Analysis of EM Emission from Cryptographic Devices

Hideaki Sone[1], Yu-ichi Hayashi[2], and Takaaki Mizuki

[1]Tohoku University Cyberscience Center, Aramaki Aoba 6-3, Aoba-ku, Sendai 980-8578, Japan
[2]Graduate School of Information Sciences, Tohoku University, Aramaki Aoba 6-3-09, Aoba-ku Sendai, 980-8579
sone@isc.tohoku.ac.jp, yu-ichi@m.tohoku.ac.jp, mizuki@isc.tohoku.ac.jp

Abstract

Electromagnetic information leakage is an attack against secret information in an information-processing circuit, and realized by observing electromagnetic radiation around the circuit. When a cryptographic module works, electrical fluctuation in it can be conducted to peripheral circuits by ground bounce, resulting in electromagnetic radiation. The authors demonstrate the mechanism through experiments with an FPGA board which processes the standard cipher AES (Advanced Encryption Standard). Measurement of electromagnetic radiation from a power cable showed that correlation electromagnetic analysis (CEMA) reveals the secret keys. The leakage is possible even if voltage regulators are placed as a disturbing factor between the module and the measurement points. Circuit-level countermeasures against CEMA are also discussed, and an information suppression technique is proposed by the authors.

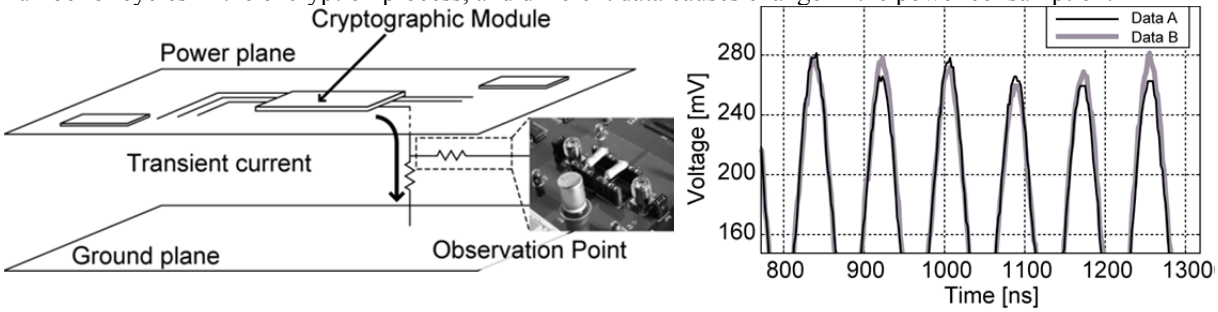
1. Introduction

The electromagnetic information leakage is an attack against secret information in an information-processing system such as a smartcard or an embedded cryptosystem, and realized by observing electromagnetic radiation around the system. When a cryptographic module operates, electrical fluctuation in it can be conducted to peripheral circuits by ground bounce. Such transient current and near-field radiation can act as side-channel information for cryptanalysis which reveals secret key information stored in the module.

Researches on the side-channel attacks mainly focus on algorithms and implementation at both hardware and software levels [1, 2]. The power-analysis attack is usually conducted for cryptographic modules where an attacker can easily obtain side-channel information. The power consumption of a module is observed as current waveform by use of a small resistor inserted on a power pin [1]. Electromagnetic analysis (EMA) attacks, which measure electromagnetic fields around the cryptographic modules, have also been proposed [3]. These attacks assume close access to the modules so far, but feasibility of such observation is not discussed well. This paper demonstrates the possibility of EMA attacks at a distance from a cryptographic module. The authors focus on common-mode current, which is studied extensively in the EMC field, as the main source of information leakage. The feasibility of an EMA attack is experimentally examined using common-mode currents on a power cable.

2. Power Analysis Attack for Common-mode Current

Figure 1 shows a cryptographic module on the Side-channel Attack Standard Evaluation Board (SASEBO) and observed waveforms. The standard block cipher Advanced Encryption Standard (AES) module processes one encryption with 10 clock cycles. A part of the waveform shows six peaks which correspond to the same number of cycles in the encryption process, and different data causes change in the power consumption.



