Journal of Signal Processing,Vol.16,No.3,pp.241-250,May 2012

PAPER

Electromagnetic Analysis Enhancement Based on Near-Field Scan

Hongying Liu[1] , Yukiyasu Tsuoo[2] , Yibo Fan[3] , Bin Hu[1] and Satoshi Goto[1]

[1]Graduate School of Information, Production and Systems, Waseda University,
Kitakyushu 808-0135, Japan, E-mail: liuhongying@fuji.waseda.jp
[2]Information and Media Processing Laboratories, NEC Corp., Kawasaki 211-8666, Japan, E-mail: tsunoo@bl.jp.nec.com
[3]State-Key Lab of ASIC & System, Fudan University, Shanghai 201203, China, E-mail: fanyibo@fudan.edu.cn

Abstract **Electromagnetic emissions leak confidential data of cryptographic devices. By exploiting such emissions, electromagnetic analysis (EMA) is performed with EM probes to extract secret information from these devices. Owing to the locality of EM emissions, namely, secret information may leak from multiple locations around cryptographic devices, it is difficult to determine the exact location before conducting an EMA. In this paper, *signal variance* of EM emissions during encryption is proposed to identify the information leakage of unprotected and protected cryptographic modules. We prove that *signal variance* is an equivalent metric to Difference of Means (DoM). Thus, by computing the higher *signal variances* based on near-field scan, the data-dependent EM emissions are disclosed, namely, the leakage locations are found. In addition, a small and low-cost probe is made to verify the proposed EMA on application-specific integrated circuit (ASIC) implementations. The experiment on AES PPRM1 implementation indicates that misjudgments of leakage are reduced, and the accuracy is improved 48.6% compared with existing methods. Moreover, the experiment of EMA against AES WDDL implementation shows that *signal variance* is also effective in exposing the leakage locations in the presence of countermeasures. The performance of EMA is enhanced.**

Keywords: electromagnetic analysis, information leakage, data dependence, magnetic-field probe, s-box

1. Introduction

The security of a cipher depends on not only its mathematical properties but also its implementations. Side channel attack (SCA) has become a serious threat to the security of cryptographic devices. It is based on exploiting the power consumption, electromagnetic emission and timing information, as well as the variation of cache content of a cryptographic module to expose the secrets. Electromagnetic analysis (EMA) is performed with electromagnetic (EM) probes to extract the secret information from devices even at a distance. It has been actively investigated and studied. The simple EMA (SEMA) and differential EMA (DEMA) have been demonstrated [1]. EM leakage has been assessed in [2]. Gebotys et al.[3] showed EMA attacks on a PDA which runs Rijndeael and elliptic curve cryptography.

To protect cryptographic devices from SCAs, abundant countermeasures have been designed and implemented, such as Mask[4], Wave Dynamic Differential Logic (WDDL)[5], and Masked Dual-Rail Logic (MDPL)[6]. All these make the attacks difficult. Different approaches have been proposed to improve the performance of attacks. For example, switching distance model was proposed for both EMA and power analysis [7]. Some researches concentrated on noise reduction of acquired signals [8, 9].

Although most techniques that enhance the performance of power analysis and EMA can be shared, such as the leakage models, one characteristic that distinguishes EMA from power analysis is that EM emissions might be radiated from multiple locations around a cryptographic module, while power consumption is simply observed through an inserted resistor. Then for conducting EMA attacks, majority of the published works use probes of small size, in the millimeter range or even smaller. The benefit of this probe is that it distinguishes EM emissions from close locations, thus the noise caused by modules not related to cryptographic computation is attenuated. An example of a handmade probe described in literature was 3 mm long [1]. The commercially available tiny magnetic-field probes, which are designed for electromagnetic compatibility (EMC) analysis, such as the one mentioned in [10], were also used for EMA.

In this case, a challenging issue is where the possible locations are before conducting EMA attacks. In general, an attacker lacks the knowledge of the exact locations from which EM signals are emitted by a cryptographic module or communication interface. He may open the package of cryptographic LSI to recognize its different modules with a microscope. Nevertheless this is a semi-invasive approach, which is destructive [11].

Another way is to put the probe blindly, for example, far away from the cryptographic module, which leads to a very slow key detection or even failure. The drawback of this approach which is named “blind placement”, is that the leakage regions are not localized accurately.

Other approaches have been proposed. Quisquater and Samyde[12] exploited EM Cartography, which is an imaging technique, to observe the EM emissions of a smart card. Sauvage et al. [10] applied this technique to reveal the active regions of DES encryption modules on FPGA. In their work, 50 points x 50 points on a region of 2.08 cm x 2 cm over the FPGA were scanned, and the maximum peak-to-peak amplitudes of EM signals in the time domain were extracted to acquire an EM map. Then the most radiating point was identified based on the EM map and used to perform EMA. This approach is named "peak-to-peak amplitude" in this paper. It is feasible and more accurate than blind placement.

However, it is noted that the maximum peak-to-peak amplitude of EM signals after a subtraction computation between the active and idle phase of the DES module is utilized to draw the EM map, which is not an optimal indicator for revealing the locations of highest leakage and probably causes misjudgment, because the maximum peak-to-peak amplitude only represents the region where EM emissions are highest, but not necessarily the data-dependent EM signals, which are crucial for the success of EMA. Additionally, though the influence of surrounding noise might be reduced by the subtraction computation, numerous other data-independent EM signals, such as signals from communication interfaces, still exist and may prevent correct judgments of information leakage. Furthermore, when countermeasures are applied, the data dependence of encryption is concealed. The peak-to-peak amplitude of EM signals does not expose real leakage locations.

In order to solve these problems, a new leakage indicator: signal variance, is proposed to localize the locations of information leakage. The statistical characteristics of EM signals during encryption and the computation of higher values of signal variance from near-field scan over the surface of cryptographic devices enable the detection of leakage locations of the cryptographic module. We prove that signal variance is an equivalent metric to Difference of Means (DoM) used in DEMA. It identifies the data-dependent EM signals without preknowledge of the layout of cryptographic modules, and decreases the misjudgments of information leakage. To verify the proposition, a small and low-cost probe was developed and fixed to a near-field scanning system to acquire time-domain EM signals over the surface of a cryptographic LSI. By computing the signal variance, the leakage points of AES PPRM1 (Positive Prime Reed Muler 1-stage based s-box) implementation are localized. The misjudgment of the information leakage is reduced and the accuracy is increased by 48.6% compared with the method of peak-to-peak amplitude. Furthermore, with the signal variance, the leakage points are exposed in the presence of WDDL countermeasures. Therefore, EMA is expedited.

