Linear Cryptanalysis

1. Construction 1

$$C = M \oplus K$$

$\Rightarrow$ 1 Known Plaintext Attack $\quad Q = (M_1, C_1)$

$$K = M_1 \oplus C_1$$

2. Construction 2

$$C_1 = m_1 \oplus m_2 \oplus k_1 \oplus k_2$$
$$C_2 = m_3 \oplus k_2 \oplus k_3$$
$$C_3 = m_4 \oplus m_1 \oplus k_3 \oplus k_1$$
$$C_4 = m_1 \oplus m_2 \oplus k_4 \oplus k_2$$

$\{ M = m_1 \| m_2 \| m_3 m_4$

$\Rightarrow$ 1 known Plaintext Attack

$Q = (M_1, C_1)$

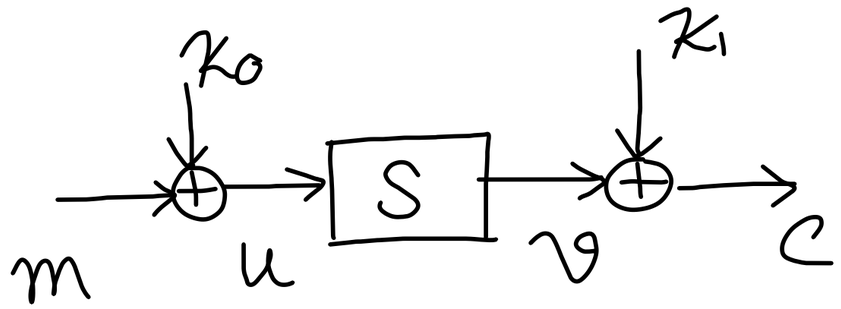
$|K| = 2^4 \Rightarrow |K| = 2$

3. Construction 3

$$C = \alpha \cdot M \oplus \beta \cdot K$$

$\Downarrow$

Key Recovery Attack



u_1, u_2, u_3, u_4
v_1, v_2, v_3, v_4

Suppose, $u_1 \oplus u_2 \oplus u_3 = v_1 \oplus v_2$

$$\underbrace{(1110)}_{\alpha}\begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix} = \underbrace{(1100)}_{\beta}\begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix}$$

Try to approximate some linear relation between the S-box i/p & o/p.

- $\alpha \cdot u = \beta \cdot v$
- $\alpha(m \oplus K_0) = \beta(c \oplus K_1)$
- $\alpha \cdot K_0 \oplus \beta \cdot K_1 = \alpha \cdot m \oplus \beta \cdot c$

$|K| = 2^8$

$\Downarrow$

- $|K| = 2^7$ (KPA with 1 query)

$$\left| \Pr[\alpha \cdot u \oplus \beta \cdot v = 0] - \frac{1}{2} \right|$$

$\Downarrow$

Should be maximized

$$\Pr[\alpha \cdot u \oplus \beta \cdot v = 0] = \frac{7}{8}$$

Piling-Up Lemma

$\Pr[X_1 = 0] = p_1$ bias $\epsilon_1 = \left(p_1 - \frac{1}{2}\right)$

$\Pr[X_2 = 0] = p_2$ $\epsilon_2 = \left(p_2 - \frac{1}{2}\right)$

① X_1, X_2 independent; bias of $X_1 = \epsilon_1$, bias of $X_2 = \epsilon_2$, What is the bias of $(X_1 \oplus X_2)$?

$$\Pr[X_1 \oplus X_2 = 0] = p_1 p_2 + (1-p_1)(1-p_2)$$

$$= \left(\epsilon_1 + \tfrac{1}{2}\right)\left(\epsilon_2 + \tfrac{1}{2}\right) + \left(\tfrac{1}{2} - \epsilon_1\right)\left(\tfrac{1}{2} - \epsilon_2\right)$$

$$= \epsilon_1\epsilon_2 + \tfrac{1}{2}(\epsilon_1 + \epsilon_2) + \tfrac{1}{4} + \tfrac{1}{4} - \tfrac{1}{2}(\epsilon_1 + \epsilon_2) + \epsilon_1\epsilon_2$$

$$= \frac{1}{2} + 2\epsilon_1\epsilon_2$$

bias $= 2\epsilon_1\epsilon_2$

$X_1, X_2, \ldots, X_n \rightarrow \epsilon_1, \ldots \epsilon_n$

$X_1 \oplus X_2 \oplus \cdots \oplus X_n$

$\hookrightarrow \epsilon_{1\ldots n} = 2^{n-1}\epsilon_1 \cdots \epsilon_n$

(use induction)