Vorlesung Sicherheit

Dennis Hofheinz

ITI, KIT

05.05.2014

Überblick

Überblick

Erinnerung Hashfunktion

- Kurzer „Fingerabdruck“ großer Daten:

$$\mathrm{H} : \{0,1\}^* \to \{0,1\}^k$$

- Keine „Kollisionen“ ($X \neq X'$ mit $\mathrm{H}(X) = \mathrm{H}(X')$)
  - Problem: Kollisionen existieren zwangsläufig
  - Bestmöglich: Kollisionen schwer zu finden
- Für unsere Zwecke (kryptographische Hashfunktion):

Definition (Kollisionsresistenz, informell)

Eine Hashfunktion H ist *kollisionsresistent*, wenn jeder effiziente Algorithmus nur mit kleiner Wahrscheinlichkeit eine Kollision findet.

Überblick

Formalisierungen

- **Diskussion:** Wie könnte Formalisierung aussehen?
  - Was könnte ein „effizienter“ Algorithmus sein?
  - Was könnte eine „kleine“ Wahrscheinlichkeit sein?

Sicherheitsparameter

- *Asymptotische* Definition
- Idee: Sicherheitsparameter $k \in \mathbb{N}$ parametrisiert System
- Beispiel: $\mathrm{H} = \mathrm{H}_k$ mit $\mathrm{H}_k : \{0,1\}^* \to \{0,1\}^k$
- Intuition: größeres $k \Rightarrow$ mehr Sicherheit

Effizienz und kleine Wahrscheinlichkeiten

- Effizient: Polynomialzeit (in k), kurz: PPT
  - Beispiel: Algorithmus, der Kollision durch vollständige Suche aller $X \in \{0,1\}^{k+1}$ findet, ist nicht effizient
- Kleine Wahrscheinlichkeit: vernachlässigbar (in k)
  - $f : \mathbb{N} \to \mathbb{R}$ vernachlässigbar $:\Leftrightarrow |f|$ verschwindet asymptotisch schneller als Kehrwehrt jedes vorgegebenen Polynoms
  - Formal: f vernachlässigbar $:\Leftrightarrow \forall c \exists k_0 \forall k \geq k_0 : |f(k) \leq k^{-c}|$
  - Beispiel: $1/2^k$ vernachlässigbar, aber $1/k$ nicht
- Alternative (auch üblich, anwendungsnäher, unhandlicher): *konkrete* Sicherheit (Verfahren ist $(t(k), \varepsilon(k))$-sicher)

Kollisionsresistenz (formal)

Definition (Kollisionsresistenz)

Eine über k parametrisierte Funktion H ist *kollisionsresistent*, wenn jeder PPT-Algorithmus nur mit höchstens vernachlässigbarer Wahrscheinlichkeit eine Kollision findet.
Genauer: für jeden PPT-Algorithmus $\mathcal{A}$ ist

$$\mathrm{Adv}^{\mathrm{cr}}_{\mathrm{H},\mathcal{A}}(k) := \Pr\left[(X, X') \leftarrow \mathcal{A}(1^k) \ : \ X \neq X' \wedge \mathrm{H}_k(X) = \mathrm{H}_k(X')\right]$$

vernachlässigbar.

Einwegeigenschaft

- Weitere nützliche Eigenschaft von H: Einwegfunktion
  - Für Hashfunktionen auch „Preimage Resistance“ genannt
- Intuition: gegeben $\mathrm{H}(X)$, schwierig, X zu finden
- (Einwegfunktionen zentrales Konzept in Kryptographie)

Einwegeigenschaft

- Einwegfunktionen z.B. nützlich für Passwortabfragen
  1. Server speichert $\mathrm{H}(\texttt{pass})$ statt $\texttt{pass}$
  2. Benutzer gibt $\texttt{pass'}$ ein
  3. Server testet $\mathrm{H}(\texttt{pass}) \stackrel{?}{=} \mathrm{H}(\texttt{pass'})$

