7.8 Kryptographische Basisfunktionen

Damit haben wir auch die theoretische Grundlage, um Einwegfunktionen und starke symmetrische Chiffren exakt zu definieren:

Definition 5. Gegeben sei $f : L \longrightarrow \mathbb{F}_2^*$ wie in (2). Eine Rechtsinverse zu f ist eine Abbildung $g : f(L) \longrightarrow L \subseteq \mathbb{F}_2^*$ mit $f(g(y)) = y$ für alle $y \in f(L)$ – d. h., g findet Urbilder für f. f heißt **Einwegfunktion**, wenn jede Rechtinverse von f hart ist.

Nach dieser Definition ist die diskrete Exponentialfunktion in endlichen Primkörpern (bei entsprechender Interpretation) vermutlich Einwegfunktion.

Zur Definition einer starken Chiffre sehen wir uns erst nochmal eine „gewöhnliche“ Blockchiffre

$$F \colon \mathbb{F}_2^r \times \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^r$$

an. Die zugehörige Entschlüsselungsfunktion ist ein

$$G \colon \mathbb{F}_2^r \times \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^r$$

mit $G(F(x,k),k) = x$ für alle $x \in F_2^r$ und $k \in F_2^q$.

Ein Angriff mit bekanntem Klartext findet zu gegebenen $x, y \in \mathbb{F}_2^r$ einen passenden Schlüssel $k \in F_2^q$ mit $F(x,k) = y$. Formalisieren lässt sich das als Abbildung

$$H \colon \mathbb{F}_2^r \times \mathbb{F}_2^r \longrightarrow \mathbb{F}_2^q$$

mit $F(x, H(x,y)) = y$ für alle $x, y \in \mathbb{F}_2^r$ mit $y \in F(x, \mathbb{F}_2^q)$ („mögliche Paare“ (x,y)).

Allgemeiner benutzt ein solcher Angriff ja mehrere bekannte Klartextblöcke, sagen wir s Stück. Er verwendet also eine Abbildung

$$H \colon \mathbb{F}_2^{rs} \times \mathbb{F}_2^{rs} \longrightarrow \mathbb{F}_2^q$$

mit $F(x_i, H(x_i, y_i)) = y_i$ für $i = 1, \ldots s$ für alle möglichen Paare $x, y \in \mathbb{F}_2^{rs}$.

Übungsaufgabe. Formuliere, was ein mögliches Paar ist.

Daraus soll jetzt die komplexitätstheoretische Definition abgeleitet werden.

Definition 6. Eine **symmetrische Chiffre** ist eine Familie $F = (F_n)_{n \in \mathbb{N}}$ von Blockchiffren

$$F_n \colon \mathbb{F}_2^{r(n)} \times \mathbb{F}_2^{q(n)} \longrightarrow \mathbb{F}_2^{r(n)}$$

mit streng monoton wachsenden r und q, so dass $F_n(\bullet, k)$ für jedes $k \in \mathbb{F}_2^{q(n)}$ bijektiv ist und

- F effizient berechenbar ist und
- es eine effizient berechenbare Familie $G = (G_n)_{n\in\mathbb{N}}$ von zugehörigen Entschlüsselungsfunktionen gibt.

Definition 7. Ein **Angriff** auf eine symmetrische Chiffre F **mit bekanntem Klartext** ist eine Familie $H = (H_n)_{n\in\mathbb{N}}$ von Abbildungen

$$H_n \colon \mathbb{F}_2^{r(n)s(n)} \times \mathbb{F}_2^{r(n)s(n)} \longrightarrow \mathbb{F}_2^{q(n)}$$

mit

$$F_n(x_i, H_n(x_i, y_i)) = y_i \quad \text{für } i = 1, \ldots, s(n)$$

für alle möglichen $x, y \in \mathbb{F}_2^{r(n)s(n)}$.

F heißt **starke symmetrische Chiffre**, wenn jeder Angriff auf F mit bekanntem Klartext hart ist.

Die Definition einer Hash-Funktion ist etwas kniffliger und wird hier nicht ausgeführt.