Efficient Method for Estimating Propagation Area of Information Leakage via EM Field

Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, and Hideaki Sone

Tohoku University
6-6-3 Aramaki Aza, Sendai 980-8579, Japan
yu-ichi@m.tains.tohoku.ac.jp

Abstract—**Information leakage via electromagnetic (EM) radiation is an emerging issue for designers and users of electrical information devices. The importance of estimating the propagation area of information leakage is increasing due to the high demand for protecting such devices from eavesdroppers. We propose an efficient method for estimating the propagation area of information leakage via an EM field. The idea behind the method is to exploit the temporal variance of noise at the area of interest in addition to the source intensity and the transfer function. We show that the values of information acquisition estimated by our method are in good agreement with actual information acquisition as measured in the EM field at an area of interest.**

I. Introduction

Implementation attacks against cryptographic devices using side-channel information, such as timing, power consumption, and electromagnetic (EM) radiation, are a major issue for designers of such devices. An EM analysis attack obtains intermediate data via EM radiation from the target device during encryption/decryption operations, and reveals secret information correlated to the obtained data by signal processing and statistical techniques. A major feature of EM analysis attacks is that EM waveforms are obtained by noncontact probing.

Conventional attacks are performed very close to the target device in order to measure EM waveforms. The use of near-field probing makes it easier to obtain detailed information about an unpacked 8-bit microcontroller from its EM radiation. In general, semi-invasive side-channel attacks are effective because plastic mold package devices can be accessed easily at low cost. Previous studies [1]–[4] have shown a definite possibility of obtaining secret keys from EM radiation measured outside of cryptographic devices. In particular, successful EM analysis of an SSL accelerator was carried out in [2] by measuring the accelerator's radiation. This suggests that we need to consider the threat of EM analysis attacks even without close access to the device. These types of attacks are an emerging issue for designers and users of cryptographic devices.

To protect cryptographic devices from such attacks, pinpointing the source, path, and antenna of EM information leakage and the frequency band including the significant information is essential. In addition to countermeasures suppressing EM radiation, preventing attackers from accessing the information propagation area is required as an alternative countermeasure. To implement countermeasures in an efficient manner, we need to correctly estimate the propagation area of information leakage via the EM field. Previous studies [5][6] have reported that the intensity of information leakage is dependent on not the intensity of EM radiation but the signal-to-noise ratio (SNR), assuming that EM radiation could be interpreted as a signal encoding secret information. However, it is not practical to use such greedy methods for evaluating the SNR at all possible measurement points by actual EM analysis, since analysis requires an hour or more to calculate the SNR, even when using a high-end PC.

To address this issue, we present an efficient method for estimating the propagation area of information leakage via EM field. The basic idea is to exploit a transfer function from the source of information leakage to the area of interest with the time variances of noise. We demonstrate the validity of the proposed method through an experiment using Advanced Encryption Standard (AES) implemented on an evaluation board. We confirm that the estimated value is in fair agreement with the value obtained from actual EM analysis.

II. Proposed Method

This section presents our concept for estimating the probability of information acquisition from EM radiation.

When EM radiation from an electrical device (called the "source" [7]) is evaluated, the EM radiation is measured in a low-noise environment such as an anechoic chamber, shielded room, or quiet site, based on a test method defined by a standards committee such as the U.S. Federal Communications Commission or the Comité International Spécial des Perturbations Radioélectriques. This estimates just the radiation that causes interference in other electrical devices (the "victims" [7]) from the device under test. Through this evaluation, EMC countermeasures are applied to the electrical device if its radiation exceeds regulation levels. In such a case, the estimation of EM field propagation from the source to the victim is given by the product of a source spectrum $S(f)$ and a transfer function $H(f)$. Note that the transfer function is the attenuation factor of the EM field from the source to the victim at frequency f.

