Efficient mapping of EM radiation associated with information leakage for cryptographic devices

Haruki Shimada†, Yu-ichi Hayashi†, Naofumi Homma†, Takaaki Mizuki†, Takafulmi Aoki†, Hideaki Sone†, Laurent Sauvage†, and Jean-Luc Danger††

†Tohoku University, 6-6-3 Aramaki Aza, Sendai 980-8579, Japan
yu-ichi@m.tains.tohoku.ac.jp
††Telecom ParisTech, 46 rue Barrault, F-75634 Paris Cedex 13, France

Abstract— This paper presents an efficient map generation technique for evaluating the intensity of electromagnetic (EM) radiation associated with information leakage for cryptographic devices at the PCB level. First, we investigate the relation between the intensity of the overall EM radiation and the intensity of EM information leakage on a cryptographic device. For this purpose, we prepare a map of the magnetic field on the device by using an EM scanning system, after which we perform correlation electromagnetic analysis (CEMA) at all measurement points on the device, including points above the cryptographic module. The examined device is a standard evaluation board for cryptographic modules (SASEBO), where a cryptographic circuit is implemented on one of the FPGAs on the board. With this experiment, we demonstrate that an efficient map of EM radiation associated with information leakage can be generated on the basis of an EM radiation map. We also confirm that the generated map is in fair agreement with the corresponding map obtained from exhaustive CEMA.

I. INTRODUCTION

The exploitation of information leakage from cryptographic modules (software or hardware implementations of cryptographic algorithms) by side-channel attacks is of major concern for designers and evaluators of such modules. When a cryptographic module performs encryption or decryption, secret parameters related to the intermediate data being processed can be revealed from side-channel information, such as operation timing and power dissipation. A typical type of side-channel attack is the power analysis attack [1][2]. Electromagnetic (EM) analysis using the EM field generated by a cryptographic module has also been proposed as an extension of the power analysis attack [3].

One of the characteristics of EM analysis is that EM waveforms can be obtained by noncontact probing. Conventional attacks usually require direct physical access to the target module in order to acquire side-channel information. However, several studies [4]-[6] have demonstrated the possibility of obtaining secret keys from EM radiation measured at a distance from the cryptographic module. In particular, successful EM analysis of an SSL accelerator was carried out in [4] by measuring EM radiation emitted from the accelerator. In [6], it was reported that side-channel information was successfully acquired from power and communication lines connected to a device equipped with a cryptographic module. Thus, EM analysis at the PCB board level could pose a nontrivial threat to a vast group of cryptographic devices (i.e., electronic devices containing cryptographic modules), even if the modules are equipped with conventional countermeasures against direct access and EM radiation measurement, such as EM shielding packaging.

EM radiation emitted from electronic devices has been regarded as noise in the field of electromagnetic compatibility (EMC), and a number of studies on noise suppression and reduction have been conducted to prevent noise interference that causes damage to other electronic devices [7]. Based on knowledge and experience acquired through such studies, EMC-related committees have established guidelines on standardized acceptable values of EM radiation and corresponding immunity during device operation. Current electronic devices usually comply with EMC standards. However, the main objective of these standards is to ensure the suppression and reduction of EM radiation that disturbs other devices, and they do not concern radiation associated with leakage of sensitive information. In this regard, even if the amount of EM radiation (e.g., common-mode current) is below the value specified in the guidelines, extraction of sensitive information, such as secret keys from cryptographic devices, remains a strong possibility. In fact, previous studies [8][9] have demonstrated that information can be extracted from EM radiation from electronic devices that comply with the abovementioned guidelines. Therefore, rather than regarding EM radiation as plain noise, it is necessary to discuss specific countermeasures against the possible extraction of sensitive information from EM radiation.

