Linear Cryptanalysis

Beispiel: cipher ONE attackieren

Die Werte in der LA-Table geben Relationen an, große Beträge hohe Wahrscheinlichkeiten.

LAT-Eintrag $0x8 \rightsquigarrow 0x1$

1 0 0 0 . 0 0 0 1

$x_3 x_2 x_1 x_0$. $y_3 y_2 y_1 y_0$

$1 \cdot x_3 = 1 \cdot y_0$

$\Rightarrow x_3 = y_0$ in $\frac{8+4}{16}$ alle Fälle

4 DDT

difference distribution table

DC

LAT

linear approximation table

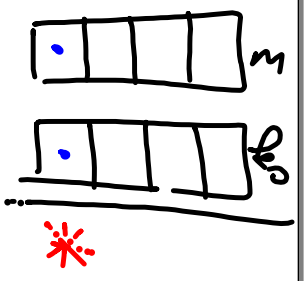
LC

cipher ONE

$$c = \underbrace{S(m + k_0)}_{x_3 = y_0} + k_1$$

in 3/4 aller Fälle

- x_3 Eingabe der S-Box (3. Bit)
- 3. Bit von $m + k_0$ wird benötigt
- " $(m + k_0)_3$ " entsteht durch $m_3 + k_{03}$



- $m_3 + k_{03}$ mit 75% Wahrscheinlichkeit das 0-te Bit der Ausgabe
- weil aber $S(in + k_0) + k_1 = c$

  folgt $S(m + k_0) = c + k_1$

  daher $S(m + k_0)_0 = c_0 + k_{10}$
- also $m_3 + k_{03} = c_0 + k_{10}$ mit W. 75 %

Insgesamt

$$k_{03} + k_{10} = m_3 + c_0$$

mit 75 % Wahrscheinlichkeit.

$\Rightarrow$ eine Relation erspart dem Angreifer das Ausprobieren eines Key bits

Ebenso

$Oxc \rightsquigarrow Oxc$

1100

$k_{03} + k_{02} + k_{13} + k_{12} + 1 = m_3 + m_2 + c_3 + c_2$

mit Wahrscheinlichkeit $\frac{8+6}{16} = \frac{7}{8} \approx 87\%$

Übung:

konkreter Ablauf für relevante Relationen

1: $k_{00} + k_{12} = 0$

⋮

32: $k_{00} + k_{01} + \ldots = 1$

0	1	1	1	1	1	0	1	1	0	0	0	1	0	0	0
k_{03}	…		k_{00}	k_{13}	…	k_{10}									

zwei Lösungen