When EM radiation including information from an electrical device is evaluated, EM fields and the ambient noise level in the area of interest should be measured, because the feasibility of an EM analysis attack is heavily dependent on the SNR [5][6]. Therefore, to estimate the probability of information acquisition, the EM field including information reaches the observation point is given by:

$$M(f) = S(f) \cdot H(f) + N(f) \quad (1)$$

Here, $N(f)$ is background noise, including that radiated by other electronic devices in an area of interest. Also, as the probability is mainly determined by time variances of the signal and noise, not their spectra, information leakage is generally evaluated in the time domain. We therefore convert frequency-domain Eq. (1) to the following time-domain equation by Laplace transform.

$$m(t) = s(t) * h(t) + n(t) \quad (2)$$

Thus, at the area of interest, the measured EM radiation $m(t)$ is composed of (i) EM radiation at the source point (over a cryptographic module), $s(t)$; (ii) a transfer function from the source to the area of interest, $h(t)$; and (iii) noise at the area of interest, $n(t)$.

Our method estimates the intensity of information leakage by Eq. (2), considering the time variance of noise at the area of interest. One straightforward way of obtaining noise data is to measure noise at the area of interest during each encryption operation. Such measurements are time-consuming, however, and environmental noise seems to have a constant variance under the assumption that there is no specific electronic device radiating a significant EM wave near the target device. This assumption makes our method more efficient. Actual measurement results are shown in the following experiment.

III. Experiment

To validate our experimental environment we first compare the results of information acquisition between actual measurements and estimations based on Eq. (2). An EM field is radiated from the physical structure of an electrical device behaving as an antenna [8]–[12]. To clarify the antenna structure, we observe EM radiation from a loop antenna. To change transfer functions, we change distances between the transmitting and receiving antennas.

A. Experimental Conditions

We first extract the leakage signal from a Side-channel Attack Standard Evaluation Board (SASEBO) [13]. We implemented an AES hardware module on the FPGA1 chip, and extracted its transient current during encryption. AES is an ISO/IEC 18033-3 block cipher [14], and the AES hardware module is referred to as a standard module, performing one encryption operation in 11 cycles. The extraction signal is applied to the transmitting antenna (ETS Passive Loop

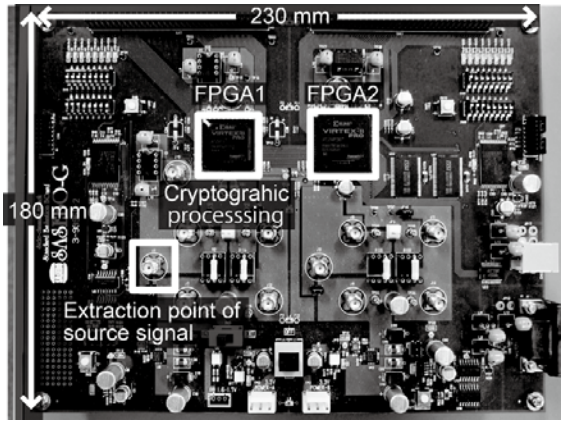
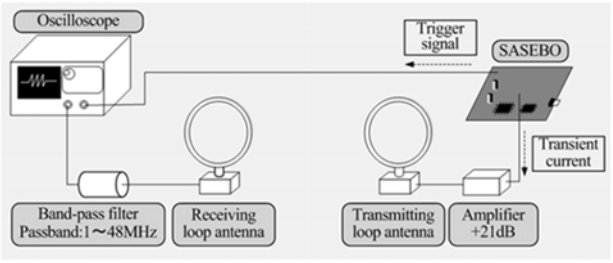
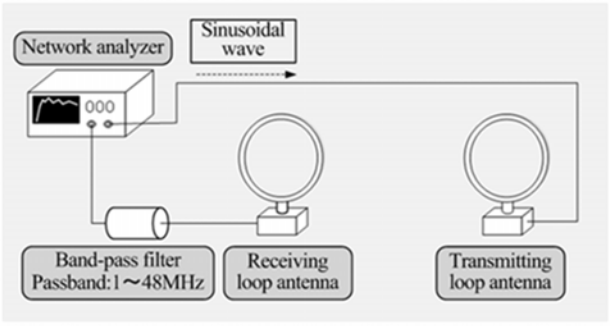


