Prof. C. P. Schnorr Sommersemester 2015

Kryptographie

Zusatzblatt 11, 05.07.2017, Abgabe 12.07.2017

Es bezeichene RSA_m die Menge der RSA–Moduln $N = pq$ mit

$$p - 1 = 2^m \bmod 2^{m+1},\ q - 1 \neq 0 \bmod 2^{m+1}.$$

Aufgabe 1 Zeige für $N \in \mathrm{RSA}_m$:

a) $\mathbf{Z}_N^{*2^m} = \mathbb{Z}_N^{*2^{m+1}}$,

b) $-1 \notin \mathbf{Z}_N^{*2^m}$,

c) $x \mapsto x^2$ permutiert $\mathbf{Z}_N^{*2^m}$.

Aufgabe 2 Schnelle Variante des Paillier–Schemas

Sei $\alpha \in \mathbb{Z}_{N^2}^*$ mit $\mathrm{ord}(\alpha) = N\lambda'$ und $\lambda' | \lambda(N)$. Zeige für die Kodierung
$E_\alpha(m, r) : \mathbb{Z}_N \times \mathbb{Z}_N^* \to \mathbb{Z}_{N^2}^*$ und $\mathrm{cip} := E_\alpha(m, r)$ mit $\mathrm{ord}(r) | N\,\lambda'$
dass $m = L(\mathrm{cip}^{\lambda'}) \,/\, L(\alpha^{\lambda'}) \bmod N$.
(Korrektheit und Durchführbarkeit der Dekodierung)

Aufgabe 3 Zeige, dass $(\mathcal{P}, \mathcal{V})_{\mathrm{GPS}}$ stat. ZK ist, falls $kBX/A < 2^{-100}$ und B polynomial in der Bitlänge von (h, A) ist.

Hinweis: Jäger Skript, Kap. 5

Punktzahl pro Aufgabe 5.

Aufgabe 4 Sei $\widetilde{P}$ aktiver Angreifer auf $(P,V)_{OS}$ mit Erfws $\varepsilon > 2^{-\ell k+1}$ zu $\mathbf{v} = \mathbf{s}^{2^t}$, $\mathbf{s} \in_R (\mathbb{Z}_N^*)^k$.
Zeige: Mit $\mathrm{Ws}_{\mathbf{s}} \geq 1/2$ gibt es zur Hinterlegung $r^{2^t} = x \in_R \mathbb{Z}_N^{*2^t}$ mindestens $2^{(t-\ell)k}$ viele $\mathbf{c} \in [0, 2^t[^k$ für die $\widetilde{P}$ Erfolg hat.

Aufgabe 5 Sei $\widetilde{P}$ aktiver Angreifer auf $(P,V)_{BM}$ mit Erfws $\varepsilon > 2^{-t+1}$ $\widetilde{P} : \ell$ mal $(\widetilde{P}, V_{\widetilde{P}})_{BM}$, dann $(\widetilde{P}, V)_{BM}$. .
Skizziere einen prob. Alg. $AL : (\widetilde{P}, qw, x) \mapsto \{q, w\}$ mit $E_w|AL| = O(\widetilde{P}/\varepsilon)$.