  - Kollisionsresistenz $\Rightarrow$ äquivalent zu $\texttt{pass} \stackrel{?}{=} \texttt{pass'}$
    (oder Benutzer/Angreifer findet Kollision)
  - Einwegeigenschaft $\Rightarrow$ Server findet $\texttt{pass}$ nicht heraus
  - Noch besser (vorgreifend): „gesalzene“ Passwörter
    - Server speichert $(R, \mathrm{H}(\texttt{pass}, R))$ für zufälliges R
    - Verschiedene Server können Passwörter nicht vergleichen

Einwegeigenschaft

- Intuition: gegeben $\mathrm{H}(X)$ ist es schwierig, X zu finden
- **Frage:** wie sollte $X \in \{0,1\}^*$ dabei verteilt sein?
  - Bei wenigen „Kandidaten“-X Raten möglich
  - Grundsätzlich möglich: $\Pr[X = X^*] > 0$ für alle $X^* \in \{0,1\}^*$
  - Aber: was sind „wahrscheinliche Urbilder“?
- Üblich, aber nicht immer realistisch für Anwendung:
  X gleichverteilt über endlicher Teilmenge

Einwegeigenschaft

Definition (Einwegfunktion)

Eine über k parametrisierte Funktion H ist eine *Einwegfunktion* bzgl. der Urbildverteilungen $\{\mathcal{X}_k\}_k$, wenn jeder PPT-Algorithmus nur mit höchstens vernachlässigbarer Wahrscheinlichkeit ein Urbild eines gegebenen, aus $\mathcal{X}_k$ gezogenen Bildes findet.
Genauer: für jeden PPT-Algorithmus $\mathcal{A}$ ist

$$\mathrm{Adv}^{\mathrm{ow}}_{\mathrm{H},\mathcal{A}}(k) := \Pr\left[X' \leftarrow \mathcal{A}(1^k, \mathrm{H}(X)) \ : \ \mathrm{H}(X) = \mathrm{H}(X')\right]$$

vernachlässigbar, wobei $X \leftarrow \mathcal{X}_k$ gewählt wurde.

- Bemerkung: $\mathcal{A}$ muss nicht notwendig $X' = X$ zurückgeben

Kollisionsresistenz und Einwegeigenschaft

Theorem (Kollisionsresistenz $\Rightarrow$ Einwegeigenschaft)

Jede kollisionsresistente Hashfunktion $\mathrm{H} : \{0,1\}^* \to \{0,1\}^k$ *ist eine Einwegfunktion bzgl. der Gleichverteilung auf* $\{0,1\}^{2k}$.

Beweis.

- Wir geben zu jedem H-Invertierer $\mathcal{A}$ einen H-Kollisionsfinder $\mathcal{B}$ an mit

$$\mathrm{Adv}^{\mathrm{cr}}_{\mathrm{H},\mathcal{B}}(k) \geq \frac{1}{2} \cdot \mathrm{Adv}^{\mathrm{ow}}_{\mathrm{H},\mathcal{A}}(k) - 1/2^{k+1}$$

- $\mathcal{B}$ wählt $X \leftarrow \{0,1\}^{2k}$ glv., setzt $X' \leftarrow \mathcal{A}(1^k, \mathrm{H}(X))$, gibt (X, X') aus
- Bei $\mathrm{H}(X) = \mathrm{H}(X')$ ist $X = X'$ mit Wahrscheinlichkeit $\leq 1/|\mathrm{H}^{-1}(\mathrm{H}(X))|$
- Mit Wahrscheinlichkeit $\geq 1 - 1/2^k$ hat $\mathrm{H}(X)$ mehr als ein Urbild
- Zusammengenommen hat $\mathcal{B}$ Erfolg $\geq 1/2 \cdot \mathrm{Adv}^{\mathrm{ow}}_{\mathrm{H},\mathcal{A}}(k) - 1/2^{k+1}$

