Prof. C. P. Schnorr Sommersemester 2007

# Kryptographie

Blatt 12, 06.07.07, Abgabe 11.07.07

Wir verallgemeinerrn das Kryptoschema von Paillier von $\mathrm{ord}(g) = \lambda N$ auf den Fall $\mathrm{ord}(y) = \alpha N$, $1 \leq \alpha \leq \lambda$.

**Aufgabe 1.** Definiere $\mathrm{Pail}_{N,g} : (\mathbb{Z}_N, +) \times (\mathbb{Z}_N^*, \cdot) \to (\mathbb{Z}_{N^2}^*, \cdot)$ durch $(m, r) \mapsto g^m r^N$. Zeige für $\mathrm{ord}(g) = \alpha N$:

$\mathrm{Pail}_{N,g}$ liefert einen Isomorphismus $(\mathbb{Z}_N, +) \times (\mathbb{Z}_N^*, \cdot) \cong (\mathbb{Z}_{N^2}^*, \cdot)$.

**Aufgabe 2.** Erläutere die Dekodierung des Ziffertextes $c := \mathrm{Pail}_{N,g}(m, r)$ im allgemeinen Fall $\mathrm{ord}(g) = \alpha\, N$ und zeige die Korrektheit.

Wie muss man $\alpha := \mathrm{ord}(g)/N$ zur Sicherheit wählen?

**Aufgabe 3.** Sei $N = pq$ RSA Modul, $p - 1 = \alpha p_2$, $g \in \mathbf{Z}_{N^2}^*$ habe die Ordnung $\alpha\, N$.

Die Nachricht $m \in \mathbb{Z}_p \cong [0, p[$ werde verschlüsselt zu $c = g^m r^N$ mit $r \in_R \langle g \rangle$.
Zeige : $m = L(c^\alpha)/L(g^\alpha) \bmod p$ für $L(u) := \frac{u-1}{N}$.

Welche Vorsichtsmassnahmen erfordert dieses Kryptoschema ?

**Aufgabe 4.** Sei $p$ prim, $g \in \mathbb{Z}_{p^2}^*$ habe Ordnung $\alpha\, p$ mit $1 \leq \alpha \leq p - 1$, $\alpha | p - 1$. Zu $u \in \mathbb{Z}_{p^2}$ mit $u = 1 \mod p$ sei $L_p(u) = \frac{u-1}{p}$.

Die Nachricht $m \in \mathbb{Z}_p \cong [0, p[$ werde verschlüsselt zu $c := g^m r^p$ mit $r \in_R \langle g \rangle$.

Zeige: $m = L_p(c^\alpha)/L_p(g^\alpha) \mod p$.

Ist das Kryptoschema sicher ?