4th URSI AT-RASC, Gran Canaria, 19-24 May 2024

Fundamental Study on Methods of Protecting Cryptographic Modules from IEMI Fault Injection Using Spread Spectrum Clocking

Hikaru Nishiyama, Daisuke Fujimoto, and Yuichi Hayashi
Nara Institute of Science and Technology, Nara, Japan

Abstract

A threat of intentional electromagnetic interference (IEMI) fault injection has been reported to extract the secret key of cryptographic devices by superimposing electromagnetic (EM) waves on the clock supplied to the cryptographic module via power cable. Furthermore, a threat has been demonstrated to reduce the time cost required for secret key analysis by synchronizing the clock and EM waves and controlling the phase of EM waves. In response, this paper proposes a countermeasure involving the disruption of EM wave synchronization and phase control through dynamic phase variation of the clock in each cycle.

In this paper, we specifically focus on the spread spectrum clocking (SSC), which is a technique to vary the phase of the clock. And we demonstrate that using SSC to the cryptographic module can make it more difficult to apply to synchronize to the clock and control the phase of CW, thereby increasing the time cost required for key analysis. We experimentally confirmed that a clock with 1.0 % frequency modulation can increase the time cost required for secret key analysis by about 38 times using an evaluation board.

1. Introduction

A threat of intentional electromagnetic interference (IEMI) has been reported to occur faults necessary for secret key analysis of cryptographic modules without obtaining signals related to synchronization, such as triggers, by superimposing electromagnetic (EM) waves on the clock supplied to the cryptographic module via power cables [1].

Additionally, a method has been proposed to synchronize the continuous wave (CW) used as EM waves with the clock supplied to the cryptographic module and controlling the phase of CW to increase the occurrence rate of faults which can use for secret key analysis [2].

To counter this threat, it is effective to vary the phase of the clock at each clock cycle. Such a clock phase variation can make more difficult to synchronize the clock and CW even though an attacker controls the phase of CW, thereby reducing the occurrence rate of faults which can use for secret key analysis.

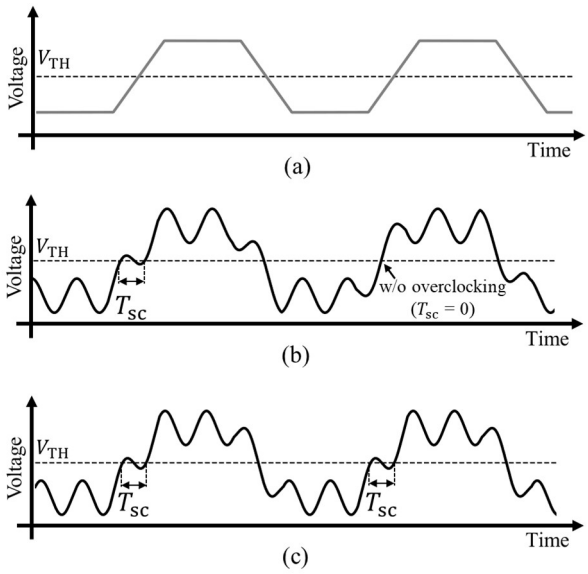


Figure 1. (a) Clock signal without injecting CW. (b) Clock signal with injecting CW. (c) Clock signal with injecting CW and applying a method of [2].

Therefore, in this paper, we focus on spread spectrum clocking (SSC) as a technique to vary the phase of such clocks, which is easy to implement, and show that it is possible to increase the time cost required for key analysis using fault injection applying a method in [2].

2. Methods of Protecting Cryptographic Modules from IEMI Fault Injection Using SSC

In this section, we shortly describe the fault occurrence mechanism by superimposing CW on the clock and about the method in [2]. After that, the effect of the using SSC for cryptographic module on the fault injection method in [2] is then described.

In the case of synchronous circuits which is a common implementation of cryptographic modules, cryptographic operations are executed in synchronization with a clock. The cryptographic operations are executed in units called

round operation, and the period of the clock signal is set with a sufficient margin for the execution time of the round operation. As shown in Figure 1(a), the round operation starts when the rising edge of the clock signal exceeds the threshold voltage (V_{TH}) of the circuit.

On the other hand, as shown in Figure 1(b), when a clock glitch generated in the clock due to the superimposition of CW is superimposed near V_{TH}, in addition to the original rising edge of the clock, an illegal rising edge due to the glitch occurs. This causes a forced increase in operating frequency (overclocking). If overclocking occurs before the round operation has not been completed, the calculation result will be incorrect, and a fault occurs.