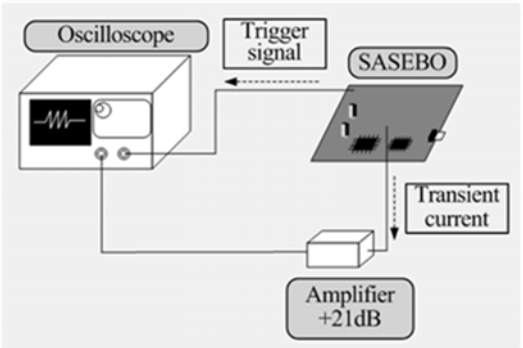
Fig. 1: Cryptographic device.



(a) Measurement environment of EM radiation and noise.



(b) Measurement environment of transfer function.



(c) Measurement environment of source signal.

Fig. 2: Experimental setup.

Antenna 6505). EM fields are filtered using a bandpass filter (Mini-Circuits SLP-50+, 0–48 MHz), and then measured using an oscilloscope (Agilent MSO 6104A) at 4 GSamples/s with a loop antenna (ETS active receiving loop antenna 6507). We measure the EM fields as temporal traces, since EM attacks usually analyze such EM fields in the time domain. The measured EM traces are stored in a PC through the oscilloscope.

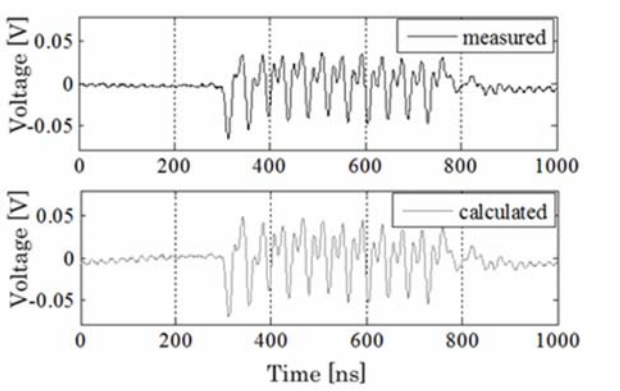
Assuming different estimation points of information leakage, we changed the distance between the antennas to 100, 200, and 300 cm, distances that are clearly in the transfer function. When the distance is changed, the EM field is observed by the active receiving loop antenna, and the experimentally observed EM fields are compared with the estimated EM field in each condition by using Eq. (2).

To estimate the EM field as a leakage signal, the input signal and the transfer function in the leakage path and the noise at the area of interest are obtained using a network analyzer (Rohde & Schwarz ZVL, 9 kHz to 3 GHz). We measure each parameter that is required for the estimation in the experimental environment shown in Figs. 2(a), (b), and (c). After turning off the power to the SASEBO and amplifier, the noise is measured in Fig. 2(a) as with measuring the EM field. As we consider that the transfer function is a contact value that does not depend on time in each case, we use an input signal at an adequately large voltage to ignore noise.

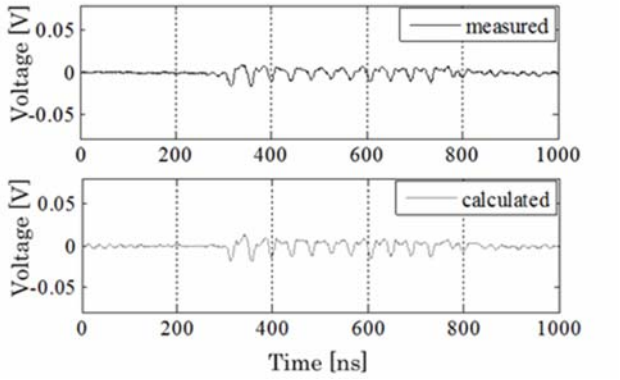
B. Comparison of Information Acquisition between Measurement and Estimation

In this section, waveforms of EM field measured in experiment are compared with waveforms estimated using Eq. (2). The waveforms are in good agreement, including secret-key information in each case shown in Fig. 3. To validate whether we can estimate the information acquisition by using estimation waveforms, the waveforms were examined for each case by correlation EM analysis (CEMA), which is a variation of correlation power analysis (CPA) [5][15]. Figure 4 shows the CEMA results, where the vertical axis indicates the number of incorrectly extracted round-key bytes (the "error rate"), and the horizontal axis indicates the number of traces. In these CEMA analyses, the key extraction was performed when the difference between the maximum and minimum correlation values was a maximum among all the CEMA results given by all the estimated keys. In the result of comparison, there is good agreement in each error rate between the measurement case and the estimation case.

