

1 Kryptografische Hashverfahren

Kryptografische Hashverfahren sind ein wirksames Werkzeug zur Sicherstellung der Integrität von Nachrichten oder generell von digitalisierten Daten. In der Tat nehmen kryptografische Hashverfahren beim Schutz der Datenintegrität eine ähnlich herausragende Stellung ein wie sie Kryptosystemen bei der Wahrung der Vertraulichkeit zukommt. Daneben finden kryptografische Hashfunktionen aber auch vielfach als Bausteine von komplexeren Systemen Verwendung. Wie wir noch sehen werden, sind kryptografische Hashfunktionen etwa bei der Bildung von digitalen Signaturen sehr nützlich. Auf weitere Anwendungsmöglichkeiten werden wir später eingehen.

Den überaus meisten Anwendungen von kryptografischen Hashfunktionen h liegt die Idee zugrunde, dass sie zu einem vorgegebenen Text x eine zwar kompakte aber dennoch repräsentative Darstellung $h(x)$ liefern, die unter praktischen Gesichtspunkten als eine eindeutige Identifikationsnummer von x fungieren kann. Die Berechnungsvorschrift für h muss daher gewissermaßen darauf abzielen, „charakteristische Merkmale“ von x in den Hashwert $h(x)$ einfließen zu lassen. Da der Fingerabdruck eines Menschen ganz ähnliche Eigenschaften besitzt (was ihn für Kriminalisten bekanntlich so wertvoll macht), wird der Hashwert $h(x)$ auch oft als ein **digitaler Fingerabdruck** von x bezeichnet. Gebräuchlich sind auch die Bezeichnungen **kryptografische Prüfsumme** oder *message digest* (englische Bezeichnung für „Nachrichtenextrakt“).

Typische Schutzziele, die sich mittels Hashfunktionen realisieren lassen, sind die Nachrichten- und Teilnehmerauthentikation.

- „Nachrichtenauthentikation“ (message authentication)
 - Wie lässt sich sicherstellen, dass eine Nachricht (oder eine Datei) während einer (räumlichen oder auch zeitlichen) Übertragung nicht verändert wurde?
 - Wie lässt sich der Urheber (oder Absender) einer Nachricht zweifelsfrei feststellen?
- „Teilnehmerauthentikation“ (entity authentication, identification)
 - Wie kann sich eine Person (oder ein Gerät) anderen gegenüber zweifelsfrei ausweisen?

1.1 Klassifikation von Hashverfahren

Kryptografische Hashverfahren lassen sich grob danach klassifizieren, ob der Hashwert lediglich in Abhängigkeit vom Eingabetext berechnet wird oder zusätzlich von einem symmetrischen Schlüssel abhängt (siehe Abbildung 1 auf der nächsten Seite).

Kryptografische Hashfunktionen, bei deren Berechnung keine Schlüssel benutzt werden, dienen vornehmlich der Erkennung von unbefugt vorgenommenen Manipulationen an Dateien oder Nachrichten. Daher werden sie auch als **MDC** bezeichnet

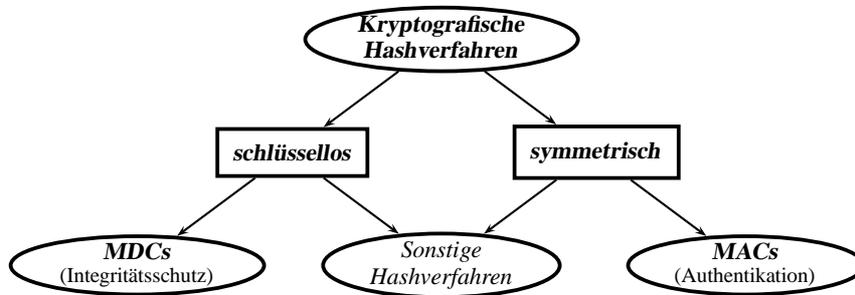


Abbildung 1 Eine grobe Einteilung von kryptografischen Hashverfahren.

(**Manipulation Detection Code** [englisch] = Code zur Erkennung von Manipulationen). Zuweilen wird das Kürzel **MDC** auch als eine Abkürzung für **Modification Detection Code** verwendet. Seltener ist dagegen die Bezeichnung **MIC** (**message integrity codes**). Abbildung 2 zeigt eine typische Anwendung von MDCs.

Um die Integrität eines Datensatzes x sicherzustellen, der über einen ungesicherten Kanal gesendet (bzw. auf einem vor Manipulationen nicht sicheren Webserver abgelegt) wird, kann man wie folgt verfahren. Man sendet den **MDC**-Hashwert von x über einen authentisierten Kanal und prüft, ob der Datensatz nach der Übertragung noch denselben Hashwert liefert.

Kryptografische Hashverfahren mit symmetrischen Schlüsseln finden hauptsächlich bei der Authentifizierung von Nachrichten Verwendung. Diese werden daher auch als **MAC** (**message authentication code** [englisch] = Code zur Nachrichtenauffertifizierung) oder als **Authentikationscode** bezeichnet. Daneben gibt es auch Hashverfahren mit asymmetrischen Schlüsseln. Diese werden jedoch der Rubrik der Signaturverfahren zugeordnet, da mit ihnen ausschließlich digitale Unterschriften gebildet werden. Wie sich

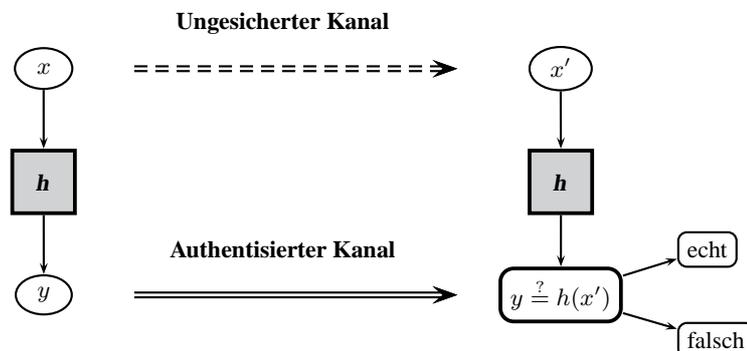


Abbildung 2 Einsatz eines MDC h zur Überprüfung der Integrität eines Datensatzes x .

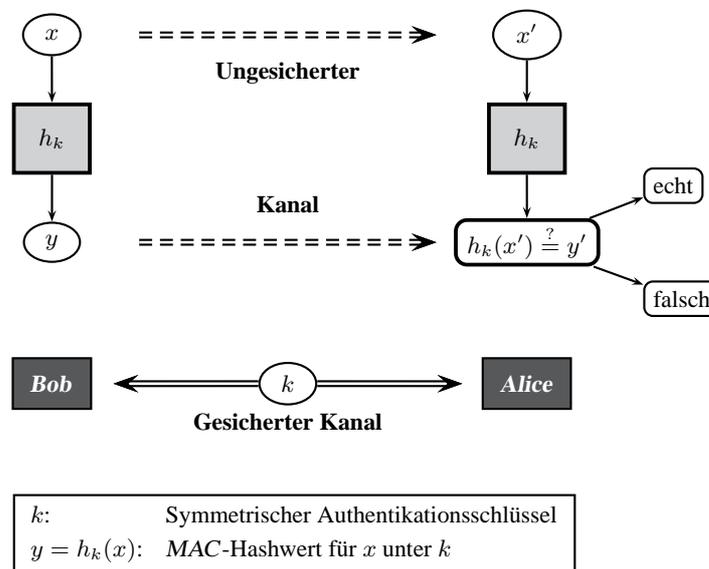


Abbildung 3 Verwendung eines MAC zur Nachrichtenaufklärung.

Nachrichten mit einem MAC authentisieren lassen, ist in Abbildung 3 dargestellt. Man beachte, dass nun auch der Hashwert über den unsicheren Kanal gesendet wird.

Möchte Bob eine Nachricht x an Alice übermitteln, so berechnet er den zugehörigen MAC-Hashwert $y = h_k(x)$ und fügt diesen der Nachricht x hinzu. Alice überprüft die Echtheit der empfangenen Nachricht (x', y') , indem sie ihrerseits den zu x' gehörigen Hashwert $h_k(x')$ berechnet und das Ergebnis mit y' vergleicht. Der geheime Authentifikationsschlüssel k muss hierbei genau wie bei einem symmetrischen Kryptosystem über einen gesicherten Kanal vereinbart werden.

Indem Bob seine Nachricht x um den Hashwert $y = h_k(x)$ ergänzt, gibt er Alice nicht nur die Möglichkeit, anhand von y die empfangene Nachricht auf Manipulationen zu überprüfen. Die Benutzung des geheimen Schlüssels k erlaubt zudem eine Überprüfung der Herkunft der Nachricht.

1.2 Sicherheit von schlüssellosen Hashfunktionen

In diesem Abschnitt betrachten wir verschiedene Sicherheitsanforderungen an einzelne Hashfunktionen h . Dabei nehmen wir an, dass h öffentlich bekannt ist, d.h. h ist eine schlüssellose Hashfunktion (MDC).

Sei $h : X \rightarrow Y$ eine Hashfunktion. Ein Paar $(x, y) \in X \times Y$ heißt **gültig** für h , falls $h(x) = y$ ist. Ein Paar (x, x') mit $h(x) = h(x')$ heißt **Kollisionspaar** für h . Die Anzahl $\|Y\|$ der Hashwerte bezeichnen wir mit m . Ist auch der Textraum X endlich, $\|X\| = n$, so heißt h eine (n, m) -**Hashfunktion**. In diesem Fall verlangen wir meist, dass $n \geq 2m$ ist, und wir nennen h dann eine **Kompressionsfunktion** (*compression function*).

Da h öffentlich bekannt ist, ist es sehr einfach, für einen vorgegebenen Text x ein gültiges Paar (x, y) zu erzeugen. Für bestimmte kryptografische Anwendungen ist es wichtig, dass dies nicht möglich ist, falls der Hashwert y vorgegeben wird.

