Authentisierung und Verschlüsselung [WIP]

Sommersemester 2023

mail@nilslambertz.de
nilslambertz

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

mail@nilslambertz.de
nilslambertz

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 $m_1, \ldots, m_q$
   - Angreifer erhält **danach** pk und Signaturen $\sigma_1, \ldots, \sigma_q$
3. **(adaptive) chosen-message attack (CMA)**
   - Angreifer erhält pk
   - Angreifer wählt dann (adaptiv) $m_1, \ldots, m_q$ und erhält Signaturen $\sigma_1, \ldots, \sigma_q$
   - 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

mail@nilslambertz.de
nilslambertz

2. **Existential Unforgeablility (EUF)**
   - Angreifer kann Nachricht m beliebig wählen und diese signieren

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

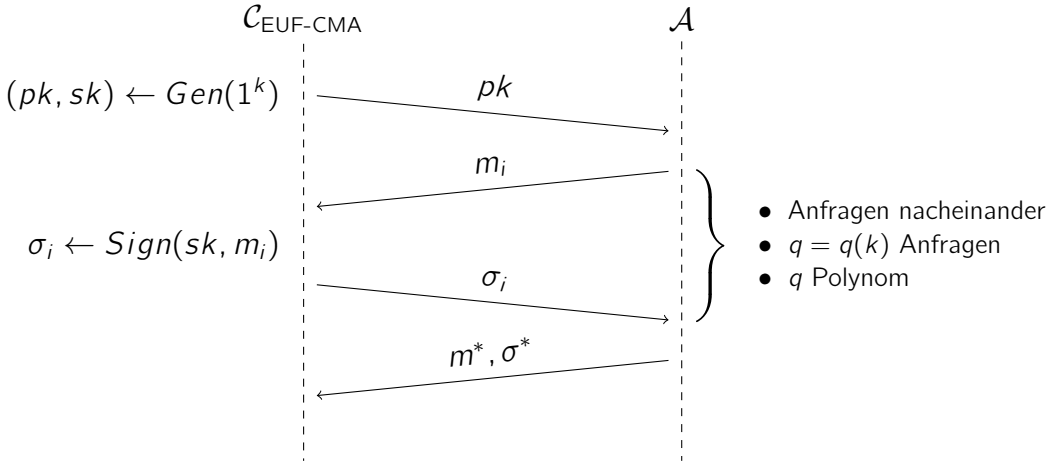
- EUF-CMA
- EUF-naCMA

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



$$Vfy(pk, m^*, \sigma^*) = 1?$$
$$\wedge$$
$$m^* \notin \{m_1, \ldots, m_q\}?$$

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

1.5.2 Definition: Vernachlässigbarkeit

Eine Funktion $negl : \mathbb{N} \to [0, 1]$ 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 $\Sigma = (Gen, Sign, Vfy)$ ist *EUF-CMA-sicher*, wenn für alle PPT $\mathcal{A}$ gilt, dass

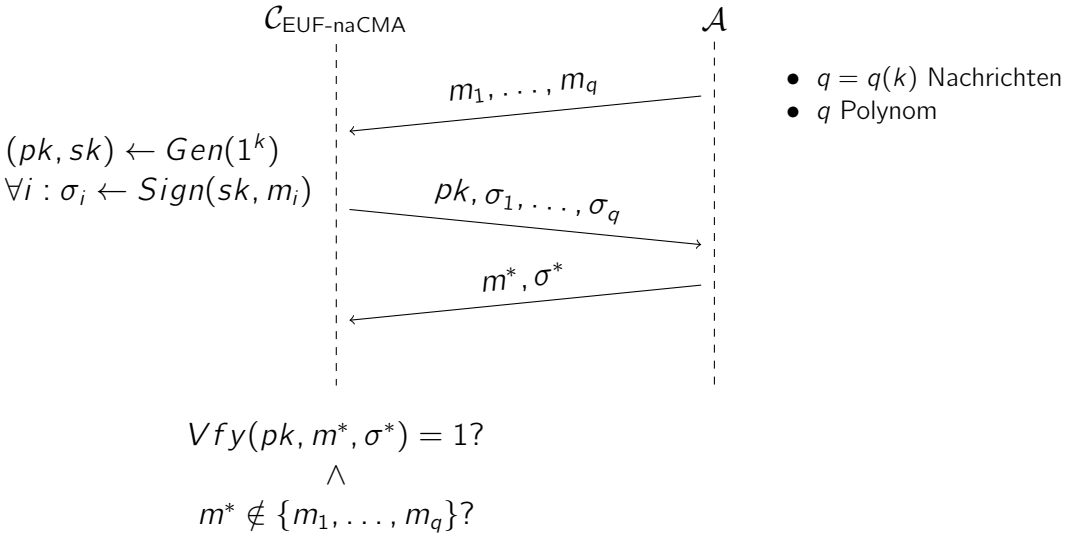
$$\begin{aligned}&\Pr[\mathcal{A} \text{ gewinnt EUF-CMA-Experiment}]\\ &= \Pr[\mathcal{A}^{\mathcal{C}_{\text{EUF-CMA}}}(pk) = (m^*, \sigma^*) : Vfy(pk, m^*, \sigma^*) = 1 \wedge m^* \notin \{m_1, \ldots, m_q\}]\\ &\leq negl(k)\end{aligned}$$

für eine im Sicherheitsparameter k vernachlässigbare Funktion $negl$.

mail@nilslambertz.de
nilslambertz

1.6 EUF-naCMA-Sicherheitsexperiment

1.6.1 Visualisierung: EUF-naCMA-Sicherheitsexperiment



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

1.6.2 Definition: EUF-naCMA

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

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

für eine im Sicherheitsparameter k vernachlässigbare Funktion $negl$.

1.7 Einmalsignaturen

- Signaturen, die viele Nachrichten signieren können
- Vorstufe: Signaturen, die nur **eine** Nachricht **sicher** signieren können (**Einmalsignaturen**)
- für jeden *public key* sollte nur eine einzige Signatur ausgestellt werden, sonst evtl. unsicher

1.7.1 Sicherheitsbegriffe für Einmalsignaturen

Analog zum vorherigen Kapitel definieren wir **EUF-1-CMA** und **EUF-1-naCMA** für Einmalsignaturen.

1.7.2 Beziehungen zwischen Sicherheitsdefinitionen