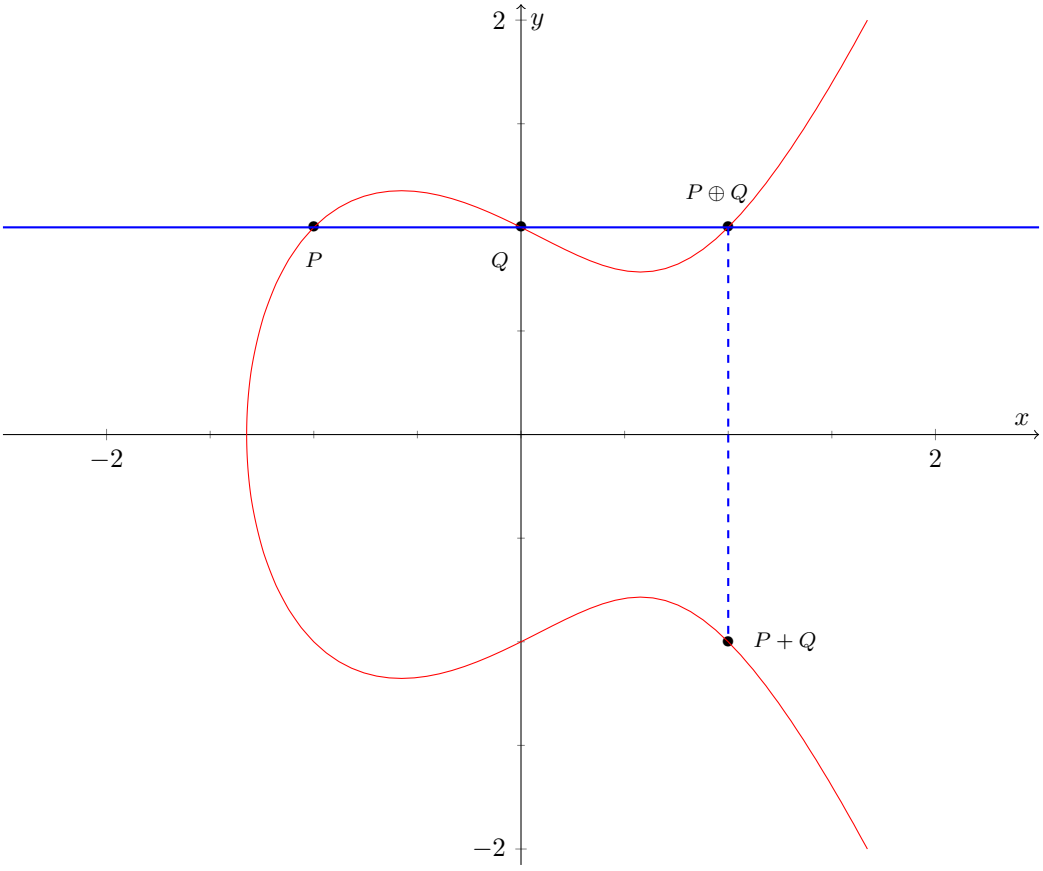
Elliptische-Kurven-Kryptographie

Kevin Kappelmann, Lukas Stevens

4. Mai 2016



Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung und Motivation

Kryptosysteme wie RSA, Diffie-Hellman[1] und ElGamal[1], die sich auf die Schwere der Primafaktorzerlegung bzw. dem diskreten Logarithmenproblem über Ganzzahlen stützen, benötigen sehr große Schlüssellängen, um eine ausreichend hohe Sicherheit zu garantieren. Daraus ergibt sich sowohl eine 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. [3, 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 [10] und Victor S. Miller [11] 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. [16]

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 $\mathrm{PG}(2, \mathbb{F})$ über einen beliebigen Körper $(\mathbb{F}, +, *)$.

In den folgenden Kapiteln kürzen wir zu Gunsten der Notation den Körper $(\mathbb{F}, +, *)$ mit $\mathbb{F}$ ab.

[1] In der jeweiligen Implementierung als Gruppe über ganze Zahlen

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** 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. [7, Seite 16]

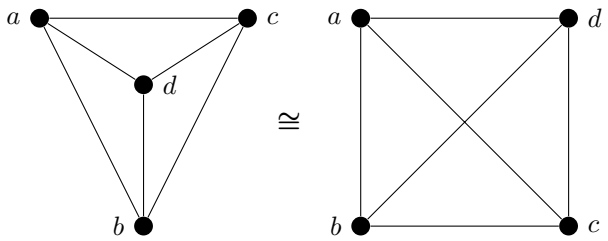


Abbildung 1: Minimalmodell einer affinen Ebene

Satz 2.3. *Es sei $\mathbb{F}$ ein beliebiger Körper und $\mathbb{F}^2$ der zweidimensionale $\mathbb{F}$-Vektorraum mit Nullvektor $\mathbf{0}$. Wir setzen*

$$\mathcal{G} \coloneqq \{a + \mathbb{F}b \mid a, b \in \mathbb{F}^2 \wedge b \neq \mathbf{0}\}$$

wobei $\mathbb{F}b = \{\lambda b \mid \lambda \in \mathbb{F}\}$ den von b erzeugten eindimensionalen Untervektorraum von $\mathbb{F}^2$ darstellt. Dann ist $(\mathbb{F}^2, \mathcal{G})$ eine affine Ebene.

Beweis. Wir verweisen hier auf [4, Seite 87]. □

Beispiel 2.4. Wählen wir für $\mathbb{F}$ den Körper $\mathbb{R}$, so erhalten wir für $(\mathbb{R}^2, \mathcal{G})$ die reelle affine Ebene (*"Den zweidimensionalen Raum unserer Anschauung"*) mit Punkten und Geraden in der uns üblichen Interpretation.

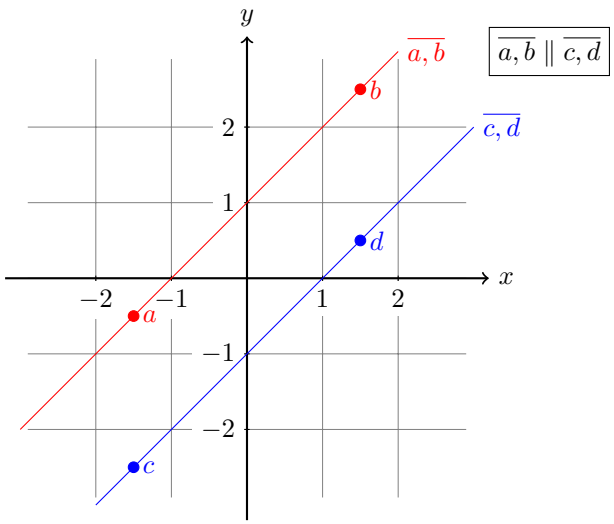


Abbildung 2: Parallelen in der reellen affinen Ebene

2.2 Projektive Ebenen

Definition 2.5. Es sei $\mathcal{P}$ eine Menge und $\mathcal{G}$ eine Teilmenge der Potenzmenge von $\mathcal{P}$, d.h. $\mathcal{G} \subseteq Pot(\mathcal{P})$. 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 2.6. Die **Fano-Ebene** ist das Minimalmodell einer projektiven Ebene und umfasst genau 7 Punkte (beachte: auch der Kreis gilt hier als Gerade!). [5, Seite 9]
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.

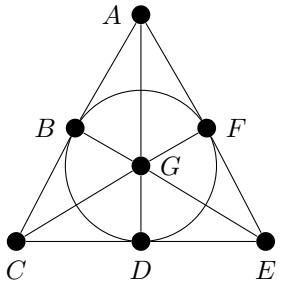


Abbildung 3: Fano-Ebene

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

Es sei $\mathbb{F}$ ein beliebiger Körper mit Nullelement 0 und $\mathbb{F}^3$ der dreidimensionale $\mathbb{F}$-Vektorraum mit Nullvektor $\mathbf{0}$. Wir definieren eine Äquivalenzrelation $\sim$ für alle $a, b \in \mathbb{F}^3 \setminus \{\mathbf{0}\}$ wie folgt:

$$a \sim b \Leftrightarrow \exists \lambda \in \mathbb{F} \setminus \{0\} : \lambda a = b$$

Wir schreiben $[a]$ oder auch $(a_1 : a_2 : a_3)$ für die Äquivalenzklassen von $a = (a_1, a_2, a_3) \in \mathbb{F}^3 \setminus \{\mathbf{0}\}$.
Man bemerke: Für einen Vektor $a \in \mathbb{F}^3 \setminus \{\mathbf{0}\}$ stellt $[a] \cup \{\mathbf{0}\}$ gerade den von a aufgespannten eindimensionalen Untervektorraum $\langle a \rangle = \mathbb{F}a = \{\lambda a \mid \lambda \in \mathbb{F}\}$ dar.

