Smashing SMASH

Christian Stöffler

8.6.2005

Gliederung

Hashfunktion H

H bildet einen beliebig großen Input $m \in \{0,1\}^*$ auf einen kleinen Output $H(m) \in \{0,1\}^n$ ab.

Kryptographische Hashfunktion:

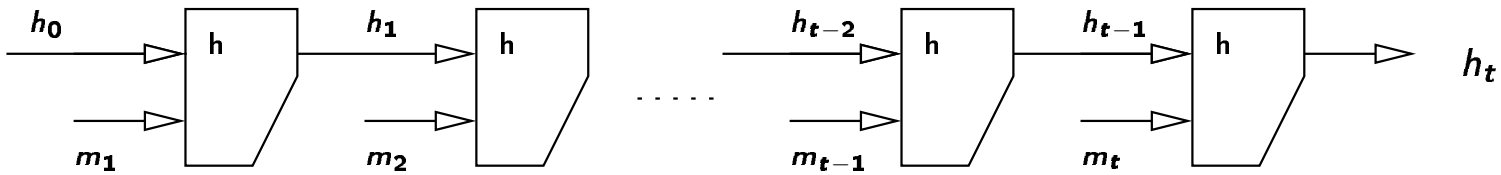
1. **Kollisionsresistenz**: Es ist hart, x und x' zu finden mit $x \neq x'$ und $H(x) = H(x')$
2. **Preimage-Resistenz**: Zu gegebenem $y = H(x)$ ist es hart ein x' zu finden mit $H(x') = y$
3. **2nd Preimage-Resistenz**: Zu gegebenen x und $y = H(x)$ ist es hart, ein $x' \neq x$ zu finden mit $H(x') = y$

Aus der Kollisionsresistenz folgen die beiden anderen Eigenschaften

Komplexität eines brute-force-Angriffs (Geburtstagsangriff): $\Theta(2^{n/2}) \Rightarrow$ Designziel: Es gibt keine Angriffe, die besser als dieser!

Konstruktion Iterierter Hashfunktionen

Mit Hilfe einer **Kompressionsfunktion**
$h\{0,1\}^n \times \{0,1\}^l \rightarrow \{0,1\}^n$ nach folgendem Schema gebaut:



Hashwert $H(m)$ einer Nachricht $m = (m_1, ..., m_t)$ mit $m_i \in \{0,1\}^n$:
$H = h_t$, mit $h_i = h(h_{i-1}, m_i) \forall i = 1..t$, $h_0 = iv$, iv Initialwert

$h : \{0,1\}^n \times \{0,1\}^l \rightarrow \{0,1\}^n$ verkürzt den Input von $n + l$ auf n bits.

Beispiel für Kompressionsfunktion: AES mit Nachrichtenblöcken als Schlüssel

Eigenschaften

- **Vorteil:** Kollisionsresistenz von H kann auf die Kollisionsresistenz der Kompressionsfunktion h zurückgeführt werden
- **Nachteil:** h definiert gleichzeitig 2^l Funktionen von $\{0,1\}^n \rightarrow \{0,1\}^l$ (Abbildung Nachrichtenblöcke neuer interner Zustand h_i) und 2^n Bijektionen von $\{0,1\}^l \rightarrow \{0,1\}^l$ (Abbildung h_{i-1} auf h_i)

$\Rightarrow$ Falls nur einige dieser Funktionen kryptographisch „schwach“ sind, entsteht direkt ein Ansatzpunkt für Angreifer!

Idee von SMASH

Nur eine einzige bijektive Abbildung $f : \{0,1\}^n \rightarrow \{0,1\}^n$

Vermutung: Es dann hart ist, eine solche Konstruktion anzugreifen, falls diese Bijektion „kryptographisch sinnvoll“ gewählt ist.