The remainder of this paper is organized as follows. Section 2 presents the proposed EMA in detail. Section 3 shows the experimental environment. Section 4 demonstrates the experimental results. Conclusions are drawn in section 5.

2. Proposed EMA

The proposed EMA includes two steps: near-field scan and leakage localization. In near-field scan, EM signals are acquired. In leakage localization, a leakage indicator is used to identify leakage locations. They are explained in detail in this section.

2.1 Near-field scan

Near-field scan is a technique that is used to specify the radiated source on LSIs or printed circuit boards (PCBs). It has been standardized as International Electro-technical Commission (IEC) 61967-3[13]. The near-field scanning system comprises a magnetic-field probe, a device under test (DUT), a sustentation and positioning instrument which is used to fix and move the probe over the DUT. Moreover, a spectrum analyzer or oscilloscope is required to receive the measured values from the magnetic-field probe. A preamplifier, which magnifies weak signals, is optional.

A typical near-field scanning system for EMA is shown in Fig. 1. In the context of EMA, an exact computation for the strength of the measured EM field is not necessary because the voltage output from the probe is proportional to the EM field around the cryptographic LSI and it represents the activity of each encryption. In DEMA or CEMA, a differential voltage or correlation coefficient is sufficient to detect the correct key. In addition, although the quality of the obtained EM signals depends on the utilized probes, there is no standard for its size in the application to EMA.

After setting up of a near-field scanning system, it is used to acquire EM signals over the surface of DUT when the encryption algorithm runs. Suppose that at each scanning point, N different random plaintexts are used, during each run i (i =1,2,…, N), an EM signal trace $W_i(t)$ is recorded, which consists of encryption-related signals $S_i(t)$ and independent noise η, expressed by

$$W_i(t) = S_i(t) + \eta \quad (1)$$

where t is sampling time. In this paper, we assume that noise is well reduced by preprocessing techniques.

2.2 Leakage localization

To localize hot spots of DUT, i.e., cryptographic LSI, the most accurate method is to perform EMA with signal traces at each scanning point. Then the locations where EMA succeeds faster are hot spots. However, the time computation for such an exhaustive method is quite large. Every key candidate must be examined to test the success of EMA at each location. Moreover, hot spots cannot be exposed unless EMA is conducted. To enable an accurate prediction of the hot spots and reduce the computation, we attempt to devise a leakage indicator, which is an equivalent metric for EMA to localize hot spots and avoid the computation of key searches. Signal variance is such a metric. The derivation and proposition are shown below.

Suppose that at one scanning point, a leakage model is used. We adopt the widely admitted leakage model. It is assumed that the EM signal $S(t)$ depends on a selection function H, which is an intermediate value of encryption,

and is related to plaintext and key[14], given by Eq.(2), where t is sampling time, a represents a scalar gain, and b denotes the offset, and time-dependent components.

$$S(t) = aH + b \tag{2}$$

Then a distinguisher is applied to test the dependence between $S(t)$ and H. Our leakage indicator is from the distinguisher DoM, which is briefly reviewed here. To determine whether one candidate key K_c is correct or not, DoM uses N random plaintexts C_i (i =1,2,…, N) which yield N sampling signals, $S(t) = S_i(t)$. The selection function $H = H(C_i, \beta, K_c)$ partitions $S_i(t)$ into two sets: $S^1=\{S_i(t) \mid H(C_i, \beta, K_c)=1\}$ and $S^0 =\{S_i(t) \mid H(C_i, \beta, K_c)=0\}$ under an examined bit β. For example, H is the Hamming weight of a single-bit output of SubBytes computation for AES, and $H \in \{0,1\}$. β denotes one bit of s-box. Then DoM computes a differential trace $D_\beta(t)$, which is the difference between the averaged S^1 and S^0, given by

$$D_\beta(t) = \frac{1}{|S^1|}\sum_{S_i(t)\in S^1} S_i(t) - \frac{1}{|S^0|}\sum_{S_i(t)\in S^0} S_i(t) \tag{3}$$

where $|S^1| + |S^0| = N$. It is simplified to

$$D_\beta(t) = \mathrm{E}[S(t) \mid H = 1] - \mathrm{E}[S(t) \mid H = 0] \tag{4}$$

$D_\beta(t)$ tends to 0 for a wrong key guess because the partitioning is statistically random. $D_\beta(t) \neq 0$ for a correct key and this results in a peak. The correct key is identified as the one that yields the highest peak in the differential trace at some instant $t = \tau$. In fact, we do not compute $D_\beta(t)$ to localize hot spots at the scanning point, but attempt to look for a substitute. It is noted that the variance of EM signal $S(t)$ is $Var[S(t)]$, given by

$$\begin{aligned} Var[S(t)] &= \mathrm{E}[(S(t) - \mathrm{E}[S(t)])^2] \\ &= \mathrm{E}[(aH + b - \mathrm{E}[aH + b])^2] \\ &= a^2 Var[H] \end{aligned} \tag{5}$$

The covariance of $S(t)$ and H is expressed as

$$\begin{aligned} Cov[S(t), H] &= Cov[aH + b, H] \\ &= Cov[aH, H] + Cov[b, H] \\ &= aVar[H] \end{aligned} \tag{6}$$

where $Cov[b, H] = 0$, since b and selection function H are independent. Then Eq. (5) rewrites as

$$Var[S(t)] = a(aVar[H]) = aCov[S(t), H] \tag{7}$$

The covariance of $S(t)$ and H is calculated as

$$\begin{aligned} Cov[S(t), H] &= \mathrm{E}[(S(t) - \mathrm{E}[S(t)]) \cdot (H - \mathrm{E}[H])] \\ &= \mathrm{E}[S(t) \cdot (H - \mathrm{E}[H]) - \mathrm{E}[S(t)] \cdot H + \mathrm{E}[S(t)] \cdot \mathrm{E}[H]] \\ &= \mathrm{E}[S(t) \cdot (H - \mathrm{E}[H])] - \cancel{\mathrm{E}[S(t)] \cdot \mathrm{E}[H]} + \cancel{\mathrm{E}[S(t)] \cdot \mathrm{E}[H]} \\ &= \mathrm{E}[S(t) \cdot (H - \mathrm{E}[H])] \end{aligned} \tag{8}$$

