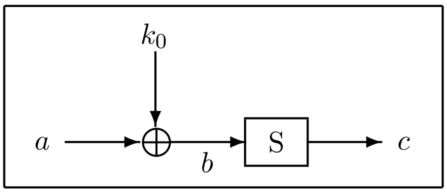
3 Beispiel: Eine Einrunden-Chiffre

Es werden Beispiele betrachtet, die als ernsthafte Blockchiffren viel zu einfach sind, aber das Prinzip der linearen Kryptoanalyse sehr anschaulich und nachvollziehbar demonstrieren. Dabei werden stets Rundenfunktionen der Gestalt $f(a+k)$ betrachtet, d. h., der Schlüssel wird vor der Anwendung einer bijektiven S-Box $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ binär auf den Klartext aufaddiert. Das einfachste denkbare Modell, die Verschlüsselung nach der Vorschrift

$$c = f(a+k),$$

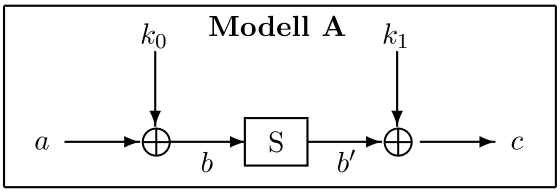


ist dabei witzlos, da bei bekanntem Klartext die Gleichung nach dem Schlüssel k auflösbar ist:

$$k = f^{-1}(c) + a.$$

Dieser einfache Angriff wird bei dem etwas komplizierteren Modell „A“

$$c = f(a + k_0) + k_1$$



verhindert [in den grafischen Darstellungen wird die Abbildung f immer durch die S-Box S repräsentiert]; hier ist der Ansatz der linearen Kryptoanalyse bereits sinnvoll: Sei (α, β) ein Paar von Linearformen mit

$$\beta \circ f(x) \stackrel{p}{\approx} \alpha(x),$$

wobei das Symbol $\stackrel{p}{\approx}$ gelesen wird als „ist gleich mit Wahrscheinlichkeit p“. Dann gilt

$$\begin{aligned} \beta(c) &= \beta(b' + k_1) = \beta(b') + \beta(k_1) \\ &\stackrel{p}{\approx} \alpha(b) + \beta(k_1) = \alpha(a + k_0) + \beta(k_1) = \alpha(a) + \alpha(k_0) + \beta(k_1). \end{aligned}$$

Hierbei wird k als fest angesehen und zur Spezifikation der Wahrscheinlichkeit über alle Klartexte a gemittelt. Als lineare Relation für einige Bits des Schlüssels $k = (k_1, k_2)$ erhalten wir also

$$\alpha(k_0) + \beta(k_1) \stackrel{p}{\approx} \alpha(a) + \beta(c).$$

Sie gilt genau mit der Wahrscheinlichkeit p $= p_f(\alpha, \beta)$. Ein analoger Schluss lässt sich für die Relation

$$\beta \circ f(x) \overset{1-p}{\approx} \alpha(x) + 1$$

durchführen. Insgesamt ist damit gezeigt:

Satz 1 *Im Modell A sei (α, β) eine lineare Relation für f mit der Wahrscheinlichkeit p. Dann ist $p_1 = \max\{p, 1-p\}$ die Erfolgswahrscheinlichkeit der linearen Kryptoanalyse mit* einem *bekannten Klartext.*

Nehmen wir zunächst als konkretes Beispiel $n = 4$ und für f die S-Box S_0 von LUCIFER. Aus der Analyse dieser BOOLEschen Abbildung wissen wir, dass das lineare Potenzial von $\frac{9}{16}$ z. B. von dem Paar $\alpha = 0001$ und $\beta = 1101$ mit $\hat{\vartheta}_f(\alpha, \beta) = 12$ angenommen wird. Die zugehörige Wahrscheinlichkeit ist $p_f(\alpha, \beta) = \frac{7}{8}$. Als konkrete Rundenschlüssel werden $k_0 = 1000$ und $k_1 = 0001$ gewählt. Eine Tabelle über alle 16 möglichen Klartexte sieht dann so aus (unter Verwendung der bekannten Wertetabelle von f):

a	b	b'	c	$\alpha(a) + \beta(c)$
0000	1000	0010	0011	1
0001	1001	0110	0111	1
0010	1010	0011	0010	0
0011	1011	0001	0000	1
0100	1100	1001	1000	1
0101	1101	0100	0101	1
0110	1110	0101	0100	1
0111	1111	1000	1001	1
1000	0000	1100	1101	1
1001	0001	1111	1110	1
1010	0010	0111	0110	1
1011	0011	1010	1011	1
1100	0100	1110	1111	1
1101	0101	1101	1100	1
1110	0110	1011	1010	1
1111	0111	0000	0001	0

Der Wert $1 = \alpha(k_0) + \beta(k_1)$ wird also, wie es sein soll, genau 14-mal angenommen.

Wie groß ist nun die Erfolgswahrscheinlichkeit p_N dafür, diesen Wert richtig zu schätzen, wenn man $N = 1, 2, \ldots$ zufällige bekannte Klartexte aus der Menge der 2^n möglichen zur Verfügung hat? (Zu gegebenen festen Linearformen α und β mit $p = p_f(\alpha, \beta)$ für einen beliebigen – unbekannten, gesuchten – Schlüssel k.) Das ist genau die Fragestellung der hypergeometrischen Verteilung, und daher gilt:

Satz 2 *Im Modell A sei* (α, β) *eine lineare Relation für* f *mit der Wahrscheinlichkeit* $p = \frac{s}{2^n}$. *Dann ist die Erfolgswahrscheinlichkeit der linearen Kryptoanalyse mit* N *bekannten Klartexten gerade die kumulierte Wahrscheinlichkeit* $p_N = p_N^{(s)}$ *der hypergeometrischen Verteilung zu den Parametern* 2^n, $s = p_1 2^n$ *und* N *mit* $p_1 = \max\{p, 1-p\}$.

Korollar 1 $p_N = 1$, *wenn* $N > 2^{n+1} \cdot (1 - p_1)$.

Im konkreten Beispiel oben wird diese Bedingung zu $N > 32 \cdot \frac{1}{8} = 4$, also $N \geq 5$.

Korollar 2 *Ist* $p \approx \frac{1}{2}$, $N \ll 2^n$ *und* N *nicht zu klein, so*

$$p_N \approx \frac{1}{\sqrt{2\pi}} \cdot \int_{\infty}^{\sqrt{r\lambda}} e^{-t^2/2} dt.$$