(1) Observation of current waveform **(2) Observed waveforms**

Fig. 1: Measurement of transient current from cryptographic module

The authors carried out measurement of common-mode current from outside the SASEBO board and analyzed possibility to extract a secret key from the side-channel information. The measurement conditions are given in Table 1 and Fig. 2. A hardware intellectual property (IP) [4] is used for AES implementation in this measurement. Waveform acquisition and analysis are conducted as follows: We use the standard test vector that

978-1-4673-5225-3/14/$31.00 ©2014 IEEE

appears in the AES specification [5] as the secret key to be stored. Sequences of 30,000 numbers are used as plaintexts, and their corresponding 30,000 waveforms are captured. The acquired waveforms are aligned with a trigger signal generated by the AES circuit. Neither averaging nor filtering is applied during the acquisition. A power model based on the Hamming distance [2] of resistor transition is used as a selection function to analyze the AES circuit, where linearity between power consumption (amplitude of the waveform) and Hamming distance is evaluated by using Pearson's correlation coefficient [2].

Table 1: Measurement parameters

	(i) Resistor	(ii) Power cable
Environment	SASEBO	
Algorithm	AES (128bit)	
Operation frequency	12 MHz	
Oscilloscope	Agilent MSO6104A	
Selection function	Hamming Distance	
Number of acquired waveforms	30,000	
Measurement point	Resistor attached to FPGA GND	Twisted cable attached to Power supply
Probe	Agilent 1130A with SMA probe head	Fischer F-2000

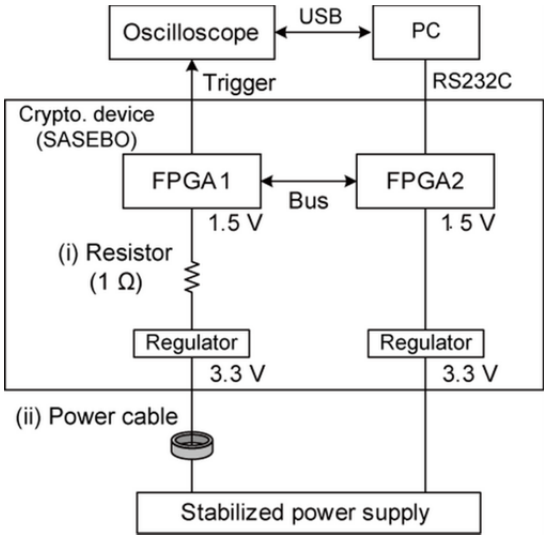


Fig. 2: Experimental setup

We adopted correlation power analysis (CPA) [6], a power analysis method, for the analysis of secret key information. Common-mode current is observed as side-channel information on a power cable ((ii) in Fig. 2) as well as transient currents near the cryptographic module ((i) in Fig. 2) as a comparative reference. The upper waveform of Fig. 3 is transient current given by a voltage drop across a 1-Ω resistor inserted between the ground pin of FPGA1 and the ground plane of the PCB, and is measured by a differential voltage probe. The lower waveform of Fig. 3 is common-mode current given by currents flowing in a regulator, and is measured by a current probe clamped to the cables.

Figure 4 shows result of extraction of secret key information. In this Figure, measurement-to-disclosure (MTD) shows how many waveforms are required to distinguish between correct and wrong estimates. In the case of a correct estimate, the correlation between a correct estimate and side-channel information is higher than the cases of wrong estimates. When the number of waveforms used for analysis increases, correlation values of correct and wrong estimations are clearly distinguished. For correct estimations, correlations using common-mode currents as a side channel on the power cable ((ii) in Fig. 2) is lower than the correlation using transient currents at the resistor ((i) in Fig. 2). In addition, the convergence speed of the correlation value to the analysis of common-mode currents is slower than the value of the analysis of transient currents.

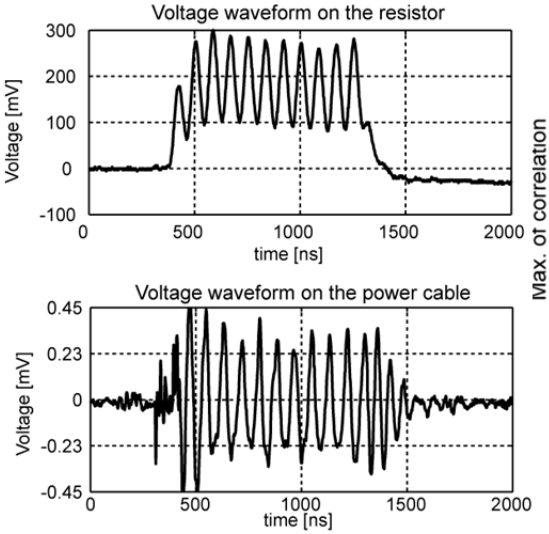


Fig. 3: Observation waveforms at each measurement point.

