

RSA Full Domain Hash (RSA-FDH) Signaturen

Signatur RSA-FDH

Sei $H : \{0, 1\}^* \rightarrow \mathbb{Z}_N^*$ ein Random-Oracle.

① **Gen:** $(N, e, d) \leftarrow \text{GenRSA}(1^n)$ mit $pk = (N, e)$ und $sk = (N, d)$.

② **Sign:** Für eine Nachricht $m \in \{0, 1\}^*$ berechne

$$\sigma \leftarrow H(m)^d \bmod N.$$

③ **Vrfy:** Für (m, σ) überprüfe

$$\sigma^e \stackrel{?}{=} H(m) \bmod N.$$

Anmerkung:

- RSA-FDH entspricht Hashed-RSA mit einem Random Oracle als Hashfunktion.

CMA-Sicherheit von RSA-FDH

Satz CMA-Sicherheit von RSA-FDH

Unter der RSA-Annahme und für ein Random-Oracle H ist RSA-FDH ein CMA-sicheres Signaturverfahren.

Beweisskizze:

- Sei $\Pi = \text{RSA-FDH}$ und $\epsilon = \text{Ws}[\text{Forge}_{\mathcal{A},\Pi}(n) = 1]$.
- OBdA gelten folgende Annahmen für die Orakelanfragen von \mathcal{A} :
 - 1 \mathcal{A} fragt verschiedene x_1, \dots, x_q an $H(\cdot)$.
 - 2 Bevor \mathcal{A} Anfrage m an $\text{Sign}_{sk}(\cdot)$ stellt, fragt er $H(m)$ an.
 - 3 Für eine Fälschung (m, σ) hat \mathcal{A} zuvor Anfrage $H(m)$ gestellt.
- Konstruieren RSA-Invertierer \mathcal{A}' mittels \mathcal{A} .

Beweis der CMA-Sicherheit von RSA-FDH

Algorithmus RSA-Invertierer \mathcal{A}'

EINGABE: $N, e, y = x^e \bmod N$

1 Wähle $j \in_R \{1, \dots, q\}$.

2 $(m, \sigma) \leftarrow \mathcal{A}^{\text{Sign}_{sk}(\cdot)}(N, e)$.

▶ Beantworte Orakelanfragen m_i an $H(\cdot)$ konsistent mit

$$H(m_i) = \begin{cases} \sigma_i^e \bmod N & \text{für ein selbst gewähltes } \sigma \in_R \mathbb{Z}_N^* \text{ für } i \neq j \\ y & \text{sonst} \end{cases}$$

▶ Beantworte Orakelanfragen m_i an $\text{Sign}_{sk}(\cdot)$ mit

$$\text{Sign}_{sk}(H(m_i)) = \begin{cases} \sigma_i & \text{für } i \neq j \\ \text{Abbruch} & \text{sonst} \end{cases}$$

3 Falls $m = m_j$ und $\sigma^e = y \bmod N$, setze $x \leftarrow \sigma$.

AUSGABE: x

• Unter der RSA-Annahme gilt $\text{negl}(n) \geq \text{Ws}[\mathcal{A}'(N, e, x^e) = x]$
 $= \text{Ws}[m = m_j] \cdot \text{Ws}[\text{Forge}_{\mathcal{A}, \Pi}(n) = 1] = \frac{\epsilon(n)}{q}$.

• Damit ist $\epsilon(n) \leq q \cdot \text{negl}(n)$ vernachlässigbar für polynomielles q .

Hash-and-Sign Paradigma

Ziel: Signaturen für Nachrichten beliebiger Länge

- Starten mit Signaturverfahren Π für $m \in \{0, 1\}^n$.
- Verwenden Hashfunktion $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$.
- Unterschreiben Hashwerte statt der Nachrichten.

Definition Hash-and-Sign Paradigma

Sei $\Pi = (\text{Gen}, \text{Sign}, \text{Vrfy})$ und $\Pi_H = (\text{Gen}_H, H)$ eine Hashfunktion.

- 1 **Gen'**: $(pk, sk) \leftarrow \text{Gen}(1^n)$, $s \leftarrow \text{Gen}_H(1^n)$.
Ausgabe $pk' = (pk, s)$ und $sk' = (sk, s)$.
- 2 **Sign'**: Für eine Nachricht $m \in \{0, 1\}^*$ berechne
$$\sigma \leftarrow \text{Sign}_{sk}(H_s(m)).$$
- 3 **Vrfy'**: Für eine Nachricht $m \in \{0, 1\}^*$ mit Signatur σ prüfe
$$\text{Vrfy}_{pk}(H_s(m), \sigma) \stackrel{?}{=} 1.$$

Intuition: Fälschung impliziert Fälschung in Π oder Kollision in H .

Sicherheit von Hash-and-Sign

Satz Sicherheit des Hash-and-Sign Paradigmas

Sei Π CMA-sicher und Π_H kollisionsresistent. Dann ist das Hash-and-Sign Signaturverfahren Π' CMA-sicher.

Beweis:

- Sei \mathcal{A} ein Angreifer für Hash-and-Sign Π' mit Ausgabe (m, σ) .
- Sei $Q = \{m_1, \dots, m_q\}$ die Menge der von \mathcal{A} an das Signierorakel $Sign_{sk}(\cdot)$ gestellten Anfragen. Es gilt $m \notin Q$.
- Sei $coll$ das Ereignis, dass $m_i \in Q$ mit $H_s(m_i) = H_s(m)$.
- Dann gilt $W_s[Forge_{\mathcal{A}, \Pi'}(n) = 1]$
$$= W_s[Forge_{\mathcal{A}, \Pi'}(n) = 1 \wedge coll] + W_s[Forge_{\mathcal{A}, \Pi'}(n) = 1 \wedge \overline{coll}]$$

$$\leq W_s[coll] + W_s[Forge_{\mathcal{A}, \Pi'}(n) = 1 \wedge \overline{coll}]$$
- Wir zeigen nun, dass beide Summanden vernachlässigbar sind.

