Elliptische Kurven & Kryptologie Serie 11

Elliptische Kurven über Körpern der Charakteristik 2 Abgabe: 19. Mai

---

1. ***DSA mit elliptischen Kurven***: Formuliere eine Variante von *DSA* auf elliptischen Kurven der Form $C : Y^2 + XY = X^3 + a_2X^2 + a_6$ über einem Körper $\mathbb{F}_q$ der Charakteristik 2, *d.h.* die Koeffizienten a_2 und a_6 sind aus $\mathbb{F}_q$ und $q = 2^n$.

Bestimme eine natürliche Zahl M und eine Funktion $f : C \to \mathbb{Z}/M\mathbb{Z}$ so, dass jedes $m \in \mathbb{Z}/M\mathbb{Z}$ unter f höchstens zwei Urbilder besitzt.

2. Sei $C : Y^2 + XY = X^3 + a_2X^2 + a_6$ eine cubische Kurve über einem Körper $\mathbb{F}_q$ der Charakteristik 2 und sei $(X_0, Y_0) \in C$ mit $X_0 \neq 0$.

(a) Dividiere $Y^2 + XY = X^3 + a_2X^2 + a_6$ durch X_0^2, setze $X := X_0$ und $U := \frac{Y}{X_0}$, und schreibe die entsprechende quadratische Gleichung in U auf.

(b) Zeige, dass nebst $U_0 := \frac{Y_0}{X_0}$ auch $U_0 + 1$ eine Lösung dieser quadratischen Gleichung ist und finde so einen weiteren Punkt (X_0, Y_1) auf C.

3. Sei $\mathbb{F}_{64} = \mathbb{Z}_2[x]/(x^6 + x^5 + 1)$ und sei $C[a_2, a_6] : Y^2 + XY = X^3 + a_2X^2 + a_6$ eine cubische Kurve über $\mathbb{F}_{64}$. Ferner sei $a_2 = (x^4 + x + 1)$.

(a) Bestimme a_6 so, dass $\left(x^2 + 1, x^3 + x + 1\right)$ auf $C[a_2, a_6]$ liegt.

(b) Bestimme einen weiteren Punkt auf $C[a_2, a_6]$.

(c) Berechne (in $\mathbb{F}_{64}$) die beiden Ausdrücke

$$\frac{x^3 + x + 1}{x^2 + 1} \qquad \text{und} \qquad \frac{a_6}{(x^2 + 1)^2}\,.$$