Evaluation of Statistical Fault Analysis Using Input Timing Violation of Sequential Circuit on Cryptographic Module Under IEMI

Daisuke Fujimoto, *Member, IEEE*, Takumi Okamoto, Yang Li, *Member, IEEE*, Youngwoo Kim, *Member, IEEE*, and Yuichi Hayashi, *Senior Member, IEEE*

***Abstract*—In encryption circuits, the threat of fault injection analysis remains a considerable problem. More specifically, clock glitches generated by intentional electromagnetic (EM) irradiation cause faulty operations and estimate internal secret keys. Generating clock glitches via intentional EM interference (IEMI) can be performed without opening the equipment, which makes it a real threat. Previous secret key analysis via IEMI has focused on setup time violations. It requires the clock glitch to occur near the critical path delay of the encryption circuit. This article examines the faults owing to timing violations of inputs to the sequential circuit and discusses the possibility of obtaining the secret key from the output of the faulty ciphertext. The input timing violation of the sequential circuit covers all times during the operation. The bias of the output value of the sequential circuit owing to input timing violations is evaluated using a measurement system in which the sequential circuit alone was extracted. Secret key analysis of encryption circuits using the bias of output values is performed for three different implementations of the advanced encryption standard to demonstrate its feasibility. The results indicate that secret key analysis is possible over a wide range of shortened clock period, regardless of the implementation method.**

***Index Terms*—Clock glitch, fault injection, fault injection analysis, intentional electromagnetic interference (IEMI), statistical fault analysis (SFA).**

I. Introduction

THE threat of fault injection attacks aimed at acquiring confidential information has been highlighted [1]. Faults are generated by applying a disturbance, such as a laser, voltage fluctuation, or electromagnetic (EM) wave, to a cryptographic device. The fault injection attack model can be applied to numerous cryptographic algorithms, such as public key cryptography [1], DES [2], and advanced encryption standard (AES) [3], [4], [5]. In AES, it is well established that the secret key can be analyzed with a few faults in the analysis (differential fault analysis [DFA]) based on the difference between normal and faulty cipher text.

To perform a secret key analysis, the faults should be generated in only a part of the operation. Various studies have been performed on fault injection methods for a cryptographic module, such as a method of lowering the power supply voltage [6] and a laser irradiation method [7]. The fault injection method using clock glitch [8], [9], [10] has been adopted in several studies owing to its feasibility. A method using intentional EM interference (IEMI) [11], [12] has been proposed as a method for generating clock glitches inside the device. Accordingly, the target of the attack is extended to the device that cannot be opened by inducing the EM wave via the power line.

The conventional fault injection methods using clock glitch [11], [12] have primarily focused on the setup time violation of computation. If a fault occurs only in the slowest operation in the encryption process, a fault occurs depending on the operation. This is exploited to analyze the secret key. Therefore, to perform an analysis, the clock glitch should be inserted into the device at the appropriate timing. However, when injecting from the outside using EM waves, it cannot be synchronized with the internal circuit, and it is difficult to insert the clock glitch at appropriate timing.

In this article, we focus on the input timing violation fault that occurs in the sequential circuit. Input timing violation occurs when the input of the sequential circuit is in transition. During the encryption process, the input of the sequential circuit significantly changes before computation is complete. Consequently, this type of fault may expand the threat of IEMI fault injection. The evaluation environment only implements the sequential circuit in IC to validate the bias of the output value caused by the input timing violation. To validate the feasibility of secret key analysis using such a type of bias, we demonstrate the secret key analysis on three types of implementations of AES using clock glitch injection.

The remainder of this article is organized as follows. In Section II, the phenomenon of input timing violation in the sequential circuit is described, and the new fault injection method using this phenomenon is proposed. In Section III, we validate the effect of input timing violation in the sequential circuit using

Manuscript received 8 June 2022; revised 14 September 2022; accepted 11 October 2022. Date of publication 28 October 2022; date of current version 16 February 2023. This work was supported by JSPS KAKENHI Grant 19H01104 and Grant 21K19772. *(Corresponding author: Yuichi Hayashi.)*

Daisuke Fujimoto, Takumi Okamoto, Youngwoo Kim, and Yuichi Hayashi are with the Nara Institute of Science and Technology, Ikoma 6300192, Japan (e-mail: fujimoto@is.naist.jp; cocet33000@gmail.com; youngwoo@is.naist.jp; yu-ichi@is.naist.jp).

Yang Li is with the Department of Informatics, University of Electro Communications, Tokyo 182-8585, Japan (e-mail: liyang@uec.ac.jp).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TEMC.2022.3215583.