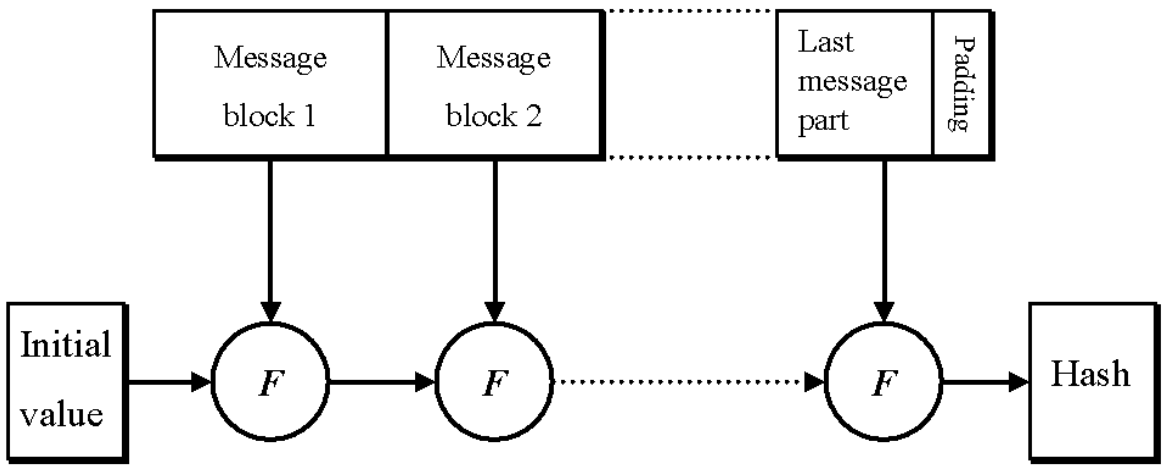
Weitere Sicherheitseigenschaften

- Weitere Sicherheitseigenschaft: Target Collision Resistance
  - Auch: Second Preimage Resistance, Universal One-Way
  - Informell: gegeben X, finde X' mit $\mathrm{H}(X) = \mathrm{H}(X')$
- Wird impliziert von Kollisionsresistenz
- Impliziert Einwegeigenschaft
- Beispielszenario: Sicherheit von Zertifikaten
  - Gegeben ein Zertifikat eines gehashten Public Keys ...
  - ... finde einen neuen Public Key, für den dieses Zertifikat gilt

Überblick

Merkle-Damgård-Konstruktion

- Ziel: Hashfunktion H_{MD} aus einfacherem Baustein bauen
- Baustein: Kompressionsfunktion $\mathrm{F} : \{0,1\}^{2k} \to \{0,1\}^{k}$
- Konstruktion:



Quelle: `rsa.com`

- **Wichtig:** Padding enthält Nachrichtenlänge

Sicherheit von Merkle-Damgård

Theorem

Ist F *kollisionsresistent, so ist auch* H_{MD} *kollisionsresistent.*

Beweis.

