Authentication Using Side-Channel Information

Kazuo Sakiyama[1], Takanori Machida[1], Arisa Matsubara[1], Yunfeng Kuai[1], Yu-ichi Hayashi[2], Takaaki Mizuki[3], Noriyuki Miura[4], and Makoto Nagata[4]

[1] The University of Electro-Communications, Tokyo, Japan
{sakiyama, machida, matsubara, kuaiyf}@uec.ac.jp
[2] Tohoku Gakuin University, Sendai, Japan
yu-ichi@mail.tohoku-gakuin.ac.jp
[3] Tohoku University, Sendai, Japan
tm-paper+eprint2015@g-mail.tohoku-university.jp
[4] Kobe University, Kobe, Japan
{miura, nagata}@cs.kobe-u.ac.jp

Abstract. Authentication based on cryptographic protocols is a key technology for recent security systems. However, the so-called relay attack where a malicious attacker tries to assume the role of the prover, is known to be a serious threat even for the cryptographically-secure authentication systems. This paper proposes a new authentication method that utilizes the side channel that already exists in many authentication systems. The side channel has been studied intensively from the attacker viewpoint, and it is best known for the key-recovery attack against cryptographic implementations via physical information. Here, reversing our way of thinking, we propose to use the information constructively via the side channel to enhance the existing cryptographic protocols. Using symmetric-key-based authentication as an example, we show based on experiments using an FPGA that each of the side-channel information leaked from provers is unique enough for the purpose of authentication.

Keywords: side-channel analysis, relay attacks, two-factor authentication

1 Introduction

This paper proposes a new authentication technique called *side-channel authentication* that utilizes the side-channel information as a device fingerprint. Since the side-channel information leaked during the operation of a cryptographic algorithm is identical for each secret key, it can be used to identify multiple provers that simply operate a secret-key-dependent operation, *e.g.,* AES encryption. It is worth mentioning that no additional special circuits such as PUFs (Physical Unclonable Functions) and Trojans, are needed in the proposed side-channel authentication method. To our best knowledge, this is the first proposal employing the side-channel information in cryptographic authentication protocols.

The main features of the proposed side-channel authentication method are summarized below:

- It bounds the communication distance between the verifier and the prover; hence, it could be a practical countermeasure to relay attacks.
- The prover devices do not require any change as far as they can generate identical side-channel information depending on their own keys.
- The side-channel information is analog data, *e.g.,* power consumption and electromagnetic radiation.
- The measurement noise, which is dependent on factors such as the quality of the employed side-channel probe, measurement distance between the probe and target, and environmental noise, strongly affects the side-channel information.

We assume that it is difficult for an attacker attempting a relay attack to generate a copy of the side-channel information that is indistinguishable from the original.

1.1 Relay Attacks

Authentication between two parties, prover and verifier, is an initial procedure to give permission so that the prover can enjoy some service. It is often used to log into a system or enter a restricted area. Recently, small devices or tags using radio frequency identification (RFID) technology enable us to accelerate the wireless authentication process. The amount of data transmitted between the RFID tag (prover) and reader (verifier) is usually just a few hundred bits, which attracts attackers to launch man-in-the-middle (MITM) attacks, where the attacker eavesdrops on the communication on a secure channel, and manipulates it without the knowledge of the two parties. The relay attacks, discussed in the following, are one type of MITM attacks.

Suppose that the verifier sends challenge c to the prover who has secret data sk and the prover performs a one-way function f on c to return $f(c, sk)$ to the verifier. The verifier checks the value of $f(c, sk)$ against the database, and identifies the prover. In a replay attack, the attacker eavesdrops on the communication data between the prover and the verifier. If the challenge c is repeatedly used in different authentication trials, the attacker can impersonate the prover by recording $f(c, sk)$ and sending it back to the verifier in an appropriate length of time, t, after observing c. In this way, the success of the replay attack is based on two types of information; the duplication of the digital data, $f(c, sk)$, and the short response time, t. Therefore, in order to counteract the attack, the challenge should not be repeated and the response time must be checked. That is, as a simple countermeasure, the verifier sends random challenge c_r for each authentication, and checks whether or not the arrival time of $f(c_r, sk)$ is shorter than a pre-determined threshold. Note that the threshold value is closely related to the trade-off between security and usability of the system, which could lead to setting a high threshold value.

In a relay attack scenario where the prover is located separately from the verifier, the attacker can still successfully achieve authentication even against the above mentioned countermeasure. The attacker launches two high-speed transponders nearby the prover and verifier. One transponder on the verifier

side eavesdrops on c_r, and forwards it to the other transponder placed near the verifier. The value of c_r transmitted to the prover is performed as a challenge, and the prover outputs $f(c_r, sk)$. The response, $f(c_r, sk)$, is sent back to the verifier via the two transponders. That is, regardless the position of the prover, the authenticated channel could be constructed as if the prover and the verifier are sufficiently close for authentication. Thus, the relay attack is feasible if the arrival time of $f(c_r, sk)$ is shorter than the threshold value. Note that, in the case that when the prover and the verifier are relatively close, *e.g.,* a few meters, a wireless repeater that extends the range of the communication area could be replaced with the transponders. Such an attack scenario is simpler and faster in terms of the communication overhead compared to the scenario with transponders that require analog-digital and digital-analog conversions.

Under these circumstances, there are several countermeasures for the relay attack [4, 2, 17]. They are basically based on the idea of the distance-bounding protocol [1] in which the upper-bound on the distance between the prover and the verifier is checked by a single-bit challenge and rapid single-bit response.

1.2 Side-Channel Analysis

Side-channel analysis can utilize the physical information leaked from a cryptographic device, and is often used to retrieve the secret key. In other words, side-channel analysis research has been focused on the key-recovery attacks on cryptographic algorithms since it was proposed in [6] and [7].

Recently, several papers discussed intentional induction of the side-channel information. In [10], the concept of Trojan side-channels was first proposed. Hardware Trojans denote a malicious circuit implemented in a device, and they perform unintentional operations such as disabling security protection and leaking sensitive information. In [5], using Trojan side-channels was proposed in which side-channel leakage could be used as a building block for Trojan circuitry. They implemented a Trojan circuit using less than 100 gates that intentionally induces physical side-channel information leakage to convey secret information.

