An Information Theoretic Perspective on the Differential Fault Analysis against AES

Yang Li[1], Shigeto Gomisawa[1], Kazuo Sakiyama[1], Kazuo Ohta[1]

The University of Electro-Communications
1-5-1 Chofugaoka, Chofu-shi, Tokyo 182-8585, Japan
{liyang,g-shigeto-lfat,saki,ota}@ice.uec.ac.jp

Abstract. Differential Fault Analysis (DFA) against AES has been actively studied these years. Based on similar assumptions of the fault injection, different DFA attacks against AES have been proposed. However, it is difficult to understand how different attack results are obtained for the same assumption of fault injection. It is also difficult to understand the relationship between similar assumptions of fault injections and the corresponding attack results. This paper reviews the previous DFA attacks against AES from an information theoretic point of view, and gives a general understanding for DFA attacks against AES.

Keywords: Differential Fault Analysis, AES, Information theory

1 Introduction

In 1997, public key cryptosystems were pointed to be vulnerable to fault attacks that use computational errors during the execution [3]. At the same year, Biham and Shamir applied this idea to block cipher DES and introduced the concept of Differential Fault Analysis (DFA) [1]. Given an encryption of a block cipher, a fault-free ciphertext can be obtained for a plaintext, and then by injecting a certain kind of fault during an execution of the cryptographic calculation, attackers can obtain a faulty ciphertext as well. The assumptions of the fault injection are referred as the **fault model** in this paper. DFA obtains the information of the secret based on the fault-free ciphertext and the faulty ciphertext under a certain fault model.

This paper focuses on the DFA attacks against Advanced Encryption Standard (AES) excluding the cases where faults are injected at the key schedule. In the early stage of DFA attacks against AES, the full recovery of the secret key were likely to require 50 to 250 faulty ciphertexts [4, 5, 8]. Later in researches shown in [7, 9, 10], only two or one faulty ciphertext enabled attackers to recovery the secret key. However, these papers presented different attack results for the same fault model that disturbs a random single byte. In 2009, a DFA attack called diagonal fault analysis was proposed [2]. Their attack can retrieve the full key with one faulty ciphertext with a fault model allowing multiple faulty bytes. In 2006, Moradi, Shalmani and Salmasizadeh proposed a generalized DFA attack against AES [6]. In brief, the generality of their attack is achieved by dividing all possible faults into two groups, and giving attack methods for each group. Based on the simulation, they found that 6 faulty ciphertexts in average can identify the secret key for the first group, while 1500 faulty ciphertexts were needed for the second group. It is not difficult to find that the fault models used in [2], [6] are also similar to those used in [7, 9, 10], however different attack results were obtained as well.

In this paper, DFA attacks against AES are analyzed through an information theoretic point of view. Assumptions in a fault model are regarded as the information of the differential between a fault-free intermediate value and a faulty intermediate value. Based on revealing the relationship between the differential of intermediate values and the information of secret key, we give a simple understanding for the existing DFA attacks against AES. Our analyses find that there is a limitation of the attack efficiency for each fault model. The DFA attacks in [10], [2] and [6] reached the limitations of their fault models, while attacks in [7, 9] do not. Also, we propose a simple model for predicting the attack efficiency. Our prediction model obtains the similar results with the simulation results provided in the previous papers. In other word, this paper provides a generalized and simple understanding for the DFA attacks based on the similar fault models, and proposes an optimized attack flow for the DFA attacks as well.

This paper is organized as follows. In Sect. 2, we briefly explain the structure of AES. In Sect. 3, we generally analyze the DFA attacks against AES through the perspective of information theory. In Sect. 4, several related previous DFA attacks against AES are reviewed on the observation of information theory. In Sect. 5, we discuss possible future research about the DFA attacks against AES. In Sect. 6, we conclude this paper.

