Prof. C. P. Schnorr Sommersemester 2007

Kryptographie

Blatt 5, 18.05.2007, Abgabe 25.05.2007

Aufgabe 1 (3 Punkte). Seien G_1, G_2 zyklische Gruppen der Ordnung q_1, q_2, $s := \mathrm{ggT}(q_1, q_2)$. Zeige $G_1^s \times G_2^s \subset G_1 \times G_2$ ist zyklische Gruppe der Ordnung $q_1 q_2 / s^2$.

Aufgabe 2 (6 Punkte). $x^3 + ax + b \in \mathbb{K}[x]$ habe eine doppelte Nullstelle in $\mathbb{K}$, $\mathrm{char}(\mathbb{K}) > 3$. Zeige:

1. $4a^3 + 27b^2 = 0$, und die doppelte Nullstelle ist $\sqrt{-\frac{a}{3}}$.
2. Die übliche Punkte-Addition ist für $P_a = (\sqrt{-\frac{a}{3}}, 0)$ nicht erklärt.
3. $E_{a,b}(\mathbb{K}) - \{P_a\}$ ist abgeschlossen gegen die übliche Punkte-Addition.

Aufgabe 3 (6 Punkte). Zeige: das Protokoll $(\mathcal{P}^k, \mathcal{V}^k)$ der k-fach sequentiellen DL-Identifikation ist „perfect zero-knowledge“, falls 2^t polynomial ist, d.h. $t = O(\log(\log p))$ für Eingaben der Länge $\log_2 p$.

Skizziere einen perfekten Simulator $\mathcal{S} : (\tilde{V}, h) \mapsto (\bar{\mathbf{g}}, \mathbf{c}, \mathbf{y})$ mit $\mathrm{E}|\mathcal{S}(\tilde{V}, h)| \leq (|\mathcal{P}^k| + |\tilde{\mathcal{V}}|)2^t$.

Aufgabe 4 (5 Punkte). Eine Zeile der Erfolgsmatrix zum Extraktor AL von Satz 2 heiße k-schwer, wenn sie mindestens $2^t \, \varepsilon / k$ viele Einsen enthält. Zeige:

1. Der Anteil A_k der Einsen in k-schweren Zeilen ist $\geq 1 - 1/k$.
2. A_1 kann beliebig klein sein.