# VII.4 Parametrisierte Hashfunktionen (MACs)

- Hashfunktionen liefern Integrität, aber nicht Authentizität.
- Vertraulichkeit liefert nicht notwendig Authentizität.
- Benötigen neben Verschlüsselungsverfahren und Hashfunktionen weitere Technik.
- Parametrisierte Hashfunktionen als Erweiterung von Hashfunktionen.
- Heißen auch Authentifizierungscodes, engl. message authentication codes (MACs)

# Message authentication codes (MACs)

**Definition 7.4** Ein Authentifizierungscode oder parametrisierte Hashfunktion ist eine Familie $\{h_k : k \in K\}$ von Hashfunktionen $h_k : \Sigma^* \to \Sigma^n$, wobei $\Sigma$ und K endliche Mengen sind.
(auch message authentication code (MAC))

Ein Authentifizierungscode für Nachrichten fester Länge oder parametrisierte Kompressionsfunktion ist eine Familie $\{h_k : k \in K\}$ von Kompressionsfunktionen $h_k : \Sigma^m \to \Sigma^n$, wobei $\Sigma$ und K endliche Mengen und $n,m \in \mathbb{N}$ mit $m > n$ sind.

# Beispiele

**Beispiel 1** Sei $h:\{0,1\}^* \to \{0,1\}^n$ eine Hashfunktion.

Setze $K := \{0,1\}^n$ und für $k \in \{0,1\}^n$ definiere

$$\begin{array}{lccc} h_k: & \{0,1\}^* & \to & \{0,1\}^n \\ & x & \mapsto & h(x) \oplus k \end{array}$$

# Beispiele

**Beispiel 2 (CBC-MAC)** $(P,C,K,E,D)$ Blockchiffre mit

$P = C = K = \{0,1\}^n$, $b \in \mathbb{N}$ fest.

parametrisierte Kompressionsfunktion $\{h_k : k \in K\}$

$h_k : \{0,1\}^{b \cdot n} \to \{0,1\}^n$

**Definition** $h_k(x), x = x_1 \cdots x_{b,} x_j \in \{0,1\}^n$

$$
\begin{aligned}
z_0 &:= 0^n \\
z_i &:= E_k(z_{i-1} \oplus x_i), i = 1,\ldots,b \\
h_k(x) &:= z_b
\end{aligned}
$$

# Beispiele

## Beispiel 3 (MAC aus Schwammfunktion)

$\mathrm{sponge} : \{0,1\}^* \to \{0,1\}^l$ Schwammfunktion mit Blocklänge r

$K = \{0,1\}^r$ und für $k \in \{0,1\}^r$

$$\begin{aligned} \mathrm{sponge}_k : \quad \{0,1\}^* &\to \{0,1\}^l \\ x &\mapsto \mathrm{sponge}(k \,\|\, x) \end{aligned}$$

# Anwendung parametrisierter Hashfunktionen

- Authentisierung der Kommunikation zwischen Prüfungs-sekretariat und Lehrenden.
- Nutzen parametrisierte Hashfunktion $\{h_k : k \in K\}$.
- Jeder Lehrende L erhält geheimen Schlüssel $k_L \in K$ vom PSek zugeteilt.
- Bei Übermittlung einer Nachricht m mit Noten einer Prüfung sendet L zusätzlich $h_{k_L}(m)$.
- Bei erhalt von Notenübermittlung (m,t) von L akzeptiert PSek die Noten in m dann und nur dann, wenn $t = h_{k_L}(m)$.

# Fälschungssichere MACs

**Fälschungssicherheit** Eine parametrisierte Hashfunktion $\{h_k : k \in K\}$ heißt fälschungssicher, wenn es für keinen Angreifer mit vertretbarem Aufwand möglich ist zu unbekanntem $k \in K$ ein Paar $(x, h_k(x))$ zu erzeugen.

Dies muss auch noch gelten, wenn der Angreifer verschiedene Paare $(x_j, h_k(x_j)), j = 1, \ldots, l,$ kennt, und er ein Paar $(x, h_k(x))$ mit $x \neq x_{j,} j = 1, \ldots, l,$ zu erzeugen versucht.

# Zwei allgemeine Konstruktionen

## Hash-then-MAC

$\{h_k : k \in K\}$ parametrisierte Kompressionsfunktion,

$h_k : \{0,1\}^m \to \{0,1\}^n, k \in K$

Hashfunktion $h : \{0,1\}^* \to \{0,1\}^m$

parametrisierte Hashfunktion $\{H_k : k \in K\}$

$$\begin{array}{rccc} H_k: & \{0,1\}^* & \to & \{0,1\}^n \\ & x & \mapsto & h_k(h(x)) \end{array}$$

**Beispiel** Kombination CBC-MAC mit Hashfunktion.

# Zwei allgemeine Konstruktionen

## Hash-then-MAC

$\{h_k : k \in K\}$ parametrisierte Kompressionsfunktion,

$h_k : \{0,1\}^m \to \{0,1\}^n, k \in K$

Hashfunktion $h : \{0,1\}^* \to \{0,1\}^m$

parametrisierte Hashfunktion $\{H_k : k \in K\}$

$$\begin{aligned} H_k : \quad \{0,1\}^* &\to \{0,1\}^n \\ x &\mapsto h_k(h(x)) \end{aligned}$$

**Eigenschaft** Ist h kollisionsresistent und ist $\{h_k : k \in K\}$ fäschungssicher, dann ist $\{H_k : k \in K\}$ fäschungssicher.

# Zwei allgemeine Konstruktionen

## HMAC

$\{h_k : k \in K\}$ parametrisierte Kompressionsfunktion, $K = \{0,1\}^l$

$h_k : \{0,1\}^{2l} \to \{0,1\}^l, k \in K$

$H_k : \{0,1\}^* \to \{0,1\}^l, k \in K,$ aus $h_k$ durch Merkle-Damgård

parametrisierte Hashfunktion $\left\{G_{(s,k)} : (s,k) \in \{0,1\}^l \times \{0,1\}^l\right\}$

$$G_{(s,k)} : \{0,1\}^* \to \{0,1\}^l$$

$$x \mapsto H_k\left(IV \| s \oplus opad \| H_k\left(IV \| s \oplus ipad \| x\right)\right),$$

$IV, opad, ipad \in \{0,1\}^l$ konstant.