Weiters definieren wir uns die *Quotientenmenge*, d.h. die Menge aller Äquivalenzklassen, als unsere Punktmenge:

$$\mathcal{P} \coloneqq (\mathbb{F}^3 \setminus \{\mathbf{0}\})/\sim = \big\{[a] \mid a \in \mathbb{F}^3 \setminus \{\mathbf{0}\}\big\}$$

$\mathcal{P}$ stellt ein sogenanntes **homogenes Koordinatensystem** dar. Im Gegensatz zu den uns vertrauten (inhomogenen) Koordinaten, die jeden Punkt eindeutig identifizieren, haben homogene Koordinaten die Eigenschaft, dass sie für einen gegebenen Punkt nicht eindeutig bestimmt sind. So wird beispielsweise der Punkt $P = (2, 4, 8) \in \mathbb{R}^3$ sowohl von den homogenen Koordinaten $(1 : 2 : 4)$ als auch $(2 : 4 : 8)$ beschrieben.

Für zwei Punkte $P = [a], Q = [b] \in \mathcal{P}$ mit $P \neq Q$ setzen wir die Verbindungsgerade zwischen P und Q fest mit:

$$\overline{P, Q} \coloneqq \big\{[\lambda a + \mu b] \mid (0, 0) \neq (\lambda, \mu) \in \mathbb{F}^2\big\}$$

Mit $\lambda = 1$ und $\mu = 0$ bzw. $\lambda = 0$ und $\mu = 1$ folgt direkt $P, Q \in \overline{P, Q}$.

Nun bilden wir noch die Menge aller Geraden:

$$\mathcal{G} \coloneqq \{\overline{P, Q} \mid P, Q \in \mathcal{P} \wedge P \neq Q\}$$

Man beachte, dass die Bedingung $[a] = P \neq Q = [b]$ gleichbedeutend ist mit der linearen Unabhängigkeit der Vektoren $a, b \in \mathbb{F}^3$. Für zwei Punkte $P, Q \in \mathcal{P}$ stellt $\overline{P, Q} \cup \{\mathbf{0}\}$ also gerade den zweidimensionalen Untervektorraum $\langle a, b \rangle = \mathbb{F}a + \mathbb{F}b = \{\lambda a + \mu b \mid \lambda, \mu \in \mathbb{F}\}$ dar. Die Menge der Punkte einer Geraden $\overline{P, Q}$ entsprechen somit der Menge der eindimensionalen Untervektorräume, die jeweils als Teilmenge in $\mathbb{F}a + \mathbb{F}b$ enthalten sind. Formell ausgedückt:

$$[c] \in \overline{[a], [b]} \Leftrightarrow \mathbb{F}c \subseteq \mathbb{F}a + \mathbb{F}b \Leftrightarrow c \in \mathbb{F}a + \mathbb{F}b$$

Definition 2.7. Es sei V ein n-dimensionaler Vektorraum, U ein beliebiger $(n-1)$-dimensionaler Untervektorraum von V und $v \in V$ beliebig. Eine Teilmenge $H \subset V$ nennt man **Hyperebene** von V, wenn gilt:

$$H = v + U = \{v + u \mid u \in U\}$$

Wird für den Vektor v der Nullvektor gewählt, so wird die erzeugte Ebene auch als *lineare Hyperebene* bezeichnet.
In unserem Fall stellt also jede Gerade $\overline{P,Q} \cup \{\mathbf{0}\}$ eine lineare Hyperebene über $\mathbb{F}^3$ dar.

Satz 2.8. *Es sei V ein n-dimensionaler Vektorraum, U ein beliebiger $(n-1)$-dimensionaler Untervektorraum von V und $v \in V$ beliebig. Jede Hyperebene $H = v + U$ lässt sich für ein geeignetes $n \in V \setminus \{\mathbf{0}\}$ äquivalent als Lösungsmenge einer homogenen linearen Gleichung beschreiben:*

$$H = \{w \in V \mid \langle n, w - v\rangle = 0\}$$

Wobei $\langle a, b\rangle$ das Standardskalarprodukt zweier Vektoren a, b darstellt.

Beweis. Wir verweisen hier auf [2, Seite 189]. □

Bemerkung: Es ergibt sich, dass n ein Normalenvektor zu H sein muss.

Satz 2.8 lässt eine alternative Definition unserer Geraden zu, die uns oft nützlich sein wird. Da alle Geraden $\overline{P,Q} \cup \{\mathbf{0}\}$ lineare Hyperebenen sind, gilt nämlich für ein geeignetes $n = (n_1, n_2, n_3) \in \mathbb{F}^3 \setminus \{\mathbf{0}\}$:

$$\overline{P,Q} = \{(a_1 : a_2 : a_3) \in \mathcal{P} \mid n_1a_1 + n_2a_2 + n_3a_3 = 0\}$$

und somit

$$[c] \in \overline{P,Q} \Leftrightarrow n_1c_1 + n_2c_2 + n_3c_3 = 0$$

Satz 2.9. *Es ist* $\mathrm{PG}(2, \mathbb{F}) \coloneqq (\mathcal{P}, \mathcal{G})$ eine projektive Ebene über $\mathbb{F}$.

Beweis. Wir müssen zeigen, dass die unter Definition 2.5 festgelegten Bedingungen (P1), (P2) und (P3) gelten.

(P1) Es sei $P, Q \in \mathcal{P}$ mit $P \neq Q$. Durch Definition unserer Menge $\mathcal{G}$ folgt direkt $\overline{P,Q} \in \mathcal{G}$. Die Eindeutigkeit ergibt sich aus (P2).

(P2) Es sei $G, H \in \mathcal{G}$ mit $P \neq Q$. Es gibt also zwei linear unabhängige Vektoren $(a, b, c), (a', b', c') \in \mathbb{F}^3 \setminus \{\mathbf{0}\}$ mit:

$$G = \{(x : y : z) \in \mathcal{P} \mid ax + by + cz = 0\} \quad \textit{und}$$
$$H = \{(x : y : z) \in \mathcal{P} \mid a'x + b'y + c'z = 0\}$$

Es folgt:

$$G \cap H = \{(x : y : z) \in \mathcal{P} \mid ax + by + cz = 0 \wedge a'x + b'y + c'z = 0\}$$

Dieses lineare Gleichungssystem hat als Lösungsmenge einen eindimensionalen Untervektorraum, also genau einen Punkt in $\mathcal{P}$. Folglich gilt $|G \cap H| = 1$.

(P3) Die vier Punkte $(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1), (1 : 1 : 1)$ erfüllen die Bedingung.

□

Beispiel 2.10. Mit Wahl von $\mathbb{F} = \mathbb{R}$ erhält man für PG(2,$\mathbb{R}$) die relle projektive Ebene, die über dasselbe Koordinatensystem, wie der euklidische Raum (*"Der dreidimensionale Raum unserer Anschauung"*), definiert ist.
Die projektiven Punkte entsprechen den eindimensionalen Untervektorräumen von $\mathbb{R}^3$, d.h. die Menge aller Geraden durch den Ursprung und die Menge der projektiven Geraden entspricht analog der Menge aller Ebenen durch den Ursprung. Der Punkt $(0,0,0)$ ist dabei nicht enthalten.
Der Schnittpunkt zweier projektiven Geraden, d.h. anschaulich betrachtet zweier Ursprungsebenen, ergibt geanu eine Ursprungsgerade, also einen projektiven Punkt.
Wählt man zwei projektive Punkte P, Q, d.h. anschaulich betrachtet zwei Ursprungsgeraden, so ergibt sich als Verbindungsgerade $\overline{P,Q}$ die Ebene, die beide Geraden umfässt und durch den Ursprung verläuft.