Most of the existing studies on key analysis methods [3,4,5] assume the occurrence of faults only for a specific single round. Therefore, the attacker needs to increase the probability of occurrence of single-round faults since the time cost of key analysis increases when faults other than those that can be used for key analysis.

On the other hand, as shown in Figure 1(b), if the injection time of CW is asynchronous to the start time of the encryption process, whether overclocking occurs and the length of the shortened clock cycle(T_{sc}) by overclocking are randomly changed for each clock cycle. In this case, it is difficult to control the number of fault rounds, and the number of single-round faults is low.

In contrast, as shown in Figure 1(c), clock glitches are generated at a constant T_{sc} per clock cycle using the method in [2]. And this method increases the occurrence rate of single-round faults by manipulating the length of T_{sc} so that it is shortened for only the longest processing time (T_{CP}) among all rounds.

Specifically, the phase between clock and CW can be synchronized by setting the CW frequency to an integer multiple of the clock frequency, thereby the situation shown in Figure 1(c) can be realized. Under this condition, if the phase of CW is controlled from θ_A to θ_B, the length of T_{sc} can be manipulated in the range from t_{min} to t_{max} as shown in Figure 2. Then, when the length of T_{sc} is changed by controlling phase of CW, it can be assumed that the probability of total faults and single-round faults among them gradually change as shown in Figure 3.

Also, from the general assumption of fault injection, it is known whether a fault has occurred or not by the attacker. Therefore, the attacker can observe only changes in the total number of faults. The attacker can estimate the phase of the CW (θ_{target}) where single-round faults occur with high probability from the change in the total number of faults and apply only the faulty output obtained around that phase to the key analysis to make it more efficient.

In contrast, when SSC is applied to the clock, the phase of the clock glitch superimposed on the clock varies with each clock cycle as shown in Figure 4. Therefore, whether

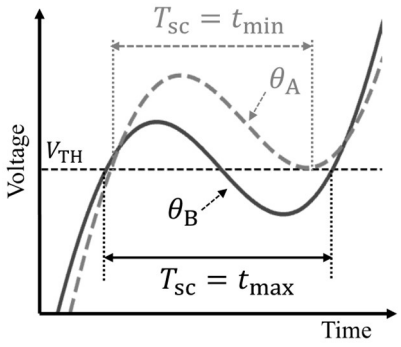


Figure 2. Image of varying the length of T_{sc} by controlling phase of CW.

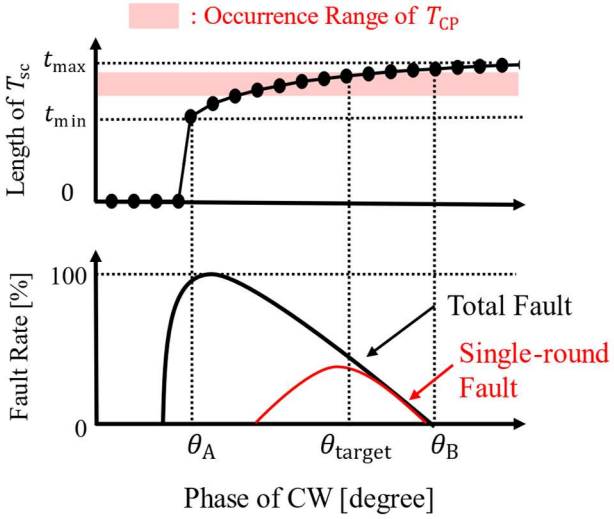


Figure 3. Relationship between the length of T_{sc} by controlling phase and the number of total faults and single-round faults.

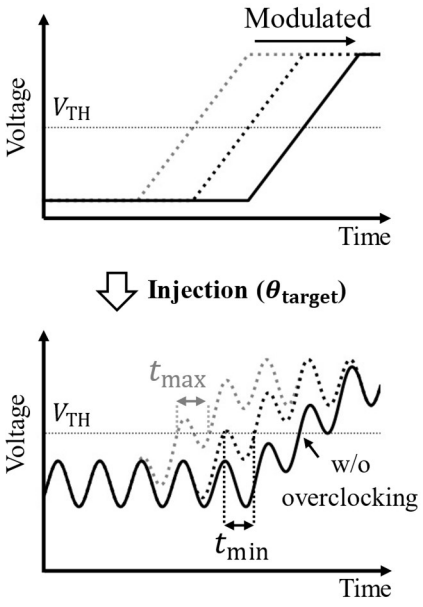


Figure 4. Image of frequency modulation of clock by SSC and variation of whether overclocking occurs and the length of T_{sc}.

overclocking occurs and the length of T_{sc} are not uniquely determined and change with each clock cycle. As a result, even though the attacker controls the phase of CW to search for the phase of θ_{target}, there is no dependency of total faults and single-round faults with the CW phase, thereby invalidating the fault injection method in [2].