Kompressionsfunktion $h : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ ist allgemein

$$h_i = h(A, B) = f(A) \oplus B$$

mit den Variablen A und B, die von h_{i-1} und m_i abhängen

$$\Rightarrow (A, B) = e(h_{i-1}, m_i)$$

mit e soll keine Kollisionen verursachen $\Rightarrow$ invertierbar

Kompressionsfunktion

Falls e zu einfach (z.B. $e(h_{i-1}, m_i) = (h_{i-1}, m_i \oplus h_{i-1}) \Rightarrow$ sehr einfach Angriffe insbesondere weil e invertierbar ist

Deswegen: Sei $\theta * m_i,\ \theta \in \mathbb{F}_{2^n},\ \theta \notin \{0,1\}$ die Multiplikation im endlichen Körper $\mathbb{F}_{2^n}$

$$h_0 = f(iv) \oplus iv$$
$$h_i = h(h_{i-1}, m_i) = f(h_{i-1} \oplus m_i) \oplus h_{i-1} \oplus \theta * m_i \qquad \forall i = 1..t$$
$$h_{t+1} = f(h_t) \oplus h_t$$

Ausgabe der Hashfunktion: $H(m) = h_{t+1}$

Eigenschaften

Forward prediction Eigenschaft:
Seien h_{i-1} und h'_{i-1} zwei Inputs für H mit $\alpha = h_{i-1} \oplus h'_{i-1}$. Für beliebiges m_i und $m'_i = m_i \oplus \alpha$ gilt:

$$\begin{aligned} h_i \oplus h'_i &= f(h_{i-1} \oplus m_i) \oplus h_{i-1} \oplus \theta * m_i \oplus f(h'_{i-1} \oplus m'_i) \oplus h'_{i-1} \oplus \theta * m'_i \\ &= \theta * \alpha \oplus \alpha \end{aligned}$$

Hash-Aufbau: Padding

Nachricht $m = (m_1, ..., m_t)$ der Länge $t < 2^{128}$ bit

Ausgabe: 256 bit langer Hashwert

Padding: zuerst ein „1“ -Bit anhängen, anschließend u „0“ -Bits mit:

$$(t + 1) + u \equiv 128 \ mod \ 256$$

Als letztes: String der Länge 128 bit (Länge t)

$\Rightarrow$ genau m Blöcke der Länge 256 bit

Hash-Aufbau: Die Bijektion f

Herz von SMASH: bijektive Abbildung f

Besteht aus mehreren „Runden“: drei H-Runden und einee L-Runde:

$$H_1 \circ H_3 \circ H_2 \circ L \circ H_1 \circ H_2 \circ H_3 \circ L \circ H_2 \circ H_1 \circ H_3 \circ L \circ H_3 \circ H_2 \circ H_1(\cdot)$$

Sei $a = (a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0)$ der 256-bit Input für eine Runde

L-Runden Output:

$$\begin{aligned} a_3 &= a_3 \oplus \mathit{Linksshift}(a_7, 8) \\ a_2 &= a_2 \oplus \mathit{Linksshift}(a_6, 8) \\ a_1 &= a_1 \oplus \mathit{Rechtsshift}(a_5, 8) \\ a_0 &= a_0 \oplus \mathit{Rechtsshift}(a_4, 8) \end{aligned}$$

H-Runden

Drei verschiedene 4×4 bijektive S-Boxen S_j und Linksrotationen R_j

S-Boxen im „bit-slice“ Modus $\Rightarrow$ Parallelität

H_j-Runde berechnen:

$$
\begin{aligned}
(a_7, a_6, a_5, a_4) &= S_j(a_7, a_6, a_5, a_4) \\
a_{i+4} &= a_{i+4} \oplus R_j(a_i, r_i) && \forall i = 0, \ldots, 3 \\
(a_3, a_2, a_1, a_0) &= S_j(a_3, a_2, a_1, a_0) \\
a_i &= a_i \oplus R_j(a_{i+4}, r_{i+4}) && \forall i = 0, \ldots, 3 \\
(a_7, a_6, a_5, a_4) &= S_j(a_7, a_6, a_5, a_4) \\
a_{i+4} &= a_{i+4} \oplus R_j(a_i, r_{i+8}) && \forall i = 0, \ldots, 3 \\
(a_3, a_2, a_1, a_0) &= S_j(a_3, a_2, a_1, a_0) \\
a_i &= a_i \oplus R_j(a_{i+4}, r_{i+12}) && \forall i = 0, \ldots, 3
\end{aligned}
$$

S-Boxen

In S_j für $i = 0, ..., 31$ die vier i-ten Bits als $s_i \in \mathbb{F}_{16}$ auffassen und dem Wert $S_j(s_i)$ zuordnen:

s_i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1:	6	13	12	7	15	1	3	10	8	11	5	0	2	4	14	9
S_2:	1	11	6	0	14	13	5	10	12	2	9	7	3	8	15	4
S_3:	4	2	9	12	8	1	14	7	15	5	0	11	6	10	3	13

