Korrektheit elliptischer Kryptosysteme und Fundierung in der algebraischen Geometrie

Diese Seminararbeit wurde vorgelegt am

Fachbereich 9

Medizintechnik und Technomathematik

FH Aachen, Campus Jülich

von

Fabian Schuller
Matrikelnummer: 3646801

und wurde betreut von

Erstprüfer: Prof. Dr. rer. nat. Alexander Voß

Zweitprüfer: Thorsten Adrian, MSc

8. Juli 2025

Inhaltsverzeichnis

1 Vorwort

In der vorliegenden Arbeit wird die Kryptographie mit elliptischen Kurven vorgestellt. Insbesondere wird das Diffie-Hellman-Protokoll betrachtet. Dabei wird ausgenutzt, dass auf den Kurven eine algebraische Struktur (Gruppenstruktur) besteht. Somit kann man mit Punkten auf der Kurve „plus rechnen“, ähnlich wie man es intuitiv mit ganzen Zahlen tut. In der Kryptographie ist die Korrektheit der Algorithmen von äußerster Bedeutung. Das motiviert eine rigorose mathematische Auseinandersetzung mit den elliptischen Kurven. Darüber hinaus soll eine zufriedenstellende Antwort auf das „Warum“ hinter der Struktureigenschaft gegeben werden. Hierzu wurde ein Beweisansatz ausgewählt, der eine ausgewogene Kombination aus Effizienz, Allgemeingültigkeit und Klarheit bietet.

Elliptische Kurven werden als Objekte der algebraischen Geometrie eingeführt. Dazu werden Gruppen definiert (das ist die Rechengrundlage, mit der z. B. der öffentliche Schlüssel berechnet wird) sowie anschließend Körper und Polynome. Körper sind algebraische Strukturen, auf denen elliptische Kurven überhaupt erst allgemein definiert werden können.

Dann folgt ein Abschnitt zur algebraischen Geometrie. Geometrische Objekte (z. B. Geraden) werden nun nicht mehr im Reellen, sondern über Körpern definiert. Des Weiteren wird der projektive Raum eingeführt. Das hat den Zweck, dass die Gruppenstruktur auf elliptischen Kurven einen zusätzlichen Punkt benötigt (siehe unten): den Punkt im Unendlichen. Im affinen Raum (z. B. $\mathbb{R}^d$) wird das Unendliche (negativ) als Unbeschränktheit definiert, was die Handhabung erschwert. Der projektive Raum stellt eine *Kompaktifizierung* des affinen Raums dar: Der Punkt im Unendlichen ist wohldefiniert, und man kann damit einfacher rechnen, und eben auch die Gruppeneigenschaft nachweisen. Für Beweis werden die allgemeine Kurven in den projektiven Raum und in einen erweiterten Körper eingebettet, wobei die Resultate dann weiterhin für die ursprüngliche Kurve gelten.

Es folgen einige technische Bemerkungen zur Implementierung des Diffie-Hellman-Protokolls mit elliptischen Kurven. Hier werden optimierte Additionsformeln hergeleitet. Diese Formeln per Hand zu verifizieren ist aufwendig; Daher wird ein weiterer Korrektheitsbeweis vorgestellt, mit dem man konkrete Formeln verifizieren kann. Diesmal wird ein anderer Ansatz verwendet, bei dem ein Computeralgebrasystem zum Einsatz kommt. Dazu werden weitere algebraische Strukturen eingeführt (Ringe und Ideale). Für die Legitimierung wird darüber hinaus der Begriff des Isomorphismus definiert.

2 Kryptographie

2.1 Grundsätze

Unter einem *Kryptosystem*[1] versteht man die Gesamtheit des kryptographischen Sachverhalts: Einen *Klartext-* und *Chiffretextraum*, einen *Schlüsselraum* und die Abbildungen *chiffriere* und *dechiffriere*.

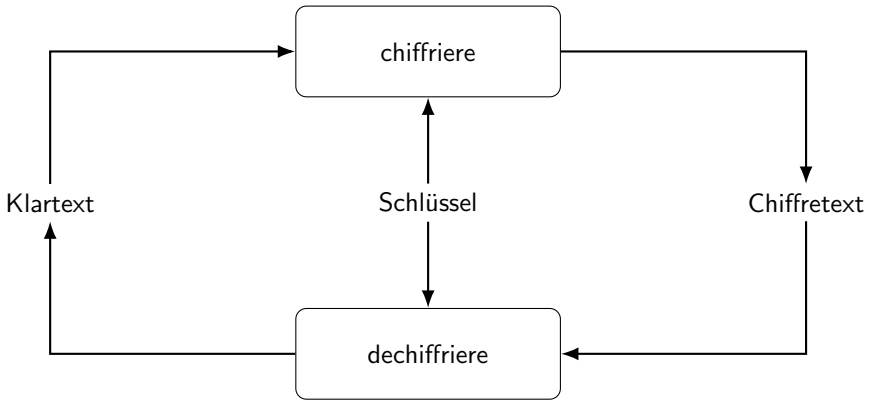

Abbildung 1: Kryptosystem

Ein Kryptosystem ist *gut*[2], wenn die Chiffren-Abbildung bijektiv ist, und man den Chiffretext ohne den Schlüssel mit praktischen Mitteln nicht dechiffrieren kann. Ein wichtiges Maß dafür ist die Laufzeitkomplexität. Wenn ein gemeinsamer Schlüssel benutzt wird, heißt das Kryptosystem *symmetrisch*. Alice und Bob könnten im Vorhinein einen gemeinsamen Schlüssel festlegen. Wenn jede Partei einen eigenen Schlüssel oder mehrere Schlüssel hat, spricht man von *asymmetrischen* Systemen. Beim Diffie-Hellman-Schlüsselaustausch wird ein gemeinsamer Schlüssel vereinbart, indem ein öffentlicher Schlüssel ausgetauscht und dann mit einem privaten Schlüssel verrechnet wird (wobei letztere danach verworfen werden): Man spricht von einem *hybriden* Kryptosystem. Asymmetrische Kryptosysteme beruhen meistens auf einer sogenannten *mathematischen Einwegfunktion*. Das sei eine Funktion, deren Ausführung eine geringe Laufzeitkomplexität hat, deren Umkehrfunktion jedoch eine sehr hohe Laufzeitkomplexität hat. Die vorliegende Arbeit behandelt lediglich die Korrektheit von Einwegfunktionen und nicht die Laufzeitanalyse.

