

Vorlesung Sicherheit

Dennis Hofheinz

ITI, KIT

29.05.2017

1 Symmetrische Authentifikation von Nachrichten

- Ziel
- Sicherheit
- Konstruktionen
- MACs aus PRFs
- Konkrete Konstruktionen und HMAC
- Zusammenfassung

2 Asymmetrische Authentifikation von Nachrichten

- Motivation
- Sicherheit
- RSA als Signaturschema

1 Symmetrische Authentifikation von Nachrichten

■ Ziel

- Sicherheit
- Konstruktionen
- MACs aus PRFs
- Konkrete Konstruktionen und HMAC
- Zusammenfassung

2 Asymmetrische Authentifikation von Nachrichten

- Motivation
- Sicherheit
- RSA als Signaturschema

- Authentifizierte Übermittlung auf unauthentifiziertem Kanal:

Alice $\xleftarrow{(M,\sigma)}$ Bob

- Nachricht M soll vor Veränderungen geschützt werden
- Idee: Sende „Unterschrift“ σ mit Nachricht
- Anforderungen:
 - Bob muss σ (aus/für Nachricht M) berechnen können
 - Alice muss σ (zusammen mit M) verifizieren können
 - Außenseiter soll kein gültiges σ für neues M erzeugen können

- Annahme: Alice und Bob besitzen gemeinsames Geheimnis K

Alice _{K} $\xleftarrow{(M,\sigma)}$ Bob _{K}

- Signieren: $\sigma \leftarrow \text{Sig}(K, M)$
- Verifizieren: $\text{Ver}(K, M, \sigma) \in \{0, 1\}$
- Korrektheit: $\text{Ver}(K, M, \sigma) = 1$ für alle K, M und $\sigma \leftarrow \text{Sig}(K, M)$
- Wird „MAC“ (Message Authentication Code) genannt

1 Symmetrische Authentifikation von Nachrichten

- Ziel
- **Sicherheit**
- Konstruktionen
- MACs aus PRFs
- Konkrete Konstruktionen und HMAC
- Zusammenfassung

2 Asymmetrische Authentifikation von Nachrichten

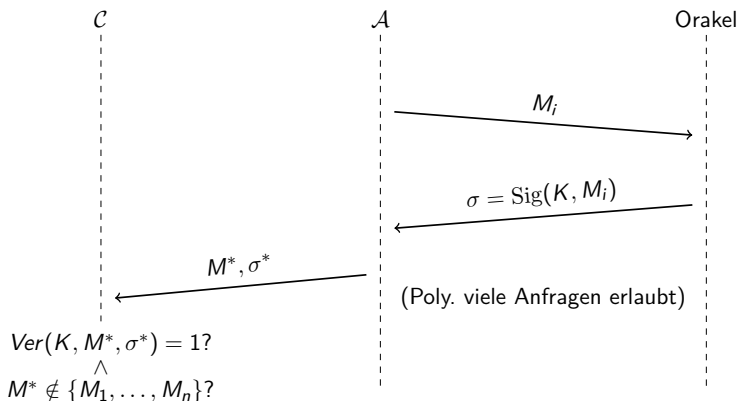
- Motivation
- Sicherheit
- RSA als Signaturschema

- **Diskussion:** Wünschenswerte Sicherheitseigenschaften?

- Schema EUF-CMA-sicher \Leftrightarrow kein PPT-Angreifer \mathcal{A} gewinnt folgendes Spiel nicht-vernachlässigbar oft:
 - 1 \mathcal{A} erhält Zugriff auf ein $\text{Sig}(K, \cdot)$ -Orakel
 - 2 \mathcal{A} gibt Ausgabe (M^*, σ^*)
 - 3 \mathcal{A} gewinnt, wenn $\text{Ver}(K, M^*, \sigma^*) = 1$ und M^* „frisch“ (d.h. M^* ungleich aller Nachrichten, die \mathcal{A} an das Orakel gesendet hat)

MACs – EUF-CMA: Spiel

- Herausforderer \mathcal{C} wählt Schlüssel K zufällig.
- \mathcal{C} stellt $\text{Sig}(K, \cdot)$ -Orakel für \mathcal{A} bereit (aber kein Ver-Orakel!).