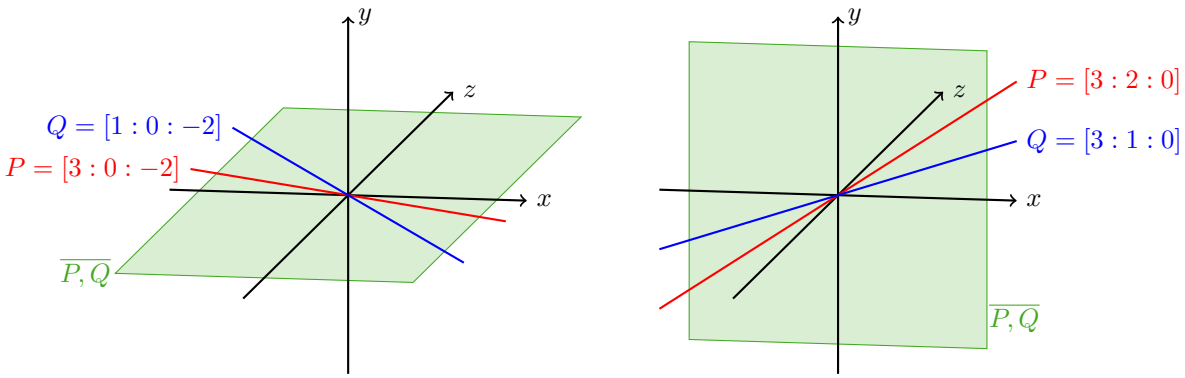


Abbildung 4: Punkte und Geraden projektiver reeller Ebenen

2.2.2 Konstruktion affiner Ebenen aus projektiven Ebenen

Wie wir bereits im Beispiel 2.6 erkannt haben, erhält man durch Entfernen einer beliebigen Gerade einer projektiven Ebene und aller sich darauf befindenden Punkten, eine affine Ebene. Dies wollen wir nun beweisen.

Satz 2.11. *Es sei $(\mathcal{P}, \mathcal{G})$ eine projektive Ebene und $U \in \mathcal{G}$ beliebig. Wir definieren:*

$$\mathcal{P}_U := \mathcal{P} \setminus U, \quad \mathcal{G}_U := \{G \cap \mathcal{P}_U \mid G \in \mathcal{G} \setminus \{U\}\} = \{G \setminus U \mid G \in \mathcal{G} \setminus \{U\}\}$$

Dann ist $(\mathcal{P}_U, \mathcal{G}_U)$ eine affine Ebene.

Beweis. Wir müssen zeigen, dass die unter Definition 2.1 festgelegten Bedingungen (A1), (A2) und (A3) gelten.

(A1) Zwei beliebige Punkte $P, Q \in \mathcal{P}_U$ sind wegen (P1) durch genau eine Gerade verbunden. Diese Gerade wurde nicht entfernt, denn sonst wären auch auch die beiden Punkte P, Q entfernt worden.

(A2) Es sei $G_U \in \mathcal{G}_U$, $G \in \mathcal{G}$ mit $G_U = G \setminus U$ und $P \in \mathcal{P}_U \setminus G_U$. Die Gerade G hatte wegen (P1) einen Schnittpunkt F mit der Geraden U, der in G_U entfernt wurde. Ebenfalls

gibt es wegen (P1) eine Gerade $H_U \in \mathcal{G}_U$ und eine Gerade $H \in \mathcal{G}$ mit $H_U = H \setminus U$, sodass $F, P \in H$. Da nach (P2) sich alle Geraden in genau einem Punkt schneiden und H und G sich im entfernten Schnittpunkt F geschnitten haben, gilt $H_U \cap G_U = \emptyset$
Jede andere Gerade in $\mathcal{G}_U$ hat nach (P2) einen Schnittpunkt mit G_U, der nicht entfernt wurde. H_U ist also die einzige Parallele von G_U durch P.

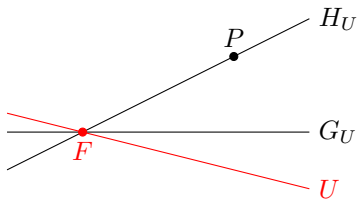


Abbildung 5: Parallelen in PG(2, $\mathbb{F}$) nach Entfernen einer Geraden

(A3) Wegen (P3) gibt es vier verschiedene Punkte $A, B, C, D \in \mathcal{P}$, sodass nie drei davon auf derselben Gerade liegen.
Lag höchstens ein Punkt auf der entfernten Gerade U, folgt die Aussage mit den drei übrigen Punkten.
Lagen zwei der vier Punkte auf U, o.B.d.A. sei dies A, B, so existiern zwei Geraden $\overline{A, C}$ und $\overline{B, D}$, die sich in einem Punkt E schneiden, der nicht inzident zu $U = \overline{A, B}$ ist. Wäre nämlich E inzident zu $\overline{A, B}$, dann würde aufgrund von (P1) $A \in \overline{B, D}$ und $B \in \overline{A, C}$ folgen, was im Widerspruch zur Annahme steht. Es gilt somit $E \in \mathcal{P}_U$.
E kann nicht inzident zu $\overline{C, D}$ sein, denn sonst würde aufgrund von (P1) $A, B \in \overline{C, D}$ gelten. Es folgt somit $E \notin \overline{C, D}$.

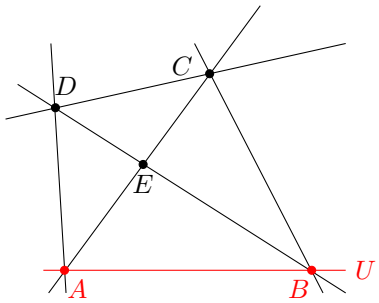


Abbildung 6: Nicht kollineare Punkte in PG(2, $\mathbb{F}$) nach Entfernen einer Geraden

□

3 Elliptische Kurven E

3.1 Die unendliche Gerade über 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 $(\mathcal{P}, \mathcal{G})$ = 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 Weierstraß-Gleichung (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 $(\mathcal{P}, \mathcal{G}) = PG(2, \mathbb{F})$ und die unendlich ferne Gerade U, dann ist die Abbildung*

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

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

Beweis. Wie im Satz 2.11 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.

Jede Gerade in $\mathbb{F}^2$ ist von der Form $\overline{a, b} = \left\{a + \lambda b \mid \lambda \in \mathbb{F} \wedge a, b \in \mathbb{F}^2 \wedge b \neq \mathbf{0}\right\}$. Für einen Punkt $P = a + \lambda b \in \overline{a, b}$ gilt dann:

$$\begin{aligned}\phi(a + \lambda b) &= (a_1 + \lambda b_1 : a_2 + \lambda b_2 : 1) = (a_1 : a_2 : 1) + \lambda(b_1 : b_2 : 0) \\ &\sim \mu(a_1 : a_2 : 1) + \mu\lambda(b_1 : b_2 : 0)\end{aligned}$$

Hierbei ist zu beachten, dass $\mu \in \mathbb{F} \setminus \{0\}$ laut Definition der Äquivalenzrelation $\sim$ gilt. Man betrachte nun die Gerade

$$G \coloneqq \left\{u(a_1 : a_2 : 1) + v(b_1 : b_2 : 0) \mid (u, v) \in \mathbb{F}^2 \setminus \{\mathbf{0}\}\right\}.$$

Alle Punkte der Bildmenge von ϕ liegen auf der Gerade G. Es wird nur ein Punkt nicht erreicht, nämlich der Punkt $R = (b_1 : b_2 : 0)$. Wie man sehen kann, gilt $G \cap U = R$. Es folgt $\phi(\overline{a, b}) = G \cap \mathcal{P}_U \in \mathcal{G}_U$. □

Insgesamt kann man sehen, dass man affine Geraden auf eine Teilmenge der projektiven Geraden abbilden kann. Außerdem bekommen diese affinen Geraden im Projektiven dann einen Schnittpunkt, der auf der unendlich fernen Gerade U liegt.