2.2 Die Vigenère-Chiffre

Die *Vigenère-Chiffre* ist ein Beispiel für eine Chiffrierfunktion. Sie beruht auf verschobenen Alphabeten: Der Schlüssel ist eine Folge von Buchstaben $K =$

[1] Für die Definition des Kryptosystems, RSA, der Vigenère Chiffre und Diffie Hellman vgl. [Wätjen 2018].

[2] [Wätjen 2018] beschreibt in Abschnitt 1.2 Authentizitätsanforderungen und Geheimhaltungsanforderungen. Gut heißt hier: erfüllt diese.

$(k_1, \cdots, k_d)$, wobei $k_i, i = 1, \ldots, d$ die Größe der Verschiebung im i-ten Alphabet angibt. Es sei $f_i(a) := (a + k_i) \bmod n$, wobei n die Länge des Alphabets ist. Man definiert die Chiffrierfunktion, als dass f_i auf jeden Buchstaben m_i des Klartextes angewendet wird. Wenn man beim letzten Buchstaben k_d angekommen ist, macht man mit k_1 weiter:

$$\text{chiffriere} : K(M) := f_1(m_1) \ldots f_d(m_d) f_1(m_{d+1}) \ldots f_d(m_{2d}) \ldots f_a(m_{ld+a})$$

mit $a \in 1, \ldots, d, n \in \mathbb{N}_0$. Moderne Chiffren werden auf Bit-Ebene durchgeführt[3].

2.3 Das RSA-Kryptosystem

Das *Rivest-Shamir-Adleman-Verfahren* (RSA-Verfahren) ist ein asymmetrisches Kryptosystem. Es gibt einen öffentlichen Schlüssel und einen privaten Schlüssel pro Teilnehmer. Das Ziel ist, dass Alice die Nachricht M mit Bobs öffentlichem Schlüssel chiffriert. Nur mit dem privaten Schlüssel ist Bob dann in der Lage, die Nachricht zu lesen. Die Faktorisierung einer großen Zahl in ihre Primfaktoren und das Berechnen des diskreten Logarithmus sind Beispiele für mathematische Einwegfunktionen, die hierbei eine Rolle spielen. Im Folgenden werden kurz die zahlentheoretischen Grundlagen aufgeführt, die dann die kryptographischen Routinen legitimieren.

Definition und Proposition 2.3.1 (Wätjen 2018, 3.3 und 3.8, Eulersche φ-Funktion). $\varphi(n) := \#\{x \in \{1, \ldots, n\} : \text{ggT}(x, n) = 1\}$. Sei p eine Primzahl. Dann ist einfach zu sehen dass $\varphi(p) = (p - 1)$. □

Theorem 2.3.2 (Wätjen 2018, Satz 3.9, Satz von Euler). Es sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\text{ggT}(a, p) = 1$. Dann gilt

$$a^{\varphi(n)} \mod n = 1.$$

Wird hier nicht Bewiesen. □

Theorem 2.3.3 (Wätjen 2018, Satz 5.2). Es sei $n = pq$ mit Primzahlen $p \neq q$ und weiter $e, d \in \mathbb{N}$ mit $ed \bmod \varphi(n) = 1$ und schließlich $M \in \{1, \ldots n\}$. Dann ist

$$(M^e \mod n)^d \mod n = M.$$

Wird hier nicht Bewiesen. □

Die folgenden Algorithmen werden u. A. im RSA-System benutzt:

[3] vgl. [Wätjen 2018], Einleitung Kapitel 4

Algorithmus 2.3.4: RSA-Schlüsselerzeugung

Input: Zwei große Primzahlen p und q
Output: Öffentlicher Schlüssel (e, n), Privater Schlüssel (d, n)

1 $n \leftarrow p \cdot q$
2 $\phi \leftarrow (p-1)(q-1)$
3 Wähle e mit $1 < e < \phi$ und $\gcd(e, \phi) = 1$
4 Berechne d mit $e \cdot d \equiv 1 \mod \phi$ (dazu z. B. Wätjen 2018, Algorithmus 3.3)
5 **return** (e, n), (d, n)

Algorithmus 2.3.5: RSA-Chiffrierung

Input: Klartext m, Öffentlicher Schlüssel (e, n)
Output: Chiffretext c

1 $c \leftarrow m^e \mod n$
2 **return** c

Algorithmus 2.3.6: RSA-Dechiffrierung

Input: Chiffretext c, Privater Schlüssel (d, n)
Output: Klartext m'

1 $m' \leftarrow c^d \mod n$
2 **return** m'

2.4 Der Diffie-Hellman-Schlüsselaustausch

In der ersten Fassung des Diffie-Hellman-Austausches finden die Rechnung auf endlichen Menge $M = \{1, \ldots, p\}$ mit Multiplikation Modulo p, d. h. $a \otimes b := a \cdot b \mod p$. Das Protokoll ist auf beliebigen Gruppen möglich, insbesondere auch auf der Gruppenstruktur von elliptischen Kurven (dazu s. u.).

Definition 2.4.1 (Diffie-Hellman-Protokoll). Gegeben sind eine Primzahl p, und $g \in M$. Alice und Bob wählen zwei private Schlüssel X_A und X_B. Beide berechnen

$$\mathrm{DH}_A : P_A = g^{X_A} \mod p = (g \otimes g) \otimes g \ldots, \qquad \mathrm{DH}_B : P_B = g^{X_B} \mod p.$$

Die beiden Ps werden dann über einen öffentlichen Kanal ausgetauscht, und schließlich die Operation DE darauf wiederholt ausgeführt. Das Resultat $Y_A = Y_B$ wird folglich als Chiffre genutzt. Die Anforderungen an den Algorithmus sind geringer als bei RSA, da der Schlüssel bloß ausgetauscht werden muss. Wichtig ist lediglich, dass die Funktionen DH_A, DH_B kommutieren.

Bemerkung 2.4.2. Es ist sinnvoll, g so zu wählen, das g ein Generator der zyklischen Gruppe $(\mathbb{Z}/p\mathbb{Z}, \otimes)$ (vgl. 6.2.1 und das folgende Kapitel) ist. Dann kommen für einen Angreifer beliebige Werte X in Frage. Weil p eine Primzahl ist gilt das für jedes $g \in M$.