From the viewpoint of such countermeasures, noise suppression and reduction techniques for EMC can be useful if they are tailored to the requirements for prevention of information extraction from EM radiation leakage. Until now, a number of countermeasures against side-channel attacks have been considered at the algorithm and logic-gate level in cryptographic modules [2], [10], and their effectiveness has been demonstrated. However, emerging EM analysis techniques can be applied to a wider variety of legacy devices which have not been equipped with conventional countermeasures. For example, a cryptographic module in a tamper-resistant HDD whose security level according to Federal Information Processing Standard (FIPS) 140-2 is 2 or higher might not be equipped with countermeasures against side-channel attacks since the HDD prevents attackers from

978-1-4673-2060-3/12/$31.00 ©2012 IEEE 794
accessing the module by employing tamper-resistant coating or sealing. Here, we assume that an attacker attempts to perform an emerging type of EM analysis attack from a distance (e.g., above the device or via power/communication cables), thus rendering the requirement for direct access to the cryptographic module unnecessary. The target design is in accordance with EMC standard but without any specific countermeasure for the attacks. Under such attacker model, electrical-level countermeasures derived from EMC viewpoint can provide a sufficiently strong and cost-effective solution for existing devices which are equipped with unprotected cryptographic modules.

To take advantage of conventional noise suppression techniques (and corresponding countermeasures) at the board level, critical parts (i.e., noise sources and noise propagation paths) on the board should be identified in advance. One of the straightforward methods for identifying such critical parts is to map the intensity of EM radiation onto the board. In conventional experiments, measurements are performed on as many points on the board as possible, and the intensity map produced in this way allows for devising effective countermeasures against EM radiation.

Based on the above considerations, this paper discusses a method for identification of critical parts related to information leakage (i.e., information propagation paths and antennae) at the board level, which allows for devising effective EMC countermeasures for suppression of information leakage. Recent studies on EMC have shown that the intensity of EM radiation associated with information leakage is not the same as the overall EM radiation [13]. In addition, information leakage is strongly dependent on the signal-to-noise ratio (SNR) at the measurement point [11], [12]. Also, several studies have demonstrated methods for mapping EM information leakage by conducting EM analysis at a large number of points above the cryptographic modules, which is effective for identifying such critical parts [13]-[15]. In contrast, the intensity of EM radiation associated with information leakage at the board level and methods for its mapping have not been studied since conventional attacks are usually performed near the module. It is noteworthy that the intensity of EM radiation associated with information leakage at the board level can be estimated from EM radiation measured at a distance from the device or via attached cables.

In this paper, first we investigate the relation between the intensity of EM radiation and the intensity of EM information leakage at the PCB level. For this purpose, a magnetic field map above an evaluation board (i.e., a device without any specific EMC protection such as decoupling condensers), including the cryptographic module, is prepared with an EM scanning system, after which an exhaustive EM analysis is performed at all measurement points. We examine the differences and similarities between the two maps from the experimental results. Next, we present an efficient mapping method which can identify critical parts on the board prone to information leakage. According to [13], the basic idea behind this method is to extract a specific frequency band containing sensitive information. Through this experiment, we confirm that our map is in fair agreement with the information leakage map generated by exhaustive EM analysis. This suggests that both an EM radiation map and an information leakage map can be obtained simultaneously by measuring EM radiation around the board only once. In addition, we confirm from the experiment using a device with decoupling condensers that the proposed method is useful to evaluate the effect of countermeasures from the viewpoint of EMC.

II. PRELIMINARY EXAMINATION OF EM RADIATION AND INFORMATION LEAKAGE

A. Experimental results

Figure 1 shows an overview and a block diagram of our experimental setup. We employed SASEBO-G (Side-channel Attack Standard Evaluation Board) as the test device [16] (Fig.2), which is equipped with two field-programmable gate arrays (FPGAs) denoted as FPGA1 and FPGA2. An Advanced Encryption Standard (AES) circuit supporting 128-bit key length [17] was implemented on FPGA1, and a control and communication circuit was implemented on FPGA2. The secret key for the AES circuit was a reference value (0x2b7e151628aed2a6abf7158809cf4f3c), as given in the
algorithm specification [18]. The clock frequency and the supply voltage on SASEBO-G are 24 MHz and 3.3 V, respectively. EM radiation at the surface of the board was measured with an oscilloscope (Agilent MSO 6104A) at 4 GSamples/s via a magnetic field probe (MT-545) with a bandwidth between 150 kHz and 3 GHz, attached to an EMC noise scanner (WM7400). Note that the coil face of the probe was placed parallel to the board, and the vertical component of the EM radiation was measured by the probe. The test board was controlled by a PC, which fed input strings (i.e., plaintexts) to FPGA1 via FPGA2 and stored the encrypted outputs (i.e., ciphertexts). The corresponding EM radiation was measured synchronously with each encryption operation with the oscilloscope. The probe of the EMC scanner was 1.8 cm above the surface of the board and scanned both the vertical and horizontal axes every 5 mm. In total, the number of measurement points was 1240 (=31 × 40) over the entire surface. All sockets on SASEBO where shunt resistors can be inserted were short-circuited with jumpers. The frequency range observed in this experiment was between 0 and 500 MHz, which is in accordance with the range of frequencies carrying sensitive information as mentioned in [19].

