

Alle Angaben ohne Gewähr. Keine Garantie auf Vollständigkeit oder Richtigkeit.

1	Einführung	2
1.1	Ziel von Kryptographischen Verfahren	2
1.2	Informelle Definition von Signaturen	2
1.3	Digitale Signaturen	2
1.3.1	Definition	2
1.3.2	Correctness	2
1.4	Sicherheitsdefinitionen	2
1.4.1	Angreifermodelle	2
1.4.2	Angreiferziele	2
1.5	EUFCMA-Sicherheitsexperiment	3
1.5.1	Visualisierung: EUFCMA-Sicherheitsexperiment	3
1.5.2	Definition: Vernachlässigbarkeit	3
1.5.3	Definition: EUFCMA	3
1.6	EUFCMA-Sicherheitsexperiment	4
1.6.1	Visualisierung: EUFCMA-Sicherheitsexperiment	4
1.6.2	Definition: EUFCMA	4

1 Einführung

1.1 Ziel von Kryptographischen Verfahren

Kryptographische Verfahren sollen **Authentizität** (Dokument wurde von einer bestimmten Person signiert) und **Integrität** (Dokument wurde nicht verändert) sicherstellen.

1.2 Informelle Definition von Signaturen

- **asymmetrische** Verfahren
- Schlüsselpaar (pk, sk)
- Nachricht m wird mit sk signiert und erzeugt Signatur σ
- Mit pk kann überprüft werden, ob eine Signatur σ gültig für eine Nachricht m ist

1.3 Digitale Signaturen

1.3.1 Definition

Ein digitales Signaturverfahren für einen Nachrichtenraum \mathcal{M} ist ein Tupel $\Sigma = (Gen, Sign, Vfy)$ von probabilistischen Polyzeit (PPT) Algorithmen:

- $Gen(1^k) \rightarrow (pk, sk)$
- $Sign(sk, m) \rightarrow \sigma, m \in \mathcal{M}$
- $Vfy(pk, m, \sigma) \in \{0, 1\}$

1.3.2 Correctness

Correctness ("Das Verfahren funktioniert"): $\forall (pk, sk) \leftarrow Gen(1^k) \forall m \in \mathcal{M} : Vfy(pk, m, Sign(sk, m)) = 1$

1.4 Sicherheitsdefinitionen

Sicherheit besteht aus einem **Angreifermodell** (was kann der Angreifer tun, welche Angriffsmöglichkeiten stehen zur Verfügung) und einem **Angreiferziel** (was muss der Angreifer tun, um das Verfahren zu brechen).

1.4.1 Angreifermodelle

1. no-message attack (NMA)
 - Angreifer erhält nur pk
2. **non-adaptive chosen-message attack (naCMA)**
 - Angreifer wählt m_1, \dots, m_q
 - Angreifer erhält **danach** pk und Signaturen $\sigma_1, \dots, \sigma_q$
3. **(adaptive) chosen-message attack (CMA)**
 - Angreifer erhält pk
 - Angreifer wählt dann (adaptiv) m_1, \dots, m_q und erhält Signaturen $\sigma_1, \dots, \sigma_q$
 - Adaptiv: Angreifer darf Wahl von m_i abhängig von vorherigen σ_j ($j < i$) und pk machen

1.4.2 Angreiferziele

1. Universal Unforgeability (UUF)
 - Nachricht m wird zufällig gewählt
 - Angreifer muss m signieren

2. Existential Unforgeability (EUF)

- Angreifer kann Nachricht m beliebig wählen und diese signieren

In den **Sicherheitsdefinitionen** werden **Angreiferziel** und **Angreifermodell** kombiniert, z.B.

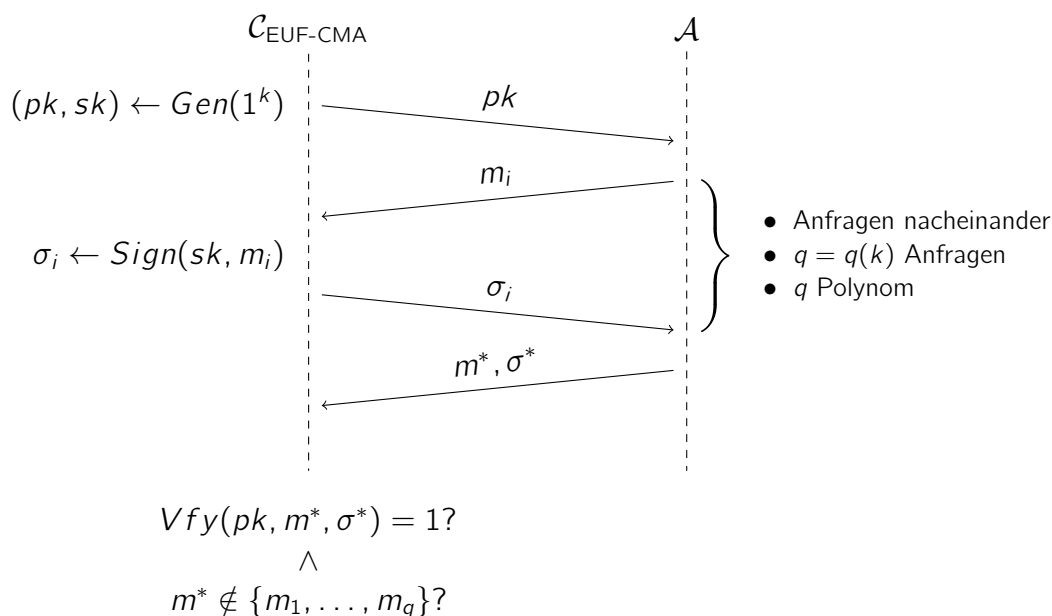
- EUF-CMA
- EUF-naCMA

1.5 EUF-CMA-Sicherheitsexperiment

Bei Sicherheitsexperimenten spielt ein Angreifer \mathcal{A} gegen einen Challenger \mathcal{C} . \mathcal{A} gewinnt, falls er die Sicherheit des Verfahrens bricht.

