5 Kryptoanalyse von Bitblock-Chiffren

Für die Kryptoanalyse von Bitblock-Chiffren sind folgende allgemeine Ansätze bekannt:

1. Exhaustion = vollständige Schlüsselsuche. Sie wird durch Wahl einer genügend großen Schlüssellänge unmöglich gemacht. – Viele der weiteren bekannten Angriffe zielen darauf ab, den Suchraum für die Exhaustion signifikant zu verkleinern.

2. Algebraischer Angriff. Er wird durch die Nichtlinearität der Chiffre erschwert oder verhindert.

3. Statistische Angriffe auf versteckte Linearität:

   (a) Lineare Kryptoanalyse (Matsui/Yamagishi, Eurocrypt 92). Sie ist das Hauptthema dieses Abschnitts.

   (b) Differenzielle Kryptoanalyse (Murphy, Shamir, Biham 1990 – bei IBM und NSA schon 1974 bekannt). Sie wird im Anschluss daran kurz erläutert.

   (c) Verallgemeinerungen und Mischformen, s. u.

Im Gegensatz zur differenziellen Kryptoanalyse war die lineare Kryptoanalyse den DES-Entwicklern wahrscheinlich nicht bekannt; demgemäß ist DES gegen sie nicht optimal resistent. Es gab nur das Design-Kriterium

- Die S-Boxen sollen so nichtlinear wie möglich sein.

Aber Shamir bemerkte schon früh (Crypto 85), dass es „lineare Approximationen“ für die S-Boxen gibt, deren Übereinstimmung besser als zufällig ist. Es dauerte allerdings weitere 8 Jahre, bis es Matsui gelang, diese Beobachtung systematisch auszunutzen.

Darüber hinaus sind in den letzten Jahren verschiedene Verallgemeinerungen und Kombinationen von linearer und differenzieller Kryptoanalyse entwickelt worden:

- Angriff mit verwandten Schlüsseln – ‘related keys’ (Biham 1992, Schneier).

- Differenziale höherer Ordnung (Harpes 1993, Biham 1994, Lai 1994).

- Differenziell-lineare Kryptoanalyse (Langford/Hellman 1994).

- Partielle Differenziale (Knudsen 1995).

- I/O-Summen-Analyse (Harpes/Kramer/Massey 1995).

- S-Box-Paar-Analyse (Davies/Murphy 1995, Mirza 1996).
- Bumerang-Angriff (Wagner 1999).
- Slide-Attacken auf (evtl. versteckte) Periodizität in Chiffren oder Schlüsselauswahl-Schemata (Biryukov/Wagner 1999).
- Unmögliche Differenziale (Biham/Biryukov/Shamir 1999).

Alle diese Verfahren einschließlich der linearen und der differenziellen Kryptoanalyse sind allerdings kaum konkret zum Brechen einer Chiffre im Sinne der klassischen Kryptoanalyse anwendbar. Sie setzen so viele bekannte Klartexte voraus, wie man in realistischen Situationen kaum je erhalten kann. Ihr Sinn liegt aber vor allem darin, sinnvolle Maße für die Sicherheit von Bitblock-Chiffren zu gewinnen. Ein solches Sicherheitsmaß ist z. B. die Anzahl bekannter Klartextblöcke, die man für einen Angriff benötigt. Chiffren, die selbst unter unrealistischen Annahmen über die Kenntnisse des Angreifers sicher sind, können als in der Praxis besonders sicher gelten.

Hier zeigt sich die Kryptoanalyse in ihrem „legalen“ Aspekt – sie dient nicht zu kriminellen Ausspähaktionen, sondern ist ein wichtiges Werkzeug für die Konstruktion starker Chiffren.

Bei Feistel- oder ähnlichen iterierten Chiffren startet man die Angriffe bei den nichtlinearen Bestandteilen der einzelnen Runden – die wie bei LUCIFER und DES meist S-Boxen genannt werden – und versucht, den Angriff über mehrere Runden auszudehnen. Dabei sieht man oft, wie die Schwierigkeit des Angriffs mit der Rundenzahl zunimmt. So erhält man Kriterien, ab wievielen Runden eine Chiffre „sicher“ ist.

Man darf dabei nicht vergessen, dass sich der Angriff immer auf eine bestimmte algebraische Struktur bezieht; hier auf die $\mathbb{F}_2$-Vektorraumstruktur des Klartextblock-Raums. Selbstverständlich kann man ähnliche Angriffsversuche auch auf andere Strukturen ansetzen; eine Abbildung, die komplex aussieht, könnte z. B. plötzlich einfach aussehen, wenn man ihre Wirkung auf die Struktur als zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ untersucht – oder gar auf „exotische“ Strukturen, die extra zur Untersuchung dieser einen Abbildung eingeführt werden. Wir beschränken uns hier exemplarisch auf die $\mathbb{F}_2$-Vektorraumstruktur, über die man am meisten weiß.

Kriterien für Bitblock-Chiffren

... bzw. deren Runden-Abbildungen oder deren nichtlineare Bausteine, die S-Boxen. [Sie werden zum großen Teil im mathematischen Einschub „Linearitätsmaße für BOOLEsche Abbildungen“ behandelt.]

- **Diffusion/Lawineneffekt:** Bei Änderung eines Klartextbits ändern sich ca. 50% der Geheimtextbits. Hierdurch sollen statistische Unregelmäßigkeiten vermieden werden.

- **Balanciertheit:** Alle Urbildmengen sind gleich groß, d. h., die Werte der Abbildung sind gleichmäßig verteilt. Unregelmäßigkeiten in der Verteilung würden einen Ansatz zur statistischen Kryptoanalyse bieten.