3.2 Definiton elliptischer Kurven

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

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

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. [12, Seite 54] Da der zugrundeliegende Raum PG(2, $\mathbb{F}$) eine projektive Ebene ist, handelt es sich um eine projektive Kurve. Wenn man die Gleichung als Polynom

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

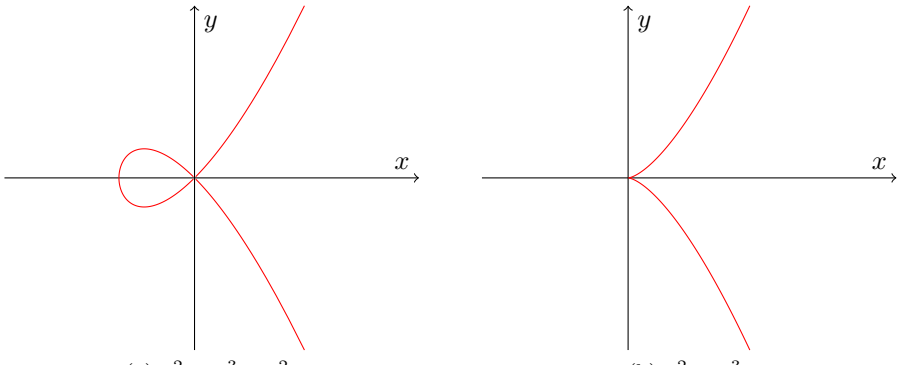
schreibt, dann ist E genau die Nullstellenmenge des Polynoms F. Bemerkenswert ist hier, dass es sich um ein homogenes Polynom vom Grad 3 handelt, d.h. für jedes Summenglied $a_{k,l,m}X^kY^lZ^m$ mit $a_{k,l,m} \neq 0$ gilt $k + l + m = 3$.

Definition 3.3 (Singularitäten)**.** Eine Kurve E ist singulär 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 singulär ist, dann bezeichnet man sie als nicht-singulär. [4, Seite 227]

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



(a) $y^2 = x^3 + x^2$ (b) $y^2 = x^3$

Abbildung 7: Kurven mit Singularitäten (Knoten und Spitze)

Wir hatten eine elliptische Kurve E als Nullstellenmenge des Polynoms $F(X, Y, Z)$ mit $E \coloneqq \{(u : v : w) \in \mathcal{P} \mid F(u, v, w) = 0\}$ definiert. Jedoch handelt es sich bei Punkten in der projektiven Ebene und damit auch bei den Elementen von E um Äquivalenzklassen. Deswegen müssen wir noch die Wohldefiniertheit der Nullstellen begründen. Wir rufen uns dazu noch einmal die Definition der Äquivalenzrelation $\sim$ ins Gedächtnis:

$$(u : v : w) \sim (u' : v' : w') \Leftrightarrow \exists \lambda \in \mathbb{F} \setminus \{0\} : (u, v, w) = \lambda(u', v', w')$$

Wir setzen ein:

$$F(u', v', w') = F(\lambda u, \lambda v, \lambda w) = \lambda^3 F(u, v, w).$$

Die zweite Äquivalenz folgt aus der Homogenität des Polynoms. Daraus folgt, dass die Nullstellen von F in $\mathcal{P}$ wohldefiniert sind:

$$F(u, v, w) = 0 \Leftrightarrow F(\lambda u, \lambda v, \lambda w) = 0.$$

Wir wollen nun noch eine Einschränkung treffen: die Charakteristik des Körpers $\mathbb{F}$ soll nicht 2 und nicht 3 sein. Wir schreiben $char\ \mathbb{F} \neq 2$ bzw. $char\ \mathbb{F} \neq 3$. Dies bedeutet, dass $1 + 1 \neq 0$ bzw. $1 + 1 + 1 \neq 0$, oder anders gesagt: Wenn wir das neutrale Element der Multiplikation 2 bzw. 3 mal addieren, dann erhalten wir nicht das neutrale Element der Addition, welches kein multiplikatives Inverses hat.
Dadurch wird die Allgemeinheit für den Fall, dass $\mathbb{F}$ eine dieser Charakteristiken hat, eingeschränkt. Grundsätzlich können die folgenden Methoden auch auf Körper mit $char\ \mathbb{F} = 2$ oder $char\ \mathbb{F} = 3$ angewandt werden. Es sind dann jedoch meistens Fallunterscheidungen notwendig. Wir verweisen dafür auf Silverman [14, Seite 44].

Wenn $char\ \mathbb{F} \neq 2$ und $char\ \mathbb{F} \neq 3$ gegeben ist, dann können wird die Weierstraß-Gleichung (3.2), welche die Form

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

hat, umformen. Mit einer Koordinatentransformation kann man die Gleichung

$$Y^2Z = X^3 + aXZ^2 + bZ^3 \tag{1}$$

herleiten [12, Seite 50].

3.3 Affine Darstellung elliptischer Kurven

Wir wollen eine affine Darstellung herleiten. Dazu zeigen wir zunächst, dass nur ein Punkt der unendlich fernen Gerade U, nämlich der Punkt $\mathcal{O} = (0 : 1 : 0)$, auf E liegt. Für $P \in U$ gilt $P = (u : v : 0)$ mit $u, v \in \mathbb{F}$. Es gibt, bis auf Äquivalenz, drei Möglichkeiten Punkte zu erzeugen, die 0 als Z-Koordinate haben: $P = (1 : 0 : 0)$, $Q = (u : v : 0)$ mit $u, v \in \mathbb{F} \setminus \{0\}$ und $\mathcal{O} = (0 : 1 : 0)$. Wenn wir diese Punkte in die Gleichung (1) einsetzen, dann löst nur $\mathcal{O}$ die Gleichung.
Deswegen gilt für jeden Punkt $P \in E$ mit $P \neq \mathcal{O}$, dass die Z-Koordinate ungleich null ist. Es gilt also $P \in \mathcal{P}_U$, d.h. alle Punkte, bis auf $\mathcal{O}$, liegen auf dem affinen Teil der projektiven Ebene PG(2, $\mathbb{F}$) . Aufgrund der Äquivalenzrelation $\sim$ können wir o.B.d.A. annehmen, dass $P \in \{(u : v : 1) \mid u, v \in \mathbb{F}\}$. Wenn wir also nur diese Punkte betrachten, können wir die Gleichung (1) vereinfachen und erhalten die affine Gleichung $y^2 = x^3 + ax + b$ oder als Polynom:

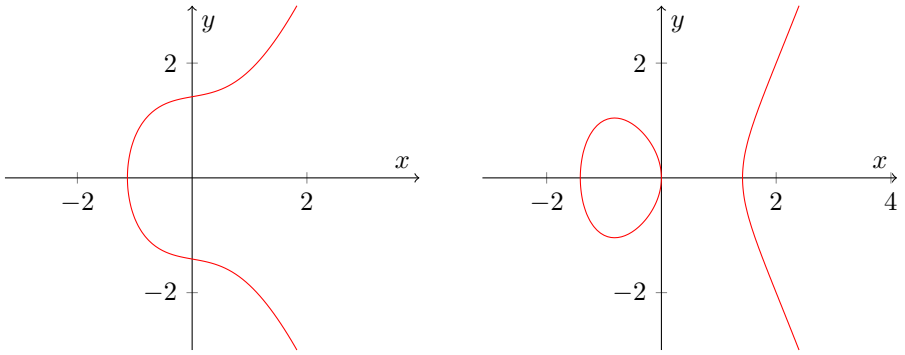
$$f(x, y) \coloneqq y^2 - x^3 - ax - b \tag{2}$$

Wir wissen aus Satz 2.11, dass $\mathcal{P}_U$ genau die Punktmenge einer affinen Ebene ist. Wenn wir zusätzlich die Abbildung ϕ aus Lemma 3.1 auf $\mathcal{P}_U$ anwenden, dann zerfällt die Punktmenge der elliptischen Kurve E in zwei Teilmengen, einen affinen Teil und den unendlichen Punkt $\mathcal{O}$:

$$E = \{(u : v : 1) \mid (u, v) \in \mathbb{F}^2 \wedge f(u, v) = 0\} \cup \{\mathcal{O}\} \tag{3}$$

Wir können im Anschluss nur den affinen Teil betrachten, wenn wir den Punkt $\mathcal{O}$ nicht außer Acht lassen.

Beispiel 3.5. Skizzen elliptischer Kurven über dem Körper $\mathbb{R}$.



