A Differential Fault Analysis on AES Key Schedule Using Single Fault

Sk. Subidh Ali and Debdeep Mukhopadhyay

Dept. of Computer Science and Engineering

IIT Kharagpur

Outline

- Introduction
- Recent contributions
- Proposed DFA against AES-128 key schedule
  - Fault model used
  - Attack mechanism
  - Time complexity reduction
  - Experimental results
- Conclusions

Introduction

- Differential Fault Analysis (DFA) uses the difference between the correct and faulty ciphertexts to deduce the secret key
- Required:
  - To induce fault in a particular location
  - Pair of fault-free and faulty ciphertexts
- The target of the attack can be either an intermediate state of AES or the key schedule

AES-128 Key Schedule

Knowledge of any
one round key
is enough to get
the master key

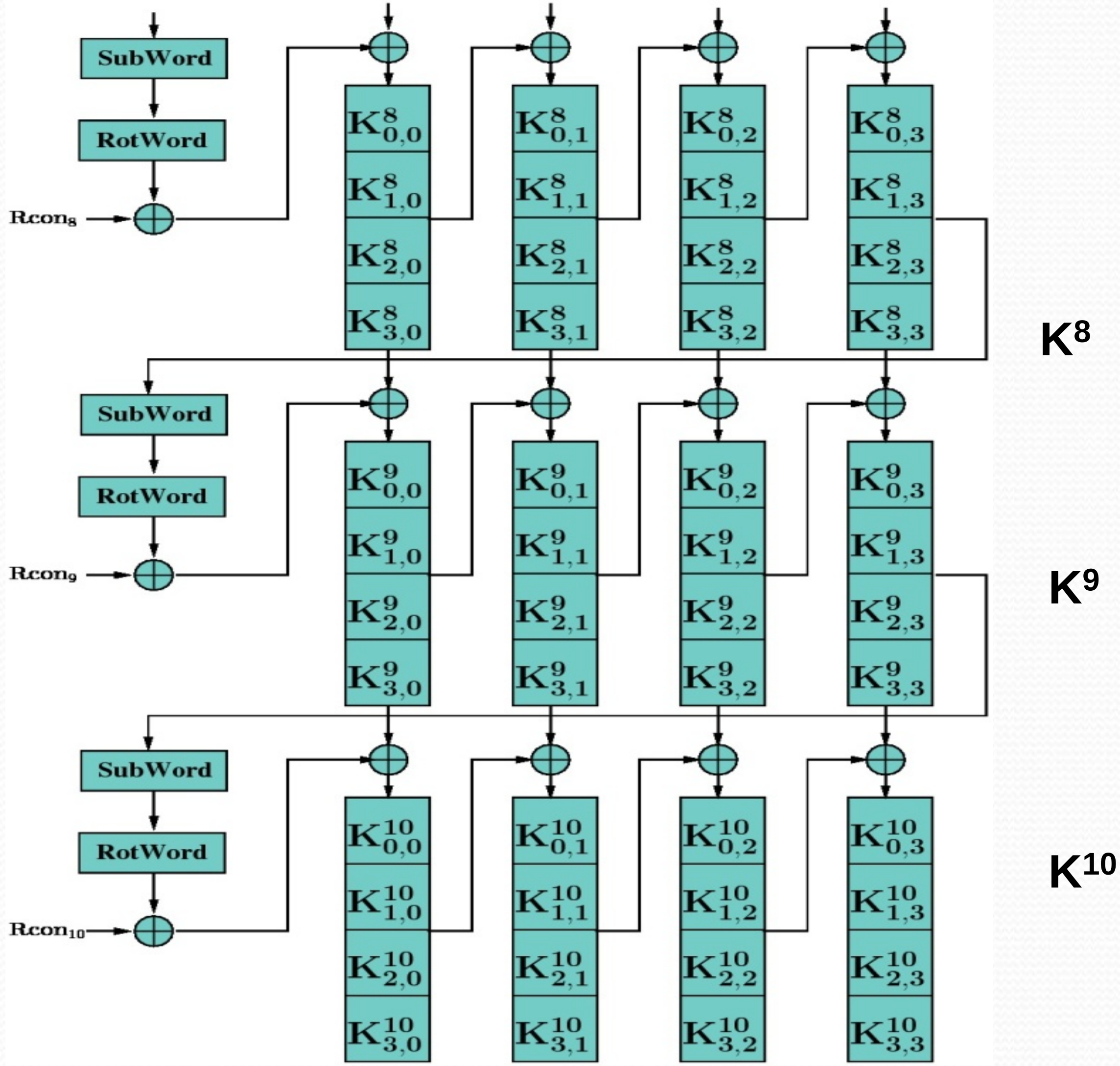
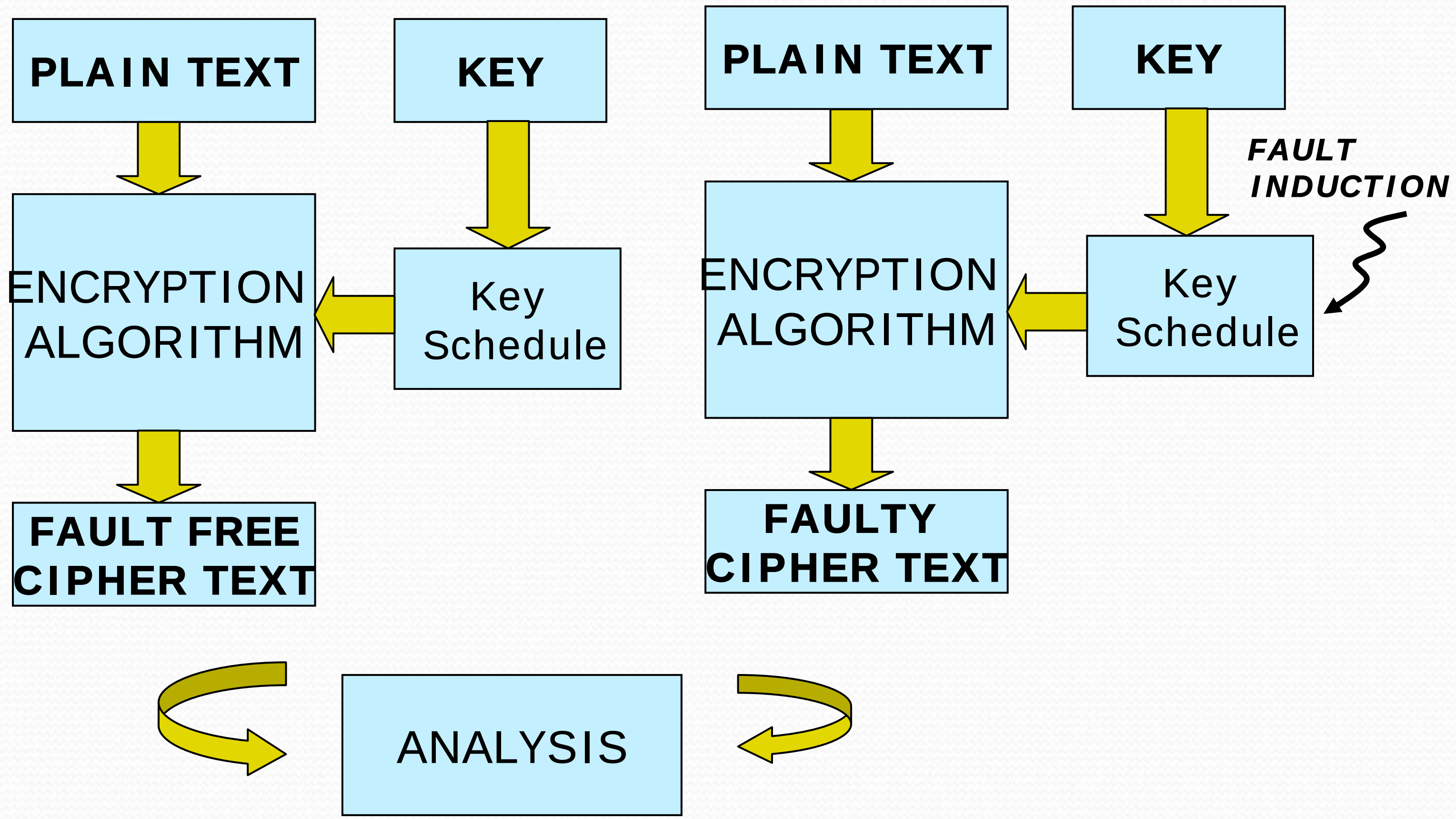