Then, according to the definition of mathematical expectation, Eq. (8) rewrites as

$$\begin{aligned} Cov[S(t), H] &= \sum_s \sum_h \mathrm{P}[S(t) = s, H = h] \cdot s \cdot (h - \mathrm{E}[H]) \\ &= \sum_s \sum_h \mathrm{P}[S(t) = s \mid H = h] \cdot \mathrm{P}[H = h] \cdot s \cdot (h - \mathrm{E}[H]) \end{aligned} \tag{9}$$

For single-bit selection function H, the probability of its value being 1 and 0 is equal, namely, $\mathrm{P}[H=1]=\mathrm{P}[H=0]=1/2$, and $H-\mathrm{E}[H] \in \{-1/2,+1/2\}$. Thus Eq. (9) rewrites as

$$\begin{aligned} Cov[S(t), H] &= \sum_s \mathrm{P}[S(t) = s \mid H = 1] \cdot s \cdot (-\frac{1}{2}) \\ &\quad + \sum_s \mathrm{P}[S(t) = s \mid H = 0] \cdot s \cdot (+\frac{1}{2}) \\ &= \frac{1}{2}\sum_s -\mathrm{P}[S(t) = s \mid H = 1] \cdot s + \sum_s \mathrm{P}[S(t) = s \mid H = 0] \cdot s \\ &= \frac{1}{2}\mathrm{E}[S(t) \mid H = 1] - \mathrm{E}[S(t) \mid H = 0] \\ &= \frac{1}{2} D_\beta(t) \end{aligned} \tag{10}$$

From Eq. (8) and Eq. (10), we have the relation

$$D_\beta(t) = \frac{2}{a} Var[S(t)] \tag{11}$$

When the selection function is multi bit, $H=H(C_i, \mathcal{C}, K_c)$, where $\mathcal{C} =\beta_1\beta_2...\beta_G$. For example, H is the Hamming weight of the 8-bit output of SubBytes computation for AES, and $H \in\{0,1,2,3,4,5,6,7,8\}$. $\mathcal{C}$ denotes 8 bits of the s-box, and G=8. DoM computes the differential trace $D(t)$ as a sum of each examined bit in the case of single bit, given by

$$\begin{aligned} D(t) &= D_{\beta_1}(t) + D_{\beta_2}(t) + ... + D_{\beta_G}(t) \\ &= G \cdot D_\beta(t) \end{aligned} \tag{12}$$

$$= \frac{2G}{a} Var[S(t)] \tag{13}$$

under the assumption that each bit contributes identically to the power dissipation. Indeed, this assumption is true for a number of hardware platforms, such as ASIC. Thus, Eq. (13) is obtained, which proves that DoM is equal to the signal variance of EM emissions despite a constant gain of $\frac{2G}{a}$.

Therefore, our proposition is: the signal variance $Var[S(t)]$ at time t for N leakage signals, given by Eq. (14), is used as an equivalent metric to DoM to test data dependence.

$$Var[S(t)] = \frac{1}{N}\sum_{i=1}^{N}(S_i(t) - \frac{1}{N}\sum_{i=1}^{N} S_i(t))^2 \tag{14}$$

This proposition means that signal variance is the equivalent metric for evaluating the dependence between EM emissions and data encryption, because DEMA identifies the correct key by DoM test, whereby the dependence between EM emission and data encryption can be evaluated. For a certain encryption implementation, a high signal variance denotes intensive fluctuation of the EM field, which is caused by the dynamic change of instantaneous current in the LSI. This dynamic change is due to the switching activities of its components, i.e., from 0 to 1, or 1 to 0. In other words, a high variance represents strong dependence on input data, and a low variance means that the instantaneous signal remains the same and is independent of input data. This is the reason why signal variance can reveal information leakage. It also indicates that there is no direct relationship between "peak-to-peak amplitude" and the evaluation metric. Although a high "peak-to-peak amplitude" means strong EM emission, this emission is not necessarily data-dependent. Thus it cannot accurately express the data dependence of cryptographic operation, and it may result in misjudgments of hot spots. It

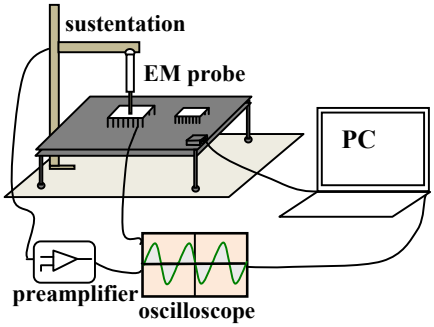


Fig. 1 Typical near-field scanning system for EMA

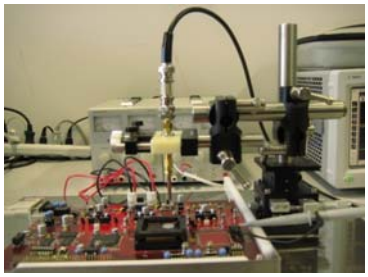


Fig. 2 Experimental environment

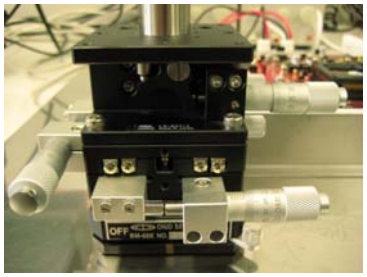


Fig. 3 Scales on 3D-positioning sustentation

Fig. 4 Handmade probe

is not an optimal indicator for localizing leakage.

The time complexity is reduced by computing signal variance. Suppose that the sampling length is M for each of N signal traces. DoM decides the correctness of only one partitioning at each run. Thus for a DEMA attack that attempts L partitioning, where L is the size of one subkey, e.g., $L=2^8$ for AES, it requires a time complexity of $\theta(NML)$. For a CEMA attack, the correlation coefficient between signal traces and leakage model must be calculated. It is $\theta(2NML)$. With our proposition, the time complexity is $\theta(NM)$, because the partitioning for guessing key is avoided.

Signal variance can be used to disclose the information leakage of implementations with countermeasures. As we know, when countermeasures, either masking or hiding, are applied to cryptographic modules, information leakage becomes difficult to detect by SCAs because of the concealment of data-dependent operations. However, they still exist. In a masked circuit, a logic gate potentially switches more than once during one clock cycle, which results in considerable amount of power dissipation. Thus this dissipation of the gate is still correlated to some unmasked inputs and outputs. The masked implementations are susceptible to DEMA and DPA attacks. For countermeasures that use dual-rail circuits, such as WDDL, MDPL, when input signals have a difference of delay time, the timing of starting the power dissipation varies independent of the signal values during an operation cycle. Then the difference of power dissipation remains detectable by DEMA and DPA. Thereby, the signal variance is still capable of identifying information leakage in these cases. But more signal traces are required to expose hot spots.