(a) $y^2 = x^3 + 0.5x + 2$ (b) $y^2 = x^3 - 2x$

Abbildung 8: Beispiele elliptischer Kurven

4 Eine Gruppe über E

Nachdem wir die Menge E einer elliptischen Kurve definiert haben, wollen wir nun eine abelsche Gruppe über diese Menge konstruieren. Hierzu führen wir zunächst Tangenten für die Punktmenge elliptischer Kurven ein und stellen dann eine Verknüpfungsoperation auf.

In den folgenden Kapiteln beschränken wir uns auf auf elliptische Kurven E über Körpern $\mathbb{F}$ mit folgenden Voraussetzungen:

- Es gelte $char\ \mathbb{F} \neq 2, 3$
- E sei nicht singulär, d.h. insbesondere das Polynom $x^3 + ax + b \in \mathbb{F}[x]$ hat keine mehrfache Nullstelle.

4.1 Tangenten elliptischer Kurven

Definition 4.1. Es sei P ein Punkt der elliptischen Kurve E. Wir definieren die Tangente an E im Punkt P:

$$T_P := \left\{(u : v : w) \in \mathcal{P} \mid \frac{\partial F}{\partial X}(P)u + \frac{\partial F}{\partial Y}(P)v + \frac{\partial F}{\partial Z}(P)w = 0\right\}$$

Wir zeigen nun, dass T_P eine Gerade in $\mathrm{PG}(2, \mathbb{F})$ ist, die den Punkt P enthält. Wie gewohnt bezeichne $U = \{(x : y : z) \in \mathcal{P} \mid z = 0\}$ die unendlich ferne Gerade.

Lemma 4.2. *Es sei P ein Punkt der elliptischen Kurve E. Dann gilt $T_P \in \mathcal{G}$ und $P \in T_P$.*

Beweis. Wir bestimmen die partiellen Ableitungen von F:

$$\frac{\partial F}{\partial X} = -3X^2 - aZ^2, \quad \frac{\partial F}{\partial Y} = 2YZ, \quad \frac{\partial F}{\partial Z} = Y^2 - 2aZX - 3bZ^2$$

1. Fall: $P = \mathcal{O} = (0 : 1 : 0)$. Dann gilt:

$$\frac{\partial F}{\partial X}(\mathcal{O}) = \frac{\partial F}{\partial Y}(\mathcal{O}) = 0, \quad \frac{\partial F}{\partial Z}(\mathcal{O}) = 1$$

Das bedeutet:

$$T_{\mathcal{O}} = \{(u : v : w) \in P \mid 0u + 0v + 1w = 0\} = \{(u : v : w) \in P \mid w = 0\} = U$$

Die Tangente im Punkt $\mathcal{O}$ ist also genau die unendlich ferne Gerade U.

2. Fall: $P \neq \mathcal{O}$. Es gilt also $P \notin U$ womit wir ohne Einschränkung $P = (x : y : 1)$ voraussetzen können. Für die Tangente erhalten wir:

$$T_P = \{(u : v : w) \in P \mid (-3x^2 - a)u + 2yv + (y^2 - 2ax - 3b)w = 0\}$$

T_P stellt also ein lineares homogenes Gleichungssystem mit drei Variablen u, v, w dar und besitzt somit als Lösungsmenge einen zweidimensionalen Untervektorraum von $\mathbb{F}^3$, falls nicht alle Koeffizienten gleich 0 sind. Hieraus folgt, dass T_P eine Gerade in $\mathrm{PG}(2, \mathbb{F})$ ist.
Wir zeigen nun, dass im Fall $y = 0$ sofort $3x^2 + a \neq 0$ folgt, also immer mindestens ein Koeffizient des Gleichungssystems nicht 0 ist.
Sei also $y = 0$. Dann gilt $x^3 + ax + b = 0$, da $P = (x : 0 : 1)$ auf E liegt. Dieses Polynom hat nach Voraussetzung keine mehrfachen Nullstellen, deshalb ist x nicht Nullstelle der Ableitung $3x^2 + a$, also $3x^2 + a \neq 0$.
Nun müssen wir noch $P \in T_P$ zeigen. Dazu setzen wir den Punkt P in das Gleichungssystem für T_P ein:

$$\begin{aligned}(-3x^2 - a)x + 2yy + (y^2 - 2ax - 3b) &= -3x^3 - 3ax + 3y^2 - 3b \\ &= 3\underbrace{(y^2 - x^3 - ax - b)}_{=f(x,y)=0} \overset{(3)}{=} 0\end{aligned}$$

Folglich gilt $P \in T_P$. □

Beispiel 4.3. Wir bestimmen die Tangente an E über $F(X, Y, Z) = Y^2Z - X^3 + 2XZ^2$ im Punkt $P = (0 : 0 : 1)$. Die Ableitungen sind:

$$\frac{\partial F}{\partial X} = -3X^2 + Z, \quad \frac{\partial F}{\partial Y} = 2YZ, \quad \frac{\partial F}{\partial Z} = Y^2 + 4XZ$$

Somit folgt:

$$\frac{\partial F}{\partial X}(P) = 1, \quad \frac{\partial F}{\partial Y}(P) = 0, \quad \frac{\partial F}{\partial Z}(P) = 0$$

Für die Tangente ergibt sich also:

$$T_P = \{(u : v : w) \in \mathcal{P} \mid u = 0\}$$

Affin gedeutet ist P der Nullpunkt und T_P genau die y-Achse. Die Tangente entspricht genau dem, was man sich anschaulich als Tangente für den Punkt vorstellen würde. Dies ist in Abbildung 8(b) sichtbar.

Nun wollen wir die Tangenten der Kurve E ins affine Übersetzen. Die affine Darstellung wird uns dabei vor allem in Abschnitt 4.3 als nützlich erweisen.

Lemma 4.4. *Für $P = (x : y : 1) \in E \setminus \{\mathcal{O}\}$ dürfen wir ohne Einschränkung $P = (x, y)$ als affinen Punkt auffasen. Dann gilt:*

$$T_P \setminus U = \left\{(u, v) \mid \frac{\partial f}{\partial x}(P)(u - x) + \frac{\partial f}{\partial y}(P)(v - y) = 0\right\}$$

Beweis. Wir bestimmen die partiellen Ableitungen von F an der Stelle P:

$$\frac{\partial F}{\partial X} = -3x^2 - a = \frac{\partial f}{\partial x}, \quad \frac{\partial F}{\partial Y} = 2y = \frac{\partial f}{\partial y}, \quad \frac{\partial F}{\partial Z} = y^2 - 2ax - 3b$$

Da P auf T_P liegt gilt:

$$\frac{\partial f}{\partial x}(P)x + \frac{\partial f}{\partial y}(P)y = -\frac{\partial F}{\partial Z}(P) \tag{4}$$

Für einen beliebigen Punkt $Q \in \mathcal{P}$ erhalten wir:

$$\begin{aligned} Q \in T_P \setminus U &\Leftrightarrow Q = (u : v : 1) \in T_P \\ &\Leftrightarrow \frac{\partial F}{\partial X}(P)u + \frac{\partial F}{\partial Y}(P)v + \frac{\partial F}{\partial Z}(P) = 0 \\ &\overset{(4)}{\Leftrightarrow} \frac{\partial f}{\partial x}(P)u + \frac{\partial f}{\partial y}(P)v - \frac{\partial f}{\partial x}(P)x - \frac{\partial f}{\partial y}(P)y = 0 \\ &\Leftrightarrow \frac{\partial f}{\partial x}(P)(u - x) + \frac{\partial f}{\partial y}(P)(v - y) = 0 \end{aligned}$$

Somit gilt die Behauptung. □

Setzen wir einen Punkt $(u, v) = Q \neq P = (x, y) \neq (x, 0)$ mit $Q \in T_P \setminus U$ und somit $u \neq x$ in die Tangentengleichung ein, so können wir die Steigung von $T_P \setminus U$ bestimmen:

$$\begin{aligned} & (-3x^2 - a)(u - x) + 2y(v - y) = 0 \\ \Leftrightarrow \quad & 2y(v - y) = -(-3x^2 - a)(u - x) \\ \overset{x \neq u, y \neq 0}{\Leftrightarrow} \quad & \frac{v - y}{u - x} = \frac{3x^2 + a}{2y} \end{aligned}$$

4.2 Schnittpunkte von Geraden mit elliptischen Kurven

Bevor wir im nächsten Abschnitt eine Verknüpfungsoperation definieren, betrachten wir die Menge der Schnittpunkte einer Geraden mit der Punktmenge E.

