Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Eike Kiltz
Gottfried Herold

Hausübungen zur Vorlesung

Kryptographie II

SS 2012

Blatt 4 / 24. Mai 2012 / Abgabe **bis spätestens Mittwoch, 13.06.2012 10:00 Uhr**

AUFGABE 1:

Sei $N \in \mathbb{Z}$ beliebige ungerade zusammengesetzte Zahl, $x, x' \in \mathrm{QR}_N, y, y' \in \mathrm{QNR}_N^{+1}$ Zeigen Sie:

(a) $x \cdot x' \in \mathrm{QR}_N$. [1 Punkte]

(b) Im Allgemeinen gilt *nicht*, dass $y \cdot y' \in \mathrm{QR}_N$ ist. [2 Punkte]

Bemerkung zu (b): Sie sollen hier ein Gegenbeispiel angeben. Beachten Sie, dass N hier allgemein gewählt ist, insbesondere also kein RSA-Modulus sein muss. Für *RSA-Moduli* N (siehe Vorlesung) gilt in der Tat $y \cdot y' \in \mathrm{QR}_N$.

AUFGABE 2:

Sei $\Pi_f = (\mathbf{Gen}, \mathrm{Samp}, f)$ eine Einwegpermutation und $H : \{0,1\}^n \to \{0,1\}^{l(n)}$ ein Random Oracle. Zeigen Sie, dass dann H eine Hardcore-Funktion für Π_f ist. [5 Punkte]

Dabei sind Hardcore-Funktionen genauso definiert wie Hardcore-Prädikate (H eine $l(n)$-Bit Ausgabe statt 1-Bit Ausgabe hat und, dass in der Definition des Vorteils natürlich $\frac{1}{2^{l(n)}}$ statt $\frac{1}{2}$ steht).

AUFGABE 3:

Zeigen Sie, dass das Goldwasser-Micali Kryptosystem *nicht* CCA-sicher ist. [2 Punkte]

bitte wenden

AUFGABE 4:

Wir betrachten folgende Variation $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec})$ des Goldwasser-Micali-Kryptosystems:

Gen Ruft GenModulus auf und erhalte $p, q, N = p \cdot q$.
N ist public key, (p, q) der secret key.

Enc$_N$ Verschlüssle ein Bit b durch $c_1, \dots c_n$.
Falls $b = 0$, wähle $c_1, \dots, c_n \in \mathrm{QR}_N$ unabhängig uniform.
Falls $b = 1$, wähle $c_1, \dots, c_n$ unabhängig uniform in $\{x \in \mathbb{Z}_N^* \mid (\frac{x}{N}) = 1\}$

(a) Wie kann die Verschlüsselung in Polynomialzeit implementiert werden, d.h. wie kann man c_i in beiden Fällen uniform aus den entsprechenden Mengen wählen? [2 Punkte]

(b) Wie kann man hier entschlüsseln [1 Punkt]

(c) Zeigen Sie, dass das Verfahren CPA-sicher ist, falls die QR-Annahme bzgl. GenModulus gilt. [3 Punkte]

Bemerkung: Bei (a) und (b) dürfen Ver- und Entschlüsselung mit vernachlässigbarer Wahrscheinlichkeit fehlschlagen/das falsche Ergebnis liefern.