Differential Fault Analysis against AES-192 and AES-256 with Minimal Faults

Chong Hee KIM

Information Security Group Université Catholique de Louvain, Belgium

August 21, 2010

Chong Hee KIM, Université Catholique de Louvain DFA against AES-192 and AES-256 with Minimal Faults

Outline

Introduction

- Differential fault analysis against AES
- AES
- AES key scheduling
- 2 Fault model and basic concept of DFA against AES
 - Fault model
 - Basic concept of DFA against AES-128
- 3 Proposed attacks
 - DFA against AES-192
 - DFA against AES-256
- 4 Comparison and conclusions

・ 同 ト ・ ヨ ト ・ ヨ ト

Fault model and basic concept of DFA against AES Proposed attacks Comparison and conclusions Differential fault analysis against AES AES AES key scheduling

(ロ) (同) (E) (E)

Outline



- Differential fault analysis against AES
- AES
- AES key scheduling
- 2 Fault model and basic concept of DFA against AES
 - Fault model
 - Basic concept of DFA against AES-128
- 3 Proposed attacks
 - DFA against AES-192DFA against AES-256
- 4 Comparison and conclusions

Fault model and basic concept of DFA against AES Proposed attacks Comparison and conclusions Differential fault analysis against AES AES AES key scheduling

Differential fault analysis

DFA (Differential fault analysis)

- DFA uses differential information between correct and faulty ciphertexts to figure out the secret key
- Normally attacker gets faulty ciphertexts by giving external impact with voltage variation, glitch, laser, etc
- The first DFA: against DES by Biham and Shamir, 1997

DFA against AES-128

- Piret and Quisquater (2003)
 - 2 pairs, practical fault model (random byte error)
- Fukunaga and Takahashi: 1 pair with 2³² exhaustive search (8-35 minutes at Core2 Duo 3.0GHz PC)

Tunstall and Mukhopadhyay: 1 pair with 2⁸ exhaustive search

Fault model and basic concept of DFA against AES Proposed attacks Comparison and conclusions Differential fault analysis against AES AES AES key scheduling

Differential fault analysis

DFA (Differential fault analysis)

- DFA uses differential information between correct and faulty ciphertexts to figure out the secret key
- Normally attacker gets faulty ciphertexts by giving external impact with voltage variation, glitch, laser, etc
- The first DFA: against DES by Biham and Shamir, 1997

DFA against AES-128

- Piret and Quisquater (2003)
 - 2 pairs, practical fault model (random byte error)
- Fukunaga and Takahashi: 1 pair with 2³² exhaustive search (8-35 minutes at Core2 Duo 3.0GHz PC)
- Tunstall and Mukhopadhyay: 1 pair with 2⁸ exhaustive search

Fault model and basic concept of DFA against AES Proposed attacks Comparison and conclusions Differential fault analysis against AES AES AES key scheduling

・ロン ・回 と ・ヨン ・ ヨン

Differential fault analysis

DFA against AES-192 and AES-256

- Application of Piret and Quisquter's: 4 pairs
- 2009, Li et al.: 16 or 3000 pairs
- 2010, Barenghi et al.: 16 pairs
- 2010, Takahashi and Fukunaga: 3 pairs for AES-192, 4 pairs for AES-256 (2 faulty plaintexts)
- Proposed methods: 2 pairs for AES-192, 3 pairs for AES-256

Fault model and basic concept of DFA against AES Proposed attacks Comparison and conclusions Differential fault analysis against AES AES AES key scheduling

AES



• Intermediate result, called *State*, is represented as a two-dimensional byte array with 4 rows and 4 columns

S _(0,0)	S _(0,1)	S _(0,2)	S _(0,3)
S _(1,0)	S _(1,1)	S _(1,2)	S _(1,3)
S _(2,0)	S _(2,1)	S _(2,2)	S _(2,3)
S _(3,0)	S _(3,1)	S _(3,2)	S _(3,3)

・ロン ・回 と ・ ヨ と ・ ヨ と …

臣

Fault model and basic concept of DFA against AES Proposed attacks Comparison and conclusions Differential fault analysis against AES AES AES key scheduling

AES



• Each round is composed of 4 transformations except the last round:

- SubBytes: 16 identical 8 \times 8 S-boxes, non-linear byte substitution
- ShiftRows: Each row is cyclically shifed over different offsets
- MixColumns: A linear transformation to each column
- AddRoundKey: A bitwise XOR with a round key

Number of rounds

Chong Hee KIM, Université Catholique de Louvain

DFA against AES-192 and AES-256 with Minimal Faults

• • E • • E •

Fault model and basic concept of DFA against AES Proposed attacks Comparison and conclusions Differential fault analysis against AES AES AES key scheduling