- **Algebraische Komplexität:** Die Bestimmung von Urbildern oder Teilen davon soll auf möglichst schwer lösbare Gleichungen führen. Diese Forderung hängt mit dem algebraischen Grad der Abbildung zusammen, aber nicht auf leicht zu beschreibende Weise.

- **Nichtlinearität:** Hier gibt es eine Reihe von Kriterien, die auch „versteckte“ Nichtlinearität messen und vergleichsweise leicht zu beschreiben und handzuhaben sind; sie zeigen u. a., wie anfällig die Abbildungen für lineare oder differenzielle Kryptoanalyse sind.

  - Das „lineare Potenzial“ soll möglichst gering, das „Linearitätsprofil“ möglichst ausgeglichen sein.
  - Das „differenzielle Potenzial“ soll möglichst gering, das „Differenzenprofil“ möglichst ausgeglichen sein.
  - Die „Nichtlinearität“, der Abstand (HAMMING-Distanz) zu affinen Abbildungen, soll möglichst groß sein.
  - Die „Linearitätsdistanz“, der Abstand zu Abbildungen mit „linearer Struktur“, soll möglichst groß sein.

Einige dieser Kriterien lassen sich gleichzeitig erfüllen, andere widersprechen sich teilweise, so dass das Design einer Bitblock-Chiffre insbesondere eine Abwägung der verschiedenen Kriterien erfordert; statt der Optimierung nach einem Kriterium ist ein möglichst gleichmäßig hohes Niveau bezüglich aller Kriterien anzustreben.

Zur Zeit wird grundsätzlich der Konflikt zwischen Balanciertheit und Nichtlinearität zu Gunsten der Balanciertheit entschieden. Dafür gibt es aber keinen wirklich stichhaltigen Grund; statistische Angriffe, die die Ungleichverteilung der Bilder bei nicht balancierten Abbildungen ausnutzen, sind einfach leichter zu begreifen und werden daher höher gewichtet. Die Abstriche bei der Nichtlinearität bekommt man durch Erhöhung der Rundenzahl in den Griff.

Die Bezeichnungen und Ergebnisse des Abschnitts „Linearitätsmaße für BOOLEsche Abbildungen“ werden im folgenden, oft ohne expliziten Hinweis, verwendet.

5.1 Die Idee der linearen Kryptoanalyse

Sei

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

eine Bitblock-Chiffre. Wir stellen uns die Argumente von F als Klartexte $a \in \mathbb{F}_2^n$ und Schlüssel $k \in \mathbb{F}_2^l$, die Werte von F als Geheimtexte $c \in \mathbb{F}_2^n$ vor. Dann kann man zu zwei Linearformen

$$\alpha\colon \mathbb{F}_2^n \times \mathbb{F}_2^l \longrightarrow \mathbb{F}_2, \quad \text{und} \quad \beta\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$$

die Wahrscheinlichkeit der linearen Relation (α, β) beziehungsweise ihr Potenzial betrachten:

$$\begin{aligned} p_F(\alpha,\beta) &= \frac{1}{2^{n+l}} \cdot \#\{(a,k,c) \in \mathbb{F}_2^n \times \mathbb{F}_2^l \times \mathbb{F}_2^n \mid c = F(a,k), \alpha(a,k) = \beta(c)\}, \\ \lambda_F(\alpha,\beta) &= (2p_F(\alpha,\beta) - 1)^2 = \frac{1}{2^{2n+2l}} \cdot \hat{\vartheta}_F(\alpha,\beta)^2, \end{aligned}$$

wobei in der Notation nicht zwischen einer Linearform und dem zugehörigen Vektor unterschieden wird. Zerlegt man $\alpha(a,k)$ in die Summe $\alpha'(a) + \gamma(k)$ – und schreibt dann statt α' einfach in neuer Bedeutung α –, so kann man sagen, dass $p_F((\alpha,\gamma),\beta)$ die Wahrscheinlichkeit dafür angibt, dass bei bekanntem Klartext a die lineare Relation

$$\gamma(k) = \alpha(a) + \beta(c)$$

für die Schlüsselbits $k_{i_1}, \ldots, k_{i_r}$ gilt, wenn $I = (i_1, \ldots, i_r)$ die Indexmenge ist, die der Linearform γ entspricht. Dabei ist $\gamma(k) = k_{i_1} + \cdots + k_{i_r}$ ein einzelnes Bit, das die durch I definierte Summe einiger Bits des Schlüssels k darstellt. Das Potenzial $\lambda_F((\alpha,\gamma),\beta)$ misst die Abweichung der Wahrscheinlichkeit vom Wert $\frac{1}{2}$, denn eine Wahrscheinlichkeit $< \frac{1}{2}$ ist genauso gut wie eine $> \frac{1}{2}$: Sie sagt, dass die komplementäre Relation

$$\gamma(k) = \alpha(a) + \beta(c) + 1$$

überzufällig oft gilt.

Daraus leitet man folgendes Vorgehen für die Schätzung von $\gamma(k)$ ab (im Fall $p_F > \frac{1}{2}$, sonst komplementär):

1. **[Sammelphase]** Man sammelt N Klartext-Geheimtextpaare $(a_1, c_1), \ldots, (a_N, c_N)$.

2. **[Auszählung]** Man bestimmt die Anzahl

$$t := \#\{i = 1, \ldots, N \mid \alpha(a) + \beta(c) = 0\}.$$

3. **[Mehrheitsentscheidung]** aufgrund von t:

- Ist $t > \frac{N}{2}$, schätzt man $\gamma(k) = 0$.
- Ist $t = \frac{N}{2}$, „randomisiert“ man die Entscheidung, d. h., man entscheidet sich zufällig für 0 oder 1, jeweils mit Wahrscheinlichkeit $\frac{1}{2}$.
- Ist $t < \frac{N}{2}$, schätzt man $\gamma(k) = 1$.