2 Overview: Side-Channel Authentication

The most straightforward method using side-channel authentication assumes that physical information leaked from a device is used as side-channel information in addition to a pair comprising a challenge and response transmitted over a conventional communication channel. Three additional types can be considered for a side-channel authentication method depending on whether or not the challenge and/or response is transmitted over the conventional communication channel. In this section, four different authentication methods are proposed and their advantages and disadvantages are discussed in detail.

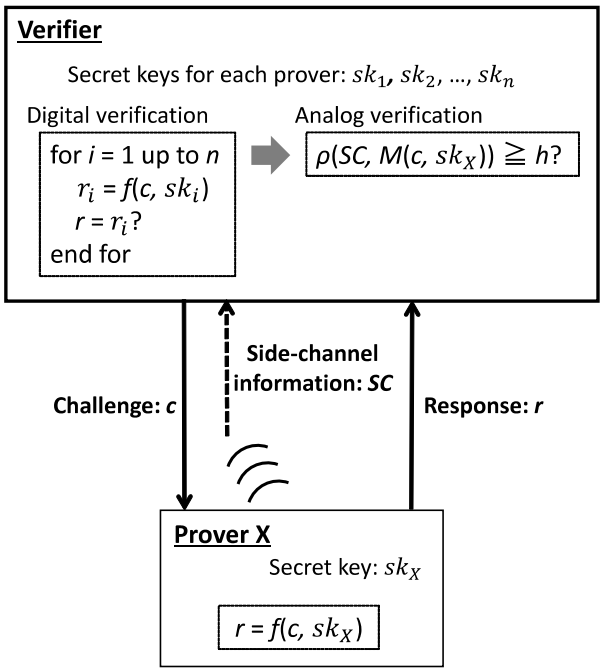


Fig. 1. Challenge-SC-response authentication method

2.1 Challenge-SC-Response Authentication

In the *challenge-SC-response authentication*, the verifier checks the side-channel information in addition to the conventional challenge-response verification. Accordingly, this authentication is regarded as a kind of two-factor authentication scheme.

As shown in Fig. 1, the verifier first sends challenge c to the prover X. For simplicity, we assume that f is an AES encryption. The prover performs AES encryption using c and its unique secret key, sk_X, as $r = f(c, sk_X)$. We assume that multiple provers are registered in the database of the verifier, and each prover has a different secret key that is pre-shared with the verifier. Therefore, in order to verify prover X, the verifier must perform $r_i = f(c, sk_i)$ and compare r_i to the received response, r, as many times as there are registered provers. The above procedure is denoted as *digital verification*. If the prover is identified by digital authentication, the verifier performs *analog verification* to confirm the validity of the side-channel information (SC) that is obtained during the computation of the prover X. Note that the analog verification is a newly proposed step in addition to the conventional challenge-response authentication. Namely, both digital and analog information are verified in the challenge-SC-response method.

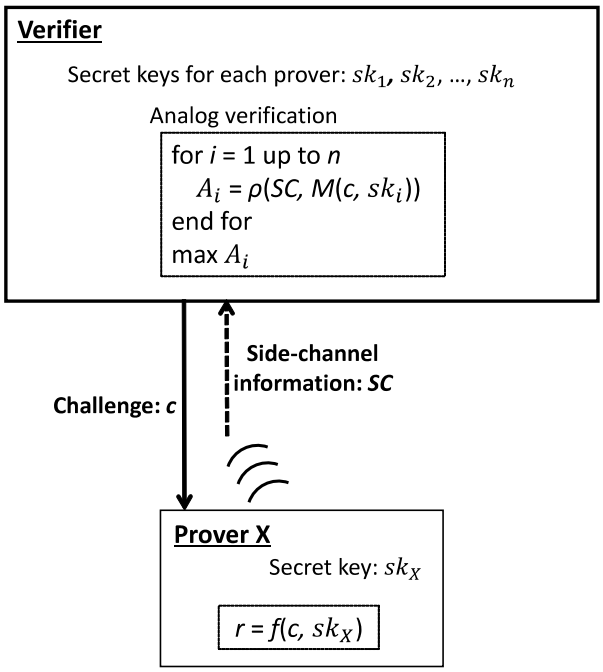


Fig. 2. Challenge-SC authentication method

Let SC be the side-channel information leaked from the prover at time t during the computation of challenge c with device-identical information sk, *e.g.*, secret key of AES. Since the side-channel information is strongly influenced by the system environment between the prover and the verifier, SC can be expressed as leakage function L as $SC = L(t, c, sk, N)$, where N is the measurement noise that usually follows a normal distribution. The verifier prepares roughly-modeled side-channel information based on a leakage model[5] as $M(c, sk_X)$, and checks whether or not the correlation between SC and $M(sk_X, c)$ is sufficiently high. More precisely, Pearson's correlation coefficient, $\rho(SC, M(sk_X, c))$, is evaluated if it satisfies predetermined threshold h. In order to reduce the noise, the verifier could use several challenges to perform side-channel analysis on multiple sets of side-channel information.

2.2 Challenge-SC Authentication

For the second method, the prover only returns SC corresponding to the challenge, c, as shown in Fig. 2. The so-called *challenge-SC authentication* assumes

[5] Hamming weight and Hamming distance of the intermediate values of $r = f(c, sk_X)$ are well-known leakage models.

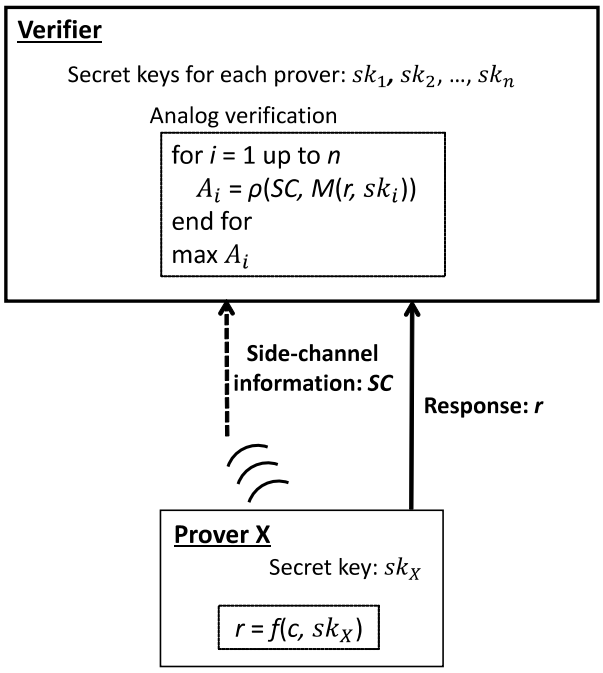


Fig. 3. SC-response authentication method

that SC contains sufficient information to identify prover X without digital response r. The prover is not required to send response r, which simplifies the communication between the verifier and the prover. It is true that the challenge-SC authentication requires more computations for the verifier since $\rho(SC, M(c, sk_i))$ should be performed as many times as there are provers stored in the database. However, it is considered that millions of provers can be handled without significant time overhead using the recent computational power for such signal processing.

