2012 International Conference on Information and Computer Networks (ICICN 2012)
IPCSIT vol. 27 (2012) © (2012) IACSIT Press, Singapore

Dedicated Evaluation System for Fault Attacks

Masaya Yoshikawa [1], Makoto Katsube [2] and Toshiya Asai [1]

[1] Department of Information Engineering, Meijo University, JAPAN

[2] Graduate School of Science and Technology, Meijo University, JAPAN

Abstract. Generally, integrated circuit (IC) chips (cryptographic circuits) used for credit and cash cards are secured by encrypting data. The encryption standard, which has been widely diffused in recent years, is certified that its decryption is computationally impossible. However, it was recently reported that even if an encryption algorithm is theoretically secured, when the algorithm is incorporated into hardware, confidential information about the algorithm could be improperly specified when the hardware is operated. Such improper specifications are generally called side-channel attacks. In particular, the fault attack, which is causing failure intentionally and reveals a secret key, is very risky. In this paper, we proposed new dedicated evaluation system for fault attacks. The proposed system achieves evaluations of the resistance against the fault attack on actual devices. Experimental result using FPGA board shows the validity of the proposed evaluation system.

Keywords: Information Security, Fault attack, Tamper Resistance, Cryptographic System

1. Introduction

Security LSI stores monetary and personal identifiable information as electronic circuit data, and is used for electronic money or electronic identification devices. Cryptographic circuits are used to protect confidential information incorporated into LSI, and an internal confidential key of a cryptograph, which is an essential element of security is protected not to be illegally read. It is sufficiently proven that encryption standard algorithms used in cryptographic circuits cannot be decrypted computationally. However, studies on various physical analysis attacks that steal internal information by physically attacking LSI have been advanced [1]-[5]. In particular, the fault attack, which is causing failure intentionally and reveals a secret key, is very risky. Therefore, when an encryption algorithm is incorporated into hardware, it is important to evaluate the resistance against the fault attack.

However, almost all previous studies on the fault attack focused to the theoretical analysis. By contrast, there are few studies which discuss how to generate the fault on actual devices.

In this paper, we proposed new dedicated evaluation system for fault attacks. The proposed system achieves evaluations of the resistance against the fault attack on actual devices. Experimental result using FPGA board shows the validity of the proposed evaluation system.

2. Fault attack for Advanced Encryption Standard

Advanced encryption standard (AES) is one of encryption standards and it is widely used. The round processing of AES is performed in the form of a byte unit, and a plain text, a cryptogram and a secret key are composed of 16 8-bit sub-blocks. In AES, since MixColumns processing is not performed in the 10th round (final round), a cryptogram corresponds to the medium value of the round before the final round in the form of a byte unit.

On the other hand, the fault attack injects faults during encryption processing and it reveals the secret key using cipher texts with faults. Differential Fault Analysis (DFA) is one of fault attacks. Fig.1 shows an example of DFA which is applied to AES. In DFA, faults have to be injected between the rounds 8 and 9.

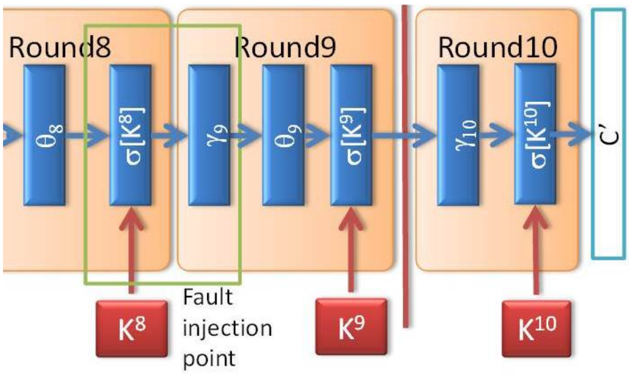


Fig. 1 Example of DFA which is applied to AES

It assumes K^{10}, which is the key on the round 10, and the value of cipher text on the beginning of the round 10 is calculated using that on the end of the round 10.

$$\gamma_{10}^{-1}\circ\sigma\left[K^{10}\right](C) = \text{4C CC 9C A2 AC 4B DB 61 87 23 6A 5B EA 1A 9F 15} \tag{1}$$

$$\gamma_{10}^{-1}\circ\sigma\left[K^{10}\right](C') = \text{4C CC 9C A2 AC 4B DB 61 }\underline{\text{A6}}\ \underline{\text{02}}\ \underline{\text{09}}\ \underline{\text{19}}\text{ EA 1A 9F 15} \tag{2}$$

Here, *C* indicates a cipher text, and C' indicates a cipher text with faults. The difference of the correct cipher text and the cipher text with faults is calculated.

$$\gamma_{10}^{-1}\circ\sigma\left[K^{10}\right](C)\oplus\gamma_{10}^{-1}\circ\sigma\left[K^{10}\right](C')$$
$$= \text{00 00 00 00 00 00 00 00 21 21 63 42 00 00 00 00} \tag{3}$$

Thus, the difference can reduce the number of the candidates of the secret key. The secret key is revealed by repeating this procedure..