AES



• Each round is composed of 4 transformations except the last round:

- SubBytes: 16 identical 8 \times 8 S-boxes, non-linear byte substitution
- ShiftRows: Each row is cyclically shifed over different offsets
- MixColumns: A linear transformation to each column
- AddRoundKey: A bitwise XOR with a round key

Number of rounds

Chong Hee KIM, Université Catholique de Louvain

DFA against AES-192 and AES-256 with Minimal Faults

Fault model and basic concept of DFA against AES Proposed attacks Comparison and conclusions Differential fault analysis against AES AES AES key scheduling

AES



- Each round is composed of 4 transformations except the last round:
 - SubBytes: 16 identical 8 \times 8 S-boxes, non-linear byte substitution
 - ShiftRows: Each row is cyclically shifed over different offsets
 - MixColumns: A linear transformation to each column
 - AddRoundKey: A bitwise XOR with a round key

• Number of rounds

	Key length	Number of rounds r
AES-128	128	10
AES-192	192	12
AES-256	256	14

Chong Hee KIM, Université Catholique de Louvain

DFA against AES-192 and AES-256 with Minimal Faults

Fault model and basic concept of DFA against AES Proposed attacks Comparison and conclusions Differential fault analysis against AES AES AES key scheduling

AES



- Each round is composed of 4 transformations except the last round:
 - SubBytes: 16 identical 8 \times 8 S-boxes, non-linear byte substitution
 - ShiftRows: Each row is cyclically shifed over different offsets
 - MixColumns: A linear transformation to each column
 - AddRoundKey: A bitwise XOR with a round key
- Number of rounds

	Key length	Number of rounds r
AES-128	128	10
AES-192	192	12
AES-256	256	14

Chong Hee KIM, Université Catholique de Louvain

DFA against AES-192 and AES-256 with Minimal Faults

- 4 回 2 - 4 □ 2 - 4 □

Fault model and basic concept of DFA against AES Proposed attacks Comparison and conclusions Differential fault analysis against AES AES AES key scheduling

◆□ > ◆□ > ◆臣 > ◆臣 > ○

Э

AES key scheduling



Fault model and basic concept of DFA against AES Proposed attacks Comparison and conclusions Differential fault analysis against AES AES AES key scheduling

・ロン ・回 と ・ ヨ と ・ ヨ と …

臣

AES key scheduling





Fault model Basic concept of DFA against AES-128

(ロ) (同) (E) (E)

Outline

Introduction

- Differential fault analysis against AES
- AES
- AES key scheduling

2 Fault model and basic concept of DFA against AES

- Fault model
- Basic concept of DFA against AES-128

3 Proposed attacks

DFA against AES-192DFA against AES-256

4 Comparison and conclusions

Fault model

Fault model Basic concept of DFA against AES-128

- We assume that
 - a byte of the AES intermediate state is corrupted by fault injection
 - the corrupted value is random and unkonw to the attacker
- Location of corrupted byte among 16 bytes
 - may be known to the attacker: ex) in [6], it was shown that precise control of fau
 - was possible
 - may be not:
 - perform 16 independent equivalent analysis
 - we assume that the attacker knows the location
- We assume that the attacker can get a pair of correct and faulty ciphertexts

Fault model

Fault model Basic concept of DFA against AES-128

- We assume that
 - a byte of the AES intermediate state is corrupted by fault injection
 - the corrupted value is random and unkonw to the attacker

• Location of corrupted byte among 16 bytes

- may be known to the attacker:
 ex) in [6], it was shown that precise control of fault injection was possible
- may be not:

perform 16 independent equivalent analysis

• we assume that the attacker knows the location

• We assume that the attacker can get a pair of correct and faulty ciphertexts

Fault model

Fault model Basic concept of DFA against AES-128

(ロ) (同) (E) (E) (E)

- We assume that
 - a byte of the AES intermediate state is corrupted by fault injection
 - the corrupted value is random and unkonw to the attacker
- Location of corrupted byte among 16 bytes
 - may be known to the attacker:
 ex) in [6], it was shown that precise control of fault injection was possible
 - may be not:
 - perform 16 independent equivalent analysis
 - we assume that the attacker knows the location
- We assume that the attacker can get a pair of correct and faulty ciphertexts

Fault model Basic concept of DFA against AES-128

・ロン ・回 と ・ヨン ・ ヨン

Basic concept of DFA against AES-128

- Based on Piret and Quisquater's method + recent improvement
- A 1-byte fault between MixColumns of rounds 7th and 8th

