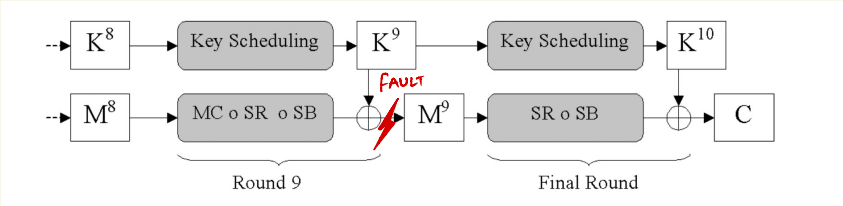
1.4/ 1.5 :: Bit fault attack - Description



-> If “C” is the correct cipher text without any faults and M^9 is the input to the 10th round,..

$$C = ShiftRows(SubBytes(M^9)) \oplus K^{10}$$

$$C_{ShiftRow(i)} = SubByte(M_i^9) \oplus K^{10}_{ShiftRow(i)}, \quad \forall i \in \{0, ..., 15\}$$

-> If a fault is injected (e_j) at the input M_j^9 , then the faulty input D is ..

$$D_{ShiftRow(j)} = SubByte(M_j^9 \oplus e_j) \oplus K^{10}_{ShiftRow(j)}$$

-> Taking XOR of the precious two equations we get the equation below ($K_{shiftrow}$ is cancelled out).

$$C_{ShiftRow(j)} \oplus D_{ShiftRow(j)} = SubByte(M_j^9) \oplus SubByte(M_j^9 \oplus e_j) \quad (1)$$

-> Using the above equation, we can obtain the input to the 10th round and taking XOR of that input with the correct cipher text will result in the 10th round key.
-> Further, we can put the 10th round key in inverses key scheduling and get the original key.i

Into more detail : (1.4)

-> Doing an XOR operation on the correct and faulty cipher texts will provide us with the LHS of equation 1. For every byte we will have 3 different values.

-> Now in order to find M9 from RHS we need to find all the possible values of (M XOR e) and equate it to LHS to find a possible match.

Note: M can have values from 0 to 255, &
E can have 8 values (0x01, 0x02, 0x04, 0x08, 0x10, 0x20, 0x40, 0x80) — 1 bit fault

-> After calculating all the possible values of M and E and making a list for all possible values of RHS after performing operations such as subByte, we search for our LHS value through that list and find matches for that value.

Note: For each byte we have 3 different XOR values and for each of that values we will find multiple possible values of M & E.
The common M value among this list is our M value for that byte.

EXAMPLE

→ We have 3 different XOR values from multiple 1 bit faults.

Say the 3 values are →

9e 000...0 (9e)
3c 000...0 (3c)
2d 000...0 (2d)

} LHS.

→ We have the list (2D Array) of all possible values for RHS.

$$\text{list} = \begin{bmatrix} \vdots & \vdots & \vdots \\ M_j^9 & e_j & \{SB(M_j^9) \oplus SB(M_j^9 \oplus e_j)\} \\ \vdots & \vdots & \vdots \end{bmatrix}$$

check LHS with this value.

2048×3

$M \rightarrow 0$ to 2^8
$e \rightarrow 8$ values

∴ Total possible cases $= 2^8 \times 8$
$= 2048$

→ Say for (9c) we find 3 possible values of M & e →

(M, e)

7, 0x80

25, 0x40

128, 0x10

} For 9c

Similarly,

3c { 25, 0x40 ; 4, 0x10

2d { 3, 0x80 ; 9, 0x10 ; 25, 0x40

* From the above lists, the common value of M & e (25, 0x40) is our M value (for j^{th} Byte)

* Taking XOR of M_j & j^{th} Byte of Cipher text, we get key of j^{th} Byte (round key).