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

Präsenzübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 12 / 20./21. Januar 2014

AUFGABE 1:

Sei $\Pi' = (\mathsf{Gen}', \mathsf{Samp}, f, \mathsf{Inv})$ eine Familie von Trapdoor-Einwegpermutationen und hc ein Hardcoreprädikat für Π'. Wir konstruieren daraus folgendes asymmetrische Verfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ für Nachrichten $m \in \{0, 1\}$.

$\mathsf{Gen}(1^n)$: $(I, \mathsf{td}) \leftarrow \mathsf{Gen}'(1^n)$. Gib $\mathsf{pk} = I$ und $\mathsf{sk} = \mathsf{td}$ zurück.

$\mathsf{Enc}_{\mathsf{pk}}(m)$: Wähle ein $x \in_R \mathcal{D}_I$, so dass $\mathsf{hc}_I(x) = m$ und gib den Chiffretext $c := f_I(x)$ zurück.

(a) Begründen Sie, dass die Verschlüsselung in (erwarteter) Polynomialzeit berechnet werden kann.

(b) Geben Sie eine effiziente Entschlüsselungsfunktion an und zeigen Sie die Korrektheit.

(c) Zeigen Sie, dass Π CPA-sicher ist.

AUFGABE 2:

Sei $H : \{0, 1\}^n \to \{0, 1\}^{\ell(n)}$ ein Random Oracle. Zeigen Sie:

(a) Für $\ell(n) = 2n$ verhält sich H wie ein Pseudozufallsgenerator.

(b) Für $\ell(n) = n$ verhält sich H wie eine Einwegfunktion.

(c) Für $\ell(n) = n/2$ verhält sich H wie eine kollisionsresistente Hashfunktion.

Bitte wenden!

AUFGABE 3:

Sei $\Pi_f = (\mathsf{Gen}, \mathsf{Samp}, f_I)$ mit $f_I : \{0,1\}^n \to \{0,1\}^n$ eine Einwegpermutationsfamilie. Sei dh ein deterministischer pt Algorithmus. $\mathsf{dh} : \{0,1\}^n \to \{0,1\}^2$ heißt Doppelhardcoreprädikat für f, falls für alle ppt-Algorithmen $\mathcal{A}$ gilt

$$\mathsf{Ws}[\mathcal{A}(1^n, I, f_I(x)) = \mathsf{dh}(x)] \leq \frac{1}{4} + \mathsf{negl}(n).$$

Sei $\Pi_f = (\mathsf{Gen}, \mathsf{Samp}, f_I)$ eine Familie von Einwegpermutationen und $H : \{0,1\}^n \to \{0,1\}^2$ ein Random Oracle. Zeigen Sie, dass H dann ein Doppelhardcoreprädikat für Π_f ist.

AUFGABE 4:

Sei $N = p \cdot q$ für prime, ungerade $p \neq q$. Zur Erinnerung:

$$\mathcal{J}_N^{+1} := \{x \in \mathbb{Z}_N^* \mid \left(\frac{x}{N}\right) = +1\}$$

ist die Menge aller x mit Jacobi-Symbol $+1$,

$$\mathcal{QR}_N := \{x \in \mathbb{Z}_N^* \mid \exists\, y \in \mathbb{Z}_N^* \text{ mit } x = y^2 \bmod N\}$$

die Menge aller quadratischen Reste, $\mathcal{QNR}_N := \mathbb{Z}_N^* \setminus \mathcal{QR}_N$ die Menge aller quadratischen Nichtreste und $\mathcal{QNR}_N^{+1} := \mathcal{J}_N^{+1} \setminus \mathcal{QR}_N$ die Menge aller quadratischen Nichtreste mit Jacobi-Symbol $+1$. Zeigen Sie:

(a) $|\mathcal{J}_N^{+1}| = \frac{1}{2} \cdot |\mathbb{Z}_N^*|$

(b) $\mathcal{QR}_N \subset \mathcal{J}_N^{+1}$

(c) $|\mathcal{QR}_N| = \frac{1}{2} \cdot |\mathcal{J}_N^{+1}|$