Fault model Basic concept of DFA against AES-128

э

Basic concept of DFA against AES-128



Fault model Basic concept of DFA against AES-128

э

Basic concept of DFA against AES-128



Fault model Basic concept of DFA against AES-128

3

Basic concept of DFA against AES-128



Fault model Basic concept of DFA against AES-128

3

Basic concept of DFA against AES-128



Fault model Basic concept of DFA against AES-128

Basic concept of DFA against AES-128



Chong Hee KIM, Université Catholique de Louvain

Fault model Basic concept of DFA against AES-128

・ロット (雪) (目) (日)

3

Basic concept of DFA against AES-128

$$\begin{aligned} \mathbf{SB}^{-1}(C_{0,0} \oplus \mathcal{K}_{0,0}^{10}) \oplus \mathbf{SB}^{-1}(C_{0,0}^* \oplus \mathcal{K}_{0,0}^{10}) &= 2\sigma, \\ \mathbf{SB}^{-1}(C_{1,3} \oplus \mathcal{K}_{1,3}^{10}) \oplus \mathbf{SB}^{-1}(C_{1,3}^* \oplus \mathcal{K}_{1,3}^{10}) &= \sigma, \\ \mathbf{SB}^{-1}(C_{2,2} \oplus \mathcal{K}_{2,2}^{10}) \oplus \mathbf{SB}^{-1}(C_{2,2}^* \oplus \mathcal{K}_{2,2}^{10}) &= \sigma, \\ \mathbf{SB}^{-1}(C_{3,1} \oplus \mathcal{K}_{3,1}^{10}) \oplus \mathbf{SB}^{-1}(C_{3,1}^* \oplus \mathcal{K}_{3,1}^{10}) &= 3\sigma. \end{aligned}$$

Fault model Basic concept of DFA against AES-128

Basic concept of DFA against AES-128



Chong Hee KIM, Université Catholique de Louvain

Fault model Basic concept of DFA against AES-128

Basic concept of DFA against AES-128



Fault model Basic concept of DFA against AES-128

Basic concept of DFA against AES-128



Fault model Basic concept of DFA against AES-128

Basic concept of DFA against AES-128



According to [12], we can further reduce the number of candidates to 2^8 .

Chong Hee KIM, Université Catholique de Louvain

DFA against AES-192 and AES-256 with Minimal Faults

・ロン ・回 と ・ ヨ と ・ ヨ と …

Fault model Basic concept of DFA against AES-128

Basic concept of DFA against AES-128



Chong Hee KIM, Université Catholique de Louvain DFA

Fault model Basic concept of DFA against AES-128

Basic concept of DFA against AES-128



Chong Hee KIM, Université Catholique de Louvain

Fault model Basic concept of DFA against AES-128

Basic concept of DFA against AES-128



Chong Hee KIM, Université Catholique de Louvain

Introduction Fault model and basic concept of DFA against AES Proposed attacks

Comparison and conclusions

DFA against AES-192 DFA against AES-256

Outline

Introduction

- Differential fault analysis against AES
- AES
- AES key scheduling
- 2 Fault model and basic concept of DFA against AES
 - Fault model
 - Basic concept of DFA against AES-128

3 Proposed attacks

- DFA against AES-192
- DFA against AES-256

4 Comparison and conclusions

(ロ) (同) (E) (E)

DFA against AES-192 DFA against AES-256

Objective

- With a current normal PC, an exhaustive search of 2³² can be done within tens of minutes.
- Therefore we try to minimize the required number of faults with up to 2³² exhaustive search.

◆□▶ ◆□▶ ◆目▶ ◆目▶ ●目 - のへで

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 1

Attack procedure

- Obtain 2 pairs of (C₁, C^{*}₁) and (C₂, C^{*}₂). Where the faults are injected between *MixColumns* of round 9 and 10.
- Find K¹².
- Find the left-half of K¹¹ with key schedule.
- Find 2³² candidates for the right-half of K¹¹.
- Find the master secret key with an exhaustive search of 2³²

Chong Hee KIM, Université Catholique de Louvain DFA against AES-192 and AES-256 with Minimal Faults

(ロ) (同) (E) (E) (E)

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 1

Attack procedure

- Obtain 2 pairs of (C₁, C₁^{*}) and (C₂, C₂^{*}). Where the faults are injected between *MixColumns* of round 9 and 10.
- 2 Find K¹².
- Find the left-half of K¹¹ with key schedule.
- Find 2³² candidates for the right-half of K¹¹.
- Find the master secret key with an exhaustive search of 2³²

Chong Hee KIM, Université Catholique de Louvain DFA against AES-192 and AES-256 with Minimal Faults

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 1

Attack procedure

- Obtain 2 pairs of (C_1, C_1^*) and (C_2, C_2^*) . Where the faults are injected between *MixColumns* of round 9 and 10.
- 2 Find *K*¹².
- Ind the left-half of K¹¹ with key schedule.
- Find 2³² candidates for the right-half of K¹¹.
- Ind the master secret key with an exhaustive search of 2³².