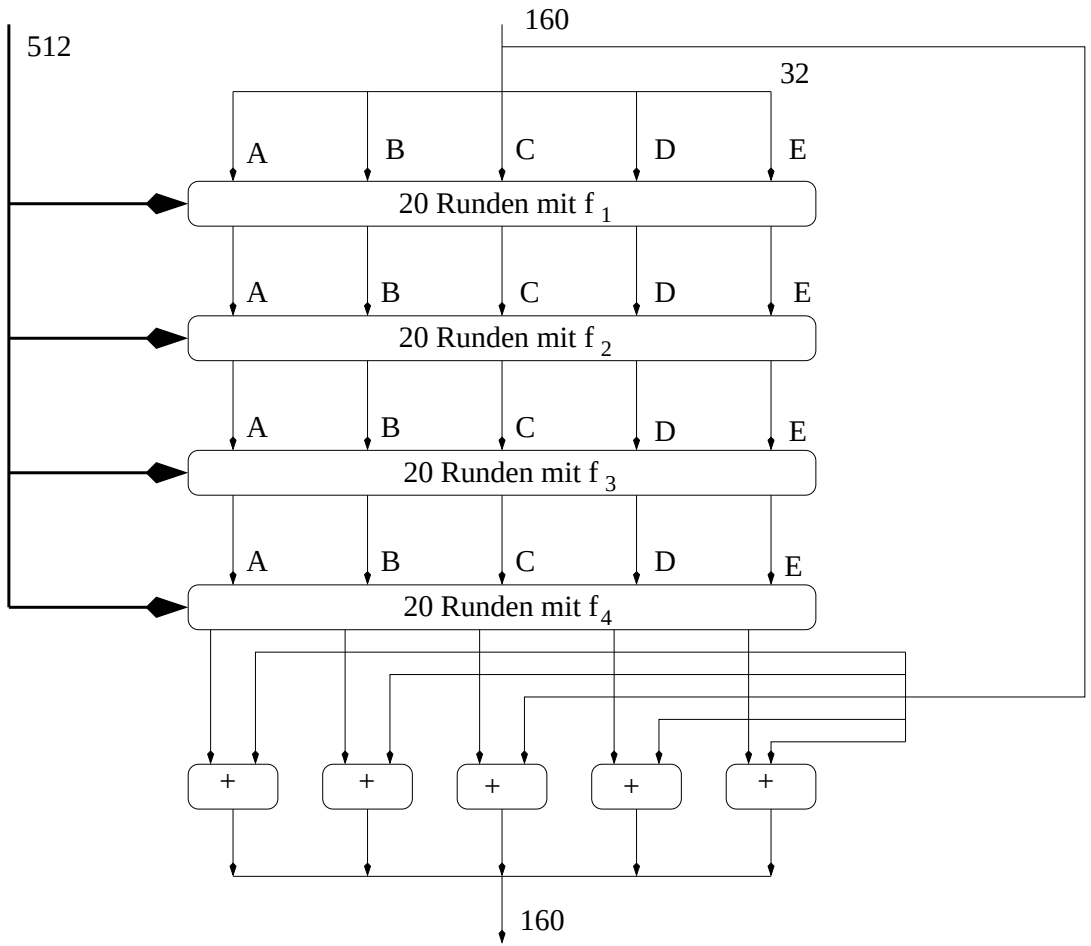
- Geg. $X \neq X'$ mit $\mathrm{H}_{\mathrm{MD}}(X) = \mathrm{H}_{\mathrm{MD}}(X')$, finde F-Kollision
- Schreibe $X = (X_i)_{i=1}^{n}, X' = (X'_i)_{i=1}^{n'}$ (mit $X_i, X'_i \in \{0,1\}^k$)
- MD-Zwischenwerte: $Z_0 := IV$, $Z_i := \mathrm{F}(Z_{i-1}, X_i)$ (Z'_i analog)
- Es ist $Z_n = \mathrm{F}(Z_{n-1}, X_n) = \mathrm{F}(Z'_{n'-1}, X'_{n'}) = Z'_{n'}$
- $Z_{n-1} \neq Z_{n'-1}$ oder $X_n \neq X'_{n'} \Rightarrow$ F-Kollision
- Andernfalls ist $X_n = X'_{n'}$ (und damit $n = n'$), und weiter
$$Z_{n-1} = \mathrm{F}(Z_{n-2}, X_{n-1}) = \mathrm{F}(Z'_{n'-2}, X'_{n'-1}) = Z'_{n'-1}$$
- ...wegen $X \neq X'$ kann nicht $Z_i = Z'_i \ \forall i$ sein $\Rightarrow$ F-Kollision

