

Elliptische-Kurven-Kryptographie

Kevin Kappelmann, Lukas Stevens

22. April 2016

Inhaltsverzeichnis

1	Einleitung und Motivation	1
2	Grundbegriffe	1
2.1	Affine Ebenen	1
2.2	Projektive Ebenen	3
2.2.1	Die projektive Ebene $\text{PG}(2, \mathbb{F})$	3
2.2.2	Konstruktion affiner Ebenen aus projektiven Ebenen	3
3	Elliptische Kurven E	4
3.1	Die unendliche Gerade über $\text{PG}(2, \mathbb{F})$	4
3.2	Definiton elliptischer Kurven	4
3.3	Affine Darstellung elliptischer Kurven	5
4	Eine Gruppe über E	5
4.1	Tangenten elliptischer Kurven	6
4.2	Schnittpunkte von Geraden mit elliptischen Kurven	6
4.3	Die Schnittpunkt-Verknüpfung \oplus über E	6
4.4	Die Gruppe $(E, +)$	6
5	Anwendung elliptischer Kurven in der Kryptologie	6
5.1	ElGamal	6
5.2	Noch einen für Signaturen	6

Abbildungsverzeichnis

1	Minimalmodell einer affinen Ebene	2
2	Parallelen in der euklidischen Ebene	2
3	Fano-Ebene	3
4	Kurven mit Singularitäten(Knoten und Spitze)	5

Tabellenverzeichnis

1	Vergleich Schlüssellängen	1
---	-------------------------------------	---

1 Einleitung und Motivation

Kryptosysteme wie RSA, Diffie-Hellman¹ und ElGamal¹, die sich auf die Schwere der Primfaktorzerlegung bzw. dem diskreten Logarithmenproblem über Ganzzahlen stützen, benötigen sehr große Schlüssellängen, um eine ausreichend hohe Sicherheit zu garantieren. Daraus ergibt sich sowohl ein hoher Energie- als auch Speicherbedarf für die Berechnung der Algorithmen, was vor allem für Microchips und eingebettete Systeme ein Problem darstellt.

Eine Lösung für dieses Problem sind elliptische Kurven. Diese algebraischen Kurven tragen eine Gruppenstruktur, über die das diskrete Logarithmenproblem deutlich schwerer lösbar ist, als über Gruppen mit Ganzzahlen. Kryptosysteme, die auf elliptische Kurven beruhen, kommen dadurch mit erheblich kürzeren Schlüsseln bei vergleichbarer Sicherheit aus. [2, Seite 53]

Nachfolgende Tabelle verdeutlicht diesen Sachverhalt. Spalte 1 kennzeichnet die maximale Sicherheit (in Bits) für den jeweiligen Algorithmus und der angegebenen Schlüssellänge (in Bits). Rot markierte Felder gelten als kryptographisch unsicher, grüne als aktuell sicher.

Sicherheitsniveau	RSA/Diffie-Hellman ¹	Elliptische-Kurven
≤ 80	1024	160-223
112	2048	224-255
128	3072	256-383
192	7680	384-511
256	15360	512+

Tabelle 1: Vergleich Schlüssellängen

Die Verwendung elliptischer Kurven in der Kryptographie wurde Mitte der 1980er Jahre von Neal Koblitz [5] und Victor S. Miller [6] unabhängig voneinander vorgeschlagen. Aufgrund der vorteilhaften Eigenschaften gewinnt die **Elliptische-Kurven-Kryptographie** (kurz **ECC** für Elliptic Curves Cryptography) stets mehr an Bedeutung und löst ältere Verfahren wie RSA in den verschiedensten Bereichen ab. Vor allem in Umgebungen mit begrenzten Kapazitäten, wie z.B. Smartcards, ist ECC bereits weit verbreitet.

So verwendet beispielsweise Österreich seit 2004 als Vorreiter für alle gängigen Bürgerkarten ECC [1]. Aber auch die Reisepässe der meisten Europäischen Staaten nutzen inzwischen meist in einer Form ECC. [8]

2 Grundbegriffe

Um elliptische Kurven einführen zu können, müssen wir uns zunächst mit affiner und projektiver Geometrie und ihrer Verwandtheit auseinander setzen. Wir führen hierfür zunächst allgemein die Begriffe der affinen und projektiven Ebene ein und konstruieren uns eine projektive Ebene $PG(2, \mathbb{F})$ über einen beliebigen Körper \mathbb{F} .