Rotationen

R_j rotiert a_i um eine bestimmt Anzahl bits nach links

Anzahl der Bits r_i wie folgt:

R_j	r_0	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8	r_9	r_{10}	r_{11}	r_{12}	r_{13}	r_{14}	r_{15}
R_1:	19	18	17	7	1	7	26	20	0	16	20	5	28	2	20	4
R_2:	22	29	12	4	18	2	13	29	26	20	16	29	18	4	10	9
R_3:	4	21	19	5	24	20	12	16	14	30	3	4	23	15	13	12

Aufbau einer Kollision

Wahl von $\theta \in \mathbb{F}_{2^n}$ mit: $(1+\theta)$ hat Ordnung 3

Seien $z_1, z_2, z_3, x \in \mathbb{F}_{2^n}$ beliebig. Berechne $h_0 = f(iv) \oplus iv$ sowie:

$$m_1 = z_1 \oplus x \qquad f_1 = f(m_1 \oplus h_0)$$
$$m_2 = z_2 \oplus a \qquad f_2 = f(m_2 \oplus h_1)$$
$$m_3 = z_3 \oplus (1+\theta) * a \qquad f_3 = f(m_3 \oplus h_2)$$

$$m_4 = z_1 \oplus f_1 \oplus f_2 \oplus f_3 \oplus \theta * (m_1 \oplus m_2 \oplus m_3) \oplus a * (1+\theta)^2 \oplus x$$
$$a = f_1 + f(m_1 \oplus h_0 \oplus x) \oplus \theta * x$$

Bemerkung: Falls $x = 0$ dann ist auch $a = 0$.

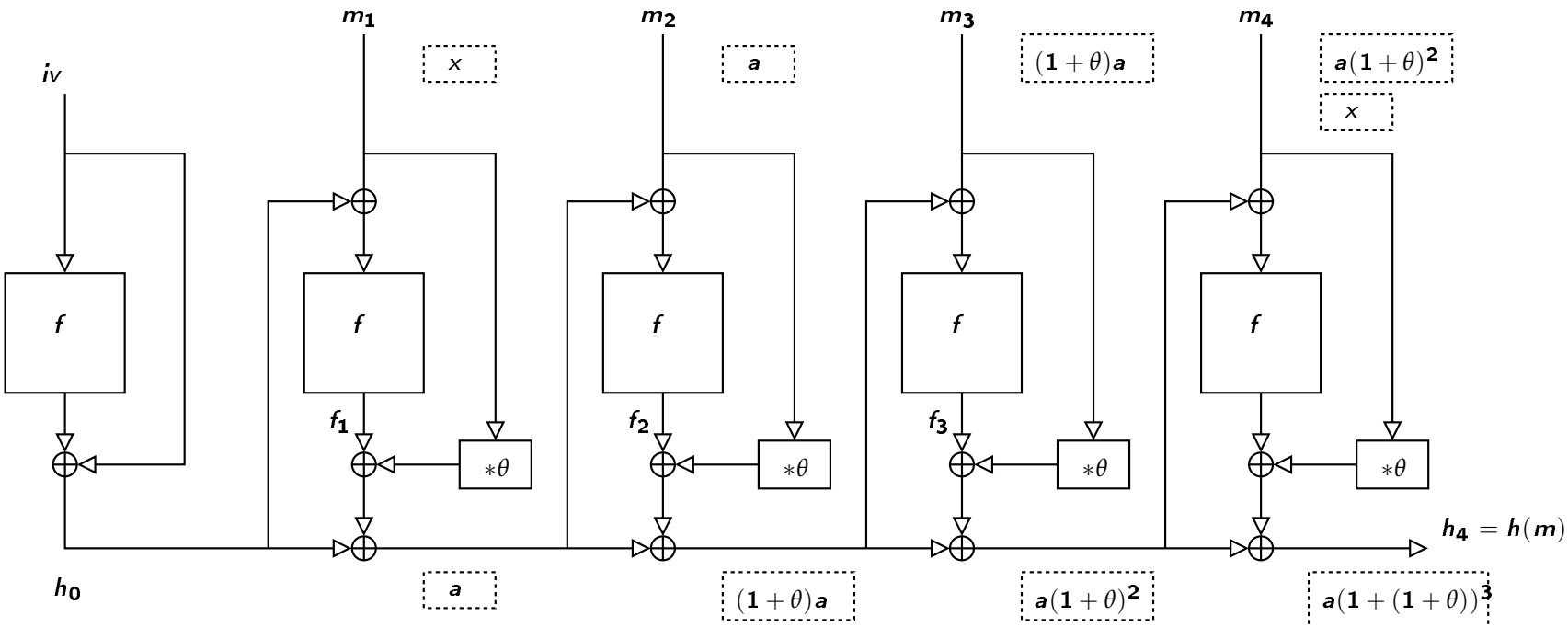
$\Rightarrow$ Alle Nachrichten $m = m_1 m_2 m_3 m_4$ haben gleichen Hashwert