Digital Object Identifier 10.1109/TEMC.2022.3215583

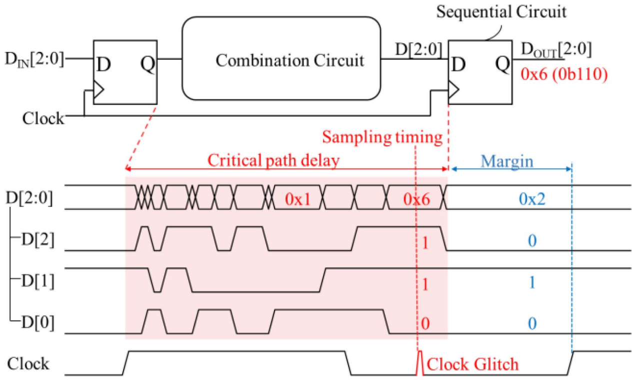


Fig. 1. Image of setup time violation for secret key analysis with clock glitch around critical path delay of encryption.

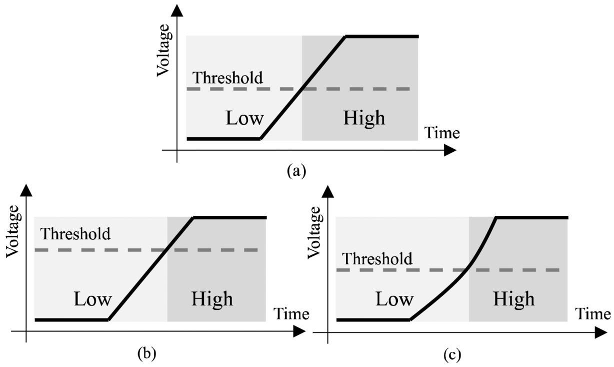


Fig. 2. Hold value bias of sequential circuit caused by an imbalance of threshold voltage or non-linear input voltage. (a) Threshold is center of input range. (b) Threshold is lower than center. (c) Nonlinear input voltage.

a simple circuit structure. Subsequently, we demonstrate secret key analysis using this type of fault injection on three types of AES implementation. The conclusion of this article is presented in Section IV.

II. Secret Key Analysis Using Fault Injection Focusing on Sequential Circuits

A. Fault Injection Analysis Using Setup Time Violation

When plaintext is given as an input to a cryptographic circuit, it processes the plaintext and outputs ciphertext. Processing is performed by a combination logic circuit in synchronization with the clock. Generally, the period of the clock must be greater than the propagation delay time until the combinatorial logic circuit stabilizes at the normal output. Inserting a clock glitch shortens the clock cycle. As a result, a fault occurs when the shortened clock cycle is shorter than the propagation delay time, which is known as setup time violation. In a previous research on the fault injection method using IEMI [11], DFA [4] was used as the analysis method based on the assumption that a fault occurs only in a part of the encryption process. Therefore, to obtain the faults required for secret key analysis, it is necessary to shorten the period by clock glitch near the critical path delay of the circuit (see Fig. 1). However, when EM waves are applied from outside the cryptographic circuit, it is difficult to synchronize them; thus, the timing at which the clock glitch is inserted is random. Moreover, the insertion of the clock glitch depends on the rising edge of the clock signal [13]. Therefore, the method proposed in [11] requires a large number of trials to successfully perform key analysis.

B. Fault Injection Analysis Using Biased Faulty Output Generated in the Sequential Circuit

In the encryption process, the plaintext input is randomized by the secret key. The value is not biased even if the calculation is terminated in the middle of the calculation due to the insertion of the clock glitch. However, in an actual logic circuit, bias may occur due to the analog behavior of a digital circuit. In particular, in a sequential circuit that holds a value, it affects the calculation in the next clock cycle.

Fig. 2 illustrates the evaluation image of the digital value when the rising slope and the threshold voltage are nonuniform. Generally, the cryptographic circuit is composed of a digital circuit and operates by determining logic high (high) / logic value low (low) with a certain threshold value for the voltage of the input electric signal. Therefore, as depicted in Fig. 2, the high / low boundary concerning the input voltage value exists at the center when the time change of the input signal is linear and the threshold value is in the center of the input voltage range.

However, the actual clock signal does not have an ideal shape. Imbalance in drivability of positive-channel metal-oxide semiconductor (PMOS) and negative-channel metal-oxide semiconductor (NMOS) [14] changes the threshold voltage, as shown in Fig. 2(b). In this case, the high / low logic value boundary is not divided at the center of voltage swing. This imbalance might occur with the whole logic chip. Furthermore, the superimposed noise, such as IEMI [11], causes a nonlinear shape in the clock input at the I/O circuit, as shown in Fig. 2(c). This nonlinearity causes a time change in crossing the threshold voltage. This causes a change in the presence probability of high / low value. Collectively, these two phenomena cause the bias in the captured value in sequential circuits. As sequential circuits capture the input value at the timing of crossing threshold, and high and low value of input signal determined by the threshold and the voltage of input signal.

The calculated value becomes random if the processing of the encryption circuit is interrupted by the shortening of the random clock generated by IEMI. However, since it is in the middle of processing, many data signals undergo a transition. In that case, it is biased toward either high or low owing to the bias, as described above. Then, the Hamming weight (HW) changes over the entire intermediate value of the encryption circuit.

