## 2.5 FEISTEL-Chiffren

### Die Kernabbildung

Die Blockgröße $n = 2s$ wird als gerade vorausgesetzt. Blöcke $a \in \mathbb{F}_2^n$ werden in ihre linke und rechte Hälfte zerlegt:

$$a = (L, R) \in \mathbb{F}_2^s \times \mathbb{F}_2^s$$

(groß geschrieben, um die Verwechslung mit der Dimension $l$ des Schlüsselraums zu vermeiden). Hierfür muss man sich auf eine Nummerierung der Bits in einem Block einigen:

- In der **natürlichen Nummerierung**, die auch hier meistens verwendet wird, steht das LSB (Least Significant Bit) immer rechts und trägt die Nummer 0, das MSB (Most Significant Bit) steht links und trägt die Nummer $n - 1$:

  $$b = (b_{n-1}, \ldots, b_0) \in \mathbb{F}_2^n.$$

  Dies entspricht der Darstellung natürlicher Zahlen im ganzzahligen Intervall $[0 \ldots 2^n[$ zur Basis 2:

  $$b_{n-1} \cdot 2^{n-1} + \cdots b_1 \cdot 2 + b_0 \in \mathbb{N}.$$

- In der **IBM-Nummerierung** stehen die Bits umgekehrt und werden von 1 bis $n$ nummeriert:

  $$a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n.$$

  Dies entspricht der üblichen Nummerierung der Komponenten von Vektoren eines Vektorraums. Manchmal wird auch 0 bis $n - 1$ nummeriert.

Eine FEISTEL-Chiffre beruht auf einer **Kernabbildung**

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

an die formal keine weiteren Anforderungen gestellt werden; insbesondere brauchen die $f(\bullet, k)$ nicht bijektiv zu sein.

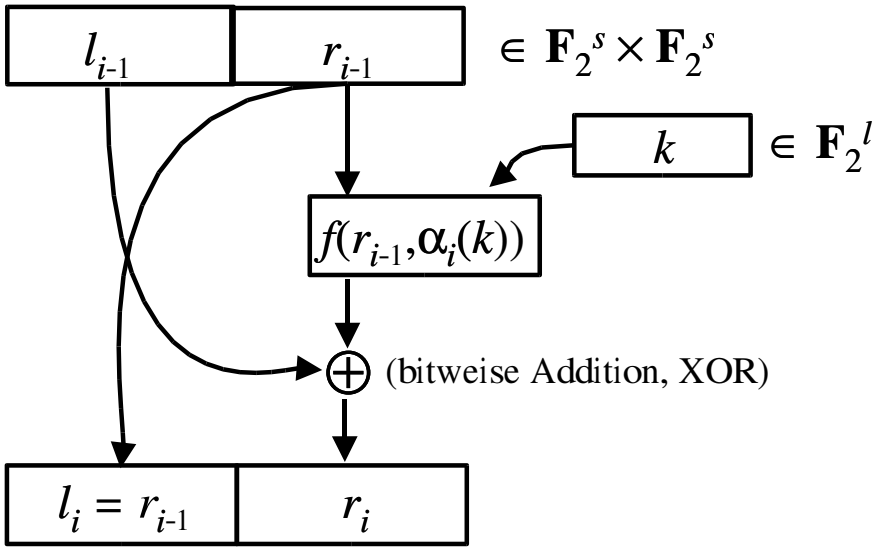
> Um ein brauchbares Verschlüsselungsverfahren zu erhalten, fordert man jedoch, dass $f$ möglichst gute Konfusion und Diffusion bietet, etwa bereits aus Substitutionen und Transpositionen zusammengesetzt und hochgradig nichtlinear ist.

**Beschreibung der Runden**

Eine FEISTEL-Chiffre besteht aus $r$ Runden, wobei jeweils aus dem Schlüssel $k \in \mathbb{F}_2^l$ ein $q$-Bit-Rundenschlüssel gebildet wird mit Hilfe der $i$-ten **Schlüsselauswahl**

$$\alpha_i \colon \mathbb{F}_2^l \longrightarrow \mathbb{F}_2^q \quad \text{für } i = 1, \ldots, r.$$

Die $i$-te Runde soll dann so aussehen:




Man erkennt in der Addition der linken Hälfte auf die transformierte rechte eine Spur des Autokey-Prinzips.

**Algorithmische Beschreibung**

Aus der graphischen Beschreibung leitet man leicht eine algorithmische ab:

| | | | | |
|---|---|---|---|---|
| **Input** | $\longrightarrow$ | $a$ | $=$ | $(a_0, a_1) \in \mathbb{F}_2^s \times \mathbb{F}_2^s$ |
| | | $a_2$ | $:=$ | $a_0 + f(a_1, \alpha_1(k))$ |
| | | | | – 1. Runde, Ergebnis $(a_1, a_2)$ |
| | | $\vdots$ | | $\vdots$ |
| | | $a_{i+1}$ | $:=$ | $a_{i-1} + f(a_i, \alpha_i(k))$ |
| | | | | – $i$-te Runde, Ergebnis $(a_i, a_{i+1})$ |
| | | | | – $[a_i = r_{i-1} = l_i,\ a_{i+1} = r_i]$ |
| | | $\vdots$ | | $\vdots$ |
| **Output** | $\longleftarrow$ | $c$ | $=$ | $(a_r, a_{r+1}) =: F(a, k)$ |

**Die Entschlüsselung**

Entschlüsselt wird nach der Formel

$$a_{i-1} = a_{i+1} + f(a_i, \alpha_i(k)) \quad \text{für } i = 1, \ldots, r.$$

Das entspricht dem gleichen Algorithmus, nur werden die Runden in umgekehrter Reihenfolge durchlaufen – mit anderen Worten: Die Schlüsselauswahl wird in umgekehrter Reihenfolge ausgeführt.

