Class Test - 2

Total — 30

1. a) $Y = AX^{-1} + B$

$TY = TAX^{-1} + TB$

$\Rightarrow TY = TAT^{-1}\, TX^{-1} + TB$

$\Rightarrow TY = TAT^{-1}(T(X))^{-1} + TB \qquad \because T[X^{-1}] = [TX]^{-1}$

$\Rightarrow Y' = A'X'^{-1} + B'$

$\therefore A' = TAT^{-1}$

5

b)

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

— Each row has 5 ones. Thus for multiplying with A we need 4 XORs per row

$\therefore 8 \times 4 = 32$ XORs.

$$A' = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{array}{l} \to 1 \\ \to 3 \\ \to 3 \\ \to 3 \\ \to 1 \\ \to 2 \\ \to 3 \\ \to 2 \end{array} \begin{array}{c} \text{No. of XORs} \\ 0 \\ 2 \\ 2 \\ 2 \\ 0 \\ 1 \\ 2 \\ 1 \\ \hline 10 \text{ XORs} \end{array}$$

5

$\therefore$ 10 XOR's are required to multiply with A' which is very much ~~less~~ compared to A.

2. (a) $T(3)(a_1 x + a_0) = T(2)(a_1 x + a_0) + (a_1 x + a_0)$

5

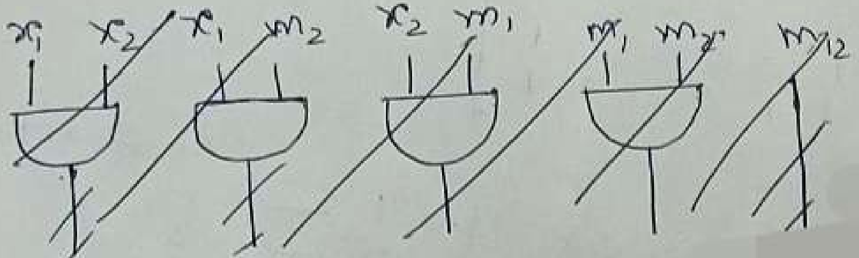
3. $f = x_1 x_2 + x_3 x_4$

Let m_1, m_2, m_3, m_4 be the masks for x_1, x_2, x_3 & x_4 respectively and let m_{12} and m_{34} be the masks corresponding to the two product terms

