Measurement on Effect of Controlled Wave Phase in EM Fault Injection Attack

Yuto Shinoda
Graduate Schiool of Information Sciences,
Tohoku University
Sendai, Miyagi, Japan
Email: yuto.shinoda.q7@dc.tohoku.ac.jp

Mitsuki Takenouchi
Graduate Schiool of Information Sciences,
Tohoku University
Sendai, Miyagi, Japan

Yu-ichi Hayashi
Graduate School of Science and Technology
Nara Institute of Science and Technology
Nara, Japan

Takaaki Mizuki
Cyberscience Center
Tohoku University
Sendai, Miyagi, Japan

Hideaki Sone
Cyberscience Center
Tohoku University
Sendai, Miyagi, Japan

***Abstract*— The intentional electromagnetic interference (IEMI) injection method using sinusoidal waves cannot be protected with conventional countermeasures proposed and expanded the range of target devices. Therefore, evaluating devices against side-channel attacks is more important than in the past. A control in the phase of sinusoidal waves used in this attack can affect the extraction of secret keys. Nevertheless, there was not enough discussion about the effects of the controlled phase in conventional studies. We considered the effect of control in the phase of sinusoidal waves and proposed the new evaluation method based on this consideration. This method makes it possible to evaluate the devices taking into account the effects of controlled phases that have not been considered before. This method was devised based on the idea that evaluation is performed while changing the phase of sinusoidal waves. We experimented using actual cryptographic hardware to substantiate the effect of changing the phase of the sinusoidal wave on the attack and verify the validity of the proposed method. We confirmed that the phase of sinusoidal waves affects the attack as expected and showed that the proposed method is more suitable for evaluation than the conventional method. We also pointed out the problems of the proposed method and indicated the point of possible further improvement.**

Keywords—side-channel attack, fault analysis, intentional electromagnetic interference

I. INTRODUCTION

The side-channel attack is the threat that tries to obtain secret information, for example, by injecting irregular inputs into cryptographic hardware and analyzing the obtained outputs [1]. The differential fault analysis (DFA) was proposed as a kind of attack method [2]. Attack methods against the Advanced Encryption Standard (AES), which is a major encryption algorithm, have been proposed to apply DFA [3]-[5].

Nowadays, as a new fault injection method, a non-invasive attack has been proposed [6] where injecting sinusoidal waves can cause transient failures from the power line of devices without approaching or invading to hardware. Figure 1 shows the conceptual diagram of the non-invasive fault injection method. A probe is connected to the power line of the device, and then the attacker injects sinusoidal waves from a probe without synchronizing with the encryption. The novel method causes failure during encryption in this way. The attack does not need to open or approach to devices. Past countermeasures cannot be applied for that reason. Since this injection method is easier than the past method, this method extends the range of target devices. Therefore, the tolerance evaluation method for this attack has been more important than before. Some

