<u>Sunandan Adhikary</u>

<u>21CS91R14</u>

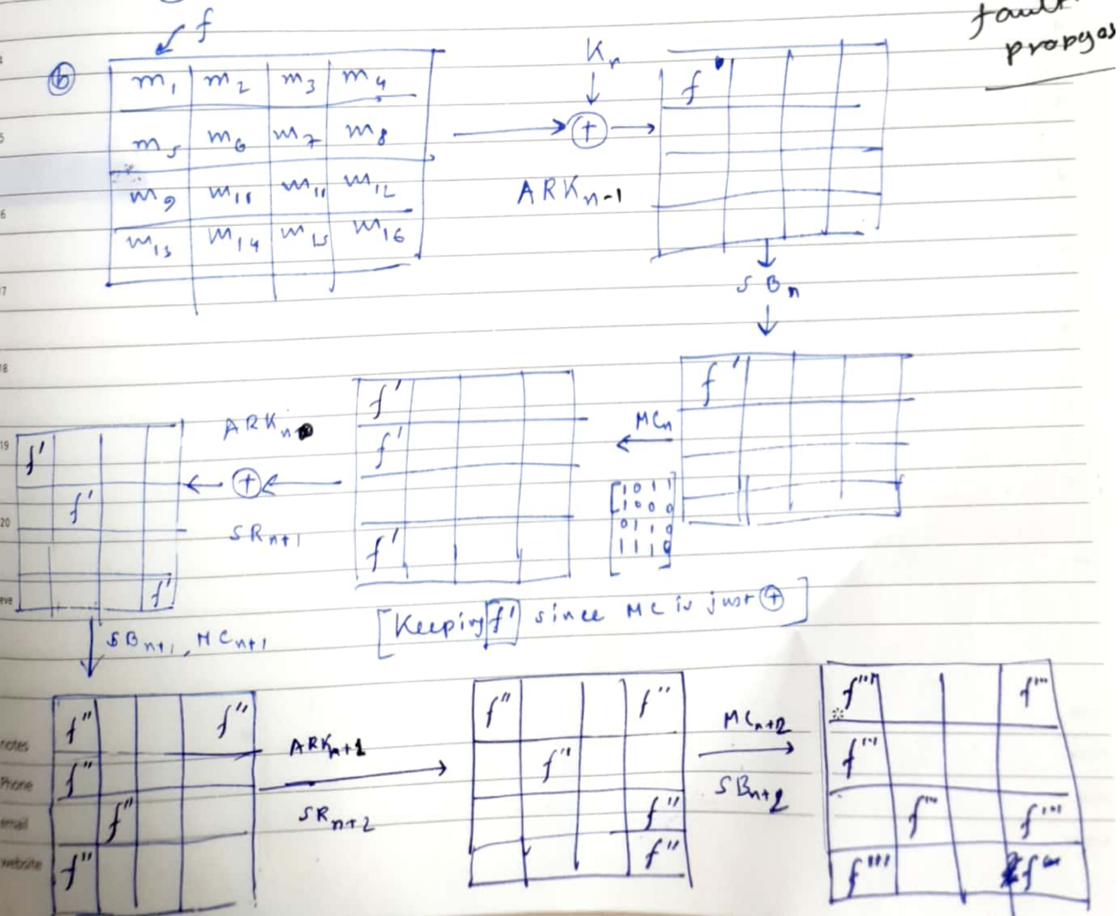
End Sem : HWSec

21CS91R14

~~1~~ 2 (a) We should take a nibble fault model since the 64 bit PT is arranged as 4x4 matrix of nibbles. This would help us compute the fault spreading following the steps of AES - SKINNY

(b)