B. Intensity map of the magnetic field above the board
Figure 3 shows the map of EM radiation (or magnetic field) during encryption as measured with the above setup, where the intensity is between 48 and 60 dBμV and the frequency range is between 0 and 500 MHz. The frequency spectrum was calculated by applying Discrete Fourier Transform (DFT) to the average EM traces measured in the time domain. The intensity corresponds to the maximum amplitude over the full frequency spectrum. The highest value was observed around a condenser near FPGA2, and relatively high values were observed at the two crystal oscillators. Figure 4 shows the frequency spectrum above the AES circuit in FPGA1.

C. Intensity map of information leakage above the board
The intensity map of EM information leakage was derived from the measured EM traces for the same board. Side-channel information in the form of EM radiation was examined for each point by Correlation EM Analysis (CEMA), which is a variation of Correlation Power Analysis (CPA) [20]. CEMA utilizes a large number of EM traces and the corresponding outputs for calculating the correlation coefficients for the measured values and the values estimated from the correct key. We used the Hamming distance model [2], in which the number of changed bits at the final round of AES is used to calculate each estimated EM value (see [20] for details). In addition, we used a predefined set of plaintexts in order to reduce the computation time [21].

In this experiment, we assumed that the correlation coefficients correspond to the SNR. To extract a significant frequency range, we calculated the correlation coefficients in the frequency domain rather than in the time domain, following [19]. Figure 5 shows the resulting information leakage map (i.e., correlation coefficients) corresponding to the EM radiation map in Fig. 3, where the frequency range is between 0 and 500 MHz. The analysis revealed the secret key faster as the (maximum) correlation value increased. The highest value was observed at FPGA1 and its ground and power lines. The correlation map is clearly different from the corresponding magnetic field map. This result confirms that the intensity of EM radiation associated with information leakage is not directly related to the intensity of the overall EM radiation as described in [11]-[13].

III. MAPPING OF EM RADIATION ASSOCIATED WITH INFORMATION LEAKAGE
This section describes an efficient method for generation of maps of EM radiation associated with information leakage.
First, we select a specific frequency band containing sensitive side-channel information. For this purpose, we focus on the results of CEMA in the frequency domain [19][22] at the measurement point with the highest correlation coefficient. Figure 6 shows the correlation coefficient spectrum in the frequency domain above FPGA1, where it is clear that the coefficient values are highest between 5 and 20 MHz even if the original intensity is relatively low as shown in Fig.4. This suggests that the resulting information leakage map of the PCB board would be strongly dependent on the specific frequency band.

With this information, we proceeded to generate an EM radiation map for this frequency band. Figure 7 shows the resulting map obtained as the EMC scanner swept the frequency band between 5 and 20 MHz at 250-kHz increments. The generated map in Fig. 7 is in fair agreement with that in Fig. 5, which suggests that an information leakage map can be prepared within a short time from an EM radiation map without performing exhaustive CEMA of the surface of the board. In other words, both an EM radiation map and an information leakage map can be prepared simultaneously by scanning the board only once, which can considerably reduce the computation time. For example, a Windows PC with an Intel Xeon W3680 3.33 GHz processor and 16 GB of memory required at least 5 h to generate the correlation map in Fig. 5 (in this experiment, the computation time was drastically reduced by selecting a set of predefined plaintexts, and the analysis was conducted with 100 waveforms; in comparison, obtaining the same map with a set of random plaintexts would have required more than 2,500 h). On the other hand, the map in Fig. 7 was obtained within 0.5 h on the same PC since the computation cost was comparable with that for the preparation of the EM radiation map.

In this experiment, we performed one CEMA in the frequency domain above the cryptographic module in order to extract the specific frequency band. Designers and evaluators of cryptographic devices usually know the most appropriate measurement point for performing CEMA. If the point is not clearly identified, several measurements can be performed at highly likely points near the module, and the obtained CEMA results can be integrated to determine the frequency band carrying sensitive information. The development of an effective method for selection of such a representative measurement point is a topic for future study.