- Modelliert passive Angriffe (\mathcal{A} erhält keinen Ver-Zugriff)
 - Für viele Verfahren (z.B. bei eindeutigem σ) äquivalent zu Definition mit Ver-Orakel für \mathcal{A}
 - Intuition: wenn \mathcal{A} Ver-Anfrage mit $\text{Ver}(K, M, \sigma) = 1$ und „frischem“ (also nicht schon von Sig erzeugtem) σ generiert, ist das schon eine gefälschte Signatur

1 Symmetrische Authentifikation von Nachrichten

- Ziel
- Sicherheit
- **Konstruktionen**
- MACs aus PRFs
- Konkrete Konstruktionen und HMAC
- Zusammenfassung

2 Asymmetrische Authentifikation von Nachrichten

- Motivation
- Sicherheit
- RSA als Signaturschema

Hash-Then-Sign-Paradigma

- **Problem:** viele Verfahren signieren nur kurze Bitstrings
- **Lösung:** signiere $H(M) \in \{0, 1\}^k$ anstelle von $M \in \{0, 1\}^*$

Theorem (Sicherheit des Hash-Then-Sign-Paradigmas)

Sei (Sig, Ver) EUF-CMA-sicher und H eine kollisionsresistente Hashfunktion. Dann ist der durch $\text{Sig}'(K, M) = \text{Sig}(K, H(M))$, $\text{Ver}'(K, M, \sigma) = \text{Ver}(K, H(M), \sigma)$ erklärte MAC EUF-CMA-sicher.

Beweis.

Beweisstrategie: ein EUF-CMA-Angreifer \mathcal{A}' auf $(\text{Sig}', \text{Ver}')$ muss entweder eine H-Kollision oder eine Signatur σ für einen „frischen“ Hashwert $H(M)$ finden, um das EUF-CMA-Spiel zu gewinnen. \square

Pseudorandom Functions

- Nützlicher theoretischer Baustein: Pseudorandom Functions

Definition (Pseudorandom Function, PRF)

Sei $\text{PRF} : \{0, 1\}^k \times \{0, 1\}^k \rightarrow \{0, 1\}^k$ eine über $k \in \mathbb{N}$ parametrisierte Funktion. PRF heißt Pseudorandom Function (PRF), falls für jeden PPT-Algorithmus \mathcal{A} die Funktion

$$\text{Adv}_{\text{PRF}, \mathcal{A}}^{\text{prf}}(k) := \Pr \left[\mathcal{A}^{\text{PRF}(K, \cdot)}(1^k) = 1 \right] - \Pr \left[\mathcal{A}^{\text{R}(\cdot)}(1^k) = 1 \right]$$

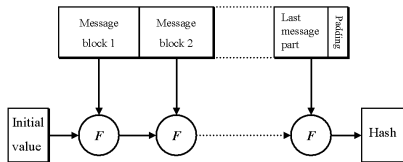
vernachlässigbar ist, wobei $\text{R} : \{0, 1\}^k \rightarrow \{0, 1\}^k$ eine echt zufällige Funktion ist.

Kandidat für eine Pseudorandom Function

- PRF-Kandidat, ausgehend von Hashfunktion H :

$$\text{PRF}(K, X) := H(K \| X)$$

- **Vorsicht:** diese Konstruktion hat ihre Tücken
 - Manchmal (Merkle-Damgård) lässt sich Hashwert „erweitern“:



- $H(K \| X)$ kann zu $H(K \| X \| X')$ erweitert werden
- Bricht PRF-Eigenschaft für Eingaben unterschiedlicher Länge

1 Symmetrische Authentifikation von Nachrichten

- Ziel
- Sicherheit
- Konstruktionen
- **MACs aus PRFs**
- Konkrete Konstruktionen und HMAC
- Zusammenfassung

2 Asymmetrische Authentifikation von Nachrichten

- Motivation
- Sicherheit
- RSA als Signaturschema

Theorem (MACs aus PRFs und Hashfunktionen)

Sei $\text{PRF} : \{0, 1\}^k \times \{0, 1\}^k \rightarrow \{0, 1\}^k$ eine PRF und $H : \{0, 1\}^* \rightarrow \{0, 1\}^k$ eine kollisionsresistente Hashfunktion. Dann ist der durch $\text{Sig}(K, M) = \text{PRF}(K, H(M))$ gegebene MAC EUF-CMA-sicher.

Beweis.