Wenn man ein lineare Relation mit hinreichend hohem Potenzial erwischt hat, wird die Erfolgswahrscheinlichkeit dieses Verfahrens bei hinreichend großem N hinreichend gut sein.

Findet man mehrere solche lineare Relationen mit hinreichender Gewissheit, so hat man den Schlüsselraum auf einen Unter-Vektorraum eingeschränkt und kann über diesen eine Exhaustion versuchen. Das ist die Grundidee der linearen Kryptoanalyse – es gibt je nach dem konkreten Aufbau einer Chiffre verschiedene Varianten, wie in den folgenden Abschnitten deutlich wird.

Als theoretisches Ergebnis aus der Analyse einer Chiffre erhält man dadurch einen Zusammenhang zwischen der Menge von benötigtem Klartext und der Erfolgswahrscheinlichkeit oder auch der Dimension des übriggebliebenen Suchraums.

Damit das Verfahren anwendbar ist, sind folgende Fragen zu klären:

1. Wie findet man lineare Relationen von möglichst großem Potenzial?
2. Da Bitblock-Chiffren meistens aus vielen Runden zusammengestzt, sind, fragt man weiter:
   (a) Wie findet man bei einer iterierten Bitblock-Chiffre brauchbare lineare Relationen für die Rundenfunktion?
   (b) Wie setzt man diese über die Runden hinweg zu linearen Relationen für die ganze Chiffre zusammen, so dass Aussagen über Schlüsselbits resultieren?
   (c) Wie bestimmt man die Wahrscheinlichkeit einer zusammengesetzten linearen Relation für die ganze Chiffre aus der für die einzelnen Runden?
3. Wie hängt die Erfolgswahrscheinlichkeit von der Zahl N der bekannten Klartext-Blöcke ab?

Die Antwort auf die erste Frage und Teil (a) der zweiten heißt: Aus dem linearen Profil, also durch FOURIER-Analyse. Die anschließenden Teilfragen führen zur Untersuchung von „linearen Pfaden“ und „linearen Hüllen“ und der Kumulation von Wahrscheinlichkeiten.

Nun ist die FOURIER-Analyse zwar sehr effizient, wenn man den Aufwand (Zeit und Speicherplatz) als Funktion der Größe des Inputs betrachtet. Leider wächst diese Größe aber exponenziell mit der Dimension; daher wird die

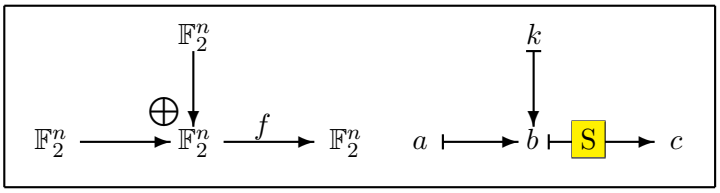
FOURIER-Analyse bei aller Effizienz schon bei Dimensionen von etwas über 10 undurchführbar; die für ernsthafte Blockchiffren relevanten Dimensionen, also Blockgrößen und Schlüssellängen von 64, besser aber 128 Bits, liegen weit darüber.

Dieser Einwand gilt auch für die erste Teilfrage von Frage 2. Da die einzelnen Runden aber meist wiederum im wesentlichen aus einer parallelen Abarbeitung kleinerer Stücke, der S-Boxen, bestehen, wird man versuchen, das Problem auf die Analyse der S-Boxen zurückzuspielen, und diese ist realistisch durchführbar; selbst das AES-Verfahren verwendet nur 8-dimensionale S-Boxen.

5.2 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

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

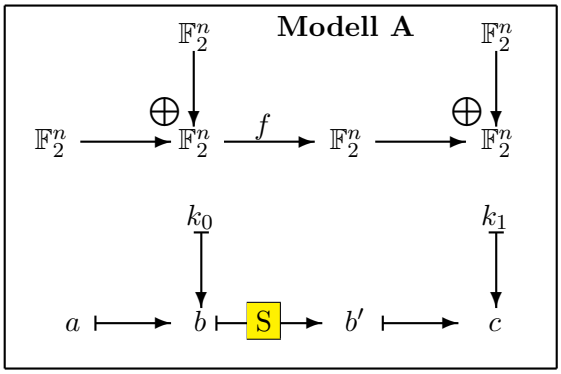


ist dabei witzlos, da bei bekanntem Klartext die Gleichung nach dem Schlüssel k auflösbar ist:

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

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

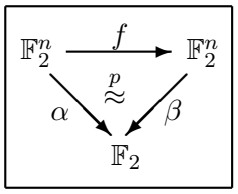
$$c = f(a + k_0) + k_1$$



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

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

wobei das Symbol $\overset{p}{\approx}$ gelesen wird als „ist gleich mit Wahrscheinlichkeit p“. Repräsentiert wird dies durch das Diagramm



Dann gilt

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

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

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

Sie gilt genau mit der Wahrscheinlichkeit $p = p_f(\alpha, \beta)$. Ein analoger Schluss lässt sich für die komplementäre 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 (Asymptotik) *Ist $p \approx \frac{1}{2}$, $N \ll 2^n$ und N nicht zu klein, so*

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

5.3 Die hypergeometrische Verteilung

Das Urnenmodell für die hypergeometrische Verteilung ist die „Ziehung ohne Zurücklegen“. Die Urne enthalte n Kugeln, davon s schwarze und $w = n - s$ weiße. Der Anteil

$$p := \frac{s}{n}$$

der schwarzen Kugeln sei bekannt und o. B. d. A. $p > \frac{1}{2}$. (Der Fall $p = \frac{1}{2}$ ist uninteressant, der Fall $p < \frac{1}{2}$ symmetrisch zum ersten.)