2 Overview of the Structure of AES-128

In 2000, AES was selected as the new standard of symmetric key encryption by the US government. AES is 128-bit block cipher, and has three kinds of key sizes as 128, 192 and 256 bits. This paper only deals with the encryption of AES with 128-bit secret key (AES-128). In this paper a plaintext, an intermediate value and a ciphertext of AES-128 are denoted by P, I and C, respectively. AES operates on a 4×4 state matrix as shown in Table 1. Every element of the state matrix is a byte represented by I_{ij}, where $i, j \in [0, 3]$ and i, j are its row and column positions, respectively. Notice that, P, K and C can be expressed in the same manner.

I_{00}	I_{01}	I_{02}	I_{03}
I_{10}	I_{11}	I_{12}	I_{13}
I_{20}	I_{21}	I_{22}	I_{23}
I_{30}	I_{31}	I_{32}	I_{33}

Table 1. AES state matrix

AES-128 consists of 10 rounds. Each round has its own round key denoted by K^i, where $i \in [1, 10]$. Each round key can be expanded from the original key K by the AES key schedule scheme. Conversely, obtaining a round key is equivalent to obtaining the original key and all the other round keys. After the initial AddRoundKey, the first 9 rounds of AES consist of four AES round operations as SubBytes, ShiftRows, MixColumns and AddRoundKey. The last round of AES-128 only consists of SubBytes, ShiftRows and AddRoundKey.

Before we introduce the details, we list several notations used in this paper. We denote the faulty intermediate value and the faulty ciphertext by I' and C', respectively. The differential between I and I' $(I \oplus I')$ is denoted by $\mathit{\Delta} I$, and that between C and C' $(C \oplus C')$ is denoted by $\mathit{\Delta} C$.

The functionalities of AES operations on the real values (*e.g.* I, I') and the differential values (*e.g.* $\mathit{\Delta} I$) are briefly explained as follows.

AddRoundKey(ARK)

As shown in Table 2, the AddRoundKey performs the exclusive OR calculation ($\oplus$) between the current state and the corresponding round key. AddRoundKey affects the real value of each byte in the state, but does not affect the differential between the fault-free state and faulty state.

$$\begin{array}{|c|c|c|c|}\hline I'_{00} & I'_{01} & I'_{02} & I'_{03} \\ \hline I'_{10} & I'_{11} & I'_{12} & I'_{13} \\ \hline I'_{20} & I'_{21} & I'_{22} & I'_{23} \\ \hline I'_{30} & I'_{31} & I'_{32} & I'_{33} \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline I_{00} \oplus K_{00} & I_{01} \oplus K_{01} & I_{02} \oplus K_{02} & I_{03} \oplus K_{03} \\ \hline I_{10} \oplus K_{10} & I_{11} \oplus K_{11} & I_{12} \oplus K_{12} & I_{13} \oplus K_{13} \\ \hline I_{20} \oplus K_{20} & I_{21} \oplus K_{21} & I_{22} \oplus K_{22} & I_{23} \oplus K_{23} \\ \hline I_{30} \oplus K_{30} & I_{31} \oplus K_{31} & I_{32} \oplus K_{32} & I_{33} \oplus K_{33} \\ \hline \end{array}$$

Table 2. AES AddRoundKey

SubBytes(SB)

Each byte of the state is substituted by another value according to the AES S-box table. The mapping of AES S-box is bijective. On the other hand, any non-zero differential byte will be substituted by another value, and the zero differential byte will still be zero.

ShiftRows(SR)

As shown in Table 3, the rows of the state are cyclically shifted according to the row number, so does the differential values.

$$\begin{array}{|c|c|c|c|} \hline I_{00} & I_{01} & I_{02} & I_{03} \\ \hline I_{10} & I_{11} & I_{12} & I_{13} \\ \hline I_{20} & I_{21} & I_{22} & I_{23} \\ \hline I_{30} & I_{31} & I_{32} & I_{33} \\ \hline \end{array} \xrightarrow{SR} \begin{array}{|c|c|c|c|} \hline I_{00} & I_{01} & I_{02} & I_{03} \\ \hline I_{11} & I_{12} & I_{13} & I_{10} \\ \hline I_{22} & I_{23} & I_{20} & I_{21} \\ \hline I_{33} & I_{30} & I_{31} & I_{32} \\ \hline \end{array}$$

Table 3. AES ShiftRows

MixColumns(MC)

A linear transformation performed on each column of the state computed by

$$\begin{bmatrix} I'_{0i} \\ I'_{1i} \\ I'_{2i} \\ I'_{3i} \end{bmatrix} = \begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{bmatrix} \cdot \begin{bmatrix} I_{0i} \\ I_{1i} \\ I_{2i} \\ I_{3i} \end{bmatrix},$$

where $i \in [0, 3]$ and the multiplication is performed in GF(2^8). The differentials are affected in the same manner with the real values of the state.

