

## Kryptographie

Blatt 8, 03.06.05, Abgabe 10.06.05

**Aufgabe 1** Sei  $N = p \cdot q$  eine Blumzahl, d.h.  $p, q \equiv 3 \pmod{4}$ . Zeige:

$\text{Rabin}_N: \text{QR}_N \rightarrow \text{QR}_N, a \mapsto a^2 \pmod{N}$  ein Isomorphismus.

*Hinweis:*  $-1 \notin \text{QR}_p, -1 \notin \text{QR}_q$ .

**Aufgabe 2** Zeige: Die einfache Fiat-Shamir Identifikation ist perfekt zeroknowledge. Gib einen prob. pol. Zeit Simulator an.

**Aufgabe 3** Der betrügerische Prover  $\tilde{\mathcal{P}}$  zur einfachen Fiat-Shamir Identifikation habe Erfolgsws.  $\geq \frac{1}{2}(1 + \varepsilon), \varepsilon > 0$ . Die  $W_s$  bezieht sich auf die Münzwürfe von  $\tilde{\mathcal{P}}, \mathcal{V}$  und  $s \in_R \mathbf{Z}_N^*$ . Gib einen Algorithmus an, der  $N$  mittels  $\mathcal{P}$  in Laufzeit  $O(|\tilde{\mathcal{P}}| \varepsilon^{-1} \log N)$  zerlegt.

**Aufgabe 4** Präzisiere und analysiere folgenden Lösungsalgorithmus für das 2-Summenproblem über  $\{0, 1\}^n$ :

Verteile die  $x_1 \in L_1, x_2 \in L_2$  in  $2^{n/2}$  Fächer nach den niedrigsten  $2^{n/2}$  Bits.

Suche die Teil-Kollisionen über  $\{0, 1\}^{n/2}$  nach Kollisionen über  $\{0, 1\}^n$  ab.

Bilde z.B.  $L = \{(x_1, x_2, x_1 \oplus x_2) \mid \text{low}_{n/2}(x_1) = \text{low}_{n/2}(x_2)\}$ . Zeige:

Für  $|L_1| = |L_2| = 2^{n/2}$  geht das Verfahren in  $O(2^{n/2})$  arithm. + Adress-Schritten. Ein  $\log n$  Faktor für Sortieren tritt nicht auf.