Vorlesung am 30.04.2015

5 Hashfunktionen

Bildet Bitstrings beliebiger Länge auf Bitstrings fester Länge ab:
$H : \{0,1\}^* \longrightarrow \{0,1\}^n$

Wichtige kryptographische Primitive: Für Authentisierung, Signatur, DPRNG.

Verschiedene Eigenschaften hinsichtlich Sicherheit (abhängig vom Einsatz)

Einwegfunktion: H ist effizient berechenbar, Umkehrung aber nicht:

- Für alle $x \in \{0,1\}^*$ lässt sich $H(x)$ effizient berechnen
- Für alle $y \in \{0,1\}^n$ ist es schwer $m \in H^{-1}(y)$ zu finden.

Einsatz für: Anonymisierung von Daten, Schutz von Passwörtern

Schwache Kollisionsresitenz: Schwer, bestimmte Kollisionen zu finden:

- für alle $m \in \{0,1\}^*$ ein $m' \in \{0,1\}^* \backslash \{m\}$ mit $H(m) = H(m')$

Einsatz für: Integritätssicherung, z.B.
Hashwert einer Software wird auf Internetseite veröffentlicht

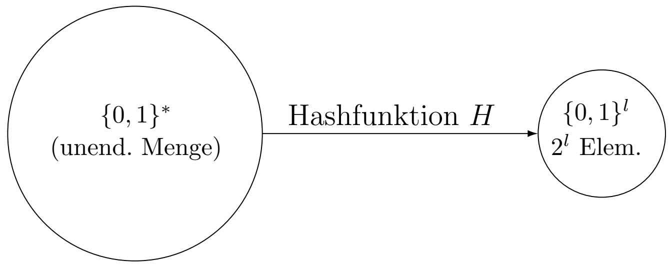
Starke Kollisionsresitenz: Schwer, allgemeine Kollisionen zu finden:

- $m, m' \in \{0,1\}^*$, $m \neq m'$ mit $H(m) = H(m')$

Zusammenhang aller drei Eigenschaften (Beweis in Vorlesung Kryptologie):

- Es gibt Einwegfunktionen, die nicht schwach kollisionsresistent sind
- Es gibt schwach kollisionsresistente, die nicht Einwegfunktionen sind
- Starkte Kollisionsresistenz ist Verallg. der Eigenschaften 1 und 2, d.h.
  - Stark kollisionsresistente Funktion sind Einwegfunktionen
  - Stark kollisionsresistente Funktion sind schwach kollisionsresistent

Hashfunktionen können nicht kollisionsfrei sein:



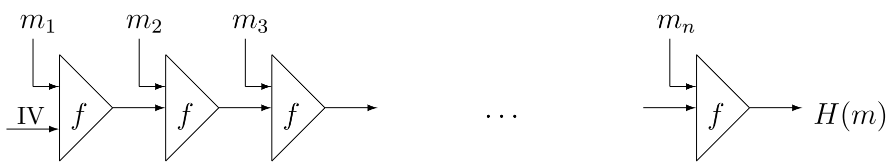
- Unendliche Menge kann nicht injektiv auf endliche Menge abbilden
- Es gibt also Kollisionen (sogar unendlich viele)

Schwer (praktisch unmöglich): Sicherheitsniveau 100 Bit:
Angreifer benötigt ca. 2^{100} Versuche, Eigenschaft zu brechen

Konstruktion nach Merkle-Damgård: Gegeben Kompressionsfunktion

$$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n.$$

Hashfunktion basierend auf f:



Kompressionsfunktion muss alle für H gewünschten Eigenschaften erfüllen

Übung: Zeigen Sie: Wenn f eine Einwegfunktion ist, dann auch H
Hinweis: Kontraposition.

Beispiel (für sichere Kompressionsfunktion).

Sei $E : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n$ eine sichere Blockchiffre.
Kompressionsfunktion: $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n, (m,k) \mapsto E(m,k) \oplus m$

Frage: Wann erreicht $H : \{0,1\}^* \longrightarrow \{0,1\}^n$ Sicherheitsniveau 100 Bit? (bzgl. Eigenschaft 3: starke Kollisionsresistenz)

- Betrachte nur folgenden Angriff (Brute Force):
  - Wähle zufällig k Werte $m_1, \dots, m_k$, berechne $h_i = H(m_i)$.
  - Frage: Wahrscheinlichkeit eine Kollision zu finden?
- Offensichtlich: Je kleiner Bildraum $\{0,1\}^n$, desto größer.
- Also gesucht: Untere Schranke für Bildraum, d.h. für n.
- Schätzung: $n = 100$, also Bildraum $\{0,1\}^{100}$.