Chong Hee KIM, Université Catholique de Louvain DFA against AES-192 and AES-256 with Minimal Faults

◆□▶ ◆□▶ ◆目▶ ◆目▶ 目 のへの
DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 1

Attack procedure

- Obtain 2 pairs of (C_1, C_1^*) and (C_2, C_2^*) . Where the faults are injected between *MixColumns* of round 9 and 10.
- Find K¹².
- Find the left-half of K^{11} with key schedule.
- Find 2³² candidates for the right-half of K¹¹.
- Ind the master secret key with an exhaustive search of 2³².

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 1

Attack procedure

- Obtain 2 pairs of (C_1, C_1^*) and (C_2, C_2^*) . Where the faults are injected between *MixColumns* of round 9 and 10.
- **2** Find K^{12} .
- **③** Find the left-half of K^{11} with key schedule.
- Find 2^{32} candidates for the right-half of K^{11} .
 - **5** Find the master secret key with an exhaustive search of 2^{32} .

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 1

Attack procedure

- Obtain 2 pairs of (C_1, C_1^*) and (C_2, C_2^*) . Where the faults are injected between *MixColumns* of round 9 and 10.
- Find K¹².
- Find the left-half of K^{11} with key schedule.
- Find 2^{32} candidates for the right-half of K^{11} .
- Find the master secret key with an exhaustive search of 2^{32} .

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三 のへで

DFA against AES-192 DFA against AES-256

Comparison and conclusions

DFA against AES-192: Method 1



1 Find K^{12} with 2 pairs

Find the left-half of K¹¹ with key schedule

Find 2³² candidates for the right-half of K¹¹

• Find the master secret key with an exhaustive search of 2³²

Chong Hee KIM, Université Catholique de Louvain DFA against AES-192 and AES-256 with Minimal Faults

DFA against AES-192 DFA against AES-256

Comparison and conclusions

DFA against AES-192: Method 1



Find K^{12} with 2 pairs

Find the left-half of K¹¹ with key schedule

Find 2³² candidates for the right-half of K¹¹

• Find the master secret key with an exhaustive search of 2³²

Chong Hee KIM, Université Catholique de Louvain DFA against AES-192 and AES-256 with Minimal Faults

DFA against AES-192 DFA against AES-256

Comparison and conclusions

DFA against AES-192: Method 1



- Find K¹² with 2 pairs
- Find the left-half of K¹¹ with key schedule
- Find 2³² candidates for the right-half of K¹¹
 - Find the master secret key with an exhaustive search of 2³²

Chong Hee KIM, Université Catholique de Louvain

DFA against AES-192 and AES-256 with Minimal Faults

・ロン ・回 と ・ ヨ と ・ ヨ と

DFA against AES-192 DFA against AES-256

Comparison and conclusions

DFA against AES-192: Method 1



• Find K¹² with 2 pairs

- Find the left-half of K¹¹ with key schedule
- Find 2^{32} candidates for the right-half of K^{11}
 - Find the master secret key with an exhaustive search of 2³²

Chong Hee KIM, Université Catholique de Louvain

DFA against AES-192 and AES-256 with Minimal Faults

・ロン ・回 と ・ ヨ と ・ ヨ と

э

DFA against AES-192 DFA against AES-256

Comparison and conclusions

DFA against AES-192: Method 1



Find K¹² with 2 pairs
 Find the left-half of K¹¹ with key schedule

- Find 2^{32} candidates for the right-half of K^{11}
 - Find the master secret key with an exhaustive search of 2³²

Chong Hee KIM, Université Catholique de Louvain

DFA against AES-192 and AES-256 with Minimal Faults

・ロン ・四 ・ ・ ヨ ・ ・ ヨ ・ ・

3

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 1



Find K¹² with 2 pairs
 Find the left-half of K¹¹ with key schedule

- Find 2³² candidates for the right-half of K¹¹
- Find the master secret key with an exhaustive search of 2³²

・ロン ・回 と ・ ヨ と ・ ヨ と …

AES - 192

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 2

- Obtain a pair of (C₁, C₁^{*}). Where the faults are injected between *MixColumns* of round 9 and 10.
 Obtain a pair of (C₂, C₂^{*}). Where the faults are injected between *MixColumns* of round 8 and 9
- **3** Find 2^{32} candidates for K^{12} with (C_1, C_1^*) .
- Ompute the 2³² for left-half of K¹¹ with key schedule.
- **()** Reduce the candidates for K^{12} and the left-half of K^{11} to 2^{24}
- Find the left-half of K^{11} and K^{12} with (C_2, C_2^*) .
- Find the 2⁸ candidates for right-half of K^{11} with (C_2, C_2^*) .