3. Proposed system

The proposed evaluation system injects faults during encryption processing using glitch pulse on the system clock. Fig.2 shows the proposed system.

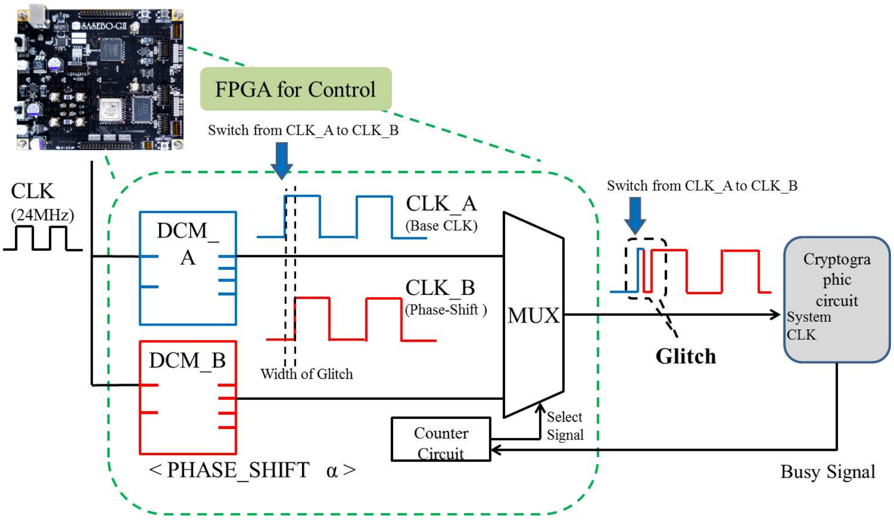


Fig. 2 The proposed evaluation system

It generates two clock signals with the difference phases, using two digital clock managers (DCMs) as shown in Fig.2. Here, these clock signals are switched to arbitrary timing using a counter circuit. Specifically, the number of rounds is counted using the busy signal from the counter circuit. In order to inject faults, the glitch pulse has to satisfy logic thresholds. Fig.3 shows an example of a generated glitch pulse during encryption processing of the round 8.

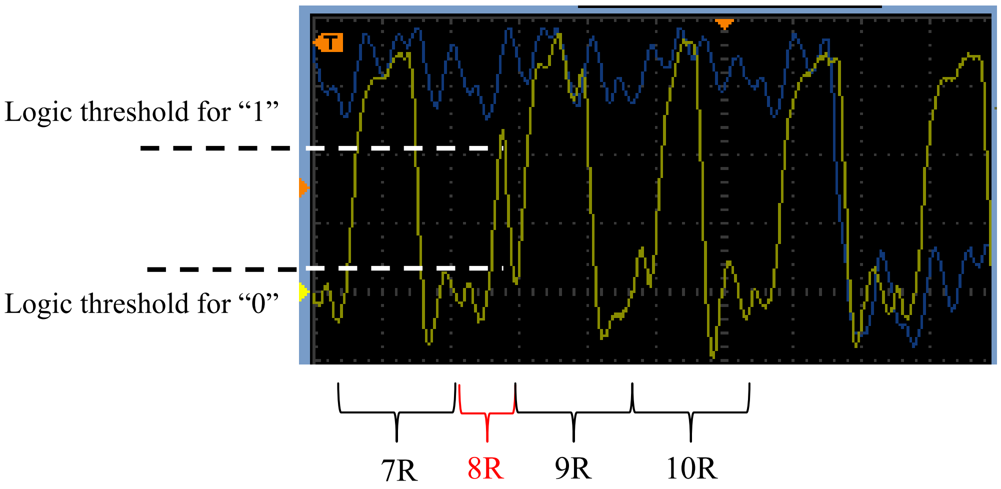


Fig.3 Example of a generated glitch pulse during encryption processing of the round 8

4. Experiment

To verify the validity of the proposed evaluation system, several experiments were performed. In experiments with an actual device, SASEBO-GII, a board for evaluating side-channel attacks, was used. A module of SubBytes transformation of AES was described by applying the truth table method to circuit. In this experiment, the fault of which "7F" converted to "7E" was injected at the 7th state on round 8. The correct cipher text is as follows.