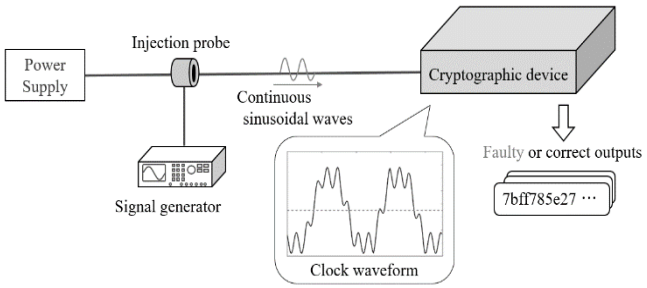


Fig. 1. Conceptual diagram of non-invasive fault injection method

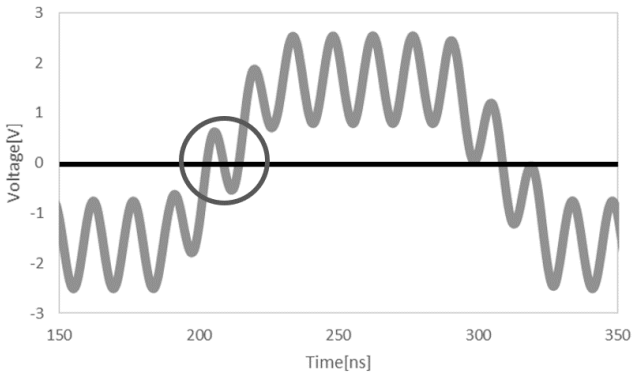
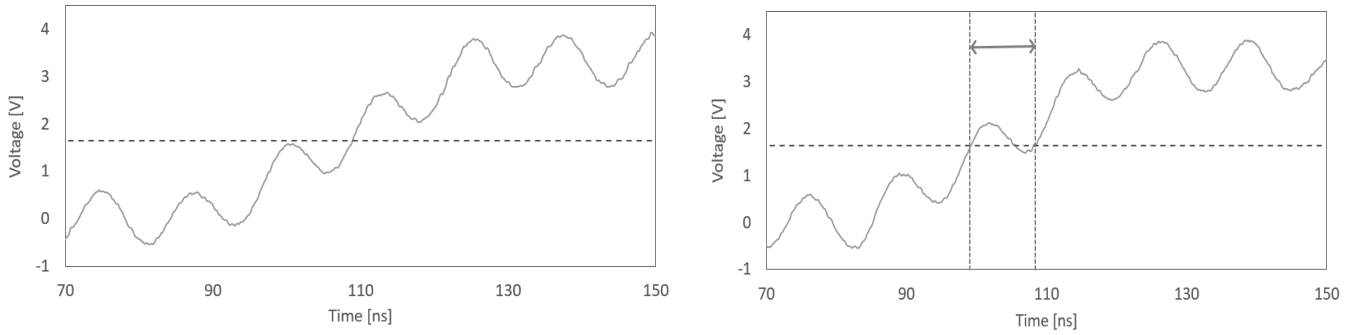


Fig. 2. Clock signal superimposed sinusoidal wave signal

attack methods and evaluation methods for side-channel attacks have been proposed based on this attack. Methods for specifying outputs that can be used for side-channel attacks [7][8] and the fault injection method using the frequency of applied sinusoidal waves as a parameter have been proposed [9].

Since the non-invasive fault injection method is executed on the bases of difficulty to obtain the trigger, there is a problem that the timing of occurrences of faults cannot be operated. By using this method, a clock signal of a cryptographic module is superimposed a sinusoidal wave signal which is shown in Fig. 2. Calculation errors arise because of overclocking by stepping over a threshold in a short time by an oscillation of sinusoidal waves like in the circle in Fig. 2. Therefore, it is considered that occurrences of faults depend on the frequency or the phase of sinusoidal waves superimposed on the clock signal. The attack method using frequency as a parameter was proposed in the past [9]. On the other hand, the non-invasive fault injection method is unsynchronized with the clock signal; therefore, we cannot decide a phase uniquely. Consequently, past studies have not

978-1-7281-5579-1/20/$31.00 ©2020 IEEE



(a) Case of non-failure **(b) Case of failure**

Fig. 3. Clock signal superimposed sinusoidal wave controlled phase

dealt with phases of sinusoidal waves superimposed on the clock signal.

We focus on the phase of sinusoidal waves superimposed on a clock signal. We discuss the relationship between the phase and the fault by considering the change of faults because of the control in the phase. We also propose the evaluation method considering the effect of changing the phase. Our method can be implemented by injecting the sinusoidal wave by sweeping the phase from 0 to 360 degrees. We performed the fault injection experiment using this method. From the result of this experiment, we confirmed that our method revealed the effect of phase by showing the change of faults with the controled phase. We besides discovered the periodicity of the change in the number of faulty outputs with the controled phase.

II. PROPOSAL OF THE METHOD CONSIDERING THE PHASE

We discuss the evaluation method in this section. A study of the relation between the change of occurrence of faults and the control of the phase is presented in part A. We presented the summary of the evaluation method considering the phase in part B.

A. Consideration of the relationship between the faulty outputs and the phase of applied sinusoidal waves

Figure 3 shows clock signals superimposing sinusoidal waves of distinct phases. A horizontal line in Fig. 3 is the threshold about clocks. The clock signal in Fig. 3 (a) steps over the threshold only once, and hence, the hardware operates normally. The clock signal in Fig. 3 (b) is below the threshold after stepping over it due to the oscillation of sinusoidal waves; moreover, the clock signal steps over it again. Since the clock time shortens, a calculation error arises, and the faulty output occurs. We consider that occurrences of faults depend on the phase of sinusoidal waves from this consideration.