2.1 Affine Ebenen

Definition 2.1. Es sei \mathcal{A} eine Menge und \mathcal{G} eine Teilmenge der Potenzmenge von \mathcal{A} , d.h. $\mathcal{G} \subseteq Pot(\mathcal{A})$. Die Menge \mathcal{A} nennt man die **Punktmenge** und die Menge \mathcal{G} die **Geradenmenge**

¹In der jeweiligen Implementierung als Gruppe über ganze Zahlen

der affinen Ebene $(\mathcal{A}, \mathcal{G})$, falls folgende drei Bedingungen erfüllt sind:

- (A1) Zu je zwei Elementen $a, b \in \mathcal{A}$ mit $a \neq b$ existiert genau ein $G \in \mathcal{G}$ mit $a, b \in G$ (durch zwei verschiedene Punkte geht genau eine Gerade).
Wir schreiben $\overline{a, b}$ für dieses G .
- (A2) Zu $G \in \mathcal{G}$ und $a \in \mathcal{A} \setminus G$ existiert genau ein $G' \in \mathcal{G}$ mit $a \in G'$ und $G \cap G' = \emptyset$ (durch jeden Punkt geht genau eine Gerade, die zu einer gegebenen Gerade parallel ist).
Das sogenannte **Parallelenaxiom**.
- (A3) Es existieren drei Elemente $a, b, c \in \mathcal{A}$ mit $c \notin \overline{a, b}$ (es gibt drei Punkte, die nicht alle auf einer Gerade liegen).

Beispiel 2.2. Das **Minimalmodell** einer affinen Ebene umfasst genau 4 Punkte. [4, Seite 16]

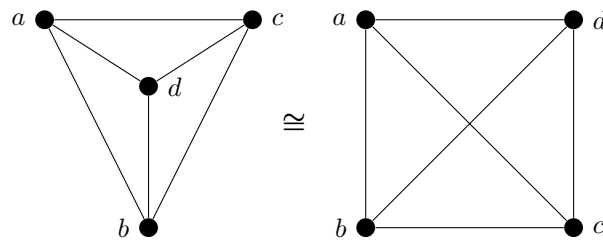


Abbildung 1: Minimalmodell einer affinen Ebene

Beispiel 2.3. Die euklidische Ebene (“Der zweidimensionale Raum unserer Anschauung”) ist eine affine Ebene, in der zusätzlich Längen- und Winkelmaß definiert sind.

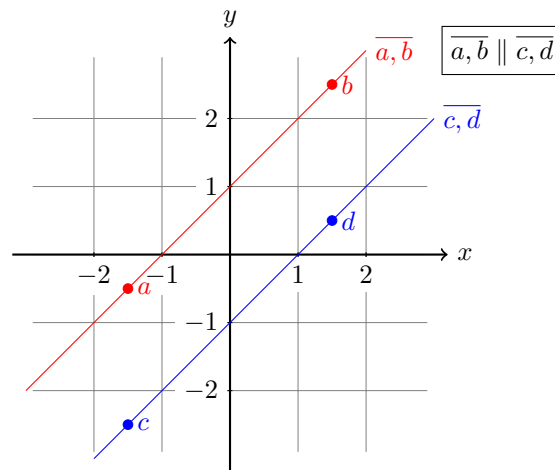


Abbildung 2: Parallelen in der euklidischen Ebene

2.2 Projektive Ebenen

Definition 2.4. Es sei \mathcal{P} eine Menge und \mathcal{G} eine Teilmenge der Potenzmenge von \mathcal{P} , d.h. $\mathcal{G} \subseteq \text{Pot}(\mathcal{P})$. Die Menge \mathcal{P} nennt man die **Punktmenge** und die Menge \mathcal{G} die **Geradenmenge** der projektiven Ebene $(\mathcal{P}, \mathcal{G})$, falls folgende drei Bedingungen erfüllt sind:

- (P1) Zu je zwei Elementen $P, Q \in \mathcal{P}$ mit $P \neq Q$ existiert genau ein $G \in \mathcal{G}$ mit $P, Q \in G$ (durch zwei verschiedene Punkte geht genau eine Gerade).
Wir schreiben $\overline{P, Q}$ für dieses G .
- (P2) Für je zwei $G, H \in \mathcal{G}$ mit $G \neq H$ gilt $|G \cap H| = 1$ (zwei verschiedene Geraden schneiden sich in genau einem Punkt).
- (P3) Es existieren vier verschiedene Elemente in \mathcal{P} , sodass immer höchstens zwei davon in jedem beliebigen $G \in \mathcal{G}$ liegen (es gibt vier Punkte, sodass nie drei davon auf derselben Gerade liegen).

