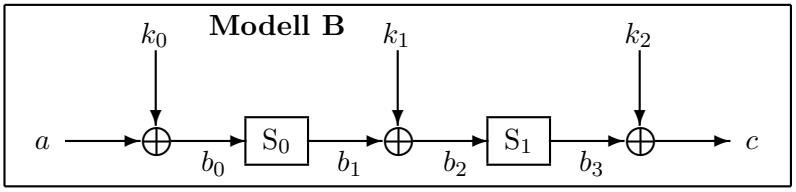
5 Beispiel: Eine Zweirunden-Chiffre

Für die Analyse von Chiffren über mehrere Runden beginnen wir wieder mit einem einfachen Beispiel, dem Modell „B“:



Die Verschlüsselung geschieht also sukzessive nach den Formeln

$$b_0 = a + k_0,\ b_1 = f_1(b_0),\ b_2 = b_1 + k_1,\ b_3 = f_2(b_2),\ c = b_3 + k_2,$$

oder in einem Schritt:

$$c = f_2[f_1(a + k_0) + k_1] + k_2.$$

[Dabei wird f_1 durch die S-Box S_0 und f_2 durch die S-Box S_1 beschrieben.]

Nach Analyse der S-Boxen wissen wir über die linearen Relationen für die Rundenabbildungen f_1 und f_2 Bescheid. Was können wir daraus über lineare Relationen für die ganze Chiffre herleiten?

Sei (α, β) eine lineare Relation für f_1 mit Wahrscheinlichkeit p_1 und (β, γ) eine für f_2 mit Wahrscheinlichkeit p_2. Dann gilt

$$\begin{aligned} \gamma(c) &= \gamma(b_3) + \gamma(k_2) \overset{p_2}{\approx} \beta(b_2) + \gamma(k_2) = \beta(b_1) + \beta(k_1) + \gamma(k_2) \\ &\overset{p_1}{\approx} \alpha(b_0) + \beta(k_1) + \gamma(k_2) = \alpha(a) + \alpha(k_0) + \beta(k_1) + \gamma(k_2) \end{aligned}$$

Wir erhalten also eine Relation für das eine Schlüsselbit $\alpha(k_0)+\beta(k_1)+\gamma(k_2)$ in der Form

$$\alpha(k_0) + \beta(k_1) + \gamma(k_2) \overset{p}{\approx} \alpha(a) + \gamma(c)$$

mit noch unbekannter Wahrscheinlichkeit p. Diese ist im allgemeinen sehr schwer explizit zu bestimmen. Betrachten wir das folgende *konkrete Beispiel*:

Es sei $n = 4$, und S_0 und S_1 seien die beiden S-Boxen von Lucifer. Die Linearformen $\alpha = 0001$ und $\beta = 1101$ seien wie in Abschnitt 3 gewählt. Passend dazu sei $\gamma = 1100$ gewählt, so dass das Paar (β, γ) das maximale Potenzial $\frac{1}{4}$ für S_1 annimmt, und $\hat{\vartheta}_{f_2}(\beta, \gamma) = -8$. Als konkrete Rundenschlüssel werden $k_0 = 1000$, $k_1 = 0001$ – wie in 3 – und $k_2 = 0110$ gewählt. Die Tabelle über alle 16 möglichen Klartexte ist:

a	b_0	b_1	b_2	b_3	c	$\alpha(a)+\gamma(c)$
0000	1000	0010	0011	1001	1111	0
0001	1001	0110	0111	0100	0010	1
0010	1010	0011	0010	1110	1000	1
0011	1011	0001	0000	0111	0001	1
0100	1100	1001	1000	1100	1010	1
0101	1101	0100	0101	1011	1101	1
0110	1110	0101	0100	0011	0101	1
0111	1111	1000	1001	1101	1011	0
1000	0000	1100	1101	1111	1001	1
1001	0001	1111	1110	1000	1110	1
1010	0010	0111	0110	0000	0110	1
1011	0011	1010	1011	1010	1100	1
1100	0100	1110	1111	0101	0011	0
1101	0101	1101	1100	0110	0000	1
1110	0110	1011	1010	0001	0111	1
1111	0111	0000	0001	0010	0100	0

Da $\hat{\vartheta}_{f_2}(\beta,\gamma) = -8$, soll das Bit $\alpha(k_0)+\beta(k_1)+\gamma(k_2)+1 = 1$ erkannt werden; dies geschieht in 12 von 16 Fällen korrekt, also mit Wahrscheinlichkeit $p = \frac{3}{4}$ bzw. mit Potenzial $\lambda = 1/4$.

Es gibt auch andere „Pfade“ von α nach γ, z. B. über $\beta' = 0001$ mit $\hat{\vartheta}_{f_1}(\alpha,\beta') = -4$, $\lambda'_1 = \frac{1}{16}$, $p'_1 = \frac{1}{4}$ und $\hat{\vartheta}_{f_2}(\beta,\gamma) = 4$, $\lambda'_2 = \frac{1}{16}$, $p'_2 = \frac{3}{4}$. Hier wird also versucht, das Bit $\alpha(k_0)+\beta'(k_1)+\gamma(k_2)+1 = 1$ zu finden. Auch hierfür ist die Erfolgswahrscheinlichkeit also $p' = \frac{3}{4}$.