2.3 SC-Response Authentication

In the third type, denoted as *SC-response authentication*, the verifier does not send a challenge, but receives response r from the prover as shown in Fig. 3. The prover can calculate the response, $r = f(c, sk_X)$; hence, the verifier cannot identify the prover using only r. However, the verifier can perform analog authentication using SC and r . More precisely, the verifier performs $\rho(SC, M(r, sk_i))$ when searching for the secret key of the prover. Note that the number of computations is the same as that for the challenge-SC authentication since calculation of the intermediate values is considered the same, *i.e.,* encryption and decryption of AES requires almost the same amount of calculation.

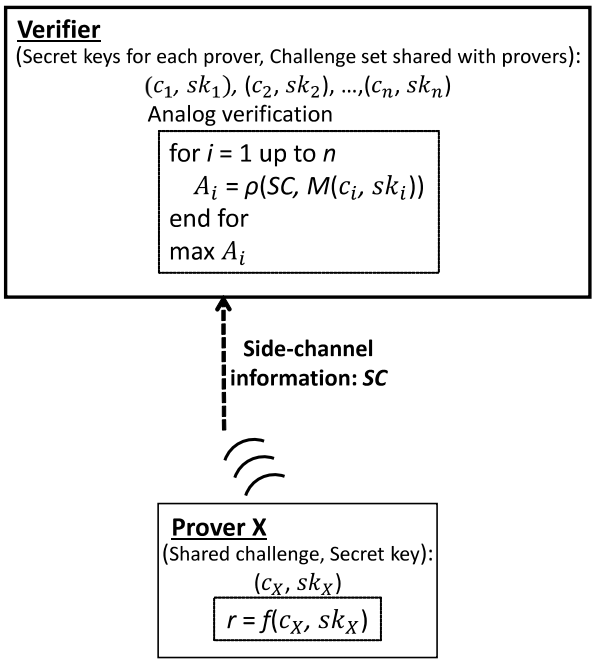


Fig. 4. Only-SC authentication method

2.4 Only-SC Authentication

In the fourth authentication method, the verifier neither sends a challenge nor receives a response, and only SC is checked on the verifier side as shown in Fig. 4. In *only-SC authentication*, it is assumed that the set of challenges is shared beforehand with the prover in addition to the secret key. The great advantage of the only-SC authentication is that no digital communication channel is needed between the prover and the verifier. Therefore, even a device without any wireless communication functions can be used as a prover.

The verifier searches for prover X from the database by performing $\rho(SC, M(c_i, sk_i))$. The only-SC authentication method requires more computations compared to the challenge-SC and SC-response authentication methods if provers store multiple challenges. Note that, as far as when the symmetric-key ciphers are used[6], the only-SC authentication method makes the key-recovery attack extremely difficult since the attackers must obtain the value of the challenge or response to derive the modeled leakage values. Table 1 summarizes the features of the four authentication methods.

[6] As for the public-key cryptography such as RSA, it is known that simple power analysis on a naive modular exponentiation algorithm can reveal the private key from only side-channel information.

Table 1. Comparison of proposed authentication methods

Methods \ Features	Challenge	Response	Verifier computation	Conventional channel
Challenge-SC-Response	✓	✓	$r = f(c, sk_i)$	Verifier ⇔ Prover
Challenge-SC	✓		$\rho(\mathrm{SC}, M(c, sk_i))$	Verifier ⇒ Prover
SC-Response		✓	$\rho(\mathrm{SC}, M(r, sk_i))$	Verifier ⇐ Prover
Only-SC	(Pre-Shared)		$\rho(\mathrm{SC}, M(c_i, sk_i))$	None

3 Preliminary Experiments Using AES

We clarify that the side-channel information leaked from each prover device with different secret key is sufficiently unique to distinguish it from other prover devices.

3.1 Overview

Here, we assume that side-channel authentication is based on near-field wireless communication, and therefore the verifier can obtain electromagnetic (EM) radiation as side-channel information. Signal switching in the prover device is the source of EM radiation. Since the switching activities are dependent on the intermediate values in the operation of the prover, the Hamming distance (HD) of intermediate values is correlated with the EM radiation in general. In fact, correlation EM analysis (CEMA), one of the existing side channel attacks using HD values, recovers the secret key in AES hardware. Therefore, our experiments on the side-channel authentication also employ CEMA. Note that, in side-channel authentication, all the round keys are available to the verifier, which is an unequivocal advantage for the verifier in performing CEMA.

The procedure in our experiments for the EM-based side-channel authentication is summarized as follows[7].

- 128-bit AES encryption hardware is implemented in a prover device.
- Assuming that the only-SC authentication method is employed, the prover and the verifier share a pair of challenges and a secret key that is different from one prover to another.
- The verifier calculates intermediate values of AES based on the challenge and secret key for all registered provers, and prepares the HD of intermediate values at a specific target round as a leakage model.
- The prover is located nearby the verifier, and starts encrypting the challenge with the secret key when triggered by a start signal[8].

[7] It is based on the concept of power-based side-channel reported in [12]

[8] We send the signal by pushing a button on the prover device. However, this can be substituted for other signals such as a near-field beacon generated by the verifier.

- The verifier obtains EM radiation as side-channel information during the prover AES encryption.
- The verifier derives correlation coefficients between the EM radiation trace at target timing, t_a[9], and prepars HD values.
- The verifier compares the correlation coefficients, and identifies or rejects the prover.