We also consider the relationship between the state of the error and the phase. The arrow in Fig. 3 (b) shows a fault clock time due to the sinusoidal wave. Figure 4 shows the mechanism of occurrence of fault during a fault clock time. There is a time when the clock signal is below the threshold due to sinusoidal waves in Fig. 3 (b). This is a clock glitch in Fig. 4. In the normal clock cycle, the calculation of the third byte in Fig. 4 is performed normally because the clock time is long enough compared to the calculation time. However, when a clock glitch occurs as in Fig. 4, the clock time is shorter than the calculation time [10]. Thus, the calculation of the third byte cannot be completed during the clock time. The

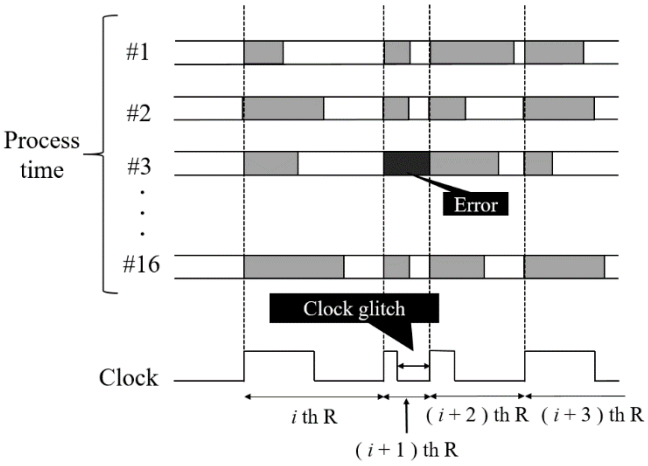


Fig. 4. Fault injection and faulty byte

error occurs in the third byte for this reason. The length of the clock time affects the number of faulty bytes. For example, in hardware encryption, calculations of several bytes are processed in parallel. If the clock time becomes shorter, some calculations except for the third byte cannot be completed within the clock time, so that the number of faulty bytes increases. If the clock time is long enough to complete the calculation of the third byte, all bytes are successfully calculated, so that the number of faulty bytes is reduced. we consider that the state of fault depends on the phase of the sinusoidal waves from these considerations.

Only 1-byte error in the 8th round (8R1B error) or 9th round (9R1B error) input can be used for DFA. For this reason, we counted the number of 8R1B errors in addition to the number of faulty outputs in the experiment in the experiment of section 3.

B. Proposal of the evaluation method

Considering the relationship between the fault and the phase, we propose an evaluation method considering the control of the phase. Specifically, we let the initial phase of the sinusoidal wave to x degrees and the interval between the evaluated phases to a degrees. Since it is difficult to specify the first phase, variable x is used here. First, we perform evaluation experiments many times with the phase set to x degrees. Next, we set the phase to $(x+a)$ degrees, and then we perform experiments similarly. We perform it until $(x+na) \geq 360$ repeatedly. Here, n is the number of experiments. If an available output to DFA appears, we finish the experiment.

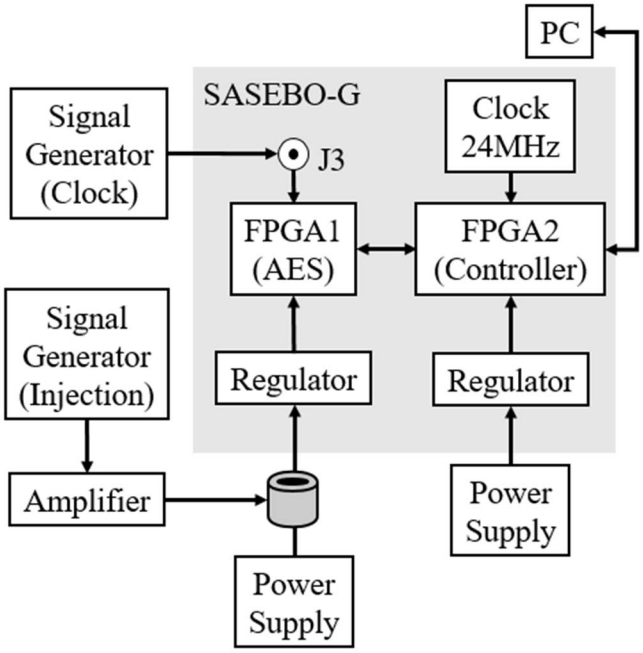


Fig. 5. Block diagram of the experiment

An example is x = 0 degrees and a = 10 degrees. First, evaluators inject sinusoidal waves with phase 0 degrees and perform evaluation experiments many times. Next, evaluators set the phase to (x+a) = 10 degrees, and perform evaluation experiments many times. If they perform this process 37 times, they set the phase to 360 degrees. If they cannot obtain a faulty output, they can finish the evaluation after completing the process 37 times in this example.

