although previous studies of IEMI showed that devices can be permanently damaged or destroyed by the effects of IEMI, a recent study [9] showed that transient IEMI could be remotely injected into a cryptographic device via a power cable attached to the device without disrupting its function or damaging its components. Such temporal faults can be used for another type of side-channel attack known as fault analysis. A case study in which an Advanced Encryption Standard (AES) secret key could be extracted through fault analysis was shown in [9]. The above studies suggest that intensive research focusing on EM radiation from/to crypgoraphic devices should be conducted in order to complement conventional studies in the fields of cryptography and EMC.

For the introduction to suhc EM information leakage, this paper presents an overview of recent trends in research into EM analysis attacks on cryprographic devices, examples of typical attacks against the ISO/IEC standard ciphers, countermeasures, and related activities in the security evaluation of cryptographic devices.

II. The EM leakage process

This section presents an overview of the information leakage processes through EM radiation especially from cryptographic devices. During operation, any ICT device generates and emits radio signals encoding information as a result of the electrical switching processes in digital circuits, even if the emitted signal is suppressed in accordance with EMC standards. The intermediate or final result of the device operation can be obtained from such EM emission signal(s), typically by the following two methods.

A. Information leakage based on single observation

One method is based on the acquisition of one or several EM signal(s) emitted during a cryptographic operation. After acquisition, attackers attempt to extract secret key information directly from the EM trace. Although the method requires detailed knowledge about the implementation of the target device, it is feasible even if only one or a few traces are available.

Secret key information can be acquired directly from cryptographic devices by this method, in which case it is referred to as simple electromagnetic analysis (SEMA) [5],[6]. When

978-1-4673-4980-2/13/$31.00 ©2013 IEEE

ALGORITHM I

MODULAR EXPONENTIATION (LEFT-TO-RIGHT BINARY METHOD) FOR A k-BIT SECRET KEY.

Input:	X, N, $E = (e_{k-1}, ..., e_1, e_0)_2$
Output:	$Z = X^E \bmod N$

```
1 : Z := 1;
2 : for i = k − 1 downto 0
3 :     Z := Z * Z mod N;        – squaring
4 :     if (e_i = 1) then
5 :         Z := Z * X mod N;    – multiplication
6 :     end if
7 : end for
```

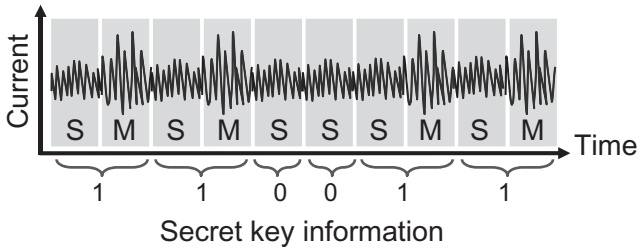


Fig. 1. Information leakage based on single observation.

a cryptographic device performs two operations (A and B) depending on a secret key, attackers identify the difference between the EM traces of A and B within a single execution step and subsequently estimate the secret key from the sequence pattern. In general, SEMA is suitable for public-key ciphers, which require a large number of computations for calculating each bit of the secret key. For example, the RSA cryptosystem [10], which is one of the most popular public-key ciphers, performs encryption and decryption by simple modular exponentiation. The typical exponentiation algorithm performs multiplication and squaring sequentially in accordance with the bit pattern of the exponent corresponding to the secret key such as in **ALGORITHM I**. Thus, the key bit pattern can be derived by the knowledge of the algorithm when the difference between multiplication and squaring operations appears in an EM trace. Figure 1 shows an image of the EM trace. Until now, some advanced analysis methods using chosen-message techniques have also been reported [11]–[13].

B. Information leakage based on multiple observations

The other acquisition method is based on the acquisition of a large number of EM traces during a target operation, followed by statistical analysis to reduce noise and retrieve secret information. This method is powerful in certain cases since it can be applied to ICT devices where the EM emissions are extremely low and noisy. In addition, attackers do not require detailed knowledge about the implementation of the target cryptographic device. This method is also known as differential electromagnetic analysis (DEMA) [6], which is another major type of side-channel attack on cryptographic devices.

