Prof. C. P. Schnorr Sommersemester 2011

Kryptographie

Blatt 5, 18.05.2011, Abgabe 27.05.2011

Aufgabe 1. Die Schnorr Signaturen (c_i, y_i) zur Nachricht m_i seien nach Vorschrift mit $r_i \in \mathbb{Z}_q^*$ für $i = 1, ..., t$ zum Schlüssel $x, h = g^x$ erzeugt. Zeige: Kennt man zu (c_i, y_i, m_i) $i = 1, \ldots, t$ die Koeffizienten $a_0, ..., a_t$ einer Gleichung $\sum_{i=1}^{t} a_i r_i = a_0$ so erhält man $x = \log_g h$ sofern $\sum_{i=1}^{t} a_i c_i \neq 0$.
Hinweis: $g^{r_i} = g^{y_i} h^{-c_i}$.

Aufgabe 2. $x^3+ax+b \in \mathbb{K}[x]$ 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. Seien $X_1, \ldots, X_i, \ldots$ unabh. Zufallsvariable über $\{0, 1\}$ mit $\Pr_D[X_i = 1] = \varepsilon$. Zeige für $u := \min\{i \mid X_i = 1\}$ und $k\varepsilon^{-1} \in \mathbb{N}$:
1. $0 < \mathrm{Ws}[u \leq k\varepsilon^{-1}] = 1 - (1-\varepsilon)^{k\varepsilon^{-1}} = 1 - e^{-k} + O(ke^{-k}\varepsilon)$.
2. $0 < e^{-\frac{1}{k}} - \mathrm{Ws}[u > \varepsilon^{-1}/k] = O(e^{-\frac{1}{k}}\varepsilon)$.

Benutze dass $0 < e^{\pm 1} - (1 \pm \frac{1}{n})^n = O(\frac{1}{n})$.

Punktzahl pro Aufgabe 5.