How fault propagates



1 (a)

$$R^{top}_{i+1} = \frac{1+c_{i+1}}{2}\left(R^{top}_i + p_{i+1}\right) + \frac{1-c_{i+1}}{2}\left(R^{top}_i + r_{i+1}\right)$$

$$R^{bot}_{i+1} = \frac{1+c_{i+1}}{2}\left(R^{bot}_i + q_{i+1}\right) + \frac{1-c_{i+1}}{2}\left(R^{bot}_i + s_{i+1}\right)$$

$$\Rightarrow \Delta_{i+1} = R^{top}_{i+1} - R^{bot}_{i+1}$$

$$= \frac{1+c_{i+1}}{2}\left(\Delta_i + p_{i+1} - q_{i+1}\right)$$

$$+ \frac{1-c_{i+1}}{2}\left(\Delta_i + r_{i+1} - s_{i+1}\right)$$

$$= \Delta_i + \alpha_{i+1} c_{i+1} + \beta_{i+1}$$

$$\alpha_{i+1} = \frac{p_{i+1} - r_{i+1} - q_{i+1} + s_{i+1}}{2}$$

$$\beta_{i+1} = \frac{p_{i+1} + r_{i+1} - q_{i+1} - s_{i+1}}{2}$$

(b) initial delay = 0

$$\therefore \Delta(0) = \Delta(-1) + \alpha_0 c_0 + \beta_0$$

$$\Delta_1 = \Delta(0) + \alpha_1 c_1 + \beta_1 = \alpha_0 c_0 + \beta_0 + \alpha_1 c_1 + \beta_1$$

$$\Delta_n = \sum_{i=0}^{n-1}\left(\alpha_i c_i + \beta_i\right) = \sum_{i=0}^{n} w_i \phi_i = \langle w, \phi \rangle$$

(Prove)

$$\left[w_i = \begin{cases} \alpha_i & \forall\, i \in [0, n-1] \\ \Sigma \beta_i & i = n \end{cases} \right]$$

notes

Phone

email

website

(c) PAPUF follows linear model like APUF but ~~it~~ W does not depend on $\prod_i c_i$ i.e parity of challenge bits and in APUF there is ~~Also~~ no affine term.

(3) (b) (i) $R_0 R_1$, (ii) R_0

(iii) $R_0 R_1$ (iv) R_1

(c) Real trace = $\begin{array}{ccc} T_1 & T_2 & T_3 \\ \end{array}$ $[0.827 \quad 1.060 \quad 0.99]$

mean vector = $[T_1\text{-}avg_n \quad T_2\text{-}avg_n \quad T_3\text{-}avg_n]$

(Averaging over All key instances) where $K_i = n$, $n \in [0, 1]$

variance vec = $[T_1\text{-}cov, \quad T_2\text{-}cov, \quad T_3\text{-}cov]$

$T_1\text{-}cov =$ T_1^{sim}

$$cov = \frac{Cov(T_1, T_2, T_3)}{\sqrt{Var(T_1)\, Var(T_2)\, Var(T_3)}}$$

(4)

$$RMS_{[n_1,n_2,n_3]} = \left[\left(T_1^r - T_{1}\text{-}avg_{n_1}\right)^2 + \left(T_2^r - T_{2}\text{-}avg_{n_2}\right)^2 + \left(T_3^r - T_{3}\text{-}avg_{n_3}\right)^2 \right]^{1/2}$$

$$\forall\ n_1, n_2, n_3 \in [0, 1]$$

the least RMS ~~gives~~ tells us the $[n_1, n_2, n_3]$

(b)

(3)

(a) (1) ~~The adver~~ Steps:

→ the adversary fills the cache

→ lets the Auth op done

→ agin runs spy code and measures at which data access time req. is high.

→ Since the digits are 8bit and there are 8 bits in a cache line then each cache miss would indicate storing of one digit at that location.

→ This way once it understands ~~the consecutive~~ three such occurrences then it gets the memory locations

→ It ~~[illegible]~~ now can ~~run brute force~~ read that memory

(ii) Hence the complexity is 10^n since it needs to only understand ~~[illegible]~~ which of 10 lines holds the keys.

notes

Phone

email

website