Prof. C. P. Schnorr Sommersemester 2011

Kryptographie

Blatt 2, 27.04.2011, Abgabe 04.05.2011

Aufgabe 1. Sei $G = \langle g \rangle$ zyklische Gruppe der Ordnung 2^e. Zeige, dass man $h \mapsto \log_g(h)$ mit $\binom{e+2}{2}$ Multiplikationen in G berechnen kann.

Hinweis: Für $a := \log_g h (\mathrm{mod} 2)$ gilt

$$\log_g(hg^a) = 2\log_{g^2}(hg^a) = a + \log_g h.$$

$$\log_g h(\mathrm{mod}2) \;=\; \begin{cases} 0 & \text{falls} \quad h^{2^{e-1}} = 1_G \\ 1 & \text{falls} \quad h^{2^{e-1}} \neq 1_G \end{cases}.$$

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. 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: $M(p_1, \ldots, p_t) \leq 2 \lg q + M(p_1, \ldots, p_{t/2}) + M(p_{t/2+1}, \ldots, p_t)$.

Punktzahl pro Aufgabe 5