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 11 / 12. Januar 2014

Abgabe: 21. Januar 2014, 14.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

Betrachten Sie das folgende Public-Key-Verschlüsselungsverfahren. Der öffentliche Schlüssel (q, g, h) und der private Schlüssel x werden analog zur ElGamal-Verschlüsselung mit Hilfe eines Algorithmus $\mathcal{G}$ generiert. Um ein Bit b zu verschlüsseln, berechnet der Sender den Chiffretext folgendermaßen:

1. Falls $b = 0$ ist, dann wählt er unabhängig gleichverteilt $y, z \in_R \mathbb{Z}_q$ und berechnet $c = (c_1, c_2) := (g^y, g^z)$.
2. Falls $b = 1$ ist, dann wählt er $y \in_R \mathbb{Z}_q$ und berechnet $c = (c_1, c_2) := (g^y, h^y)$.

(a) Zeigen Sie, dass mit Hilfe des privaten Schlüssels x eine effiziente Entschlüsselung möglich ist. (Es darf zu Entschlüsselungsfehlern kommen, Sie sollten aber begründen, warum solche nur mit vernachlässigbarer Wahrscheinlichkeit auftreten).

(b) Beweisen Sie, dass das Verschlüsselungsverfahren CPA-sicher ist, falls das DDH-Problem hart bzgl. $\mathcal{G}$ ist.

AUFGABE 2 (5 Punkte)**:**

Sei $\mathsf{hc} : \{0,1\}^n \to \{0,1\}$ ein *Hardcoreprädikat* für eine Permutation $f : \{0,1\}^n \to \{0,1\}^n$. Zeigen Sie, dass dann hc *erwartungstreu* (auch *unbiased* genannt) ist, d. h. dass

$$\left|\mathsf{Ws}_{x \in_R \{0,1\}^n}[\mathsf{hc}(x) = 0] - \mathsf{Ws}_{x \in_R \{0,1\}^n}[\mathsf{hc}(x) = 1]\right| \leq \mathsf{negl}(n)$$

gilt.

Bitte wenden!

AUFGABE 3 (5 Punkte)**:**

Sei $f : \{0,1\}^n \to \{0,1\}^n$ eine Einwegpermutation. Zeigen Sie, dass dann auch $g : \{0,1\}^{2n} \to \{0,1\}^{2n}$ definiert durch

$$g(x,r) := (f(x), r)$$

eine Einwegpermutation ist.

AUFGABE 4:

Seien $f : \{0,1\}^* \to \{0,1\}^*$ und $g : \{0,1\}^* \to \{0,1\}^*$ zwei durch deterministische pt-Algorithmen berechenbare Permutationen. Sei weiterhin mindestens eine der Permutationen f, g eine Einwegpermutation.

Zeigen Sie, dass dann

$$h(x) := f(g(x))$$

eine Einwegpermutation ist.