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

Hausübungen zur Vorlesung

Kryptographie II

SS 2013

Blatt 6 /
Abgabe: 19. Juli 2013, 10 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

Sei $\mathsf{GenModulus}$ wie aus der Vorlesung bekannt ein Algorithmus der eine *Blumzahl* $N = p \cdot q$ und die zugehörige Faktorisierung p, q liefert. Wir betrachten nun eine Rabin-Variante (Folie 103) des RSA-FDH Verfahrens aus der Vorlesung (Folie 74). Sei $H : \{0,1\}^* \to \mathcal{QR}_N$ ein Random Oracle. Wir konstruieren daraus wie folgt ein Signaturverfahren $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ für Nachrichten $m \in \{0,1\}^*$.

$\mathsf{Gen}(1^n)$: Berechne $(N, p, q) \leftarrow \mathsf{GenModulus}(1^n)$. Setze $\mathsf{pk} = N$ und $\mathsf{sk} = (p, q)$.

$\mathsf{Sign}_{\mathsf{sk}}(m)$: Bestimme $H(m)$ und gib die Hauptwurzel σ von $H(m)$ zurück.

(a) Geben Sie eine Verifizierungsfunktion an und zeigen Sie die Korrektheit.

(b) Zeigen Sie, dass Π im ROM unter der Faktorisierungsannahme CMA-sicher ist.

Bitte wenden!

AUFGABE 2 (5 Punkte)**:**

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 $\mathsf{sk}_1, \mathsf{sk}_2 \in_R \{0,1\}^n$, $\mathsf{pk}_1 := f^p(\mathsf{sk}_1)$ und $\mathsf{pk}_2 := f^p(\mathsf{sk}_2)$.
Setze $\mathsf{sk} := (\mathsf{sk}_1, \mathsf{sk}_2)$ und $\mathsf{pk} := (\mathsf{pk}_1, \mathsf{pk}_2)$.

$\mathsf{Sign}_{\mathsf{sk}}(m)$: Berechne $\sigma_1 := f^{p-m}(\mathsf{sk}_1)$ und $\sigma_2 := f^{m-1}(\mathsf{sk}_2)$. Gib $\sigma := (\sigma_1, \sigma_2)$ zurück.

$\mathsf{Vrfy}_{\mathsf{pk}}(m, \sigma)$: Falls $\mathsf{pk}_1 = f^m(\sigma_1)$ und $\mathsf{pk}_2 = f^{p-m+1}(\sigma_2)$ gib eine 1 zurück, sonst eine 0.

(a) Zeigen Sie, dass Π korrekt ist.

(b) Zeigen Sie, dass Π ein CMA-sicheres Einwegsignaturverfahren ist, falls f eine Einwegpermutation ist.

AUFGABE 3 (5 Punkte)**:**

Betrachten Sie für diese Aufgabe das Signaturverfahren auf Präsenzblatt 6, Aufgabe 3. Wir haben in der Präsenzübung gezeigt, dass das Verfahren eine *schwach* CMA-sichere *Einweg*signatur ist.

(a) Zeigen Sie: Jedes CMA-sichere Signaturverfahren (Folie 123) ist auch ein schwach CMA-sicheres Einwegsignaturverfahren (Definition: siehe Präsenzblatt).

(b) Zeigen Sie, dass die Rückrichtung nicht gilt, indem Sie einen Angreifer auf die CMA-Sicherheit (Folie 123) angeben, auch wenn das Diskrete Logarithmus Problem hart ist.

AUFGABE 4 (5 Punkte)**:**

Sei $f : \{0,1\}^n \to \{0,1\}^n$ eine Funktion. Betrachten Sie eine Variante $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ des Lamport Verfahrens, parametrisiert durch $\ell \in \mathbb{N}$ mit $\ell = \ell(n)$ polynomiell in n, für Nachrichten $m \subset \{1, \ldots, 2\ell\}$ mit $|m| = \ell$, d.h. für insgesamt $\binom{2\ell}{\ell}$ Nachrichten:

$\mathsf{Gen}(1^n)$: Wähle $x_1, \ldots, x_{2\ell} \in_R \{0,1\}^n$ und setze $y_i = f(x_i)$ für $1 \leq i \leq 2\ell$.
Setze $\mathsf{sk} := (x_1, \ldots, x_{2\ell})$ und $\mathsf{pk} := (y_1, \ldots, y_{2\ell})$.

$\mathsf{Sign}_{\mathsf{sk}}(m)$: Falls $m \not\subset \{1, \ldots, 2\ell\}$ oder $|m| \neq \ell$ gib $\perp$ zurück, sonst gib $\sigma := \{x_i\}_{i \in m}$ zurück.

In jeder Nachrichten werden also genau ℓ der 2ℓ Elemente ausgewählt. Mögliche Nachrichten für $l = 8$ wären also $\{1, 3, 5, 6\}$ und $\{2, 3, 4, 8\}$, aber nicht $\{2, 4, 5, 6, 7\}$ (zu viele Elemente), nicht $\{1, 4, 6\}$ (zu wenige Elemente) und auch nicht $\{1, 3, 6, 9\}$ (darf nur Zahlen von 1 bis 8 enthalten). Die zugehörigen Signaturen für die gültigen Nachrichten wären $\{x_1, x_3, x_5, x_6\}$ bzw. $\{x_2, x_3, x_4, x_8\}$.

(a) Geben Sie eine Vrfy-Funktion an und zeigen Sie die Korrektheit von Π.

(b) Zeigen Sie, dass Π ein CMA-sicheres Einwegsignaturverfahren ist, falls f eine Einwegfunktion ist.