In the research on theoretical analysis methods, a statistical fault analysis (SFA) method that acquires a secret key using a bias in the HW has been proposed [15], [16]. The analysis method is also applied to fault injection using glitch insertion by IEMI.

III. Experiment

In this section, we present the environment that simulates the shortening of the random clock that occurs when a clock glitch

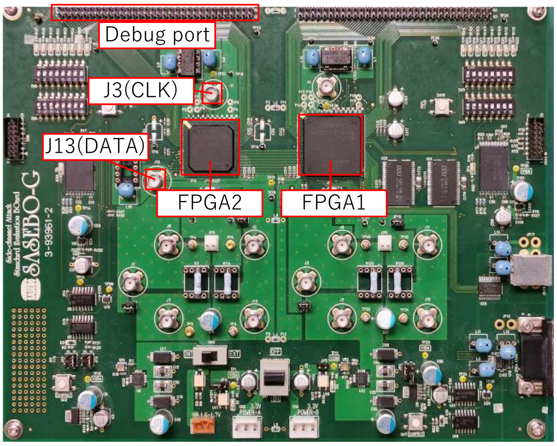


Fig. 3. Evaluation board.

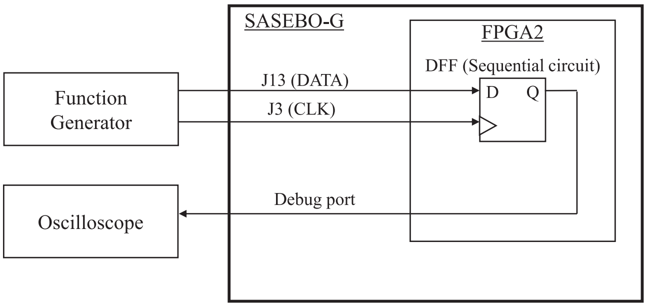


Fig. 4. Experimental set-up for validating the input time violation on sequential circuit.

occurs via EM waves and demonstrate that the output value is biased in the sequential circuit. Thereafter, we demonstrate that secret key analysis can be performed when a clock glitch occurs in the implementation of multiple AES cryptographic circuits.

A. Bias of Faulty Output Value Generated in Sequential Circuit

In this experiment, the side channel standard evaluation board, shown in Fig. 3, was used. The block diagram and measurement equipment are displayed in Fig. 4. We used the internal D flip-flop (D-FF) of the field programmable gate array (FPGA2) as the target sequential circuit. The data signal was provided as input into the FPGA2 at the rising edge of the clock. The clock signal and data signal that served as inputs to the internal D-FF of the FPGA2 were input from ports J3 and J13 on the board. Moreover, the output signal of D-FF was output from the I/O and observed with an oscilloscope (Keysight DSOX3054T) to determine which of High and Low was captured. Data signal and clock signal were generated using a function generator (Keysight 81160A). The pulse width of the clock and data signal was set to 200 ns. The rising and falling edges of each signal were set to 1 ns. To check the bias of the output signal, the delay time between the clock and data was changed in the range of 0 ns to 500 ns in increments of 0.01 ns. If there is no bias on output of DFF, the term High should be 200 ns, while the Low term should be 300 ns.

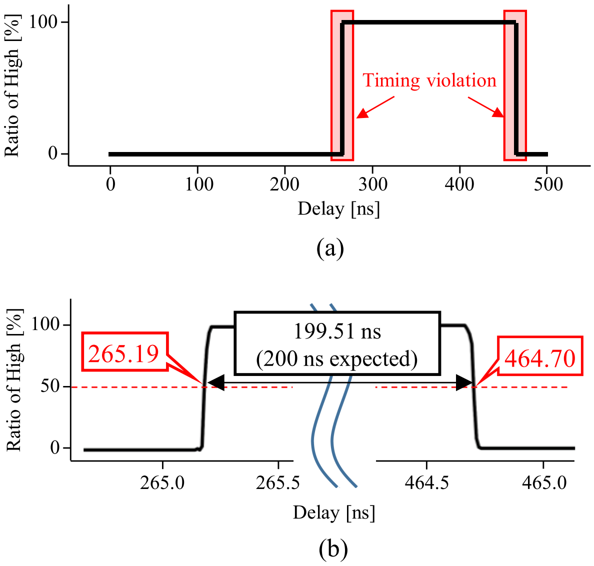


Fig. 5. Result of the output value bias of the sequential circuit.

Fig. 5 illustrates the results of 100 captures in each delay between the clock signal and data signal input to sequential circuit. The vertical axis of Fig. 5 represents the probability that High is captured. Fig. 5(a) presents all the capture results, and Fig. 5(b) illustrates an enlarged view of the capture results when the input timing of the sequential circuit in which an invalid value during the transition is captured violates. The expected width of high is 200 ns. However, the actual width of High in Fig. 5(b) is 199.51 ns. It can be confirmed that the captured value is biased to low when sweeping the delay between clock signal and data signal. The result indicates the possibility that the intermediate HW value can be manipulated by injecting a fault into the input transition of the sequential circuit during the operation of encryption.

