

2.4 SP-Netze

SHANNONS Konstruktionsprinzipien

Nach SHANNON sollen Blockchiffren folgendes leisten:

Diffusion (Durchmischung): Die Bits des Klartextblocks werden über den gesamten Block „verschmiert“. Quantitativ ausdrücken kann man das durch den „Lawinen-Effekt“ (englisch: avalanche effect):

- Jedes Bit des Geheimtextblocks hängt von jedem Bit des Klartextblocks ab.
- Bei Änderung eines Klartextbits ändern sich ca. 50% der Geheimtextbits.

Grundbausteine zur Erreichung von Diffusion sind Transpositionen.

Konfusion (Komplexität des Zusammenhangs): Die Beziehung zwischen Klartextblock und Geheimtextblock soll möglichst kompliziert sein (insbesondere hochgradig nichtlinear). Ähnlich komplex soll auch die Abhängigkeit des Geheimtextblocks vom Schlüssel sein, insbesondere sollen sich bei Änderung eines Schlüsselbits möglichst viele Geheimtextbits ändern, und zwar möglichst unvorhersagbar. Es soll für den Angreifer unmöglich sein zu erkennen, dass er einen Schlüssel „fast“ richtig geraten hat.

Grundbausteine hierfür sind vor allem Substitutionen.

Produktchiffren nach SHANNON

SHANNON schlug als Konstruktionsprinzip für starke Blockchiffren vor, Produktchiffren aus einer wechselnden Folge von Substitutionen und Transpositionen (= Permutationen) zu bilden – sogenannte **SP-Netze**. Im einfachsten Fall sieht das so aus:

$$\begin{array}{ccccccc} \mathbb{F}_2^n & \xrightarrow{S_1(\bullet, k)} & \mathbb{F}_2^n & \xrightarrow{P_1(\bullet, k)} & \mathbb{F}_2^n & \longrightarrow & \dots \\ & & & & \dots & \longrightarrow & \mathbb{F}_2^n \xrightarrow{S_r(\bullet, k)} \mathbb{F}_2^n \xrightarrow{P_r(\bullet, k)} \mathbb{F}_2^n \end{array}$$

abhängig von einem Schlüssel $k \in \mathbb{F}_2^l$. Dabei ist

$$\begin{aligned} S_i &= i\text{-te Substitution,} \\ P_i &= i\text{-te Permutation,} \\ P_i \circ S_i &= i\text{-te } \mathbf{Runde} - \end{aligned}$$

wobei insgesamt r Runden nacheinander ausgeführt werden.

Beispiel: LUCIFER I (FEISTEL 1973).