The equivalence of signal variance to the DoM test has been presented. For every scanning point, the above proposition holds. Therefore, with the signals acquired for each scanning point from near-field scan, we calculate the signal variance at instant $t = \tau$, which is the time the examined value is handled (Note that this instant is estimated in accordance with the attacked encryption operation in specific implementation). A leakage map can be plotted. Hot spots are those locations with higher values of signal variance. EMA succeeds faster at these locations.

3. Experimental Environment

The experimental environment is shown in Fig. 2. The platform is Side-channel Attack Standard Evaluation Board (SASEBO)-R[15]. A cryptographic LSI manufactured by 130 nm CMOS process and a control FPGA are mounted on the printed circuit board (PCB). RS-232 interface is provided to communicate with the host PC. A 3D-positioning sustentation with scales in three dimensions is used to control the position of the probe above the PCB. A close-up of the scales is shown in Fig. 3. Additionally, a preamplifier with gain of 51 dB is connected to the probe via a coaxial cable to magnify the weak EM signals before they are sent to the Agilent MSO 54832D oscilloscope.

A handmade magnetic-field probe is used for the near-field scan. It is a single-turn probe, in square aperture, and has a side length of 2 mm. The probe head is soldered on the inner conductor of the semi-rigid coaxial, shown in Fig. 4. The diameter of the copper loop is 150 um. Because the aperture of the loop is square and the dimensions of the loop probes are much smaller than the wavelength, the induced electric field is compensated in the loop.

4. Experimental Results

In this section, the proposed EMA is validated on unprotected implementation and protected implementation respectively. Without loss of generality, the unprotected implementation is PPRM1, and the protected implementation is WDDL for AES on SASEBO-R.

In general, the performance of EMA is assessed by measurements to disclose (MTD) [16] or success rate [17]. MTD is the number of signal traces required for a successful attack. Success rate expresses the number of correct subkey guesses among the secret key. Both of these two metrics are used in the following experiments.

4.1 Proposed EMA on unprotected module

A near-field scan over the surface of the LSI when AES PPRM1 implementation runs, is carried out. The origin of the Cartesian coordinate system is set at the corner of pin1 and pin160 of the LSI, which has a package area of 28 mm x 28 mm, shown in Fig. 5. The probe plane is kept at 0.5 mm over the packaged surface in order to receive the strong vertical field, and it moves in steps of 1.0 mm from location (1,1). Therefore, there are 784 (28x28) scanning points. Encryption proceeds with 10000 random plaintexts at each point and a fixed but randomly chosen 16-byte key (the final round): 28 AF CE 9F 5A FF C8 F1 E0 54 B3 52 B0 CE 43 0E. The EM signals $W_i(t)$ (i=1,2,…,10000, and t = [1,1000]

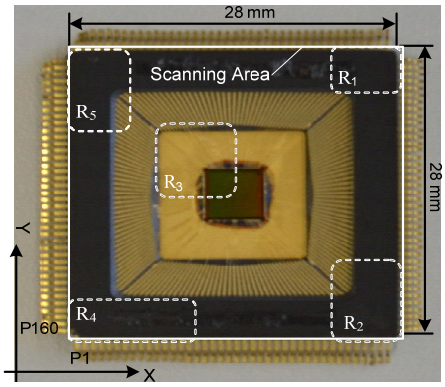


Fig. 5 Depackaged cryptographic LSI

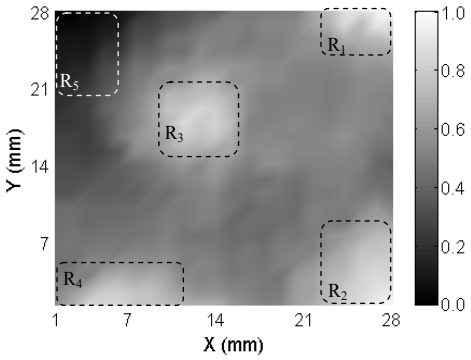


Fig. 6 Correlation coefficients of EMA for the scanning area

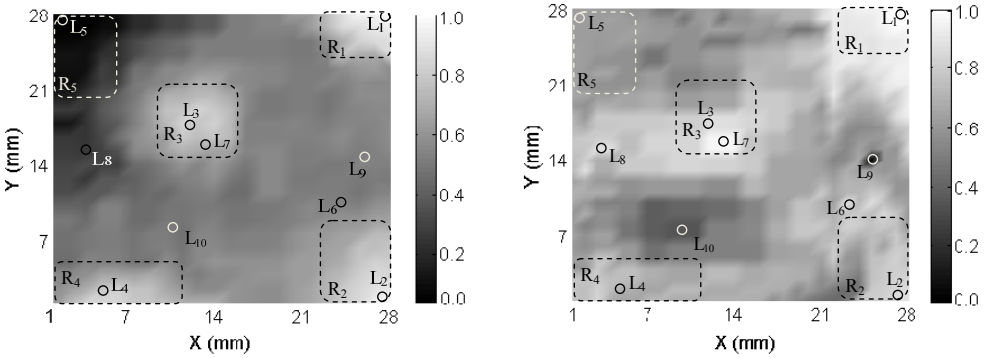


Fig.7 **(a)** Leakage map for AES PPRM1 calculated with proposed method, **(b)** Leakage map for AES PPRM1 calculated with peak-to-peak amplitude[10]

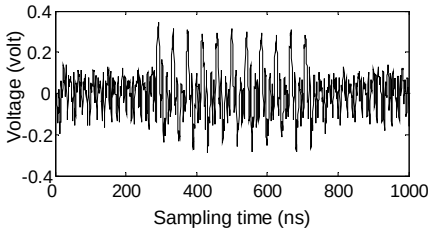


Fig. 8 Signal trace of AES PPRM1 at (1,1)

ns) are acquired and averaged 30 times by the oscilloscope. The sampling rate is 1G Sa/s, and 1000 points are recorded for each sample. This covers the total encryption period. Start timing for trigger signal is the EXEC signal, which is obtained from the pin of encryption execution on LSI. The clock cycle of encryption is 41.6 ns. A signal trace at location (1, 1) is shown in Fig. 8. The 10-round encryption and a register access are shown by 11 peaks in 11 clock cycles.

