Kryptographie

Blatt 4, 07.11.2008, Abgabe 14.11.2008

Aufgabe 1. Sei $E_{a,b}(\mathbb{K})$ elliptische Kurve . Zeige:

1. für alle $(\bar{x}, \bar{y}) \in E_{a,b}(\mathbb{K})$: $\mathrm{ord}(\bar{x}, \bar{y}) = 2$ gdw $\bar{x}^3 + a\bar{x} + b = 0$.
2. $E_{a,b}(\mathbb{K})$ zyklisch $\Longrightarrow$ #Nullstellen von $x^3 + ax + b = 0$ ist ≤ 1.
3. $|E_{a,b}(\mathbb{K})|$ ist ungerade gdw $x^3 + ax + b$ keine Nullstelle in $\mathbb{K}$ hat.

Aufgabe 2. Sei q prim. Zeige:

1. $|E_{0,b}(\mathbb{Z}_q)| = q + 1$ für $q = 2 \bmod 3$, $b \in \mathbb{Z}_q^*$.
2. $|E_{a,0}(\mathbb{Z}_q)| = q + 1$ für $q = 3 \bmod 4$, $a \in QR_q = (\mathbb{Z}_q^*)^2$.

Hinweis: $x \mapsto x^3$ ist Bijektion von $\mathbb{Z}_q$ für $q = 2 \bmod 3$, $-1 \notin (\mathbb{Z}_q^*)^2$ für $q = 3 \bmod 4$. 2. gilt für beliebige $a \in \mathbb{Z}_q^*$.

Aufgabe 3. 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: $g^{r_i} = g^{y_i} h^{-c_i}$.