Illustration of a DFA on AES Key Schedule



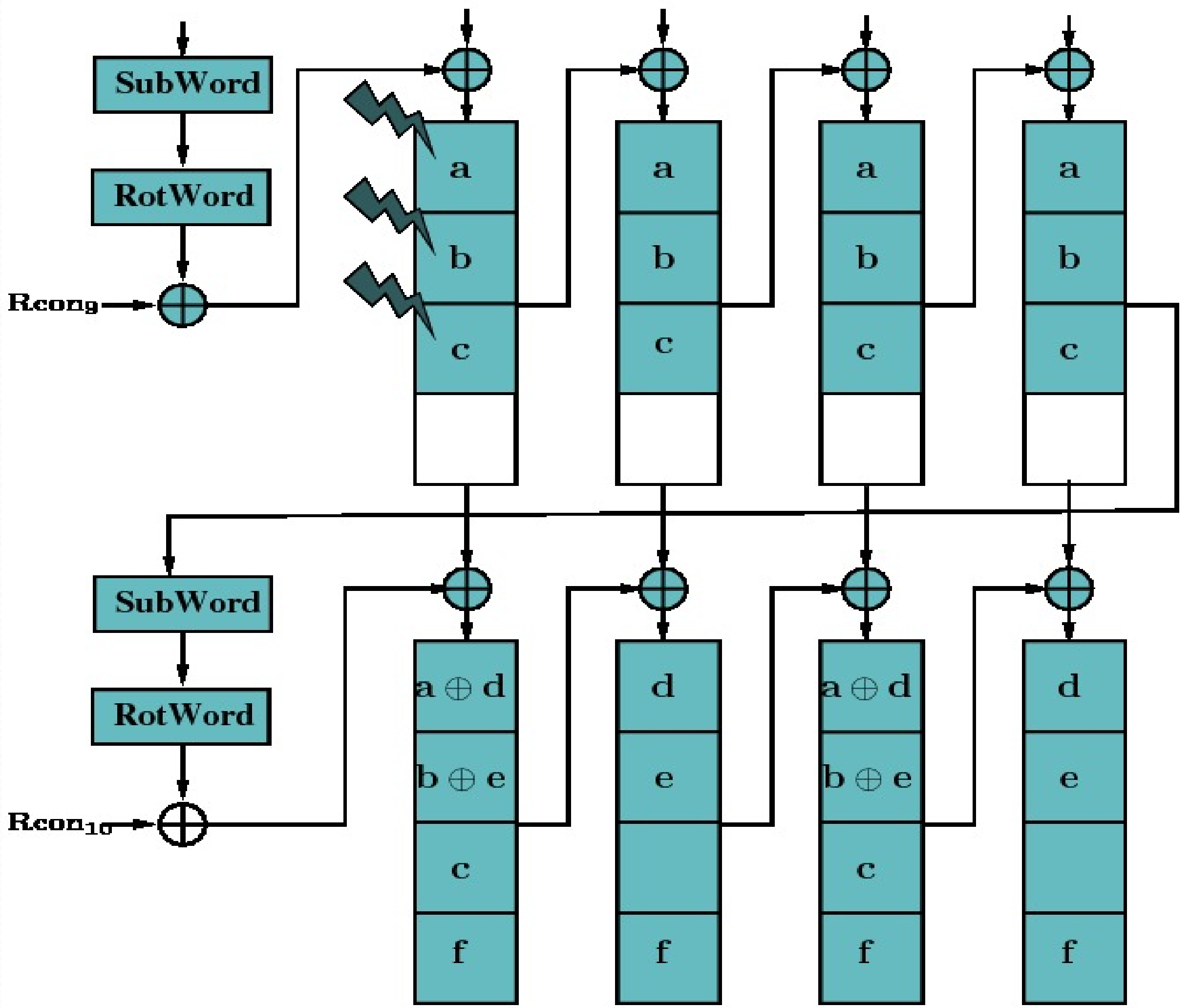
DFA against AES-128 Key Schedule

- Introduced by Christophe Giraud, 2003.
- Chen and Yen (2003): 22- 44 faulty ciphertexts.
- Peacham and Thomas (2006): 12 faulty ciphertexts.
- Takahashi et al. (FDTC 2007): 2 faulty ciphertexts with 48-bit brute-force search.
- Kim et al. (2007): 2 faulty ciphertexts with 32-bit brute-force search.
- Our attack in CARDIS'2011 : 1 faulty ciphertext with 32-bit brute-force search.