B. Fault Injection Analysis Using Biased Faulty Output Generated in the Sequential Circuit

In this section, it is confirmed that SFA analysis can be performed when a clock glitch by IEMI is input to the AES encryption circuit. More specifically, SFA is performed for three types of AES to confirm that the bias of the output value does not depend on the implementation. The target implementation methods include AES-Comp [17], AES-PPRM1 [18], and AES-PPRM3 [18]. AES-Comp is a small area implementation using a composite field expression; however, the critical path delay becomes longer. Furthermore, the transition probability of the data line is high because the exclusive OR is frequently used. Thus, the probability of fault owing to the input timing violation of the sequential circuit may be high. AES-PPRM1 is an implementation that reduces data transition via exclusive OR using AND logic gates. AES-PPRM1 is composed of 1 stage of exclusive OR and AND logic, and AES-PPRM3 is composed of 3 stages. Therefore, AES-PPRM1 has a shorter critical path than AES-PPRM3.

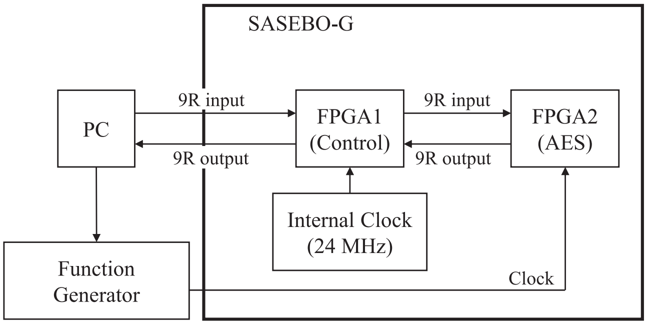


Fig. 6. Experimental set-up for faulty ciphertext acquisition due to shortened clock period which emulates clock glitch caused by the IEMI circuit.

Since the conditions are the same as possible except for the S-box mounting method, the mounting of other combinational circuits is unified, and the registers are specified at the slice level to rewrite the circuit. Additionally, FPGA1 will be equipped with a circuit that communicates with the PC and controls the FPGA2. Each FPGA operates on a different clock and consistently supplies a 24 MHz clock to control FPGA1. Generally, the clock of FPGA2 that performs encryption is designed at 24 MHz; however, the clock cycle is shortened assuming a clock glitch caused by IEMI injection. To improve the reproducibility, the shortened clock is generated by an arbitrary signal generator and supplied from the J3 port connected to the clock input of the AES circuit mounted on FPGA2.

SFA was performed in the ninth round (9R) of AES encryption. To avoid fault injection to other AES rounds, first to eighth round processing of AES was performed on PC (see Fig. 6). In an actual attack, the clock glitch occurs in various rounds. However, if the attacker focuses on side-channel information via the power line, the attacker can estimate the round with clock glitch [19]. The entire flowchart of this experiment is illustrated in Fig. 7. In this experiment, we performed an experiment using a highly reproducible setup for basic examination; however, if we assume a scenario where it is possible to invade a cryptographic module, such as a smart card, even in actual fault injection, an attacker can inject a fault in a specific round, and this experiment can simulate a realistic environment. The clock cycle has a sufficient margin for the critical path, and the upper limit is 12 ns, where no fault occurs, and the clock cycle was reduced by 0.5 ns width to inject a fault into the sequential circuit. The number of trials (N) is 5000, encryption processing was performed 5000 times in each clock cycle, and faulty ciphertexts were collected. The key used in the experiment was fixed to “0x2b7e151628aed2a6abf7158809cf4f3c”. The 5000 plaintexts are random. Using random plaintext is realistic validation of fault analysis.

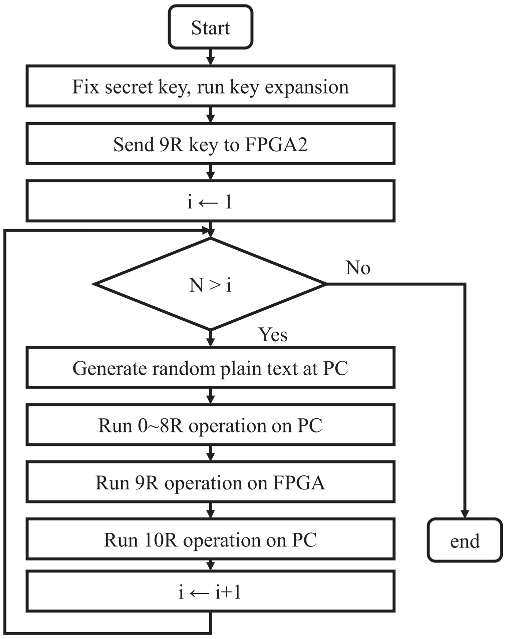


Fig. 7. Flowchart for faulty ciphertext acquisition owing to shortened clock period which emulates a clock glitch caused by IEMI.