Figure 2 shows the basic flow of DEMA (more precisely, correlation electromagnetic analysis (CEMA) [14]) In the typical scenario, the ciphertexts are known, and the plaintext

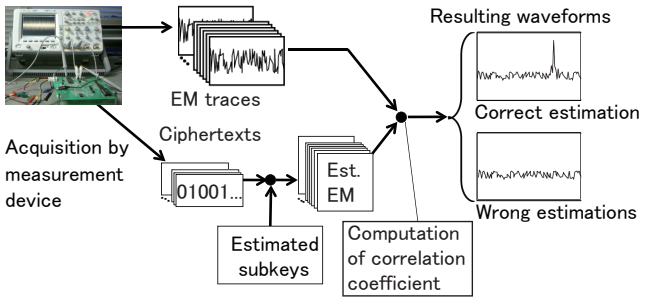


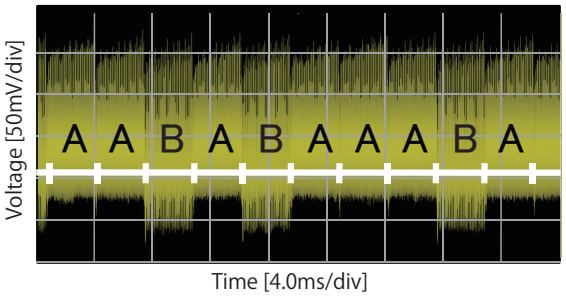
Fig. 2. Basic flow of information leakage based on multiple observations.

characters (i.e., messages) and the secret key are unknown to the attacker. The goal of the analysis is to recover the secret key. When a number of messages are encrypted, the attacker eavesdrops on the corresponding ciphertexts and acquires the corresponding EM traces at the same time. The attacker then assumes the value of a subkey and generates hypothetical EM values corresponding to the ciphertexts. Note here that there is a part of the encryption process determined by such a subkey (e.g., a 1-byte key) in modern ciphers. In the case of the 128-bit Advanced Encryption Standard (AES) [15] implementation, there are 16 S-boxes with a 1-byte input/output each, and each output is independently combined with the 1-byte subkey in the AddRoundKey operation. Therefore, the number of hypothetical EM values is at most 256 (=2^8). Lastly, the attacker calculates the correlation between the measured EM traces and the hypothetical EM values at an arbitrary time index and generates a correlation coefficient trace for each estimated sub key. If the estimation is correct, the attacker would find a high peak value anywhere in the generated trace.

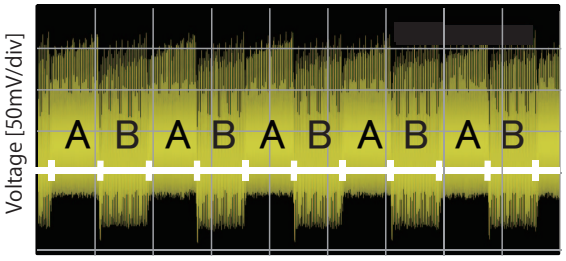
In contrast with SEMA, DEMA can be applied to symmetric block ciphers, such as AES and data encryption standard (DES) [16], where the EM emissions are much lower than in the case of public-key ciphers. Chosen-message power analysis has also been proposed as a means to expand the range of target algorithms [17][18].

III. COUNTERMEASURES

This section describes countermeasures together with some examples. Countermeasures against EM emanation from ICT devices are mainly classified into two types. The first type includes countermeasures applied to the EM emanation sources (e.g., LSI chips and devices) which process information that should be protected from leakage. The other type includes countermeasures applied to the paths (both source-antenna and antenna-receiver paths) from the source to the receiver. One or more countermeasures can be applied depending on the application and usage environment since there is no universal solution satisfying the criteria of both highest effectiveness and low implementation cost for any device. In this paper, we focus on countermeasure appliced to EM emanation soucres, which have been mainly discussed in the field of cryptographic research. Two types of the countermeasures, called hiding and masking, against EM analysis attacks have been reported until now [19].



