Meet-in-the-Middle and Impossible Differential Fault Analysis on AES

Patrick Derbez[2], Pierre-Alain Fouque[2] and Delphine Leresteux[1,3]

[1]DGA Information Superiority

[2]École Normale Supérieure

[3]Université Paris VII

30th September 2011

Presentation

- AES backgrounds
- Previous Fault Analysis on AES
- Meet-in-the-Middle Fault Analysis
- Impossible Differential Fault Analysis
- Extension to AES-192 and AES-256

Description of the AES

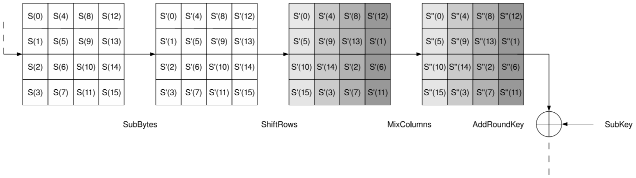


Figure: SubBytes, ShiftRows, MixColumns and AddRoundKey operations

Characteristics

- 128-bit input block,
- 128-bit keysize - 10 rounds
- 192-bit keysize - 12 rounds
- 256-bit keysize - 14 rounds

Definition

AES is a Substitution Permutation Network symmetric algorithm.

AES Properties

Subkeys

- The knowledge of only one subkey allows to retrieve the whole key for AES-128.
- The knowledge of two consecutive subkeys allows to recover the entire key for AES-192 and for AES-256.

AES diffusion

Two rounds of AES achieve a full diffusion for all keysize variants of AES.

Previous Fault Analysis on AES

Authors	Fault model	Faults	Round	AES	Paper
Tunstall *et al.*	Simple byte	1	$n-2$	128	WISTP11
Mukhopadhyay	Simple byte	1	$n-2$	128	Africa09
Piret *et al.*	Simple byte	2	$n-2$	128	CHES03
Dusart *et al.*	Simple byte	50	$n-1$	128	ACNS03

Table: Summary of differential fault analysis

Previous Fault Analysis on AES

Authors	Fault model	Faults	Round	AES	Paper
We	Simple byte	$\leq$2048	$n-3$	256	CHES11
We	Simple byte	$\leq$1000	$n-3$	128	CHES11
Tunstall *et al.*	Simple byte	1	$n-2$	128	WISTP11
Mukhopadhyay	Simple byte	1	$n-2$	128	Africa09
Piret *et al.*	Simple byte	2	$n-2$	128	CHES03
Dusart *et al.*	Simple byte	50	$n-1$	128	ACNS03

Table: Summary of differential fault analysis

CHES 2003: Piret and Quisquater

Equation on byte 0

$$SB^{-1}(C(0) \oplus K_{10}(0)) \oplus SB^{-1}(\tilde{C}(0) \oplus K_{10}(0)) = X$$

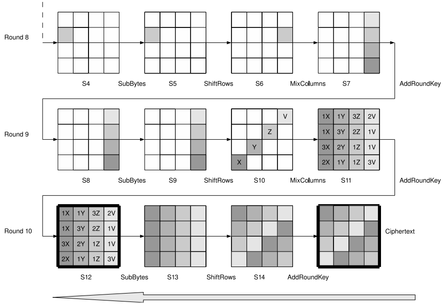


Figure: State-of-the-art differential fault analysis on AES-128

AFRICACRYPT 2009: Mukhopadhyay

Equation on byte 12

$$SB^{-1}(MC^{-1}(SB^{-1}(C \oplus K_{10}) \oplus K_9)) \oplus SB^{-1}(MC^{-1}(SB^{-1}(\tilde{C} \oplus K_{10}) \oplus K_9)) = 3X$$

