

## 2 Perfekte Sicherheit

**Definition 1.** Die Chiffre  $F$  heißt auf  $M_0$  **perfekt sicher**, wenn für alle Geheimtexte  $c \in \Sigma^*$  mit positiver Wahrscheinlichkeit  $P(c) > 0$  gilt:  $P(\bullet, c) = P$ .

**Deutung:** Die a-posteriori-Wahrscheinlichkeit  $P(a|c)$  unterscheidet sich nicht von der a-priori-Wahrscheinlichkeit  $P(a)$  eines Klartextes  $a \in M_0$ . Oder, anders ausgedrückt, der Kryptoanalytiker kann aus der Kenntnis des Geheimtextes keine zusätzliche Information über den Klartext gewinnen.

**Bezeichnungen.**

$$\begin{aligned} M_1 &:= \{a \in M_0 \mid P(a) > 0\} && \text{„mögliche Klartexte“}, \\ C_1 &:= \{c \in \Sigma^* \mid P(c) > 0\} && \text{„mögliche Geheimtexte“}. \end{aligned}$$

**Hilfssatz 1**  $\#M_1 \leq \#C_1$ .

*Beweis.* Sei  $l \in K$  ein fester Schlüssel mit  $P(l) > 0$ . Für einen Geheimtext  $c \in f_l(M_1)$ , etwa  $c = f_l(b)$ , gilt

$$P(c) = \sum_{a \in M_1} P(a) \cdot \sum_{k \in K_{ac}} P(k) \geq P(b) \cdot P(l) > 0.$$

Also ist  $c \in C_1$ . Es folgt  $f_l(M_1) \subseteq C_1$ , und da  $f_l$  injektiv ist,  $\#M_1 \leq \#C_1$ .  $\diamond$

**Hilfssatz 2** Ist  $F$  perfekt sicher, so  $K_{ac} \neq \emptyset$  für alle  $a \in M_1$  und alle  $c \in C_1$ .

*Beweis.* Wenn  $K_{ac} = \emptyset$ , ist

$$P(c|a) = \sum_{k \in K_{ac}} P(k) = 0.$$

also ist  $P(a|c) = 0 \neq P(a)$ , Widerspruch.  $\diamond$

Es kann also jeder mögliche Klartext in jeden möglichen Geheimtext verwandelt werden. Der nächste Hilfssatz sagt, dass es *sehr* viele Schlüssel geben muss.

**Hilfssatz 3** Ist  $F$  perfekt sicher, so  $\#K \geq \#C_1$ .

*Beweis.* Da  $\sum P(a) = 1$ , muss  $M_1 \neq \emptyset$  sein. Sei also  $a \in M_1$ . Wäre  $\#K < \#C_1$ , so gäbe es ein  $c \in C_1$  mit  $f_k(a) \neq c$  für alle Schlüssel  $k \in K$ , also  $K_{ac} = \emptyset$ , Widerspruch.  $\diamond$

**Satz 1** [SHANNON] *Sei  $F$  perfekt sicher. Dann ist*

$$\#K \geq \#M_1,$$

*d. h., es gibt mindestens so viele Schlüssel wie mögliche Klartexte.*

*Beweis.* Das folgt unmittelbar aus den Hilfssätzen 1 und 3.  $\diamond$

**Satz 2** [SHANNON] *Sei  $F$  eine Chiffre mit*

$$P(k) = \frac{1}{\#K} \quad \text{für alle } k \in K,$$

*d. h., alle Schlüssel sind gleich wahrscheinlich, und*

$$\#K_{ac} = s \quad \text{für alle } a \in M_1 \text{ und alle } c \in C_1.$$

*mit festem  $s \geq 1$ . Dann ist  $F$  perfekt sicher. Ferner ist  $\#K = s \cdot \#C_1$ .*

*Beweis.* Sei  $c \in C_1$  ein möglicher Geheimtext. Dann gilt für einen beliebigen möglichen Klartext  $a \in M_1$ :

$$\begin{aligned} P(c|a) &= \sum_{k \in K_{ac}} \frac{1}{\#K} = \frac{\#K_{ac}}{\#K} = \frac{s}{\#K}, \\ P(c) &= \sum_{a \in M_0} P(a) \cdot P(c|a) = \frac{s}{\#K} \cdot \sum_{a \in M_0} P(a) = \frac{s}{\#K} = P(c|a), \\ P(a|c) &= \frac{P(c|a)}{P(c)} \cdot P(a) = P(a). \end{aligned}$$

Also ist  $F$  perfekt sicher. Der Zusatz folgt, weil

$$K = \bigcup_{c \in C_1} K_{ac}$$

für jedes  $a \in M_1$ .  $\diamond$