Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Felix Heuer

RUHR UNIVERSITÄT BOCHUM RUB

Hausübungen zur Vorlesung

Kryptographie 2

SS 2011

Blatt 3 / 4. Mai 2011 / Abgabe 18. Mai, 08:30 Uhr, Kasten NA 02

AUFGABE 1. ElGamal mal anders. (5 Punkte)
Betrachten Sie das folgende Public Key Verschlüsselungsverfahren. Der öffentliche Schlüssel $(\mathcal{G}, g, q, h)$ und der private Schlüssel x werden analog zur ElGamal Verschlüsselung generiert. Um ein Bit b zu verschlüsseln berechnet der Sender den Chiffretext folgendermaßen:

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

a) Zeigen Sie, dass mit Hilfe des privaten Schlüssels x eine effiziente Dechiffrierung Dec möglich ist (hierbei darf es zu Entschlüsselungsfehlern kommen, Sie sollten aber begründen, warum diese nur mit vernachlässigbarer Wahrscheinlichkeit auftreten).

b) Beweisen Sie, dass das Verschlüsselungsschema CPA-sicher ist, falls das *Decisional Diffie Hellman Problem* schwer bzgl. der Gruppe $\mathcal{G}$ ist.

AUFGABE 2. Harte Kerne. (5 Punkte)
Sei $f : \{0,1\}^n \to \{0,1\}^n$ eine Permutation. Beweisen Sie: Wenn es ein Hardcore-Prädikat $\mathsf{hc} : \{0,1\}^n \to \{0,1\}$ für f gibt, so erfüllt f die Einwegeigenschaft, d.h. f ist eine *Einwegpermutation*.

AUFGABE 3. Fehlkonstruktion. (10 Punkte)
Sei $f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ eine Einwegfunktion. Zeigen Sie, das dann im Allgemeinen die Funktion $f' : \{0,1\}^{2n} \to \{0,1\}^{2n}$ definiert durch $f'(x) := f(x) \oplus x$ *keine* Einwegfunktion ist. Gehen Sie hierbei wie folgt vor:

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

$$f(x) = f(x_1, x_2) := (g(x_1) \oplus x_2, x_2)$$

eine Einwegfunktion ist (hierbei teilen wir die Eingabe $x \in \{0,1\}^{2n}$ in zwei gleichgroße Hälften $x_1, x_2 \in \{0,1\}^n$ auf).

Hinweis: Beim Nachweis der Einwegeigenschaft kann es hilfreich sein, zunächst die Mengengleichheit $f^{-1}(a,b) = g^{-1}(a \oplus b) \times \{b\}$ zu zeigen. Hierbei bezeichnet $f^{-1}(a,b) := \{(x_1, x_2) \in \{0,1\}^{2n} | f(x_1, x_2) = (a,b)\}$ das *Urbild* von (a,b) unter f.

b) Benutzen Sie das in a) konstruierte f und betrachten Sie das entsprechende f'. Zeigen Sie, dass dieses f' keine Einwegfunktion sein kann.