3 Information Theoretic Perspective on DFA

3.1 The Fault Model for DFA

Every fault model assumes that it is possible to inject a certain type of faults at a certain state of the AES calculation. For example, the most frequently discussed fault model is the one that assumes attackers can disturb a random byte at the input of the 8^{th} round of AES. Hereafter we refer this fault model as **Piret's fault model**, since it was first introduced by Piret *et al.* [9]. And we refer the state where a fault is injected by **injection state**. Through the perspective of information theory, the fault model can be considered as the information of ΔI at the injection state (differential between the fault-free intermediate value and the faulty one). In addition to the values of (C, C'), DFA is regarded as cryptanalysis where attackers try to obtain the information of a secret key based on the information of $\varDelta I$ at the injection state.

The differential between two different random 128-bit values has $2^{128} - 1$ candidates. While in Piret's fault model, the differential only has 255×16 candidates, where 255 and 16 correspond to 255 possible differential values and 16 possible fault positions. We can see that this fault model provides $-\log_2 \frac{1}{2^{128}} - (-\log_2 \frac{1}{255\times16}) = 116$ bits of information of $\varDelta I$ at the injection state. In [9], based on a pair of (C, C'), the key space of AES-128 can be restricted to 2^{40}. This result can be understood as this DFA attack obtains $128 - 40 = 88$ bits information of a secret key from a pair of (C, C') and $128 - 12 = 116$ bits information of $\varDelta I$ at the injection state.

3.2 Basic Attacks for DFA

In the sense of information theory, given a pair of plaintext and ciphertext (P, C), the secret key K can be identified theoretically. As far as our knowledge, since there is no practical cryptanalysis against full round AES-128 so far, so that attackers can only use the information of (P, K) by exhaustive searan In the exhaustive search, every possible key candidate is used to encrypt the plaintext to get a ciphertext candidate. Only when a tested key is correct, the obtained ciphertext candidate is the same as the real one. Practically, the key has 128 bits and the exhaustive search over 2^{128} key candidates cannot be performed in a practical time.

The exhaustive search for DFA based on (C, C') and the information of $\varDelta I$ at the injection state also exists. The similar idea was explained as the **basic attack** for DFA in [9]. Under a certain fault model, attackers need to get the correct ciphertext C and the faulty ciphertext C'. Every pair of (C, C') and the fault model can provide information of a key and restrict the key space. Repeatedly restricting the key space based on a different faulty ciphertext, the key can be identified in final. The algorithm of the basic attack for DFA is shown as follows.

1. Have a guess of the secret key K_g from a list of possible keys.
2. Calculate the values of I and I' at the fault injection state based on (C, K_g) and (C', K_g), respectively.
3. Calculate the differential $\varDelta I$ and check whether $\varDelta I$ satisfies the fault model or not. If not, delete K_g from the key list. Otherwise, keep it in the list.

4. If the key list has more than one candidate, take another faulty ciphertext and repeat steps 1, 2 and 3 to restrict the current key list. Hereafter we refer steps 1, 2 and 3 as a **DFA search**.

On the one hand, according to this basic attack algorithm, the exhaustive search for DFA has to be performed for at least 2^{128} keys, so that it could not be practical with regard to the computational cost. On the other hand, the basic attack can fully use the information provided by any fault model to restrict the key space, so that it could reach the maximal attack efficiency with regard to the information theory.

3.3 Divide and Conquer used in DFA Attacks

The basic technique used for turning the basic attack into a practical DFA attack is **divide and conquer**. By dividing the 128-bit key into several parts and analyze them part by part, the key search space can be reduced dramatically.