Problem P1: Bestimmung eines Urbilds

Gegeben: Eine Hashfkt. $h : X \rightarrow Y$ und ein Hashwert $y \in Y$.

Gesucht: Ein Text $x \in X$ mit $h(x) = y$.

Falls es einen immensen Aufwand erfordert, für einen *vorgegebenen* Hashwert y einen Text x mit $h(x) = y$ zu finden, so heißt h **Einweg-Hashfunktion** (*one-way hash function* bzw. *preimage resistant hash function*). Diese Eigenschaft wird beispielsweise benötigt, wenn die Hashwerte der Benutzerpasswörter in einer öffentlich zugänglichen Datei abgespeichert werden, wie es bei manchen Unix-Systemen der Fall ist.

Problem P2: Bestimmung eines zweiten Urbilds

Gegeben: Eine Hashfkt. $h : X \rightarrow Y$ und ein Text $x \in X$.

Gesucht: Ein Text $x' \in X \setminus \{x\}$ mit $h(x') = h(x)$.

Falls sich für einen *vorgegebenen* Text x nur mit großem Aufwand ein weiterer Text $x' \neq x$ mit dem gleichen Hashwert $h(x') = h(x)$ finden lässt, heißt h **schwach kollisionsresistent** (*weakly collision resistant* bzw. *second preimage resistant*). Diese Eigenschaft wird in der durch Abbildung 2 skizzierten Anwendung benötigt. Beim Versuch, eine digitale Signatur zu fälschen (siehe unten), sieht sich der Gegner dagegen mit folgender Problemstellung konfrontiert.

Problem P3: Bestimmung einer Kollision

Gegeben: Eine Hashfkt. $h : X \rightarrow Y$.

Gesucht: Texte $x \neq x' \in X$ mit $h(x') = h(x)$.

Falls sich dieses Problem nur mit einem immensen Aufwand lösen lässt, heißt h (**stark**) **kollisionsresistent** (*collision resistant*).

Obwohl die schwache Kollisionsresistenz eine gewisse Ähnlichkeit mit der Einweg-Eigenschaft aufweist, sind die beiden Eigenschaften im allgemeinen unvergleichbar. So muss eine schwach kollisionsresistente Funktion nicht notwendigerweise eine Einwegfunktion sein, da die Bestimmung eines Urbildes gerade für diejenigen Funktionswerte einfach sein kann, die nur ein einziges Urbild besitzen. Umgekehrt impliziert die Einweg-Eigenschaft auch nicht die schwache Kollisionsresistenz, da die Kenntnis eines Urbildes das Auffinden weiterer Urbilder sehr stark erleichtern kann.

Algorithmus FindPreimage(h, y, q)

```

1 wähle eine beliebige Menge  $X_0 \subseteq X$  mit  $\|X_0\| = q$ 
2 for each  $x \in X_0$  do
3   if  $h(x) = y$  then
4     output  $x$ 
5   end
6 end
7 output „?“
```

Abbildung 4 Bestimmung eines Urbilds für einen Hashwert

1.3 Das Zufallsorakelmodell (ZOM)

Das ZOM dient dazu, die Effizienz verschiedener Angriffe auf eine Hashfunktion $h : X \rightarrow Y$ nach oben abzuschätzen. Sind X und Y vorgegeben, so können wir eine Hashfunktion $h : X \rightarrow Y$ dadurch „konstruieren“, dass wir für jedes $x \in X$ zufällig ein $y \in Y$ wählen und $h(x)$ auf y setzen. Äquivalent hierzu ist, für h eine zufällige Funktion aus der Klasse $F(X, Y)$ aller n^m Funktionen von X nach Y zu wählen. Dieses Verfahren ist auf Grund des hohen Aufwands zwar nicht mehr praktikabel, wenn $n = \|X\|$ eine bestimmte Größe übersteigt. Es liefert uns aber ein theoretisches Modell für eine Hashfunktion mit „idealen“ kryptografischen Eigenschaften. Offensichtlich besteht für den Gegner die einzige Möglichkeit, Informationen über h zu erhalten, darin, sich für eine Reihe von Texten die zugehörigen Hashwerte zu besorgen (was der Befragung eines funktionalen Zufallsorakels entspricht).

Dass eine Zufallsfunktion h gute kryptografische Eigenschaften aufweist, rührt daher, dass der Hashwert $h(x)$ für einen neuen Text x auch dann noch schwer vorhersagbar ist, wenn der Gegner bereits die Hashwerte einer beliebigen Zahl von Texten kennt.

Proposition 1 Sei $X_0 = \{x_1, \dots, x_k\}$ eine beliebige Menge von k verschiedenen Texten aus X und seien $y_1, \dots, y_k \in Y$. Dann gilt für eine zufällig aus $F(X, Y)$ gewählte Funktion h und für jedes Paar $(x, y) \in (X - X_0) \times Y$,

$$\Pr[h(x) = y \mid h(x_i) = y_i \text{ für } i = 1, \dots, k] = 1/m.$$

Um eine obere Komplexitätsschranke für das Urbildproblem im ZOM zu erhalten, betrachten wir den in Abbildung 4 dargestellten Algorithmus. Hier (und bei den beiden folgenden Algorithmen) gibt der Parameter q die Anzahl der Hashwertberechnungen (also die Anzahl der gestellten Orakelfragen an das Zufallsorakel h) wider. Der Zeitaufwand der Berechnung ist dabei proportional zu q .

Satz 2 FINDPREIMAGE(h, y, q) gibt mit Wahrscheinlichkeit $\varepsilon = 1 - (1 - 1/m)^q$ ein Urbild von y aus (unabhängig von der Wahl der Menge X_0).

Beweis: Sei $y \in Y$ fest und sei $X_0 = \{x_1, \dots, x_q\}$. Für $i = 1, \dots, q$ bezeichne E_i das Ereignis „ $h(x_i) = y$ “. Nach Proposition 1 sind diese Ereignisse stochastisch

Algorithmus FindSecondPreimage(h, x, q)

```

1   $y \leftarrow h(x)$ 
2  wähle eine beliebige Menge  $X_0 \subseteq X - \{x\}$  mit  $\|X_0\| = q - 1$ 
3  for each  $x_0 \in X_0$  do
4    if  $h(x_0) = y$  then
5      output  $x_0$ 
6    end
7  end
8  output „?“
```

Abbildung 5 Bestimmung eines zweiten Urbilds

unabhängig und ihre Wahrscheinlichkeit ist $Pr[E_i] = 1/m$ ($i = 1, \dots, q$). Also folgt

$$Pr[E_1 \cup \dots \cup E_q] = 1 - Pr[\overline{E_1} \cap \dots \cap \overline{E_q}] = 1 - (1 - 1/m)^q. \quad \blacksquare$$

Der in Abbildung 5 dargestellte Algorithmus liefert uns eine obere Schranke für die Komplexität des Problems, ein zweites Urbild für $h(x)$ zu bestimmen. Die Erfolgswahrscheinlichkeit lässt sich vollkommen analog zum vorherigen Satz bestimmen.

Satz 3 FINDSECONDPREIMAGE(h, x, q) gibt mit Wahrscheinlichkeit $\varepsilon = 1 - (1 - 1/m)^{q-1}$ ein zweites Urbild $x_0 \neq x$ von $y = h(x)$ aus.

Ist q vergleichsweise klein, so ist bei beiden bisher betrachteten Angriffen $\varepsilon \approx q/m$. Um also auf eine Erfolgswahrscheinlichkeit von $1/2$ zu kommen, ist $q \approx m/2$ zu wählen.

Geht es lediglich darum, irgendein Kollisionspaar (x, x') aufzuspüren, so bietet sich ein sogenannter **Geburtstagsangriff** an. Dieser ist deutlich zeiteffizienter zu realisieren. Wie der Name schon andeutet, basiert dieser Angriff auf dem sogenannten Geburtstagsparadoxon, welches in seiner einfachsten Form folgendes besagt.

Geburtstagsparadoxon: Bereits in einer Schulklasse mit 23 Schulkindern haben mit einer Wahrscheinlichkeit größer $1/2$ mindestens zwei Kinder am gleichen Tag Geburtstag (dies erscheint zwar verblüffend, wird aber durch die Praxis mehr als bestätigt).

Tatsächlich zeigt der nächste Satz, dass bei q -maligem Ziehen (mit Zurücklegen) aus einer Urne mit m Kugeln mit einer Wahrscheinlichkeit von

$$1 - \frac{(m-1)(m-2) \cdots (m-q+1)}{m^{q-1}}$$

eine Kugel zweimal gezogen wird. Für $m = 365$ und $q = 23$ ergibt dies einen Wert von ungefähr 0,507.

Algorithmus Collision(h, q)

```

1 wähle eine beliebige Menge  $X_0 \subseteq X$  mit  $\|X_0\| = q$ 
2 for each  $x \in X_0$  do
3    $y_x \leftarrow h(x)$ 
4 end
5 if  $y_x = y_{x'}$  für zwei Texte  $x \neq x'$  in  $X_0$  then
6   output  $(x, x')$ 
7 else
8   output „?“
9 end

```

Abbildung 6 Bestimmung eines Kollisionspaares

Zur Kollisionsbestimmung verwenden wir den in Abbildung 6 dargestellten Algorithmus. Bei einer naiven Implementierung würde zwar der Zeitaufwand für die Auswertung der if-Bedingung quadratisch von q abhängen. Trägt man aber jeden Text x unter dem Suchwort $h(x)$ in eine (herkömmliche) Hashtabelle der Größe q ein, so wird der Zeitaufwand für die Bearbeitung jedes einzelnen Textes x im wesentlichen durch die Berechnung von $h(x)$ bestimmt.

Satz 4 COLLISION(h, q) gibt mit Erfolgswahrscheinlichkeit

$$\varepsilon = 1 - \frac{(m-1)(m-2)\cdots(m-q+1)}{m^{q-1}}$$

ein Kollisionspaar (x, x') für h aus.