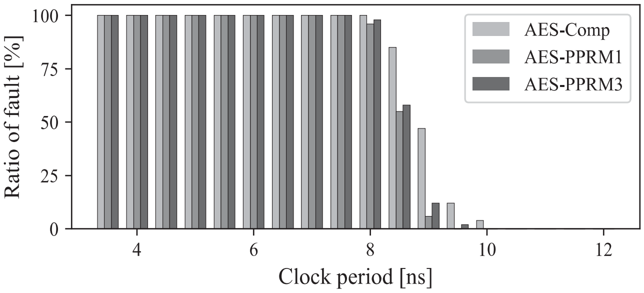


Fig. 8. Fault rate occurred by shorten clock period.

As a result of the experiment, the encryption process was completely stopped on FPGA2 from 3 ns, which is shorter than the minimum operation cycle of FPGA2, in any AES implementation. The result when the glitch timing is from 3.5 to 12 ns is shown. Fig. 8 illustrates the fault rate for each AES implementation. The horizontal axis of Fig. 8 displays the cycle of the clock signal as if it were glitch, and the vertical axis represents the fault rate for 5000 rounds of encryption. From Fig. 8, it can be confirmed that in the AES-Comp implementation with the longest critical path, the fault occurs in the longest clock cycle, and in the AES-PPRM1 implementation with the shortest critical path, the fault does not occur unless the clock cycle is short.

Using conventional DFA, since the critical path differs depending on the implementation, fault analysis using setup time violation requires a detailed search for the clock period used for analysis for each implementation. Fig. 9 presents the number of 1 B faults used in conventional DFA. The result illustrates that the range of shortened clock period is narrow. Moreover, the range among different implementations varies. In this case, the attacker must control the clock glitch owing to the variance in the range of the shortened clock period.

The flow of the SFA using the captured faulty ciphertext is depicted in Fig. 10.

1) The SFA assumes the HWs of the intermediate values, which constitute the input to the operation depending on the partial secret key. In the case of faults caused by IEMI,

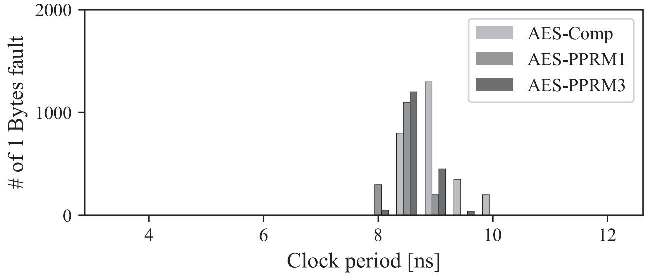


Fig. 9. Number of 1 B fault which can be used for conventional DFA analysis on each shortened clock period.

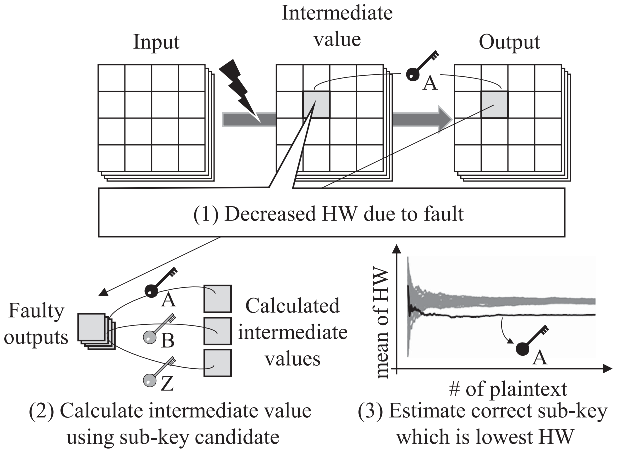

Input
Intermediate value
Output
A
(1) Decreased HW due to fault
Faulty outputs
A
B
Z
Calculated intermediate values
mean of HW
# of plaintext
A
(2) Calculate intermediate value using sub-key candidate
(3) Estimate correct sub-key which is lowest HW

Fig. 10. Flow of SFA.

the intermediate values change. Based on the experiment in Section III-A, the faulty value goes Low, and the HWs also become Low.