Theorem 2.4.3 (Korrektheit von Diffie-Hellman). *Beweis.*

$$\begin{aligned}\mathrm{DH}_A(\mathrm{DH}_B(M)) &= P_B^{X_A} \mod p = (g^{X_B} \mod p)^{X_A} \mod p = g^{X_A X_B} \mod p \\ &= (g^{X_A} \mod p)^{X_B} \mod p = P_A^{X_B} \mod p \\ &= \mathrm{DH}_B(\mathrm{DH}_A(M))\end{aligned}$$

Bemerkung 2.4.4 (mathematische Einwegfunktion). Die mathematische Einwegfunktion der Potenzierung auf Gruppen endlicher Ordnung nennt man auch *diskretes Logarithmus-Problem*. Gemeint ist die Schwierigkeit, aus einer Gleichung $x^d = y$ auf x zu schließen, sofern d, y gegeben sind. Statt x^d wird auch $[d]x$ geschrieben.

3 Algebra und algebraische Geometrie

Im Folgenden werden Gruppen[4] und Körper definiert sowie ausgewählte Eigenschaften und Erweiterungen beschrieben. Ein wesentliches Ziel dieser Arbeit ist es, elliptische Kurven als Gruppen zu definieren und dies als Grundlage für das Diffie-Hellman-Protokoll zu nutzen. Dafür betrachtet man den Graphen der impliziten Funktion, die eine elliptische Kurve darstellt. Zwei Punkte zu addieren bedeutet, beide mit einer Geraden zu verbinden, den dritten Schnittpunkt von Kurve und Gerader zu finden und diesen anschließend an der X-Achse zu spiegeln (siehe Abschnitt 4.2, Abbildung 2).

Körper bilden eine weitere Grundlage: Das sind algebraische Strukturen, die sich aus zwei Gruppen zusammensetzen: Addition und Multiplikation werden erklärt. Dies ermöglicht eine allgemeine Definition von Polynomen (mit n Koeffizienten), aus denen elliptische Kurven hergeleitet werden. Das Prinzip des algebraisch abgeschlossenen Körpers[5] wird eingeführt, um auf solchen Körpern Aussagen über Polynome zu beweisen, insbesondere den Satz von Bézout. Dieser trifft eine Aussage über die Anzahl der Schnittpunkte von Kurven was offenbar relevant für die Gruppenaktion ist. Eine abgeschwächte Version davon lässt sich dann wieder auf allgemeine Körper übertragen.

3.1 Gruppen

Sei M eine nicht-leere Menge und $\oplus : M \times M \to M$ eine Abbildung. $(M, \oplus)$ heißt *Gruppe*, wenn gilt: (1) $\exists e \in M : a \oplus e = e \oplus a = a \forall a \in M$ (*neutrales Element*); (2) $\forall a \in M \exists a^{-1} \in M : a \oplus a^{-1} = e$; (3) $(a \oplus b) \oplus c = a \oplus (b \oplus c) \forall a, b, c \in M$ (*Assoziativität*). Eine Gruppe heißt *abelsch* oder kommutativ wenn $a \oplus b = b \oplus a \forall a, b \in M$. $\oplus$ nennt man *Gruppenaktion* und M *Basismenge*. $\#M$ (Mächtigkeit der Basismenge) nennt man *Ordnung* der Gruppe. Im Gruppenkontext bedeutet

[4] Für die folgenden Definitionen vgl. [Karpfinger 2024] oder ein anderes Lehrbuch zur Algebra.

[5] Bemerkung. Die komplexen Zahlen sind ein algebraisch abgeschlossener Körper. Mit dem Lefschetz-Prinzip [Eklof 1973] kann man somit Ergebnisse aus der Funktionentheorie in die algebraische Geometrie übertragen.

x^n die n-fache Ausführung der Gruppenaktion auf das Element x (auf sich selbst). Man schreibt auch $[n]x$. Gibt es ein $d \in M$ so dass $M = \{d^n : n \in \mathbb{N}\}$ spricht man von einer *zyklischen* Gruppe mit *Generator* d.

3.2 Körper

Sei K eine nicht-leere Menge. Weiter seien $\oplus : K \times K \to K$ und $\otimes : K \times K \to K$ Abbildungen. $(K, \oplus, \otimes)$ heißt *Körper*, wenn (1) $(K, \oplus)$ eine Gruppe ist, (2) $(K \setminus \{e_\oplus\}, \otimes)$ eine Gruppe ist, und (3) das Distributivgesetz $a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c; (b \oplus c) \otimes a = b \otimes a \oplus c \otimes a$ gilt. Eine Teilmenge $L \subseteq K$ mit $e_+, e_\cdot \in L$, so dass $(L, \oplus, \otimes)$ wieder ein Körper ist nennt man *Teilkörper* zu K. Man nennt K *Erweiterungskörper* zu L. Man definiert die *Charakteristik* eines Körpers, als die kleinste natürliche Zahl n, mit der $[n]_\oplus e_\oplus = e_\otimes$ gilt. Das heißt: Wie oft muss man die 1 auf sich selbst addieren, damit sich 0 ergibt. Für den Körper $\mathbb{R}$ geht das nicht und man setzt $\text{char}(\mathbb{R}) = \infty$. Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom (s. u.) mit Koeffizienten in K eine Nullstelle in K hat. Dort zerfällt das Polynom in Linearfaktoren. Der kleinste Erweiterungskörper $J =: \bar{K}$ zu K, so dass J algebraisch abgeschlossen ist, nennt man *algebraischen Abschluss* zu K. Nach dem *Fundamentalsatz der Algebra* gilt $\bar{\mathbb{R}} = \mathbb{C}$. Ganze Zahlen stellen in der Praxis endliche Körper da, Stichwort Integer Overflow.

3.3 Polynome

$K[X_1, \ldots, X_n]$ bezeichnet die Menge der Polynome in n Variablen über K. Das ist

$$\{F : K \times \cdots \times K \to K,$$
$$(X_1, \ldots, X_n) \mapsto \sum_{(i_1,\ldots,i_n), i_j \in \{0,\ldots n\}} a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$$
$$|a_{i_1,\ldots,i_n} \in K, i_j \in \{0, \ldots n\}\}$$

natürlich bezogen auf die Körper-Addition und -Multiplikation. Wenn alle bis auf ein $a_{i_1,\ldots,i_m} = 0$ sind, und das restliche $a_j = 1$, nennt man F *Monom*. $K[X_1, \ldots, X_n]$ besteht folglich aus den Linearkombinationen der Monome über K. Ein Polynom $f \in K[X_1, \ldots, X_n]$ heißt *irreduzibel* in $K[X_1, \ldots, X_n]$ falls es keine nicht-konstanten Polynome $g, h \in K[X_1, \ldots, X_n]$ gibt so dass $f = g \cdot h$. Man sagt ein Polynom E *teilt* F, wenn bei der Polynomdivision ein Polynom D entsteht. Irreduzible Polynome bilden somit ein Analogon zu den Primzahlen, weil sie nicht teilbar sind.