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 2

Attack procedure

- Obtain a pair of (C_1, C_1^*) . Where the faults are injected between *MixColumns* of round 9 and 10.
- **2** Obtain a pair of (C_2, C_2^*) . Where the faults are injected between *MixColumns* of round 8 and 9
- Find 2^{32} candidates for K^{12} with (C_1, C_1^*) .
- Ompute the 2³² for left-half of K¹¹ with key schedule.
- **(3)** Reduce the candidates for K^{12} and the left-half of K^{11} to 2^{24} .
- Find the left-half of K^{11} and K^{12} with (C_2, C_2^*)
- Find the 2⁸ candidates for right-half of K^{11} with (C_2, C_2^*) .

Chong Hee KIM, Université Catholique de Louvain DFA against AES-192 and AES-256 with Minimal Faults

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 2

- Obtain a pair of (C_1, C_1^*) . Where the faults are injected between *MixColumns* of round 9 and 10.
- **2** Obtain a pair of (C_2, C_2^*) . Where the faults are injected between *MixColumns* of round 8 and 9
- Solution Find 2^{32} candidates for K^{12} with (C_1, C_1^*) .
- **(**) Compute the 2^{32} for left-half of K^{11} with key schedule.
- Seduce the candidates for K¹² and the left-half of K¹¹ to 2²⁴.
- Find the left-half of K^{11} and K^{12} with (C_2, C_2^*) .
- Find the 2⁸ candidates for right-half of K¹¹ with (C₂, C₂*).
 Find the MC⁻¹(K¹¹) with (C₁, C₁*).

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 2

- Obtain a pair of (C_1, C_1^*) . Where the faults are injected between *MixColumns* of round 9 and 10.
- **2** Obtain a pair of (C_2, C_2^*) . Where the faults are injected between *MixColumns* of round 8 and 9
- Solution Find 2^{32} candidates for K^{12} with (C_1, C_1^*) .
- **(**) Compute the 2^{32} for left-half of K^{11} with key schedule.
- **③** Reduce the candidates for K^{12} and the left-half of K^{11} to 2^{24} .
- Find the left-half of K^{11} and K^{12} with (C_2, C_2^*) .
- Find the 2⁸ candidates for right-half of K^{11} with (C_2, C_2^*) .
- **3** Find the $MC^{-1}(K^{11})$ with (C_1, C_1^*)

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 2

- Obtain a pair of (C_1, C_1^*) . Where the faults are injected between *MixColumns* of round 9 and 10.
- **2** Obtain a pair of (C_2, C_2^*) . Where the faults are injected between *MixColumns* of round 8 and 9
- Solution Find 2^{32} candidates for K^{12} with (C_1, C_1^*) .
- **(**) Compute the 2^{32} for left-half of K^{11} with key schedule.
- **③** Reduce the candidates for K^{12} and the left-half of K^{11} to 2^{24} .
- Find the left-half of K^{11} and K^{12} with (C_2, C_2^*) .
- Find the 2⁸ candidates for right-half of K^{11} with (C_2, C_2^*) . • Find the $MC^{-1}(K^{11})$ with (C_1, C_2^*)
- Compute master secret key.

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 2

- Obtain a pair of (C_1, C_1^*) . Where the faults are injected between *MixColumns* of round 9 and 10.
- **2** Obtain a pair of (C_2, C_2^*) . Where the faults are injected between *MixColumns* of round 8 and 9
- Solution Find 2^{32} candidates for K^{12} with (C_1, C_1^*) .
- **(**) Compute the 2^{32} for left-half of K^{11} with key schedule.
- **③** Reduce the candidates for K^{12} and the left-half of K^{11} to 2^{24} .
- Find the left-half of K^{11} and K^{12} with (C_2, C_2^*) .
- Find the 2^8 candidates for right-half of K^{11} with (C_2, C_2^*) .
- **3** Find the $MC^{-1}(K^{11})$ with (C_1, C_1^*)
- Ompute master secret key.

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 2

Attack procedure

- Obtain a pair of (C_1, C_1^*) . Where the faults are injected between *MixColumns* of round 9 and 10.
- **2** Obtain a pair of (C_2, C_2^*) . Where the faults are injected between *MixColumns* of round 8 and 9
- Solution Find 2^{32} candidates for K^{12} with (C_1, C_1^*) .
- **(**) Compute the 2^{32} for left-half of K^{11} with key schedule.
- **③** Reduce the candidates for K^{12} and the left-half of K^{11} to 2^{24} .
- Find the left-half of K^{11} and K^{12} with (C_2, C_2^*) .
- Find the 2^8 candidates for right-half of K^{11} with (C_2, C_2^*) .
- Find the $MC^{-1}(K^{11})$ with (C_1, C_1^*) .