Beweis: Sei $X_0 = \{x_1, \dots, x_q\}$. Für $i = 1, \dots, q$ bezeichne E_i das Ereignis

$$“h(x_i) \notin \{h(x_1), \dots, h(x_{i-1})\}.”$$

Dann beschreibt $E_1 \cap \dots \cap E_q$ das Ereignis “COLLISION(h, q) gibt ? aus” und für $i = 1, \dots, q$ gilt

$$Pr[E_i | E_1 \cap \dots \cap E_{i-1}] = \frac{m-i+1}{m}.$$

Dies führt auf die Erfolgswahrscheinlichkeit

$$\begin{aligned} \varepsilon &= 1 - Pr[E_1 \cap \dots \cap E_q] \\ &= 1 - Pr[E_1]Pr[E_2 | E_1] \cdots Pr[E_q | E_1 \cap \dots \cap E_{q-1}] \\ &= 1 - \left(\frac{m-1}{m}\right) \left(\frac{m-2}{m}\right) \cdots \left(\frac{m-q+1}{m}\right). \quad \blacksquare \end{aligned}$$

Mit $1 - x \approx e^{-x}$ folgt

$$\varepsilon = 1 - \prod_{i=1}^{q-1} \left(1 - \frac{i}{m}\right) \approx 1 - \prod_{i=1}^{q-1} e^{-\frac{i}{m}} = 1 - e^{-\frac{1}{m} \sum_{i=1}^{q-1} i} = 1 - e^{-\frac{q(q-1)}{2m}} \approx q^2/2m.$$

```

1 wähle zufällig  $x \in X$ 
2  $x' \leftarrow A(x)$ 
3 if  $x' \neq x$  then
4   output  $(x, x')$ 
5 else
6   output „?“
7 end

```

Abbildung 7 Reduktion des Kollisionsproblems auf das Problem, ein zweites Urbild zu bestimmen

Somit erhalten wir die Abschätzung

$$q \approx c_\varepsilon \sqrt{m}$$

mit $c_\varepsilon = \sqrt{2\varepsilon}$. Für $\varepsilon = 1/2$ ergibt sich also $q \approx \sqrt{m}$. Besitzt also eine binäre Hashfunktion $h : \{0, 1\}^n \rightarrow \{0, 1\}^m$ die Hashwertlänge $m = 128$ Bit, so müssen im ZOM $q \approx \cdot 2^{64}$ Texte gehasht werden, um mit einer Wahrscheinlichkeit von $1/2$ eine Kollision zu finden. Um einem Geburtstagsangriff widerstehen zu können, sollte eine Hashfunktion mindestens eine Hashwertlänge von 128 oder besser 160 Bit haben.

1.4 Vergleich von Sicherheitsanforderungen

In diesem Abschnitt zeigen wir, dass stark kollisionsresistente Hashfunktionen sowohl schwach kollisionsresistent als auch Einweghashfunktionen sein müssen.

Satz 5 Sei $h : X \rightarrow Y$ eine (n, m) -Hashfunktion. Dann ist das Problem P3, ein Kollisionspaar für h zu bestimmen, auf das Problem P2, ein zweites Urbild zu bestimmen, reduzierbar. Folglich sind stark kollisionsresistente Hashfunktionen auch schwach kollisionsresistent.

Beweis: Sei A ein Las-Vegas Algorithmus, der für ein zufällig aus X gewähltes x mit Erfolgswahrscheinlichkeit ε ein zweites Urbild x' für h liefert. Dann ist klar, dass der in Abbildung 7 dargestellte Las-Vegas Algorithmus mit Wahrscheinlichkeit ε ein Kollisionspaar ausgibt. ■

Als nächstes zeigen wir, wie sich das Kollisionsproblem auf das Urbildproblem reduzieren lässt.

Satz 6 Sei $h : X \rightarrow Y$ eine (n, m) -Hashfunktion mit $n \geq 2m$. Dann ist das Problem P3, ein Kollisionspaar für h zu bestimmen, auf das Problem P1, ein Urbild zu bestimmen, reduzierbar.

Beweis: Sei A ein Invertierungsalgorithmus für h , d.h. A berechnet für jeden Hashwert y in $W(h) = \{h(x) \mid x \in X\}$ ein Urbild x mit $h(x) = y$. Betrachte den in Abbildung 8 dargestellten Las-Vegas Algorithmus B.

```

1 wähle zufällig  $x \in X$ 
2  $y \leftarrow h(x)$ 
3  $x' \leftarrow A(y)$ 
4 if  $x \neq x'$  then
5   output  $(x, x')$ 
6 else
7   output „?“
8 end

```

Abbildung 8 Reduktion des Kollisionsproblems auf das Urbildproblem

Sei $\mathcal{C} = \{h^{-1}(y) \mid y \in Y\}$. Dann hat B eine Erfolgswahrscheinlichkeit von

$$\sum_{C \in \mathcal{C}} \frac{\|C\|}{\|X\|} \cdot \frac{\|C\| - 1}{\|C\|} = \frac{1}{n} \sum_{C \in \mathcal{C}} (\|C\| - 1) = (n - m)/n \geq \frac{1}{2}. \quad \blacksquare$$

1.5 Iterierte Hashfunktionen

In diesem Abschnitt beschäftigen wir uns mit der Frage, wie sich aus einer kollisionsresistenten Kompressionsfunktion

$$h : \{0, 1\}^{m+t} \rightarrow \{0, 1\}^m$$

eine kollisionsresistente Hashfunktion

$$\hat{h} : \{0, 1\}^* \rightarrow \{0, 1\}^l$$

konstruieren lässt. Hierzu betrachten wir folgende kanonische Konstruktionsmethode.

Preprocessing: Transformiere $x \in \{0, 1\}^*$ mittels einer Funktion

$$y : \{0, 1\}^* \rightarrow \bigcup_{r \geq 1} \{0, 1\}^{rt}$$

zu einem String $y(x)$ mit der Eigenschaft $|y(x)| \equiv_t 0$.

Processing: Sei $IV \in \{0, 1\}^m$ ein öffentlich bekannter Initialisierungsvektor und sei $y(x) = y_1 \cdots y_r$ mit $|y_i| = t$ für $i = 1, \dots, r$. Berechne eine Folge z_0, \dots, z_r von Strings $z_i \in \{0, 1\}^m$ wie folgt:

$$z_i = \begin{cases} IV, & i = 0, \\ h(z_{i-1}y_i), & i = 1, \dots, r. \end{cases}$$

Optionale Ausgabetransformation: Berechne den Hashwert $\hat{h}(x) = g(z_r)$, wobei $g : \{0, 1\}^m \rightarrow \{0, 1\}^l$ eine öffentlich bekannte Funktion ist. (Meist wird für g die Identität verwendet.)

Um $\hat{h}(x)$ zu berechnen, muss also die Kompressionsfunktion h genau r -mal aufgerufen werden. Wir formulieren nun eine für Preprocessing-Funktionen wünschenswerte Eigenschaft.

Definition 7 (suffixfrei)

Eine Funktion $y : \{0, 1\}^* \rightarrow \{0, 1\}^*$ heißt **suffixfrei**, falls es keine Strings $x \neq \tilde{x}$ und z in $\{0, 1\}^*$ mit $y(\tilde{x}) = zy(x)$ gibt (d.h. kein Funktionswert $y(x)$ ist Suffix eines Funktionswertes $y(\tilde{x})$ an einer Stelle $\tilde{x} \neq x$).

Man beachte, dass jede suffixfreie Funktion insbesondere injektiv ist.

Satz 8 Falls die Preprocessing-Funktion y suffixfrei und die Ausgabetransformation g injektiv ist, so ist mit h auch \hat{h} kollisionsresistent.

Beweis: Angenommen, es gelingt, ein Kollisionspaar x, \tilde{x} für \hat{h} mit $\hat{h}(x) = \hat{h}(\tilde{x})$ zu finden. Sei

$$y(x) = y_1 y_2 \dots y_{k-1} y_k \text{ und } y(\tilde{x}) = \tilde{y}_1 \tilde{y}_2 \dots \tilde{y}_{l-1} \tilde{y}_l \text{ mit } k \leq l.$$

Da y suffixfrei ist, muss ein Index $i \in \{1, \dots, k\}$ mit $y_i \neq \tilde{y}_{l-k+i}$ existieren. Weiter seien z_i ($i = 0, \dots, k$) und \tilde{z}_j ($j = 0, \dots, l$) die in der Processing-Phase berechneten Hashwerte. Da g injektiv ist, muss mit $g(z_k) = \hat{h}(x) = \hat{h}(\tilde{x}) = g(\tilde{z}_l)$ auch $z_k = \tilde{z}_l$ gelten. Sei i_{max} der größte Index $i \in \{1, \dots, k\}$ mit $z_{i-1} y_i \neq \tilde{z}_{l-k+i-1} \tilde{y}_{l-k+i}$. Dann bilden $z_{i_{max}-1} y_{i_{max}}$ und $\tilde{z}_{l-k+i_{max}-1} \tilde{y}_{l-k+i_{max}}$ wegen

$$h(z_{i_{max}-1} y_{i_{max}}) = z_{i_{max}} = \tilde{z}_{l-k+i_{max}} = h(\tilde{z}_{l-k+i_{max}-1} \tilde{y}_{l-k+i_{max}})$$

ein Kollisionspaar für h . ■

1.6 Die Merkle-Damgard-Konstruktion

Merkle und Damgard schlugen 1989 folgende konkrete Realisierung ihrer Konstruktion vor. Als Initialisierungsvektors wird der Nullvektor $IV = 0^m$ benutzt, die optionale Ausgabetransformation entfällt, und für $y(x)$ wird im Fall $t \geq 2$ die folgende Funktion verwendet. (Den Fall $t = 1$ betrachten wir später.)

