Elliptische Kurven

Kevin Kappelmann, Lukas Stevens

29. März 2016

Inhaltsverzeichnis

1 Abstract

Was wird in dieser Arbeit behandelt.

2 Motivation

Einleitung, warum elliptische Kurven, etc. (geschichtliches?)

3 Grundbegriffe

3.1 Affine Ebenen

Definition, Beispiele

3.2 Projektive Ebenen

Definition

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

Konstruktion, Beispiel

3.2.2 Konstruktion affiner Ebenen aus projektiven Ebenen

Beweis, Beispiel

4 Elliptische Kurven E

4.1 Definiton elliptischer Kurven

Weierstraßgleichung, Nullstellenmenge des Polynoms, Charakteristiken(Singularitäten), affine Koordinatentransformation?

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

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

4.3 Affine Darstellung elliptischer Kurven

Erklärung, Beispiel(Graphen)

5 Eine Gruppe über E

5.1 Tangenten elliptischer Kurven

5.2 Schnittpunkte von Geraden mit elliptischen Kurven

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

5.3 Die Schnittpunkt-Verknüpfung $\oplus$ über E

Definition, Beweis der Abgeschlossenheit, graphische Interpretation

5.4 Die Gruppe $(E, +)$

Gruppe ist abelsch mit neutralem Element $\mathcal{O}$, Beispiel

6 Anwendung elliptischer Kurven in der Kryptologie

6.1 Elgamal mit der Gruppe $(E, +)$

Beschreibung, Beispiel

6.2 Effizienz und Sicherheit

Schlüssellänge im Vergleich zu RSA u.ä., Eigenschaften der Domänenparameter

6.3 Weitere Anwendungen und Algorithmen?

7 Fazit und Ausblick