Physical Authentication Using Side-Channel Information

Kazuo Sakiyama, Momoka Kasuya, Takanori Machida,
Arisa Matsubara, and Yunfeng Kuai
The University of Electro-Communications, Chofu, Tokyo 182-8585, Japan
Email: {sakiyama, m.kasuya, machida, matsubara, kuaiyf}@uec.ac.jp

Yu-ichi Hayashi
Tohoku Gakuin University
Tagajo, Miyagi 985-8537, Japan
Email: yu-ichi@mail.tohoku-gakuin.ac.jp

Takaaki Mizuki
Tohoku University
Aoba-ku, Sendai 980-8578, Japan
Email: tm-paper+sichauth@g-mail.tohoku-university.jp

Noriyuki Miura and Makoto Nagata
Kobe University,
Nada-ku, Kobe 657-8501, Japan
Email: {miura, nagata}@cs.kobe-u.ac.jp

***Abstract*—Authentication based on cryptographic protocols is a key technology for recent security systems. This paper proposes a new authentication method that utilizes the side channel that already exists in many authentication systems. Side-channel analysis has been studied intensively from the attacker viewpoint and is best known for key-recovery attacks against cryptographic implementations using physical information. In this paper, reversing the traditional thought, we propose to use the key-dependent side-channel information constructively to enhance, or as an alternate to, existing cryptographic protocols. Using Advanced Encryption Standard (AES)-based authentication as an example, we demonstrate, based on experiments using an Field Programmable Gate Array (FPGA), that the side-channel information leaked from cryptographic devices is sufficiently unique for authentication.**

I. Introduction

This paper proposes a new authentication technique called *side-channel authentication* that utilizes side-channel information as a device fingerprint. Because 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., Advanced Encryption Standard (AES) [17] encryption. The main features of the proposed side-channel authentication method are:

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

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

One of the possible applications of side-channel authentication is secure machine-to-machine (M2M) communication, where machines must confirm the authenticity of each other to prevent contamination by a malicious entity in a system, e.g., counterfeit parts in a car's electrical system or fake silicon chips. All electrical devices intrinsically generate side-channel information that propagates through a wired or wireless communication channel. That is, they are capable of sending information. If a receiver device can decode the analog side-channel information, the above-mentioned secure M2M communication can be constructed. Although an EM probe and an oscilloscope are used in this paper for the receiver device, it can be realized with components similar to conventional wireless communications that rely on signal modulation, analog-digital conversion, and a digital communication protocol. Note that there are no signal modulations and no complicated protocols in the side-channel authentication, which makes the receiver device considerably simpler than a conventional wireless system.

A. MITM Attacks in Authentication System

Authentication between two parties, prover and verifier, is an initial procedure to grant permission to a prover to use a specific service. It is frequently 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 typically only a few hundred bits. This attracts attackers to launch man-in-the-middle (MITM) attacks where the attacker eavesdrops on the communication on a secure channel and manipulates this without the knowledge of the two parties. Relay attacks, discussed in the following segment, are one type of MITM attack.

ISBN: 978-1-4673-9879-4 (c) 2016 IEEE

Suppose that the verifier sends a 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 a 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 manner, 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, to counteract the attack, the challenge should not be repeated and the response time should be verified. That is, as a simple countermeasure, the verifier sends a random challenge c_r for each authentication and checks whether or not the arrival time of $f(c_r, sk)$ is less than a predetermined 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 away from the verifier, the attacker can still successfully achieve authentication, even against the above-mentioned countermeasure. The attacker launches two high-speed transponders near the prover and verifier. The 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 returned to the verifier via the two transponders. That is, regardless the position of the prover, the authenticated channel can 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 less than the threshold value. Note that in the case when the prover and 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 requires analog-digital and digital-analog conversions[1]. Under these circumstances, there are several countermeasures for the relay attack [8], [4], [20]. They are 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 verified by a single-bit challenge and rapid single-bit response.

B. Side-Channel Analysis

Side-channel analysis can utilize the physical information leaked from a cryptographic device and is frequently used to retrieve the secret key. Side-channel analysis research mainly focuses on key-recovery attacks on cryptographic algorithms, such as in [11] and [12].

Several papers have discussed the intentional induction of side-channel information. In [13], 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 [10], using Trojan side-channels was proposed where 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 induced physical side-channel information leakage to convey secret information. In [3], EM waves observed around integrated circuits were utilized as fingerprints for detecting a hardware Trojan. They preliminarily prepared a reference wave and compared it to a wave obtained from a test device.