3.4 Äquivalenzrelationen

Eine Relation $\sim$ heißt *Äquivalenzrelation*, falls sie reflexiv, transitiv und symmetrisch ist. Sei M eine nicht-leere Menge und $\sim$ eine Äquivalenzrelation auf M. Für ein $x \in M$ bezeichnet $[x]_\sim := \{y \in M : x \sim y\}$ die Äquivalenzklasse von x. Dann bezeichnet $M/\sim := \{[x]_\sim : x \in M\}$ die *Menge der Äquivalenzklassen* von

$\sim$. Oft werden durch Äquivalenzklassen Eigenschaften der Menge M übertragen, zum Beispiel eine Metrik. Dann nennt man $M/\sim$ Quotientenraum. Die Abbildung $\pi : M \to M/\sim, m \mapsto [m]$ nennt man *kanonische Projektion*. Ein Element $a \in [x]$ nennt man *Repräsentanten* von $[x]$. Mit Äquivalenzrelationen wird im Folgenden der projektive Raum konstruiert, in den die elliptischen Kurven eingebettet werden.

Beispiel 3.4.1 (Möbiusband). Sei $B = \{(x, y) \in \mathbb{R} \times \mathbb{R} : |x| \leq 10, |y| \leq 2\}$ ein Rechteck. B ist mit der *euklidischen Metrik* $d(a, b) = \sqrt{(a_x - b_x)^2 + (a_y - b_y)^2}$ ein metrischer Raum. Sei $\sim$ eine (leicht überprüfbare) Äquivalenzrelation mit

$$a \sim b :\iff a = b \vee (a_y = -b_y \wedge a_x \neq b_x \wedge |a_x| = |b_x| = 10)$$

Man erhält das Möbiusband[6] als Quotientenraum $B/\sim$. Wobei eine Metrik induziert wird durch

$$d([a], [b]) = \min_{a \in [a], b \in [b]} (d(a, b)).$$

Die Äquivalenzrelation klebt die Ränder des Rechtecks verdreht aneinander.

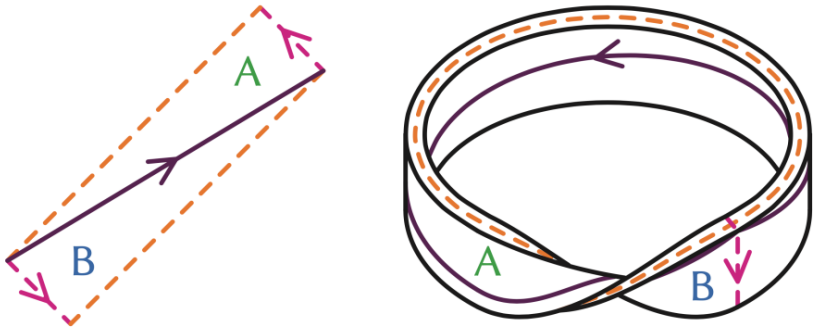

Abbildung 2: Visualisierung Möbiusband

3.5 Der projektive Raum

Zwei parallele Graden treffen sich im Unendlichen, nämlich im Fluchtpunkt. Im Folgenden wird eine Anschauungsweise vorgestellt, in der der Fluchtpunkt, den man nun den „Punkt im Unendlichen“ nennt, konkret verortet ist. Der Fall, dass auf der elliptischen Kurve Punkte addiert werden, so dass Verbindungsgrade und Kurve parallel sind, wird somit elegant abgehandelt. Ebenfalls wichtig ist das Konzept von homogenen Polynomen.

[6] vgl. [Jänich 1990], Kap. 3, §7, Beispiel 4

Definition 3.5.1 (Washington 2008, Der projektive Raum). Man definiert den projektiven Raum $P^n_{\mathbb{R}}$ als Quotientenraum der Relation $\sim$: $y \sim x \iff (x = \lambda y)$ auf $\mathbb{R}^{n+1}$, also die Menge der Äquivalenzklassen (aber kein Körper). Die Äquivalenzklassen $[x]_\sim$ entsprechen den Graden durch den Ursprung. Koordinaten im projektiven Raum schreibt man $(x_1 : x_2 : \cdots : x_{n+1})$. Die kanonische Projektion ist $h([x]_\sim) = (x_1/x_{n+1}, \ldots, x_n/x_{n+1})^T$, falls $x_{n+1} \neq 0$. Die Punkte $(x_1 : \cdots : x_n : 0)$ nennt man Punkte im unendlichen. Statt $\mathbb{R}$ wählt man oft beliebige Körper K. Man nennt P^n_K den n-dimensionalen projektiven Raum über K. $A^n_K = K^n$ heißt affiner Raum über K. Der Prägnanz halber wird auch A^n und P^n geschrieben, falls K nicht weiter relevant ist. Man kann A^n als Teilraum von P^n betrachten mit $(x_1, \ldots, x_n) \sim (x_1 : \cdots : x_n : 1)$. $(0 : 0 : 0)$ ist im projektiven Raum ausgeschlossen. Man erhält die Definition $P^n_K = (K \setminus \{0\})/\sim$.

Bemerkung 3.5.2. Im Folgenden wird Punkten $(X : Y : Z)$ wie mit cartesischen Koordinaten gerechnet, nicht explizit mit Äquivalenzklassen. Ggf. wird der Koordinatenpunkt in Beweisen skaliert, da im Quotientenraum $(x, y, z) \equiv_\sim \lambda(x, y, z)$.

Bemerkung 3.5.3 (Motivation des projektiven Raums). Man sagt, Punkte im projektiven Raum sind in *homogenen Koordinaten* geschrieben. Man kann sich den Übergang zu homogenen Koordinaten anhand dem perspektivischen Zeichnen vorstellen. Die Graden durch den Ursprung sind dann Sichtlinien, und die Hyperebene $\{(X, Y, Z)^T : Z = 1\} \subset K^3$ ist die Landschaft. Um sich die Menge der Graden (s. o.) besser vorzustellen, kann man sie auf eine Sphäre (s. Abb. 4) projizieren. Man betrachtet somit den projektiven Raum als eine solche Sphäre. Die Punkte im unendlichen bilden in der Analogie den Horizont. Das sind genau die Graden, bei denen $Z = 0$ ist. Da diese Punkte einen konkreten Ort auf der Sphäre darstellen (und nicht bloß einen Grenzwert), spricht man von einer *Kompaktifizierung* des affinen Raums. Offenbar schneiden die Graden die Sphäre aber in einem zweiten Punkt, hier ist das der Hinterkopf des Malers. Man muss diese Punkte auf der Sphäre folglich identifizieren, was man sich dann nicht mehr so leicht vorstellen kann. Auch die kanonische Projektion π wird durch diese Ansichtsweise motiviert. Weil $(X : Y : Z) = \lambda(X : Y : Z)$ wählt man $\lambda = \frac{1}{Z}$ für die nicht-unendlichen Punkte $(Z \neq 0)$. Man erhält Punkte auf der Landschaft zurück. Das wird in Abbildung 5 verdeutlicht.