Compute master secret key.

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 2

- Obtain a pair of (C_1, C_1^*) . Where the faults are injected between *MixColumns* of round 9 and 10.
- **2** Obtain a pair of (C_2, C_2^*) . Where the faults are injected between *MixColumns* of round 8 and 9
- Find 2^{32} candidates for K^{12} with (C_1, C_1^*) .
- **(**) Compute the 2^{32} for left-half of K^{11} with key schedule.
- **③** Reduce the candidates for K^{12} and the left-half of K^{11} to 2^{24} .
- Find the left-half of K^{11} and K^{12} with (C_2, C_2^*) .
- Find the 2^8 candidates for right-half of K^{11} with (C_2, C_2^*) .
- Find the $MC^{-1}(K^{11})$ with (C_1, C_1^*) .
- Compute master secret key.

DFA against AES-192 DFA against AES-256

Comparison and conclusions

DFA against AES-192: Method 2



- Find 2^{32} candidates for K^{12} with (C_1, C_1^*)
 - Compute the 2³² candidates for left-half of K¹¹ with key schedule.
- Reduce the candidates for *K*¹² and the left-half of *K*¹¹ to 2²⁴.
- Find the left-half of K^{11} and K^{12} with (C_2, C_2^*) .

Chong Hee KIM, Université Catholique de Louvain DFA against AES-192 and AES-256 with Minimal Faults

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 2



- Find 2³² candidates for K¹² with (C₁, C₁^{*})
- Compute the 2³²
 candidates for left-half of K¹¹ with key schedule.
 - Reduce the candidates for K¹² and the left-half of K¹¹ to 2²⁴.
 - Find the left-half of K^{11} and K^{12} with (C_2, C_2^*) .

Chong Hee KIM, Université Catholique de Louvain DFA against AES-192 and AES-256 with Minimal Faults

DFA against AES-192 DFA against AES-256

Comparison and conclusions

DFA against AES-192: Method 2



- Find 2³² candidates for K¹² with (C₁, C₁^{*})
- Compute the 2³² candidates for left-half of K¹¹ with key schedule.
- Reduce the candidates for K¹² and the left-half of K¹¹ to 2²⁴.

Find the left-half of K^{11} and K^{12} with (C_2, C_2^*) .

Chong Hee KIM, Université Catholique de Louvain

DFA against AES-192 and AES-256 with Minimal Faults

(日) (同) (E) (E) (E)

DFA against AES-192 DFA against AES-256

Comparison and conclusions

DFA against AES-192: Method 2



- Find 2³² candidates for K¹² with (C₁, C₁^{*})
- Compute the 2³² candidates for left-half of K¹¹ with key schedule.
- Reduce the candidates for K¹² and the left-half of K¹¹ to 2²⁴.
 - Find the left-half of K^{11} and K^{12} with (C_2, C_2^*) .

(日) (同) (E) (E) (E)

DFA against AES-192 and AES-256 with Minimal Faults

Chong Hee KIM, Université Catholique de Louvain

DFA against AES-192 DFA against AES-256

Comparison and conclusions

DFA against AES-192: Method 2



- Find 2³² candidates for K¹² with (C₁, C₁^{*})
- Compute the 2³² candidates for left-half of K¹¹ with key schedule.
- Reduce the candidates for K¹² and the left-half of K¹¹ to 2²⁴.
- Find the left-half of K^{11} and K^{12} with (C_2, C_2^*) .

(ロ) (同) (E) (E) (E)

Chong Hee KIM, Université Catholique de Louvain DFA against AES-192 and A

DFA against AES-192 and AES-256 with Minimal Faults

DFA against AES-192 DFA against AES-256

Comparison and conclusions

DFA against AES-192: Method 2



Find 2^{32} candidates for K^{12} with (C_1, C_1^*)

compute the 2^{44} candidates for left-half of K^{11} with key schedule.

Reduce the candidates for K¹² and the left-half of K¹¹ to 2²⁴.

• Find the left-half of K^{11} and K^{12} with (C_2, C_2^*) .

DFA against AES-192 and AES-256 with Minimal Faults

Chong Hee KIM, Université Catholique de Louvain

DFA against AES-192 DFA against AES-256

Comparison and conclusions

DFA against AES-192: Method 2



Find 2³² candidates for K¹² with (C₁, C₁)
Compute the 2³² candidates for left-half of K¹¹ with key schedule.
Reduce the candidates for K¹² and the left-half of K¹¹ to 2²⁴.

• Find the left-half of K^{11} and K^{12} with (C_2, C_2^*) .

