Prof. C. P. Schnorr Sommersemester 2007

Kryptographie

Blatt 3, 04.05.2007, Abgabe 11.05.2007

Aufgabe 1. Sei $G = \langle g \rangle$ zyklische Gruppe gerader Ordnung $|G|$. Zeige

1. $\log_g(h) = 0 \bmod 2 \iff h \in G^2$,

2. $G \ni h \mapsto \log_g(h) \bmod 2$ ist in $\leq \lg |G|$ Multiplikationen berechenbar,

3. Berechne $\log_2(5) \bmod 2$ zu $G = \mathbb{Z}_{71}^*$.

Aufgabe 2. Zur Gruppe $G = \langle g \rangle, |G| \leq 2^{hvw}$ seien $g^{E_\ell} = \{g^s \mid s \in E_\ell\}$ für $\ell = 0, \ldots, v-1$ durch Vorberechnung gegeben.

Gib ein Verfahren an, das zu $a_0, \ldots, a_{hvw-1} \in \{0,1\}$ und den $s_{j,\ell} \in E_\ell$ nach Aufgabe 3, Blatt 2, $(g, a) \mapsto g^a$ in $wv - 1$ Multiplikationen und $w - 1$ Quadrierungen in G berechnet.
Für welche Werte h, w, v mit $hvw = h'v'w'$ ist der Fall $v = 2$ generell besser als $v' = 1$ (d.h. schneller bei kleinerer Grösse der vorberechneten Menge)?

Aufgabe 3. Zeige, dass für die generische ElGamal-Verschl. die Aufgabe zu gegebenem m gültige von ungültigen Ziffertexten von m zu unterscheiden, so schwierig ist wie DDH: DDH $\leq_{\text{pol}}$ IND.

Aufgabe 4. Sei $q - 1 = \prod_i p_i^{e_i}$ gegeben mit q, p_i prim.
Zeige für $a \in \mathbb{Z}_q^*$: $\langle a \rangle = \mathbb{Z}_q^* \Leftrightarrow \forall_i : a^{(q-1)/p_i} \neq 1 \bmod q$.
Gib einen prob. pol.–Zeit Algorithmus an zur Erzeugung eines Generators von $\mathbb{Z}_q^*$.