> In der Anwendung auf die lineare Kryptoanalyse werden die Kugeln alle möglichen Klartexte sein und die „Ziehung“ die Auswertung einer linearen Relation für einen bekannten Klartext.

Es werden r Kugeln zufällig gezogen ($r \leq n$). Die Wahrscheinlichkeit, dabei genau ν weiße Kugeln zu ziehen, ist

$$q_r^{(s)}(\nu) = \frac{\binom{s}{r-\nu}\binom{w}{\nu}}{\binom{n}{r}}.$$

Die Funktion

$$q_r^{(s)} \colon \mathbb{Z} \longrightarrow \mathbb{R}$$

heißt die **hypergeometrische Verteilung** (zu den Parametern n, s und r). Dabei ist $q_r^{(s)}(\nu) = 0$ für $\nu < 0$ und für $\nu > r$. Die Wahrscheinlichkeit, dass mehr schwarze als weiße Kugeln gezogen werden, ist

$$p_r^{(s)} = \begin{cases} \sum_{\nu=0}^{\frac{r-1}{2}} q_r^{(s)}(\nu), & \text{wenn } r \text{ ungerade,} \\ \sum_{\nu=0}^{\frac{r}{2}-1} q_r^{(s)}(\nu) + \frac{1}{2} q_r^{(s)}(\frac{r}{2}), & \text{wenn } r \text{ gerade,} \end{cases}$$

wenn im Falle des Gleichstands zufällig mit Wahrscheinlichkeit jeweils $\frac{1}{2}$ für schwarz oder weiß entschieden wird.

> Im uninteressanten Fall $p = \frac{1}{2}$ sind offensichtlich alle $p_r^{(s)} = \frac{1}{2}$.

Hilfssatz 1 *Es gilt:*
(i) $p_1^{(s)} = p$.
(ii) $p_2^{(s)} = p_1^{(s)}$ (falls $w \geq 1$).
(iii) $p_3^{(s)} = \frac{s(s-1)}{n(n-1)} \cdot \left[3 - 2 \cdot \frac{s-2}{n-2}\right]$ (falls $w \geq 2$).
(iv) $p_4^{(s)} = p_3^{(s)}$ (falls $w \geq 2$).
(v) $p_r^{(s)} = 1$ für $r > 2w$.

Beweis. (i) ist trivial.

(ii) Da bei jeweils einer weißen und schwarzen Kugel zufällig entschieden wird, ist der Zähler gleich

$$\binom{s}{2} + \frac{1}{2}\binom{s}{1}\binom{w}{1} = \frac{s(s-1)}{2} + \frac{s(n-s)}{2} = \frac{s(n-1)}{2},$$

der Nenner gleich $\frac{n(n-1)}{2}$, der Quotient

$$p_2^{(s)} = \frac{s(n-1)}{n(n-1)} = p.$$

(iii) Hier ist der Zähler

$$\begin{aligned}\binom{s}{3} + \binom{s}{2} \cdot (n-s) &= \frac{s(s-1)(s-2) + 3s(s-1)(n-s)}{6} \\ &= \frac{s(s-1)}{6} \cdot [s-2+3\cdot(n-s)] \\ &= \frac{s(s-1)}{6} \cdot [3\cdot(n-2) - 2\cdot(s-2)].\end{aligned}$$

Der Nenner ist $\frac{1}{6} \cdot n(n-1)(n-2)$, also hat $p_3^{(s)}$ den behaupteten Wert.

(iv) Die Rechnung wird weggelassen, da im nächsten Hilfssatz eine allgemeinere Aussage bewiesen wird.

(v) folgt, weil dann auf jeden Fall mehr schwarze Kugeln gezogen werden. ◇

Hilfssatz 2 *Ist r gerade und $2 \le r \le 2w$, so*

$$p_{r+1}^{(s)} > p_r^{(s)} = p_{r-1}^{(s)}.$$

Beweis. Sei $A_r^{(s)}(\nu) = \binom{n}{r} \cdot q_r^{(s)}(\nu)$ der Zähler von $q_r^{(s)}(\nu)$ und $B_r^{(s)} = \binom{n}{r} \cdot p_r^{(s)}$ der Zähler von $p_r^{(s)}$.

Beim Übergang von r nach $r+1$ wird die Mehrheitsentscheidung „schwarz“ nach $r+1$ Zügen in $B_{r+1}^{(s)}$ Fällen getroffen. Darunter sind:

- $\sum_{\nu=0}^{\frac{r}{2}-1} A_r^{(s)}(\nu)$ Fälle, in denen bereits nach r Zügen mindestens $\frac{r}{2}+1$ schwarze Kugeln gezogen worden waren. Für die $(r+1)$-te Kugel gibt es noch $n-r$ Möglichkeiten, die aber alle an der Entscheidung nichts ändern. Wir haben hier also

$$X_1 = (n-r) \cdot \sum_{\nu=0}^{\frac{r}{2}-1} A_r^{(s)}(\nu)$$

  Fälle, in denen „schwarz“ enschieden wird.

- $A_r^{(s)}(\frac{r}{2})$ Fälle, bei denen nach r Zügen genau $\frac{r}{2}$ schwarze Kugeln gezogen worden waren. Von den $n-r$ Möglichkeiten für die $(r+1)$-te Kugel sind
  - $s-\frac{r}{2}$ schwarz und führen zur Entscheidung „schwarz“,
  - $w-\frac{r}{2}$ weiß und führen zur Entscheidung „weiß“.

  Es kommen also
  $$X_2 = (s-\frac{r}{2}) \cdot A_r^{(s)}(\frac{r}{2})$$
  Fälle hinzu, in denen „schwarz“ enschieden wird.