3

DFA against AES-192 and AES-256 with Minimal Faults

・ロ・ ・ 日・ ・ ヨ・ ・ 日・

Chong Hee KIM, Université Catholique de Louvain

DFA against AES-192 DFA against AES-256

Comparison and conclusions

DFA against AES-192: Method 2



Find the 2⁸ candidates for right-half of K¹¹ with (C₂, C₂^{*}).

Find the MC⁻¹(K¹¹) with (C₁, C₁^{*}).

 Compute the master secret key.

Chong Hee KIM, Université Catholique de Louvain

DFA against AES-192 and AES-256 with Minimal Faults

・ロン ・日ン ・日ン ・日ン

3

DFA against AES-192 DFA against AES-256

DFA against AES-192: Method 2



- Find the 2⁸ candidates for right-half of K¹¹ with (C₂, C₂^{*}).
- Find the $MC^{-1}(K^{11})$ with (C_1, C_1^*) .
 - Compute the master secret key.

Chong Hee KIM, Université Catholique de Louvain DFA a

DFA against AES-192 and AES-256 with Minimal Faults

DFA against AES-192 DFA against AES-256

Comparison and conclusions

DFA against AES-192: Method 2



Find the 2⁸ candidates for right-half of K¹¹ with (C₂, C₂*).

- Find the $MC^{-1}(K^{11})$ with (C_1, C_1^*) .
- Compute the master secret key.

・ロン ・日ン ・日ン ・日ン



DFA against AES-192 DFA against AES-256

DFA against AES-256

Attack procedure

- Obtain two pairs of correct and faulty ciphertexts (C₁, C₁^{*}) and (C₂, C₂^{*}) by giving faults between *MixColumns* of round 11 and 12.
- **2** Obtain a pair of correct and faulty ciphertexts (C_3, C_3^*) by giving faults between *MixColumns* of round 10 and 11.
- **5** Find K^{14} with (C_1, C_1^*) and (C_2, C_2^*) .
- Find 2^{32} candidates for $MC^{-1}(K^{13})$ with (C_3, C_3^*) .
- **•** Find K^{13} with (C_1, C_1^*) and (C_2, C_2^*) .

O Find the master secret key with key scheduling.

DFA against AES-192 DFA against AES-256

DFA against AES-256

Attack procedure

- Obtain two pairs of correct and faulty ciphertexts (C₁, C₁^{*}) and (C₂, C₂^{*}) by giving faults between *MixColumns* of round 11 and 12.
- **2** Obtain a pair of correct and faulty ciphertexts (C_3, C_3^*) by giving faults between *MixColumns* of round 10 and 11.
- Find K^{14} with (C_1, C_1^*) and (C_2, C_2^*) .
- Find 2^{32} candidates for $MC^{-1}(K^{13})$ with (C_3, C_3^*) .
- Find K^{13} with (C_1, C_1^*) and (C_2, C_2^*) .

Find the master secret key with key scheduling.

DFA against AES-192 DFA against AES-256

DFA against AES-256

Attack procedure

- Obtain two pairs of correct and faulty ciphertexts (C₁, C₁^{*}) and (C₂, C₂^{*}) by giving faults between *MixColumns* of round 11 and 12.
- **2** Obtain a pair of correct and faulty ciphertexts (C_3, C_3^*) by giving faults between *MixColumns* of round 10 and 11.
- Find K^{14} with (C_1, C_1^*) and (C_2, C_2^*) .
- Find 2^{32} candidates for $MC^{-1}(K^{13})$ with (C_3, C_3^*) .
- **5** Find K^{13} with (C_1, C_1^*) and (C_2, C_2^*) .

Find the master secret key with key scheduling.

DFA against AES-192 DFA against AES-256

DFA against AES-256

Attack procedure

- Obtain two pairs of correct and faulty ciphertexts (C₁, C₁^{*}) and (C₂, C₂^{*}) by giving faults between *MixColumns* of round 11 and 12.
- **2** Obtain a pair of correct and faulty ciphertexts (C_3, C_3^*) by giving faults between *MixColumns* of round 10 and 11.
- Find K^{14} with (C_1, C_1^*) and (C_2, C_2^*) .
- Find 2^{32} candidates for $MC^{-1}(K^{13})$ with (C_3, C_3^*) .
- Find K^{13} with (C_1, C_1^*) and (C_2, C_2^*) .

Find the master secret key with key scheduling.

DFA against AES-192 DFA against AES-256

DFA against AES-256

Attack procedure

- Obtain two pairs of correct and faulty ciphertexts (C₁, C₁^{*}) and (C₂, C₂^{*}) by giving faults between *MixColumns* of round 11 and 12.
- **2** Obtain a pair of correct and faulty ciphertexts (C_3, C_3^*) by giving faults between *MixColumns* of round 10 and 11.
- Find K^{14} with (C_1, C_1^*) and (C_2, C_2^*) .
- Find 2^{32} candidates for $MC^{-1}(K^{13})$ with (C_3, C_3^*) .
- Find K^{13} with (C_1, C_1^*) and (C_2, C_2^*) .
- Ind the master secret key with key scheduling.