Insbesondere ist damit bewiesen:

**Satz 3 (**FEISTEL**)** *Sei* $F\colon \mathbb{F}_2^{2s} \times \mathbb{F}_2^l \longrightarrow \mathbb{F}_2^{2s}$ *die Blockabbildung zur Kernabbildung* $f : \mathbb{F}_2^s \times \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^s$ *und zur Schlüsselauswahl* $\alpha = (\alpha_1, \ldots, \alpha_r)$, $\alpha_i\colon \mathbb{F}_2^l \longrightarrow \mathbb{F}_2^q$.

*Dann ist die Verschlüsselungsfunktion* $F(\bullet, k) : \mathbb{F}_2^{2s} \longrightarrow \mathbb{F}_2^{2s}$ *für jeden Schlüssel* $k \in \mathbb{F}_2^l$ *bijektiv.*

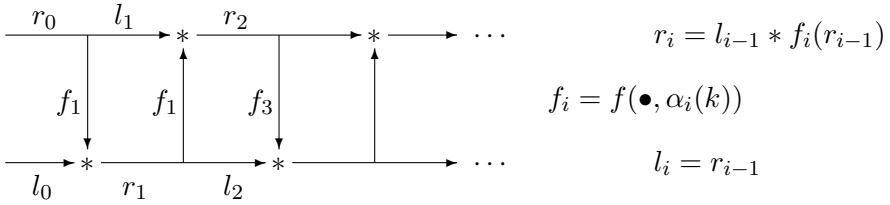
**Zusatz.** *Die Entschlüsselung ist die Blockabbildung zur gleichen Kernabbildung* $f$ *und zur umgekehrten Schlüsselauswahl* $(\alpha_r, \ldots, \alpha_1)$.

**Achtung:** Beginnt man die Entschlüsselung mit $c = (a_r, a_{r+1})$, so sind zuerst *die Seiten zu vertauschen*, denn der Algorithmus beginnt mit $(a_{r+1}, a_r)$. Daher wird bei der letzten Runde einer FEISTEL-Chiffre meist die Seitenvertauschung weggelassen.

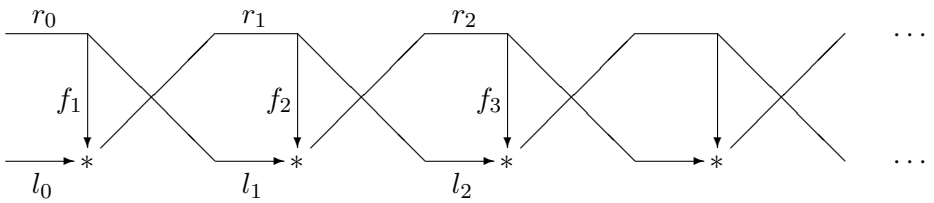
**Anmerkungen**

- Sind $f$ und die $\alpha_i$ linear, so auch $F$.
- Für die $\alpha_i$ nimmt man meist nur eine Bitauswahl, also eine Projektion $\mathbb{F}_2^l \longrightarrow \mathbb{F}_2^q$.
- Alternative graphische Beschreibungen:

**a) Leiter**




**b) Verdrehte Leiter**



**Verallgemeinerungen**

1. Die Gruppe $(\mathbb{F}_2^s, \oplus)$ wird durch eine beliebige Gruppe $(G, *)$ ersetzt. Die Formeln für Verschlüsselung und Entschlüsselung werden dann zu:

$$\begin{aligned} a_{i+1} &= a_{i-1} * f(a_i, \alpha_i(k))), \\ a_{i-1} &= a_{i+1} * f(a_i, \alpha_i(k)))^{-1}. \end{aligned}$$

2. Unbalancierte Feistel-Chiffren (Schneier/Kelsey): Hier werden die Blöcke in zwei ungleich große Hälften zerteilt: $\mathbb{F}_2^n = \mathbb{F}_2^s \times \mathbb{F}_2^t$, $x = (L(x), R(x))$. Die Formel für die Verschlüsselung wird dann zu:

$$\begin{aligned} l_i &= R(l_{i-1}, r_{i-1}) && \in \mathbb{F}_2^s, \\ r_i &= L(l_{i-1}, r_{i-1}) \oplus f(l_i, \alpha_i(k))) && \in \mathbb{F}_2^t. \end{aligned}$$

**Beispiele**

1. Lucifer II (von Feistel 1971 entwickelt, 1975 veröffentlicht),
2. DES (von Coppersmith u. a. bei der IBM 1974 entwickelt, 1977 als US-Norm veröffentlicht),
3. u. v. a. neuere Bitblock-Chiffren.

Die **Bedeutung** der Feistel-Netze liegt in den empirischen Beobachtungen:

- Die „$(s, q)$-Bit-Sicherheit“ der Kernfunktion $f$ wird durch die Mehrfach-Ausführung im Runden-Schema zu einer „$(n, l)$-Bit-Sicherheit“ der Feistel-Chiffre $F$ erweitert.
- Die gesamte Chiffre ist lässt sich aus handhabbaren, auf Sicherheit optimierbaren Stücken zusammensetzen.

Die erste dieser Beobachtungen lässt sich auch theoretisch untermauern: Nach einem Ergebnis von Luby/Rackoff ist eine Feistel-Chiffre mit mindestens vier Runden nicht mehr effizient von einer zufälligen Permutation zu unterscheiden, wenn die Kernfunktion zufällig ist. D. h., eine an sich gute, aber zu kurze zufällige Funktion wird durch diese Konstruktion zu einer ausreichend langen erweitert.