IV. Evaluation of Countermeasures Based on Information Leakage Maps

The validity of the above map generation technique is also demonstrated through evaluation of board-level countermeasures. As an example, we evaluated the effect of installing bypass capacitors on the back surface of SASEBO for the prevention of information leakage through side channels. Figure 8 shows an overview of the implementation, where we placed 8 capacitors of 0.1µF and 16 capacitors of 0.01 µF on the reverse face of FPGA1. We expected that the conducted noise including significant information was effectively shunted through the capacitors.

Fig. 9 shows the map generated by our proposed method, which is the EM radiation map with a specific frequency band from 5 to 20 MHz corresponding to Fig. 7. As a result, we confirmed that the EM radiation was fairly lowered in comparison with that of the previous board without the bypass capacitors. At the same time, however, we can find two distinct points showing higher intensity of EM radiation appeared at the upper sides of the FPGAs as seen from above. More specifically, the two points are located near the oscillators supplying clock signals to the FPGAs, which suggests the possibility of information leakage in the form of EM radiation around these two points.
For comparison, Fig. 10 shows an information leakage map obtained by exhaustive CEMA, which corresponds to the map in Fig. 5. In other words, this figure should reveal any points where information leakage occurs. However, it is clear that there are no such points at the board level, showing that the bypass capacitors have reduced the intensity of information leakage, at least at the front surface of the board. Note that with this countermeasure the installed capacitors might increase the possibility for attacking the module by conducting an attack targeting the back surface of the board, and therefore both the front and back surfaces of the board must be evaluated. Nevertheless, we were unable to obtain any information about the secret keys by CEMA even around the two points visible in Fig. 9. Figure 11 shows the correlation coefficient spectrum above the energetic point corresponding to Fig. 6.

The above results show that the EM radiation emitted by the oscillators in the target frequency band was not related to information leakage. This is a limitation of our map generation technique, whereby even if the most likely frequency band carrying side-channel information is selected, it is difficult to evaluate only the EM radiation responsible for information leakage. On the other hand, the nature of our technique is acceptable from the viewpoint of fail-safe evaluation. Essentially, since any point at which there is a possibility of information leakage should be investigated, our map effectively reduces the number of investigation points. It would also be possible to remove EM radiation unrelated to information leakage if the differences between the EM radiation profiles of the device obtained during operation and while the device is idle can be mapped clearly.

V. CONCLUSION

This paper investigated the relation between the intensities of overall EM radiation and EM information leakage on cryptographic devices at the PCB level. For this purpose, first we prepared a map of the magnetic field above the device by using an EM scanning system, after which we performed exhaustive CEMA at all measurement points on the device. The device used in the experiment was a standard evaluation board for cryptographic modules (SASEBO), and an AES circuit was implemented on one of the FPGAs on the board. We confirmed that the two types of maps were notably different when a specific frequency band carrying sensitive information was not considered. Next, we presented an efficient method for preparing an information leakage map based on the EM radiation map without the need for conducting exhaustive CEMA. Through this experiment, we demonstrated that the map obtained in this way was in fair agreement with the information leakage map obtained from exhaustive CEMA. This suggests that both an EM radiation map and an information leakage map can be generated simultaneously by scanning the board only once. Our technique can drastically reduce the computation time. In addition, we confirmed that our technique was available for evaluating whether an EMC protection is useful to protect against EM information leakage.

Given the possibility of information leakage, the proposed technique can be used to facilitate the identification of points of vulnerability and the application of effective countermeasures against such leakage to the affected device. The identification of the most appropriate measurement points for the target device will be the subject of future work. In addition, the back side analysis at PCB level with the same method and comparisons with methods described in [13-15] are being left for the prospective works.

ACKNOWLEDGEMENT

This research was supported by the Strategic International Cooperative Program (Joint Research Type) jointly funded by the Japan Science and Technology Agency (JST) and the French National Research Agency (ANR).

REFERENCES


Fig.9: Magnetic field map (5-20 MHz) after implementing the bypass condensers.

Fig. 10: Correlation map (5-20 MHz) after implementing the bypass condensers.

Fig.11: Correlation coefficient spectrum in the frequency domain above the oscillator.