Fault Model

- Single Byte Fault
  - Attacker induces single byte fault at the first column of the 8^{th} round key during execution of key schedule.
  - Fault subsequently propagates to 9^{th} and 10^{th} round key.
  - No knowledge is required of the fault value

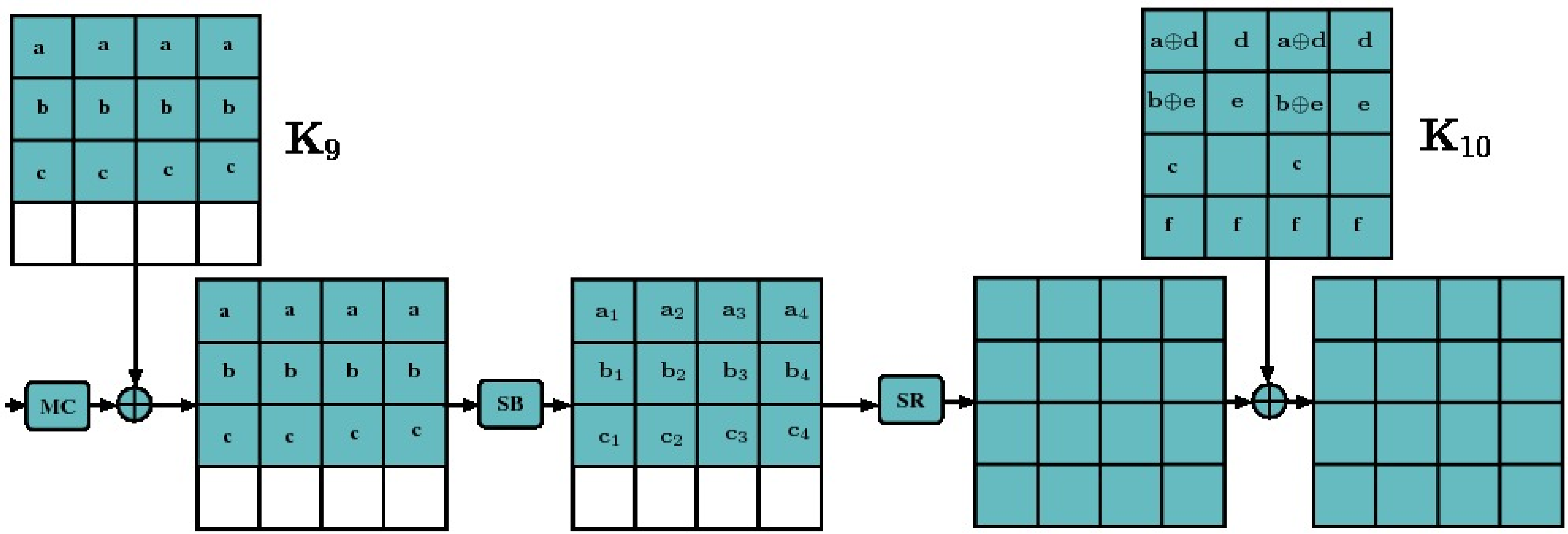
Kim and Quisquater's attack in 2008



Required faults:

Faults induced in 3 bytes out of 4 in the first column of 9th round key-schedule.