(a) Without countermeasure.



(b) With countermeasure.

Fig. 3. Countermeasure preventing an attacker from deducing the specific pattern of A and B operations depending on the secret key.

Hiding is implemented by breaking the correspondence between the side-channel information (i.e., power consumption and EM radiation) and the processed data/operations. A typical countermeasure of the hiding type against EM analysis attacks is to change the algorithm and/or circuit of the cryptographic module in order to obtain constant EM radiation regardless of the processed data. Figure 3 presents the concept of a hiding-type countermeasure. In Fig. fig3(a), we assume that operations "A" and "B" are performed in accordance with the bit pattern of a secret key. We can reveal the secret key from the pattern in Fig. 3(a) because without a countermeasure the EM trace of A is different from that of B. In contrast, with a countermeasure (inserting a dummy B operation after each A operation) results in the EM trace shown in Figure 3(b), performing both A and B operations for each bit. This countermeasure prevents an attacker from deducing the specific pattern of A and B operations depending on the secret key.

In comparison, masking is performed by randomizing the intermediate data processed in the module. In particular, message masking is essential for preventing the application of chosen-message techniques. The effectiveness of this countermeasure depends on the size and the frequency of updating the mask value (a random number). To achieve higher level of security, the mask value should be sufficiently large and should be generated randomly for each encryption process.

These countermeasures have been proposed mainly at the algorithm, architecture, and circuit levels. Whereas countermeasures at the algorithm level [20]–[22] can be implemented easily, they are also potentially prone to newly developed algorithmic attacks [12][23]. On the other hand, countermeasures at the circuit level can provide a general-purpose solution at the

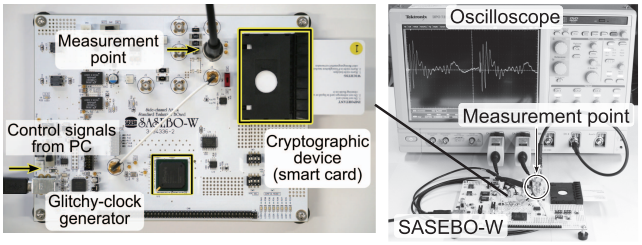


Fig. 4. Overview of SASEBO-W and its experimental setup.

expense of the difficulty of designing such measures. In this regard, random switching logic (RSL) [24] and wave dynamic differential logic (WDDL) [25] are well-known as typical countermeasures for masking and hiding, respectively. RSL uses random data to mask the transition probabilities of inputs and outputs, whereas WDDL is an extended version of the sense amplifier based logic (SABL) [26] and successfully balances circuit activity by using complementary logic gates and a precharge phase. Note that both countermeasures must be carefully designed to achieve the completely-masked/hidden values.

IV. Standardization works

This section introduces work on standardization associated with risk evaluation and countermeasures used in EM information security.

There is ongoing effort to standardize the requirements that should be satisfied by cryptographic modules with respect to side-channel attacks on cryptographic modules. International Standard ISO/IEC 15408 (known as Common Criteria) [27] is a standard for evaluating whether IT-related products or systems are properly designed and correctly implemented. Note that the security target is defined by each developer, although all IT-related products are covered by the Common Criteria. In contrast, there is another specific standard for evaluating cryptographic modules. Currently, both FIPS 140-2, issued by the National Institute of Standards and Technology (NIST) [28], and ISO/IEC 19790 [29] serve as security evaluation standards for cryptographic modules, which cover 11 points related to the design and implementation of cryptographic modules. ISO/IEC 24759 [30] provides the derived test requirements for ISO/IEC 19790 [29]. However, since these standards do not include detailed technical descriptions related to side-channel attacks, they are currently undergoing revision.