III. APPLCIATION OF PROPOSED METHOD

We show the experiment applied our method. The implementation of the method in this experiment is presented in part A. we presented the experiment conditions in part B. we show the result of the experiment and we discuss it in part C.

A. The implementation of the proposed method

We let the first phase x to 0 degrees and the interval a to 10 degrees based on the proposed method. Here, "0 degrees" does not mean that we actually set the phase to 0 degrees. We found it difficult to identify the initial phase. We wrote the initial phase as 0 degrees for ease of expression for that reason. 1000 encryption processes were performed per evaluation phase. In brief, experiments were performed every 10 degrees from the initial phase set to 0 degrees to 360 degrees, and encryption was performed 1000 times for each phase.

B. Experiment conditions

Figure 5 shows the block diagram of this experiment. Side-channel Attack Standard Evaluation Board (SASEBO-G) [11] was used for the encryption. Figure 6 shows SASEBO-G. For encryption, AES-Comp [12] was implemented to FPGA 1 in Fig. 6. Table 1 shows the experimental equipment.

We applied only the clock signal to the SASEBO-G directly. We generated the injection sinusoidal wave with a signal generator, after that, it is amplified by an amplifier, and then it was applied by an injection probe from the power line of the device. Table 2 shows the parameters of the clock signal. The fault injection from the power supply line is based on the conventional method [6]. The frequency and the

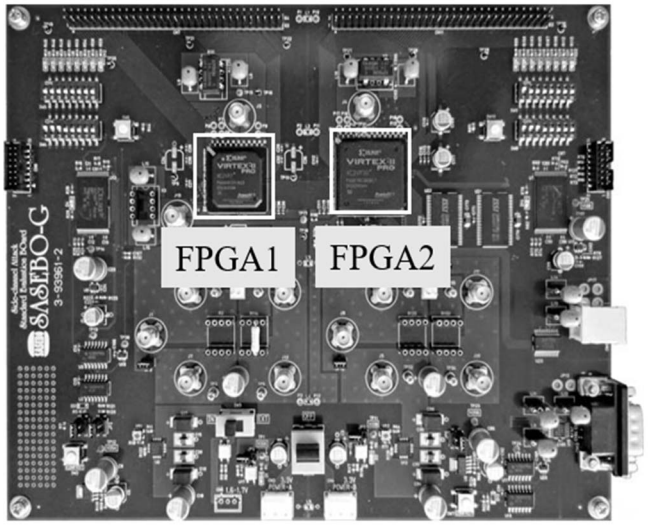


Fig. 6. Side-channel Attack Standard Evaluation Board (SASEBO-G)

TABLE 1 Equipment in Experiment

Cryptographic Device	SASEBO-G
Signal Generator	Keysight 81160A
DC-Block	Mini-Circuits BLK-89-S+
Amplifier	Mini-Circuits ZHL-2-12
Injection Probe	FCC F-140

TABLE 2 CLOCK SIGNAL ON SASEBO-G

FPGA1 clock frequency	8MHz
FPGA1 clock voltage	$1.4V_{pp}$
FPGA1 clock rise time	9ns
FPGA2 clock frequency	24MHz
FPGA2 clock voltage	$3.3V_{PP}$

amplitude about sinusoidal waves for fault injection were set to 212MHz and 107dBμV. These were fixed to focus on the phase. Moreover, the study which focused on frequencies and amplitudes has already been done [13]. The frequency of the electromagnetic field applied to the power line was set to 212MHz considering the transfer characteristics from the power supply line to the clock line of the encryption FPGA and the ease of observing the change in fault. We investigated the frequency which presented a low attenuation rate to the cryptographic module and a high attenuation rate to other modules [13], and then we set to 212MHz.

An encryption key was set to test vector (0x2b7e151628aed2a6abf7158809cf4f3c) in AES specifications [14]. The same 1000 plaintexts were used for encryption. We counted the number of faulty outputs and the number of 8R1B errors, and then we compared each phase.