Propagation of the fault pattern



Requires two faulty ciphertexts (each with 3 simultaneous byte faults) to retrieve 12 bytes of the AES 10th round key.

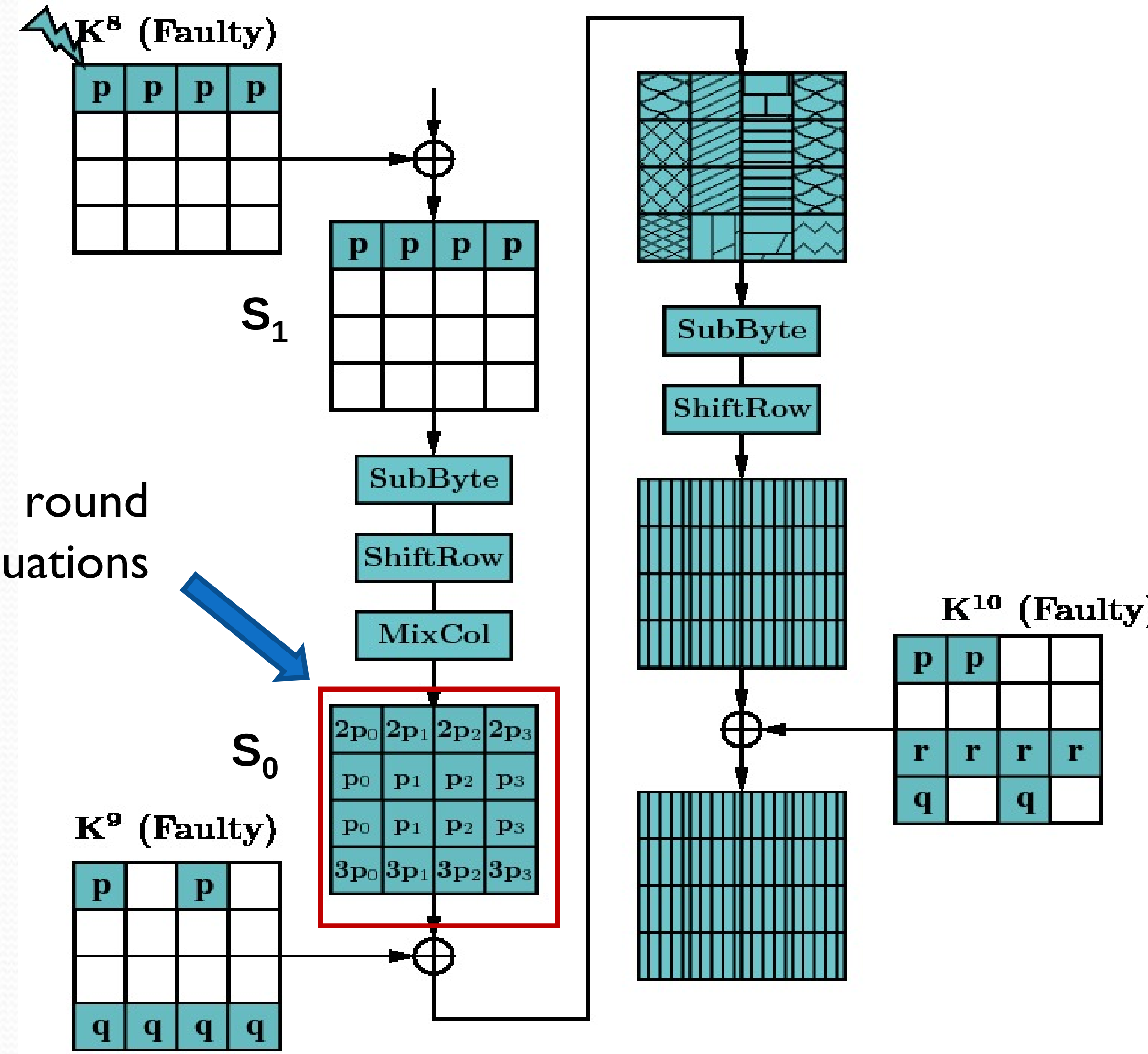
Thus brute force search of 2^{32} is still needed!