3. Evaluation of the Proposed Method

3.1 Experimental Setups.

Figure 6 shows a block diagram of the experimental setup. As the cryptographic device, we use SASEBO-G that is an evaluation board [6]. As the cryptographic module, 128-bit Advanced Encryption Standards (AES-128) was implemented in the FPGA on SASEBO-G. The clock supplied to the cryptographic module is a 24 MHz square wave generated from a signal generator and supplied to the SMA port connected to FPGA clock input.

The generation of SSC is realized by frequency modulation using a function of signal generator, and the modulated signal is a sinusoidal wave. The modulation degree of the frequency is started from 0.0 %, which is the unmodulated state. And it increments for 0.1 % step until no change in the number of total faults caused by CW phase control is observed.

The CW used as EM waves is generated using the same signal generator for the clock and injected via injection probe on power supply cable. The injection frequency is fixed at 144 MHz and the amplitude at 32.0 dBm same as [2]. The phase of CW is swept by 3° and the number of total faults and single-round faults is measured when the encryption process is performed using 200 random plaintexts for each CW phase.

3.2 Experimental Results

Figure 7 shows the distribution of the total number of faults and the number of single-round faults over 200 encryption operations when the CW phase is controlled.

Figure 7(a) shows the results for a frequency modulation degree of 0.0 % that is before using SSC. The total number of faults changes and the number of single-round faults increases in the phase range of 30° to 120°. Since the attacker can observe the change in the total number of faults, the analysis can be made more efficient by using only the fault output obtained in this phase range.

Next, Figure 7(b) shows the case of 0.1 % modulation. The variations of the number of total faults and single-round faults are slower than in Figure 7(a), but it is still visible. The reason for this is that when the modulation degree is small, the variation of the clock phase per clock cycle is also small. As a result, the phase of CW remains close to the phase targeted by the attacker, and the dependency

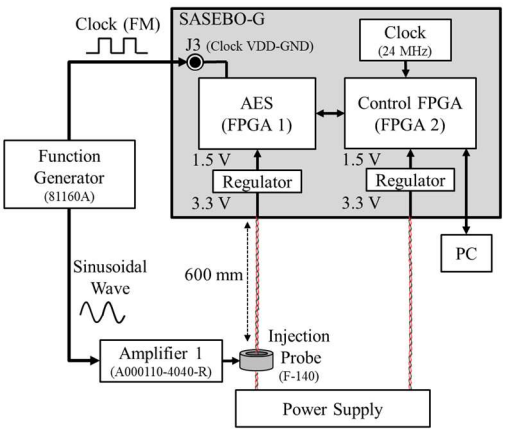
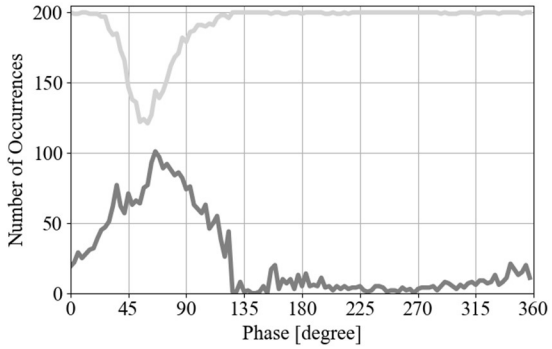
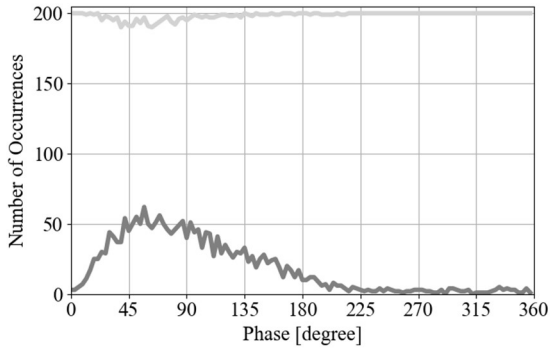


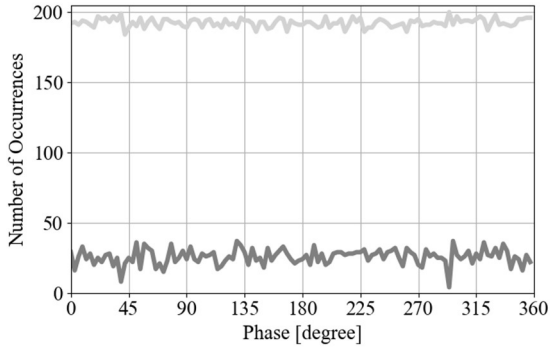
Figure 6. Block diagram of experimental setup.