Für $x = \varepsilon$ sei $y(x) = 0^t$ und für $x \in \{0, 1\}^n$ mit $n > 0$ sei $k = \lceil \frac{n}{t-1} \rceil$ und $x = x_1 x_2 \dots x_{k-1} x_k$ mit $|x_1| = |x_2| = \dots = |x_{k-1}| = t-1$ sowie $|x_k| = t-1-d$, wobei $0 \leq d < t-1$. Dann ist $y(x) = y_1 \dots y_{k+1}$ definiert durch

$$y_i = \begin{cases} 0x_1, & i = 1 < k, \\ 1x_i, & 2 \leq i < k, \\ 0x_1 0^d, & i = k = 1, \\ 1x_k 0^d, & i = k > 1, \\ 1bin_{t-1}(d), & i = k + 1, \end{cases} \quad (1)$$

wobei $bin_{t-1}(d)$ die durch führende Nullen auf die Länge $t-1$ aufgefüllte Binärdarstellung von d ist.

Satz 9 Die durch (1) definierte Preprocessing-Funktion y ist suffixfrei.

Beweis: Seien $x \neq \tilde{x}$ zwei Texte mit $|x| \leq |\tilde{x}|$. Wir müssen zeigen, dass $y(x) = y_1 y_2 \dots y_{k+1}$ kein Suffix von $y(\tilde{x}) = \tilde{y}_1 \tilde{y}_2 \dots \tilde{y}_{l+1}$ ist. Im Fall $x = \varepsilon$ ist dies klar. Für $x \neq \varepsilon$ machen wir folgende Fallunterscheidung.

1. Fall: $|x| \not\equiv_{t-1} |\tilde{x}|$. Dann folgt $d \neq \tilde{d}$ und somit $y_{k+1} \neq \tilde{y}_{l+1}$.
2. Fall: $|x| = |\tilde{x}|$. In diesem Fall ist $k = l$. Wegen $x \neq \tilde{x}$ existiert ein Index $i \in \{1, \dots, k\}$ mit $x_i \neq \tilde{x}_i$. Dies impliziert $y_i \neq \tilde{y}_i$, also ist $y(x)$ kein Suffix von $y(\tilde{x})$.
3. Fall: $|x| \neq |\tilde{x}|$ und $|x| \equiv_{t-1} |\tilde{x}'|$. In diesem Fall ist $k < l$. Da $y(x)$ mit einer Null beginnt, aber das $(l - k + 1)$ -te Bit von $y(\tilde{x})$ eine Eins ist, kann $y(x)$ kein Suffix von $y(\tilde{x})$ sein. ■

Nun kommen wir zum Fall $t = 1$. Sei y die durch $y(x) := 11f(x)$ definierte Funktion, wobei f wie folgt definiert ist:

$$f(x_1, \dots, x_n) = f(x_1) \dots f(x_n) \text{ mit } f(0) = 0 \text{ und } f(1) = 01.$$

Dann ist leicht zu sehen, dass y suffixfrei ist. Da die Kompressionsfunktion h bei der Berechnung von $\hat{h}(x)$ im Fall $t = 1$ für jedes Bit von $y(x)$ einmal aufgerufen wird, wird h genau $|y(x)| \leq 2(n + 1)$ -mal aufgerufen. Im Fall $t > 1$ werden dagegen nur $k + 1 = \lceil \frac{n}{t-1} \rceil + 1$ Aufrufe benötigt.

1.7 Die MD4-Hashfunktion

Die MD4-Hashfunktion (*Message Digest*) wurde 1990 von Rivest vorgeschlagen. Eine verbesserte Version (MD5) wurde von ihm 1991 präsentiert. Die Bitlängen von MD4 und MD5 betragen $l = 128$ Bit. Der *Secure Hash Algorithm* (SHA-1) ist eine Weiterentwicklung des MD4 bzw. MD5 Algorithmus. Er gilt in den USA als Standard und ist Bestandteil des DSS (Digital Signature Standard). Die Bitlänge von SHA-1 beträgt $l = 160$ Bit. Bei einer Wortlänge von 32 Bit entspricht dies 5 Wörtern. MD4, MD5 und SHA-1 benutzen folgende Operationen auf Wörtern.

Operatoren auf $\{0, 1\}^{32}$	
$X \wedge Y$	bitweises „Und“ von X und Y
$X \vee Y$	bitweises „Oder“ von X und Y
$X \oplus Y$	bitweises „exklusives Oder“ von X und Y
$\neg X$	bitweises Komplement von X
$X + Y$	Ganzzahl-Addition modulo 2^{32}
$X \leftrightarrow s$	zirkulärer Linksshift um s Stellen

Während die Ganzzahl-Addition bei MD4 und MD5 in *little endian* Architektur (d.h. ein aus 4 Bytes $a_0 a_1 a_2 a_3$, $0 \leq a_i \leq 255$ zusammengesetztes Wort repräsentiert die

Zahl $a_32^{24} + a_22^{16} + a_12^8 + a_0$ ausgeführt wird, verwendet SHA-1 eine *big endian* Architektur (d.h. $a_0a_1a_2a_3$, $0 \leq a_i \leq 255$ repräsentiert die Zahl $a_02^{24} + a_12^{16} + a_22^8 + a_3$).

Der MD4-Algorithmus benutzt die folgenden Konstanten $y_j, z_j, s_j, j = 0, \dots, 47$

	y_j (in Hexadezimaldarstellung)
$j = 0, \dots, 15$	0
$j = 16, \dots, 31$	5a827999
$j = 32, \dots, 47$	6ed9eba1
	z_j
$j = 0, \dots, 15$	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
$j = 16, \dots, 31$	0, 4, 8, 12, 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 15
$j = 32, \dots, 47$	0, 8, 4, 12, 2, 10, 6, 14, 1, 9, 5, 13, 3, 11, 7, 15
	s_j
$j = 0, \dots, 15$	3, 7, 11, 19, 3, 7, 11, 19, 3, 7, 11, 19, 3, 7, 11, 19
$j = 16, \dots, 31$	3, 5, 9, 13, 3, 5, 9, 13, 3, 5, 9, 13, 3, 5, 9, 13
$j = 32, \dots, 47$	3, 9, 11, 15, 3, 9, 11, 15, 3, 9, 11, 15, 3, 9, 11, 15

und folgende Funktionen $f_j, j = 0, \dots, 47$

$$f_j(X, Y, Z) := \begin{cases} (X \wedge Y) \vee (\neg X \wedge Z), & j = 0, \dots, 15, \\ (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z), & j = 16, \dots, 31, \\ X \oplus Y \oplus Z, & j = 32, \dots, 47. \end{cases}$$

Für MD4 konnten nach ca. 2^{20} Hashwertberechnungen Kollisionen aufgespürt werden. Deshalb gilt MD4 nicht mehr als kollisionsresistent.

Algorithmus MD4(x)

```

1  Eingabe:  $x \in \{0, 1\}^*, |x| = n$ 
2   $y \leftarrow x10^k \text{bin}_{64}(n), k \in \{0, 1, \dots, 511\}$  mit  $n + 1 + k + 64 \equiv 0 \pmod{512}$ 
3   $(H_1, H_2, H_3, H_4) \leftarrow (67452301, \text{efcdab89}, 98\text{badcfe}, 10325476)$ 
4  sei  $y = M_1 \cdots M_r, r = (n + 1 + k + 64)/512$ 
5  for  $i \leftarrow 1$  to  $r$  do
6    sei  $M_i = X[0] \cdots X[15]$ 
7     $(A, B, C, D) \leftarrow (H_1, H_2, H_3, H_4)$ 
8    for  $j \leftarrow 0$  to 47 do
9       $(A, B, C, D) \leftarrow (D, (A + f_j(B, C, D) + X[z_j] + y_j) \leftarrow s_j, B, C)$ 
10   end
11    $(H_1, H_2, H_3, H_4) \leftarrow (H_1 + A, H_2 + B, H_3 + C, H_4 + D)$ 
12  end
13  Ausgabe:  $H_1H_2H_3H_4$ 

```

1.8 Die MD5-Hashfunktion

In MD5 werden teilweise andere Konstanten als in MD4 verwendet. Zudem besitzt MD5 eine zusätzliche 4. Runde ($j = 48, \dots, 63$), in der die Funktion $f_j(X, Y, Z) = Y \oplus (X \vee \neg Z)$ verwendet wird. Außerdem wurde die in Runde 2 von MD4 verwendete Funktion durch $f_j(X, Y, Z) := (X \wedge Z) \vee (Y \wedge \neg Z)$, $j = 16 \dots 31$, ersetzt. Die y -Konstanten sind definiert als $y_j :=$ die ersten 32 Bit der Binärdarstellung von $\text{abs}(\sin(j + 1))$, $0 \leq j \leq 63$, und für z_j und s_j werden folgende Konstanten benutzt.

	z_j
$j = 0, \dots, 15$	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
$j = 16, \dots, 31$	1, 6, 11, 0, 5, 10, 15, 4, 9, 14, 3, 8, 13, 2, 7, 12
$j = 32, \dots, 47$	5, 8, 11, 14, 1, 4, 7, 10, 13, 0, 3, 6, 9, 12, 15, 2
$j = 48, \dots, 63$	0, 7, 14, 5, 12, 3, 10, 1, 8, 15, 6, 13, 4, 11, 2, 9
	s_j
$j = 0, \dots, 15$	7, 12, 17, 22, 7, 12, 17, 22, 7, 12, 17, 22, 7, 12, 17, 22
$j = 16, \dots, 31$	5, 9, 14, 20, 5, 9, 14, 20, 5, 9, 14, 20, 5, 9, 14, 20
$j = 32, \dots, 47$	4, 11, 16, 23, 4, 11, 16, 23, 4, 11, 16, 23, 4, 11, 16, 23
$j = 48, \dots, 63$	6, 10, 15, 21, 6, 10, 15, 21, 6, 10, 15, 21, 6, 10, 15, 21

Für MD5 konnten bisher keine Kollisionspaare gefunden werden (allerdings gelang dies für die Kompressionsfunktion von MD5).