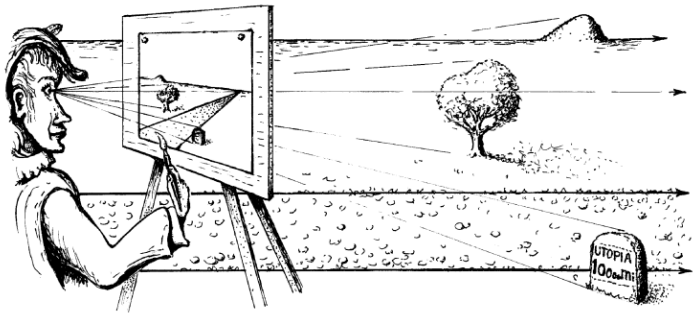

Abbildung 3: Perspektive

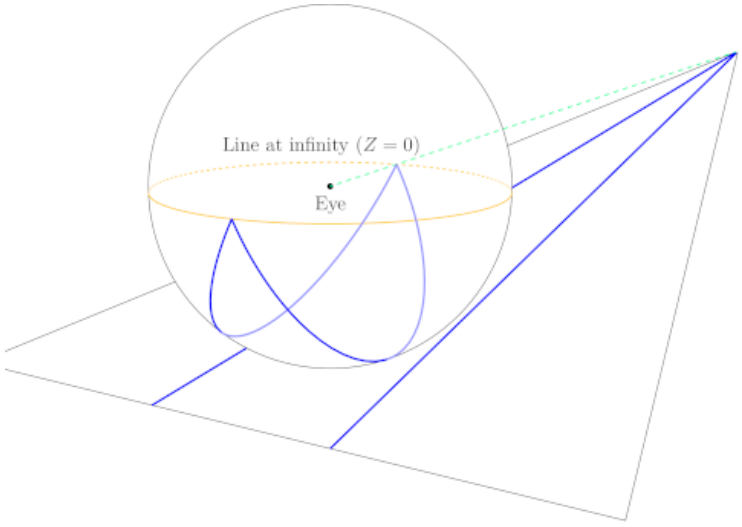

Abbildung 4: Visualisierung des projektiven Raums - Das Auge des Malers

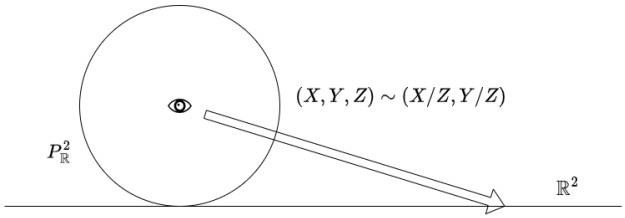

Abbildung 5: Die kanonische Projektion

Definition 3.5.4 (Washington 2008, homogene Polynome). Ein Polynom $f(X,Y,Z) = \sum_{i=1}^{n} a_i X^{j_i} Y^{k_i} Z^{l_i}$ heißt *homogen* mit Grad m falls $m = j_i + k_i + l_i, \forall i = 1,\ldots,n$. Homogene Polynome werden auch Formen genannt (als geometrische Objekte, s.u.). Jedes Monom hat dort also den gleichen Grad. Homogene Polynome haben wohldefinierte Nullstellen im projektiven Raum: Es gilt $f(\lambda X, \lambda Y, \lambda Z) = \lambda^m f(X,Y,Z)$. Ist $(x : y : z)$ also eine Nullstelle von f, so verschwindet f bei $(x_2, y_2, z_2) \sim (x, y, z)$ ebenso. Beliebige Polynome in A_K können zu homogenen Polynomen in P_K umgewandelt werden: (1) Wähle m als die maximale Potenz (2) ergänze jeweils z^l mit $l = m - i_1 - \cdots - i_m$. Beispiel: $\tilde{f}(X,Y) = Y^2 - X^3$, $f(X,Y,Z) = Y^2Z - X^3$. Man nennt das *Homogenisierung*. Somit kann man Polynome im affinen Raum in den projektiven Raum fortsetzen, so dass sie homogen sind. Weil der affine Raum in den projektiven Raum durch $(x_1,\ldots,x_n) \sim (x_1 : \cdots : x_n : 1)$ eingebettet ist, erhält man durch $x_{n+1} \overset{!}{=} 1$ (im P_K^2 also $Z = 1$) im homogenen Polynom das affine Ursprungspolynom. Man nennt das *Dehomogenisierung*.

Proposition 3.5.5 (Linearfaktoren von homogenen Polynomen in zwei Variablen). Sei $h(X,Y) \in K[X,Y]$ ein homogenes Polynom vom Grad $d \geq 1$ und $(\xi : \eta) \in P^1_{\bar{K}}$ mit $H(\xi,\eta) = 0$. Dann ist $(\eta X - \xi Y)$ ein Teiler von H in $\bar{K}[X,Y]$. *Beweis.* Ohne Einschränkung sei $\eta \neq 0$. Dann gilt: $h(\xi,\eta) = \eta^d \cdot h\left(\frac{\xi}{\eta}, 1\right) = 0$, also ist $x - \frac{\xi}{\eta}$ ein Teiler von $\tilde{h}(x) := h(x,1)$ (Dehomogenisierung).

Daher ist $h(X,Y) = Y^d \cdot \tilde{h}(X/Y)$ durch $(X - \frac{\xi}{\eta}Y)$ teilbar, also auch durch $(\eta X - \xi Y)$.

