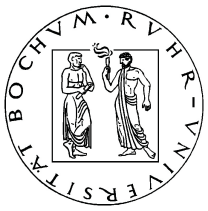
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann




**Hausübungen zur Vorlesung**

# Kryptographie 2

**SS 2009**

Blatt 4 / 03. Juni 2009 / Abgabe spätestens 17. Juni, 8:30 Uhr

**AUFGABE 1** (5 Punkte)**:**
Sei $\Pi$ ein CCA-sicheres Public-Key Verfahren und $\Pi'$ ein CCA-sicheres Private-Key Verfahren. Ist das mit $\Pi$ und $\Pi'$ instanzierte Hybride Verschlüsselungsverfahren (vgl. Skript Folie 26) CCA-sicher? Beweisen Sie Ihre Aussage.

**AUFGABE 2** (5 Punkte)**:**
In dieser Aufgabe betrachten wir quadratische Reste in der additiven Gruppe $\mathbb{Z}_N$. Ein Element $y \in \mathbb{Z}_N$ heißt quadratischer Rest, genau dann wenn es ein $x \in \mathbb{Z}_N$ gibt mit $2x = y \bmod N$.

1. Was sind die quadratischen Reste in $\mathbb{Z}_p$ für eine ungerade Primzahl $p$?
2. Sei $N = pq$ das Produkt zweier ungerader Primzahlen $p$ und $q$. Was sind die quadratischen Reste in $\mathbb{Z}_N$?
3. Sei $N$ eine gerade Zahl. Was sind die quadratischen Reste in $\mathbb{Z}_N$?

**AUFGABE 3** (5 Punkte)**:**
Betrachten Sie folgende Variante der Goldwasser-Micali Verschlüsselung: $GenModulus(1^n)$ liefert $(N, p, q)$ mit $p = q = 3 \bmod 4$, d.h. $N$ ist eine Blum-Zahl. Der öffentliche Schlüssel ist $N$, der private Schlüssel ist $(p, q)$. Um $m \in \{0, 1\}$ zu verschlüsseln wählt der Sender ein zufälliges $x \in \mathbb{Z}_N$ und berechnet den Chiffretext $c := [(-1)^m \cdot x^2 \bmod N]$.

1. Zeigen Sie, dass für eine Blum-Zahl $N$ gilt: $[-1 \bmod N] \in \mathcal{QNR}_N^{+1}$.
2. Zeigen Sie, dass das beschriebene System ununterscheidbare Verschlüsselungen unter CPA besitzt, falls das Unterscheiden Quadratischer Reste hart bezüglich $GenModulus$ ist.

**AUFGABE 4** (5 Punkte)**:**
Sei $\mathcal{G}$ ein Polynomialzeit Algorithmus, der bei Eingabe $1^n$ eine Primzahl $p$ mit $||p|| = n$ und einen Generator $g$ von $\mathbb{Z}_p^*$ ausgibt.
Zeigen Sie, dass das DDH problem *nicht* hart bezüglich $\mathcal{G}$ ist.
*Hinweis:* Quadratische Residuosität modulo einer Primzahl ist entscheidbar.