3A A2 1F 26 72 B2 91 2D E4 A5 79 64 CA 60 89 FC (4)

By contrast, the cipher text with faults is as follows.

3A A2 1C 26 72 E3 91 2D D7 A5 79 64 CA 60 89 11 (5)

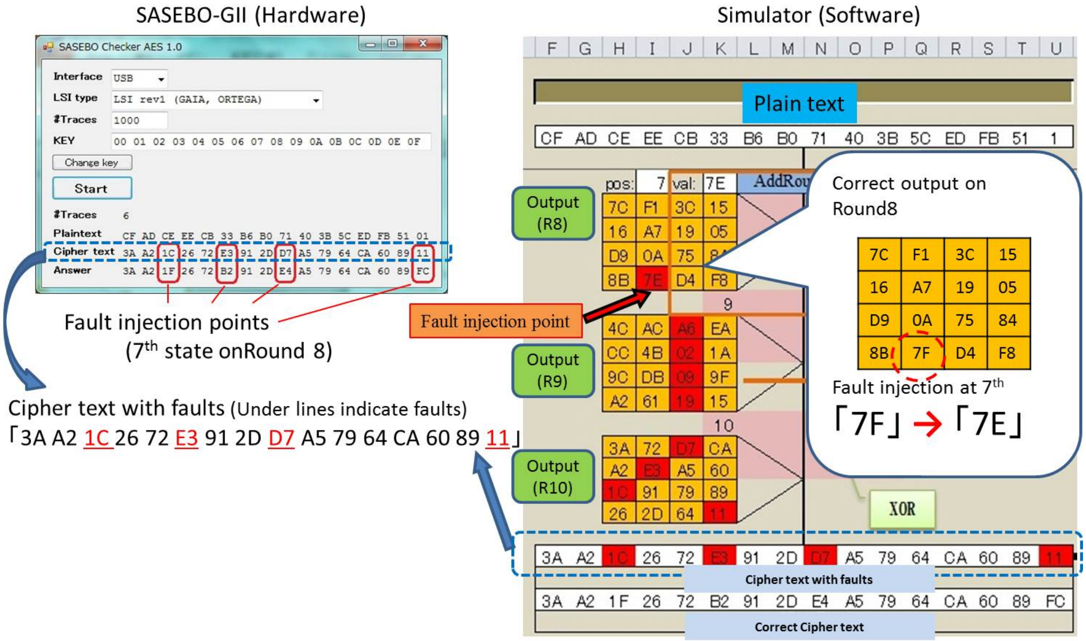
Fig.4 shows the experimental result. The proposed system was able to inject the fault at specific timing on actual device as shown in Fig.4.

5. Conclusion

This study proposed new dedicated evaluation system for fault attacks. The proposed system achieves evaluations of the resistance against the fault attack on actual devices. Experimental result using FPGA board shows the validity of the proposed evaluation system. In the future, we will evaluate the other SubBytes transformation modules such as PPRM1, PPRM3, and composite field type. We will also apply the proposed method to resistance verification against the other fault attack methods.

6. Acknowledgements

This study is supported by Japan Science and Technology Agency (JST), Core Research for Evolutional Science and Technology (CREST).



Interface USB
LSI type LSI rev1 (GAIA, ORTEGA)
#Traces 1000
KEY 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
#Traces 6
Plaintext CF AD CE EE CB 33 B6 B0 71 40 3B 5C ED FB 51 01
Cipher text 3A A2 1C 26 72 E3 91 2D D7 A5 79 64 CA 60 89 11
Answer 3A A2 1F 26 72 B2 91 2D E4 A5 79 64 CA 60 89 FC

Fig.4 Experimental result

7. References

[1] S.S.Ali, D.Mukhopadhyay, "A Differential Fault Analysis on AES Key Schedule Using Single Fault", *Proc. of 2011 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp.35-42, 2011.

[2] Chong Hee Kim, J.J.Quisquater, "Faults, Injection Methods, and Fault Attacks", IEEE Design & Test of Computers, Vol.24, No.6, pp.544-545, 2007.

[3] Gaoli Wang, Shaohui Wang, "Differential Fault Analysis on PRESENT Key Schedule", Proc. of 2010 International Conference on Computational Intelligence and Security (CIS), pp.362-366, 2010.

[4] Wei Li, Dawu Gu, Yong Wang, Juanru Li, Zhiqiang Liu, "An Extension of Differential Fault Analysis on AES", *Proc. of Third International Conference on Network and System Security (NSS)*, pp.443-446, 2009.

[5] P.Maistri, R.Leveugle,"Double-Data-Rate Computation as a Countermeasure against Fault Analysis", IEEE Transactions on Computers, Vol.57, No.11, pp.1528-1539, 2008.