- In den übrigen Fällen liegen nach r Zügen höchstens $\frac{r}{2}-1$ schwarze Kugeln vor, und die $(r+1)$-te Kugel kann somit die Entscheidung für „weiß“ nicht ändern.

Da von den gezählten Fällen jeweils $r+1$ dieselbe Menge von gezogenen Kugeln ergeben, ist

$$B_{r+1}^{(s)} = \frac{1}{r+1} \cdot (X_1 + X_2) = \frac{n-r}{r+1} \cdot \left[\sum_{\nu=0}^{\frac{r}{2}-1} A_r^{(s)}(\nu) + \frac{s-\frac{r}{2}}{n-r} \cdot A_r^{(s)}(\frac{r}{2}) \right].$$

Für den Koeffizienten des letzten Terms gilt

$$\frac{s-\frac{r}{2}}{n-r} > \frac{1}{2} \Longleftrightarrow 2s-r > n-r \Longleftrightarrow s > \frac{n}{2}.$$

(Da $r \leq 2w$, ist $r < n$.) Also folgt

$$B_{r+1}^{(s)} > \frac{n-r}{r+1} \cdot B_r^{(s)}$$

und somit der erste Teil der Behauptung.

Etwas komplizierter ist der Übergang von $r-1$ nach r. Die Entscheidung „schwarz“ wird nach r Zügen in $B_r^{(s)}$ Fällen getroffen. Darunter sind

- $\sum_{\nu=0}^{\frac{r}{2}-2} A_{r-1}^{(s)}$ Fälle, wo nach $r-1$ Zügen mindestens $\frac{r}{2}+1$ schwarze Kugeln gezogen worden waren. Die $n-r+1$ Möglichkeiten für die r-te Kugel ändern die Entscheidung nicht. Es gibt hier also
  $$Y_1 = (n-r+1) \cdot \sum_{\nu=0}^{\frac{r}{2}-2} A_{r-1}^{(s)}$$
  Fälle, in denen „schwarz“ entschieden wird.

- $A_{r-1}^{(s)}(\frac{r}{2}-1)$ Fälle, wo nach $r-1$ Zügen genau $\frac{r}{2}$ schwarze Kugeln gezogen worden waren. Die $n-r+1$ Möglichkeiten für die r-te Kugel zerfallen in

– $s - \frac{r}{2}$ schwarze, die zu der Entscheidung „schwarz“ führen; hier gibt es also

$$Y_2 = (s - \frac{r}{2}) \cdot A^{(s)}_{r-1}(\frac{r}{2} - 1)$$

zusätzliche Fälle.

– $w + 1 - \frac{r}{2}$ weiße, wo die Entscheidung mit jeweils der Wahrscheinlichkeit $\frac{1}{2}$ zufällig getroffen wird; es kommen also

$$Y_3 = \frac{1}{2} \cdot (w + 1 - \frac{r}{2}) \cdot A^{(s)}_{r-1}(\frac{r}{2} - 1)$$

Fälle hinzu.

- $A^{(s)}_{r-1}(\frac{r}{2})$ Fälle, wo nach $r - 1$ Zügen genau $\frac{r}{2} - 1$ schwarze Kugeln gezogen worden waren. Die $n - r + 1$ Möglichkeiten für die r-te Kugel zerfallen in

  – $s + 1 - \frac{r}{2}$ schwarze, wo die Entscheidung zufällig mit jeweils der Wahrscheinlichkeit $\frac{1}{2}$ getroffen wird – es kommen also

$$Y_4 = \frac{1}{2} \cdot (s + 1 - \frac{r}{2}) \cdot A^{(s)}_{r-1}(\frac{r}{2})$$

  Fälle hinzu –,

  – $w - \frac{r}{2}$ weiße, in denen die Entscheidung bei „weiß“ bleibt.

- In den übrigen Fällen, wo nach $r - 1$ Zügen höchstens $\frac{r}{2} - 2$ schwarze Kugeln gezogen worden waren, bleibt die Entscheidung ebenfalls bei „weiß“.

Da jeweils r der gezählten Fälle dieselbe Menge von gezogenen Kugeln ergeben, gilt

$$\begin{aligned} B^{(s)}_r &= \frac{1}{r} \cdot (Y_1 + Y_2 + Y_3 + Y_4) \\ &= \frac{n - r + 1}{r} \cdot \sum_{\nu=0}^{\frac{r}{2}-2} A^{(s)}_{r-1} + \frac{1}{r} \cdot (s - \frac{r}{2} + \frac{w}{2} + \frac{1}{2} - \frac{r}{4}) \cdot A^{(s)}_{r-1}(\frac{r}{2} - 1) \\ &\quad + \frac{1}{2r} \cdot (s - \frac{r}{2} + 1) \cdot A^{(s)}_{r-1}(\frac{r}{2}) \end{aligned}$$

Da $s + \frac{w}{2} = n - \frac{w}{2}$, ist der Koeffizient des mittleren Terms gleich

$$s - \frac{r}{2} + \frac{w}{2} - \frac{r}{4} + \frac{1}{2} = n - \frac{w}{2} - r + \frac{r}{4} + 1 - \frac{1}{2} = (n - r + 1) - \frac{1}{2} \cdot (w - \frac{r}{2} + 1).$$

Also ist

$$\begin{aligned} B^{(s)}_r &= \frac{n - r + 1}{r} \cdot \sum_{\nu=0}^{\frac{r}{2}-1} A^{(s)}_{r-1} \\ &\quad - \frac{1}{2r}(w - \frac{r}{2} + 1)\binom{s}{\frac{r}{2}}\binom{w}{\frac{r}{2} - 1} + \frac{1}{2r}(s - \frac{r}{2} + 1)\binom{s}{\frac{r}{2} - 1}\binom{w}{\frac{r}{2}}. \end{aligned}$$

