Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptographie II

SS 2013

Blatt 6 / 12. Juli 2013

AUFGABE 1:

Sei f eine Permutation und $f^i(x)$ die i-fache Hintereinanderausführung von f bei Eingabe x mit $f^0(x) := x$. Betrachten Sie folgendes Signaturverfahren $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ für Nachrichten $m \in \{1, \ldots, p\}$ mit $p = p(n)$ polynomiell in n.

$\mathsf{Gen}(1^n)$: Wähle $\mathsf{sk} \in_R \{0,1\}^n$ und $\mathsf{pk} := f^p(\mathsf{sk})$.

$\mathsf{Sign}_{\mathsf{sk}}(m)$: Gib $\sigma := f^{p-m}(\mathsf{sk})$ zurück.

$\mathsf{Vrfy}_{\mathsf{pk}}(m, \sigma)$: Falls $\mathsf{pk} = f^m(\sigma)$ gib eine 1 zurück, sonst eine 0.

(a) Zeigen Sie, dass Π korrekt ist.

(b) Zeigen Sie, dass Π kein CMA-sicheres Einwegsignaturverfahren ist, auch wenn f eine Einwegpermutation ist. Für welche Nachrichten lässt sich effizient eine gefälschte Signatur erzeugen, wenn die Signatur σ' der angefragten Nachricht m' bekannt ist?

(c) Zeigen Sie, dass Signaturen für alle anderen (nicht in (b) gefälschten) Nachrichten nur mit vernachlässigbarer Wahrscheinlichkeit gefälscht werden können, wenn f eine Einwegpermutation ist.

AUFGABE 2:

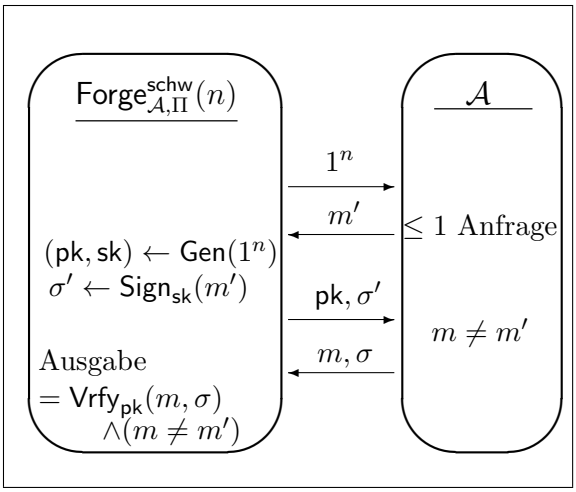
Wir betrachten das Lamport Einwegsignaturverfahren (Folie 141). Beschreiben Sie einen Angreifer, der Signaturen von zwei Nachrichten seiner Wahl erhält und anschließend Signaturen für andere Nachrichten fälschen kann.

Bitte wenden!

AUFGABE 3:

Wir definieren zunächst einen neuen Sicherheitsbegriff, der auch in der Hausaufgabe untersucht wird.

Definition: Ein Signaturverfahren $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ heißt *schwach* CMA-sichere *Einweg*signatur, falls für alle ppt-Angreifer $\mathcal{A}$ gilt $\mathsf{Ws}[\mathsf{Forge}^{\mathsf{schw}}_{\mathcal{A},\Pi}(n) = 1] \leq \mathsf{negl}(n)$.



Im Vergleich zur gewöhnlichen CMA-sicheren Einwegsignatur erhält der Angreifer $\mathcal{A}$ den öffentlichen Schlüssel folglich erst *nach* der Anfrage der Nachricht.

Wir betrachten zudem das folgende Signaturverfahren $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ mit Nachrichten- und Signaturraum $\mathbb{Z}_p$. Sei $\mathcal{G}$ ein Algorithmus, der eine Gruppe primer Ordnung p erzeugt.

$\mathsf{Gen}(1^n)$: $(g, p) \leftarrow \mathcal{G}(1^n)$, $x \in_R \mathbb{Z}_p^*$, $y \in_R \mathbb{Z}_p$, $u := g^x$, $v := g^y$, $\mathsf{pk} := (g, u, v)$, $\mathsf{sk} := (p, x, y)$.

$\mathsf{Sign}_{\mathsf{sk}}(m)$: Gib $\sigma := (y - m) \cdot x^{-1} \bmod p$ zurück.

$\mathsf{Vrfy}_{\mathsf{pk}}(m, \sigma)$: Falls $v = g^m \cdot u^\sigma$ gib eine 1 zurück, sonst eine 0.

(a) Zeigen Sie, dass Π korrekt ist.

(b) Zeigen Sie, dass Π eine schwach CMA-sichere Einwegsignatur ist, wenn das Diskrete Logarithmus Problem hart bzgl. $\mathcal{G}$ ist.

Hinweis: Wählen Sie in der Reduktion $u := g^x$ (wobei p, g, g^x die Eingabe des Unterscheiders ist) und wählen Sie v abhängig von der angefragten Nachricht, indem Sie die zugehörige Signatur uniform aus $\mathbb{Z}_p$ wählen. Der private Schlüssel ist dem Unterscheider damit nicht bekannt. Überlegen Sie, wie Sie schließlich mit Hilfe der ausgegebenen Nachricht m und ausgegebenen Signatur σ (zusammen mit m' und σ') das Diskrete Logarithmus Problem lösen.