Algorithmus MD5(x)

- 1 **Eingabe:** $x \in \{0, 1\}^*$, $|x| = n$
- 2 $y \leftarrow x10^k \text{bin}_{64}(n)$, $k \in \{0, 1, \dots, 511\}$ mit $n + 1 + k + 64 \equiv 0 \pmod{512}$
- 3 $(H_1, H_2, H_3, H_4) \leftarrow (67452301, \text{efcdab89}, \text{98badcfe}, 10325476)$
- 4 sei $y = M_1 \dots M_r$, $r = (n + 1 + k + 64)/512$
- 5 **for** $i \leftarrow 1$ **to** r **do**
- 6 sei $M_i = X[0] \dots X[15]$
- 7 $(A, B, C, D) \leftarrow (H_1, H_2, H_3, H_4)$
- 8 **for** $j \leftarrow 0$ **to** 63 **do**
- 9 $(A, B, C, D) \leftarrow (D, (A + f_j(B, C, D) + X[z_j] + y_j) \leftarrow s_j, B, C)$
- 10 **end**
- 11 $(H_1, H_2, H_3, H_4) \leftarrow (H_1 + A, H_2 + B, H_3 + C, H_4 + D)$
- 12 **end**
- 13 **Ausgabe:** $H_1 H_2 H_3 H_4$

1.9 Die SHA-1-Hashfunktion

SHA-1 unterscheidet sich nur geringfügig von der SHA-0 Hashfunktion, in der eine Schwachstelle dazu führt, dass nach Berechnung von ca. 2^{61} Hashwerten ein Kollisionspaar gefunden werden kann (obwohl bei einem Geburtstagsangriff auf Grund der Hashwertlänge von 160 Bit ca. 2^{80} Berechnungen erforderlich sein müssten). Diese potentielle Schwäche von SHA-0 wurde im SHA-1 dadurch entfernt, dass SHA-1 in Zeile 8 einen zirkulären Shift um eine Bitstelle ausführt.

Der SHA-1-Algorithmus benutzt die folgenden Konstanten K_j , $j = 0, \dots, 79$

	K_j (in Hexadezimaldarstellung)
$j = 0, \dots, 19$	5a827999
$j = 20, \dots, 39$	6ed9eba1
$j = 40, \dots, 59$	8f1bbcdc
$j = 60, \dots, 79$	ca62c1d6

und folgende Funktionen f_j , $j = 0, \dots, 79$

$$f_j(X, Y, Z) := \begin{cases} (X \wedge Y) \vee (\neg X \wedge Z), & j = 0, \dots, 19, \\ X \oplus Y \oplus Z, & j = 20, \dots, 39, \\ (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z), & j = 40, \dots, 59, \\ X \oplus Y \oplus Z, & j = 60, \dots, 79. \end{cases}$$

Algorithmus SHA-1(x)

```

1  Eingabe:  $x \in \{0, 1\}^*$ ,  $|x| = n$ 
2   $y \leftarrow x10^k \text{bin}_{64}(n)$ ,  $k \in \{0, 1, \dots, 511\}$  mit  $n + 1 + k + 64 \equiv 0 \pmod{512}$ 
3   $(H_0, H_1, H_2, H_3, H_4) \leftarrow (67452301, \text{efcdab89}, 98\text{badcfe}, 10325476, \text{c3d2e1f0})$ 
4  sei  $y = M_1 \cdots M_r$ ,  $r = (n + 1 + k + 64)/512$ 
5  for  $i \leftarrow 1$  to  $r$  do
6    sei  $M_i = X[0] \cdots X[15]$ 
7    for  $t \leftarrow 16$  to  $79$  do
8       $X[t] \leftarrow (X[t - 3] \oplus X[t - 8] \oplus X[t - 14] \oplus X[t - 16]) \leftarrow 1$ 
9    end
10    $(A, B, C, D, E) \leftarrow (H_0, H_1, H_2, H_3, H_4)$ 
11   for  $j \leftarrow 0$  to  $79$  do
12      $\text{temp} \leftarrow (A \leftarrow 5) + f_j(B, C, D) + E + X[t] + K_t$ 
13      $(A, B, C, D, E) \leftarrow (\text{temp}, A, B \leftarrow 30, C, D)$ 
14   end
15    $(H_0, H_1, H_2, H_3, H_4) \leftarrow (H_0 + A, H_1 + B, H_2 + C, H_3 + D, H_4 + E)$ 
16 end
17 Ausgabe:  $H_0H_1H_2H_3H_4$ 

```

1.10 Kryptoanalyse von Hashfunktionen

Bereits 1991 wurden von Den Boer und Bosselaers Schwächen im MD4 aufgedeckt. Im August 2004 erschien ein Bericht [1] mit einer Anleitung, wie sich Kollisionen für MD4 mittels “hand calculation” finden lassen.

In 1993, fanden den Boer und Bosselaers einen Weg, so genannte “Pseudo-Kollisionen” für die MD5 Kompressionsfunktion zu generieren. In 1996, fand Dobbertin ein Kollisionspaar für die MD5 Kompressionsfunktion.

Im August 2004 wurden schließlich Kollisionen für MD5 von Xiaoyun Wang, Dengguo Feng, Xuejia Lai and Hongbo Yu berechnet. Der benötigte Aufwand wurde mit ca. 1 Stunde auf einem IBM p690 Cluster abgeschätzt.

Im März 2005 veröffentlichten Arjen Lenstra, Xiaoyun Wang, and Benne de Weger zwei X.509 Zertifikate mit unterschiedlichen Public-keys, die auf denselben MD5-Hashwert führten. Nur wenige Tage später beschrieb Vlastimil Klima eine Möglichkeit, Kollisionen für MD5 innerhalb weniger Stunden auf einem Notebook zu berechnen. Mittels der so genannten Tunneling-Methode wurde die Rechenzeit vom gleichen Autor im März 2006 auf eine Minute verkürzt.

Auf der CRYPTO 98 stellten Chabaud und Joux einen Angriff auf SHA-0 vor, der ein Kollisionspaar mit nur 2^{61} Hashwertberechnungen (anstelle von 2^{80} bei einem Geburts-tagsangriff) aufspürt.

In 2004 fanden Biham und Chen Beinahe-Kollisionen für den SHA-0, bei denen sich die Hashwerte nur an 18 von den 160 Bitpositionen unterschieden. Zudem legten sie volle Kollisionen für den auf 62 Runden reduzierten SHA-0 Algorithmus vor.

Schließlich wurde im August 2004 die Berechnung einer Kollision für den vollen 80-Runden SHA-0 Algorithmus von Joux, Carribault, Lemuet and Jalby bekannt gegeben. Hierzu wurden lediglich 2^{51} Hashwerte berechnet, die ca. 80 000 Stunden CPU-Rechenzeit auf einem 2-Prozessor 256-Itanium Supercomputer benötigten.

Im August 2004 wurde von Wang, Feng, Lai und Yu auf der CRYPTO 2004 eine Angriffsmethode für MD5, SHA-0 und andere Hashfunktionen vorgestellt, mit der sich die Anzahl der Hashwertberechnungen auf 2^{40} senken lässt. Dies wurde im Februar 2005 von Xiaoyun Wang, Yiqun Lisa Yin und Hongbo Yu leicht auf 2^{39} Hashwertberechnungen verbessert.

Aufgrund der erfolgreichen Angriffe auf SHA-0 rieten mehrere Experten von einer weiteren Anwendung des SHA-1 ab. Daraufhin kündigte die amerikanische Behörde NIST an, SHA-1 in 2010 zugunsten der SHA-2 Varianten abzulösen.

In 2005 veröffentlichten Rijmen und Oswald einen Angriff, der mit weniger als 2^{80} Hashwertberechnungen ein Kollisionspaar für den auf 53 Runden reduzierten SHA-1 Algorithmus findet. Nur wenig später kündigten Xiaoyun Wang, Yiqun Lisa Yin und Hongbo Yu einen Angriff auf den vollen 80-Runden SHA-1 mit 2^{69} Hashwertberechnungen an. Im August 2005 erfuhr der benötigte Aufwand von Xiaoyun Wang, Andrew Yao and Frances Yao auf der CRYPTO 2005 eine weitere Reduktion auf 2^{63} Berechnungen.

1.11 Nachrichten-Authentikationscodes (MACs)

Definition 10 (Hashfamilie)

Eine **Hashfamilie** \mathcal{H} wird durch folgende Komponenten beschrieben:

- X , eine endliche oder unendliche Menge von Texten,
- Y , endliche Menge aller möglichen **Hashwerte**, $\|Y\| \leq \|X\|$,
- K , endlicher **Schlüsselraum** (*key space*), wobei jeder Schlüssel $k \in K$ eine Hashfunktion $h_k : X \rightarrow Y$ spezifiziert.

Im folgenden werden wir die Größe $\|X\|$ des Textraumes mit n , die des Hashwertbereiches Y mit m und die des Schlüsselraumes K mit l bezeichnen. Wir nennen dann (X, Y, K, H) auch eine (n, m, l) -Hashfamilie.

Sicherheitseigenschaften von MACs

Damit ein geheimer Schlüssel k für die Authentifizierung mehrerer Nachrichten benutzt werden kann, ohne dass dies einem potentiellen Gegner zur nichtautorisierten Berechnung von gültigen MAC-Werten verhilft, sollte folgende Bedingung erfüllt sein.

Berechnungsresistenz: Auch wenn eine Reihe von unter einem Schlüssel k generierten Text-Hashwert-Paaren $(x_1, h_k(x_1)), \dots, (x_n, h_k(x_n))$ bekannt ist, erfordert es einen immensen Aufwand, in Unkenntnis von k ein weiteres Paar (x, y) mit $y = h_k(x)$ zu finden.

Bei Verwendung einer berechnungsresistenten Hashfunktion ist es einem Gegner nicht möglich, an Alice eine Nachricht x zu schicken, die Alice als von Bob stammend anerkennt.

Verwendung eines MAC zur Versiegelung von Software

Mithilfe einer berechnungsresistenten Hashfunktion kann der Integritätsschutz für mehrere Datensätze auf die Geheimhaltung eines Schlüssels k zurückgeführt werden.