Die beiden letzten Terme heben sich weg, und es bleibt

$$B_r^{(s)} = \frac{n-r+1}{r} \cdot B_{r-1}^{(s)}.$$

Daraus folgt der zweite Teil der Behauptung. $\diamond$

Damit ist insbesondere gezeigt:

Satz 3 *Die Wahrscheinlichkeit $p_r^{(s)}$ wächst mit r monoton von $p_1^{(s)} = p$ bis $p_{2w+1}^{(s)} = 1$.*

Wenn die Quotienten

$$\frac{rs}{n}, \frac{rw}{n}, \frac{(n-r)s}{n}, \frac{(n-r)w}{n}$$

hinreichend groß sind (FISHERs Faustregel sagt: ≥ 5 reicht), kann man die hypergeometrische Verteilung durch die Normalverteilung approximieren; das bedeutet insbesondere

$$\sum_{\nu=0}^{x} q_r^{(s)}(\nu) \approx \Phi(\frac{x-\mu}{\sigma}) = \frac{1}{\sqrt{2\pi}} \cdot \int_{-\infty}^{\frac{x-\mu}{\sigma}} e^{-t^2/2} dt,$$

wobei μ der Mittelwert und σ^2 die Varianz der hypergeometrischen Verteilung (zu den Parametern n, s und r) und Φ die Verteilungsfunktion der Normalverteilung ist. Für Mittelwert und Varianz gilt

Hilfssatz 3

$$\begin{aligned} \mu &= \frac{rw}{n}, \\ \sigma^2 &= \frac{r(n-r) \cdot w(n-w)}{n^2(n-1)}. \end{aligned}$$

Beweis. Bei einer zufälligen Stichprobenziehung von r Kugeln der Reihe nach sei $X_k \colon \Omega \longrightarrow \mathbb{R}$ eine Zufallsvariable, die 0 ist, wenn die k-te Kugel schwarz ist, und 1, wenn sie weiß ist. Dann ist $S = X_1 + \cdots + X_r : \Omega \longrightarrow \mathbb{R}$ eine Zufallsvariable, die die Anzahl der weißen Kugeln in der Stichprobenziehung angibt. Es ist $\mu = \mathrm{E}(S)$ der Erwartungswert und $\sigma^2 = \mathrm{Var}(S)$ die Varianz dieser Zufallsvariablen.

Klar ist $\mathrm{E}(X_k) = \frac{w}{n}$ also $\mathrm{E}(S) = r \cdot \frac{w}{n}$.

Für die Berechnung der Varianz bemerken wir zuerst, dass $X_k^2 = X_k$, also

$$\mathrm{Var}(X_k) = \mathrm{E}(X_k^2) - \mathrm{E}(X_k)^2 = \frac{w}{n} - \frac{w^2}{n^2} = \frac{w(n-w)}{n^2}.$$

Da $X_j X_k(\omega) = 1 \iff X_j(\omega) = 1$ *und* $X_k(\omega) = 1$, ist die Wahrscheinlichkeit dafür $\frac{w(w-1)}{n(n-1)}$, der Erwartungswert also $\mathrm{E}(X_j X_k) = \frac{w(w-1)}{n(n-1)}$. Daher ist die Covarianz

$$\begin{aligned}\mathrm{Cov}(X_j, X_k) &= \mathrm{E}(X_j X_k) - \mathrm{E}(X_j)\mathrm{E}(X_k) = \frac{w(w-1)}{n(n-1)} - \frac{w^2}{n^2} \\ &= \frac{w(n(w-1) - w(n-1))}{n^2(n-1)} = \frac{w(w-n)}{n^2(n-1)}.\end{aligned}$$

Die Varianz von S ist also

$$\begin{aligned}\mathrm{Var}(S) &= \sum_{k=1}^{r} \mathrm{Var}(X_k) + 2 \cdot \sum_{1 \le j < k \le r} \mathrm{Cov}(X_j, X_k) \\ &= \frac{rw(n-w)}{n^2} + r(r-1) \cdot \frac{w(w-n)}{n^2(n-1)} = \frac{rw(n-w)}{n^2} \cdot \left[1 - \frac{r-1}{n-1}\right] \\ &= \frac{rw(n-w)}{n^2(n-1)} \cdot [n-r],\end{aligned}$$

wie behauptet. $\diamond$

Satz 4 (Asymptotische Verteilung) *Die Wahrscheinlichkeit, mehr schwarze Kugeln zu ziehen, ist*

$$p_r^{(s)} \approx \frac{1}{\sqrt{2\pi}} \cdot \int_{-\infty}^{\sqrt{r\lambda}} e^{-t^2/2} dt$$

mit $\lambda = (2p-1)^2$*, wenn* $p \approx \frac{1}{2}$*,* $r \ll n$ *und* r *nicht zu klein.*

[Nach FISHERs Faustregel reicht $10 \le r \le n - 10$ für $p \approx \frac{1}{2}$.]
Beweis. Die obere Grenze des Integrals ist für $x = \frac{r}{2}$ zu berechnen:

$$\begin{aligned}\frac{x-\mu}{\sigma} &= \frac{(\frac{r}{2} - \frac{rw}{n}) \cdot n \cdot \sqrt{n-1}}{\sqrt{r(n-r)w(n-w)}} = \frac{(rn - 2rw)\sqrt{n-1}}{2 \cdot \sqrt{r(n-r)w(n-w)}} \\ &= \frac{\sqrt{r}\sqrt{n-1}}{\sqrt{n-r}} \cdot \frac{s-w}{2\sqrt{sw}} = \frac{\sqrt{n-1}}{\sqrt{n-r}} \cdot \sqrt{r} \cdot \frac{2p-1}{2\sqrt{p(1-p)}} \\ &\approx 1 \cdot \sqrt{r} \cdot \frac{2p-1}{2 \cdot \sqrt{\frac{1}{4}}} = \sqrt{r\lambda},\end{aligned}$$

wie behauptet. $\diamond$

5.4 Die Erfolgswahrscheinlichkeit

Die Überlegung aus Abschnitt 5.2 sieht im allgemeinen Rahmen von Abschnitt 5.1 genauso aus und liefert eine zufriedenstellende Antwort auf die dortige Frage 2:

