2.6 Algebraische Angriffe bei kleiner Rundenzahl

Formeln für kleine Rundenzahlen

Die Rekursionsformel für eine FEISTEL-Chiffre kann man in der Form

$$(L_i, R_i) = (R_{i-1}, L_{i-1} + f(R_{i-1}, k_i))$$

schreiben mit dem Rundenschlüssel $k_i = \alpha_i(k)$.

Satz 4 *Die Ergebnisse einer* FEISTEL*-Chiffre nach* 2, 3 *und* 4 *Runden erfüllen die Gleichungen*

$$\begin{aligned} L_2 - L_0 &= f(R_0, k_1), \\ R_2 - R_0 &= f(L_2, k_2); \end{aligned}$$

$$\begin{aligned} L_3 - R_0 &= f(L_0 + f(R_0, k_1), k_2), \\ R_3 - L_0 &= f(L_3, k_3) + f(R_0, k_1); \end{aligned}$$

$$\begin{aligned} L_4 - L_0 &= f(R_0, k_1) + f(R_4 - f(L_4, k_4), k_3), \\ R_4 - R_0 &= f(L_4, k_4) + f(L_0 + f(R_0, k_1), k_2). \end{aligned}$$

Die Minuszeichen stehen hier, damit die Formeln auch noch für die Verallgemeinerung auf abelsche Gruppen gut sind, wo nicht, wie „im Binären“, Plus und Minus zusammenfallen. Der Sinn dieser Formeln ist, dass außer den Rundenschlüsseln k_i jeweils nur der Klartext (L_0, R_0) und der Geheimtext (L_r, R_r) vorkommen, also Größen, die bei der algebraischen Kryptoanalyse als bekannt angenommen werden.

Beweis. Im Fall von zwei Runden sind die Gleichungen

$$\begin{aligned} L_1 &= R_0, \\ R_1 &= L_0 + f(R_0, k_1), \\ L_2 &= R_1 = L_0 + f(R_0, k_1), \\ R_2 &= L_1 + f(R_1, k_2) = R_0 + f(L_2, k_2); \end{aligned}$$

und daraus folgt die Behauptung.

Im Fall von drei Runden ist analog

$$\begin{aligned} L_1 &= R_0, \\ R_1 &= L_0 + f(R_0, k_1), \\ L_2 &= R_1 = L_0 + f(R_0, k_1), \\ R_2 &= L_1 + f(R_1, k_2) = R_0 + f(L_2, k_2), \\ L_3 &= R_2 = R_0 + f(L_0 + f(R_0, k_1), k_2), \\ R_3 &= L_2 + f(R_2, k_3) = L_0 + f(R_0, k_1) + f(L_3, k_3). \end{aligned}$$

Die Berechnung für vier Runden bleibt dem Leser überlassen. ◇

Zweirunden-Chiffren

Bei einem Angriff mit einem bekannten Klartextblock sind L_0, R_0, L_2 und R_2 gegeben. Aufzulösen sind die Gleichungen

$$\begin{aligned} L_2 - L_0 &= f(R_0, k_1), \\ R_2 - R_0 &= f(L_2, k_2); \end{aligned}$$

nach k_1 und k_2. Die Sicherheit der Chiffre hängt also ganz von der Kernfunktion f ab. Da q, die Bitlänge der Teilschlüssel, allerdings in der Regel wesentlich kleiner als die Gesamtschlüssellänge l ist, sind die für einen Exhaustionsangriff nötigen 2^{q+1} Auswertungen von f eventuell im Bereich des Möglichen. Bemerkenswert ist, dass diese Überlegung unabhängig von der Schlüsselauswahl α ist – es werden einfach die tatsächlich verwendeten Schlüsselbits (k_1, k_2) bestimmt.

Beispiel: Auf $\mathbb{F}_2^s$ wird die Multiplikation „$\cdot$“ des Körpers $\mathbb{F}_t$ mit $t = 2^s$ verwendet [diese wird in einem späteren Abschnitt genauer erklärt] und

$$f(x, y) = x \cdot y$$

gesetzt. Die Schlüsselauswahl sei durch $l = 2q$ und $k_i =$ linke oder rechte Hälfte von k, je nachdem ob i ungerade oder gerade ist, gegeben. Dann werden die Gleichungen zu

$$\begin{aligned} L_2 - L_0 &= R_0 \cdot k_1, \\ R_2 - R_0 &= L_2 \cdot k_2, \end{aligned}$$

sind also leicht zu lösen. (Falls einer der Faktoren R_0 oder L_2 Null ist, braucht man natürlich einen anderen bekannten Klartextblock.)

Dreirunden-Chiffren

Hier sind die zu lösenden Gleichungen deutlich komplexer, da f bereits iteriert wird. Allerdings ist mit einem bekanntem Klartextblock ein Treffpunktangriff (Meet in the Middle) durchführbar, wenn die Bitlänge q der Teilschlüssel nicht zu groß ist: Man berechnet für alle möglichen Teilschlüssel k_1 das Zwischenergebnis (L_1, R_1) nach der ersten Runde und speichert es in einer Tabelle. Über die letzten beiden Runden macht man eine Exhaustion, wie für die Zweirunden-Chiffre beschrieben. Der Gesamtaufwand beträgt also $3 \cdot 2^q$ Auswertungen von f und 2^q Speicherplätze.

Daraus resultiert die Faustregel: Feistel-*Chiffren sollten stets mindestens vier Runden haben.* Das ist eine passende Ergänzung zu dem zitierten Ergebnis von Luby/Rackoff. Man sieht, wie mit wachsender Rundenzahl, wenn nur f genügend komplex ist, die Resistenz des gesamten Schemas gegen den algebraischen Angriff wächst.

In der **Beispiel**chiffre mit Kernfunktion = Multiplikation im Körper mit 2^s Elementen werden die Gleichungen zu:

$$\begin{aligned} L_3 - R_0 &= [L_0 + R_0 \cdot k_1)] \cdot k_2, \\ R_3 - L_0 &= [R_0 + R_3] \cdot k_1. \end{aligned}$$

Sie sind offensichtlich leicht zu lösen.

Vierrunden-Chiffren

Hier sind die Gleichungen noch komplexer, und selbst im **Beispiel**

$$\begin{aligned} L_4 - L_0 &= [R_0 + R_4 + L_4 \cdot k_2] \cdot k_1, \\ R_4 - R_0 &= [L_4 + L_0 + R_0 \cdot k_1] \cdot k_2, \end{aligned}$$

sind sie schon quadratisch in zwei Unbekannten (wenn auch in diesem Trivialbeispiel noch leicht zu lösen – die Elimination von k_1 führt auf eine quadratische Gleichung für k_2 – **Übungsaufgabe**).