Um die Datensätze x_1, \dots, x_n gegen unbefugt vorgenommene Veränderungen zu schützen, legt man sie zusammen mit ihren Hashwerten $y_1 = h_k(x_1), \dots, y_n = h_k(x_n)$ auf einem unsicheren Speichermedium ab und bewahrt den geheimen Schlüssel k an einem sicheren Ort auf. Bei einem späteren Zugriff auf einen Datensatz x_i lässt sich dessen Unversehrtheit durch einen Vergleich von y_i mit dem Ergebnis $h_k(x_i)$ einer erneuten MAC-Berechnung überprüfen.

Da auf diese Weise ein wirksamer Schutz der Datensätze gegen Viren und andere Manipulationen erreicht wird, spricht man von einer Versiegelung der gespeicherten Datensätze.

1.12 Angriffe gegen symmetrische Hashfunktionen

Ein Angriff gegen einen MAC hat die unbefugte Berechnung von Hashwerten zum Ziel. Das heißt, der Gegner versucht, Hashwerte $h_k(x)$ ohne Kenntnis des geheimen Schlüssels k zu berechnen. Entsprechend der Art des zur Verfügung stehenden Textmaterials lassen sich die Angriffe gegen einen MAC wie folgt klassifizieren.

Impersonation

Der Gegner kennt nur den benutzten MAC und versucht ein Paar (x, y) mit $h_k(x) = y$ zu generieren, wobei k der (dem Gegner unbekante) Schlüssel ist.

Substitution

Der Gegner versucht in Kenntnis eines Paares $(x, h_k(x))$ ein Paar (x', y') mit $h_k(x') = y'$ zu generieren.

Angriff bei bekanntem Text (*known-text attack*)

Der Gegner kennt für eine Reihe von Texten x_1, \dots, x_n (die er nicht selbst wählen konnte) die zugehörigen MAC-Werte $h_k(x_1), \dots, h_k(x_n)$ und versucht, ein Paar (x', y') mit $h_k(x') = y'$ und $x' \notin \{x_1, \dots, x_n\}$ zu generieren.

Angriff bei frei wählbarem Text (*chosen-text attack*)

Der Gegner kann die Texte x_i selbst wählen.

Angriff bei adaptiv wählbarem Text (*adaptive chosen-text attack*)

Der Gegner kann die Wahl des Textes x_i von den zuvor erhaltenen MAC-Werten $h_k(x_j), j < i$, abhängig machen.

Wechseln die Anwender nach jeder Hashwertberechnung den Schlüssel, so genügt es, dass \mathcal{H} einem Substitutionsangriff widersteht.

1.13 Informationstheoretische Sicherheit von MACs

Modell: Schlüssel k und Nachrichten x werden unabhängig gemäß einer Wahrscheinlichkeitsverteilung $p(k, x) = p(k)p(x)$ generiert, welche dem Gegner (im Folgenden auch Oskar genannt) bekannt ist. Wir nehmen o.B.d.A. an, dass $p(x) > 0$ und $p(k) > 0$ für alle $x \in X$ und alle $k \in K$ gilt.

Erfolgswahrscheinlichkeit für Impersonation

α : Wahrscheinlichkeit mit der sich ein Gegner bei optimaler Strategie als Bob ausgeben kann, ohne dass Alice dies bemerkt.

Für ein Paar (x, y) sei $p(x \mapsto y)$ die Wahrscheinlichkeit, dass ein zufällig gewählter Schlüssel den Text x auf den Hashwert y abbildet:

$$p(x \mapsto y) = \sum_{k \in K(x, y)} p(k).$$

wobei $K(x, y) = \{k \in K \mid h_k(x) = y\}$ alle Schlüssel enthält, die x auf y abbilden. D.h. $p(x \mapsto y)$ ist die Wahrscheinlichkeit, dass Alice das (vom Gegner gewählte) Paar (x, y) als echt akzeptiert. Dann gilt

$$\alpha = \max\{p(x \mapsto y) \mid x \in X, y \in Y\}.$$

Beispiel 11 Sei $X = Y = \{0, 1, 2\} = \mathbb{Z}_3$ und sei $K = \mathbb{Z}_3 \times \mathbb{Z}_3$. Für $k = (a, b) \in K$ und $x \in X$ sei

$$h_k(x) = ax + b \pmod{3}.$$

Die zugehörige Authentikationsmatrix erhalten wir, indem wir die Zeilen mit den Schlüsseln $k \in K$ und die Spalten mit den Texten $x \in X$ indizieren und in Zeile k und Spalte x den Hashwert $h_k(x)$ eintragen.

	0	1	2
(0, 0)	0	0	0
(0, 1)	1	1	1
(0, 2)	2	2	2
(1, 0)	0	1	2
(1, 1)	1	2	0
(1, 2)	2	0	1
(2, 0)	0	2	1
(2, 1)	1	0	2
(2, 2)	2	1	0

Angenommen, jeder Schlüssel (a, b) hat die gleiche Wk $p(a, b) = 1/9$. Versucht der Gegner dann eine Impersonation mit dem Paar (x, y) , so akzeptieren genau 3 der 9 möglichen Schlüssel dieses Paar. Dies liegt daran, dass in jeder Spalte jeder Hashwert genau dreimal vorkommt. Also gilt $p(x \mapsto y) = 3/9 = 1/3$ für alle Paare $(x, y) \in X \times Y$, was für α ebenfalls den Wert $\alpha = 1/3$ ergibt. \triangleleft

Satz 12 Für jeden MAC (X, Y, K, H) gilt $\alpha \geq \frac{1}{m}$.

Beweis: Sei $x \in X$ beliebig. Dann gilt

$$\sum_{y \in Y} p(x \mapsto y) = \sum_{y \in Y} \sum_{k \in K(x, y)} p(k) = \sum_{k \in K} p(k) = 1.$$

Somit existiert für jedes $x \in X$ ein $y \in Y$ mit $p(x \mapsto y) \geq \frac{1}{m}$ und dies impliziert

$$\alpha = \max_{x, y} p(x \mapsto y) \geq \frac{1}{m}.$$

■

Bemerkung 13 Wie der Beweis zeigt, gilt $\alpha = \frac{1}{m}$ genau dann, wenn für alle Paare $(x, y) \in X \times Y$ gilt,

$$\sum_{k \in K(x, y)} p(k) = \frac{1}{m}.$$

D.h. bei Gleichverteilung der Schlüssel muss in jeder Spalte jeder Hashwert gleich oft vorkommen.

Beispiel 14 Sei $K = \{1, 2, 3\}$, $M = \{a, b, c, d\}$ und $T = \{0, 1\}$.

	$\mathcal{A}(k, m)$	$\boxed{0,1}$	$\boxed{0,2}$	$\boxed{0,3}$	$\boxed{0,4}$
$\boxed{0,25}$	1	0	0	0	1
$\boxed{0,30}$	2	1	1	0	1
$\boxed{0,45}$	3	0	1	1	0

Annahme: \mathbf{K} hat Wahrscheinlichkeitsverteilung $(0, 25; 0, 3; 0, 45)$ und \mathbf{M} hat Wahrscheinlichkeitsverteilung $(0, 1; 0, 2; 0, 3; 0, 4)$.

Dann hat der Gegner folgende Erfolgsaussichten, falls er das Paar (x, y) an Alice sendet:

$\alpha(x, y)$	0	1	
a	0,7	0,3	$\Rightarrow \alpha = 0,75.$
b	0,25	0,75	
c	0,55	0,45	
d	0,45	0,55	

Erfolgswahrscheinlichkeit für Substitution

β : Wahrscheinlichkeit mit der ein Gegner bei optimaler Strategie eine von Bob gesendete Nachricht (x, y) durch eine andere Nachricht (x', y') ersetzen kann, ohne dass Alice dies bemerkt.

Angenommen, Bob sendet die Nachricht (x, y) und der Gegner ersetzt diese durch (x', y') . Dann ist die Erfolgswahrscheinlichkeit des Gegners gleich der bedingten Wk

$$p(x' \mapsto y' | x \mapsto y) = \frac{p(x \mapsto y, x' \mapsto y')}{p(x \mapsto y)} = \frac{\sum_{k \in K(x, y, x', y')} p(k)}{\sum_{k \in K(x, y)} p(k)},$$

dass ein zufällig gewählter Schlüssel k den Text x' auf y' abbildet, wenn bereits bekannt ist, dass er x auf y abbildet. Falls Bob also das Paar (x, y) sendet, so kann der Gegner bestenfalls die Erfolgswahrscheinlichkeit

$$\beta(x, y) = \max\{p(x' \mapsto y' | x \mapsto y) \mid x' \in X - \{x\}, y' \in Y\}$$

erzielen. Da Bob auf die Wahl von (x, y) keinen Einfluss hat, berechnet sich β als der erwartete Wert von $\beta(x, y)$, wobei das Paar (x, y) von Bob mit Wk

$$p(x, y) = p(x)p(y|x) = p(x)p(x \mapsto y)$$

gesendet wird. Somit ergibt sich β zu

$$\beta = \sum_{x \in X, y \in Y} p(x, y)\beta(x, y) = \sum_{x \in X} p(x) \sum_{y \in Y} \beta'(x, y),$$

wobei

$$\beta'(x, y) = \max\{p(x \mapsto y, x' \mapsto y') \mid x' \in X - \{x\}, y' \in Y\}$$

ist.

Beispiel 14 (Fortsetzung)

(x, y)	$p(x \mapsto y, x' \mapsto y')$								$\beta'(x, y)$	$\beta(x, y)$
	$(a, 0)$	$(a, 1)$	$(b, 0)$	$(b, 1)$	$(c, 0)$	$(c, 1)$	$(d, 0)$	$(d, 1)$		
$(a, 0)$			0,25	0,45	0,25	0,45	0,45	0,25	0,45	0,643
$(a, 1)$			0	0,3	0,3	0	0	0,3	0,3	1
$(b, 0)$	0,25	0			0,25	0	0	0,25	0,25	1
$(b, 1)$	0,45	0,3			0,3	0,45	0,45	0,3	0,45	0,6
$(c, 0)$	0,25	0,3	0,25	0,3			0	0,55	0,55	1
$(c, 1)$	0,45	0	0	0,45			0,45	0	0,45	1
$(d, 0)$	0,45	0	0	0,45	0	0,45			0,45	1
$(d, 1)$	0,25	0,3	0,25	0,3	0,55	0			0,55	1

Für β erhalten wir also den Wert

$$\begin{aligned} \beta &= 0,1 \cdot (0,45 + 0,3) + 0,2 \cdot (0,25 + 0,45) + 0,3 \cdot (0,55 + 0,45) + 0,4 \cdot (0,45 + 0,55) \\ &= 0,915. \end{aligned}$$

Satz 15 Für jeden MAC (X, Y, K, H) gilt $\beta \geq \frac{1}{m}$.