Motivations for a stronger fault attack on the AES key-schedule

- The attack's fault model should be practical.
  - More restrictions reduce the probability of success.
  - Larger number of faulty ciphertexts also reduce the probability of success.
- **Can we perform the attack with one fault?**
- The present attack:
  - Relies on a single-byte fault
  - Performs the attack with a single faulty ciphertext

Propagation of the fault

Generates 9^{th} round differential equations



8th Round Differential Equations

$2p_0$	$2p_1$	$2p_2$	$2p_3$
p_0	p_1	p_2	p_3
p_0	p_1	p_2	p_3
$3p_0$	$3p_1$	$3p_2$	$3p_3$

S_0

First column state matrix **S_0** gives the following equations:

$$p \oplus 2p_0 = S^{-1}\left(C_{0,0} \oplus K^{10}{}_{0,0}\right) \oplus S^{-1}\left(C^{*}{}_{0,0} \oplus K^{10}{}_{0,0} \oplus p\right)$$

$$p_0 = S^{-1}\left(C_{1,3} \oplus K^{10}{}_{1,3}\right) \oplus S^{-1}\left(C^{*}{}_{1,3} \oplus K^{10}{}_{1,3}\right)$$

$$p_0 = S^{-1}\left(C_{2,2} \oplus K^{10}{}_{2,2}\right) \oplus S^{-1}\left(C^{*}{}_{2,2} \oplus K^{10}{}_{2,2} \oplus r\right)$$

$$q \oplus 3p_0 = S^{-1}\left(C_{3,1} \oplus K^{10}{}_{3,1}\right) \oplus S^{-1}\left(C^{*}{}_{3,1} \oplus K^{10}{}_{3,1}\right)$$

Attack Results

- Fault Model: Single Byte fault in the 8^{th} round first column of AES key.
- Number of Faults: 1
- Keys remaining after the attack: 2^8.
- Time complexity of the attack is 2^{35} .
  - Improves our previous attack in CARDIS 11, which requires 2^{32} brute force key searches with a single byte multiple byte fault in the first column of the 9^{th} round AES key.

Experimental Results

The simulated attack was tested on 3 GHz Intel core 2 Duo processor running Linux (Ubuntu 10.4).

Random 128-bit AES Key	Number of Key Hypotheses	Running Time (Minutes)
6f6cd764b8ab8f18b8a867642371 47cd	$253 = 2^{7.08}$	33.677
9c1933a4f72386 13f85db821f4e49e65	$262=2^{8.03}$	35.716
f0003d186fd9c1282c2c7b3f578f39e8	$262=2^{8.03}$	35.291
d4e278834cfe91970bcb5eaf2317623a	$281=2^{8.13}$	36.716
71d1e622409256bbDade1874f57bd79c	$266=2^{8.05}$	35.516
9c1b15b1b49d76ad9dc359d265b52c84	$264=2^{8.04}$	36.666

Comparison with previous Works

Reference	Fault Model	Number of Faults	Exhaustive Search
Chen & Yen	Single Byte	22 to 44	1
Peacham et. al.	Multi Byte	12	1
Takahashi et.al.	Multi Byte	2	2^{48}
Kim et. al.	Multi Byte	2	2^{32}
Our attack in CARDIS 2011	Multi Byte	1	2^{32}
Our attack	Single Byte	1	2^{8}

DFA on AES Key-schedule
vs
DFA on AES datapath

- This attack shows that a single byte fault, in the AES-128 key schedule, reduces the AES key size to 2^8 values:
  - This result is analogous to the single byte fault induction in the AES-128 datapath, where also the remaining key size is 2^{32} (published in WISTP 11).

  - However the time complexity in this present attack is 2^{35}, while for the datapath it was 2^{30}

Conclusions

- We proposed an improved DFA on AES-128 key-schedule using single byte-fault
- DFA on AES-128 key schedule has almost the same effectiveness as the DFA on AES-datapath
- Both requires a single fault

Thank You

Please write to us if you have any question at

subidh@gmail.com,debdeep@cse.iitkgp.ernet.in