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

Hausübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 13 / 24. Januar 2014

Abgabe: 4. Februar 2014, 14.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

Beweisen Sie: Wenn das DCR-Problem hart ist bzgl. GenModulus (siehe Folie 109), so ist auch Faktorisieren hart bzgl. GenModulus (siehe Folie 55). Gehen Sie wie folgt vor:

(a) Zeigen Sie, dass man bei bekannter Faktorisierung effizient $f^{-1} : \mathbb{Z}_{N^2}^* \to \mathbb{Z}_N \times \mathbb{Z}_N^*$ berechnen kann.

(b) Zeigen Sie durch Angabe eines Unterscheiders, dass man das DCR-Problem effizient lösen kann, wenn f^{-1} effizient berechenbar ist.

AUFGABE 2 (5 Punkte)**:**

Sei 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 101) 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 3 (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 4 (5 Punkte)**:**

Betrachten Sie für diese Aufgabe das Signaturverfahren auf Präsenzblatt 13, Aufgabe 4. Wir haben in der Präsenzübung gezeigt, dass das Verfahren eine *schwach* CMA-sichere *Einweg*signatur ist.

(a) Zeigen Sie: Jedes CMA-sichere Signaturverfahren (Folie 121) 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 angeben, auch wenn das Diskrete Logarithmus Problem hart ist.