Im wesentlichen Unterschied zu affinen Ebenen existieren in einer projektiven Ebene **keine Parallelen**.

Beispiel 2.5. Die **Fano-Ebene** ist das Minimalmodell einer projektiven Ebene und umfasst genau 7 Punkte. *TODO Quelle fuer minimalitaet*

Bemerkenswert ist die Tatsache, dass durch Entfernen einer beliebigen Gerade und den daraufliegenden Punkten eine affine Ebene entsteht. Dies ist kein Spezialfall sondern funktioniert immer, was wir auch im Abschnitt 2.2.2 zeigen werden.

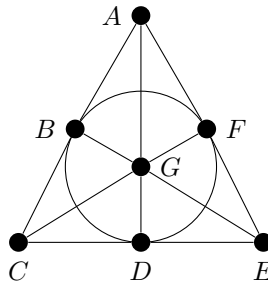


Abbildung 3: Fano-Ebene

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

Konstruktion, Beispiel

2.2.2 Konstruktion affiner Ebenen aus projektiven Ebenen

Beweis, Beispiel

Lemma 2.6. \mathcal{P}_U und \mathcal{G}_U definieren.

3 Elliptische Kurven E

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

Um in 3.2 elliptische Kurven genau beschreiben zu können und in 3.3 eine affine Darstellung elliptischer Kurven herzuleiten, müssen wir $(\mathcal{P}, \mathcal{G}) = \text{PG}(2, \mathbb{F})$ nochmal betrachten. Wir wählen dazu eine Gerade $U \in \mathcal{G}$ aus. Prinzipiell kann dazu jede Gerade gewählt werden. Es ist jedoch von Vorteil eine bestimmte Gerade zu wählen um das Rechnen mit der Weierstraßgleichung(3.2) zu vereinfachen.

Dazu wählen wir die Verbindungsgerade $U = \overline{P, Q}$ der Punkte $P = (1 : 0 : 0)$ und $Q = (0 : 1 : 0)$, d.h. $U = \{(x : y : z) \in \mathcal{P} \mid z = 0\}$. Diese Menge U bezeichnen wir im Folgenden als unendlich ferne Gerade. Im dreidimensionalen Raum ist das genau die x, y -Ebene mit $z = 0$.

Lemma 3.1 (Isomorphismus von \mathcal{P}_U und \mathbb{F}^2). *Gegeben die projektive Ebene $(\mathcal{P}, \mathcal{G}) = \text{PG}(2, \mathbb{F})$ und die unendlich ferne Gerade U , dann ist die Abbildung*

$$\phi : \mathbb{F}^2 \rightarrow \mathcal{P}_U, (a, b) \mapsto (a : b : 1)$$

bijektiv und bildet Geraden auf Geraden ab, d.h. ϕ ist ein Isomorphismus von affinen Ebenen.

Beweis. Wie im Lemma 2.6 gezeigt wurde, erhält man eine affine Ebene, wenn man aus einer projektiven Ebene eine Gerade mitsamt allen ihren Punkten entfernt. Daraus folgt, dass es sich bei $(\mathcal{P}_U, \mathcal{G}_U)$ um eine affine Ebene handelt. Es sei $(a : b : c) \in \mathcal{P}_U$. Da gilt $(a : b : c) \notin U$, folgt $c \neq 0$. Das heißt c^{-1} ist definiert, womit die Abbildung

$$\phi(ac^{-1}, bc^{-1}) = (ac^{-1} : bc^{-1} : 1) = (a : b : c)$$

surjektiv ist. Die Injektivität gilt auch, da mit $(a, b) \neq (a', b')$ die Vektoren $(a, b, 1)$ und $(a', b', 1)$ linear unabhängig sind, womit $(a : b : 1) \neq (a' : b' : 1)$ folgt. TODO Rest des Lemmas \square