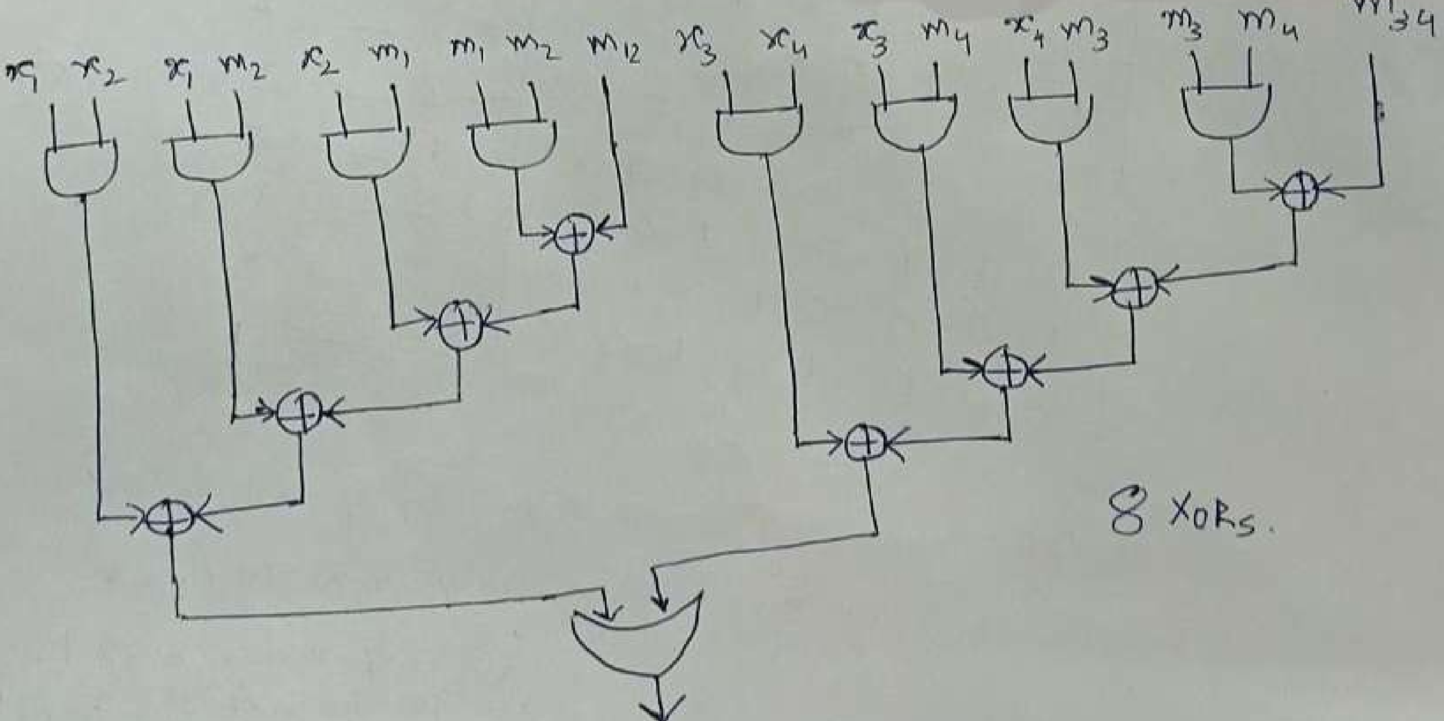
$$f = ((x_1 \oplus m_1)(x_2 \oplus m_2) \oplus m_{12}) + ((x_3 \oplus m_3)(x_4 \oplus m_4) \oplus m_{34})$$

$$= (x_1 x_2 \oplus x_1 m_2 \oplus x_2 m_1 \oplus m_1 m_2 \oplus m_{12})$$

$$+ (x_3 x_4 \oplus x_3 m_4 \oplus x_4 m_3 \oplus m_3 m_4 \oplus m_{34})$$

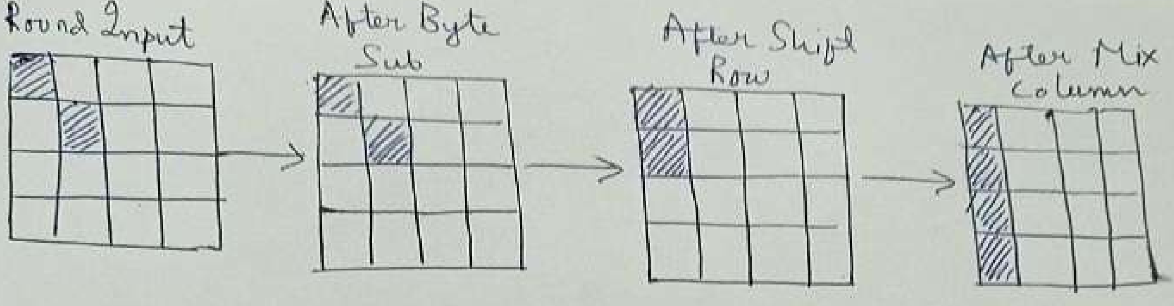


5



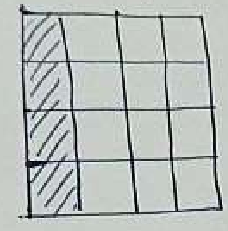
8 XORs.

7\. 8th Round



9th Round

Round Input



After Byte Sub

F_1			
F_2			
F_3			
F_4			

→ After Shift Row

F_1			
			F_2
		F_3	
	F_4		

→ After Mix Column

$2F_1$	F_4	F_3	$3F_2$
F_1	F_4	$3F_3$	$2F_3$
F_1	$3F_4$	$2F_3$	F_2
$3F_1$	$2F_4$	F_3	F_2

Thus Invariant for any fault within a diagonal

10

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$