The last three rounds of AES when one byte is disturbed at the beginning of the 8^{th} round are shown in Fig 1.

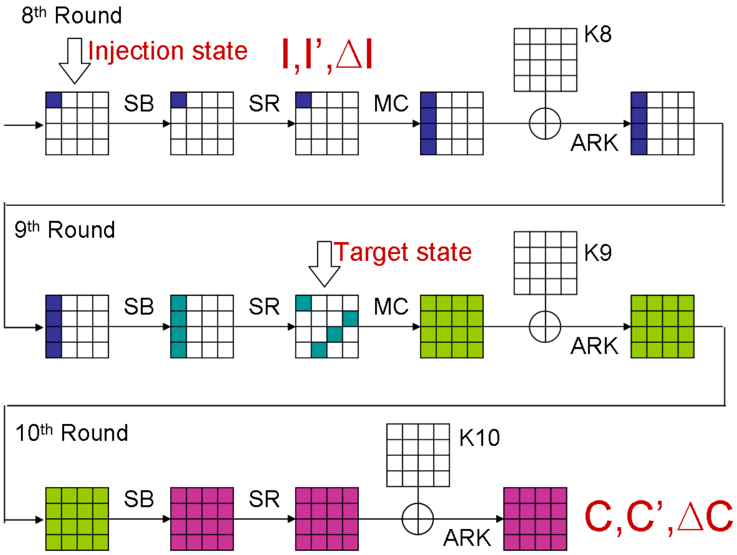

Fig. 1. The last three rounds of 128-bit AES when one byte is disturbed at the beginning of the 8^{th} round.

One byte fault injected at the beginning of the 8^{th} round propagates to four bytes of a column in the 8^{th} MixColumns. And these four non-zero faulty bytes will be reserved after the 9^{th} SubBytes, and will be shift to each row in the 9^{th} ShiftRows. Notice that from the 9^{th} MixColumns to the output of ciphertext, only the 9^{th} MixColumns performs the operation relates to 4 bytes, other operations are all byte-wise independent. Here we refer the state before the 9^{th} MixColumns as **the target state**. Notice when attackers take a guess of four related bytes of K^{10}, four bytes of differential at the target state can be calculated. So that until the target state, the DFA search of 16 bytes of K^{10} can be divided into four groups to be searched separately. Each group has four bytes, so that the total search space becomes $2^{32} \times 4 = 2^{34}$. Also this DFA search only performs about 2/10 of the AES decryption, a DFA search over 2^{32} keys can be finished in a practical time for a normal PC [1].

Under the same fault model, as long as different amounts of information from the fault model are used, different attack results will be obtained. The more information of ΔI at the injection state used in the DFA search, the less key will left, as a result the attack will be more efficient. However, not all the information of ΔI can be easily exploited considering the computational cost. There is a limitation for improving the attack efficiency of DFA under every fault model, which can be achieved by the basic attack theoretically but not practically.

4 Review the Previous DFA attacks against AES

In 2003, Piret and Quisquater proposed a DFA attack against AES based on disturbing one random byte of the AES state between the 7^{th} MixColumns and 8^{th} MixColumns [9]. We refer this attack by Piret's attack in this paper. According to their analysis method, two well-located faults are needed for easy retrieving of the key, and one fault can reduce the size of the key space to 2^{40}. According to the structure of AES shown in Fig. 1, one non-zero byte of ΔI at the injection state will propagate to 4 non-zero bytes of ΔI at the target state. Moreover, each column of ΔI at the target state will have only one non-zero byte. Then 16 bytes of K^{10} are divided into four groups to perform a DFA search independently and this DFA search checks whether a column of ΔI at the target state has only one non-zero byte. The simulations show that the average size of the key candidates of 4 bytes key is 2^{10}, so that the total

[1] We neglect analyzing the techniques that is used to speed up the DFA search over 2^{32} key candidates.

number of the key candidates is about 2^{40}. Note that some of the information of ΔI at the target state, such as the positions of 4 non-zero bytes are not used in Piret's attack.