(a) w/o SSC (Modulation Degree: 0.0 %)



(b) w/ SSC (Modulation Degree: 0.1 %)



(c) w/ SSC (Modulation Degree: 1.0 %)

Figure 7. Distribution of the number of total faults and single-round faults with controlling phase for each SSC frequency modulation degree.

between the phase of CW and the number of faults is still exists.

Finally, result at 1.0 % modulation is shown in Figure 7(c). The total number of faults and single round faults are uniform for all phases of CW. These results indicated that the application of SSC at a certain modulation degree can make it difficult to estimate the phase with many single-round faults based on the change in the number of fault occurrences due to phase control.

3.3 Comparison of Time Cost required for Key Analysis with different SSC Modulation Degree

Next, we compare the time cost required for key analysis on differential fault analysis (DFA) for each SSC modulation degrees for the one-byte fault at only the input intermediate value of the eighth round (8R1B Fault), which is assumed in the key analysis method [3]. It has been shown that this method can uniquely obtain the secret key by using only two faulty ciphertexts satisfying the 8R1B Fault [4]. On the other hand, since the attacker cannot determine whether the faulty ciphertexts are 8R1B Fault or not, it is necessary to perform a brute force analysis on ${}_{N_{\mathrm{Total}}}C_2$ streets, taking 2 out of the obtained N_{Total} faulty ciphertexts.

If we assume that the faulty ciphertext satisfying the 8R1B Fault is obtained with equal probability from all fault ciphertexts obtained, the number of DFA trials required for successful key extraction (N_{DFA}) can be expressed as in Equation (1).

$$N_{\mathrm{DFA}} = {}_{N_{\mathrm{Total}}}C_2 / {}_{N_{\mathrm{8R1B}}}C_2 \qquad (1).$$

Table 1 shows the results of N_{Total}, N_{8R1B} and N_{DFA} calculated from Equation (1) in range of 30 ° to 120 ° for each SSC frequency modulation degree in Figure 7. From these results, it can be confirmed that N_{DFA} tends to increase with the application of SSC and its modulation degree and N_{DFA} can be increased from 621 to 23,675 at a modulation of 1.0 %, where the number of faults is uncorrelated with the number of single-round faults. Furthermore, we confirmed that the time cost required for key analysis can be increased by about 38 times (≈23,675/621).

4. Conclusion

In this paper, we proposed a countermeasure against a threat that involves superimposing EM waves with controlled phase onto the clock of a cryptographic module, enabling non-invasive fault injection. The concept of the countermeasure is designed to make the synchronization and phase control of EM waves more difficult by varying the phase of the clock in each cycle. Specifically, we employed a technique for varying the clock phase, known as SSC, and supplied a clock with a 1.0 % frequency modulation to the cryptographic module. Our results demonstrate that this approach can increase the time cost required for secret key analysis by approximately 38 times in the described attack method, thereby confirming the effectiveness of the proposed method as a countermeasure.

Table 1. Results of N_{Total}, N_{8R1B} and N_{DFA} for each SSC frequency modulation degrees.

	N_{Total}	N_{8R1B}	N_{DFA}
(a)	4974	200	621
(b)	5856	42	19911
(c)	5797	38	23,675

5. Acknowledgements

This work was supported by JST CREST Program under Grant JPMJCR19K5, JST FOREST Program under Grant JPMJFR206L, JSPS KAKENHI under Grant JP23H00472, and Grant JP23H03397.

References

[1] Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, and H. Sone, “Transient IEMI Threats for Cryptographic Devices,” IEEE Transactions on Electromagnetic Compatibility, 2013.

[2] H. Nishiyama, D. Fujimoto, H. Sone, Y. Hayashi. "Efficient Noninvasive Fault Injection Method Utilizing Intentional Electromagnetic Interference." IEEE Transactions on Electromagnetic Compatibility, 2023.

[3] G. Piret and J.-J. Quisquater, “A differential fault attack technique against SPN structures, with application to the AES and khazad,” in Cryptographic Hardware and Embedded Systems—*CHES 2003 (LNCS 2779)*, 2003.

[4] C. Giraud, A. Thillard, “Piret and Quisquater’s DFA on AES Revisited,” Cryptology ePrint Archive, Report 2010/440, 2010.

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

[6] “Side-channel attack standard evaluation board,” 2007. [Online]. Available: https://www.risec.aist.go.jp/project/sasebo/