Comparison and conclusions

DFA against AES-192 DFA against AES-256

DFA against AES-256



- Find K^{14} with (C_1, C_1^*) and (C_2, C_2^*) .
- 2 Find 2^{32} candidates for $MC^{-1}(K^{13})$ with (C_3, C_3^*) .
- Find K^{13} with (C_1, C_1^*) and (C_2, C_2^*) .
 - Find the master secret key with key scheduling.

◆□▶ ◆□▶ ◆目▶ ◆目▶ 目 のへの

Chong Hee KIM, Université Catholique de Louvain DFA against AES-192 and AES-256 with Minimal Faults

DFA against AES-192 DFA against AES-256

Comparison and conclusions

DFA against AES-256



- Find K^{14} with (C_1, C_1^*) and (C_2, C_2^*) .
- Find 2³² candidates for MC⁻¹(K¹³) with (C₃, C₃^{*}).
 - **3** Find K^{13} with (C_1, C_1^*) and (C_2, C_2^*) .

Find the master secret key with key scheduling.

(ロ) (同) (E) (E) (E)

Chong Hee KIM, Université Catholique de Louvain

DFA against AES-192 and AES-256 with Minimal Faults

Comparison and conclusions

DFA against AES-192 DFA against AES-256

DFA against AES-256



- Find K^{14} with (C_1, C_1^*) and (C_2, C_2^*) .
- 2 Find 2^{32} candidates for $MC^{-1}(K^{13})$ with (C_3, C_3^*) .
- Find K^{13} with (C_1, C_1^*) and (C_2, C_2^*) .

Find the master secret key with key scheduling.

◆□ → ◆□ → ◆三 → ◆三 → ● ● ● ● ●

DFA against AES-192 and AES-256 with Minimal Faults

Chong Hee KIM, Université Catholique de Louvain

Comparison and conclusions

DFA against AES-192 DFA against AES-256

DFA against AES-256





- Find K^{14} with (C_1, C_1^*) and (C_2, C_2^*) .
- Find 2³² candidates for MC⁻¹(K¹³) with (C₃, C₃^{*}).
- Find K^{13} with (C_1, C_1^*) and (C_2, C_2^*) .
- Find the master secret key with key scheduling.

(日) (部) (E) (E)
Fault model and basic concept of DFA against AES Proposed attacks Comparison and conclusions

Outline

Introduction

- Differential fault analysis against AES
- AES
- AES key scheduling
- 2 Fault model and basic concept of DFA against AES
 - Fault model
 - Basic concept of DFA against AES-128
- Proposed attacks
 DFA against AES-192
 DFA against AES-256
- 4 Comparison and conclusions

(日) (同) (三) (三)

Introduction Fault model and basic concept of DFA against AES Proposed attacks Comparison and conclusions

Comparisons with existing DFA's against AES-192

Reference	Fault model	No. of	Exhaustive
		faults	search
Piret and Quisquater	1 byte	4	1
Li et al. method 1	1-4 bytes	12^{\dagger}	1
Li et al. method 2	4 bytes	3000 [†]	1
Barenghi et al.	1 byte	16^{\dagger}	1
Takahashi and Fukunaga	1 byte	3	2 ⁸
Our attack 1	1 byte	2	2 ³²
Our attack 2	1 byte	2	1

[†]: with same plaintext

・ロン ・回 と ・ ヨ と ・ ヨ と …

Introduction Fault model and basic concept of DFA against AES Proposed attacks Comparison and conclusions

Comparisons with existing DFA's against AES-256

Reference	Fault model	No. of	Exhaustive
		faults	search
Piret and Quisquater	1 byte	4	1
Li et al. method 1	1-4 bytes	12^{\dagger}	1
Li et al. method 2	4 bytes	3000 [†]	1
Barenghi et al.	1 byte	16^{\dagger}	1
Takahashi and Fukunaga	1 byte	4 [‡]	2 ¹³
Our attack	1 byte	3	1

[†]: with same plaintext

[‡]: 2 faulty plaintexts and 2 faulty ciphertexts

・ロン ・回 と ・ ヨン ・ ヨン

Introduction Fault model and basic concept of DFA against AES Proposed attacks Comparison and conclusions

Questions and answers

- Thank you!
- Questions?

Chong Hee KIM, Université Catholique de Louvain DFA against AES-192 and AES-256 with Minimal Faults

◆□ → ◆□ → ◆三 → ◆三 → ● ● ● ●