Beweis: Sei $(x, y) \in X \times Y$ ein Paar mit $p(x, y) > 0$. Dann gilt für beliebige $x' \in X - \{x\}$,

$$\sum_{y' \in Y} p(x' \mapsto y' \mid x \mapsto y) = \frac{\sum_{y' \in Y} \sum_{k \in K(x', y'; x, y)} p(k)}{\sum_{k \in K(x, y)} p(k)} = 1.$$

Somit existiert ein $y' \in Y$ mit $p(x' \mapsto y' \mid x \mapsto y) \geq \frac{1}{m}$ und dies impliziert für alle (x, y) mit $p(x, y) > 0$,

$$\beta(x, y) = \max\{p(x' \mapsto y' \mid x \mapsto y) \mid x' \in X - \{x\}, y' \in Y\} \geq \frac{1}{m}, \quad (2)$$

was wiederum

$$\beta = \sum_{x \in X, y \in Y} p(x, y)\beta(x, y) \geq \frac{1}{m} \sum_{x \in X, y \in Y} p(x, y) = \frac{1}{m}$$

impliziert. ■

Lemma 16 Sei (X, Y, K, H) ein MAC mit $\beta = \frac{1}{m}$. Dann gilt

$$p(x' \mapsto y' | x \mapsto y) = 1/m$$

für alle Doppelpaare (x, y, x', y') mit $x \neq x'$.

Beweis: Wir zeigen zuerst, dass im Fall

$$\beta = \frac{1}{m}$$

für alle Paare $(x, y) \in X \times Y$

$$p(x \mapsto y) > 0$$

ist. Ist nämlich

$$p(w \mapsto z) = 0,$$

so ist auch

$$p(w \mapsto z | u \mapsto v) = 0,$$

wobei $(u, v) \in X \times Y$ ein beliebiges Paar mit

$$p(u \mapsto v) > 0$$

ist. Wegen

$$1 = \sum_{z' \in Y} p(w \mapsto z' | u \mapsto v) = \sum_{z' \in Y - \{z\}} p(w \mapsto z' | u \mapsto v)$$

impliziert dies die Existenz eines Hashwertes z' mit

$$p(w \mapsto z' | u \mapsto v) \geq 1/(m-1) > 1/m.$$

Dann ist aber auch

$$\beta(u, v) = \max\{p(u' \mapsto v' | u \mapsto v) \mid u' \in X - \{u\}, v' \in Y\} > 1/m.$$

Da

$$\beta(x, y) \geq 1/m$$

für alle Paare (x, y) gilt (siehe (2)) und da

$$p(u, v) = p(u)p(u \mapsto v) > 0$$

ist, folgt

$$\beta = \sum_{x \in X, y \in Y} p(x, y)\beta(x, y) > 1/m.$$

Ist nun

$$p(x' \mapsto y' | x \mapsto y) \neq 1/m$$

für ein Doppelpaar (x, y, x', y') mit $x \neq x'$, so muss wegen

$$\sum_{z' \in Y} p(x' \mapsto z' | x \mapsto y) = 1$$

auch ein Doppelpaar (x, z', x', y') mit

$$p(x' \mapsto z' | x \mapsto y) > 1/m$$

existieren, was genau wie im ersten Teil des Beweises zu einem Widerspruch führt. ■

Satz 17 Ein MAC (X, Y, K, H) erfüllt $\beta = \frac{1}{m}$ genau dann, wenn

$$p(x \mapsto y, x' \mapsto y') = 1/m^2$$

für alle Doppelpaare (x, y, x', y') mit $x \neq x'$ gilt.

Beweis: Sei (X, Y, K, H) ein MAC mit $\beta = \frac{1}{m}$. Nach obigem Lemma impliziert dies, dass

$$p(x' \mapsto y' | x \mapsto y) = 1/m$$

für alle Doppelpaare (x, y, x', y') mit $x \neq x'$ gilt. Dies impliziert nun

$$p(x' \mapsto y') = \sum_y p(x \mapsto y) p(x' \mapsto y' | x \mapsto y) = 1/m$$

und daher

$$p(x \mapsto y, x' \mapsto y') = p(x' \mapsto y') p(x \mapsto y | x' \mapsto y') = 1/m^2.$$

Umgekehrt rechnet man leicht nach, dass \mathcal{H} tatsächlich die Bedingung

$$\beta = \frac{1}{m}$$

erfüllt, wenn

$$p(x \mapsto y, x' \mapsto y') = 1/m^2$$

für alle Doppelpaare (x, y, x', y') mit $x \neq x'$ gilt. ■

Bemerkung 18 Nach obigem Satz gilt $\beta = \frac{1}{m}$ genau dann, wenn für alle Doppelpaare (x, y, x', y') mit $x \neq x'$ gilt,

$$p(x \mapsto y, x' \mapsto y') = \sum_{k \in K(x, y, x', y')} p(k) = \frac{1}{m^2}.$$

D.h. bei Gleichverteilung der Schlüssel gilt $\beta = \frac{1}{m}$ genau dann, wenn in je zwei Spalten der Authentikationsmatrix jedes Hashwertpaar gleich oft vorkommt.

Ab jetzt setzen wir voraus, dass der Schlüssel unter Gleichverteilung gewählt wird, d.h. es gilt $p(k) = \frac{1}{\|K\|}$ für alle $k \in K$.

Definition 19 (stark universale Hashfamilien) Ein MAC (X, Y, K, H) heißt **stark universal**, falls für alle $x, x' \in M$ mit $x \neq x'$ und alle $y, y' \in T$ gilt:

$$\|K(x, y, x', y')\| = \frac{\|K\|}{m^2}.$$

Bemerkung 20 Bei der Konstruktion von stark universalen Hashfamilien spielt der Parameter $\lambda = \frac{\|K\|}{m^2}$ eine wichtige Rolle. Da λ notwendigerweise positiv und ganzzahlig ist, muss insbesondere $\|K\| \geq m^2$ gelten.

Im folgenden nennen wir eine stark universale (n, m, l) -Hashfamilie mit $\lambda = l/m^2$ kurz einen (n, m, λ) -MAC.

Beispiel 21 Betrachten wir den MAC (X, Y, K, H) mit $X = \{0, 1, 2, 3\}$, $Y = \{0, 1, 2\}$, $K = \{0, 1, \dots, 8\}$, wobei H durch folgende Authentikationsmatrix beschrieben wird.

	0	1	2	3
0	0	0	0	0
1	1	1	1	0
2	2	2	2	0
3	0	1	2	1
4	1	2	0	1
5	2	0	1	1
6	0	2	1	2
7	1	0	2	2
8	2	1	0	2

Da in je zwei Spalten jedes Hashwertpaar genau einmal vorkommt, ist (X, Y, K, H) ein $(4, 3, 1)$ -MAC. ◁

Auf Grund von Bemerkung 18 ist klar, dass ein MAC bei gleichverteilten Schlüsseln genau dann die Bedingung $\beta = \frac{1}{m}$ erfüllt, wenn er stark universal ist. Auf Grund von Bemerkung 13 nimmt in diesem Fall auch α den optimalen Wert $\frac{1}{m}$ an.

Der nächste Satz zeigt für primes p eine Konstruktionsmöglichkeit von stark universalen MACs mit dem Parameterwert $\lambda = 1$.

Satz 22 Sei p prim und für $a, b, x \in \mathbb{Z}_p$ sei

$$h_{(a,b)}(x) = ax + b \pmod{p}.$$

Dann ist (X, Y, K, H) mit $X = Y = \mathbb{Z}_p$ und $K = \mathbb{Z}_p \times \mathbb{Z}_p$ ein $(p, p, 1)$ -MAC.

Beweis: Wir müssen zeigen, dass die Größe von $K(x, y, x', y')$ für alle Doppelpaare (x, y, x', y') mit $x \neq x'$ konstant ist. Ein Schlüssel (a, b) gehört genau dann zu dieser Menge, wenn er die beiden Kongruenzen

$$\begin{aligned} ax + b &\equiv_p y, \\ ax' + b &\equiv_p y' \end{aligned}$$

erfüllt. Da dies jedoch nur auf den Schlüssel (a, b) mit

$$\begin{aligned} a &= (y' - y)(x' - x)^{-1} \pmod{p}, \\ b &= y - x(y' - y)(x' - x)^{-1} \pmod{p} \end{aligned}$$

zutrifft, folgt $\|K(x', y', x, y)\| = 1$. ■

Die Hashfunktionen des vorigen Satzes erfüllen wegen $n = m = p$ nicht die Kompressionseigenschaft. Zwar lässt sich n noch geringfügig von p auf $p + 1$ vergrößern, ohne K und T (und damit λ) zu verändern (siehe Übungen), aber eine stärkere Kompression ist mit dem Parameterwert $\lambda = 1$ nicht realisierbar.

Satz 23 Für einen $(n, m, 1)$ -MAC gilt

$$n \leq m + 1$$

und somit $\|K\| = m^2 \geq (n - 1)^2$.

