Prof. C. P. Schnorr Wintersemester 2013/14

Kryptographie

Blatt 2, 22.11.2013, Abgabe 29.11.2013

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

Hinweis: Für $a := \log_g h (\mathrm{mod} 2)$ gilt $hg^a \in G^2$ und

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

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

Aufgabe 2. Sei $G = \langle g \rangle$, $|G| = q = p_1 \cdots p_t$. 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: $M(p_1, \ldots, p_t) \leq \lfloor \lg q \rfloor (1 + \lceil \lg t \rceil)$.
Hinweis: $M(p_1, \ldots, p_t) \leq \lg q + M(p_1, \ldots, p_{t/2}) + M(p_{t/2+1}, \ldots, p_t)$, sofern die g^{2^i} für $i = 0, \ldots, \lfloor \lg q \rfloor - 1$ gegeben sind.

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 $\leq_{\mathrm{pol}}$ IND.

Punktzahl pro Aufgabe 5