Signal variance in the final round of AES encryption is calculated according to Eq. (13), and normalized to [0,1]. The leakage map is shown in Fig. 7(a). Since we are interested in the output of s-box in the final round for analysis, t = 709.4 ns at each point. At this instant, the 10-round encryption is finished, and the ciphertext is to store in the data registers in the area of silicon die. The leakage map indicates several active and inactive regions. Four regions (R_1-R_4), which have hot spots, and region R_5, which has cold spot (note that cold spot is defined as the point with the minimum value on leakage map in this paper), are marked with rounded rectangles in Fig. 7(a).

The leakage map in Fig. 7(a) agrees with present activity of cryptographic LSI according to the manual of LSI [18]. These regions (R_1-R_5) are also marked in Fig. 5. Region R_3 which is around the silicon die, exhibits hot spots due to the encryption of the cryptographic core. Region R_1 which is around the pins of data output, and region R_2, which is in the vicinity of the address bus, also have hot spots. Although pins around R_4 and R_5 are not active at this moment, R_4 has hot spots because of the EXEC pin. A summarization of the connected pins, present activity, and range of signal variance of these regions is listed in Table 1.

It is noted that region R_3 is not at the exact center of the silicon die. This is probably due to the distribution of power/ground grid of the cryptographic LSI. Because of the complexity of this distribution, it is difficult to deduce any characteristic about EM emission. The mechanism behind leakage has been actively studied by researchers, such as Schmidt et al. [19]. It is not discussed further in this paper.

In order to compare the results with conventional methods, maximum peak-to-peak amplitude [10] at the same instant after a subtraction of idle sampling at each point is calculated, normalized and plotted in Fig. 7(b).

The locations of hot spots exposed in Fig. 7(a) and Fig. 7(b) are quite different. They are marked with small circles. Hot spots of Fig. 7(a) are L_1, L_2, L_3, and L_4, with L_5 as a cold spot. In Fig. 7(b), hot spots are L_1, L_6, L_7, and L_8. Cold

spots are L_9 and L_{10}. L_6, L_7, and L_8 are not hot spots, and L_9 is not a cold spot in Fig. 7(a). But they are identified as hot spots and cold spots, respectively, in Fig. 7(b).

Table 1 Summarization of regions R_1-R_5 and calculated signal variance

Region	Connected pins	Present activity	Range of signal variance
R_1	Data output	Active	[0.8712, 1.0000]
R_2	Address bus	Active	[0.7955, 0.9103]
R_3	Silicon die	Active	[0.8339, 0.8821]
R_4	N.C.*, EXEC*	Inactive, active	[0.6818, 0.8014]
R_5	Data input	Inactive	[0.0000, 0.2052]

*N.C.: denotes not connected, *EXEC: execution signal for cryptographic core

Table 2 Results of two methods at locations L_1-L_{10}

EMA results Corr., MTD, Loc.*	**Proposed** Loc.,Signal Var.*	**Method[10]** Loc.,Peak.Amp.*
0.2113, 3218, **L_1(28,28)**	**L_1**, 1.0000	L_1, 1.0000
0.1989, 3590, **L_2(27,01)**	**L_2**, 0.9103	L_7, 0.9762
0.1896, 4713, **L_3(13,16)**	**L_3**, 0.8821	L_8, 0.9215
0.1783, 5421, **L_4(05,02)**	**L_4**, 0.8014	L_6, 0.8819
0.1715, 5986, **L_7(14,17)**	**L_7**, 0.7380	L_3, 0.8734
0.1290, 6495, **L_{10}(11,08)**	**L_{10}**, 0.4979	L_2, 0.8246
0.1161, 7542, **L_6(24,11)**	**L_6**, 0.3015	L_4, 0.7043
0.1032, 8270, **L_9(26,14)**	**L_9**, 0.2928	L_5, 0.5921
0.0797, 9251, **L_8(04,16)**	**L_8**, 0.1276	L_{10}, 0.2852
0.0634, 9982, **L_5(02,27)**	**L_5**, 0.0000	L_9, 0.0000

* Corr., MTD, Loc.: correlation coefficient, MTD, and location, respectively
* Loc.,Signal Var.: location and signal variance, respectively
* Loc., Peak.Amp.: location and peak-to-peak amplitude, respectively

Table 3 Accuracy calculations for the two methods at scanning area

EMA results Corr., MTD, Loc.*	**Proposed** Loc., Signal Var.*	**Method[10]** Loc., Peak.Amp.*
0.2113, 3218, **(28,28)**	**(28,28)**, 1.0000	(28,28), 1.0000
0.2082, 3365, **(28,27)**	**(28,27)**, 0.9791	(28,27), 0.9923
0.2016, 3380, **(27,28)**	**(27,28)**, 0.9348	(28,26), 0.9881
0.2001, 3417, **(26,28)**	**(26,28)**, 0.9250	(27,28), 0.9642
0.1998, 3428, **(24,28)**	**(25,28)**, 0.9187	(28,25), 0.9576
…	…	…
0.0672,9680, **(01,25)**	**(01,25)**, 0.0236	(26,12), 0.2454
0.0663,9762, **(01,26)**	**(01,26)**, 0.0187	(25,13), 0.1730
0.0659,9775, **(02,28)**	**(02,28),** 0.0158	(25,14), 0.1326
0.0657,9831, **(01,27)**	**(01,27),** 0.0104	(26,13), 0.0578
0.0634,9982, **(02,27)**	**(02,27),** 0.0000	(26,14), 0.0000
Accuracy	**573/784≈73.1%**	**192/784≈24.5%**
Improved Accuracy	**73.1%-24.5%= 48.6%**	

* Corr., MTD, Loc.: denotes correlation coefficient, MTD, and location, respectively
* Loc.,Signal Var.: denotes location and signal variance, respectively
* Loc., Peak.Amp.: denotes location and peak-to-peak amplitude, respectively

To verify whether these hot spots shown in the above two leakage maps are true or not, EMA at 784 locations is performed. Hamming Distance model is used. Correlation coefficients between the signal traces and hypothesized leakage of the output of s-boxes in the final round are calculated to reveal each subkey. In terms of correlation-based attacks, the correlation coefficient corresponding to the correct key guess represents data dependence and determines MTD. Thereby, the value of correlation coefficient corresponding to the correct key guess at each location is used to represent the performance of EMA. It is normalized to [0,1] and plotted in Fig. 6. The correlation coefficients of 10 locations L_1-L_{10}, are sorted and listed in descending order in the first column of Table 2. In a similar way, the signal variance obtained by the proposed method and peak-to-peak amplitude in[10] are also listed in descending order in Table 2. It is expected that the orders of leakage indicators (signal variance or peak-to-peak amplitude) are consistent with the orders of the results of

EMA. In this case, the method is accurate, and the leakage indicator correctly reveals the data dependence at each location.