Differenzieller Angriff

Eine Nachricht mit $x = 0$ und eine mit $x \neq 0$

forward prediction Eigenschaft $\Rightarrow$ Differenz a:

$$a = h_{i-1} \oplus h'_{i-1} \Rightarrow h_i \oplus h'_i = a \oplus \theta * a$$



Aufbau der ersten Nachricht

Wichtig: letzter Nachrichtenblock m_4 wird so gewählt, dass:

Input für f in letzter Iteration = Input für f in erster Iteration!

$$
\begin{aligned}
m_4 \oplus h_3 &= m_1 \oplus h_0 \\
\Leftrightarrow m_4 &= m_1 \oplus h_0 \oplus h_3 \\
&= m_1 \oplus h_0 \oplus f_3 \oplus h_2 \oplus \theta * m_3 \\
&= m_1 \oplus h_0 \oplus f_3 \oplus f_2 \oplus h_1 \oplus \theta * m_2 \oplus \theta * m_3 \\
&= m_1 \oplus h_0 \oplus f_3 \oplus f_2 \oplus f_1 \oplus h_0 \oplus \theta * m_1 \oplus \theta * m_2 \oplus \theta * m_3 \\
&= m_1 \oplus f_1 \oplus f_2 \oplus f_3 \oplus \theta * (m_1 \oplus m_2 \oplus m_3) \\
&= m_1 \oplus f_1 \oplus f_2 \oplus f_3 \oplus \theta * (m_1 \oplus m_2 \oplus m_3) \oplus a * (1 + \theta)^2 \\
&= z_1 \oplus f_1 \oplus f_2 \oplus f_3 \oplus \theta * (m_1 \oplus m_2 \oplus m_3) \oplus a * (1 + \theta)^2 \oplus x
\end{aligned}
$$

Aufbau der zweiten Nachricht

Für m' mit $x \neq 0$: letzter Nachrichtenblock wie m_4 oben, sodass:

Differenz ist $(1+\theta)^2 * a \oplus x$

$\Rightarrow$ gleiche Inputs für f in erster und letzter Iteration

$\Rightarrow$ Outputs mit Differenz $a \oplus \theta * x$:

$$
\begin{aligned}
h_1 &= f(h_0 \oplus m_1) \oplus \theta * m_1 \oplus h_0 \\
h_1' &= f(h_0 \oplus m_1 \oplus x) \oplus \theta * (m_1 \oplus x) \oplus h_0 \\
a &= h_1 \oplus h_1' \\
&= f(h_0 \oplus m_1) \oplus f(h_0 \oplus m_1 \oplus x) \oplus \theta * x \\
\Leftrightarrow & f(h_0 \oplus m_1) \oplus f(h_0 \oplus m_1 \oplus x) = a \oplus \theta * x
\end{aligned}
$$

Differenz der Hashwerte

$$
\begin{aligned}
&(f(m_1 \oplus h_0) \oplus h_3 \oplus \theta * m_4) \\
&\oplus (f(m_1 \oplus h_0 \oplus x) \oplus h_3 \oplus a * (1+\theta)^2 \oplus \theta * (m_4 \oplus a * (1+\theta)^2 \oplus x)) \\
&= f(m_1 \oplus h_0) \oplus f(m_1 \oplus h_0 \oplus x) \oplus a * (1+\theta)^2 \oplus \theta * a * (1+\theta)^2 \oplus \theta * x \\
&= a \oplus \theta * x \oplus a * (1+\theta)^2 * (1+\theta) \oplus \theta * x \\
&= a \oplus a * (1+\theta)^3 \\
&= a * (1 \oplus (1+\theta)^3) \\
&= a * (1 \oplus 1) \\
&= 0
\end{aligned}
$$

da $(1+\theta)$ die Ordnung 3 hat.