3.2 Definiton elliptischer Kurven

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

$$P = \{(u : v : w) \mid (u, v, w) \in \mathbb{F}^3 \setminus (0, 0, 0)\}$$

Nun wollen wir die Punktmenge E der elliptischen Kurve einführen, welche eine Teilmenge der Punktmenge \mathcal{P} ist, d.h. $E \subseteq \mathcal{P}$. Dazu benötigen wir Polynome in drei Unbekannten. Der Polynomring mit drei Unbekannten über \mathbb{F} ist mit

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

definiert. $F(X, Y, Z) = \sum_{k, l, m \geq 0} a_{k, l, m} X^k Y^l Z^m \in \mathbb{F}[X, Y, Z]$ wird Polynom genannt.

Definition 3.2 (Elliptische Kurve). Eine elliptische Kurve E ist durch die Lösung der Weierstraß-Gleichung

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

gegeben, wobei $a_i \in \mathbb{F}$ gilt und die Lösung keine Singularitäten besitzen darf [7, Seite 54]. Da der zugrundeliegende Raum $\text{PG}(2, \mathbb{F})$ eine projektive Ebene ist, handelt es sich um eine projektive Kurve. Wenn man die Gleichung als Polynom

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

schreibt, dann ist E genau die Nullstellenmenge des Polynoms F .

Definition 3.3 (Singularitäten). Eine Kurve E ist singular in einem Punkt $P = (a : b : c) \in E$, wenn gilt

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0$$

Man sagt auch, dass die partiellen Ableitungen des Polynoms F im Punkt P verschwinden. Falls die elliptische Kurve E in keinem Punkt singular ist, dann bezeichnet man sie als nicht-singular [3, Seite 227].

Beispiel 3.4 (Singularitäten). *Die folgenden Kurven sind jeweils in einem Punkt singular. Damit gibt es mehrere Tangenten an diesen Punkt.*

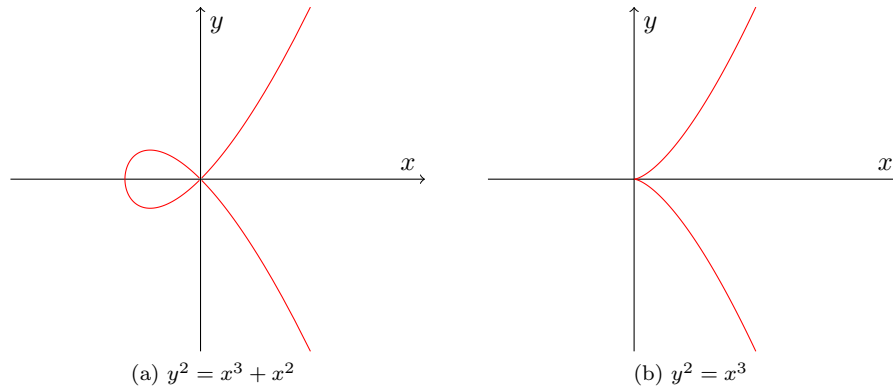


Abbildung 4: Kurven mit Singularitäten(Knoten und Spitze)

TODO char etc..

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

Literaturverzeichnis

- [1] Elliptische Kurven (Elliptic Curve Cryptography - ECC). https://www.a-sit.at/de/technologiebeobachtung/ecc_curves/index.php. Abgerufen am 15.04.2016.
- [2] Elaine Barker. Recommendation for Key Management. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf>, 2016. Abgerufen am 15.04.2016.
- [3] Hubert Kiechle Christian Karpfinger. *Kryptologie: Algebraische Methoden und Algorithmen*. 2010.
- [4] Hans-Wolfgang Henn. Elementare Geometrie und Algebra, 2003.
- [5] Neal Koblitz. Elliptic curve cryptosystems, 1987.
- [6] Victor S. Miller. Use of elliptic curves in cryptography, 1985.
- [7] J.S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006.
- [8] Zdeněk Říha. Electronic passports. https://web.archive.org/web/20100215182600/http://www.bu5lab.org/SummerSchool2008/slides/Zdenek_Riha.pdf. Archiviert vom Original, abgerufen am 15.04.2016.