The constructive use of side-channel information is also a topic of discussion. In [26], side-channel-based watermark was proposed for protecting intellectual property (IP) cores, i.e., verifying whether an IP core is manufactured by a vendor. It utilized the fact that supply voltage to the IP core depends on the switching of shift registers located in the IP core. The authors of [5], [9] combined this idea with a soft hash function that returns highly correlated digests when a similar pair of inputs is given and demonstrated this using several types of cryptographic hardware as IP cores that generate a specific power consumption trace. In [15], this was extended for a finite state machine that is typically included in IP cores, i.e., no requirement to consider the type of the IP cores.

In this paper, we attempt to confirm the identity of devices that have the same circuit design including cryptographic hardware, however, with different secret keys and grant access permission to a secure system. The previous work with these side-channel watermarks attempted to confirm whether a device had the same IP core. This is similar to an authentication using physically unclonable functions (PUFs) [22]. When a challenge is provided to a PUF, it outputs different responses because of physical variations in the manufacturing process. PUF-based authentication has the advantage that it is difficult to duplicate owing to physical variation. However, it is necessary for PUF-based authentication to pre-share multiple challenge–response pairs (CRPs), which requires a memory space depending on the number of the CRPs. Conversely, side-channel authentication requires only a secret key as pre-shared information although it has no advantage of unclonability. Further, it is relatively easy to avoid conflicting the properties of identifying information in side-channel authentication although it is difficult in PUF-based authentication.

II. Overview: Side-Channel Authentication

Side-channel authentication assumes that physical information leaked from a device is used as the 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 as side-channel authentication methods depending on whether the

[1]It is true that the authors of [7] demonstrated relay attack without modulation and demodulation on a remote access key system with an immobilizer embedded in modern cars. We consider not only this advantage but also the assumption that it is difficult to duplicate the side-channel information mentioned in Sect. I.

challenge and/or response is transmitted over the conventional communication channel. In this section, the four different authentication methods are proposed and their advantages and disadvantages are discussed in detail.

In the *challenge-SC-response authentication method*, 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 (a), 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, 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 that is obtained during the computation of the prover X. Note that the analog verification is a newly proposed step added to the conventional challenge-response authentication. Namely, both digital and analog information are verified in the challenge-SC-response 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. Because the side-channel information is strongly influenced by the system environment between the prover and verifier, SC can be expressed as leakage function L as $SC = L(t, c, sk, N)$, where N is the measurement noise, which typically follows a normal distribution. The verifier prepares roughly-modelled side-channel information based on a leakage model[2] as $M(c, sk_X)$ and checks whether 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 a predetermined threshold [3] h. To reduce the noise, the verifier can use several challenges to perform side-channel analysis on multiple sets of side-channel information.

For the second method, the prover only returns SC corresponding to the challenge c as shown in Fig. 1 (b). The *challenge-SC authentication method* assumes 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 prover. It is true that the challenge-SC authentication requires more computations for the verifier because $\rho(SC, M(c, sk_i))$ must be performed as many times as there are provers stored in the database. However, it is expected that millions of provers can be handled without significant time overhead using recent computational power for this signal processing.

In the third type, denoted as *SC-response authentication method*, the verifier does not send a challenge; rather, it receives response r from the prover as shown in Fig. 1 (c). 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 because the calculation of the intermediate values is considered the same, i.e., encryption and decryption of AES requires virtually the same amount of calculation.

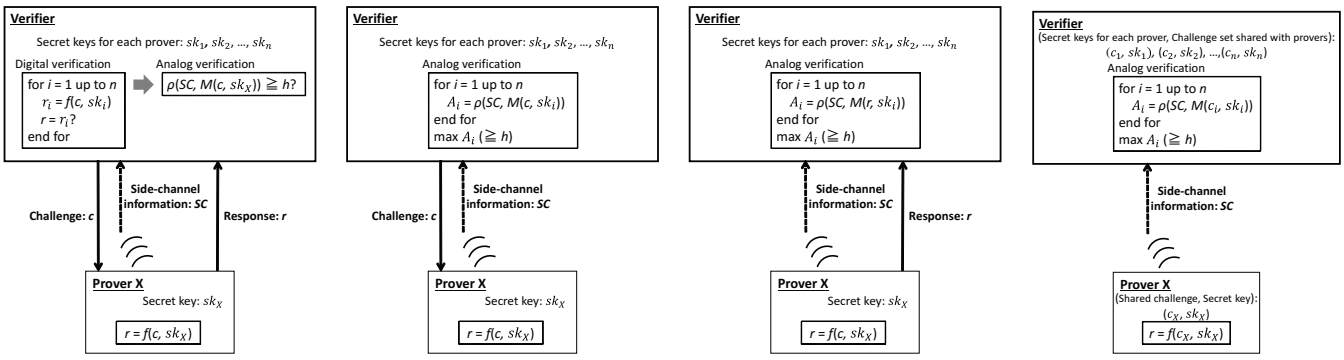
In the fourth authentication method, *only-SC authentication method*, the verifier neither sends a challenge nor receives a response, and only SC is checked on the verifier side as shown in Fig. 1 (d). In this method, it is assumed that the set of challenges is shared beforehand with the prover in addition to the secret key. The significant advantage of the only-SC authentication is that no digital communication channel is required between the prover and verifier. Therefore, even a device without 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.