Beweis: O.B.d.A. sei $\|K\| = \{1, \dots, l\}$ und $Y = \{1, \dots, m\}$. Es ist leicht zu sehen, dass eine (bijektive) Umbenennung $\pi : T \rightarrow T$ der Hashwerte in einer einzelnen Spalte der Authentifikationsmatrix A wieder auf einen stark universalen MAC führt. Also können wir weiterhin annehmen, dass die erste Zeile der Authentifikationsmatrix A nur Einsen enthält. Da A stark universal ist, gilt:

- In jeder Zeile $i = 2, \dots, m^2$ kommt höchstens eine Eins vor.
- Jede Spalte j enthält eine Eins in Zeile 1 und $m - 1$ Einsen in den übrigen Zeilen.

Da in den Zeilen $i = 2, \dots, m^2$ insgesamt genau $n(m - 1)$ Einsen vorkommen, folgt

$$\underbrace{\text{Anzahl der Zeilen}}_{m^2} \geq \underbrace{\text{Anzahl der Zeilen mit einer Eins}}_{1+n(m-1)}$$

was $m^2 - 1 \geq n(m - 1)$ bzw. $n \leq m + 1$ impliziert. ■

Der nächste Satz liefert stark universale MACs mit beliebig großem Kompressionsfaktor. Für den Beweis benötigen wir das folgende Lemma.

Lemma 24 Sei A eine $n \times k$ -Matrix über einem endlichen Körper \mathbb{F} , deren Zeilen linear unabhängig sind. Dann besitzt das lineare Gleichungssystem

$$Ax = y$$

für jedes $y \in \mathbb{F}^n$ genau $|\mathbb{F}|^{k-n}$ Lösungen $x \in \mathbb{F}^k$.

Beweis: Siehe Übungen. ■

Satz 25 Sei p prim und für $x = (x_1, \dots, x_n) \in \{0, 1\}^n$ und $k = (k_1, \dots, k_n) \in \mathbb{Z}_p^n$ sei

$$h_k(x) = kx = \sum_{i=1}^n k_i x_i \pmod{p}.$$

Dann ist (X, Y, K, H) mit $X = \{0, 1\}^l - \{0^l\}$, $Y = \mathbb{Z}_p$ und $K = \mathbb{Z}_p^l$ ein $(2^n - 1, p, p^{n-2})$ -MAC.

Beweis: Wir müssen zeigen, dass die Größe von $K(x, y, x', y')$ für alle Doppelpaare (x, y, x', y') mit $x \neq x'$ konstant ist. Es gilt

$$\begin{aligned} k \in K(x, y, x', y') &\Leftrightarrow h_k(x) = y \wedge h_k(x') = y' \\ &\Leftrightarrow k \cdot x = y \wedge k \cdot x' = y'. \end{aligned}$$

Fassen wir $x = x_1 \cdots x_n$ und $x' = x'_1 \cdots x'_n$ zu einer Matrix A zusammen, so ist dies äquivalent zu

$$\begin{pmatrix} x_1 & \cdots & x_n \\ x'_1 & \cdots & x'_n \end{pmatrix} \cdot \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} = \begin{pmatrix} y \\ y' \end{pmatrix}.$$

Da die beiden Zeilen von A verschieden und damit linear unabhängig sind, folgt mit obigem Lemma, dass genau $\|K(x, y, x', y')\| = p^{n-2}$ Schlüssel $k = (k_1, \dots, k_n)$ mit dieser Eigenschaft existieren. ■

Bemerkung 26 Obige Konstruktion liefert einen λ -Wert von $\frac{\|K\|}{m^2} = p^{n-2}$. Durch Erweiterung von X auf eine geeignete Teilmenge $X' \subseteq \mathbb{Z}_p^n$ lässt sich der Textraum von $2^n - 1$ auf $\frac{p^n - 1}{p - 1}$ vergrößern (siehe Übungen). Wie der nächste Satz zeigt, kann der Kompressionsfaktor nicht weiter verbessert werden, ohne einen größeren Wert für λ in Kauf zu nehmen.

Im Beweis des nächsten Satzes benötigen wir folgendes Lemma.

Lemma 27 Seien $b_1, \dots, b_m \in \mathbb{R}^m$. Dann gilt $(\sum_{i=1}^m b_i)^2 \leq m \sum_{i=1}^m b_i^2$.

Beweis: Siehe Übungen. ■

Satz 28 Für einen (n, m, λ) -MAC gilt

$$\lambda \geq \frac{n(m-1) + 1}{m^2}$$

und somit $\|K\| \geq n(m-1) + 1$.

Beweis: O.B.d.A. können wir wieder $\|K\| = \{1, \dots, l\}$ und $Y = \{1, \dots, m\}$ annehmen, und dass die 1. Zeile der Authentikationsmatrix A nur aus Einsen besteht. Für jede Zeile i , $1 \leq i \leq l$, bezeichne x_i die Anzahl der Einsen in Zeile i (also $x_1 = n$). Da in jeder Spalte jeder Hashwert genau λm -mal vorkommt, gilt

$$\sum_{i=1}^l x_i = \lambda n m$$

und

$$\sum_{i=2}^l x_i = \lambda n m - n = n(\lambda m - 1).$$

Nun ist die Anzahl z der Vorkommen von Indexpaaren (j, j') mit $\mathcal{A}[i, j] = \mathcal{A}[i, j'] = 1$ in den Zeilen $i = 2, \dots, l$ gleich

$$z = \sum_{i=2}^l x_i(x_i - 1) = \sum_{i=2}^l x_i^2 - \sum_{i=2}^l x_i = \sum_{i=2}^l x_i^2 - n(\lambda m - 1).$$

Mit obigem Lemma ergibt sich

$$\sum_{i=2}^l x_i^2 \geq \frac{\left(\sum_{i=2}^l x_i\right)^2}{l-1} = \frac{(n(\lambda m - 1))^2}{l-1}.$$

Da andererseits in jedem Spaltenpaar das Hashwert-Paar $(1, 1)$ in genau λ Zeilen vorkommt (genauer: einmal in Zeile 1 und $(\lambda - 1)$ -mal in den Zeilen $i = 2, \dots, l$), und da $n(n - 1)$ solche Spaltenpaare existieren, ist die Anzahl z der Vorkommen von Indexpaaren (j, j') mit $\mathcal{A}[i, j] = \mathcal{A}[i, j'] = 1$ in den Zeilen $i = 2, \dots, l$ gleich

$$z = (\lambda - 1)n(n - 1).$$

Somit ergibt sich

$$\begin{aligned} (\lambda - 1)n(n - 1) &= \sum_{i=2}^l x_i^2 - n(\lambda m - 1) \geq \frac{(n(\lambda m - 1))^2}{l-1} - n(\lambda m - 1) \\ &\Rightarrow ((\lambda - 1)n(n - 1) + n(\lambda m - 1))(\lambda m^2 - 1) \geq (n(\lambda m - 1))^2 \\ &\Rightarrow (\lambda n - n - \lambda + \lambda m)(\lambda m^2 - 1) \geq n(\lambda m - 1)^2 \\ &\Rightarrow -\lambda^2 m^2 + \lambda^2 m^3 \geq \lambda n m^2 + \lambda n - \lambda + \lambda m - 2\lambda n m \\ &\Rightarrow \lambda^2(m^3 - m^2) \geq \lambda(n(m - 1)^2 + m - 1) \\ &\Rightarrow \lambda m^2 \geq n(m - 1) + 1 \\ &\Rightarrow l \geq n(m - 1) + 1 \end{aligned}$$

■

Für den Beweis des nächsten Satzes benötigen wir folgendes Lemma (Beweis siehe Übungen).

Lemma 29 Sei \mathcal{X} eine Zufallsvariable mit endlichen Wertebereich $W(\mathcal{X}) \supseteq \mathbb{R}^+$. Dann gilt $\log E(\mathcal{X}) \geq E(\log \mathcal{X})$.

Satz 30 Für jeden MAC (X, Y, K, H) gilt:

$$\alpha \geq \frac{1}{2^{H(\mathcal{K}) - H(\mathcal{K}|\mathcal{X}, \mathcal{Y})}}.$$

Hierbei sind $\mathcal{X}, \mathcal{Y}, \mathcal{K}$ Zufallsvariablen, die die Verteilungen der Nachrichten, der Hashwerte und der Schlüssel beschreiben.

Beweis: Wir zeigen: $\log \alpha \geq H(\mathcal{K} | \mathcal{X}, \mathcal{Y}) - H(\mathcal{K})$. Es gilt: $\alpha = \max_{x,y} p(x \mapsto y)$, wobei

$$\begin{aligned}
 p(x \mapsto y) &= \text{Prob}_k[h_k(x) = y] \\
 &= \text{Prob}[\mathcal{Y} = y | \mathcal{X} = x] \\
 &=: p_{y|x} \\
 \Rightarrow \alpha &\geq \sum_{x,y} \text{Prob}[\mathcal{X} = x, \mathcal{Y} = y] \cdot p(x \mapsto y) \\
 &= E(\alpha(\mathcal{X}, \mathcal{Y})) \\
 \Rightarrow \log \alpha &\geq \log E(\alpha(\mathcal{X}, \mathcal{Y})) \\
 &\geq E(\log \alpha(\mathcal{X}, \mathcal{Y})) (*) \\
 &= \sum_{x,y} p_{x,y} \cdot \log p_{y|x} \\
 &= \sum_{x,y} p_x \cdot p_{y|x} \cdot \log p_{y|x} \\
 &= -H(\mathcal{Y} | \mathcal{X}) \\
 &\geq H(\mathcal{K} | \mathcal{X}, \mathcal{Y}) - H(\mathcal{K}) (**).
 \end{aligned}$$

Hierbei gilt (*) wegen obigem Lemma und (**) ergibt sich aus

$$\begin{aligned}
 H(\mathcal{K}, \mathcal{Y}, \mathcal{X}) &= H(\mathcal{X}) + H(\mathcal{Y} | \mathcal{X}) + H(\mathcal{K} | \mathcal{X}, \mathcal{Y}) \\
 &= \underbrace{H(\mathcal{K}, \mathcal{X})}_{=H(\mathcal{K})+H(\mathcal{X})} + \underbrace{H(\mathcal{Y} | \mathcal{K}, \mathcal{X})}_{=0}.
 \end{aligned}$$

■