In the experiments, we assume that several challenges are pre-shared between the verifier and each prover, and the authentication capability is measured with the correlation coefficients for different numbers of EM traces[10].

3.2 Experimental Parameters

Table 2 summarizes the information regarding the prover device and equipment for the preliminary experiment. A 128-bit AES-comp, *i.e.,* AES with a composite-field S-box module, is implemented on Altera Cyclone IV, which is the main device on a Terrific DE0-nano FPGA board. It is operated at 50 MHz. EM radiation from the prover is captured with an oscilloscope via an EM prove and stored as EM trace.

In order to clarify whether or not the verifier appropriately recognizes side-channel information appropriately, first, the correct key (a key registered with the verifier) and an incorrect key (another key that is not registered with the verifier) are set to the FPGA.

3.3 Results of Experiments

When using multiple EM traces, alignment of the time axis is essential to perform CEMA. In the first step, it is assumed that a digitalized trigger signal that precisely indicates the start of AES encryption precisely is available in the experiment. However, such a trigger signal does not necessarily exist in a real system. Therefore, another experiment is performed without a trigger signal.

Table 2. Experimental parameters

FPGA board	Terasic DE0-nano
FPGA	Altera Cyclone IV
Implementation	128-bit AES (S-box module: composite field)
Operation frequency of AES	50 MHz
EM prove	Langer EMV-TECHNIK (SN: 02-1076)
Oscilloscope	Agilent DSO7032A (350 MHz, 2 GSa/s)
Amplifier	Miteq P/N AU-3A-0150-1179

[9] We assume that t_a can be determined with the configuration of the prover device.

[10] It is also possible to increase the number of rounds instead of using multiple AES encryptions with different challenges.

Results with Trigger Signal The experiments confirm the error occurrence rates of a simple side-channel authentication with the EM traces aligned according to the trigger signal. When the correlation coefficient is higher than the threshold, the verifier presumes that the prover device has the correct key and accepts it. In this experiment, authentication trials are repeated 100 times with 100, 200, and 400 challenges that are randomly chosen from 500 pre-shared challenges. When the prover device has the correct key, the error occurrence rate is evaluated with the false rejection rate (FRR) for different threshold settings. For the prover with an incorrect key, the false acceptance rate (FAR) is used.

The experimental results are shown in Fig. 5. The figures show that as the number of EM traces increases, the curves for the error occurrence rate shifts to the right and left for FRR and FAR, respectively, *i.e.,* the authentication capability is improved. The experimental results based on 200 EM traces indicate that distinguishing two prover devices is feasible if the threshold is set from 0.20 to 0.27.

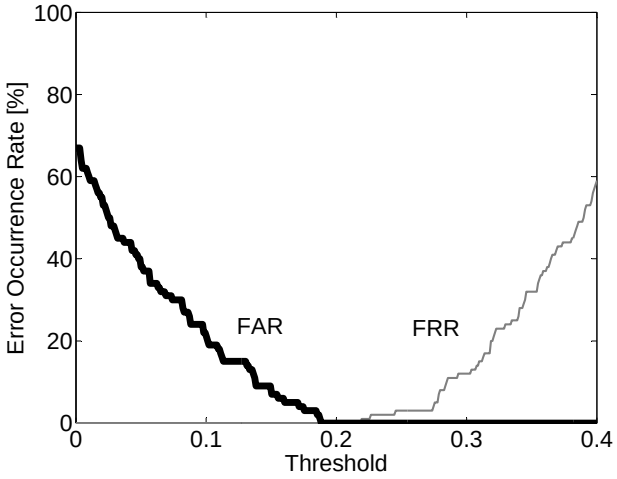
Results without Trigger Signal The same experiments are performed assuming that there is no special trigger signal. In order to achieve reasonable alignment, the fluctuation in the EM traces at the start of the AES encryption is used due to the fact that the intensity of the EM radiation becomes strong during AES encryption. This can easily be achieved with the trigger function of the oscilloscope.

The error occurrence rate with the threshold as a parameter is shown in Fig. 6. Compared to the results in Fig. 5, the authentication capability in Fig. 6 is slightly worse for 100 and 200 EM traces. This is because the correlation coefficients tend to be low for the prover devices with and without the correct key (see Figs. 7(a) and 7(b).) However, distinguishing two prover devices is still feasible by setting the threshold from 0.19 to 0.21 even with 200 EM traces.

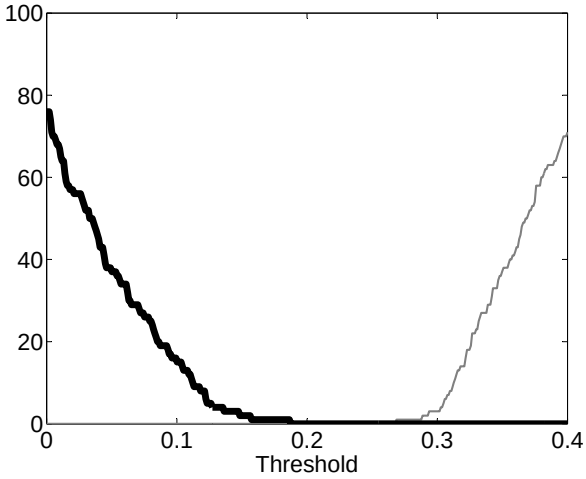
Results with Fourier Transform Another way to adjust the alignment is to apply the Fourier transform to the EM traces. Since DEMA can be performed in the frequency domain, it becomes unnecessary to apply the time alignment to the EM traces. Figure 8(a) shows the correlation coefficient spectrum in the frequency domain using 200 EM traces, where it is clear that the coefficient values are considerably high up to 200 MHz. Figure 8(b) shows the correlation coefficients derived with side-channel information at the frequency of 26.7 MHz. When comparing the results shown in Figs. 7(a) and 7(b), we find that CEMA in the frequency domain could be of use in our experiments for the side-channel authentication.