2) The SFA assumes that the attacker can get the set of output ciphertext containing the faults. Accordingly, the operation using a single 8 b partial key performs the inverse calculation of the intermediate values for all the candidate partial keys from the output ciphertext. Using the calculated intermediate candidate, the attacker can calculate the HWs of the intermediate value.
3) By repeating the above process and collecting HW for several plaintexts, the distribution of HWs of intermediate value can be examined. The distribution of HWs of intermediate value set under the assumption with an incorrect partial key are random. Meanwhile, the distribution of HWs of the intermediate values under the assumption of a correct partial key contain HWs that are reduced owing to a fault from the assumption in (1), which is used to estimate the secret key. The example illustrated in Fig. 10 assumes a bias toward low; however, the same method can be used to estimate the key for high. To obtain all the partial keys, it is necessary to manipulate the values so that the HWs of the intermediate values in each partial key is biased. Since the analysis is performed independently for each partial key of 1 B, it is possible to perform the analysis even if the HW bias occurs for multiple partial keys.

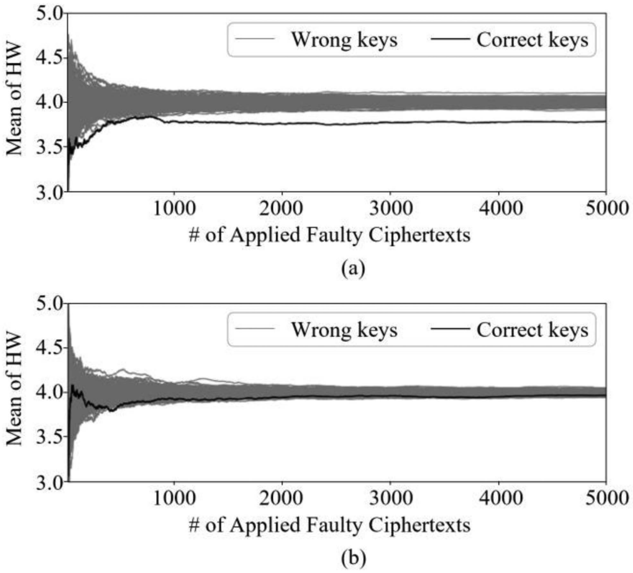


Fig. 11. Bias of HW due to input timing violation in sequential circuit. (a) Shortened clock is 4 ns. HW of correct key guess goes down. (b) Shortened clock is 3.5 ns. No bias is observed due to maximum frequency of cryptographic circuit.

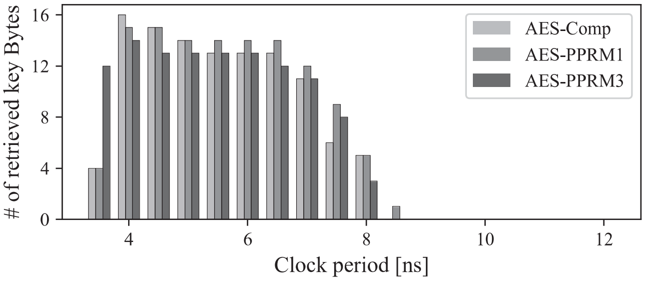


Fig. 12. SFA result on each shortened clock period.

Fig. 11 presents the results of applying the SFA to the zeroth byte of AES-Comp. The horizontal axis of Fig. 11 represents the number of faulty ciphertexts used in the analysis, and the vertical axis represents the average HW. Fig. 11(a) illustrates an example in which the HW is lower when the intermediate value is calculated back using the correct secret key, as compared to the case where the wrong key is assumed. The secret key can be obtained. Fig. 11(b) presents an example in which the HW when assuming the correct key is inseparable from the case where the wrong key is assumed, and in such a case, the secret key cannot be obtained.

In this experiment, the key candidate with the lowest average HW was estimated as the correct key. Fig. 12 presents the results of applying the same analysis to 16 B of 5000 faulty outputs of the three implementation methods obtained at each shortened clock period. The horizontal axis represents the clock period, and the vertical axis indicates how many bytes of the 16-B secret key could be correctly retrieved. From this figure, when the clock period is approximately 4–7 ns for any AES implementation, the HW of the fault value is reduced, and more than half of the secret key is successfully acquired. This suggests that in the 4–7 ns clock period, many value transitions occur in the data bus of the encryption process, resulting in a bias in the sequential circuit owing to the shortened clock period, and causing a change in the HWs across the data.

Based on the results of the experiment, the clock period was shortened for the implementation of AES with different data transition probabilities and critical paths, and the timing violation of the sequential circuit was generated. From this figure, it can be confirmed that for any implementation method, a decrease in the HW of the fault value is induced when the acquisition is performed at a clock period of approximately 4–7 ns, and more than half of the secret keys are successfully obtained. If a 12-B secret key can be obtained, it can be decrypted by a full search of the secret key because the secret key space of 2^{128} drops to 2^{32}.

In the analysis using DFA, which is a conventional method [11], the analysis is successful only when the clock glitch is inserted near 6.5 ns. In other words, it can be stated that the analysis efficiency is good because the fault caused by the input timing violation in the sequential circuit presented in this article is analyzed successfully without adjusting the clock glitch.