In 2009, Mukhopadhyay proposed a DFA attack similar to Piret's attack [7]. Under the Piret's fault model, it is considered that attackers can first guess where the faulty byte is injected at the injection state. Then the positions of faulty bytes in ΔI at the target state are fixed, so that the total key space can be restricted to 2^{32}. Since there are 16 possibilities of the original faulty byte position, the total key space for the Piret's fault model can be restricted to $2^{32} \times 16 = 2^{36}$. The improvement comes from the information about the positions of the propagated faulty bytes at the target state is used in the DFA search. However, this work still does not fully exploit the information of Piret's fault model.

Later, in the same year, Tunstall and Mukhopadhyay further improved the DFA attacks based on the Piret's fault model [10]. At the first step, they guess the fault position and get the key space with size 2^{32}. Then in the second step, they applied the key schedule scheme to obtain K^9 based on each key candidate of K^{10}. Then each key candidate can be checked whether it comes from the one faulty byte before the 8^{th} MixColumns. For each position, the key space can be restricted to 2^8, so that the total key space can be reduced to 2^{12} in the second step. We can see that this work uses all the information of Piret's fault model and reaches the limitation of Piret's fault model.

In 2009, Saha, Mukhopadhyay and RoyChowdhury proposed a Diagonal Fault Attack [2]. Their fault model is that multiple faults are injected at the diagonal of the state matrix at the beginning of the 8^{th} round. In their analysis, when only one diagonal is with fault, a pair of (C, C') can restrict the total key space to 2^{34}. We can see that this attack result is already the limitation for this fault model. Different form Piret's fault model, this fault model cannot provide any information about the fault values at the target state.

In 2006, Moradi *et al.* proposed a generalized method of Differential Fault Attack against AES [6]. In their analysis, all possible faults are divided into two groups. By taking a column of ΔI at the target state, if at least one of the 4 bytes are fault-free, then this fault belongs to the first group, otherwise, it belongs to the second group. For the first group, the corresponding 32 bits of secret key can be obtained by a fault-free ciphertext and 6 faulty ciphertexts, while it need approximately 1500 faulty ciphertexts to identify 32 key bits for the second group. The fault model of their paper only provides information of the number of faulty bytes in a column of ΔI at the target state. The information of their fault model is already fully exploited in their analysis.

The attack results of these DFA attacks against AES are summarized in Table 4.

	Fault type	Attack efficiency in average
[9]	1 non-zero byte of ΔI at the state before 8^{th} MixColumns	2^{40} key candidates for a pair of (C, C')
[7]	1 non-zero byte of ΔI at the state before 8^{th} MixColumns	2^{36} key candidates for a pair of (C, C')
[10]	1 non-zero byte of ΔI at the state before 8^{th} MixColumns	2^{12} key candidates for a pair of (C, C')
[2]	Random values of a diagonal of ΔI before 8^{th} SubBytes	2^{34} key candidates for a pair of (C, C')
[6]	At least 1 zero byte of a column of ΔI at target state	1 C and 6 C' to identify a 128-bit key
	4 non-zero bytes of a column of ΔI at target state	1 C and 1500 C' to identify a 128-bit key

Table 4. The summary of attack results of DFA attacks against AES.

4.1 The General Attack Flow of DFA

The attack flow of DFA can be mainly divided into two kinds based on whether plaintext is used. If the plaintext corresponding to the fault-free ciphertext is unknown, only faulty ciphertexts can be used to identify the key. Otherwise, attackers can first restrict the key space to a reasonable size based on faulty ciphertexts, and then apply the exhaustive search based on (P, C) to identify the correct key. We can express this attack flow of DFA as follows.

$$2^{128} \xrightarrow{C,C',\Delta I} 2^{??} \xrightarrow{P,C} 1.$$

The better DFA attacks should request fewer faulty ciphertexts and cost less computations. As a result, betters DFA attacks should use more information of every pair of (C, C') and have a reasonable computational cost at the same time. When a fault model is given, attackers directly obtains the information of ΔI at the injection state. Then attackers needs to covert the information at the injection state to the one at the target state. Different types of information at the target state cost differently in DFA searches. We try to propose the best attack flow of DFA making a good trade-off between them.

