1.2)

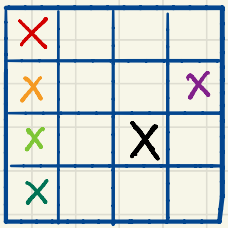
I/p M9

y = SubByte(x)

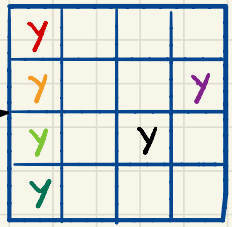
z = ShiftRow { SubByte(x) }

Key.

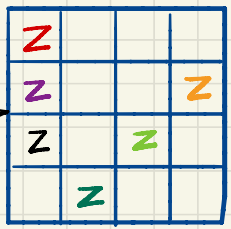
Where,
K_i ⇒ i^{th} element in the key.



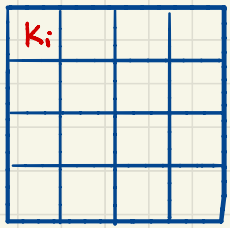
S-Box



Shift Row



(XOR)



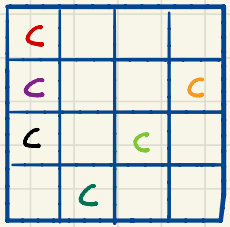
Round key

Example

Some possible positions where the fault might be injected (color coded)

Shift Row ⇒

Row 1 : NO Shift.
Row 2 : Shift Right By 1.
Row 3 : Shift Right By 2.
Row 4 : Shift Right By 3.



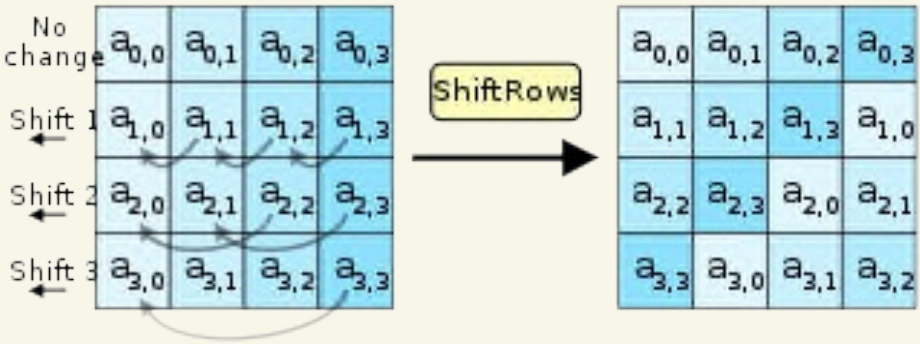
Cipher text = [Shift Row { SubByte(x) }] ⊕ K

↑ XOR operation

1.3) How does location of fault injection affect the propagation of fault?

For a bit fault attack :

-> As in bit fault attack the fault is injected at the beginning of the 10th round, we only have 3 operations: subByte (s-box), shift row and key XOR.
-> And the only operation that changes the location of fault from where it was injected is by shift row operation.



Therefore as seen from precious page, we will have elements shifting left which will change the location of faulty bit.