4 Toward Efficient Side-Channel Authentication

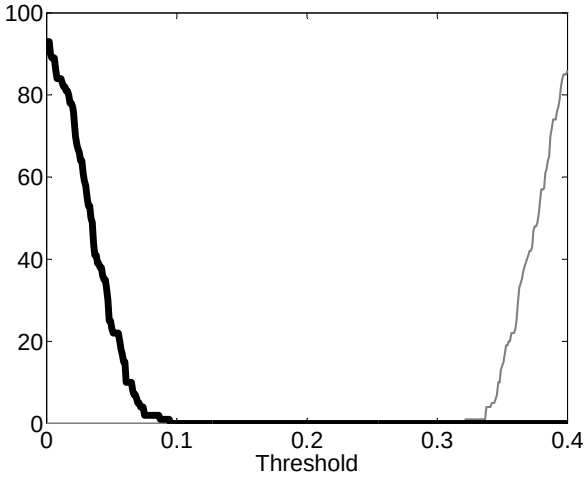
Following the preliminary experiments, this section explores three possible fundamental techniques to enhance the efficiency of the side-channel authentication.



(a) 100 EM traces

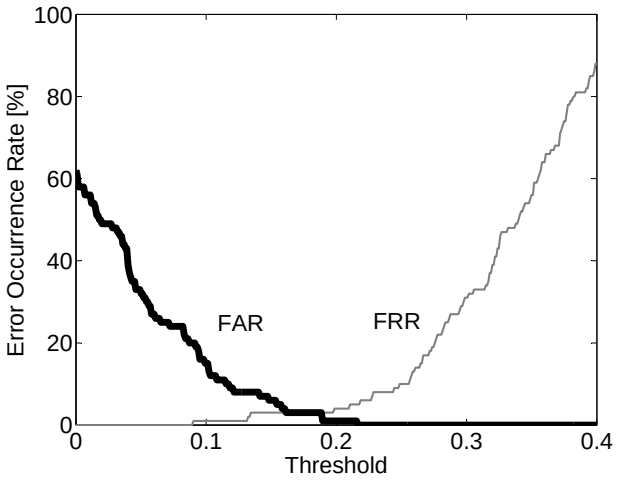


(b) 200 EM traces

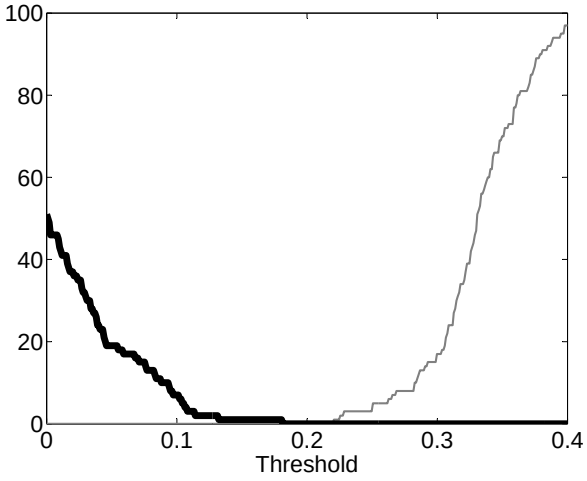


(c) 400 EM traces

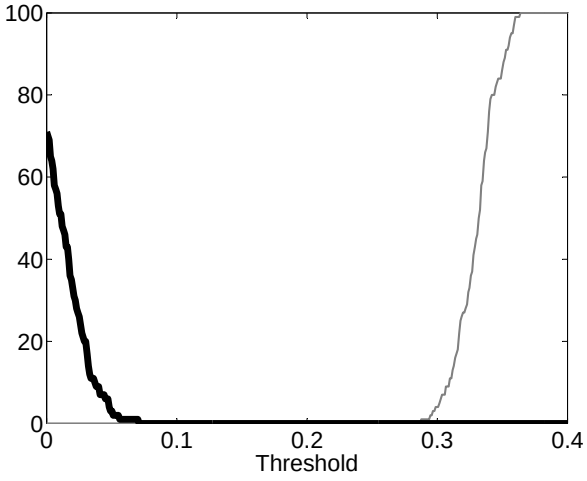
Fig. 5. Error occurrence rate when EM traces are captured with trigger signal