To identify the faulty round and the number of error bytes in the faulty output, we calculated the ciphertext without fault and the faulty output. We describe this method in detail. First, we decrypted a correct ciphertext and a faulty output by using the secret key used for encryption and obtained intermediate values in each calculation. Next, we compared the obtained intermediate values in each round and checked the number of bytes having different values. Finally, we estimate the round with the smallest number of different values as the faulty round and the number of bytes having different values in the faulty round as the number of error bytes. We thought that if this method was considered to be the effect of the phase, the

number of faulty outputs and the number of 8R1B errors change with the control of the phase.

C. Experimental result and discussion

Figure 7 shows the number of faulty outputs and Fig. 8 shows the number of 8R1B errors for each phase. Two figures show that the number of faulty outputs and 8R1B errors changed with the controlled phase. We confirmed from this result that the number of faulty outputs and the tendency of errors depends on a phase of the sinusoidal wave. We besides confirmed that there were similarities between the change from 0 degrees to 180 degrees and the change from 180 degrees to 360 degrees in the number of faulty outputs and of the 8R1B errors from Fig. 7 and Fig. 8. Figure 9 shows the ratio of the number of 8R1B errors to the number of faulty outputs for each phase. We considered that the ratio of a specific error to the number of faulty outputs may also change with the controlled phases from Fig. 9. We found that the change was similar from 0 degrees to 180 degrees and 180 degrees and 360 degrees in Fig. 9.

If the phase of the sinusoidal wave sets to the phase where it is difficult to obtain an 8R1B error, evaluators cannot obtain proper results. However, if evaluators use this method, they can obtain proper results because of considering the effect of phases. Therefore, we consider that this method is more certain than the past method.

However, the sweep range of the phase is wide in this method. For instance, if evaluators cannot obtain faulty outputs that can apply DFA, they must experiment 1000*37 times in this experiment. An evaluation hence takes a long time. We considered that these changes have a periodicity from the similarity of every 180 degrees. We are considering that we can reduce the number of evaluations by this tendency.

IV. Conclusion

We considered the effect of the phase of the injected sinusoidal wave on the output of fault injection and proposed a new evaluation method considering the effect. From comparing clock signals on which sine waves with different phases are superimposed, we confirmed that the control of the phase of sinusoidal waves was related to the occurrence of a fault and the change in the number of error bytes. We also proposed an evaluation method considering the effect of phases while changing the phase of the superimposed sinusoidal wave. If evaluators use this method, they can evaluate in consideration of the effect of the phase. Therefore, our evaluation method is more effective than the conventional method. We experimented using this method so that we confirmed that the number of faulty outputs and the tendency of errors depends on the controlled phase of the sinusoidal wave. We could confirm that the proposed method was taking into account the controlled phase from the experiment.