- Gehen wir von einem erfolgreichen EUF-CMA-Angreifer \mathcal{A} aus
- Wir dürfen annehmen, dass \mathcal{A} eine Fälschung (M^*, σ^*) mit „frischem“ (d.h. noch nicht signiertem) M^* ausgibt
- \mathcal{A} kann also als PRF-Unterscheider aufgefasst werden, der mit nicht-vernachlässigbarer Wkt. $\text{PRF}(K, H(M^*))$ vorhersagt
- Derartige Voraussage nur mit PRF (nicht aber bei R) möglich



1 Symmetrische Authentifikation von Nachrichten

- Ziel
- Sicherheit
- Konstruktionen
- MACs aus PRFs
- **Konkrete Konstruktionen und HMAC**
- Zusammenfassung

2 Asymmetrische Authentifikation von Nachrichten

- Motivation
- Sicherheit
- RSA als Signaturschema

- Unsicher (für $H \in \{\text{MD5}, \text{SHA-1}\}$):

$$\text{Sig}(K, M) = H(K \| M)$$

- Besser, gerade hergeleitet:

$$\text{Sig}(K, M) = H(K \| H(M))$$

- Noch besser, sehr populär: HMAC

$$\text{Sig}(K, M) = H((K \oplus \text{opad}) \| H((K \oplus \text{ipad}) \| M))$$

$$\text{Ver}(K, M, \sigma) = (\sigma \stackrel{?}{=} \text{Sig}(K, M))$$

($\text{opad}, \text{ipad} \in \{0, 1\}^k$ feste Konstanten)

- Erinnerung: HMAC

$$\text{Sig}(K, M) = H((K \oplus \text{opad}) \| H((K \oplus \text{ipad}) \| M))$$

- Vorteil (gegenüber $\text{Sig}(K, M) = H(K \| H(M))$):
 - Zusätzliche Parametrisierung von innerer H-Auswertung erschwert konkrete Angriffe (heuristisches Argument)
 - H-Kollisionen führen noch nicht notwendig zu Sig-Bruch
- Theoretisch und praktisch gut untersucht, de-facto-Standard
 - Achtung: Im Standard wird K noch mit 0en auf feste Länge gepaddet.

1 Symmetrische Authentifikation von Nachrichten

- Ziel
- Sicherheit
- Konstruktionen
- MACs aus PRFs
- Konkrete Konstruktionen und HMAC
- **Zusammenfassung**

2 Asymmetrische Authentifikation von Nachrichten

- Motivation
- Sicherheit
- RSA als Signaturschema

- MACs stellen Nachrichtenintegrität/-authentizität sicher
- Standard-Sicherheitsdefinition EUF-CMA
- Hash-Then-Sign-Paradigma
- Hashfunktionen als PRFs als MACs
 - Aber: Merkle-Damgård hat hier seine Tücken
- Aktueller Standard: HMAC

- Aktuelle Debatte: (Un-)Sinn verschiedener Angreifermodelle
 - Wenn wir über alle (effizienten) Angreifer quantifizieren. . .
 - . . . kennt ein Angreifer auch eine Hashkollision. . .
 - . . . und kann damit z.B. Hash-Then-Sign-Verfahren brechen
 - Deshalb sollte Angreifer für jedes k funktionieren
 - Welchen Sinn haben dann noch „konkrete“ Sicherheitsbeweise?

1 Symmetrische Authentifikation von Nachrichten

- Ziel
- Sicherheit
- Konstruktionen
- MACs aus PRFs
- Konkrete Konstruktionen und HMAC
- Zusammenfassung

2 Asymmetrische Authentifikation von Nachrichten

- Motivation
- Sicherheit
- RSA als Signaturschema

- 1 Symmetrische Authentifikation von Nachrichten
 - Ziel
 - Sicherheit
 - Konstruktionen
 - MACs aus PRFs
 - Konkrete Konstruktionen und HMAC
 - Zusammenfassung

- 2 Asymmetrische Authentifikation von Nachrichten
 - **Motivation**
 - Sicherheit
 - RSA als Signaturschema

- Authentifizierte Übermittlung auf unauthentifiziertem Kanal:

Alice $\xleftarrow{(M,\sigma)}$ Bob

- MACs: Alice und Bob besitzen gemeinsames Geheimnis K

Alice _{K} $\xleftarrow{(M,\sigma)}$ Bob _{K}

- **Probleme:** Schlüsselverteilung, viele Schlüssel nötig

- Alternative: digitale Signaturschemata

Alice_{pk} ←^(M,σ) Bob_{sk}

- $(pk, sk) \leftarrow \text{Gen}(1^k)$ wie bei Public-Key-Verschlüsselung
 - pk öffentlicher Schlüssel
 - sk geheimer Schlüssel
- Signieren: $\sigma \leftarrow \text{Sig}(sk, M)$
- Verifizieren: $\text{Ver}(pk, M, \sigma) \in \{0, 1\}$
- Korrektheit wie bei MACs: $\text{Ver}(pk, M, \sigma) \stackrel{!}{=} 1$ für alle $(pk, sk) \leftarrow \text{Gen}(1^k)$, alle M und alle $\sigma = \text{Sig}(sk, M)$