Die unendlich ferne Gerade U schneidet die Punktmenge E nur im unendlich fernen Punkt $\mathcal{O}$. Nach Lemma 4.2 gilt $U = T_{\mathcal{O}}$.

Affine Geraden der Form $y = kx + d$ schneiden die Punktmenge E wie folgt. Wir setzen $y = kx + d$ in die Gleichung (2) ein und erhalten:

$$(kx + d)^2 = x^3 + ax + b \Leftrightarrow 0 = x^3 + ax + b - (kx + d)^2 \tag{5}$$

Dies ist eine kubische Gleichung für die x-Koordinaten der Schnittpunkte bzw. der Nullstellen. Somit gibt es im Allgemeinen drei Schnittpunkte der affinen Geraden mit E, es seien dies $(x_1, y_1), (x_2, y_2), (x_3, y_3)$.
Die drei x-Koordinaten müssen nicht voneinander verschieden sein, aber falls $x_i = x_j$ für $i \neq j$ gilt, dann auch $y_i = y_j \neq 0$ und die affine Gerade ist genau die Tangente $T_P \setminus U$ an E im Punkt $P = (x_i, y_i)$. Ist nämlich x_i eine doppelte Nullstelle der Gleichung (5), muss, da E nicht singulär ist und $x^3 + ax + b$ somit keine mehrfache Nullstelle hat, $kx_i + d \neq 0$ gelten und aufgrund der Vielfachheit der Nullstelle die folgende Gleichung, die durch Ableiten aus Gleichung (5) entsteht, erfüllen:

$$2(kx_i + d)k = 3x_i^2 + a \overset{kx_i+d\neq 0}{\Leftrightarrow} k = \frac{3x_i^2 + a}{2(kx_i + d)} = \frac{3x_i^2 + a}{2y_i}$$

Die Steigung k der affinen Gerade $y = kx + d$ entspricht somit genau der Steigung von $T_P \setminus U$. Da P sowohl auf $T_P \setminus U$ als auch auf der affinen Gerade liegt, gilt folglich Gleichheit.

Eine Parallele zur y-Achse $v + \mathbb{F}(0, 1)$ mit $v = (x, y)$ hat mit E den unendlich fernen Punkt $\mathcal{O}$ gemeinsam. Es gilt nämlich:

$$\phi(v + \lambda(0, 1)) = [\mu(x, y, 1) + \mu\lambda(0, 1, 0)]$$

Somit hat die Gerade im projektiven einen Schnittpunkt mit $\mathcal{O} = (0 : 1 : 0)$.
Außerdem hat die Gerade zwei weitere affine Schnittpunkte

$$P_{1,2} = (x, \pm\sqrt{x^3 + ax + b})$$

wobei erneut im Fall von $P_1 = P_2 = (x, 0)$ aus Lemma 4.4 mit $P_i = (x, 0)$ folgt, dass die y-Achse eine Tangente an E in P_i ist.

4.3 Die Schnittpunkt-Verknüpfung $\oplus$ über E

Satz 4.5. *Definition und Beweis* $\oplus$

4.4 Die Gruppe $(E, +)$

Die Verknüpfung $\oplus$ hat schon einige Eigenschaften, die für eine Gruppenoperation wichtig sind. Sie ist kommutativ und abgeschlossen. Jedoch fehlt eine wichtige Eigenschaft, nämlich die Existenz eines neutralen Elements. Deshalb wollen wir die Verknüpfung $\oplus$ modifizieren um eine neue Verknüpfung $+$ zu erhalten, die ein neutrales Element besitzt. Damit erhalten wir dann eine Gruppe $(E, +)$ über elliptischen Kurven.
Die Definition der Verknüpfung $+$ für $P, Q \in E$ lautet folgendermaßen:

$$P + Q \coloneqq \mathcal{O} \oplus (P \oplus Q) = -(P \oplus Q). \tag{6}$$

Und es gilt:

Satz 4.6. $(E, +)$ *ist eine abelsche Gruppe mit neutralem Element* $\mathcal{O}$.

Beweis. Aus der Kommutativität von $\oplus$ folgt die Kommutativität von $+$.
Des Weiteren gilt für alle $P \in E$:

$$\mathcal{O} + P = \mathcal{O} \oplus (\mathcal{O} \oplus P) = \mathcal{O} \oplus (-P) = P$$

Damit ist $\mathcal{O}$ das neutrale Element. Außerdem gilt noch für $P \in E$:

$$P + (-P) = \mathcal{O} \oplus (P \oplus (-P)) = \mathcal{O} \oplus \mathcal{O} = \mathcal{O}.$$

Da der Beweis für die Assoziativität sehr aufwändig ist wollen, wir diesen hier nicht erbringen und auf [15, Seite 20] verweisen. Mit Assoziativität, Kommutativität und der Existenz eines neutralen Elements mit $\mathcal{O}$ folgt, dass es sich bei $(E, +)$ um eine abelsche Gruppe handelt. □

Mit Hilfe der Formeln aus Satz 4.5 können wir die Addition $P + Q \in E$ zweier Punkte explizit formulieren. Wir setzten $P = (p_1, p_2)$ und $Q = (q_1, q_2)$. Dann gilt

$$P + Q = \begin{cases} \mathcal{O}, & \text{falls } P = -Q \text{ oder } P = Q = \mathcal{O}, \\ P, & \text{falls } Q = \mathcal{O}, \\ Q, & \text{falls } P = \mathcal{O}, \\ (\omega, -\alpha(\omega - p_1) - p_2), & \text{sonst}, \end{cases}$$

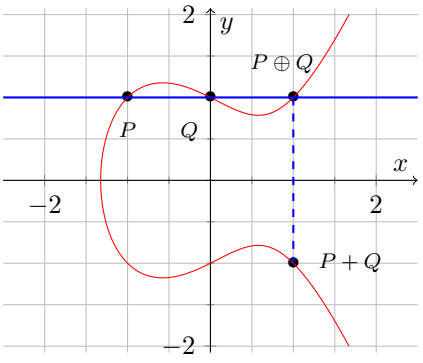
wobei

$$\omega = \alpha^2 - p_1 - q_1 \text{ und } \alpha = \begin{cases} \frac{p_2 - q_2}{p_1 - q_1}, & \text{falls } P \neq Q, -Q, \\ \frac{3p_1^2 + a}{2p_2}, & \text{falls } P = Q \neq -P. \end{cases}$$

Mit a ist hierbei der Koeffizient von x der affinen Darstellung (2) von E gemeint.

Man spricht dabei von der Sekanten-Tangenten-Konstruktion. Mit dieser Formel kann die Addition in beliebigen Körpern $\mathbb{F}$ berechnet werden ohne auf die graphische Lösung zurückzugreifen. Es ist also auch möglich Gruppen $(E, +)$ über endlichen Körpern $\mathbb{F}$ zu definieren.

Beispiel 4.7. Es ist möglich die Punkte $P = (-1, 1)$ und $Q = (0, 1)$ auf E über $\mathbb{R}$ graphisch zu addieren. Man zieht dazu eine Gerade durch die Punkte P und Q und erhält den Schnittpunkt $P \oplus Q$. Danach berechnet man den Punkt $-(P \oplus Q)$, d.h. man spiegelt an der x-Achse.



(a) $E : y^2 = x^3 - x + 1$

Abbildung 9: Addition in $(E, +)$

5 Anwendung elliptischer Kurven in der Kryptologie

Bis jetzt haben wir uns mit den mathematischen Grundlagen rund um elliptische Kurven beschäftigt. Wir haben den Begriff der projektiven Ebenen eingeführt und elliptische Kurven als eine Teilmenge dieser beschrieben. Wir haben außerdem eine Operation + über den elliptischen Kurven E eingeführt, mit der man eine Gruppe über E erhält. Die Frage ist nun, welche Relevanz diese Gruppe für die Kryptologie hat.
In der Kryptologie sind vor allem mathematische Probleme interessant, die ohne Kenntis bestimmter Variablen sehr schwer zu lösen sind. Wenn diese bestimmten Variablen bekannt sind - man spricht meist von einem Schlüssel -, dann soll das Problem jedoch leicht zu lösen sein.
Bei elliptischen Kurven wird sich dabei die Schwierigkeit des diskreten Logarithmierungsproblems zu Nutze gemacht.