\mathcal{A} muss dabei mit einer nicht vernachlässigbaren Wahrscheinlichkeit eine gültige Signatur erzeugen können, ohne den Schlüssel sk zu kennen.

1.5.1 Visualisierung: EUF-CMA-Sicherheitsexperiment



\mathcal{A} gewinnt, falls $Vfy(pk, m^*, \sigma^*) = 1$ **und** $m^* \notin \{m_1, \dots, m_q\}$

1.5.2 Definition: Vernachlässigbarkeit

Eine Funktion $negl : \mathbb{N} \rightarrow [0, 1]$ ist *vernachlässigbar*, wenn

$$\forall c \in \mathbb{N} \exists k_0 \in \mathbb{N} \forall k \geq k_0 : negl(k) < \frac{1}{k^c}$$

1.5.3 Definition: EUF-CMA

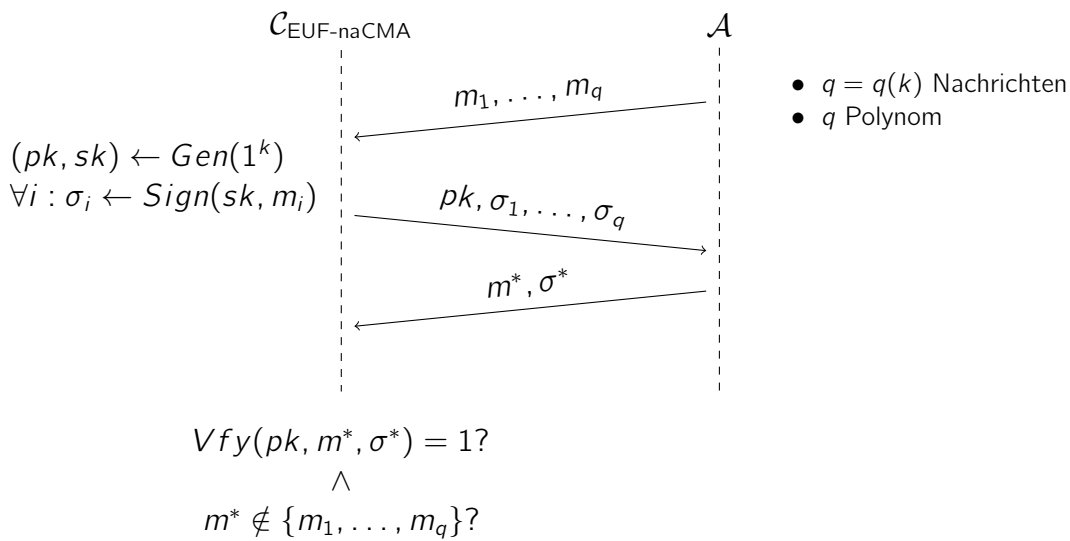
Ein digitales Signaturverfahren $\Sigma = (\text{Gen}, \text{Sign}, \text{Vfy})$ ist *EUF-CMA-sicher*, wenn für alle PPT \mathcal{A} gilt, dass

$$\begin{aligned}
 & \Pr[\mathcal{A} \text{ gewinnt EUF-CMA-Experiment}] \\
 &= \Pr[\mathcal{A}^{\mathcal{C}_{\text{EUF-CMA}}}(pk) = (m^*, \sigma^*) : Vfy(pk, m^*, \sigma^*) = 1 \wedge m^* \notin \{m_1, \dots, m_q\}] \\
 &\leq negl(k)
 \end{aligned}$$

für eine im Sicherheitsparameter k vernachlässigbare Funktion $negl$.

1.6 EUF-naCMA-Sicherheitsexperiment

1.6.1 Visualisierung: EUF-naCMA-Sicherheitsexperiment



\mathcal{A} gewinnt, falls $\text{Vfy}(pk, m^*, \sigma^*) = 1$ **und** $m^* \notin \{m_1, \dots, m_q\}$

1.6.2 Definition: EUF-naCMA

Ein digitales Signaturverfahren $\Sigma = (\text{Gen}, \text{Sign}, \text{Vfy})$ ist *EUF-naCMA-sicher*, wenn für alle PPT \mathcal{A} gilt, dass

$$\begin{aligned}
 & \Pr[\mathcal{A} \text{ gewinnt EUF-naCMA-Experiment}] \\
 &= \Pr[\mathcal{A}^{\mathcal{C}_{\text{EUF-naCMA}}} = (m^*, \sigma^*) : \text{Vfy}(pk, m^*, \sigma^*) = 1 \wedge m^* \notin \{m_1, \dots, m_q\}] \\
 &\leq \text{negl}(k)
 \end{aligned}$$

für eine im Sicherheitsparameter k vernachlässigbare Funktion *negl*.