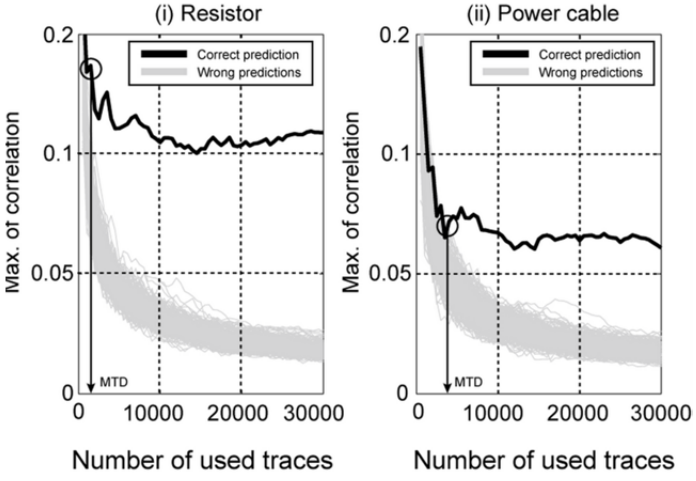


Fig. 4: Correlation profiles for CPA.

To distinguish between correct and wrong estimates, the case of common-mode currents requires about 4000 waveforms, about 3000 more waveforms than in the case of transient currents. This is why the SNR on analysis of common-mode currents is lower than that of the analysis of transient currents. This result shows that, while analysis of common-mode currents requires more waveforms than does analysis of transient currents, secret key information can be extracted using common-mode currents, which are side channels available outside of the cryptographic hardware.

3. Discussion

In Section 2, we demonstrated that a secret key can be extracted by using common-mode currents as a side channel outside of cryptographic hardware. The above results suggest that common-mode currents on attached cables have a definite possibility of CPA attacks, even on different block-cipher modules at different locations due to the following reasons. First, the AES core architecture is a common architecture used for hardware implementation, and other modern block ciphers can also be implemented with the same architecture, whose electromagnetic leakage level seems to be comparable with that of the AES core. Previous studies have further reported that common-mode current is a major factor of electromagnetic radiation from electronic devices, and that it causes radiation via antennas such as cables attached to the PCB board [7, 8]. In this sense, our demonstration of a CPA attack via common-mode current is meaningful.

The attack becomes infeasible when the SNR decreases significantly, but this condition is heavily dependent on the environment. A natural assumption is that availability of the leaked information decreases depending on the distance. However, it was reported in [2] that information availability depends not on the distance but on the SNR. For example, when a change happens in the FPGA clock frequency the curve would change with the resulting SNR, depending on the experimental environment.

Possible and effective countermeasures can be given from the perspectives of EMC. Common-mode currents outside a board are represented by electromagnetic interference (EMI) model [8]. The strength of EMI is represented by the product of three factors. “Source” is an output voltage of a large-scale integration (LSI) for actual electronics devices, “Path” refers to radiative coupling path between signal and noise, “Antenna” determines frequency characteristics of a noise emission (Fig. 5). This model implies that we can counteract EMA attacks by suppressing each of the factors and apply noise reduction techniques used in EMC.

One of the popular noise reduction techniques for EMC is the use of bypass capacitors. Voltage fluctuation can be suppressed by placing capacitors close to the pins of the cryptographic chip. This method is regarded as noise reduction in the source element. Another typical technique is to attach a ferrite core on the cables. This method is also widely used to suppress radiation from cables and is equivalent to noise reduction in the antenna element. Note however that such noise reduction techniques should be applied carefully. First, noise propagation is robust as we observed in the experiments in Section 2. Second, noise reduction should be applied within the security boundary so that attackers won’t remove it. Finally, frequency band containing information leakage should be investigated because a noise reduction usually suppresses a specific frequency band selectively. We assume that the frequency band is fairly low compared with those usually considered in the field of EMC research.

The above results suggest that the information acquisition can be prevented when only the signal (i.e., information) is suppressed. Suppression of noise would cause more information leakage. Thus, in addition to suppressing information leakage source, decreasing the SNR would be required.

