

Kryptographie

Blatt 4, 11.05.2011, Abgabe 20.05.2011

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

1. für alle $(\bar{x}, \bar{y}) \in E_{a,b}(\mathbb{K})$: $\text{ord}(\bar{x}, \bar{y}) = 2$ gdw $\bar{x}^3 + a\bar{x} + b = 0$.
2. $E_{a,b}(\mathbb{K})$ zyklisch \implies #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 $q = 2 \pmod{3}$, $b \in \mathbb{Z}_q^*$.
2. $|E_{a,0}(\mathbb{Z}_q)| = q + 1$ für $q = 3 \pmod{4}$, $a \in QR_q = (\mathbb{Z}_q^*)^2$.

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

Aufgabe 3. Ein Fälscher will DSA-Signaturen zur Nachricht „Einzugsermächtigung über 100 EURO zugunsten des XYZ-Service Providers“ für viele öffentliche Schlüssel h fälschen. Hierzu benutzt er den vom NIST vorgeschlagenen SHA H , wählt geeignete Parameter $G = \langle g \rangle \subset \mathbb{Z}_p^*$, q und fordert zu jedem h eine DSA-Signatur zu „Testnachricht“.

1. Wie wählt der Fälscher p, g, q ?
2. Wie gefährlich ist die Attacke ? Gibt es Schutzmaßnahmen ?
3. Warum geht dieser Angriff nicht für Schnorr Signaturen ?

Hinweis: <http://www.itl.nist.gov/fipspubs/fip186.htm>

Serge Vaudenay: Hidden Collisions on DSS, Crypto 96, LNCS 1109 pp.83-88.

Punktzahl pro Aufgabe 5.