Hauptsatz 1 (Formel von MATSUI**)** *Sei (α, β) eine lineare Relation mit Wahrscheinlichkeit $p = p_F(\alpha, \beta)$ und Potenzial $\lambda = \lambda_F(\alpha, \beta)$ für die Bitblock-Chiffre $F : \mathbb{F}_2^n \times \mathbb{F}_2^l \longrightarrow \mathbb{F}_2^n$. Dann ist die Erfolgswahrscheinlichkeit $P_{\alpha\beta N}$ der linearen Kryptoanalyse mit N bekannten Klartexten gerade die kumulierte Wahrscheinlichkeit $p_N^{(s)}$ der hypergeometrischen Verteilung zu den Parametern 2^n, $s = 2^n \cdot \max\{p, 1-p\}$ und N. Ist $p \approx \frac{1}{2}$, $N \ll 2^n$ und N nicht zu klein, so*

$$P_{\alpha\beta N} \approx \frac{1}{\sqrt{2\pi}} \cdot \int_{-\infty}^{\sqrt{N\lambda}} e^{-t^2/2} dt.$$

Für die exakte Verteilung haben wir die Bedingung

$$p_{\alpha\beta N} = 1, \quad \text{wenn } N > 2^{n+1}(1 - p_1).$$

Diese nützt für $p \approx \frac{1}{2}$ nichts – der Aufwand für die lineare Kryptoanalyse ist genauso groß wie der für die Exhaustion. Verzichtet man aber auf die hundertprozentige Gewissheit, so ergibt die Näherungsformel zusammen mit den bekannten Regeln für die Normalverteilung die Tabelle

$N\lambda$	1	2	3	4	...	8	9
$P_{\alpha\beta N}$	84.1%	92.1%	95.8%	97.7%	...	99.8%	99.9%

D. h., um eine Erfolgswahrscheinlichkeit von 97.7% zu erreichen, braucht man $N \approx \frac{4}{\lambda}$ bekannte Klartexte.

Zahlenbeispiel für DES: Das höchste Potenzial einer linearen Relation ist $\lambda \approx (3 \cdot 2^{-24})^2$ (siehe später), die entsprechende Wahrscheinlichkeit $p \approx \frac{1}{2} - 3 \cdot 2^{-25}$. Für eine Erfolgswahrscheinlichkeit von 97.7% benötigt man also

$$N \approx \frac{4}{\lambda} \approx \frac{4 \cdot 2^{48}}{3^2} \approx 2^{47}$$

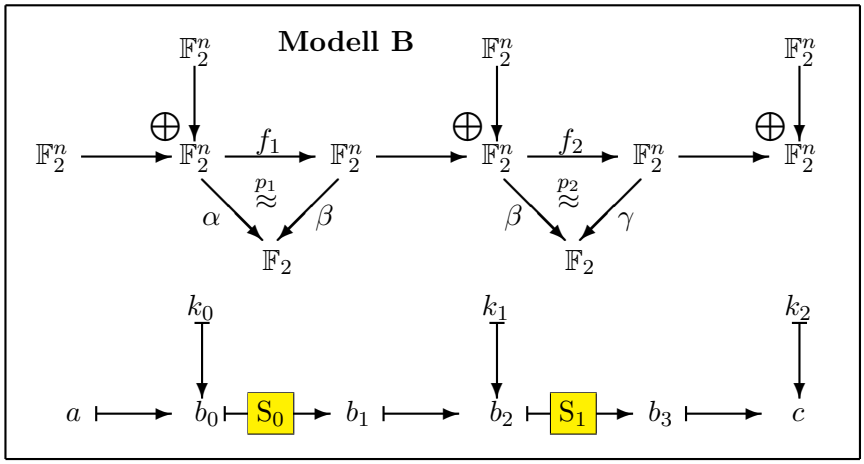
bekannte Klartexte. Damit hat man dann *ein* Schlüsselbit mit hoher Wahrscheinlichkeit bestimmt.

> Leichte Verbesserungen: Mit einer linearen Relation für die Runden 2 bis 15 und einer vollständigen Suche über die relevanten Schlüsselbits der Runden 1 und 16 konnte MATSUI die Anzahl der benötigten Klartexte auf 2^{43} drücken; durch gleichzeitiges Betrachten mehrerer linearer Relationen konnte er ferner die Anzahl der gewonnenen Schlüsselbits auf 14 erhöhen. Es bleibt die vollständige Suche nach den übrigen 42 Schlüsselbits, die auf einem PC nur noch wenige Sekunden dauert.

Dies ist der effizienteste bekannte Angriff auf das DES-Verfahren; die Anzahl der benötigten Klartexte ist allerdings immer noch so groß, daß dieser Angriff kaum als realistische Gefahr eingestuft werden kann. Dennoch offenbart er eine leichte Schwäche, die beim Design des DES übersehen wurde. Die Stabilität des DES gegen differenzielle Kryptoanalyse ist deutlich besser; diese Angriffsmöglichkeit war ja, wie heute bekannt ist, beim Design berücksichtigt worden.