Algorithmus für Kollisionen

Beweis: $Ws[coll] \leq \text{negl}(n)$

- Konstruieren mittels \mathcal{A} einen Algorithmus C für Kollisionen.

Algorithmus C

EINGABE: s

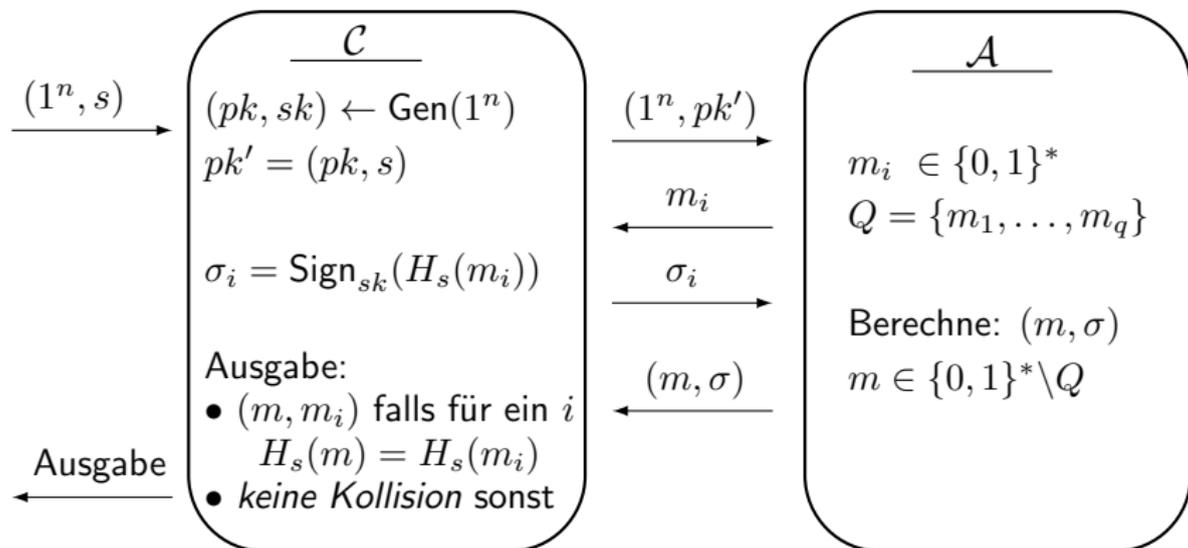
- 1 Berechne $(pk, sk) \leftarrow \text{Gen}(1^n)$. Setze $pk' \leftarrow (pk, s)$.
- 2 $(m, \sigma) \leftarrow \mathcal{A}(pk')$. Auf Orakelanfrage $m_i \in \{0, 1\}^*$, antworte mit $\sigma_i \leftarrow \text{Sign}_{sk}(H_s(m_i))$.

AUSGABE: $\begin{cases} (m, m_i) & \text{falls } H_s(m) = H_s(m_i) \text{ für ein } m_i \\ \text{keine Kollision} & \text{sonst} \end{cases}$.

- Es gilt $Ws[coll] = Ws[\text{HashColl}_{C, \Pi_H}(n) = 1]$.
- Aus der Kollisionsresistenz von H folgt

$$Ws[\text{HashColl}_{C, \Pi_H}(n) = 1] \leq \text{negl}(n).$$

Algorithmus \mathcal{C} für Kollisionen



Fälschen von Signaturen in Π

Beweis: $Ws[Forge_{\mathcal{A},\Pi'}(n) = 1 \wedge \overline{coll}] \leq \text{negl}(n)$

- Konstruieren mittels \mathcal{A} einen Angreifer \mathcal{A}' für Π .

Algorithmus \mathcal{A}'

EINGABE: pk , Zugriff auf Signierorakel $Sign_{sk}(\cdot)$

- 1 Berechne $s \leftarrow Gen_H(1^n)$. Setze $pk' = (pk, s)$.
- 2 $(m, \sigma) \leftarrow \mathcal{A}(pk')$. Beantworte Orakelanfrage $m_i \in \{0, 1\}^*$ mit Ausgabe $\sigma_i \leftarrow Sign_{sk}(H_s(m_i))$ des Signierorakels.
- 3 Setze $m' \leftarrow H_s(m)$.

AUSGABE: (m', σ)

- Falls (m, σ) gültig ist für Π' , so ist $(m', \sigma) = (H_s(m), \sigma)$ gültig für Π .
- Ereignis \overline{coll} bedeutet, dass $m' \neq H_s(m_i)$ für alle Anfragen $H_s(m_i)$.
- Damit gilt $Ws[Forge_{\mathcal{A},\Pi'}(n) \wedge \overline{coll}] = Ws[Forge_{\mathcal{A}',\Pi}(n) = 1]$.
- Aus der CMA-Sicherheit von Π folgt

$$Ws[Forge_{\mathcal{A}',\Pi}(n) = 1] \leq \text{negl}(n).$$

Algorithmus \mathcal{A} für Fälschungen

