

6.1 Einweg-Funktionen

Es wird weiterhin die informelle Definition aus 4.1 verwendet. Eine exakte Definition wird in 7.5 nachgereicht.

Anwendung: Einweg-Funktionen können direkt zur Einweg-Verschlüsselung verwendet werden. Das bedeutet:

- *Jeder* kann verschlüsseln.
- *Niemand* kann entschlüsseln.

Wozu soll das gut sein, wenn niemand entschlüsseln kann? Dafür gibt es durchaus eine Reihe von Anwendungen (die z. T. den Spezialfall der Hash-Funktionen, siehe 6.2, einsetzen):

- Die Passwort-Verwaltung, z. B. unter Unix oder MS-Windows. Hier soll niemand das verschlüsselt abgespeicherte Passwort ermitteln können, wohl aber muss das Betriebssystem die Möglichkeit haben, das neu eingebene Passwort nach Verschlüsselung mit dem verschlüsselt abgelegten zu vergleichen.
- Ähnlich sieht die Anwendung bei Pseudonymisierung aus: Die Daten eines Falls sollen mit anderswo abgelegten Daten zusammengeführt werden, ohne dass jemand die zum Fall gehörenden Identitätsdaten sehen oder ermitteln kann.
- Eine weitere Anwendung betrifft die digitale Signatur, siehe 6.2.
- Schliesslich ist auch der entscheidende Aspekt der asymmetrischen Verschlüsselung, dass niemand den privaten Schlüssel aus dem öffentlichen ableiten kann. Hierzu sind allerdings Einweg-Funktionen nicht ohne weiteres direkt einsetzbar, wie schon das Beispiel der ELGAMAL-Chiffre in 4.5 gezeigt hat.

Beispiele für mutmaßliche Einweg-Funktionen:

1. Die diskrete Exponential-Funktion, siehe 4.1.
2. Eine Standard-Methode, aus einer Bitblock-Chiffre

$$F: M \times K \longrightarrow C,$$

die resistent gegen einen Angriff mit bekanntem Klartext ist, eine Einweg-Funktion $f: K \longrightarrow C$ abzuleiten, geht so:

$$f(x) := F(m_0, x);$$

es wird also ein fester Klartext m_0 – etwa der Bitblock, der aus lauter Nullen besteht – mit einem Schlüssel, der genau aus dem

Einweg-umzuwandelnden Block x besteht, verschlüsselt. Die Umkehrung dieser Einweg-Funktion würde genau dem Angriff mit bekanntem Klartext m_0 auf die Chiffre F entsprechen.

3. Sei $n \in \mathbb{N}$ ein zusammengesetzter Modul. Wir wissen aus 5.2, dass zumindest im Fall, dass n aus zwei großen ungeraden Primzahlen zusammengesetzt ist, das Ziehen der Quadratwurzel mod n nicht effizient möglich ist. Damit ist die Quadratabbildung $x \mapsto x^2 \bmod n$ im Restklassenring $\mathbb{Z}/n\mathbb{Z}$ eine Einweg-Funktion – immer unter der Annahme, dass die Faktorisierung nicht effizient möglich ist. Allerdings ist die Umkehrung möglich, wenn eine Zusatzinformation vorliegt, nämlich die Primfaktoren von n . Eine solche Zusatzinformation heißt ‘trapdoor’ (Falltür), und man spricht dann auch von einer ‘Trapdoor-Einweg-Funktion’.
4. Das gleiche gilt für die RSA-Funktion $x \mapsto x^e \bmod n$ mit einem zu $\lambda(n)$ (oder $\varphi(n)$) teilerfremden Exponenten e .