1 Symmetrische Authentifikation von Nachrichten

- Ziel
- Sicherheit
- Konstruktionen
- MACs aus PRFs
- Konkrete Konstruktionen und HMAC
- Zusammenfassung

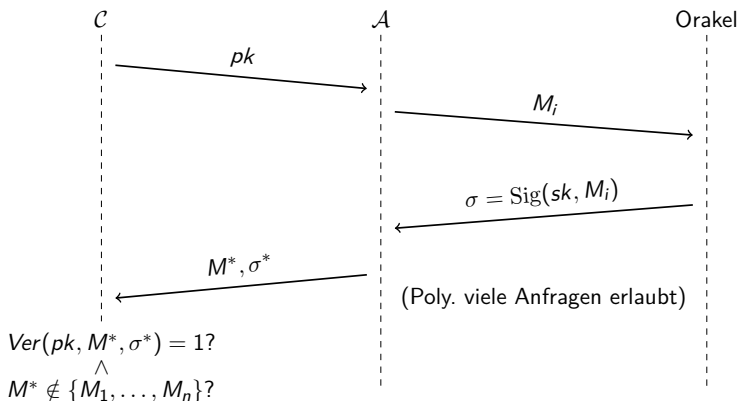
2 Asymmetrische Authentifikation von Nachrichten

- Motivation
- **Sicherheit**
- RSA als Signaturschema

- Schema EUF-CMA-sicher \Leftrightarrow kein PPT-Angreifer \mathcal{A} gewinnt folgendes Spiel nicht-vernachlässigbar oft:
 - 1 \mathcal{A} erhält pk und Zugriff auf ein $\text{Sig}(sk, \cdot)$ -Orakel
 - 2 \mathcal{A} gibt Ausgabe (M^*, σ^*)
 - 3 \mathcal{A} gewinnt, wenn $\text{Ver}(pk, M^*, \sigma^*) = 1$ und M^* „frisch“ (d.h. M^* ungleich aller Nachrichten, die \mathcal{A} an das Orakel gesendet hat)
- Standardbegriff für digitale Signaturen

Signaturen – EUF-CMA: Spiel

- Herausforderer \mathcal{C} führt $(pk, sk) \leftarrow \text{Gen}(1^k)$ aus.
- \mathcal{C} stellt $\text{Sig}(sk, \cdot)$ -Orakel für \mathcal{A} bereit.



1 Symmetrische Authentifikation von Nachrichten

- Ziel
- Sicherheit
- Konstruktionen
- MACs aus PRFs
- Konkrete Konstruktionen und HMAC
- Zusammenfassung

2 Asymmetrische Authentifikation von Nachrichten

- Motivation
- Sicherheit
- RSA als Signaturschema

- Erinnerung RSA-Verschlüsselung:

$$pk = (N, e) \quad sk = (N, d)$$

$$\text{Enc}(pk, M) = M^e \bmod N$$

$$\text{Dec}(sk, C) = C^d \bmod N$$

- (**Warnung/Erinnerung:** in dieser Form nicht sicher!)
- Betrachte RSA als Signaturschema:

$$\text{Sig}(sk, M) = M^d \bmod N$$

$$\text{Ver}(pk, M, \sigma) = 1 \quad :\iff \quad M = \sigma^e \bmod N$$

- RSA als Signaturschema:

$$\text{Sig}(sk, M) = M^d \bmod N$$

$$\text{Ver}(pk, M, \sigma) = 1 \quad :\iff \quad M = \sigma^e \bmod N$$

- PKE \rightarrow Sig-Konversion nicht allgemein
 - Allgemeiner lassen sich Nachrichten nicht unbedingt „zuerst ent-, dann wieder verschlüsseln“ (Datentypproblem)
 - Außerdem muss/sollte Enc nicht deterministisch sein
- Zahlreiche Sicherheitsprobleme (nachfolgend)
- Aber: RSA-Signaturen können „repariert“ werden