Table 2 is the comparison of the two methods with the results of EMA at 10 locations. The orders determined by the proposed method agree well with the orders of correlation coefficients from EMA. EMA succeeds fastest at L_1, where the maximum correlation coefficient reaches 0.2113, and only 3218 MTD is required to detect secrete key. Both methods correctly predict that L_1 is a hot spot. However, EMA succeeds slower at L_7, L_6, and L_8 than at L_1, L_2, L_3, and L_4. The method in[10] is unable to reveal this relative relation. On the contrary, this is correctly indicated by the proposed method. In other words, the data dependence is misjudged by method[10], whereas the hot spots indicated by our proposed method are accurate.

To determine which leakage map (Fig. 7(a) or Fig.7 (b)) better agrees with Fig. 6, namely, to quantitatively evaluate the accuracy of proposed method and the method of peak-to-peak amplitude[10], we adopt a "sorting and consistency counting" approach for all the scanning points. Firstly, sorting, the correlation coefficients from EMA are ranged in descending order. The locations identified by the proposed method and method [10] are also sorted in descending orders according to the signal variance and peak-to-peak amplitude respectively. Secondly, consistency counting, for one location, if its order determined by one method matches with its order determined by EMA, then this location is counted as consistent, and that method is considered as accurate. If there is no match, the method is not accurate. Finally, the accuracies of the two methods are evaluated and listed in Table 3.

Table 3 shows the accuracy calculations for the two methods at the scanning area. The results indicate that the leakage map Fig. 7(a) calculated by the proposed method better fits Fig. 6. Most of the orders determined by the proposed method agree with the orders determined by EMA. The proposed method has an accuracy of 73.1%. By contrast, the orders calculated from method [10] appear to be inconsistent. Only 24.5% locations agree with the order determined by EMA. The accuracy of proposed method is improved by 48.6% compared with that of the method [10].

The above experiments confirm that signal variance accurately reveals the data dependence of encryption that leads to the success of EMA, and peak-to-peak amplitude suffers from misjudgments of data dependence. In addition, it is noted that the accuracies of the two methods are not as high as expected. There are several possible reasons.

The first possible reason is the influence of noise. Signal variance and peak-to-peak amplitude of EM emission are influenced by noise during signal acquisition. To show a naive result of the proposed method, only averaging of signal traces was adopted to attenuate surrounding noise in the above experiments. More sophisticated techniques can be applied to reduce noise during the preprocessing to improve the accuracy of these methods. A detailed discussion of noise sources and reductions can be found in [8, 9]. It is not iterated here.

The second possible reason is the accuracy calculation approach. The approach of "sorting and consistency counting" was used in the experiment to quantitatively compute the accuracy of these two methods. This is a strict evaluation approach. For higher accuracy, it requires a correct relative relation between the points around hot spots. However, it is fair to use it for evaluating these two methods, and it shows that the proposed method is more accurate.

4.2 Proposed EMA on protected module

WDDL proposed by Tiri and Verbauwhede [5], is a countermeasure in the family of Dual-rail with Precharge Logic (DPL) that attempts to make power consumption independent of manipulated data. However, as pointed out by Suzuki and Saeki[20], because of the flaw that there is leakage caused by the difference in delay time between input signals of WDDL gates, it is still vulnerable to SCA.

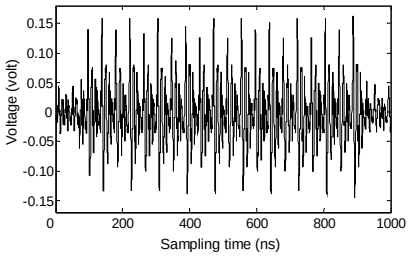


Fig. 9 Signal trace of AES WDDL at location (1,1)

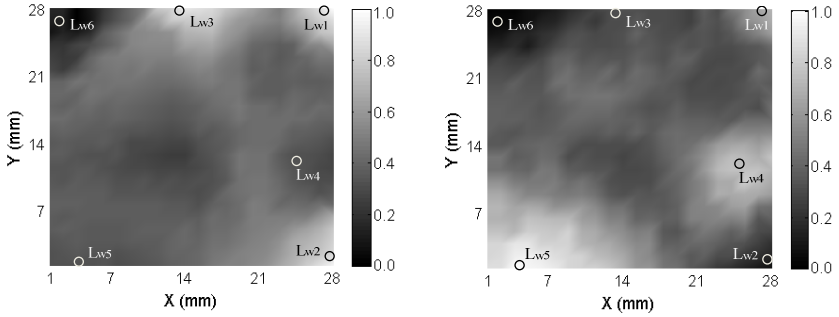


Fig. 10(a) Leakage map for WDDL calculated by proposed method (b) Leakage map for WDDL calculated with peak-to-peak amplitude[10]

Table 4 EMA results and two leakage indicators for AES WDDL at 6 locations

Loc.	Coordinates	MTD	Corr.	Proposed*	Method[10]*
Lw3	(14,28)	12,057	**0.0713**	**1.0000**	0.5205
Lw2	(28,02)	12,732	**0.0689**	**0.9732**	0.1814
Lw1	(27,28)	13,169	**0.0630**	**0.8874**	0.7829
Lw5	(04,01)	>20,000	**0.0302**	**0.4136**	1.0000
Lw4	(25,12)	>20,000	**0.0281**	**0.2912**	0.9816
Lw6	(02,27)	>20,000	**0.0154**	**0.0000**	0.0083

*Proposed: The signal variance is calculated and normalized
*Method[10]: The peak-to-peak amplitude is calculated and normalized