A. Security Consideration of the Proposed Methods

This section presents the security perspective of the aforementioned methods. First, we focus on replay/relay attacks. Under our assumption that it is difficult to copy side-channel information (see Sect. I), these attacks can be prevented. This paragraph discusses these attacks without this assumption. In the scenario of a replay attack, the simple countermeasure is to send random challenge c, as mentioned in Sect. I.A. It is also required that the verifier stores the previously used challenge c and prevents sending the same challenge. The latter two methods, i.e., SC-Response and Only-SC authentication methods, are vulnerable for this attack because they have no challenge and the responses rely only on the provers. In the SC-Response authentication method, suppose that the verifier stores the previously used response r. Even if a malicious attacker eavesdrops on the communication channel and obtains the pair of response and side-channel information (r, SC) without detection by the verifier and prover, the verifier can prevent receiving the same response using the stored responses. However, if the attacker disrupts the communication channel and obtains the pair (r, SC), the verifier cannot prevent replying. The verifier also cannot limit the response-arrival time because it has no reference time since there is no challenge. The SC-only authentication method cannot prevent both eavesdropping and replaying since it does not have both challenge and response. The other methods have a tolerance since these two methods send a challenge to the prover. For the relay attack

[2]Hamming weight and Hamming distance of the intermediate values of $r = f(c, sk_X)$ are well-known leakage models [2]. It is known that these models are enough for distinguishing 8-bit secret keys.

[3]In practice, h is determined based on the result as shown in Fig 2.



(a) Challenge-SC-response (b) Challenge-SC (c) SC-response (d) Only-SC

Fig. 1. Four types of authentication methods

scenario, even when there is no assumption as mentioned in Sect. I, side-channel authentication has the potential to become a countermeasure to a relay attack by using the arrival time of the response (side-channel information). However, the SC-Response and only-SC authentication methods cannot realize this advantage inherently since they have no reference time since there is no challenge.

Next, we evaluate the tolerance against side-channel analysis (SCA) attack[4]. In the first three methods, a malicious attacker can recover the secret key if he can obtain a sufficient number of pairs of (c, SC) or (r, SC) required for an SCA attack. This is closely related to the number of traces where side-channel authentication is performed well. However, as far as when symmetric-key ciphers are used, the only-SC authentication method makes the key-recovery attack extremely difficult because the attackers must obtain the value of the challenge or response to derive the modelled leakage values. That is, it must construct the new attacker models. For instance, previous work [14] suggested that it is possible to reduce the key space with Simple Power Analysis (SPA) on AES key expansion implemented with the software[5]. Table I summarizes the features of the four authentication methods.

III. Identifying Information from AES Hardware

In principle, the proposed analysis method used for extracting identity is similar to the one for the key-recovery attacks. However, in contrast to key recovery attack scenarios, for the purpose of authentication, the secret key is assumed to be pre-shared so that extracting the identity of AES hardware can exploit all side-channel information available from the first to the last round. In this section, we propose a new analysis method using multiple-round side-channel information. The proposed analysis method is modelled on the physical leakage of 10-round AES encryption and the corresponding leakage model. The efficiency of the analysis to extract the identifying information of AES hardware is measured as the number of AES encryptions necessary to distinguish provers with different secret keys. That is, our research goal is to reduce the number of AES encryptions in the identity extraction analysis.

A. Analysis with Single-Round Model

The so-called Hamming distance model assumes that there is a linear dependency between the leakage model W and the Hamming distance value $H(D \oplus R)$, where D and R are intermediate values in a hardware operation [2].