5.1 Verschlüsselung und das diskrete Logarithmierungsproblem

Wir wollen zunächst das diskrete Logarithmierungsproblem wiederholen. Es ist folgendermaßen definiert:

Definition 5.1. Sei G eine Gruppe und seien $x, y \in G$. y soll die Untergruppe sein, die durch x generiert wird. Das Finden von $m \in \mathbb{N} \setminus \{0\}$, so dass gilt

$$x^m = y,$$

wird diskretes Logarithmierungsproblem(DLP) genannt. In der Kryptologie betrachten wir dabei meist endliche Gruppen.

Jede Gruppe G hat ihr eigenes Logarithmierungsproblem. Bei einer elliptischen Kurve E über dem Körper F_p kann auch ein diskretes Logarithmierungsproblem konstruiert werden. Dazu wählen wir $P, Q \in E$ und ein $m \in \mathbb{N} \setminus \{0\}$. Das diskrete Logarithmierungsproblem ist dann die Lösung der Gleichung $mP = Q$, wobei P und Q bekannt sind. Die skalare Multiplikation in der Gruppe E des Punktes P wird durch wiederholtes Addieren des Punkt mit sich selbst dargestellt. Um die Sicherheit von Verschlüsselungsverfahren zu beurteilen, die die Gruppeneigenschaft der elliptischen Kurven E verwenden, müssen wir überprüfen, wie schwer das DLP elliptischer Kurven zu lösen ist.

Der erste, naive Ansatz ist das Lösen des Problems durch Ausprobieren. Es wird mit x gestartet und die Gruppenoperation so lange angewandt, bis das Ergebnis y lautet. Damit ist die Laufzeit in $O(|E|)$. Da die Anzahl der Gruppenelemente jedoch exponentiell mit der Schlüssellänge wächst, steigt die Laufzeit des naiven Ansatzes dementsprechend exponentiell mit der Schlüssellänge. In nahezu allen Gruppen kann das DLP schneller mit dem Babystep-Giantstep Algorithmus gelöst werden, welcher eine Laufzeit von $O(\sqrt{|E|})$ hat. Dadurch ist die Laufzeit jedoch immer noch exponentiell. Ein weiteres prominentes Beispiel ist Pollard's ρ Algorithmus. Auch für diesen Algorithmus kann gezeigt werden, dass die Laufzeit in $O(\sqrt{|E|})$ ist. Somit kann auch hiermit keine subexponentielle Laufzeit erreicht werden [14, Seite 386].
In der Tat wurde bis jetzt noch kein Algorithmus gefunden, der das DLP auf allgemeinen elliptischen Kurven in subexponentieller Zeit lösen kann. Wenn man jedoch bestimmte Einschränkungen für die Parameter trifft, dann sind durchaus subexponentielle Laufzeiten möglich [9]. Verschlüsselungsverfahren, die auf elliptischen Kurven basieren, sind also bei

geeigner Wahl der Domänenparameter sicher.

Interessanterweise kann das DLP in endlichen Gruppen $\mathbb{F}_{p^n}$ in subexponentieller Laufzeit mit Hilfe sogenannter Index-Calculus-Algorithmen gelöst werden [8]. Es ist möglich diese Algorithmen so abzuwandeln, dass sie auch für Primfaktorzerlegungen und damit auch als Angriff auf RSA geeignet sind [8]. Diese Angriffe verlassen sich jedoch darauf, dass die Gruppe Primzahlen besitzt. Da die Gruppe $(E, +)$ auf elliptische Kurven keine Primzahlen besitzt, können diese Algorithmen nur in Spezialfällen auf elliptische Kurven übertragen werden. Deswegen sind elliptische Kurven, bei geeigneter Wahl der Parameter gegen diese Angriffe immun. Aufgrund dessen ist das Sicherheitsniveau von ECC im Vergleich zu RSA bei gleicher Schlüssellänge deutlich höher. Dies erklärt auch die in der Einleitung gezeigte Tabelle(1).

5.2 ElGamal

5.2.1 Schlüsselgenerierung, Verschlüsselung und Entschlüsselung

Wir wissen nun, dass das DLP auf elliptische Kurven schwer zu lösen ist. Das können wir uns jetzt zu Nutze machen um tatsächlich Nachrichten zu verschlüsseln. Deshalb möchten wir kurz auf ein Verschlüsselungsverfahren eingehen, dass auf der Gruppe $(E, +)$ funktioniert, nämlich das Elgamal-Verschlüsselungsverfahren.

Wir haben einen endlichen Körper $\mathbb{F}$, eine elliptische Kurve E über $\mathbb{F}$ und einen Punkt $G \in E$ gegeben. Der Empfänger, den wir Bob nennen, wählt eine natürliche Zahl a, berechnet $Q = aG \in E$.
Bob behält a als seinen geheimen Schlüssel. Der öffentliche Schlüssel ist dann $(\mathbb{F}, E, G, Q)$. Bob schickt anschließend der Senderin Alice den öffentlichen Schlüssel. Wenn Alice den Klartext $\mathcal{P} \in E$ nun verschlüsseln will muss sie 3 Schritte durchführen:

1. Alice wählt zufällig eine Zahl $b \in \mathbb{N}$.
2. Alice berechnet $B \coloneqq bG \in E$ und $C \coloneqq bQ + \mathcal{P} \in E$.
3. Alice sendet den Geheimtext $\mathcal{C} = (B, C)$ an Bob.

Dabei kann ein Angreifer den Klartext $\mathcal{P}$ nicht effizient berechnen, da er dafür das Logarithmierungsproblem auf elliptischen Kurven lösen müsste.

Bob hat von Alice jetzt den Geheimtext $\mathcal{C} = (B, C)$ erhalten und möchte mit Hilfe seines geheimen Schlüssels den Klartext $\mathcal{P}$ berechnen. Er berechnet dazu $-aB + C$. Da $B = bG$, $C = bQ + \mathcal{P}$ und $Q = aG$ gilt, folgt:

$$-aB + C = -abG + bQ + \mathcal{P} = -abG + abG + \mathcal{P} = \mathcal{P}.$$

So erhält Bob den Klartext $\mathcal{P} \in E$ aus dem Geheimtext $\mathcal{C}$. In der Praxis muss man ein Verfahren festlegen, wie man von einer Nachricht zu einem Punkt auf der elliptischen Kurve umwandelt.

5.2.2 Effiziente Berechnung des Skalarprodukts

Wir haben bereits gesehen, dass die Skalarmultiplikation $aP = Q$ mit $a \in \mathbb{N}$ und $P, Q \in E$ die zentrale Operation bei der Ver- und Entschlüsselung ist.

Wenn man diese naiv berechnet, d.h. man berechnet $(\dots(((P+P)+P)+P)\dots)$ von innen nach außen, dann verhält sich die Laufzeit offensichtlich linear im Bezug auf a; die genaue Anzahl der Schritte beträgt $a-1$.
Man kann jedoch die Assoziativität der Operation + ausnutzen um ein deutlich effizienteres Verfahren zu erhalten. Dabei ordnet man die einzelnen Additionen neu an.

Beispiel 5.2. Wir wollen $13P$ berechnen. Wenn man die Additionen in einem Baum anordnet können Ergebnisse wiederverwendet werden. Man muss jedes Zwischenergebnis nur einmal berechnen. In diesem Beispiel verringert sich die Anzahl der Operationen von elf beim naiven Ansatz auf fünf beim effizienten Verfahren.