In order to contribute to the above standardization process, a uniform testing environment based on SASEBO (Side-channel Attack Standard Evaluation BOard) has been developed and distributed together with detailed design information to many research institutes [31][32]. There are six SASEBO variants (SASEBO and SASEBO-G/-GII/-B/-R/-W), each of which is suitable for implementing experimental cryptographic modules and performing various analyses. Figure 4 shows an overview of SASEBO and its experimental setup. SASEBO and SASBO-G/-GII are equipped with Xilinx FPGAs, SASEBO-B is equipped with ALTERA FPGA, SASEBO-R is equipped with a custom ASIC, and SASEBO-W is equipped with a smartcard interface for the cryptographic

implementation. The FPGAs include some processor cores available for software implementations. Each SASEBO variant also employs a second FPGA for communicating with a host computer through RS-232 and/or USB cables. Various experiments associated with side-channel attacks are being conducted on SASEBO, and many useful results are expected in support of the international standardization efforts [31].

V. Conclusion

This paper introduced the overview of EM information security problems tackled in recent studies. Topics in this research area include theoretical studies on information propagation via EM fields; acquisition, measurement, and analysis techniques for information leakage from information and communication devices via EM fields; modeling and simulation techniques for evaluation of EM information leakage; countermeasures against attacks based on EM information leakage; and IEMI and ESD threats related to information leakage, which are not covered by the conventional standards. In this paper, we focus on the fundamentals of EM information leakage from cryptographic devices, such as typical mechanisms of information leakage via EM fields, possible countermeasures, and ongoing standardization efforts.

VI. Acknowledgment

This research was supported by Strategic International Cooperative Program (Joint Research Type), Japan Science and Technology Agency.

References

[1] P. Kocher, “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems,” CRYPTO 1996, Lecture Notes in Computer Science, vol. 1109, pp. 104-113, 1996.

[2] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” CRYPTO 1999, Lecture Notes in Computer Science, vol. 1666, pp. 388-397, 1999.

[3] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, “Side Channel Cryptanalysis of Product Ciphers,” Journal of Computer Security, v. 8, n. 2-3, 2000, pp. 141-158.

[4] C. K. Koc, “Cryptographic Engineering,” Springer, 2009. ISBN 978-0-387-71816-3

[5] K. Gandolfi, C. Mourtel, and F. Olivier, “Electromagnetic analysis: Concrete results,” CHES 2001, Lecture Notes in Computer Science, vol. 2162, pp. 251-261, 2001.

[6] J. Quisquater and D. Samyde, “Electromagnetic analysis (EMA): Measures and counter-measures for smart cards,” E-Smart 2001, Lecture Notes in Computer Science, no. 2140, pp. 200-210, Sep. 2001.

[7] E. Peeters, X. Standaert, and J. Quisquater, “Power and electromagnetic analysis: Improved model, consequences and comparisons,” Integration, the VLSI journal, vol. 40, no. 1, pp. 52-60, 2007.

[8] D. Agrawal, , B. Archambeault, R. Rao, and P. Rohatgi, “The EM Side-channel(s),” CHES 2002, Lecture Notes in Computer Science, vol. 2523, pp. 29-45, Aug. 2002.

[9] Y. Hayashi, N. Homma, T. Sugawara, T. Mizuki, T. Aoki and H. Sone, ”Non-Invasive EMI-Based Fault Injection Attack against Cryptographic Modules,” IEEE International Symposium on Electromagnetic Compatibility, pp. 763-767, 2011.

[10] R.L. Rivest, A. Shamir, L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM 21, pp. 120-126, 1978.

[11] R. Novak, “SPA-based adaptive chosen-ciphertext attack on RSA implementation,” PKC 2002, Lecture Notes in Computer Science, vol. 2274, pp. 252-262, Feb. 2002.

[12] A. P. Fouque and F. Valette, “The doubling attack -why upwards is better than downwards,” CHES 2003, Lecture Notes in Computer Science, vol. 2779, pp. 269-280, Sep. 2003.

