Prof. C. P. Schnorr Sommersemester 2007

Kryptographie

Blatt 2, 27.04.2007, Abgabe 04.05.2007

Aufgabe 1. Sei $n = p \cdot q$, p, q prim mit $p, q = 3 \bmod 4$, n heisst *Blum–Zahl.*

Zeige 1. $|QR_n| = \varphi(n)/4 = 1 \bmod 2$,

2. $x \mapsto x^2 \bmod n$ ist bijektiv auf $QR_n = \mathbb{Z}_n^{*2}$

3. Die Berechnung $x \mapsto \sqrt{x}$ für $x \in QR_n$ geht in polynomialer Zeit, sofern $\varphi(n)$ gegeben ist.

Aufgabe 2. Es bezeichne $E_{h,k} := \left\{ \sum_{i=0}^{h-1} c_i 2^{ik} \mid c_i \in \{0,1\} \right\}$.
Zeige: Die Zerlegung $a = \sum_{j=0}^{k-1} s_j 2^j \in [0, 2^{hk}[$ mit $s_j \in E_{h,k}$ ist eindeutig.
Berechne $g^{17}, g^{19}, g^{27}, g^{29}$ jeweils mit höchstens einer Quadrierung und einer Multiplikation zu gegebenem $g^{E_{3,2}}$.

Aufgabe 3. (Lim-Lee, Crypto 94, LNCS 839, p. 95–105)
Zur Gruppe $G = \langle g \rangle$, $|G| \le 2^{hk}$ sei $k = v \cdot w$ und $E_\ell = \sum_{i=0}^{h-1} \{0,1\} 2^{ivw+\ell w}$ für $\ell = 0, \ldots, v-1$.
Zeige: die Zerlegung $a = \sum_{j=0}^{w-1} \left(\sum_{\ell=0}^{v-1} s_{j,\ell} \right) 2^j \in [0, 2^{hvw}[$ mit $s_{j,\ell} \in E_\ell$ ist eindeutig. Somit gilt $g^a = \prod_{j=0}^{w-1} (\prod_{\ell=0,\ldots,v-1} g^{s_{j,\ell}})^{2^j}$.
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. Sei $G = \langle g \rangle$, $q = p_1 \cdots p_t$. Es bezeichne $M(p_1, \ldots, p_t)$ die Anzahl der Multiplikationen in G zur Berechnung $g \mapsto g^{q/p_1}, \ldots, g^{q/p_t}$. Zeige: $M(p_1, \ldots, p_t) = O(\lfloor \lg q \rfloor (1 + \lceil \lg t \rceil))$.
Hinweis: $M(p_1, \ldots, p_t) \le 2 \lg q + M(p_1, \ldots, p_{t/2}) + M(p_{t/2+1}, \ldots, p_t)$.