3.6 Algebraische Varietäten

Definition 3.6.1. Sei im Folgenden K ein Körper, und und $L \supset K$ ein Erweiterungskörper. Man sagt eine Funktion $f : A_K^n \to K$ verschwindet bei a, falls $f(a) = e_+ = 0$. Die Menge $V(f) := \{a \in A_K^n | f(a) = 0\}$ heißt Verschwindungsmenge[7] von f. Wenn f ein irreduzibles Polynom ist, heißt $V(f)$ *Varietät*. Im Folgenden werden Varietäten z. B. mit C, D, E notiert. Man definiert den projektiven Abschluss von Varietäten als die Verschwindungsmenge im projektiven Raum, wobei das Polynom zuerst homogenisiert wird.[8]. Varietäten im A_2 werden auch Kurven genannt. Man sagt E hat den Grad n, wenn n die maximale Potenz der Monome ist. Die Verschwindungsmenge einer Varietät E wird auch $E(K)$ geschrieben. Man nennt eine Varität $E : f = 0$ *glatt* im Punkt p, wenn nicht alle partiellen Ableitungen in p verschwinden, d. h. $\nabla f(p) \neq (0,\ldots,0)$. Eine Varität E heißt *glatt*, wenn E in jedem $p \in E(K)$ glatt ist, sonst heißt E *singulär*.

[7] Bemerkung. Es gilt z. B. $V(f \cdot g) = V(f) \cup V(g)$ oder auch $V(f+g) \supseteq V(f) \cap V(g)$. Das Polynom ist nicht eindeutig bei gegebener Verschwindungsmenge: betrachte h nicht-konstant, sonst beliebig und $V(h^2) = V(h) \cup V(h) = V(h)$

[8] Für die Definition von algebraischen Varietäten vgl. [Cox, Little und O'Shea 2015 Kap. 1, §2, für den projektiven Abschluss Kap. 5, §4]

Bemerkung 3.6.2 (Synopse). Im Folgenden wird eine vereinfachte Version des Satzes von Bézout bewiesen. Der Satz besagt, dass sich eine Grade und eine elliptische Kurve insgesamt drei mal treffen. Dafür werden die geometrischen Objekte als Varietäten im projektiven Raum betrachtet. Begründung: Dabei verändert sich die Kurve im eingebetteten affinen Raum nicht. Man ergänzt also den affinen Raum formal zum projektiven, wobei effektiv bloß der Punkt im unendlichen hinzugenommen wird. Der Satz dient später als Hilfsresultat im Beweis der Assoziativität auf elliptischen Kurven. Man kann ihn als Verallgemeinerung des Fundamentalsatzes der Algebra auffassen. Zur Erinnerung: Ein Polynom vom Grad n besitzt (unter Berücksichtigung der Multiplizitäten) genau n komplexe Nullstellen. Der vereinfachte Satz von Bézout besagt analog: Eine algebraische Kurve vom Grad d schneidet eine Gerade (Grad 1) in genau d Punkten, ebenfalls unter Berücksichtigung der Multiplizitäten[9] (d.h. Schnittzahlen).

Dieses Resultat ist nützlich für Existenzbeweise, insbesondere dann, wenn bekannt ist das alle Schnittzahlen gleich eins sind.

Des Weiteren wird der Begriff des Morphismus eingeführt, basierend auf der Definition rationaler Abbildungen. Morphismen sind Abbildungen zwischen Kurven. Dies ist notwendig, da im Beweis der Assoziativität folgendes Resultat über Morphismen verwendet wird: Nicht-konstante Morphismen zwischen glatten Kurven (auf algebraisch abgeschlossenen Körpern) sind surjektiv (siehe unten). Ein Beweis dieser Aussage wird im Rahmen dieser Arbeit jedoch nicht geführt. Der Zweck ist der Folgende: Betrachtet man eine endliche Menge von Sonderfällen und findet einen Morphismus, der auf allen Punkten außerhalb der Menge gleich Null ist, sieht man leicht das dieser nicht surjektiv sein kann, wenn die Zielmenge groß genug ist. Somit erledigen sich die Sonderfälle, da der Morphismus folglich konstant ist.

Zuerst wird aber das motivierende Beispiel der parallelen Graden aufgegriffen.

Proposition 3.6.3 (Washington 2008, 2.3, Geraden im projektiven Raum). Beliebige Graden treffen sich im P_K^2.
Beweis. Für zwei parallele Geraden $f_1 : y = mx + b_1$, $f_2 : y = mx + b_2$, $b_1 \neq b_2 \in K$ ist die homogene Form

$$F_1 : y = mx + b_1 z, F_2 : y = mx + b_2 z$$

und deren Schnittpunkt ist $(x : mx : 0) = (1 : m : 0) = \infty$. Da sich nichtparallele Graden offenbar auch einmal treffen, gilt die Aussage allgemein □

Definition 3.6.4 (Stoll 2020, 4.1, Schnittzahlen, vereinfacht). Sei $P = (\xi : \eta : \zeta) \in P_K^2$ ein Punkt, $G : aX + bY + cZ = 0$ eine projektive Grade und $C : F(X, Y, Z) = 0$ eine projektive Kurve über K, so dass G kein Teiler von C ist. Man definiert $i(G, C; P)$ als die *Vielfachheit oder auch Multiplizität des*

[9] Die allgemeine Version des Satzes behandelt zwei beliebige Kurven vom Grad p bzw. q: Die Anzahl ihrer Schnittpunkte (mit Multiplizitäten) beträgt dann $p \cdot q$. Für den Beweis benötigt man Ergebnisse der lokalen Algebra [Fulton 2008], 5.3.

Schnittpunkts P von G und C: Im Fall $P \notin C(L) \cap G(L)$ sei $i = 0$. Andernfalls löst man die Gleichung von G nach einer der Variablen auf, etwa $Z = -\frac{a}{c}X - \frac{b}{c}Y$ (ohne Einschränkung $c \neq 0$) und setzen diesen Ausdruck in F ein. Man erhält ein homogenes Polynom $H(X, Y)$, dass durch $(\xi Y - \eta X)$ teilbar ist. Für den Fall das oben Y oder X eliminiert wurde, $(\xi Z - \zeta X)$ oder $(\eta Z - \zeta Y)$. Man setzt i als die Vielfachheit des Faktors $(\xi Y - \eta X)$ in H.

Bemerkung 3.6.5 (Eindeutigkeit der Schnittzahlen). Die Schnittzahl ist unabhängig davon, welche Variablen man oben zur Umformung wählt. *Beweis.* Ohne Einschränkung sei $P = (0 : 0 : 1)$ (durch eine lineare Koordinatentransformation[10] aus $PGL_3(K)$). Dann ist $c = 0$, und formt man G nach X, Y um ergibt sich $X = -\frac{b}{a}Y$ oder $Y = -\frac{a}{b}X$, die aber Äquivalent sind.