(a) 100 EM traces

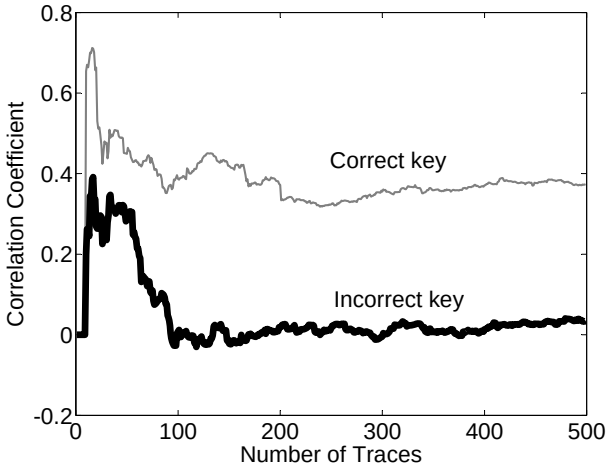


(b) 200 EM traces

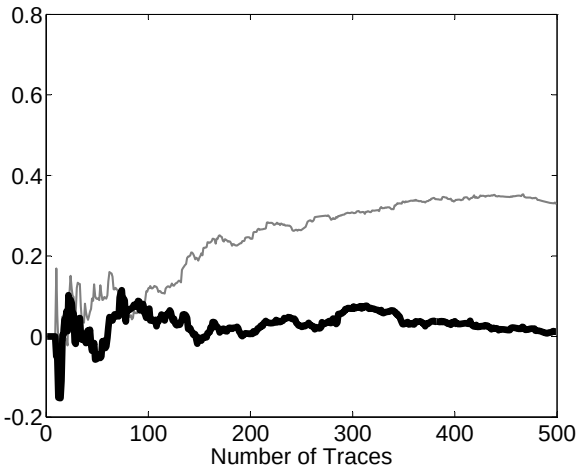


(c) 400 EM traces

Fig. 6. Error occurrence rate when EM traces are captured without trigger signal

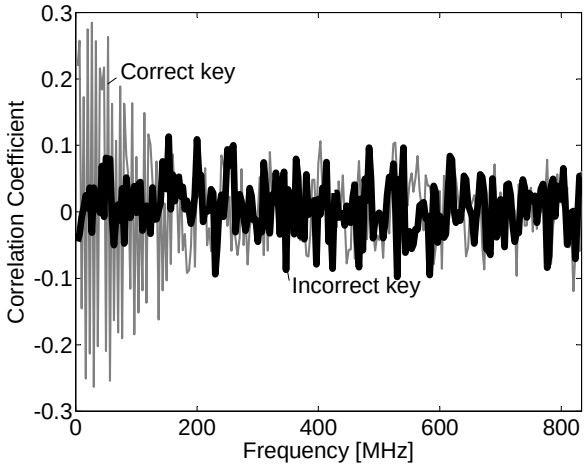


(a) Alignment with trigger signal

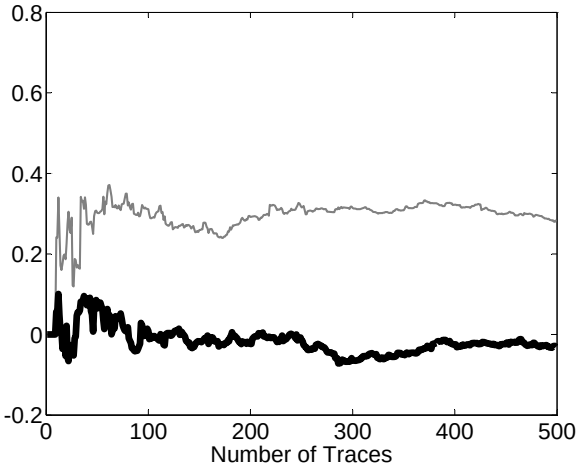


(b) Alignment with rising edge of EM traces

Fig. 7. Correlation coefficient for the number of EM traces



(a) Correlation coefficient in the frequency domain



(b) at 26.7MHz

Fig. 8. Analysis in the Fourier domain

4.1 Manipulating Side-Channel Information

When employing the so-called loop architecture, where AES hardware that operates one round operation per cycle, the AES state of the round input is stored in 16 one-byte or 128-bit registers, and the output values of the round operation are written over the AES state. Due to the ShiftRows transformation, the positions of the diagonal 4 bytes are shifted as highlighted in Fig. 9. It is known that the power consumption of AES-comp with the loop architecture becomes prominent when the number of input bytes of two consecutive cycles are totally equal, *i.e.,* HD = 0, which is called Clockwise Collision (CC) [9]. When CC occurs, there are almost no signal transitions in the combinatorial circuit. Therefore, the intensity of the EM radiation also becomes weak when CC occurs, and it becomes weaker as the number of CCs increases.

Muzuki and Hayashi proposed an algorithm to find a plaintext that induces CCs in all registers at the final round of AES, and confirms the outstanding feature called *quiet* in the corresponding EM radiation [13]. The motivation of this work was mainly to ease the security evaluation for cryptographic hardware. Since analysis in the side-channel authentication is common to security evaluation, the manipulation technique can be used as an effective way to improve the efficiency of the side-channel authentication.

Therefore, as an extension of the idea of [13], we propose an algorithm to manipulate the EM radiation in an arbitrary round of the AES-comp hardware based on the preliminary work proposed in [8].

The algorithm in [8] is briefly reviewed here. We denote the number of registers of AES in Fig. 9, and the four bytes highlighted in white and grey colors correspond to the input and output of Mixcolumns. Namely, the round input values of registers $(0, 5, a, f)$ affects the round output values of registers $(0, 4, 8, c)$ [14].

First, in order to induce a CC in register 0, we try all the possible input values for registers $(0, 5, a, f)$, and obtain the corresponding output values of registers $(0, 4, 8, c)$. We expect that CC occurs at register 0 with the probability of 2^{-8}; hence, 2^{24} input values will survive. In the same way, we induce CCs at

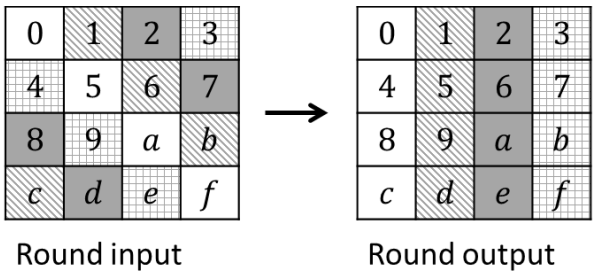
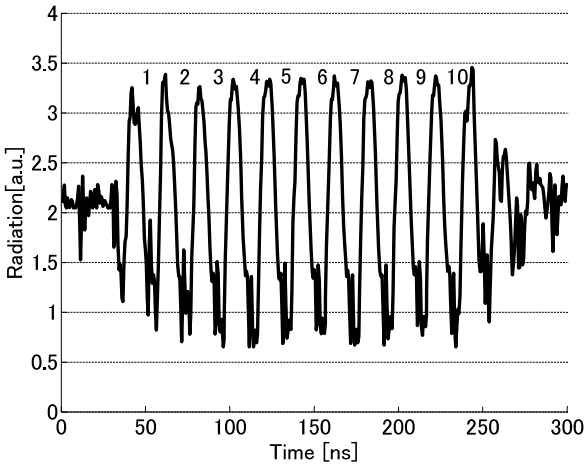
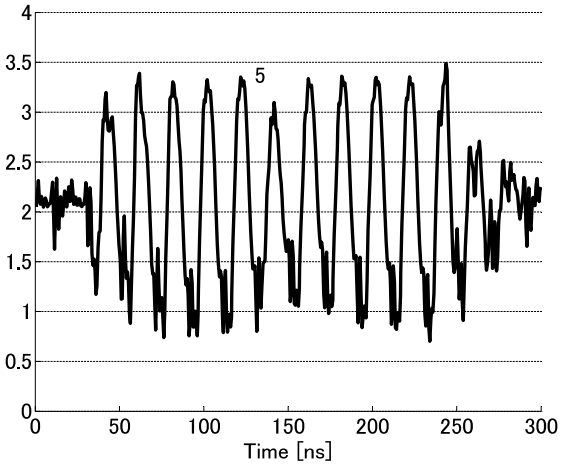


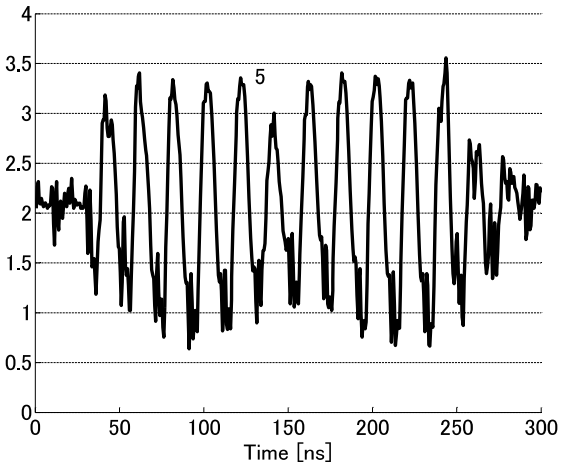
Fig. 9. States of AES for a round operation. Numbers correspond to the byte position of the flip-flops in AES hardware.