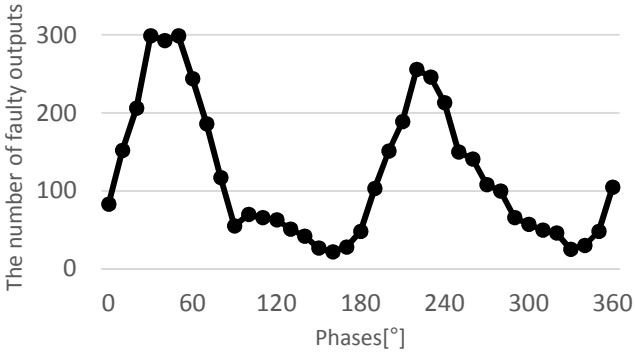


Fig. 7. The number of faulty outputs

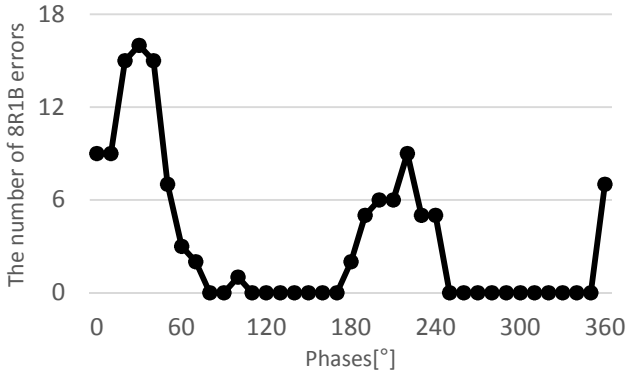


Fig. 8. The number of 8R1B errors

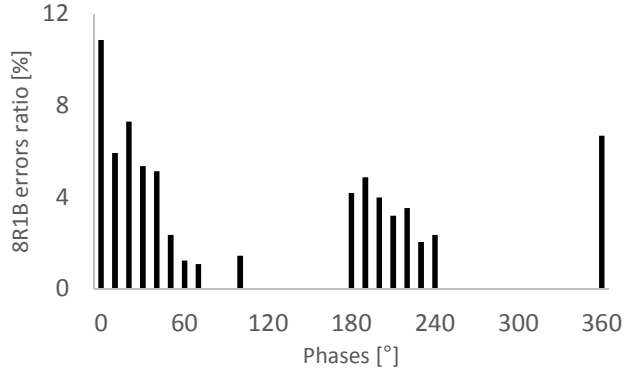


Fig. 9. The ratio of 8R1B error

References

[1] D. Boneh, R. Demillio, and R. Liotin, "On the Importance of Checking Crypto-graphic Protocols for Fault," Advances in Cryptology (Eurocrypt '97), LNCS 1233, pp. 37-51, May 1997.

[2] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," Advances in Cryptology (Crypto '97), LNCS 1294, pp.513-525, Aug. 1997.

[3] J. Blomer and J.-P. Seifert, "Fault Based Cryptanalysis of the Advanced Encryption Standard (AES)," Financial Cryptography: 7th International Conf., (FC 2003), LNCS 2742, pp. 162-181, Jan. 2003

[4] G. Piret and J.-J. Quisquater, "A Differential Fault Attack Technique against SPN Structures, with Application to the AES and Khazad," Workshop on Crypto-graphic Hardware and Embedded Systems (CHES 2003), LNCS 2779, pp.77-88, Sep. 2003.

[5] C.-N. Chen and S.-M. Yen, "Differential Fault Analysis on AES Key Schedule and Some Countermeasures," Australasian Conf. on Information Security and Privacy (ACISP 2003), LNCS 2727, pp.118-129, Jul. 2003.

[6] Y. Hayashi, N. Homma, T. Sugawara, T. Mizuki, T. Aoki, and H. Sone, "Non-Invasive EMI-Based Fault Injection Attack against Cryptographic Modules," IEEE International Symposium on Electromagnetic Compatibility, pp. 763-767, Aug 2011.

[7] K. Nakamura, Y. Hayashi, N. Homma, T. Mizuki, and H. Sone, "Method for estimation fault injection time on cryptographic devices from EM leakage," IEEE International Symposium on Electromagnetic Compatibility, pp. 235-240, Sep 2015.

[8] M. Takenouchi, N. Saga, Y. Hayashi, T. Mizuki, and H. Sone, "A Method for Distinguishing Faulty Bytes in Cryptographic Device Using EM Information Leakage," Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility, ThuPM2C.1, p. 253, Jun 2019.

[9] T. Ito, Y. Hayashi, T. Mizuki, and H. Sone, "A Timing Controlled Fault Injection Method Asynchronous to Cryptographic Processing," 2017

Symposium on Cryptography and Information Security, 2A3-2, 2017 (in Japanese).

[10] K. Nakamura, Y. Hayashi, T. Mizuki and H. Sone, "Information Leakage Threats for Cryptographic Devices Using IEMI and EM Emission", IEEE TEMC, vol. 60, no. 5, pp. 1340-1347, Oct. 2018.

[11] Side-channel Attack Standard Evaluation Board (SASEBO),http://staff.aist.go.jp/akashi.satoh/SASEBO/en/index.html

[12] A. Satoh, S. Morioka, K. Takano, S. Munetoh, “A Compact Rijindael Hardware Architecture with S Box Optimization,” International Conference on the Theory and Application of Cryptology and Information Security, pp.239 254, 2001.

[13] Y. Hayashi, N. Homma, T. Mizuki, T. Aoki and H. Sone, “Transient IEMI Threats for Cryptographic Devices,”IEEE Trans. on Electromagnetic Compatibility, vol. 55, pp. 140-148, 2013.

[14] NIST FIPS PUB. 197, Advanced encryption standard (AES), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf