Prof. C. P. Schnorr Wintersemester 2008/09

Kryptographie

Blatt 11, 14.01.2008, Abgabe 21.01.2009

Aufgabe 1 Schnelle Variante des Paillier–Schemas

Sei $\alpha \in \mathbb{Z}_{N^2}^*$ mit $\text{ord}(\alpha) = N\lambda', 1 < \lambda', \lambda' \mid \lambda(N)$. Zeige für Kodierung $\text{cip} := E_\alpha(m,r) = \alpha^m r^N \bmod N^2$ class $m = L(\text{cip}^{\lambda'}) \,/\, L(\alpha^{\lambda'}) \bmod N$.

Aufgabe 2 Zeige für das α von Aufgabe 1 und für $\text{ggT}(\varphi(N), N) = 1$ dass

$$E_\alpha(m,z) : \mathbb{Z}_N \times \mathbb{Z}_N^* \to \mathbb{Z}_{N^2}^*, \;\; (m,r) \mapsto \alpha^m r^N \mod N^2$$

ein Isomorphismus ist.

Aufgabe 3 Beispiel zum Paillier Schema

Setze $N = 143 = 11 \cdot 13$.

Berechne ein $\alpha \in \mathbb{Z}_{N^2}^*$ mit $\text{ord}(\alpha) = \lambda(N^2)$. Kodiere $m = 2$ zu

$\text{cip} = E_\alpha(2,r)$ und dekodiere cip.