Theorem 3.6.6 (Stoll 2020, Satz 4.3, Bézout, vereinfacht). Sei $C : F(X, Y, Z) = 0$ eine projektive Kurve vom Grad d über K, so wie $G : aX + bY + cZ$ eine projektive Grade über K die nicht in C enthalten ist. Dann gilt

$$\sum_{P \in C(\bar{K}) \cap G(\bar{K})} i(G, C, P) = d$$

Beweis. Sei ohne Einschränkung $c \neq 0$ und seien $a' = -a/c$, $b' = -b/c$; Dann ist die Geradengleichung $Z = a'X + b'Y$. Setzt man die Punkte in F ein bekommt man $H(X, Y) = F(X, Y, a'X + b'Y)$; das ist ein homogenes Polynom vom Grad d in $K[X, Y]$. In $\bar{K}[X, Y]$ ergeben sich Linearfaktoren:

$$H(X, Y) = \alpha(\eta_1 X - \xi_1 Y)^{d_1} \cdots (\eta_k X - \xi_k Y)^{d_k}.$$

$P = (\xi : \eta : \zeta) \in \mathbb{P}^2_{\bar{K}}(\bar{K})$ ist genau dann ein Schnittpunkt von C und G, wenn $H(\xi, \eta) = 0$ und $\zeta = a'\xi + b'\eta$ gilt. Die Schnittpunkte sind somit

$$(\xi_1 : \eta_1 : a'\xi_1 + b'\eta_1), \ldots, (\xi_k : \eta_k : a'\xi_k + b'\eta_k),$$

und deren Vielfachheiten sind per Definition $d_1, \ldots, d_k$ mit $d_1 + \cdots + d_k = d$. □

Korollar 3.6.7. Aus $K \subseteq \bar{K}$ folgt direkt dass

$$\sum_{P \in C(K) \cap G(K)} i(G, C, P) \leq d$$

wenn G kein Faktor von C ist.

Bemerkung 3.6.8 (allgemeiner Beweis). Für die allgemeine Version der Schnittzahl und einen entsprechenden Beweis von Bézout wird auf [Fulton 2008], Kapitel 5.3 verwiesen.

[10] Die Schnittzahl ist invariant in linearen Transformationen. vgl. [Cox, Little und O'Shea 2015] Kap. 8, § 7, Theorem 7. Im projektiven Raum sind affine Verschiebungen linear.

Beispiel 3.6.9. Seien $a : y = x^2 - 4$ und $b : y = -4$ affine Kurven in $\mathbb{C}$. Nach Bézout ist die Schnittzahl im Punkt $p = (0, -4)$ gleich 2. *Nachweis.* Man erhält den projektiven Punkt $P = (0 : -4 : 1) \equiv (0 : -1 : \frac{1}{4})$ und die homogenen Polynome

$$A : 0 = -YZ + X^2 - 4Z^2, B : 0 = Y + 4Z.$$

Löse B nach Z auf: $B : Y = -4Z$ und setze in A ein:

$$H(X, Z) = 4Z^2 + X^2 - 4Z^2 = X^2$$

welches von $(0Z - (-1)X) = X$ zweifach geteilt wird. □

Definition 3.6.10 (Stoll 2020, 6.1, rationale Abbildungen). Seien $C : F(X, Y, Z) = 0$ und $D : G(X, Y, Z) = 0$ irreduzible projektive Kurven über einem Körper K. Eine *rationale Abbildung* von C nach D ist eine Äquivalenzklasse von Tripeln (R_1, R_2, R_3), wo die $R_j \in K[X, Y, Z]$ homogen, vom gleichen Grad und nicht alle durch F teilbar sind und außerdem $G(R_1, R_2, R_3)$ durch F teilbar ist. Dabei gilt $(R_1, R_2, R_3) \sim (S_1, S_2, S_3)$ genau dann wenn $F | R_i S_j - R_j S_i$ für alle i, j gilt, d. h. F ist durch $R_i S_j - R_j S_i$ teilbar. Sei ϕ eine rationale Abbildung von C nach D und $P = (\alpha : \beta : \gamma) \in C(K)$. ϕ heißt *regulär* oder *definiert* in P , wenn ϕ einen Repräsentanten (R_1, R_2, R_3) hat, sodass nicht alle $R_j(\alpha, \beta, \gamma)$ verschwinden. In diesem Fall ist

$$\phi : P \mapsto (R_1(P_1, P_2.P_3), R_2(P_1, P_2.P_3), R_3(P_1, P_2.P_3))$$

wohldefiniert, und man erhält Abbildungen $\phi : \{P \in C(K) | \phi \text{ definiert in } P\} \to D(K)$.

Definition 3.6.11 (Stoll 2020, 6.1, Morphismen). Rationale Abbildungen, die auf ganz $C(K)$ regulär sind, nennt man *Morphismen.* In den beiden folgenden Beweisen spielt die Tatsache eine Rolle, dass die Gruppenaddition auf einer elliptischen Kurve ein Morphismus ist.

Theorem 3.6.12 (Hulek 2012, Satz 6.34, Surjektivität von Morphismen). Ist $f : C \to C'$ ein nicht-konstanter Morphismus zwischen glatten projektiven Kurven, dann ist f surjektiv. Wird hier nicht bewiesen. □

Theorem 3.6.13 (Fulton 2008, Kap. 6 Prop. 7, Stetigkeit von Morphismen). Sind $f, g : C \to C'$ zwei Morphismen zwischen den Varietäten C, C', die auf einer Teilmenge $D \subset C$ mit $\bar{D} = C$ übereinstimmen, gilt $f \equiv g$ auf C. Wird hier nicht bewiesen □

Bemerkung 3.6.14. Oben ist $\bar{D}$ der Abschluss bezüglich der Zariski-Topologie. Das ist die Menge aller Varietäten, die einen topologischen Raum bildet.

Das Stetigkeitsresultat wird im vorliegenden Beweis zur Assoziativität nicht genutzt, kann aber 3.6.12 ersetzen. mAllerdings ist die Anwendung im Rahmen dieser Arbeit aufwändig zu begründen, wohingegen man die Surjektivitätsaussage einfach so verwenden kann.

4 Elliptische Kurven

4.1 Definition von elliptischen Kurven

Eine elliptische Kurve ist eine glatte algebraische Varietät dritten Grades. In der Kryptographie beschränkt man sich aber meistens auf eine spezielle Darstellung (z. B. Montgomery-Form) oder sogar auf eine spezielle Kurve (z. B. beim Verfahren Curve25519[11]).