C. Discussion

The fault injection in the proposed method is based on the clock glitch. Therefore, it is assumed that the conventional countermeasure method against clock glitch can be applied. Additionally mounting a circuit for detecting a clock abnormality is a specific countermeasure method. In [20], a delay element was arranged in parallel with the combination circuit that executes the encryption process, and if the clock cycle is shorter than the delay time in the delay element, it is regarded as a clock abnormality, and an invalid value is output. Consequently, countermeasures against fault injection analysis by clock glitch are realized. It is considered that the same countermeasure method can be applied to the threat of the proposed method.

IV. Conclusion

This article evaluates a secret key analysis on encryption circuits using input timing violations of sequential circuits, which are caused by internal clock glitches in devices owing to intentional EM irradiation. Unlike conventional analysis using setup time violations, the secret key analysis attack using input timing violations of sequential circuits targets the entire logical transition during the encryption process. Consequently, it enlarges the range of clock period manipulation, which is difficult to manipulate with clock glitching using EM waves.

To confirm whether an input timing violation in the sequential circuit causes a bias in the output value, we changed the delays of the clock and data signals in an evaluation system, in which the sequential circuit alone is implemented. We confirmed the phenomenon in which the output value is biased to low. As a result, the output value is biased to low when a random fault occurs during the encryption operation.

The clock period was changed for several AES encryption circuits to confirm that secret key analysis of encryption circuits is possible due to biased output values in sequential circuits. The obtained faulty outputs were used to demonstrate that secret key analysis is possible over a wide range of clock periods using SFA. This indicates that the range of target devices may be expanded since the timing adjustment of clock glitches is enlarged in secret key analysis using input timing violations of sequential circuits. It is considered that a method to detect clock glitches is useful as a countermeasure against such attacks.

In the experiment demonstrating the effectiveness of the proposed method, AES was targeted; however, since the proposed method focuses on the incorporation of the sequential circuit, which is a general configuration of the sequential circuit, a cipher that implements another cryptographic algorithm. It may be widely applicable to modules.

References

[1] D. Boneh, R. Demillio, and R. Liotin, “On the importance of checking cryptographic protocols for fault,” in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, 1997, pp. 37–51.

[2] E. Biham and A. Shamir, “Differential fault analysis of secret key cryptosystems,” in *Proc. Annu. Int. Cryptol. Conf.*, 1997, pp. 513–525.

[3] J. Blomer and J.-P. Seifert, “Fault based cryptanalysis of the advanced encryption standard (AES),” in *Proc. Int. Conf. Financial Cryptographic*, 2003, pp. 162–181.

[4] G. Piret and J.-J. Quisquater, “A differential fault attack technique against SPN structures, with application to the AES and KHAZAD,” in *Proc. Int. Workshop Cryptographic Hardware Embedded Syst.*, 2003, pp. 77–88.

[5] C. N. Chen and S. M. Yen, “Differential fault analysis on AES key schedule and some countermeasures,” in *Proc. Australas. Conf. Inf. Secur. Privacy*, Jul. 2003, pp. 118–129.

[6] J. Schmidt and H. Christoph, “A practical fault attack on square and multiply,” in *Proc. 5th Workshop Fault Diagnosis Tolerance Cryptographic*, 2008, pp. 53–58.

[7] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, “The sorcerer’s apprentice guide to fault attacks,” *Proc. IEEE*, vol. 94, no. 2, pp. 370–382, Feb. 2006.

[8] T. Fukunaga and J. Takahashi, “Practical fault attack on a cryptographic LSI with ISO/IEC 18033-3 block ciphers,” in *Proc. 6th Workshop Fault Diagnosis Tolerance Cryptographic*, 2009, pp. 84–92.

[9] J. Balasch, G. Benedikt, and V. Ingrid, “An In-depth and Black-box characterization of the effects of clock glitches on 8-bit MCUs,” in *Proc. Workshop Fault Diagnosis Tolerance Cryptographic*, 2011, pp. 105–114.

[10] Y. Li, K. Sakiyama, S. Gomisawa, T. Hukunaga, and K. Ohta, “Fault sensitivity analysis,” in *Proc. Int. Workshop Cryptographic Hardware Embedded Syst.*, 2010, pp. 320–334.

[11] Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, and H. Sone, “Transient IEMI threats for cryptographic devices,” *IEEE Trans. Electromagn. Compat.*, vol. 55, no. 1, pp. 140–148, Feb. 2013.

[12] K. Iokibe, K. Maeshima, H. Kagotani, Y. Nogami, Y. Toyota, and T. Watanabe, “Investigation in burst pulse injection method for fault based cryptanalysis,” in *Proc. IEEE Int. Symp. Electromagn. Compat.*, 2014, pp. 743–747.