(a) Number of CCs is 0



(b) Number of CCs is 15



(c) Number of CCs is 16

Fig. 10. Electromagnetic (EM) radiation during AES encryption when the 5th round operation is controlled

registers 1, 2, and 3, and 2^{24} input values will be left for input registers $(1, 6, b, c)$, $(2, 7, 8, d)$, and $(3, 4, 9, e)$. The remaining four 2^{24} input values are stored in a list as $(L1, L2, L3, L4)$.

Then, considering the list of $(L1, L2)$, we check if the CCs occur at registers $(5, c)$. Based on the size of the lists, $L1$ and $L2$, there are 2^{24} input values for each (2^{48} in combined total), and the computational cost will be 2^{48} in a straightforward way. Therefore, we sort the lists based on the value of registers $(5, c)$, which enables us to find CCs at registers $(5, c)$ with nearly 0 computational cost. Since the probability that a 2-byte collision occurs is 2^{-16}, the size of the list, $(L1, L2)$, becomes $2^{48} \cdot 2^{-16}$ or 2^{32} in total.

While the previous step is performed on $(L1, L2)$, the same step also deals with the list $L3$. By doing so, the collision can be checked at registers $(6, 8, a, d)$. In a similar way to the previous sorting technique, we can extract the input lists that induce CCs at registers $(8, d)$, and $2^{32} \cdot 2^{24} \cdot 2^{-16}$ or 2^{40} inputs survive. Also we check whether or not CC occurs at registers $(6, a)$, which results in the computational complexity of 2^{40} since the sorting techniques cannot be used. As a result, the list size of $(L1, L2, L3)$ becomes $2^{40} \cdot 2^{-16}$ or 2^{24} in total. Currently, the inputs satisfy that CC occurs at 10 registers $(0, 1, 2, 3, 5, 6, 8, a, c, d)$.

Finally, we consider the list of $L4$. Since the collision probability of these 3 bytes is 2^{-24}, the list size is $2^{24} \cdot 2^{24} \cdot 2^{-24}$ or 2^{24}. At this moment, we have a list such that CCs occur at 13 registers $(0, 1, 2, 3, 4, 5, 6, 8, 9, a, c, d, e)$. It is possible to derive $2^{16}, 2^8$, and 1 input such that CCs occur at $14, 15$, and 16 registers from the list since the 1-, 2-, and 3-byte collision probabilities are $2^{-8}, 2^{-16}$, and 2^{-24}, respectively.

The results are summarized in Table 3. Note that the number of plaintexts foe each number of CCs is an expected value, which means that the number of CCs cannot be 16 depending on the secret key, for instance.

An example of the fixed cipher key SK and plaintext P searched using the proposed algorithm is shown in Table 4. The intermediate value in each round when using P and SK to encrypt AES is also summarized in Table 4. According to Table 4, it is clear that CCs occur in 15 registers of the 5th round.

Table 3. The number of clockwise collisions and the number of the corresponding plaintexts.

# of CCs	# of Plaintexts (Expected Value)	Computational Cost
$1, 2$	$2^{120}, 2^{112}$	2^{32}
$3, 4, 5$	$2^{104}, 2^{96}, 2^{88}$	2^{34}
$6, 7, 8$	$2^{80}, 2^{72}, 2^{64}$	
$9, 10, 11$	$2^{56}, 2^{48}, 2^{40}$	2^{40}
$12, 13, 14$	$2^{32}, 2^{24}, 2^{16}$	
$15, 16$	$2^8, 1$	

Table 4. The case that the number of CCs is 15 at the 5th round operation in AES encryption.

P	41 09 8a 21 f8 38 37 32 fc 1c c1 2f 0e 4d 26 a0
SK	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
R4	bc c4 3d 1d 8b 00 84 a6 27 9e 7d 74 d8 61 fc 50
R5	bc c4 3d 1d 8b 00 84 a6 27 9e 7d 74 d8 61 fc 4f
C	a6 92 f3 f4 5c d5 16 e7 b3 8c d8 99 0e c5 2c 5d

Table 5. The case that the number of CCs is 16 at the 5th round operation in AES encryption.

P	8e 6c ba cf 51 cd 63 bd 50 06 6f 91 fd 48 ab 78
SK	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
R4	36 c7 42 a7 82 6c ae c3 0f be 04 75 60 a6 eb f8
R5	36 c7 42 a7 82 6c ae c3 0f be 04 75 60 a6 eb f8
C	19 27 a2 8f 1c 1e 4e b8 d3 7f 49 aa 60 bc 92 66

We show the manipulation of side-channel information based on experiments using the DE0-Nano Development and Education Board. Figure 10 shows the EM radiation manipulated with special plaintexts that are determined using the proposed algorithm. We can see clear peaks corresponding to the 10 round operations[11]. The figure shows that when the number of CCs is 15 or 16, the intensity of the EM radiation becomes weaker than the case for 0 CCs.

4.2 Utilization of Frequency Spectrum

To capture efficiently leaked side-channel information from the cryptographic device, the radio frequency range contributing to the information leakage should be carefully considered. For this purpose, we utilize the results of CEMA in the frequency domain [18, 16]. A strong correlation can be found in the fairly low-frequency ranges as shown in Fig. 8(a). In [20] and [3], it is reported that the on-chip internal cryptographic module can produce side-channel information with frequencies ranging widely up to several gigahertz. However, due to low-pass filtering nature caused by parasitic inductance and capacitance in the IC package and the printed circuit board traces, the gigahertz high-frequency components are filtered out and the frequency spectrum of the leaked information can be shaped in the frequency domain [19, 15]. In this experimental configuration, the pass band is measured to be approximately 5 to 20 MHz. The circuit designer's knowledge of this electrical property can be utilized for efficient identification with the side-channel information.

