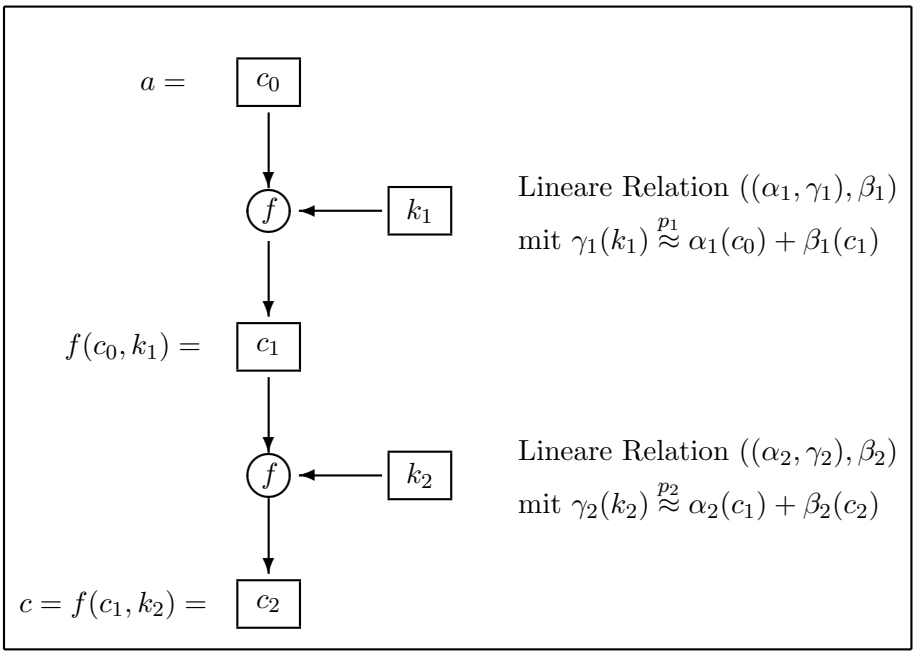
7 Lineare Pfade und lineare Hüllen

Die Rundenabbildung

$$f\colon \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^n$$

einer Bitblock-Chiffre werde jetzt über mehrere Runden iteriert mit *unabhängigen* Rundenschlüsseln $k_i \in \mathbb{F}_2^q$.

Zunächst wird der Fall von zwei Runden behandelt.



Es gelten also die linearen Relationen

$$\gamma_1(k_1) \overset{p_1}{\approx} \alpha_1(c_0) + \beta_1(c_1)$$

mit Wahrscheinlichkeit p_1 und Potenzial $\lambda_1 = (2p_1 - 1)^2$ und

$$\gamma_2(k_2) \overset{p_2}{\approx} \alpha_2(c_1) + \beta_2(c_2)$$

mit Wahrscheinlichkeit p_2 und Potenzial $\lambda_2 = (2p_2 - 1)^2$. Die beiden linearen Relationen sind **kombinierbar**, wenn $\alpha_2 = \beta_1$. Dann gilt

$$\gamma_1(k_1) + \gamma_2(k_2) \overset{p}{\approx} \alpha_1(c_0) + \beta_2(c_2)$$

mit einer Wahrscheinlichkeit p und einem Potenzial λ, die unter der Annahme, dass die Relationen stochastisch unabhängig, insbesondere k_1 und k_2 unabhängig gewählt sind, aus dem Piling-Up-Lemma folgen. Danach wäre $\lambda = \lambda_1\lambda_2$. Das Beispiel in Abschnitt 5 zeigt, dass das nicht gilt; die Annahme

unabhängiger Rundenschlüssel reicht nicht. Die Situation wird dadurch verkompliziert, dass es von der Relation α_1 zur Relation β_2 mehrere „Pfade“, d. h., mehrere Zwischenschritte gibt. Ferner werden, wenn die Rundenzahl größer ist, dabei jedesmal andere Schlüsselbits der Zwischenrunden herausgepickt.