[13] N. Saga, T. Itoh, Y. Hayashi, T. Mizuki, and H. Sone, “Study on the effect of clock rise time on fault occurrence under IEMI,” in *Proc. IEEE Int. Symp. Electromagn. Compat. IEEE Asia-Pac. Symp. Electromagn. Compat.*, 2018, p. 9. [Online]. Available: https://ieeexplore.ieee.org/document/8394009

[14] H. Fuketa, R. Takahashi, M. Takamiya, M. Nomura, H. Shinohara, and T. Sakurai, “Increase of crosstalk noise due to imbalanced threshold voltage between nMOS and pMOS in subthreshold logic circuits,” *IEEE J. Solid-State Circuits*, vol. 48, no. 8, pp. 1986–1994, Aug. 2013.

[15] T. Fuhr, E. Jaulmes, V. Lomne, and A. Thillard, “Fault attacks on AES with faulty ciphertexts only,” in *Proc. Workshop Fault Diagnosis Tolerance Cryptographic*, 2013, pp. 108–118.

[16] C. Dobraunig, S. Mangard, F. Mendel, and R. Primas, “Fault attacks on nonce-based authenticated encryption: Application to Keyak and Ketje,” in *Proc. Int. Conf. Sel. Areas Cryptographic*, 2018, pp. 257–277.

[17] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, “A compact Rijndael hardware architecture with S-Box optimization,” in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2001, pp. 239–254.

[18] S. Morioka and A. Satoh, "An optimized S-Box circuit architecture for low power AES design," in *Proc. Int. Workshop Cryptographic Hardware Embedded Syst.*, 2002, pp. 172–186. [Online]. Available: https://www.iacr.org/cryptodb/data/paper.php?pubkey=728

[19] K. Nakamura, Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, and H. Sone, "Method for estimating fault injection time on cryptographic devices from EM leakage," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, 2005, pp. 235–240.

[20] N. Selmane, S. Bhasin, S. Guilley, T. Graba, and J.-L. Danger, "WDDL is protected against setup time violation attacks," in *Proc. Workshop Fault Diagnosis Tolerance Cryptographic*, 2009, pp. 73–83.

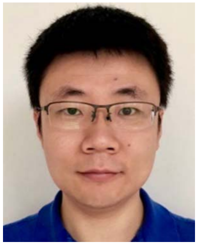
Daisuke Fujimoto (Member, IEEE) received the B.E., M.E., and Ph.D. degrees in engineering from Kobe University, Kobe, Japan, in 2009, 2011, and 2014, respectively.

He is currently an Assistant Professor with the Graduate School of Information Science, Nara Institute of Science and Technology, Nara, Japan. He is also a Visiting Assistant Professor with the Institute of Advanced Sciences, Yokohama National University, Yokohama, Japan. His research interests include hardware security and implementation of security cores.

Dr. Fujimoto is a Member of Institute of Electronics, Information and Communication Engineers.

Takumi Okamoto received the B.E. degree from the Department of Electrical and Electronic Engineering, Oita National College of Technology, Oita, Japan, in 2018, and the M.E. degree from the Nara Institute of Science and Technology, Ikoma, Japan, in 2020.

His research interests include fault injection attack on cryptographic devices.



Yang Li (Member, IEEE) received the B.E. degree in electronic and information engineering from Harbin Engineering University, Harbin, China, in 2008, and the M.E. and Ph.D. degrees in information and communication engineering from the University of Electro-Communications, Chofu, Japan, in 2011, and 2012, respectively.

He is currently an Associated Professor with the Department of Informatics, University of Electro-Communications, Chofu, Japan. His main research interests include security evaluation and improvement for cryptographic hardware and IoT devices.

Youngwoo Kim (Member, IEEE) received the B.S. degree in electrical engineering from Korea University, Seoul, South Korea, in 2013, and the M.S. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 2015 and 2018.

He has been an Assistant Professor with the Nara Institute of Science and Technology (NAIST), Division of Information Science, Nara, Japan, since 2019. Prior to joining NAIST, he was a Post-Doctoral Researcher with KAIST Information and Electronics Institute. His researches focus on system level signal/power integrity simulation methodology, statistical analysis, advanced packaging for 2.5-D/ 3-D Integration, hardware security, and electromagnetic interference/ electromagnetic compatibility.

Dr. Kim is currently an Associated Editor for IEEE TRANSACTIONS ON COMPONENTS, PACKAGING, AND MANUFACTURING TECHNOLOGY.

Yuichi Hayashi (Senior Member, IEEE) received the M.S. and Ph.D. degrees in information sciences from Tohoku University, Sendai, Japan, in 2005 and 2009, respectively.

He is currently a Professor with the Nara Institute of Science and Technology, Ikoma, Japan. He is the Chair of EM Information Leakage Subcommittee in IEEE EMC Technical Committee 5. His research interests include electromagnetic compatibility and information security.

Dr. Hayashi has been recognized through many awards and honors including the IEEE Electromagnetic Compatibility Society Technical Achievement Award, IEEE International Symposium on Electromagnetic Compatibility Best Symposium Paper Award and Workshop on Cryptographic Hardware and Embedded Systems Best Paper Award.