[11] The reason why there are eleven peaks in the EM trace is due to the employed loop architecture in which extra round operation is performed on ciphertext.

4.3 Multiple-Round Analysis

The results in Sect. 3 are all with the side-channel-information of only the 5th round operation. In order to achieve side-channel authentication with fewer EM traces, the side-channel information at multiple rounds should be considered. Therefore, we consider a leakage model can be constructed with multiple rounds. In [11], a leakage model based on multiple rounds is utilized in the context power-based side-channel authentication. Suppose that we utilize n sample points in the side-channel information as $(L(t_1, c, sk, N), \ldots, L(t_n, c, sk, N))$. When n sample points are chosen, *i.e.,* one at every round operation, the corresponding leakage model can be constructed since the verifier has all the round keys to derive the i-th round HD.

5 Conclusion

Side-channel analysis has been studied intensively mainly considering the key-recovery attack against cryptographic implementations. Reversing our way of thinking, we proposed side-channel authentication that constructively uses the physical information leakage to overcome existing threats such as impersonation. Four types of side-channel authentication methods were constructed on top of the conventional AES-based challenge-response authentication scheme, and we experimentally confirmed that the uniqueness of the side-channel information could be utilized for authenticating the provers, *i.e.,* a verifier could identify one from multiple provers with side-channel information from 200 AES encryptions with an acceptable error rate. Also several techniques to improve the side-channel authentication were discussed including manipulation of side-channel information, utilization of the frequency spectrum, and multiple-round side-channel analysis. By applying those techniques, we expect that side-channel authentication can be implemented with much fewer AES encryptions, which is the goal of future work.

Acknowledgment

This work was supported by Japan Society for the Promotion of Science (JSPS) Grants-in-Aid for Scientific Research (KAKENHI) Grant Numbers 26240005 and 15H01688.

References

1. S. Brands and D. Chaum. Distance-Bounding Protocols (extended abstract). In *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques*, pages 344–359, 1993.
2. S. Drimer and S. J. Murdoch. Keep Your Enemies Close: Distance Bounding against Smartcard Relay Attacks. In *Proceedings of the 16th USENIX Security Symposium*, 2007.

3. D. Fujimoto, N. Miura, M. Nagata, Y. Hayashi, N. Homma, Y. Hori, T. Katashita, K. Sakiyama, L. Thanh-Ha, P. Bazargan-Sabet J. Bringer, and J. Danger. On-Chip Power Noise Measurements of Cryptographic VLSI Circuits and Interpretation for Side-Channel Analysis. pages 405–410, 2013.
4. G. P. Hancke and M. G. Kuhn. An RFID Distance Bounding Protocol. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SecureComm 2005*, pages 67–73, 2005.
5. M. Kasper, A. Moradi, G. T. Becker, O. Mischke, T. Güneysu, C. Paar, and W. Burleson. Side Channels as Building Blocks. *J. Cryptographic Engineering*, 2(3):143–159, 2012.
6. P. C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference*, pages 104–113, 1996.
7. P. C. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference*, pages 388–397, 1999.
8. Y. Kuai, Y. Li, T. Machida, and K. Sakiyama. Power Consumption Control in Arbitrary Round of AES Hardware Implementation (in Japanese). In *Symposium record of SCIS'15*, volume 3A2-2, page 6, 2015.
9. Y. Li, D. Nakatsu, Q Li, K. Ohta, and K. Sakiyama. Clockwise Collision Analysis - Overlooked Side-Channel Leakage Inside Your Measurements. *IACR Cryptology ePrint Archive*, 2011:579, 2011.
10. L. Lin, M. Kasper, T. Güneysu, C. Paar, and W. Burleson. Trojan Side-channels: Lightweight Hardware Trojans Through Side-Channel Engineering. In *Cryptographic Hardware and Embedded Systems - CHES'09, 11th International Workshop*, pages 382–395, 2009.
11. A. Matsubara, T. Machida, Y. Hayashi, and K. Sakiyama. A Study on Leakage Model for Side-Channel Authentication (in Japanese). In *Symposium record of SCIS 2015*, volume 3A2-1, 2015.
12. A. Matsubara, Y. Li, Y. Hayashi, and K. Sakiyama. Consideration on Side-Channel Information Toward Authentication (in Japanese). In *Workshop record of ISEC'14*, volume ISEC2014-10, pages 1–8, 2014.
13. T. Mizuki and Y. Hayashi. AES Cipher Keys Suitable for Efficient Side-Channel Vulnerability Evaluation. *IACR Cryptology ePrint Archive*, 2014:770, 2014.
14. National Institute of Standards and Technology. *NIST FIPS PUB 197: Advanced Encryption Standard*. 2001.
15. C. R. Paul. *Introduction to Electromagnetic Compatibility (Wiley Series in Microwave and Optical Engineering)*. Wiley-Interscience, 2006.
16. T. Plos, M. Hutter, and M. Feldhofer. On Comparing Side-Channel Preprocessing Techniques for Attacking RFID Devices. In *Information Security Applications, 10th International Workshop, WISA'09*, pages 163–177, 2009.
17. K. B. Rasmussen and S. Capkun. Realization of RF Distance Bounding. In *19th USENIX Security Symposium*, pages 389–402, 2010.
18. 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. In *Information Security Applications, 10th International Workshop, WISA*, pages 66–78, 2009.
19. B. Vrignon, S. D. Bendhia, E. Lamoureux, and E. Sicard. Characterization and Modeling of Parasitic Emission in Deep Submicron CMOS. *IEEE Trans. Electromagn. Compat.*, 47(2):382–387, 2015.

20. M. Yamaguchi, H. Toriduka, S. Kobayashi, T. Sugawara, N. Homma, A. Satoh, and T. Aoki. Development of an On-Chip Micro Shielded-Loop Probe to Evaluate Performance of Magnetic Film to Protect a Cryptographic LSI from Electromagnetic Analysis. In *IEEE International Symposium on Electromagnetic Compatibility, EMC'10*, pages 103–108, 2010.