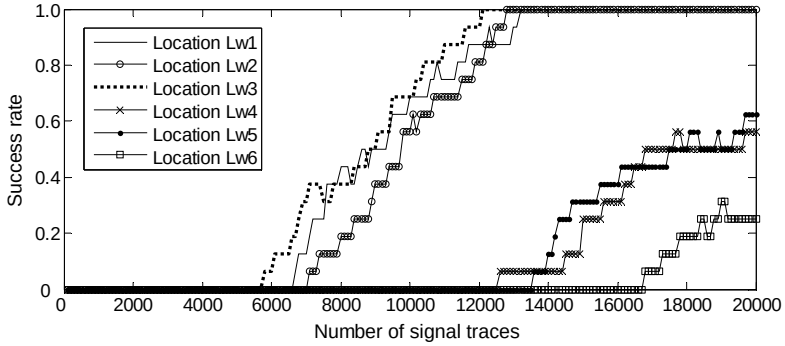


Fig.11 Success rates for AES WDDL at 6 locations

Table 5 MTD and maximal correlation for each s-box of AES WDDL at Lw3 and Lw5

S-box	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**
Lw3	**12,057**	6,739	8,806	9,503	**5,864**	11,127	9,104	10,274
	0.0713	0.0943	0.0848	0.0796	**0.1022**	0.0720	0.0815	0.0771
Lw5	**x***	14,031	19,436	x	**13,812**	x	19,815	17,523
	0.0302	0.0495	0.0342	0.0336	**0.0517**	0.0311	0.0340	0.0376
S-box	**S9**	**S10**	**S11**	**S12**	**S13**	**S14**	**S15**	**S16**
Lw3	9278	6,873	11,564	8,721	6,925	10,338	6,121	7,012
	0.0802	0.0921	0.0729	0.0867	0.0927	0.0765	0.0980	0.0913
Lw5	x	14,308	x	16,149	14,797	x	14,176	15,534
	0.0331	0.0429	0.0318	0.0382	0.0418	0.0324	0.0489	0.0407

* x: the subkey is not revealed with 20000 MTD

A near-field scan over the surface of LSI when AES WDDL runs, is conducted. 20000 samplings are acquired at each scanning point. A signal trace at (1, 1) is shown in Fig. 9. The 10-round encryption is shown by 20 peaks.

Signal variance at t = 887.1 ns in the final round of encryption for each point is computed and plotted in Fig. 10(a). A leakage map by computing peak-to-peak amplitude [10], is shown in Fig. 10(b). The hot spots in these two leakage maps are totally different. Three hot spots, Lw1, Lw2, and Lw3, are indicated by Fig. 10(a), while two other hot spots, Lw4 and Lw5 are revealed in Fig. 10(b). Their positions are further away from each other over the surface of LSI. The positions of hot spots Lw4 and Lw5 exhibit rather dark in Fig. 10(a). The cold spot Lw6 in Fig. 10(a) agrees with that in Fig. 10(b).

Correlation-based EMA at the 6 locations is performed to verify the hot spots. We are more interested in the correctness of the proposed method in the case of countermeasures. Therefore, instead of a strict "sorting and consistency counting" approach at all the scanning points to compare the accuracy, only sorting is used. The locations are shown in descending order according to the values of correlation coefficient, and the signal variance and peak-to-peak amplitude are also listed in Table 4. All the subkeys are revealed at Lw3, Lw2, and Lw1 within 20000 signal traces, but not at Lw5 and Lw4. Table 4 indicates that the values of signal variance agree well with the correlation coefficients at 6 locations.

Success rates of EMA at the 6 locations are shown in Fig. 11. It clearly displays that EMA succeeds faster at Lw3, Lw2, and Lw1. The success rate is 62.5%, namely, only 10/16 subkeys are recovered at Lw5 and 9/16 at Lw4 when signal traces reach 20000. In other words, Lw3, Lw2, and Lw1 are hot spots, but Lw5 and Lw4 are not. This is correctly indicated by the proposed method.

The results of EMA at Lw3 and Lw5 are shown in Table 5. The fastest guess for the key is the fifth s-box, where 5864 signal traces are required at Lw3 and 13812 signal traces at Lw5. The slowest guess is for the first s-box. Table 5 further demonstrates that EMA succeeds faster at Lw3

than at Lw5. This confirms that the proposed method correctly reveals this data dependence and predicts the possible leakage locations in the presence of WDDL.

It is noted that 10000 signal traces in section 4.1 and 20000 signal traces in section 4.2 are acquired for each scanning point. They are sufficient for this experimental configuration. The number of signal traces varies in terms of signal-to-noise ratio of a specific platform. For instance, if stronger countermeasures are applied, then the signal-to-noise ratio decreases, and more signal traces are required to compute signal variance.

Furthermore, a trigger signal is used to align the signal traces during signal acquisition in the experiments presented in section 4.1 and section 4.2. If other countermeasures, such as the insertion of random delays, are applied in the implementation, additional preprocessing techniques, such as phase-only correlation proposed by Homma et al.[21], are necessary to remove the displacements in signal traces.

5. Conclusions

In this paper, signal variance was proposed as an indicator for localizing hot spots over the surface of cryptographic LSI. It was proved as an equivalent metric to DoM in classical DEMA. Although signal variance does not reveal the specific locations of cryptographic modules by near-field scan, it is capable of identifying data-dependent EM emissions, which leads to the success of EMA. Blind placement is avoided, thus EMA is conducted accurately. Additionally, signal variance is also effective in finding leakage points when countermeasures are applied. Furthermore, a small and low-cost probe was made to verify the proposed method. The experiment of EMA against AES PPRM1 implementation revealed that misjudgments of the leakage are reduced and the accuracy is improved 48.6% compared with the method of peak-to-peak amplitude. The experiment on AES WDDL implementation demonstrated that a faster EMA is enabled under the guidance of signal variance. The performance of EMA is enhanced.

We have shown the richness of the information disclosed by signal variance based on near-field scan in the time domain, which is an effective tool to explore the secret of cryptographic LSI. In the future, with this tool, more features of EM emissions in the frequency domain will be studied to improve the performance of EMA.

Acknowledgment

The authors would like to thank Dr. Yuji Tanabe, Dr. Jiangtao Sun and Professor Toshihiko Yoshimasu for the discussion of related electromagnetic theory and probe making, etc. This work was supported by the “Global COE program” of MEXT and CREST of JST in Japan.

References

[1] K. Gandol, C. Mourtel, and F. Olivier: Electromagnetic analysis: concrete results, Proc. Workshop on Cryptographic Hardwar and Embedded Systems (CHES), LNCS, Vol. 2162, pp. 251-261, 2001.

[2] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi: The EM side channel(s), Proc. CHES 2002, LNCS, Vol. 2523, pp. 29-45, 2002.

[3] C. Gebotys, S. Ho and C. Tiu: EM analysis of Rijndael and ECC on a wireless Java-based PDA, Proc. CHES 2005, LNCS, Vol. 3659, pp. 250-264, 2005.

[4] E. Trichina: Combinational logic design for AES subbyte transformation on masked data, Cryptology ePrint Archive, 2003/236, 2003.

[5] K. Tiri and I. Verbauwhede: A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation, Proc. Design, Automation and Test in Europe Conference and Exposition (DATE 2004), pp. 246-251, 2004.

