7.8 Kryptographische Basisfunktionen

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

Definition 4. 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 vermutlich Einwegfunktion.

Definition 5. Sei $f : L \longrightarrow \mathbb{F}_2^*$ eine Zusammensetzung von Abbildungen

$$f_n : \mathbb{F}_2^{r(n)} \times \mathbb{F}_2^{q(n)} \longrightarrow \mathbb{F}_2^{r(n)}$$

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 sowie $(y, k) \mapsto f_n(\bullet, k)^{-1}(y)$ jeweils effizient berechenbar sind. Ein Angriff auf f mit bekanntem Klartext ist eine Abbildung g, zusammengesetzt aus Teilen

$$g_n : \mathbb{F}_2^{r(n)} \times \mathbb{F}_2^{r(n)} \longrightarrow \mathbb{F}_2^{q(n)}$$

mit

$$f_n(x, g_n(x, y)) = y \quad \text{für alle } x, y \in \mathbb{F}_2^{r(n)}.$$

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.