[13] A. Miyamoto, N. Homma, T. Aoki, and A. Satoh, “Chosen-message SPA attacks against FPGA-based RSA hardware implementations,” Proc. 2008 Int. Conf. on Field Programmable Logic and Applications, pp. 35-40, Sep. 2008.

[14] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model,” CHES 2004, Lecture Notes in Computer Science, vol. 3156, pp. 16-29, Aug. 2004.

[15] National Institute of Standards and Technology (NIST), “Advanced Encryption Standard (AES) FIPS PUB. 197,” http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, Nov. 2001.

[16] National Institute of Standards and Technology (NIST), “DATA ENCRYPTION STANDARD (DES) FIPS PUB. 46-3,” http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[17] K. Schramm, G. Leander, P. Felke, and C. Paar, “A collision-attack on AES combining side-channel and differential-attack,” CHES 2004, Lecture Notes in Computer Science, no. 3156, pp. 163-175, Aug. 2004.

[18] J. Jaffe, “More differential power analysis: Selected dpa attacks,” Presented at the Summer School on Cryptographic Hardware, Side-Channel and Fault Attacks, Jun. 2006.

[19] S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks - Revealing the Secrets of Smart Cards. Springer, 2007. R. Novak, “SPA-based adaptive chosen-ciphertext attack on RSA implementation,” PKC 2002, Lecture Notes in Computer Science, vol. 2274, pp. 252-262, Feb. 2002.

[20] J. S. Coron, “Resistance against differential power analysis for elliptic curve cryptosystems,” CHES 1999, Lecture Notes in Computer Science, vol. 1717, pp. 192-302, Aug. 1999.

[21] S. M. Yen and M. Joye, “Checking before output may not be enough against fault-based cryptanalysis,” IEEE Trans. Comput., vol. 49, no. 9, pp. 967-970, Sep. 2000.

[22] M. Joye and S. M. Yen, “The montgomery powering ladder,” CHES 2002, Lecture Notes in Computer Science, vol. 2523, pp. 291-302, Aug. 2002.

[23] N. Homma, A. Miyamoto, T. Aoki, A. Satoh, and A. Shamir, “Collisionbased power analysis of modular exponentiation using chosen-messagepairs,” CHES 2008, Lecture Notes in Computer Science, vol. 5154, pp. 15-29, Aug. 2008.

[24] D. Suzuki, M. Saeki, and T. Ichikawa, “Random switching logic: A new countermeasure against DPA and second-order DPA at the logic level,” IEICE Trans. Fundamentals., vol. E90-A, no. 1, pp. 160-168, Jan. 2007.

[25] K. Tiri, D. Hwang, A. Hodjat, B.C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, “Prototype IC with WDDL and differential routing - DPA resistance assessment,” CHES 2005, Lecture Notes in Computer Science, vol. 3659, pp. 354-365, May 2005.

[26] K. Tiri, M. Akmal, and I. Verbauwhede, “A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards,” Proc. of the 28th European Solid-State Circuits Conference, pp. 403-406, Sep. 2002.

[27] International Organization for Standardization (ISO) and INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC), “ISO/IEC 15408-1: Common Criteria for Information Technology Security Evaluation,” 2005.

[28] National Institute of Standards and Technology (NIST), “Security Requirements for Cryptographic Modules,” FIPS Publication 140-2, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[29] International Organization for Standardization (ISO) and INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC), “ISO/IEC 19790: Information technology - Security techniques - Security requirements for cryptographic modules,” 2006.

[30] International Organization for Standardization (ISO) and INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC), “ISO/IEC 24759 Information technology - Security techniques - Test requirements for cryptographic modules,” 2008.

[31] Side-channel Attack Standard Evaluation Board, http://www.rcis.aist.go.jp/special/SASEBO/, 2007

[32] Cryptographic Hardware Project, Computer Structures Laboratory, Tohoku University. http://www.aoki.ecei.tohoku.ac.jp/crypto/, 2007