First we separate the information that can be used in a DFA attacks into four types as follows.

1. The number of non-zero bytes in each column of ΔI at the target state.
2. The positions of non-zero bytes of ΔI at the target state.

3. The relationship between values of non-zero bytes of ΔI at the target state.
4. The information of (P, C).

The first type of information can be exploited by applying divide and conquer and it is the most important information that makes DFA attacks possible. The second type of information can be exploited by arranging the attack results after exploiting the first type of information. Then since checking the third type of information needs to pass at least two MixColumns, two SubBytes and key schedule, so that divide and conquer cannot be easily applied. The last information can identify the key, but it is the most costly calculation. When these four types of information are all available to attackers, the best attack flow of DFA should first use the first two types of information to restrict key space to a reasonable size. Then, the third type of information can be applied to further restrict the key space. Finally, the last information can be used to identify the key.

4.2 Predicting The Attack Efficiency of DFA

In this section, we discuss the relationship between the information of each fault model and the information of K. According to the structure of AES, (I, I') at the target state goes through MixColumns, SubBytes, ShiftRows and AddRoundKey to become (C, C'). Since MixColumns and SubBytes are bijective mapping with regard to a column of state or the entire state, and ShiftRows only change the positions of faulty bytes, we simplify this transformation as

$$BM(I) \oplus K = C, \tag{1}$$
$$BM(I \oplus \Delta I) \oplus K = C', \tag{2}$$

where BM stands for a bijective mapping, and I can be a column of target state or the entire target state.

Based on Eq. (1), when C is fixed, for each value of I, there is a corresponding value of K. The key space after a DFA search is equivalent to the number of I that can pass the Eq (3), where ΔC is fixed by (C, C') and ΔI at the target state are restricted by the information from the fault model.

$$BM(I) \oplus BM(I \oplus \Delta I) = \Delta C, \tag{3}$$

For each possible value of ΔC, the space of ΔI has been restricted by the differential distribution table of BM, but the key space has not been restricted.

After that, when we use the information from the fault model to further restrict the space of ΔI at the target state, the key space begins to be restricted.

Base on two conditions, we get a conclusion that the information of ΔI at the target state provides the same amount of information to the key. First, we assume that the information of ΔI at the target state provided by fault model is independent from that provided by the differential distribution table of BM. Then, assume the restriction condition of a DFA search covers $q\%$ of all possible faults, each possible ΔI that passed the differential distribution table of BM have the same probability of $q\%$ to pass the restriction of the fault model. Second, we assume that the value of I are uniformly distributed to the values of possible ΔI that passed the differential distribution table of BM. As a result, $q\%$ of I will pass the restriction of both the differential distribution table of BM and the fault model. Finally, $q\%$ of K are left after the DFA search.

In the case of the introduced DFA attacks against AES, the used fault model should have little correlation between the differential distribution table of BM. And according to the differential distribution table of AES S-box, the values of I are almost uniformly distributed for each possible ΔI as well. In a relaxed environment, we can use the conclusion that the size of ΔI restricted by the conditions for a DFA search is the same with the size of the key space after this DFA search. In other words, DFA attacks against AES can obtain the same amount of information about K with the information about ΔI used in this attack. It is checked that this prediction matches the simulation results given in [2, 6, 7, 9, 10].

For example, we try to predict the attack efficiency of the second type of DFA attacks in [6]. Since the fault model only has the information that four bytes of a column of ΔI at the target state are all non-zero, a pair of (C, C') provides $\log_2(\frac{2^{32}-1}{255^4}) \simeq 0.02259$ bit information of 4 bytes of ΔI at the target state. According to our prediction, the key also obtains about 0.02259 bit information from a pair of (C, C'). As a result, at lease 1420 faulty ciphertexts are needed to recover 32 bits of key ($1420 \times 0.02259 \simeq 32$), where the simulation result in [6] show that in average 1500 ciphertexts can identify 32-bit key. The simulation result also indicates that the information provided by different faulty ciphertexts are almost independent from each other.

