6.3 Umwandlungstricks

Die Äquivalenz der folgenden Aussagen (A) bis (D) und ihre Implikation von (E) wird plausibel hergeleitet; für einen richtigen mathematischen Beweis fehlen ja noch die exakten Definitionen. Die Implikationen haben durchaus auch praktische Bedeutung für die Konstruktion von Basisfunktionen aus anderen. Diese kann man stark vereinfacht in Hinblick auf die immer wieder aufkommende politische Debatte über eine Kryptographie-Regulierung so zusammenfassen:

- Wer Kryptographie verbieten will, muss auch Hash-Funktionen und Pseudozufallsgeneratoren verbieten.
- Wer Kryptographie unmöglich machen will, muss $\mathbf{P} = \mathbf{NP}$ beweisen.

(A) Es gibt eine Einweg-Funktion $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$.

($\tilde{\mathbf{A}}$) Es gibt eine Einweg-Funktion $\tilde{f}\colon \mathbb{F}_2^{2n} \longrightarrow \mathbb{F}_2^n$.

(B) Es gibt eine schwache Hash-Funktion $h\colon \mathbb{F}_2^* \longrightarrow \mathbb{F}_2^n$.

(C) Es gibt eine starke symmetrische Chiffre $F\colon \mathbb{F}_2^n \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ (d. h. eine, die sicher vor einem Angriff mit bekanntem Klartext ist).

(D) Es gibt einen perfekten Zufallsgenerator $\sigma\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^{p(n)}$.

(E) $\mathbf{P} \neq \mathbf{NP}$.

Anmerkung 1: Bei der komplexitätstheoretischen Präzisierung steht in den Aussagen (A) – (D) stets eine mit n parametrisierte Familie von Funktionen.

Anmerkung 2: Die Perfektheit des Zufallsgenerators besagt, dass bei unbekanntem Urbild $x \in \mathbb{F}_2^n$ aus einigen bekannten Bits des Bildes $\sigma(x)$ keine weiteren Bits effizient bestimmt werden können; insbesondere auch nicht das Urbild x. In der Definition ist p ein ganzzahliges Polynom, das „Streckungspolynom“ – aus einem Startvektor der Länge n werden $p(n)$ Bits erzeugt.

Die Implikation „(D) $\Longrightarrow$ (E)“ wird hier nicht bewiesen.

„(C) $\Longrightarrow$ (D)“: Man setzt $\sigma(x) = (s_1, \ldots, s_{p(n)/n})$ mit $s_0 := x$ und $s_i := F(s_{i-1}, z)$ für $i \geq 1$, wobei als Schlüssel z ein geheim gehaltener konstanter Parameter verwendet wird; man erkennt den OFB-Modus für Bitblock-Chiffren wieder. Dann kann aus jedem Block s_i der Folge der Vorgängerblock s_{i-1} nicht bestimmt werden – sonst wäre die Chiffre nicht sicher. – Dass das schon für die Perfektheit reicht, wird in Kapitel IV gezeigt.

„(D) $\Longrightarrow$ (C)“: Die Bitstrom-Chiffre mit $\sigma(x)$ als Bitstrom zum Schlüssel x ist sicher.

„(A) $\Longrightarrow$ (C)“: Am einfachsten ist der Ansatz von E. Backus; dabei wird $F(a,k) = f(a) + f(k)$ gesetzt. Bei einem Angriff mit bekanntem Klartext sind a und $c = F(a,k)$ bekannt; damit ist auch $f(k) = c + f(a)$ bekannt. Der Angriff ist also auf die Umkehrung von f reduziert. [Andere Ansätze sind MDC (= Message Digest Cryptography) von P. Gutmann und das Feistel-Prinzip.]

„(C) $\Longrightarrow$ (A)“: Das war als Beispiel in Abschnitt 6.1 vorgestellt worden.

„(A) $\Longrightarrow$ ($\tilde{\text{A}}$)“: Sei $\tilde{f}$ durch $\tilde{f}(x,y) := f(x+y)$ definiert. Ist dann zu c ein Urbild (x,y) unter $\tilde{f}$ bestimmbar, so hat man auch das Urbild $x+y$ unter f bestimmt.

„($\tilde{\text{A}}$) $\Longrightarrow$ (B)“: $x \in \mathbb{F}_2^*$ wird mit (höchstens $n-1$) Nullen zu $(x_1, \ldots, x_r) \in (\mathbb{F}_2^n)^r$ aufgefüllt. Dann setzt man

$$\begin{aligned} c_0 &:= 0, \\ c_i &:= \tilde{f}(c_{i-1}, x_i) \quad \text{für } 1 \le i \le r, \\ h(x) &:= c_r. \end{aligned}$$

Damit ist $h\colon \mathbb{F}_2^* \longrightarrow \mathbb{F}_2^n$ definiert. Findet man nun zu gegebenem $y \in \mathbb{F}_2^n$ ein Urbild $x \in (\mathbb{F}_2^n)^r$ mit $h(x) = y$, so auch ein $z \in (\mathbb{F}_2^n)^2$ mit $\tilde{f}(z) = y$, nämlich $z = (c_{r-1}, x_r)$ (wobei $y = c_r$ in der Konstruktion von h).

„(B) $\Longrightarrow$ (A)“: Die Einschränkung von h auf $\mathbb{F}_2^n$ ist auch Einweg-Funktion.