128-bit intermediate values can be employed in the Hamming distance model because AES-comp hardware [27] performs one round per cycle. The leakage model for the i-th round operation is described as $\mathbf{W}^i = (W_1^i, W_2^i, \ldots, W_l^i)$, where l is the number of EM traces. The measured side-channel information during the i-th round of AES encryption for the l plaintexts is denoted as $\mathbf{S}^i = (S_1^i, S_2^i, \ldots, S_l^i)$. Regarding the correlation coefficients derived with $\rho(\mathbf{W}^i, \mathbf{S}^i)$, if there is a clear difference between acceptance and rejection, it can be regarded as a successful extraction of identifying information from the AES hardware. For the following discussions, the case wherein the verifier scrutinizes the legitimate prover using a common registered secret key is called an *acceptance trial*. The verifier must reject the prover if s/he does not have the secret key used in the verification process; this case is referred to as a *rejection trial*.

B. Proposal: N-round AES and Its Multi-Round Model

The round operation of AES is repeated N times in series (i.e., *N-round AES*, $N > 10$) instead of calling 10-round AES several times with different challenges. The model and side-channel information of N-round AES are represented respectively as $\mathbf{W} = (\mathbf{W}^1, \mathbf{W}^2, \ldots, \mathbf{W}^N)$, and $\mathbf{S} = (\mathbf{S}^1, \mathbf{S}^2, \ldots, \mathbf{S}^N)$.

The greatest advantage of the N-round AES is that from only one trace we can obtain N sub-waveforms. The authentication with $\rho(\mathbf{W}, \mathbf{S})$ can be demonstrated with the one trace, which will be confirmed in Sect. IV.B. This is an advantageous perspective of the proposed method because it is difficult for an attacker to attack using SCA with only one pair (r, SC).

[4]Considering the threat of SCA attacks, a variant of these methods can be constructed by separately preparing the secret key for the side-channel authentication.

[5]It is known that SPA on a naive modular exponentiation algorithm of RSA can reveal the private key from only side-channel information.

TABLE I
COMPARISON OF PROPOSED AUTHENTICATION METHODS

Features \ Methods	Challenge-SC-Response	Challenge-SC	SC-Response	Only-SC
Challenge	✓	✓		(Pre-Shared)
Response	✓		✓	
Verifier computation	$r = f(c, sk_i)$ and $\rho(\mathrm{SC}, M(c, sk_X))$	$\rho(\mathrm{SC}, M(c, sk_i))$	$\rho(\mathrm{SC}, M(r, sk_i))$	$\rho(\mathrm{SC}, M(c_i, sk_i))$
Conventional channel	Verifier $\Leftrightarrow$ Prover	Verifier $\Rightarrow$ Prover	Verifier $\Leftarrow$ Prover	None
Replay Attack	Harder	Harder	Easy without assumption	Easy without assumption
Relay Attack	Harder	Harder	Easy without assumption	Easy without assumption
SCA Attack	Need lots of traces	Need lots of traces	Need lots of traces	Much harder

In the other attack scenarios, the authentication method with N-round AES is comparable to challenge-SC and only-SC authentication methods, discussed in Sect. II.A.

IV. First Experiments on FPGA

Based on Verilog codes of 128-bit AES-Comp [27], a prover device is implemented on ALTERA Cyclone I V FPGA (EP4CE22F17C6N) on Terasic DE0-Nano FPGA board [23]. The AES operation frequency is set to 50 MHz. EM radiation for the ten-round AES operation with different challenges[6] is obtained with a near-field magnetic probe (Langer-EMV RF-U 5-2) and oscilloscope (Agilent Technology DSO7032A), and store it as EM trace. In the verifier side, the EM traces are checked with the model values based on leakage models, secret key, and challenges. More precisely, the verifier needs to derive the correlation coefficients for all the registered provers' model values.

A. Single-Round Analysis

The correlation coefficient between 8-bit or 128-bit HD model and the EM radiation from a single round of the AES hardware is evaluated experimentally.

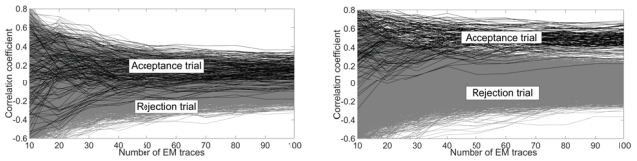
- 500 sampling data is taken with 1 GSa/s;
- 30 provers with different secret keys are prepared.

In the acceptance trial, only one prover should be accepted whereas the other 29 provers should be rejected in the rejection trials. The number of EM traces used in the experiments is set from ten to 100 every ten traces. For each prover, the acceptance and rejection trials are repeated five times for the 30 provers, i.e., 150 and $150 \cdot 29$ trials are performed in total for the acceptance and rejection trials, respectively.