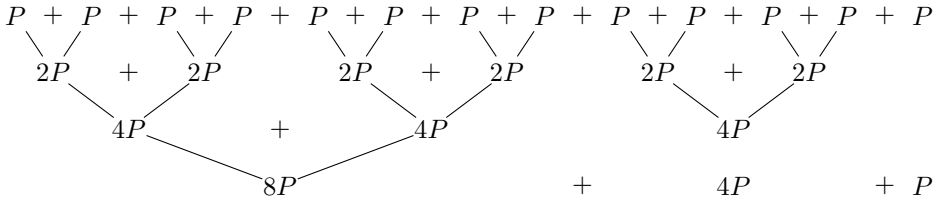


Abbildung 10: Effiziente Skalarmultiplikation mit Additionsbaum

Dieses Verfahren lässt sich auch als Algorithmus formalisieren:

Algorithm 1 Multiplikation eines Skalars $n \in \mathbb{N}$ mit einem Punkt $P \in E$

Precondition: n lässt sich binär zerlegen in $n = n_0 + n_1 \times 2 + n_2 \times 2^2 + \dots + n_t \times 2^t$

```
1:  function MULTIPLIZIERE(n, P)
2:      if n_0 = 0 then
3:          Acc ← O          ▷ O ist der unendlich ferne Punkt
4:      else
5:          Acc ← P
6:      for i ← 1 to t do
7:          P ← P + P
8:          if n_i = 1 then
9:              Acc ← Acc + P
10:     return Acc
```

Wenn man diesen Algorithmus betrachten, sieht man auch, dass höchstens $2\log_2 n$ Operationen durchgeführt werden. Die Bitlänge von n wächst mit $\log_2 n$, was auch gleich der Anzahl der Durchläufe der Schleife ist. In jedem Schleifendurchlauf wird eine Addition mit $P+P$ durchgeführt und falls $n_0 = 1$ ist, eine weitere Addition durchgeführt. Das ergibt insgesamt $2\log_2 n$ Additionen im worst-case. Diesen Verfahren kann auch auf beliebige Gruppen angewendet werden, da die Assoziativität der +-Operation in einer Gruppe gegeben sein muss.

5.3 Angriffe

5.3.1 Universelle Angriffe

Um sich gegen kryptographische Angriffe auf ECC zu wehren, müssen die Domänenparameter $(\mathbb{F}_p, E, G, n)$ gut gewählt werden. Der naheliegenste Angriff ist der bereits beschriebene naive Angriff, bei dem die Gruppenoperation so oft auf G angewendet wird, bis das Ergebnis $Q = nG$ und somit n ermittelt wurde. Diesem Angriff kann leicht vorgebeugt werden, indem man n groß genug wählt, sodass dieser Brute-Force impraktikabel wird. Des Weiteren sollte n so gewählt werden, dass n einen großen Primzahldivisor hat. Damit ist auch einer der besten universal anwendbaren Algorithmen, eine Kombination aus dem Pohlig-Hellman-Angriff und Pollards ρ Algorithmus, nicht mehr realisierbar, da dieser darauf basiert das Problem auf die Untergruppen mit Primzahlordnung der von G erzeugten zyklischen Gruppe zu reduzieren [6, Seite 154-165].

5.3.2 Isomorphismus Angriffe

Sei E eine elliptische Kurve über dem Körper $\mathbb{F}_q$ und $P \in E(\mathbb{F}_q)$ habe eine Primzahlordnung n. Sei G eine Gruppe mit Ordnung n und $\langle P \rangle$ die von P erzeugte, zyklische Untergruppe von E. Da n prim ist und $\langle P \rangle$ and G zyklisch sind, sind sie auch isomorph [6, Seite 168]. Wenn man also diesen Isomorphismus

$$\phi : \langle P \rangle \mapsto G$$

effizient berechnen kann, dann kann man das DLP auf elliptischen Kurven auf das DLP auf G reduzieren. Wie bereits erwähnt kann das DLP auch mit subexponentieller Laufzeit gelöst werden.

Ein Beispiel für elliptische Kurven, für die eine solcher Isomorphismus existiert, sind die sogenannten anomale Elliptische Kurven. Eine elliptische Kurve ist anomal, wenn $\#E(\mathbb{F}_p) = p$), d.h. die Anzahl der Punkte von E ist gleich der Anzahl der Elemente des Körpers $\mathbb{F}_p$. Für eine anomale Kurve $E(\mathbb{F}_p)$ gilt, dass sie isomorph zur additiven Gruppe $\mathbb{F}_p^+$ ist. In einer additiven Gruppe kann das Problem effizient durch Berechnen des inversen Elements mit Hilfe des euklidischen Algorithmus gelöst werden. Auch der Isomorphismus kann effizient berechnet werden [6, Seite 168]. Daraus folgt, dass das DLP auf diesen speziellen elliptischen Kurven effizient gelöst werden kann. Deshalb sollten diese Kurven nicht für Verschlüsselung verwendet werden.

Weitere Angriffe, die auf Isomorphismen beruhen, sind z.B. Weil und Tate Paarung oder der Weil Abstieg [6, Seite 169-170]. Die elliptische Kurve sollte entsprechend gewählt werden um solche Angriffe abzuwehren.

5.3.3 Seitenkanalangriffe

Bei einem Seitenkanalangriff hat der Angreifer phyische Kontrolle über das Gerät, welches für die Verschlüsselung zuständig ist. Das ermöglicht dem Angreifer durch Messsen von Werten wie Prozessorgeschwindigkeit und Stromverbrauch Rückschlüsse auf die Operationen, die das Gerät durchführt, zu ziehen. Seitenkanalangriffe sind bei elliptischen Kurven sehr interessant, da diese aufgrund der Schlüssellänge in Geräten verwendet werden, die wenig Speicherplatz und Rechenkapazität haben. Dazu gehören Smartcards welche z.B. den

ordnungsgemäßen Zugriff auf zahlungspflichtige TV-Sender sicherstellen. In diesem Fall befinden sich die Smartcard dann im physischen Besitz eines potentiellen Angreifers. Ein großes Problem bei ECC ist, dass die Operation der Verdopplung eines Punkts und die Addition zweier verschiedener Punkte unter den meisten Implementierungen unterschiedlich viel Rechenleistung benötigen, wodurch der Angreifer Rückschlüsse auf den privaten Schlüssel ziehen kann [13]. Es gibt mehrere Ansätze dieses Problem zu lösen. Ein Lösungsansatz ist das Durchführen von Dummy-Additionen, also Additionen deren Ergebnis danach wieder verworfen wird, jedoch kann es dem Angreifer möglich sein dies zu bemerken [13]. Möller schlägt daher ein speziellen Encoding-Algorithmus vor, der gegen Seitenkanalangriffe unter den meisten Bedingungen absichert [13]. Es gibt auch noch weitere Ansätze, von denen manche bestimmte elliptische Kurven verwenden um das Problem beheben zu können [13].

5.4 Edwards Kurven

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] Klaus Vetters Andreas Fischer, Winfried Schirotzek. Lineare Algebra: Eine Einführung für Ingenieure und Naturwissenschaftler, 2003.

[3] Elaine Barker. Recommendation for Key Management. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf, 2016. Abgerufen am 15.04.2016.

[4] Hubert Kiechle Christian Karpfinger. *Kryptologie: Algebraische Methoden und Algorithmen*. 2010.

[5] Schirin Gratzer. Diskrete Geometrien. http://www.uni-graz.at/~baurk/lehre/WS2014-LAK-Seminar/4_Gratzer.pdf, 2014. Abgerufen am 23.04.2016.

[6] Darrel Hankerson, Alfred J Menezes, and Scott Vanstone. *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[7] Hans-Wolfgang Henn. Elementare Geometrie und Algebra, 2003.

[8] Antoine Joux, Andrew Odlyzko, and Cécile Pierrot. *Open Problems in Mathematics and Computational Science*, chapter The Past, Evolving Present, and Future of the Discrete Logarithm, pages 5–36. Springer International Publishing, 2014.

[9] Antoine Joux and Vanessa Vitse. Elliptic curve discrete logarithm problem over small degree extension fields. *Journal of Cryptology*, 26(1):119–143, 2011.

[10] Neal Koblitz. Elliptic curve cryptosystems, 1987.

[11] Victor S. Miller. Use of elliptic curves in cryptography, 1985.

[12] J.S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006.

[13] Bodo Möller. Securing elliptic curve point multiplication against side-channel attacks. In *Information Security*, pages 324–334. Springer, 2001.

[14] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2nd edition, 2009.

[15] Lawrence C. Washington. Elliptic Curves: Number Theory and Cryptography, 2008.

[16] Zdeněk Říha. Electronic passports. https://web.archive.org/web/20100215182600/http://www.buslab.org/SummerSchool2008/slides/Zdenek_Riha.pdf. Archiviert vom Original, abgerufen am 15.04.2016.