5.5 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 5.2 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 5.2 – 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 $\lambda = \frac{1}{4}$.

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 $p' = \frac{3}{4}$.

5.6 Binäre Summen binärer Zufallsvariablen

Satz 5 („Piling Up Lemma“) *Sei Ω ein Wahrscheinlichkeitsraum und*

$$X_1, \ldots, X_r : \Omega \longrightarrow \mathbb{F}_2$$

unabhängige Zufallsvariablen mit $p_i := P(X_i = 0) = P(X_i^{-1}(0))$. Sei $X = X_1 + \cdots + X_r$ (binäre Summe in $\mathbb{F}_2$) und $p := P(X = 0)$. Sei $\lambda_i = (2p_i - 1)^2$ für $i = 1, \ldots r$ und $\lambda = (2p - 1)^2$. Dann gilt $\lambda = \lambda_1 \cdots \lambda_r$.

Beweis. Es reicht, den Beweis für $r = 2$ zu führen. Für $\omega \in \Omega$ ist $X(\omega) = 0$ genau dann, wenn $X_1(\omega)$ und $X_2(\omega)$ *beide* 0 *oder beide* 1 sind. Also ist

$$\begin{aligned} p &= p_1p_2 + (1 - p_1)(1 - p_2) = 1 - p_1 - p_2 + 2p_1p_2, \\ 2p - 1 &= 4p_1p_2 - 2p_1 - 2p_2 + 1 = (2p_1 - 1)(2p_2 - 1), \\ \lambda &= \lambda_1\lambda_2, \end{aligned}$$

wie behauptet. $\diamond$

Für die Wahrscheinlichkeiten ist die Formel etwas komplizierter:

Korollar 1 *Mit den Bezeichnungen von Satz 5 gilt*

$$p = \frac{1}{2} + 2^{r-1} \cdot \prod_{i=1}^{r} (p_i - \frac{1}{2}).$$

Korollar 2 *Ist ein $p_i = \frac{1}{2}$, so $\lambda = 0$, $p = \frac{1}{2}$.*

Korollar 3 *Mit wachsendem r ist λ monoton fallend.*

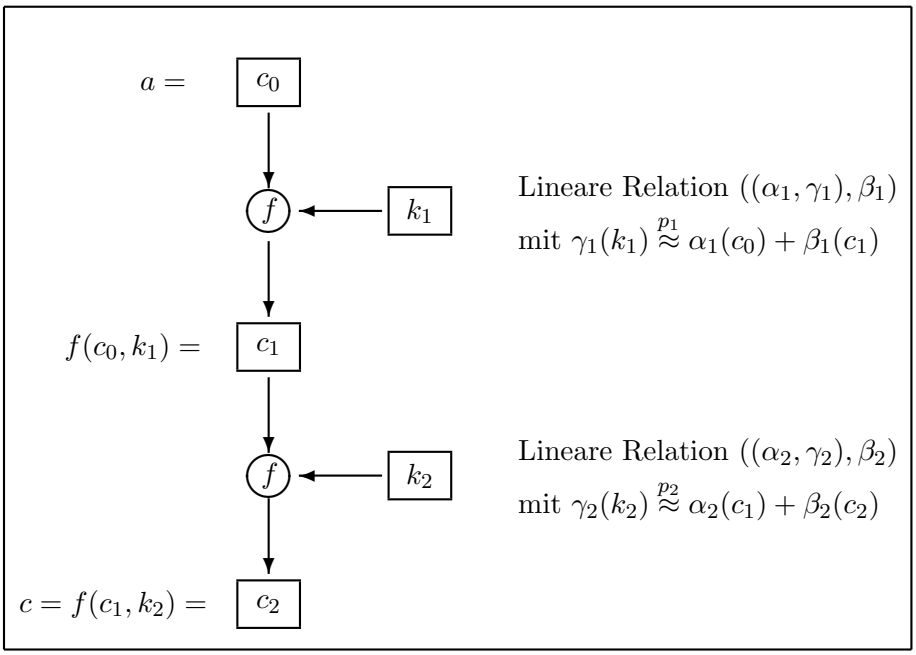
5.7 Lineare Pfade und lineare Hüllen

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 5.5 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 6 (Matsui) *Gegeben sei eine über r Runden iterierte Bitblock-Chiffre mit unabhängigen Rundenschlüsseln. Es sei eine lineare Relation für jede Runde gegeben, die das Potenzial $\lambda_1, \ldots, \lambda_r$ haben und zusammen einen linearen Pfad bilden. 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 5.4 genannte Ergebnis für DES zustande.

5.9 Die Idee der differenziellen Kryptoanalyse

Bei der differenziellen Kryptoanalyse wird analog zur linearen Kryptoanalyse die Approximation durch lineare Strukturen verwendet. Man betrachtet einen Differenzenvektor vor Anwendung einer Rundenabbildung und seine möglichen Werte nach Anwendung der Rundenabbildung. Zusammenpassende Folgen von Differenzenvektoren über die Runden einer iterierten Bitblock-Chiffre werden als **differenzieller Pfad** oder **Charakteristik** [Biham/Shamir 1990] bezeichnet; das Potenzial eines differenziellen Pfades ist nach Definition das Produkt der Potenziale der einzelnen Schritte. Eine **differenzielle Hülle** oder ein **Differential** [Lai/Massey/Murphy 1991] ist die Menge aller Pfade von einer gegebenen Input-Differenz der gesamten Chiffre zu einer gegebenen Output-Differenz. Es gilt eine analoge Faustregel, auf der die Methode der differenziellen Kryptoanalyse beruht:

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

Dieses Potenzial wiederum ergibt die Wahrscheinlichkeit, mit der eine Gleichung für Schlüsselbits hergeleitet werden kann.