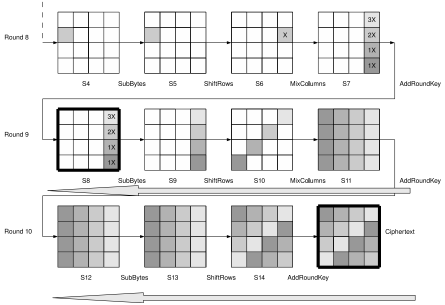


Figure: Fault path - fault analysis on l'AES-128

Meet-in-the-Middle Differential Fault Analysis (1)

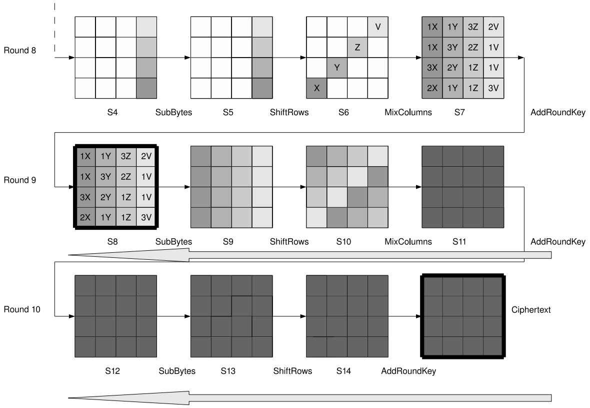
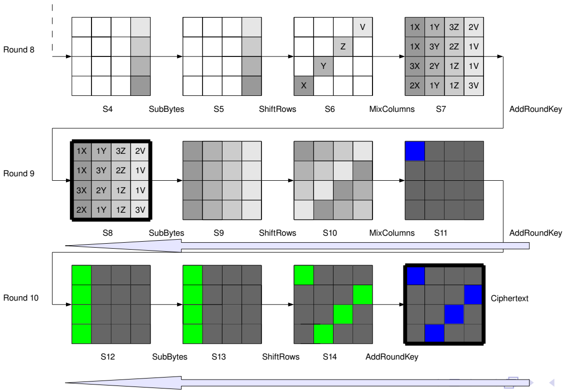


Figure: Meet-in-the-middle differential fault analysis for AES-128

Meet-in-the-Middle Differential Fault Analysis (2)

Equation on byte 0

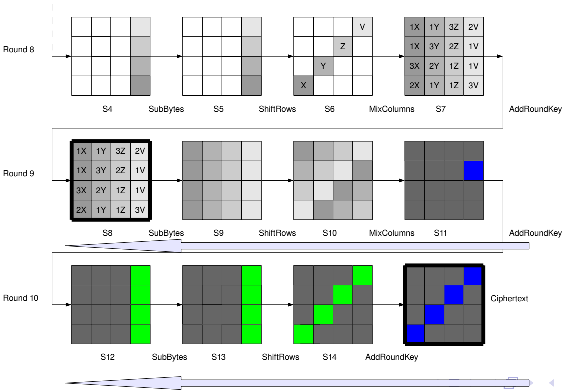
$$S_8(0) \oplus \tilde{S}_8(0) = X$$



Meet-in-the-Middle Differential Fault Analysis (3)

Equation on byte 1

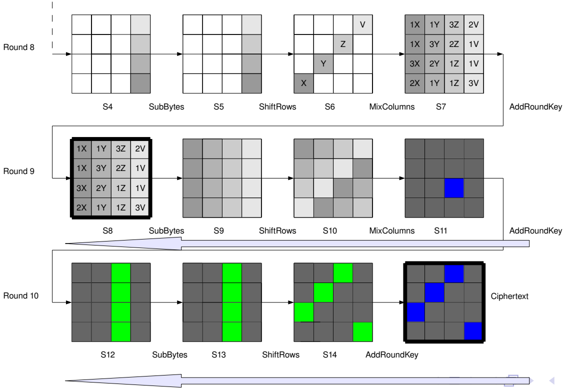
$$X = S_8(1) \oplus \tilde{S}_8(1) = S_8(0) \oplus \tilde{S}_8(0)$$