Beispiel. Geburtstagsparadoxon

- W'keit, dass 23 zufällige Personen am selben Tag Geburtstag haben (Jahrgang spielt keine Rolle)?
- Häufige Antwort: 5-10 %. Tatsächlich: 50 %.
- Berechnung:
  - W'keit, dass 1 an irgendeinem Tag Geb. hat: 365/365.
  - W'keit, dass 2 an einem anderen Tag Geb. hat: 364/365.
  - W'keit, dass k an einem anderen Tag als die ersten $k-1$ Geburtstag hat: $(365-(k-1))/365$.
- Insg.: W'keit, dass alle k Personen an untersch. Tagen Geb. haben:

$$\frac{365}{365} \cdot \frac{364}{365} \cdots \frac{363}{365} \cdots \frac{365-k+1}{365} = \prod_{i=1}^{k} \frac{365-i+1}{365}$$

- Gegenwahrscheinlichkeit: Mind. zwei haben am selben Tag:

$$1 - \prod_{i=1}^{k} \frac{365-i+1}{365}$$

- Ausrechnen zeigt:

– $k = 10$: $0,117$, $k = 23$: $0,507$, $k = 36$: $0,832$.

Anwendung für Hashfunktionen: $H : \{0,1\}^* \longrightarrow \{0,1\}^n$.

- Ziel: Wie groß ist die W'keit, eine Kollision zu finden.
- Genauer: Ausrechnen, wie viele Nachrichten $m_1, \ldots, m_k$ gewählt werden müssen, um mit hoher W'keit eine Kollision zu finden.
- Um Sicherheitsniveau zu erreichen, mind. 2^{100} Nachrichten.
- Sei $h_1 = H(m_1), \ldots, h_k = H(m_k)$.
- W'keit, dass eine Kollision gefunden wurde:

$$1 - \prod_{i=1}^{k} \frac{2^n - i + 1}{2^n} = 1 - \prod_{i=1}^{k} 1 - \frac{i-1}{2^n} = 1 - \prod_{i=2}^{k} 1 - \frac{i-1}{2^n} = 1 - \prod_{i=1}^{k-1} 1 - \frac{i}{2^n}.$$

- Grobe Abschätzung: $1 - x \approx e^{-x}$:

$$1 - \prod_{i=1}^{k-1} 1 - \frac{i}{2^n} \approx 1 - \prod_{i=1}^{k-1} e^{-i/2^n} = 1 - e^{\sum_{i=1}^{k-1} -i/2^n} = 1 - e^{-(k(k-1))/(2 \cdot 2^n)} =: p.$$

- Gaußsche Summenformel: $\sum_{i=1}^{n} i = \frac{(n+1)n}{2}$.
- Also: p W'keit, dafür, dass eine Kollision gefunden wird.
- Für uns interessant: Anzahl der Nachrichten.

- Also: Bestimme k in Abhängigkeit von p:

$$\begin{aligned}
1 - e^{-(k(k-1))/(2\cdot 2^n)} = p &\iff \\
e^{-(k(k-1))/(2\cdot 2^n)} = 1 - p &\iff \\
\frac{-k(k-1)}{2\cdot 2^n} = \ln(1-p) &\iff \\
k^2 - k = 2^{n+1} \ln \frac{1}{1-p} &\iff \\
k^2 \approx 2^{n+1} \ln \frac{1}{1-p} &\iff \\
k \approx \sqrt{2^{n+1} \ln \frac{1}{1-p}} &\iff \\
k \approx 2^{(n+1)/2} \cdot \sqrt{\ln \frac{1}{1-p}} &\iff
\end{aligned}$$

- Für $p = 1/2$ also $k \approx 2^{(n+1)/2}\sqrt{\ln(2)} \approx 0.83 \cdot 2^{(n+1)/2}$.
- Also: Sicherheitsniveau 100 Bit, $n \geq 200$.

Sichere Hashfunktionen: SHA-224, SHA-256, SHA-384, SHA-512
Zahl gibt Bitgröße des Bildraums an.