The single-round 8-bit HD model, which is often used in the key-recovery attacks, is applied to extract the identifying information from 128-bit AES hardware. The result of the first byte of AES is illustrated in Fig. 2 (a), where the black and grey lines correspond to the acceptance and rejection trials, respectively. The figure indicates that distinguishing provers is difficult. In our experiments, there is only a marginal locality effect of EM radiation because the correlation coefficients of the different bytes indicate similar results.

The correlation coefficients with the 128-bit HD model of the last round $\mathbf{W}^{10}$, calculated using the same procedure as the 8-bit HD model, are presented in Fig. 2 (b). We can clearly see an improvement of the 128-bit HD model over the 8-bit HD model. Almost all the acceptance trials are distinguishable from the rejection trials only with 100 EM traces.

[6]In the experiments, we assume that several challenges are pre-shared between the verifier and each prover.



(a) 8-bit HD model (b) 128-bit HD model

Fig. 2. Result with each model for the number of traces

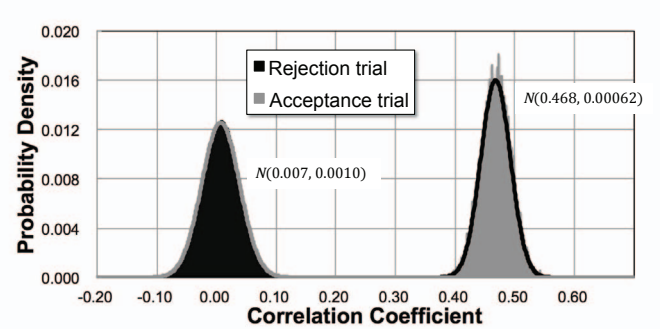


Fig. 3. Result of multi-round model with 1000-round AES

B. Multi-Round Analysis with N-round AES

We evaluate the correlation coefficients with a multi-round model using N-round AES $\mathbf{W}$ as proposed in Sect. III.B.

- 21,000 sampling data is taken with 1 GSa/s;
- 10,000 provers with different secret keys are prepared;
- For rejection trials, 10,000 models based on randomly chosen secret keys are registered.

The correlation coefficients with these acceptance and rejection trials are calculated, and a histogram of these results are constructed. The number of occurrence in each period of the histogram is represented as a percentage of the total trials, as shown in Fig. 3. Note that these coefficients are absolute values and hence the proposed authentication system tolerates polarity variation of the EM radiation. Our experimental results show that the least and greatest coefficients of the

acceptance and rejection trials are 0.36 and 0.17, respectively. Therefore, each prover can be clearly distinguished from all provers that should be rejected in the authentication system[7].

V. Conclusions and Future Work

Side-channel analysis has been studied intensively considering key-recovery attacks against AES hardware. Reversing the traditional thought, we proposed side-channel authentication that constructively uses the physical information leakage to overcome existing threats such as impersonation. We proposed N-round AES that has N-1 intermediate rounds for improving the proposed authentication in terms of performance and security. Our first experimental results successfully confirmed 10,000 authorized provers using only one trace.

Our future work includes the investigation of two fundamental techniques to enhance the efficiency of side-channel authentication. Firstly, the authors of [16] proposed manipulation techniques, which should be investigated as an effective method to improve the efficiency of side-channel authentication. Secondary, in order to capture efficiently leaked side-channel information from a cryptographic device, the radio frequency range contributing to the information leakage must be carefully considered. For this purpose, we utilize the results of CEMA in the frequency domain [21], [19]. According to another experimental result, a strong correlation can be found in the reasonably low-frequency ranges. In [25], [6], it is reported that the on-chip internal cryptographic module can produce side-channel information with frequencies ranging widely up to several gigahertz. However, owing to the 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 spectrum of the leaked information can be shaped in the frequency domain [24], [18]. 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.

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 15K12035.

References

[1] S. Brands and D. Chaum. "Distance-Bounding Protocols (extended abstract)." In *Proc. Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of Cryptographic Techniques*, pages 344–359, 1993.

[2] E. Brier, C. Clavier, and F. Olivier. "Correlation Power Analysis with a Leakage Model." In *Proc. Cryptographic Hardware and Embedded Systems - CHES'04*, pp.16–29, 2004.