[6] T. Pop and S. Mangard: masked Dual-Rail Pre-charge Logic: DPA-resistance without routing constraints, Proc. CHES 2005, LNCS 3659, pp. 172-186, Aug. 2005.

[7] E. Peeters, F. X. Standaert, and J. J. Quisquater: Power and electromagnetic analysis: improved model, consequences and comparisons, Integration, the VLSI Journal, Vol. 40, Issue 1, pp. 52-60, 2007.

[8] T. H. Le, C. Servière, J. Cledière, and J. L. Lacoume: Noise reduction in the side channel attack using fourth order cumulants, IEEE Trans. Inf. Forensic Security, Vol. 2, No. 4, pp. 710-720, 2007.

[9] H. Liu, Y. Tsunoo, and S. Goto: Electromagnetic analysis enhancement with signal processing techniques, Proc. 16th Australasian Conference on Information Security and Privacy (ACISP 2011) LNCS, Vol. 6812, pp. 456-461, 2011.

[10] L. Sauvage, S. Guilley, and Y. Mathieu: Electromagnetic radiations of FPGAs high spatial resolution cartography and attack on a cryptographic module, ACM Trans. Reconfigurable Technology and Systems, Vol. 2, No. 1, pp. 4-24, 2009.

[11] S. P. Skorobogatov: Semi-invasive attacks-a new approach to hardware security analysis, Technical Report UCAM-CL-TR-630, University of Cambridge, Computer Laboratory, April, 2005.

[12] J. J. Quisquater and D. Samyde: Electromagnetic analysis (EMA): measures and countermeasures for smart cards, Smart Card Programming and Security (E-smart 2001), Springer-Verlag, LNCS, Vol. 1240, pp. 200-210, 2001.

[13] IEC 61967-3: Integrated circuits-measurement of electromagnetic emissions, 150 kHz to 1 GHz-Part 3: measurement of radiated emissions, surface scan method (10 kHz to 3 GHz), 47A/620/NP, New Work Item Proposal, Date of proposal: Jul. 2001.

[14] P. Kocher, J. Jaffe, and B. Jun: Differential power analysis, advances in cryptology, Proc. CRYPTO 99, LNCS, Vol. 1666, pp. 388-397, 1999.

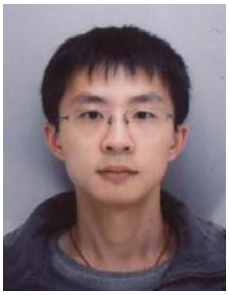
[15] Research Center for Information Security (RCIS) of AIST: Side-channel attack standard evaluation board (SASEBO)-R, http://staff.aist.go.jp/akashi.satoh/SASEBO/en/board/sasebo-r.html.

[16] S. Guilley, L. Sauvage, P. Hoogvorst, R. Pacalet, and G. M. Bertoni: Security evaluation of WDDL and SecLib countermeasures against power attacks, IEEE Trans. Computers, Vol. 57, No. 11, pp. 1482-1497, 2008.
[17] F. X. Standaert, T. G. Malkin, and M. Yung: A formal practice-oriented model for the analysis of side-channel attacks, Cryptology ePrint Archive, Report 2006/139, http://eprint.iacr.org (2006).
[18] Research Center for Information Security (RCIS) of AIST: Standard cryptographic LSI specification-with side channel attack countermeasures -Ver.1.0, http://staff.aist.go.jp/akashi.satoh/SASEBO/en/board/crypto_lsi.html.
[19] J. M. Schmidt, T. Plos, M. Kirschbaum, M. Hutter, M. Medwed, and C. Herbst: Side-channel leakage across borders, Proc. the ninth Smart Card Research and Advanced Application IFIP Conference (CARDIS 2010), LNCS 6035, pp. 36-48, 2010.
[20] D. Suzuki and M. Saeki: Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style, Proc. CHES 2006, LNCS Vol. 4249, pp. 255-269, 2006.
[21] N. Homma, S. Nagashima, T. Sugavara, T. Aoki, and A. Satoh: A high-resolution phase-based waveform matching and its application to side-channel attacks, IEICE Trans. Fundamentals., Vol. 1, E91-A, pp. 193-202, 2008.

Hongying Liu received her B.E. and M.S. degrees in Computer Science and Technology from Xi'An University of Technology, China, in 2002 and 2006, respectively. She participated in several major projects when pursued her M.E. degree, such as the National High Technology Research and Development Program of China ("863" Program). She is a member of IEEE. Currently, she is a Ph.D candidate in the Graduate School of Information, Production and Systems, Waseda University. Her major research interests include information processing, information security, signal processing etc.

Yukiyasu Tsunoo received his B.E. degree from Waseda University in 1982, M.S. degree from JAIST, and Dr. of Eng. from Chuo University. He joined NEC Software Hokuriku, Ltd. in 1985. He is now a Research Fellow of Information and Media Processing Laboratories, NEC Corp, and he has engaged in the design of common key ciphers and the study of evaluation techniques. He is a member of the Expert Commission of Information Security Research, IEICE, the Information Processing Society of Japan, and the Japan Society for Security Management and the Atomic Energy Society of Japan.

Yibo Fan received his B.E. degree in electronics and engineering from Zhejiang University, China, in 2003 and M.S. degree in Micro-electronics from Fudan University, China, in 2006 and Dr. degree in engineering from Waseda University, Japan in 2009. Currently, he is an assistant professor in State-Key lab of ASIC & System in Fudan University. His research interests include information security, video coding and VLSI Design.



Bin Hu received his B.E. degree in electronic engineering from Beijing Tsinghua University, China, in 2007 and entered the Graduate School of Information, Production and Systems, Waseda University, Japan, for his Master degree in 2010. His research interests include information security, cryptanalysis and physical unclonable functions.

Satoshi Goto received the M.S. degree and Dr. degree in electronics and communication engineering from Waseda University, Japan, in 1970 and 1981, respectively. He is currently a Professor with the Graduate School of Information, Production, and Systems, Waseda University, Kitakyushu, Japan. He joined NEC Laboratories in 1970, where he worked on LSI design, Multimedia System and Software. His current research interests include system LSI design methodology and new design tools for multimedia processing, and networking functions with security or cryptography for the Next Generation Internet and Super Internet. He has served on numerous conference committees. He was a member of the Board of Director of the IEEE Circuits and Systems. He is also an IEICE Fellow.

(Received November 21, 2011; revised March 1, 2012)