Meet-in-the-Middle Differential Fault Analysis (4)

Equation on byte 2

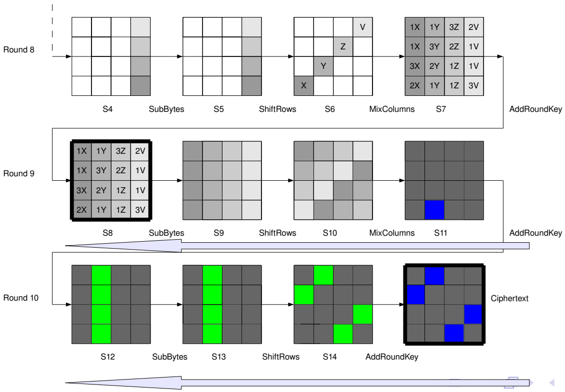
$$3X = S_8(2) \oplus \tilde{S}_8(2) = 3(S_8(0) \oplus \tilde{S}_8(0))$$



Meet-in-the-Middle Differential Fault Analysis (5)

Equation on byte 3

$$2X = S_8(3) \oplus \tilde{S}_8(3) = 2(S_8(0) \oplus \tilde{S}_8(0))$$



Resolution

Facts

- Differential no linear equation system with 10 unknown,
- Fault model: random fault on one byte at known position,
- Fault is injected between the MixColumns at the 6^{th} round and the MixColumns at the 7^{th} round,
- 10 couples of correct and faulty ciphertexts: 10 equations.

Extension of Fault Model

Known Fault Position

For each equation, less one unknown value.

Same Fault Position, but Unknown

Same mean of fault injection at the same time $\Longrightarrow$ same unknown faulty bytes $\Longrightarrow$ $4 \times$ computations.

Random and Unknown Fault Position

4 possible different cases for each couple of correct and faulty ciphertexts $\Longrightarrow$ 4^{10} cost for 10 pairs for all hypotheses $\Longrightarrow$ unpractical.

Reduction of Memory Requirement

Similar Attack

- Using the automatic research tool presented at CRYPTO 2011 by Bouillaguet, Derbez and Fouque.
- If all five faults are performed on the same byte.
- Less memory, 2^{24} instead of 2^{40} and same time complexity 2^{40}.
- Attack has been experimentally checked.

Revisited Impossible Differential Fault Analysis

CARDIS 2006: Phang and Yen

$2^{11} = 2048$ faults required

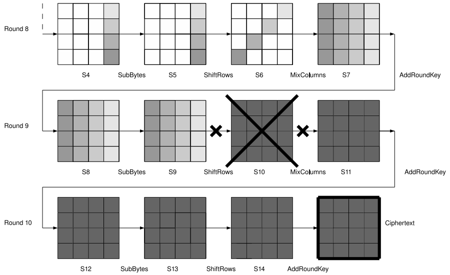


Figure: Impossible differential fault analysis on AES-128

Recovery K_{10}

Inequation on byte 0

$MC^{-1}|_0(SB^{-1}(C(0) \oplus K_{10}(0))) \oplus MC^{-1}|_0(SB^{-1}(\tilde{C}(0) \oplus K_{10}(0))) \neq 0$

Scenario

- For each pair, 4 guesses for $\{K_{10}(0), K_{10}(13), K_{10}(10), K_{10}(7)\}$.
- Delete each quadruplet of bytes from the subkey K_{10} which does not satisfy the inequation system.
- Repeat each previous step until only one possible quadruplet of K_{10} for each column or exhaustive search is possible for AES-128.

Resolution

Facts

- 4 systems of 4 inequalities,
- Fault model: random fault on one random byte,
- Fault is injected between the MixColumns at the 6^{th} round and the MixColumns at the 7^{th} round,
- 1000 couples in average + exhaustive search are required.

Recombination Property

Goal: Reduce the number of faults needed.