[3] J. Balasch, B. Gierlichs, and I. Verbauwhede. "Electromagnetic Circuit Fingerprints for Hardware Trojan Detection." In *Proc. Cryptographic Hardware and Embedded Systems - CHES'04*, pp.16–29, 2004.

[4] S. Drimer and S. J. Murdoch. "Keep Your Enemies Close: Distance Bounding against Smartcard Relay Attacks." In *Proc. the 16th USENIX Security Symp.*, 2007.

[7] This result is based on actual EM traces. However, Monte Carlo simulation

[5] F. Durvaux, B. Gerard, S. Kerckhof, F. Koeune, and F. X. Standaert. "Intellectual Property Protection for Integrated Systems Using Soft Physical Hash Function." In *Proc. WISA 2012, Proc. 7690*, pages 208–225, 2012.

[6] 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.

[7] A. Francillon, B. Danev, and S. Capkun. "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars." In *Proc. the Network and Distributed System Security Symp. (NDSS)*, 2011.

[8] G. P. Hancke and M. G. Kuhn. "An RFID Distance Bounding Protocol." In *Proc. First Int. Conf. on Security and Privacy for Emerging Areas in Communications Networks, SecureComm'05*, pages 67–73, 2005.

[9] S. Kerckhof, F. Durvaux, F. X. Standaert, B. Gerard. "Intellectual Property Protection for FPGA Designs with Soft Physical Hash Function: First Experimental Results." *Proc. IEEE Int. Symp. on Hardware-Oriented Security and Trust - HOST'13*, pages 7–12, 2013.

[10] 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.

[11] P. C. Kocher. "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems." In *Proc. Int. Cryptology Conf. (CRYPTO'96)*, pages 104–113, 1996, .

[12] P. C. Kocher, J. Jaffe, and B. Jun. "Differential Power Analysis." In *Proc. Int. Cryptology Conf. (CRYPTO'99)*, pages 388–397, 1999.

[13] L. Lin, M. Kasper, T. Güneysu, C. Paar, and W. Burleson. "Trojan Side-channels: Lightweight Hardware Trojans Through Side-Channel Engineering." In *Proc. Cryptographic Hardware and Embedded Systems - CHES'09, 11th Int. Workshop*, pages 382–395, 2009.

[14] S. Mangard. "A Simple Power-Analysis (SPA) Attack on Implementations of the AES Key Expansion." In *Proc. Information Security and Cryptology-ICISC'02*, pages 343–358, 2002.

[15] C. Marchand, L. Bossuet, and E. Jung. "IP Watermark Verification Based on Power Consumption Analysis." In *Proc. 27th IEEE Int. System-on-Chip Conf. (SOCC)*, pages 330–335, 2014.

[16] T. Mizuki and Y. Hayashi. "AES Cipher Keys Suitable for Efficient Side-Channel Vulnerability Evaluation." *IACR Cryptology ePrint Archive*, 2014:770, 2014.

[17] National Institute of Standards and Technology. "*NIST FIPS PUB 197: Advanced Encryption Standard*." 2001.

[18] C. R. Paul. "*Introduction to Electromagnetic Compatibility (Wiley Series in Microwave and Optical Engineering)*." Wiley-Interscience, 2006.

[19] T. Plos, M. Hutter, and M. Feldhofer. "On Comparing Side-Channel Preprocessing Techniques for Attacking RFID Devices." In *Proc. Information Security Applications, 10th Int. Workshop, WISA'09*, pages 163–177, 2009.

[20] K. B. Rasmussen and S. Capkun. "Realization of RF Distance Bounding." In *Proc. 19th USENIX Security Symp.*, pages 389–402, 2010.

[21] 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 *Proc. Information Security Applications, 10th Int. Workshop, WISA*, pages 66–78, 2009.

[22] G. E. Suh and S. Devadas. "Physical Unclonable Functions for Device Authentication and Secret Key Generation." In *Proc. the 44th Design Automation Conf., DAC'07*, pp.9–14, 2007.

[23] Terasic Inc., "DE0-Nano Development and Education Board." http://www.terasic.com.tw/en (Accessed 16 December 2015)

[24] 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.

[25] 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 *Proc. IEEE Int. Symp. on Electromagnetic Compatibility, EMC'10*, pages 103–108, 2010.

[26] D. Ziener, and J.Teich. "Power Signature Watermarking of IP Core for FPGAs." Journal of Signal Processing System 51, pages 123–136, 2008.

[27] Tohoku University. "Cryptographic Hardware Project." http://www.aoki.ecei.tohoku.ac.jp/crypto/ (Accessed 8 September 2015)