

Kryptographie

Blatt 3, 29.04.2005, Abgabe 06.05.2005

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

1. $\log_g(h) = 0 \pmod 2 \iff h \in G^2$,
2. $G \ni h \mapsto \log_g(h) \pmod 2$ ist in $\leq \lg |G|$ Multiplikationen berechenbar,
3. Berechne $\log_2(5) \pmod 2$ zu $G = \mathbf{Z}_{71}^*$.

Aufgabe 2. Sei $G = \langle g \rangle$ zyklische Gruppe ungerader Ordnung $|G|$. Zeige

1. $G = G^2$,
2. Mit einem Orakel zur Berechnung von $\log_{f'} h' \pmod 2$ für beliebige $h' \in \langle f' \rangle \subset G$ kann man $(f, h) \mapsto \log_f h$ in $O(\log |G|)$ Orakelaufrufen und Multiplikationen in G berechnen.

Aufgabe 3. (Lim-Lee, Crypto 94, LNCS 839, p. 95–105)

Zur Gruppe $G = \langle g \rangle$, $|G| \leq 2^{hk}$ sei $k = v \cdot w$ und $E_\ell = \sum_{i=0}^{h-1} \{0, 1\} 2^{ivw+\ell w}$ für $\ell = 0, \dots, v-1$. Zeige: Jedes $a \in [0, 2^{hvw}]$ hat genau eine Darstellung

$$a = \sum_{j=0}^{w-1} \left(\sum_{\ell=0}^{v-1} s_{j,\ell} \right) 2^j \text{ mit } s_{j,\ell} \in E_\ell, \text{ so dass dann}$$

$$g^a = \prod_{j=0}^{w-1} \left(\prod_{\ell=0, \dots, v-1} g^{s_{j,\ell}} \right)^{2^j}.$$

Entwickle eine explizite Formel für $s_{j,\ell}$ in den Bits a_i von $a = \sum_{i=0}^{hvw} a_i 2^i$.

Aufgabe 4. Zur Gruppe $G = \langle g \rangle$, $|G| \leq 2^{hvw}$ seien $g^{E_\ell} = \{g^s \mid s \in E_\ell\}$ für $\ell = 0, \dots, v-1$ durch Vorberechnung gegeben.

Gib ein Verfahren an, das zu $a_0, \dots, a_{hvw-1} \in \{0, 1\}$ und den $s_{j,\ell} \in E_\ell$ nach Aufgabe 3 $(g, a) \mapsto g^a$ 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)?