Elliptische Kurven

Kevin Kappelmann, Lukas Stevens

15. April 2016

Inhaltsverzeichnis

Darstellungsformen nicht vergessen! Edwards Kurven und so
Beispiel zitat [1, Kapitel 5, S. 215]

1 Motivation und Geschichte

Moderne asymmetrische Verschlüsselungsverfahren wie RSA leiden oft Macht Kevin Einleitung, warum elliptische Kurven, etc. (geschichtliches?)

2 Grundbegriffe

2.1 Affine Ebenen

Definition, Beispiele

2.2 Projektive Ebenen

Definition

2.2.1 Die projektive Ebene PG(2, $\mathbb{F}$)

Konstruktion, Beispiel

2.2.2 Konstruktion affiner Ebenen aus projektiven Ebenen

Beweis, Beispiel

3 Elliptische Kurven E

Macht Lukas

3.1 Definiton elliptischer Kurven

Wir haben bereits die projektive Ebene PG(2, $\mathbb{F}$) über beliebige Körper $\mathbb{F}$ eingeführt. Diese hat die folgende Punktemenge:

$$P = \left\{(u : v : w) \,|\, (u, v, w) \in \mathbb{F}^3 \setminus (0, 0, 0)\right\} \tag{1}$$

Nun wollen wir die Punktemenge der elliptischen Kurve einführen. Dazu benötigen wir Polynome in drei Unbestimmten. Der Polynomring mit drei Unbestimmten über $\mathbb{F}$ ist mit

$$\mathbb{F}[X, Y, Z] = \left\{ \sum_{k,l,m \geq 0} a_{k,l,m} \, X^k Y^l Z^m \,|\, a_{k,l,m} \in \mathbb{F} \right\} \tag{2}$$

definiert. Bemerkung von Kevin: Ich würde Unbekannte statt Unbestimmte verwenden. Ist der gebräuchliche Begriff dazu.

3.2 Die unendliche Gerade über PG(2, $\mathbb{F}$)

Isomorphismus von $\mathbb{F}^2 \to \mathcal{P}_U$

3.3 Affine Darstellung elliptischer Kurven

Erklärung, Beispiel(Graphen)

4 Eine Gruppe über E

Macht Kevin bis 4.3

4.1 Tangenten elliptischer Kurven

4.2 Schnittpunkte von Geraden mit elliptischen Kurven

Unendlich ferne Gerade mit Schnittpunkt $\mathcal{O}$, Affine Geraden, Parallele zur y-Achse

4.3 Die Schnittpunkt-Verknüpfung $\oplus$ über E

Definition, Beweis der Abgeschlossenheit, graphische Interpretation

4.4 Die Gruppe $(E, +)$

Macht Lukas bis fertig
Gruppe ist abelsch mit neutralem Element $\mathcal{O}$, Beispiel

5 Anwendung elliptischer Kurven in der Kryptologie

5.1 ElGamal

Welche Charakteristiken für elliptische Kurven, Domänenparameter

5.2 Noch einen für Signaturen

Welche Charakteristiken für elliptische Kurven, Domänenparameter

Literatur

[1] Test author. Elliptic bla bla, 2012.