□

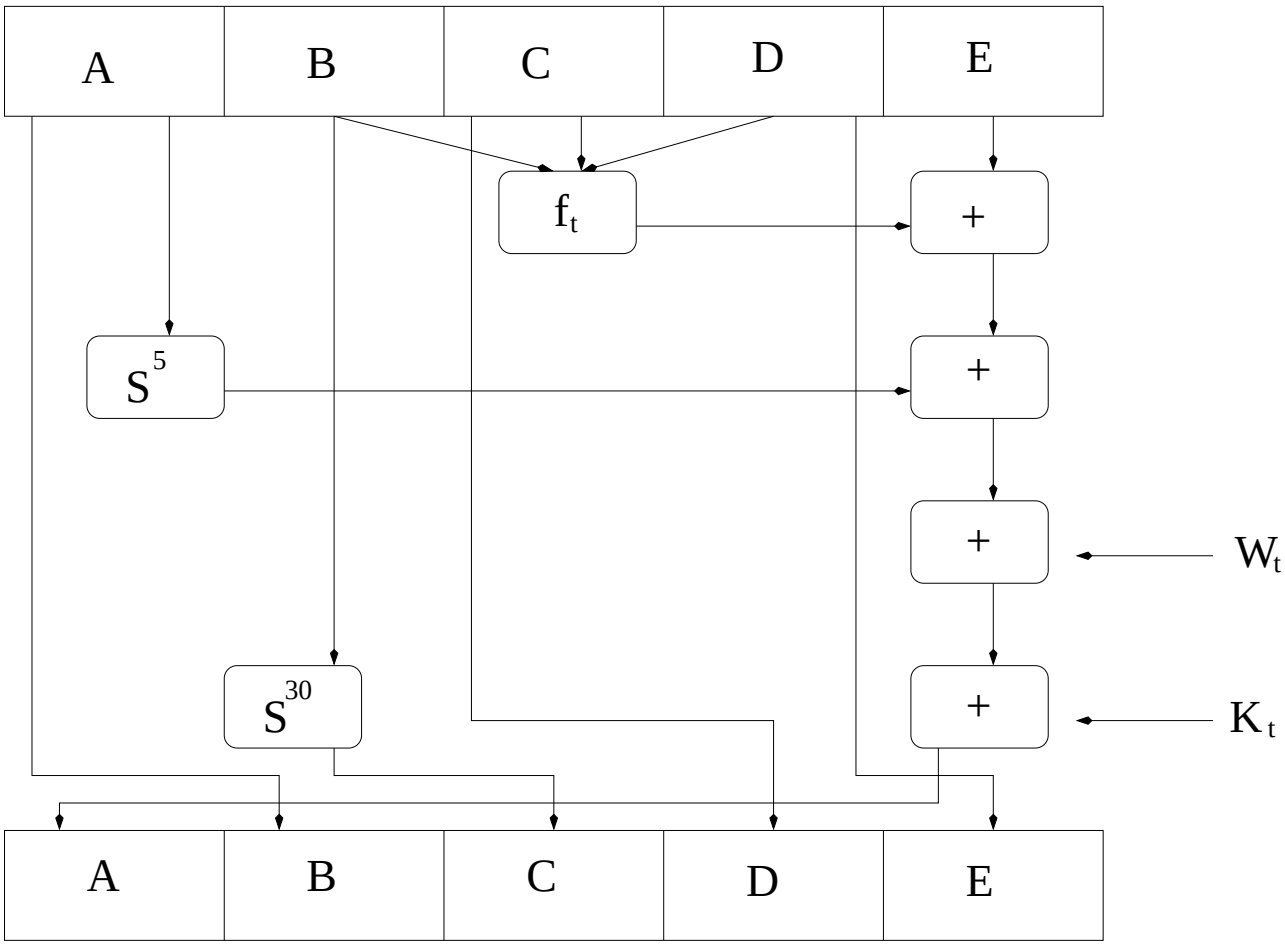
Bedeutung von Merkle-Damgård

- Mehrere (fast) aktuelle Hashfunktionen beeinflusst von MD
  - MD5 (vorgeschlagen 1992)
  - SHA-1 (vorgeschlagen 1995)
  - SHA-2 (vorgeschlagen 2001)
- MD5 und SHA-1 mittlerweile gebrochen
- Aktueller Hash-Standard SHA-3 („Keccak“) nutzt MD *nicht*

Beispiel: SHA-1 (Kompressionsfunktion)



Beispiel: SHA-1 (Rundenfunktion)



Angriffe auf SHA-1

- Kollisionen für eine Runde leicht zu finden
- Grundidee: erweitere Kollisionen auf mehrere Runden
- Auch „Fast-Kollisionen“ $(\mathrm{H}(X) \approx \mathrm{H}(X'))$ nützlich
- Bruch von SHA-1 2005:
  - zunächst theoretische 53-Runden-Kollision
  - danach theoretische (volle) 80-Runden-Kollision
- Allerdings Angriffe bislang theoretisch

  Aufwand etwa 2^{61} Schritte