Kryptographie *WS 2012/13*
Barbara Baumeister

11. Übungsblatt

Abgabe: Donnerstag, 10.1.2013

Aufgabe 1 Gegeben sei das Alphabet $\mathcal{A} = \{A, \ldots, Z\}$ und die elliptische Kurve $E : y^2 = x^3 + 300x + 1011$. Es sollen Wörter der Länge 2 über $\mathcal{A}$ in Punkte der elliptischen Kurve "umgewandelt" werden, so dass mit einer Wahrscheinlichkeit von höchstens $1/1000$ zu k gegebenen Werten x_i ein Punkt auf der Kurve mit x-Koordinate gleich x_i existiert. Wählen Sie eine geeigneten Körper und wandeln Sie das Wort "Lernen" in Punkte der Kurve um.

Einschub Sei $E : y^2 = x^3 + ax + b$ eine elliptische Kurve über dem endlichen Körper K ungerader Charakteristik. Falls die Gruppe $E(K)$ ein Element der Ordnung 4 und genau ein Element der Ordnung 2 enthält, dann gibt es ein Nichtquadrat $d \in K$ so, dass wir von der elliptischen Kurve zu einer sogenannten *Edwardskurve*

$$\mathrm{Ed} : x^2 + y^2 = 1 + dx^2y^2$$

über K übergehen können. Also anstelle von $E(K)$ können wir dann

$$\mathrm{Ed}(K) = \{(x, y) \mid x, y \in K, x^2 + y^2 = 1 + dx^2y^2\}$$

betrachten. $\mathrm{Ed}(K)$ hat auch den Vorteil, dass es hier eine geschlossene Additionsformel gibt:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}\right)$$

für $(x_1, y_1), (x_2, y_2) \in \mathrm{Ed}(K)$. Mit dieser Verknüpfung ist $\mathrm{Ed}(K)$ eine abelsche Gruppe.

Aufgabe 2 Gegeben sei die Edwardskurve $\mathrm{Ed} : x^2 + y^2 = 1 + dx^2y^2$ über einem endlichen Körper K ungerader Charakteristik. Ferner sei d ein Nichtquadrat in K. Zeige:

(a) $(0, 1)$ ist das neutrale Element in $\mathrm{Ed}(K)$.

(b) Es gilt $-(x, y) = (-x, y)$ für alle $(x, y) \in \mathrm{Ed}(K)$.

(c) Ed(K) enthält genau ein Element der Ordnung 2.

(d) Ed(K) enthält stets ein Element der Ordnung 4.

Aufgabe 3 Sei Ed : $x^2 + y^2 = 1 + 2x^2y^2$ eine Edwardskurve über $K = \mathbb{Z}_5$.

(a) Bestimmen Sie die K-rationalen Punte auf Ed(K).

(b) Zeigen Sie, dass Ed(K) zyklisch ist.

Wir – Herr Petersen und Frau Baumeister – wünschen
schöne Weihnachten