1.1 Mehrfach-Chiffren und Gruppenstruktur

Mehrfach-Chiffren

Sei $F = (f_k)_{k\in K}$ eine Chiffre über dem Alphabet Σ, also $f_k\colon \Sigma^* \longrightarrow \Sigma^*$ die zugehörige Verschlüsselungsfunktion für jeden Schlüssel $k \in K$. Die gesamte Menge von Verschlüsselungsfunktionen wird mit

$$\tilde{F} = \{f_k \mid k \in K\} \subseteq \mathrm{Abb}(\Sigma^*, \Sigma^*)$$

bezeichnet.

Der Schlüsselraum wird wesentlich vergrößert, nämlich von K zu $K \times K$, durch die Bildung der **Zweifach-Chiffre**

$$F^{(2)} = (f_h \circ f_k)_{h,k\in K}$$

Natürlich kann man ebenso die Dreifach-Chiffre $F^{(3)}$, ..., die n-fach-Chiffre $F^{(n)}$ bilden. Sinnvoll ist das alles nur, wenn

(A) $\tilde{F}$ keine Halbgruppe ist.

Ist nämlich $\tilde{F}$ eine Halbgruppe, so gibt es zu zwei Schlüsseln $h, k \in K$ stets einen weiteren Schlüssel $x \in K$ mit $f_h \circ f_k = f_x$. Durch Komposition entstehen also keine neuen Verschlüsselungsfunktionen, sie ist eine „illusorische Komplikation“.

Noch besser ist, wenn

(B) $\tilde{F}$ eine möglichst große Unter-Halbgruppe von $\mathrm{Abb}(\Sigma^*, \Sigma^*)$ erzeugt.

Und das beste, was man hier erreichen kann, ist:

(C) Die Abbildung $K \times K \longrightarrow \widetilde{F^{(2)}} \subseteq \mathrm{Abb}(\Sigma^*, \Sigma^*)$ ist injektiv;

das kann man für einen endlichen Schlüsselraum K auch so ausdrücken:

(C') $\#\widetilde{F^{(2)}} = \#\{f_h \circ f_k \mid h, k \in K\} = (\#K)^2$.

Die Gruppen-Eigenschaft von Blockchiffren

Eine Blockchiffre ist durch die Wirkung auf einem Σ^r (für einen gegebenen Exponenten r) eindeutig festgelegt. (Um die Details der Fortsetzung auf Zeichenketten beliebiger Länge und des Auffüllens oder „Padding“ von zu kurzen Ketten auf Blocklänge kümmern wir uns im Moment nicht.)

Eine Blockchiffre heißt **längentreu**, wenn sie Σ^r in sich abbildet. Insbesondere ist dann $\tilde{F}$ auf natürliche Weise Teilmenge der symmetrischen Gruppe $\mathcal{S}(\Sigma^r)$, also endlich, und man kann den Schlüsselraum K ohne Einschränkung als endlich annehmen. Für solche Blockchiffren ist die Halbgruppen-Eigenschaft (also die Negation von (A) oben) zur Gruppen-Eigenschaft äquivalent. Das folgt aus dem bekannten einfachen:

Hilfssatz 1 *Sei G eine endliche Gruppe, $H \leq G$ eine Unter-Halbgruppe, d. h., $H \neq \emptyset$ und $HH \subseteq H$. Dann ist H Gruppe, insbesondere $\mathbf{1} \in H$.*

Beweis. Jedes $g \in G$ hat endliche Ordnung, $g^m = \mathbf{1}$. Ist nun $g \in H$, so $\mathbf{1} = g^m \in H$ und $g^{-1} = g^{m-1} \in H$. $\diamond$

Daher ist bewiesen:

Satz 1 *Sei F eine längentreue Blockchiffre über einem endlichen Alphabet. Dann sind folgende Aussagen äquivalent:*

(i) *Zu je zwei Schlüsseln $h, k \in K$ gibt es $x \in K$ mit $f_h \circ f_k = f_x$.*

(ii) *Die Menge $\tilde{F}$ der Verschlüsselungsfunktionen ist eine Gruppe.*

Anmerkung

Die Wahrscheinlichkeit, dass zwei zufällige Elemente der symmetrischen Gruppe $\mathcal{S}_n$ bereits die ganze Gruppe $\mathcal{S}_n$ oder wenigstens die alternierende Gruppe $\mathcal{A}_n$ erzeugen, ist

$$> 1 - \frac{2}{(\ln \ln n)^2} \quad \text{für große } n.$$

Für $n = 2^{64}$, einen typischen Wert bei Blockchiffren, ist diese untere Schranke ≈ 0.86. Eine nicht ganz ungeschickt gewählte Blockchiffre wird also sehr wahrscheinlich die volle oder wenigstens halbe Permutationsgruppe auf den Blöcken erzeugen. Trotzdem ist der konkrete Nachweis davon oft schwer. Jedenfalls kann man davon ausgehen, dass eine Mehrfach-Chiffre „in der Regel“ stärker als die Einfach-Chiffre ist.

Quelle: John Dixon, *The probability of generating the symmetric group.* Mathematische Zeitschrift 110 (1969), 199–205.