Prof. C. P. Schnorr Sommersemester 2017

Kryptographie

Blatt 2, 03.05.2017, Abgabe 10.05.2017

Aufgabe 1. Sei $G = \langle g \rangle$ zykl. Gruppe der Ordnung 2^e, g gegeben.
Berechne $h \mapsto \log_g(h)$ mit $f(e) \leq \binom{e+2}{2} - 3$ Multiplikationen in G.

Hinweis: Für $a := \log_g h (\mathrm{mod} 2)$ gilt $hg^a \in G^2$ und $\log_g(hg^a) = 2\log_{g^2}(hg^a)$
$= a + \log_g h$. Ferner $\log_g h(\mathrm{mod}2) = \begin{cases} 0 & \text{falls } h^{2^{e-1}} = 1_G \\ 1 & \text{falls } h^{2^{e-1}} \neq 1_G \end{cases}$
Somit $f(1) = 0, f(e) \leq f(e-1)+1+e$ für $e > 1$. Dies liefert die Berechnung.

Aufgabe 2. Sei $n = p \cdot q$, p, q prim, $p, q = 3 \bmod 4$, n heisst *Blum–Zahl*.
Zeige für Euler's Totient Funktion $\varphi(\prod_i p_i^{e_i}) =_{def} \prod_i p_i^{e_i - 1}(p_i - 1)$ dass

1. $|QR_n| = \varphi(n)/4 = 1 \bmod 2$ für $QR_n := (\mathbb{Z}_n^*)^2$

2. $x \mapsto x^2 \bmod n$ ist bijektiv auf QR_n

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

Hinweis zu **3**: $\sqrt{x} = x^{2^{-1} \bmod |QR_n|} \bmod n$

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

Aufgabe 4. 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: $M(p_1, \ldots, p_t) \leq 2\lfloor \lg q \rfloor (1 + \lceil \lg t \rceil)$.

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