5 Future Research of DFA against AES

Notice that in the DFA attack flow we proposed, DFA attacks first use the information of $\varDelta I$ at the target state to restrict the key space. Then for the restricted key space, the $\varDelta I$ at injection state is calculated to restrict the key space again. Finally, an exhaustive search based on (P, C) is applied to identify the key. Divide and conquer makes the information of $\varDelta I$ at the target state can be used in a practical time. The exhaustive search based on (P, C) is quiet difficult to be further improved. A possible future work for DFA attacks against AES is to find a method to speed up the DFA search up to the injection state.

Assume that attackers get a pair of (P, C) and get only one faulty ciphertext C' with a fault that is injected trying to follow the Piret's fault model. When the injected fault actually belongs to Piret's fault model, the key can be fully retrieved in a practical time. Otherwise, we can consider that multiple faulty bytes rather than a single faulty byte is injected. If the multiple faulty bytes locate at a diagonal of $\varDelta I$ at the injection state, the key can also be fully retrieved in a practical time [10].

However, the injected fault could be a very similar situation where two faulty bytes locate at two diagonals at the beginning of the 8^{th} round. In this case, after exploiting the first type of information about $\varDelta I$ at the target state, the key space can be restricted to $2^{74.3}$. After that, exploiting the second type of information about $\varDelta I$ at the target state can restrict the key space to $2^{66.54}$. Then, theoretically, the third type of information about $\varDelta I$ at the injection state can be used to restricted the key space to $2^{22.57}$ that is small enough for an exhaustive search based on (P, C). Finding a method to exploit the third type of information keys in a practical time could be an interesting future work [2].

6 Conclusions

This paper analyzes differential fault attacks against AES from an information theoretic perspective. The assumptions of fault injection are reviewed as the information of two intermediate values. DFA attacks against AES are considered as the cryptanalysis that obtains the information of key based on the two ciphertexts and the information of the fault injection. Several previous DFA works were reviewed from the information theoretic perspective. Based on our

[2] The size of key space is calculated based on the proposed prediction method.

analysis, every fault model has a limitation of the attack efficiency and we proposed a method to predict the attack efficiency for all similar DFA attacks. We also gave a general DFA attack flow which requires the least faulty ciphertexts with a reasonable computational cost.

References

1. E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems." in *CRYPTO*, pages 513–525. Springer 1997.
2. D. Saha, D. Mukhopadhyay and D. RoyChowdhury, "A Diagonal Fault Attack on the Advanced Encryption Standard." Cryptology ePrint Archive, Report 2009/581, 2009. http://eprint.iacr.org/
3. D. Boneh, R. A. DeMillo, and R. J. Lipton. "On the Improtance of Checking Cryptographic Protocals for Faults. (Extened Abstract)" in *EUROCRYPT*, pages 37–51. Springer, 1997.
4. J. Blömer and J.-P. Seifert. "Fault based Cryptanalysis of the Advanced Encryption Standard." Cryptology ePrint Archive, Report 2002/075, 2002. http://eprint.iacr.org/
5. C. Giraud. "DFA on AES." Cryptology ePrint Archive, Report 2003/008, 2003. http://eprint.iacr.org/
6. A. Moradi, M. T. Manzuri Shalmani, and M. Salmasizadeh. "A Generalized Method of Differential Fault Attack against AES cryptosystem." In *CHES*, pages 91–100, 2006.
7. D. Mukhopadhyay. "An Improved Fault based Attack of the Advanced Encryption Standard." In *AFRICACRYPT*, pages 421–434, 2009.
8. G. Letourneux P. Dusart and O.Vivolo. "Differential Fault Analysis on A.E.S." Cryptology ePrint Archive, Report 2003/010, 2003. http://eprint.iacr.org/
9. G. Piret and J.-J. Quisquater. "A Differential Fault Attack Technique against SPN structures, with Application to the AES and $\mathrm{K}_{\mathrm{HAZAD}}$." In *CHES*, pages 77–88, 2003.
10. M. Tunstall and D. Mukhopadhyay. "Differential Fault Analysis of the Advanced Encryption Standard using a Single Fault." Cryptology ePrint Archive, Report 2009/575, 2009. http://eprint.iacr.org/