(a) 100 cm



(b) 200 cm



(c) 300 cm

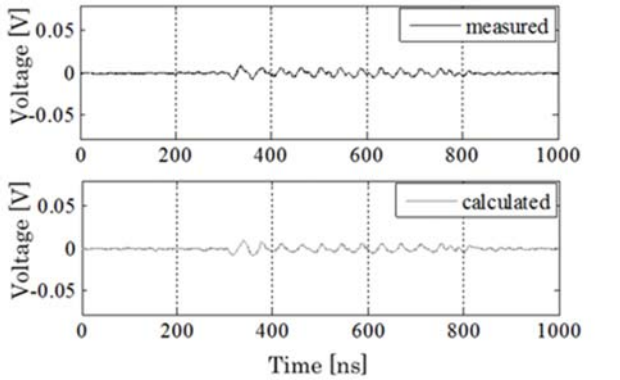


Fig. 3: Comparison of observed EM field waveform and calculated waveform for different distances between antennas.

IV. CONCLUSION

This paper presented an efficient method for estimating the propagation area of EM radiation including significant information. The basic idea is to exploit a multiplicative relation among the intensity of the information source, the transfer function, and the time variance of the signal at the area of interest. The proposed method can provide the degree of information leakage without actual EM analysis at the area of interest. Through experiments using an evaluation board, we confirmed that the estimated value was in fair agreement with the value obtained from actual EM analysis. We tested one specific environment in this experiment. A more detailed evaluation under various environmental conditions corresponding to actual usage environments is left for future study. Determining the source that causes the information leakage will require evaluation techniques from the fields of EMC and information security.

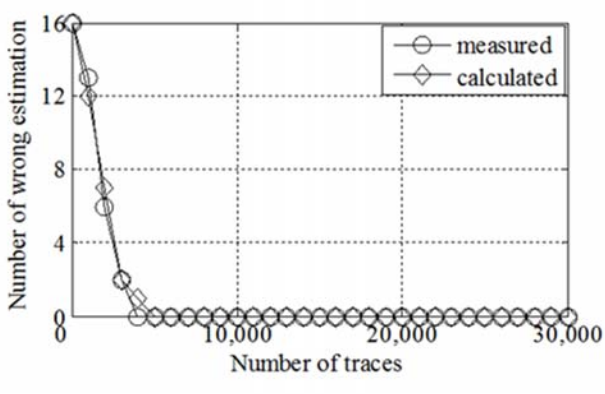
ACKNOWLEDGEMENT

This work was supported by JSPS KAKENHI Grant Numbers 25289068 and 25820098.