Recombination

Two Different Faulty Results with the Same Input Plaintext and the Same Faulty Byte

Two different faulty ciphertexts $\Longrightarrow$ inequation systems

Inequation

$S_{10}(\tilde{C}^{(1)}) \oplus S_{10}(\tilde{C}^{(2)}) \neq 0$

Number of faults required

45 couples of correct and faulty ciphertexts.

Theoretical Cost and Complexity for Impossible Differential

Complexity

- 1 couple of correct and faulty ciphertexts, delete 2^{26} quadruplets of K_{10} bytes among 2^{32} possibles.
- 2 couples of correct and faulty results, overlap of 2^{20}.
- With 1000 pairs of correct and faulty ciphertexts, we reject more than $2^{32} - 2^{10}$ quadruplets.

Extension to AES-192 and to AES-256

Description: with the same fault and for AES-192 and AES-256, we have both access to the subkeys K_n and K_{n-1}

AES-128, inject one fault between the MixColumns at the 6^{th} round and the MixColumns at the 7^{th} round

$$\Longleftrightarrow$$

AES-192, inject one fault between the MixColumns at the 8^{th} round and the MixColumns at the 9^{th} round

$$\Longleftrightarrow$$

AES-256, inject one fault between the MixColumns at the 10^{th} round and the MixColumns at the 11^{th} round.

Generalized Piret and Quisquater

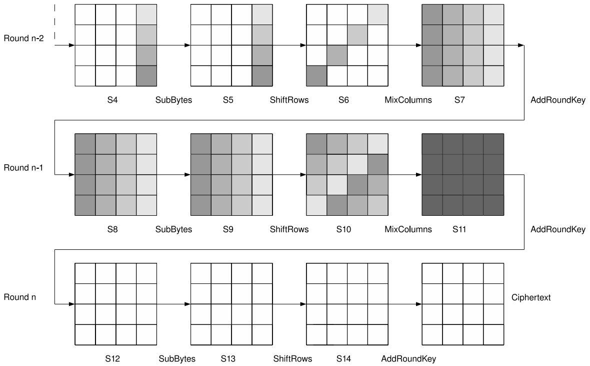


Figure: K_n is found, research of K_{n-1}

Differential Fault Analysis Presented on AES-128

Fault analysis	Fault model	Faults	Time	Memory
MiTM	known byte	10	$\simeq 2^{40}$	$\simeq 2^{40}$
MiTM	fixed unknown byte	10	$\simeq 2^{42}$	$\simeq 2^{40}$
MiTM	unknown byte	10	$\simeq 2^{60}$	$\simeq 2^{40}$
MiTM	fixed unknown byte	5	$\simeq 2^{40}$	$\simeq 2^{24}$
Impossible	unknown byte	1000	$\simeq 2^{40}$	$\simeq 2^{40}$
Impossible	fixed unknown byte	45	$\simeq 2^{40}$	$\simeq 2^{40}$

Table: Summary of new differential fault analysis presented on AES-128

Differential Fault Analysis Presented on AES-192 and AES-256

Fault analysis	Fault model	Faults	Time	Memory
MiTM	known byte	10	$\simeq 2^{40}$	$\simeq 2^{40}$
MiTM	fixed unknown byte	10	$\simeq 2^{42}$	$\simeq 2^{40}$
MiTM	unknown byte	10	$\simeq 2^{60}$	$\simeq 2^{40}$
MiTM	fixed unknown byte	5	$\simeq 2^{40}$	$\simeq 2^{24}$
Impossible	unknown byte	2048	$\simeq 2^{40}$	$\simeq 2^{40}$
Impossible	fixed unknown byte	65	$\simeq 2^{40}$	$\simeq 2^{40}$

Table: Summary of new differential fault analysis presented on AES-192 and AES-256

Conclusion

Differential Fault Analysis on AES-128, AES-192 and AES-256

- Protect all rounds of AES-128,
- Protect the last 5 rounds and the first 5 rounds for AES-192 and for AES-256.