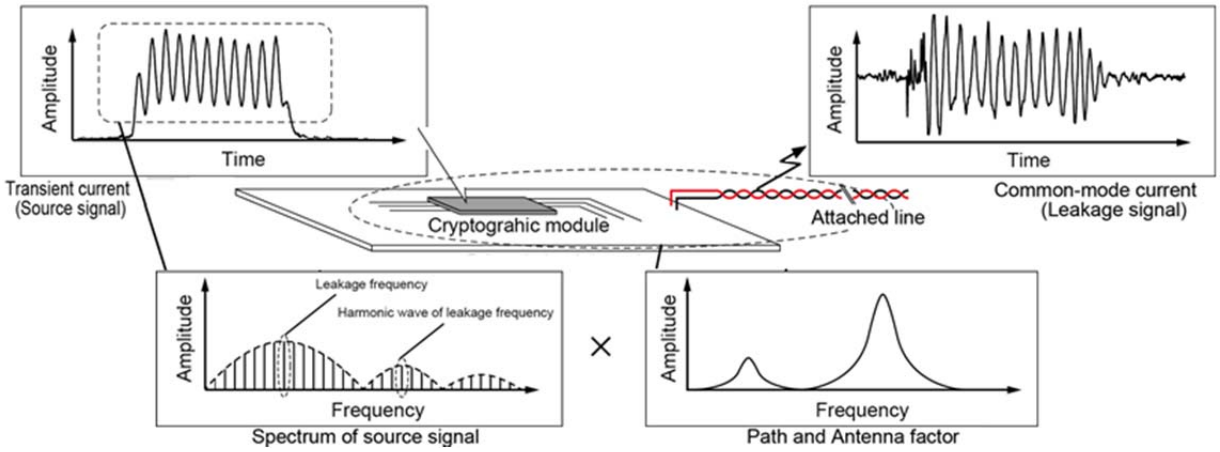


Fig.5 Leakage model from cryptographic model.

4. Conclusion

This paper investigated where and how we can obtain EM waveforms that are available for side-channel attacks from the EMC point of view. In particular, we pointed out the possibility of information leakage via common-mode current at a distance from cryptographic modules. Our result demonstrated that secret key information was leaked via common-mode current on a power cable attached to an FPGA board where an AES circuit is implemented.

Electronic devices are usually designed to satisfy EMC standards, such as those published by CISPR (the International Special Committee on Radio Interference), FCC (the U.S. Federal Communications Commission), or VCCI (the Voluntary Control Council for Information Technology Equipment). However, these standards mainly aim to suppress and reduce EM radiation that disturbs other devices, and are not aware of radiation that might leak secret information. Even if the common-mode current is below a limit in the guidelines, it might be possible to extract secret key information by acquiring side-channel information, given adequate time. To provide a secure and safe environment for information communication, it would be necessary to pinpoint and reduce specific EM radiation related to information leakage. The presented experiments provided a fundamental study of EM information leakage from various cryptographic devices, ranging from smartcards to security servers. Further analysis of actual devices with different sources, paths, and antennas, as well as more sophisticated evaluation methods, is left for future studies.

5. Acknowledgments

This work was supported by JSPS KAKENHI Grant Number 25289068.

The authors express their thanks to Professor Takafumi Aoki and Associate Professor Naofumi Homma of Tohoku University for their collaboration in carrying out the researches related to the Side-channel Attack Standard Evaluation Board (SASEBO).

6. References

1. P.C.Kocher, J.Jaffe and B.Jun, “Differential power analysis,” *Proc. CRYPTO, Lecture Notes in Computer Science*, **1666**, Springer, pp. 388-397, 1999.

2. S.Mangard, E.Oswald, T.Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

3. K.Grandolfi, C.Mourtel, and F.Olivier, “Electromagnetic Analysis: Concrete Results,” *CHES 2001, Lecture Notes in Computer Science* , **2162**, pp. 251-261, 2001.

4. Cryptographic Hardware Project, IP Cores, http://www.aoki.ecei.tohoku.ac.jp/crypto.

5. NIST FIPS PUB. 197, Advanced encryption standard (AES), http://csrc.nist.gov/publications/fips/fips197.

6. E.Brier, C.Clavier and F.Olivier, “Correlation power analysis with a leakage model,” *Proc. CHES 2004, Lecture Notes in Computer Science*, **3156**, Springer, pp. 16-29, 2004.

7. CR. Paul, *Introduction to electromagnetic compatibility*, John Wiley & Sons; 1997.

8. D.Hockanson, J.Drewniak, T.Hu bing, T.Van Doren, F.Sha and M.Wilhelm, “Investigation of fundamental EMI source mechanisms driving common-mode radiation from printed circuit boards with attached cables,” *IEEE Trans. on Electromagnetic Compatibility*, **38**(4), pp. 557-566, 1996.