Im Beispiel war $\lambda_1 = \frac{9}{16}$, $\lambda_2 = \frac{1}{4}$ und $\lambda = \frac{1}{4} = \frac{16}{64}$ deutlich größer als $\lambda_1\lambda_2 = \frac{9}{64}$.

Um wenigstens den begrifflichen Rahmen, wenn schon nicht die Ergebnisse, zu präzisieren, definiert man: Gegeben sei eine über r Runden iterierte Bitblock-Chiffre. Sei $((\alpha_i, \gamma_i), \beta_i)$ eine lineare Relation für die i-te Runde mit Potenzial λ_i. Es sei $\alpha_i = \beta_{i-1}$ für $i = 2, \ldots, r$. Sei $\beta_0 := \alpha_1$. Dann heißt die Kette $(\beta_0, \ldots, \beta_r)$ ein **linearer Pfad** für die Chiffre mit Potenzial $\lambda := \lambda_1 \cdots \lambda_r$. Die **lineare Hülle** [Nyberg 1994] zu dem Paar (β_0, β_r) ist die Menge aller linearen Pfade, die β_0 mit β_r verbinden. Ein linearer Pfad heißt **dominant**, wenn sein Potenzial maximal unter allen linearen Pfaden der zugehörigen linearen Hülle ist.

Achtung: Das Potenzial eines linearen Pfades ist im allgemeinen *nicht* das Potenzial der resultierenden linearen Relation. Vielmehr gilt (ohne Beweis):

Satz 1 (Matsui) *Gegeben sei eine über r Runden iterierte Bitblock-Chiffre mit unabhängigen Rundenschlüsseln. Es seien r lineare Relationen für die jeweilige Runde gegeben, die einen linearen Pfad bilden und das Potenzial $\lambda_1, \ldots, \lambda_r$ haben. Dann hat die kombinierte lineare Relation das Potenzial $\lambda \geq \lambda_1 \cdots \lambda_r$. Ist der lineare Pfad dominant, so gilt $\lambda \approx \lambda_1 \cdots \lambda_r$.*

Dieses Ergebnis vermittelt eine konkrete Vorstellung davon, wie der Nutzen von linearen Approximationen mit jeder Runde, wo es keine lineare Relation mit Wahrscheinlichkeit 1 oder 0 gibt, weiter abnimmt, d. h., wie die Sicherheit der Chiffre vor linearer Kryptoanalyse mit zunehmender Rundenzahl steigt.

Die Methode der linearen Kryptoanalyse beruht also auf der Faustregel:

> *Entlang eines linearen Pfades multiplizieren sich die linearen Potenziale (nach Definition). Das Potenzial einer linearen Hülle wird durch das Potenzial des dominanten linearen Pfades ausreichend approximiert.*

Allerdings muss man beachten, dass der Satz nur eine Untergrenze für das Potenzial angibt, also eine obere Schranke für den Aufwand der linearen Kryptoanalyse. Für den Sicherheitsnachweis der Chiffre bräuchte man eine untere Schranke für den Aufwand, also eine obere Schranke für das Potenzial einer kombinierten linearen Relation. Hier gilt nur die empirisch ermittelte Näherungsaussage des Satzes; ferner sind grobe obere Schranken bekannt, die allerdings nicht zur Beruhigung des Kryptographen ausreichen.

Weiter ist bei der Anwendung zu beachten, dass bei konkreten Chiffren die Rundenschlüssel nicht unabhängig sind. Allerdings ist (nach empirischen Erfahrungen) wie so oft in der Statistik der Effekt dieser Abhängigkeit vernachlässigbar, wenn die Schlüsselauswahl für die einzelnen Runden wenigstens ein bisschen komplex ist.

Auf diese Weise kommt auch das in Abschnitt 4 genannte Ergebnis für DES zustande.