$\Rightarrow$ Kollision für diese eingeschränkte SMASH-Variante

Erweiterungen

Kollisionen für Nachrichten der Länge l:
problemlos, falls $(1 + \theta)$ Ordnung $l - 1$ hat

SMASH-256: Ordnung $(2^{256} - 1)/5$
SMASH-512: Ordnung $2^{512} - 1$

Idee: **forward prediction** mehrfach ausnutzen:

Nachrichtenpaare m, m', Differenz x mehr als zweimal einfügen!

$\Rightarrow$ In all diesen Output-Blöcken: Differenz $(a \oplus \theta * x)$

$\Rightarrow$ Es kann fast jede Differenz in h_t erzeugt werden!

Für Kollision: Differenz in h_t und h'_t muss
$a * q(\theta) = a * 0 = 0 \ mod \ q(\theta)$ sein

Definitionen

- Sei d eine Funktion, die nur für zwei Werte definiert ist: $d(0) = 0$ und $d(x) = 1$.
- Sei Δm_i die Differenz der Nachrichtenblöcke m_i und m'_i.
- Sei $\delta_1 = 1$ und für $i = 2, ..., t$ sei δ_i wie folgt definiert:

$$\delta_i = d(\Delta m_i \oplus \sum_{j=1}^{i-1} (1+\theta)^{i-j-1} * a * \delta_j) \tag{1}$$

$\Rightarrow$ Konstruktion zweier Nachrichten m, m' mit Differenzen wie oben **und** Differenz von h_t und h'_t:

$$a * \sum_{i=1}^{t} (1+\theta)^{t-i} * \delta_i \tag{2}$$

Berechnen der Nachrichtenblöcke

- m_1 ist immer beliebig
- Falls $\delta_i = 0$ dann kann m_i beliebig gewählt werden
- Falls $\delta_i = 1$ und $i > 1$ dann muss $m_i = h_{i+1} \oplus m_1 \oplus h_0$ sein

$\mathbb{F}_{2^{256}}$ ist isomorph zu $\frac{\mathbb{F}_q}{q(\theta)}$ ist mit irreduziblem Polynom

$$\begin{aligned} q(\theta) &= \theta^{256} + \theta^{16} + \theta^3 + \theta + 1 \\ &= (1+\theta) + (1+\theta)^2 + (1+\theta)^3 + (1+\theta)^{16} + (1+\theta)^{256} \end{aligned}$$

$\Rightarrow$ In (2) ist $\delta_i = 1$ für $i = 1, 241, 254, 255, 257$ und $\delta_i = 0$ für alle anderen $i \leq t = 257$

Was macht man mit diesen δ_i ?

$\Rightarrow$ (1) nach den Δm_i auflösen:

$$\Delta m_1 = x$$

$$\Delta m_i = (1+\theta)^{i-2} * a \qquad \forall 1 < i \leq 240$$

$$\Delta m_{241} = x \oplus (1+\theta)^{239} * a$$

$$\Delta m_i = (1+\theta)^{i-2} * a \oplus (1+\theta)^{i-242} * a \qquad \forall 241 < i < 254$$

$$\Delta m_{254} = x \oplus (1+\theta)^{252} * a \oplus (1+\theta)^{12} * a$$

$$\Delta m_{255} = x \oplus (1+\theta)^{253} * a \oplus (1+\theta)^{13} * a \oplus a$$

$$\Delta m_{256} = (1+\theta)^{254} * a \oplus (1+\theta)^{14} * a \oplus (1+\theta) * a \oplus a$$

$$\Delta m_{257} = x \oplus (1+\theta)^{255} * a \oplus (1+\theta)^{15} * a \oplus (1+\theta)^{2} * a \oplus (1+\theta) * a$$

$\Rightarrow$ x beliebige Differenz für die Nachrichtenblöcke

$\Rightarrow$ 253 der Blöcke beliebig, 4 durch Angriff festgelegt!

Bemerkungen

- Auflösen der Gleichungen z.B. mit Maple
- Die Nachrichten des verallgemeinerten Angriffs: keine gültigen Inputs mehr nach den Spezifikationen von SMASH
- Angriff unabhängig von der Wahl der Bijektion f

$\Rightarrow$ möglicher Ansatz: in jeder Iteration eine andere Bijektion f_i?

Beispiel für Kollision:

<html>You owe me 1000.00€<\html>
und
<html>You owe me 1000000€<\html>