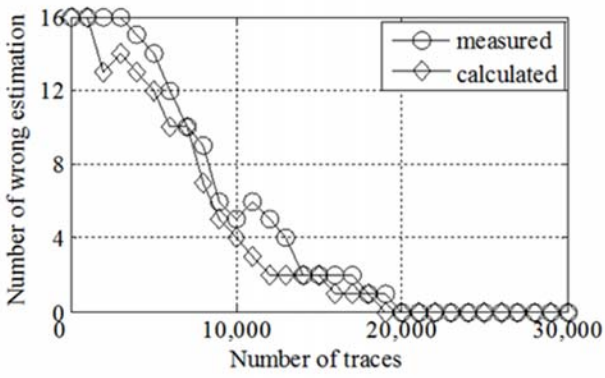
REFERENCES

[1] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," CHES 2001, Lecture Notes in Computer Science, vol. 2162, pp. 251-261, May 2001.
[2] D. Agrawal, B. Archambeault, R. Rao, and P. Rohatgi, "The EM sidechannel(s)," CHES 2002, Lecture Notes in Computer Science, vol. 2523, pp. 29-45, Aug. 2002.
[3] C. Kim, M. Schlaffer, and S. Moon, "Differential Side Channel Analysis Attacks on FPGA Implementations of ARIA," ETRI Journal, vol. 30, No. 2, pp. 315-325, Apr. 2008.
[4] T. Sugawara, Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, and A. Satoh, "Mechanism behind information leakage in electromagnetic analysis of cryptographic modules," The 10th International Workshop on Information Security Applications (WISA2009), Lecture Notes in Computer Science, vol. 5932, pp. 66–78, Aug. 2009.
[5] S. Mangard, E. Oswald, and T. Popp, "Power Analysis Attacks: Revealing the Secrets of Smart Cards," Springer-Verlag, 2007.
[6] T. Ikematsu, Y. Hayashi, T. Mizuki, N. Homma, T. Aoki, and H. Sone, "Suppression of Information Leakage from Electronic Devices Based on SNR," in IEEE International Symposium on Electromagnetic Compatibility 2011, pp. 920-924, Aug. 2011.
[7] C. R. Paul, "Introduction to Electromagnetic Compatibility (Wiley Seriesin Microwave and Optical Engineering)," Wiley-Interscience, 2006.
[8] Y. Hayashi, T. Sugawara, Y. Kayano, N. Homma, T. Mizuki, A. Satoh, T. Aoki, S. Minegishi, H. Sone, and H. Inoue, "An Analysis of Information Leakage from a Cryptographic Hardware via Common-Mode Current," EMC'09, July, 2009.
[9] Y. Hayashi, T. Sugawara, Y. Kayano, N. Homma, T. Mizuki, A. Satoh, T. Aoki, S. Minegishi, H. Sone, and H. Inoue, "Information Leakage from a Cryptographic Hardware via Common-Mode Current," in IEEE International Symposium on Electromagnetic Compatibility 2010, pp. 109-114, July. 2010.
[10] Y. Hayashi, T. Sugawara, T. Ikematsu, N. Homma, T. Mizuki, T. Aoki, and H. Sone, "Evaluation of Side-Channel Information Considering Cryptographic Device Configuration," SCIS2010，3B3-4，Jan. 2010.
[11] K. Ohmura, Y. Hayashi, T. Mizuki and H. Sone, "Influence of device structure on electromagnetic (EM) information leakage from the device," PPEMC'10，May 2010.
[12] K. Ohmura, Y. Hayashi, Mizuki, and H. Sone, "The Influence of Attached Lines for Electromagnetic Information Leakage from Information Devices," IEICE Technical Report, vol. 109, no. 241, EMCJ2009-47, Oct. 2009.
[13] Side-channel Attack Standard Evaluation Board (SASEBO),http://staff.aist.go.jp/akashi.satoh/SASEBO/en/index.html
[14] NIST FIPS PUB. 197, Advanced encryption standard (AES), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
[15] 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.

(a) 100cm



(b) 200cm



(c) 300cm

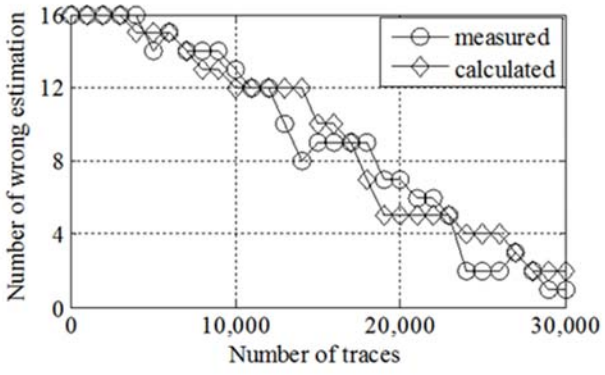


Fig. 4: Comparison of information acquisition using observed CM current waveform and calculated waveform for different line lengths.