Definition und Proposition 4.1.1 (Washington 2008, 2.1, kurze Weierstrass Form). Sei K ein Körper mit $\text{char}(K) \neq 2, 3$. Eine glatte Varietät

$$E : y^2 = x^3 + Ax + B$$

nennt man *elliptische Kurve in kurzer Weierstrass Form*. Die Bedingung der Glattheit erfordert $\nabla(x^3 + Ax + B - y^2) \neq 0$ auf dem Bild $E(K)$. Man definiert eine Kennzahl der Kurve, die *Diskriminante*: $\Delta := 4A^3 + 27B^2$. $\Delta \neq 0$ ist Äquivalent zur Glattheit der Kurve. *Beweis.*

$$\begin{aligned}
\nabla E = \begin{pmatrix} 3x^2 + A \\ -2y \end{pmatrix} \overset{!}{=} \begin{pmatrix} 0 \\ 0 \end{pmatrix} &\implies 0 = y^2 = x(\frac{-A}{3} + A) + B \\
&\implies x = \frac{3B}{2A} \\
&\implies \frac{9B^2}{4A^2} = \frac{-A}{3} \\
&\iff 4A^3 + 27B^2 = 0
\end{aligned}$$

$\text{char}(K) \neq 2, 3$ ist an der Stelle wichtig, da somit $0 \neq 2, 3$ in K.

Bemerkung 4.1.2 (weitere Darstellungen). Es gibt weitere Darstellungen von elliptischen Kurven, z. B. die Montgomery Form, oder die lange Weierstrass-Gleichung, die nicht unbedingt äquivalent sind. Kryptographisch relevante Darstellungen werden in der Explicit-Formulas-Database (EFD) aufgelistet. Die folgenden Berechnungen beschränken sich auf die kurze Weierstrass-Form.

4.2 Die Gruppenaddition

Proposition 4.2.1 (Washington 2008, 2.2, Elliptische Kurven als abelsche Gruppen). Auf der elliptischen Kurve wird eine Gruppenstruktur definiert. Zwei Punkte zu addieren bedeutet, beide mit einer Grade zu verbinden, den dritten Schnittpunkt von Kurve und Grade zu finden, und diesen dann an der X-Achse zu spiegeln. Wird ein Punkt auf sich selbst addiert ($[2]P$), verwendet man die Tangente als Verbindungsgrade. Das kann man mit einem Grenzwertargument motivieren.

In manchen Fällen sieht man gleich, dass es scheinbar keinen dritten Punkt gibt, zum Beispiel wenn man in Abbildung 6. $[2]P + R$ rechnet. Man definiert die

[11] vgl [Kleppmann 2022]

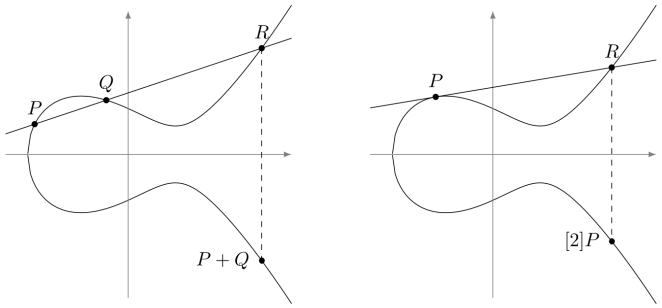

Abbildung 6: Das Gruppengesetz

Gruppe also auf $E(K) \cup \{\infty\}$, und setzt in solchen Fällen $P+Q = \infty$. Betrachtet man die Kurve im projektiven Raum verhält sich ∞ wie ein regulärer Punkt.

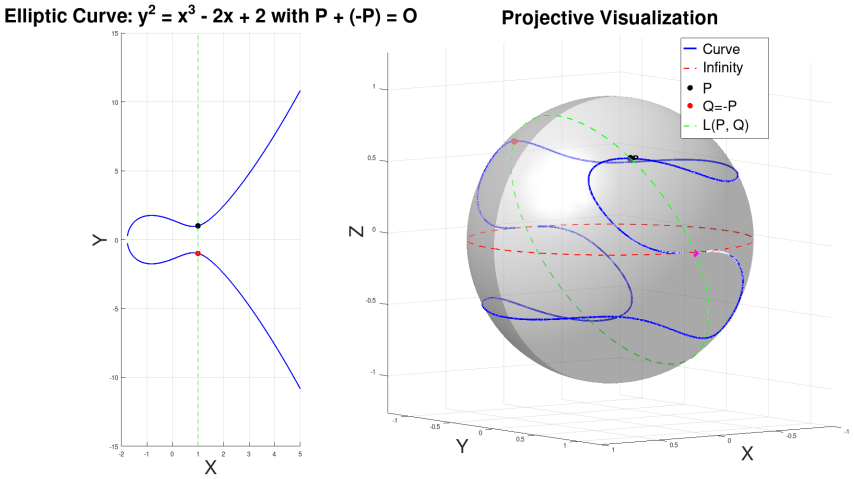

Abbildung 7: Gruppenaddition im affinen und projektiven Raum

Dass die Abbildung wohldefiniert ist, und dass die Axiome gelten wird im folgenden bewiesen, zunächst aber der Additionsvorgang formal definiert. Bei den expliziten Formeln beschränkt sich die Arbeit auf den affinen Fall.

Proposition 4.2.2 (Washington 2008, 2.2, Formeln zur Berechnung von Schnittpunkten im affinen Raum). Es ergeben sich die folgenden Fälle: (1) Ohne Einschränkung sei $Q = \infty$; setze $Q + P = P + Q := P$. (2) Angenommen $p_1 \neq q_1$. Dann ergibt sich die folgende Geraden-Gleichung: $y = m(x - p_1) + p_2$. wobei

$$m = \frac{q_2 - p_2}{q_1 - p_1}$$

ist. Um den Punkt auf E zu finden, setze ein:

$$(m(x-p_1)+p_2)^2 = x^3+ax+b$$

durch Umformen ergibt sich:

$$\begin{aligned} 0 &= x^3 - m^2x^2 + \dots \\ \text{Linearfaktoren: } r_1, p_1, q_1 & \\ &= (x-r_1)(x-p_1)(x-q_1) \\ &= x^3 - (r_1+p_1+q_1)x^2 + \dots \end{aligned}$$

durch Koeffizientenvergleich ergibt sich

$$m^2 = r_1+p_1+q_1 \iff r_1 = m^2 - q_1 - p_1$$

und aus der Geradengleichung und X-Spiegelung folgt $r_2 := m(p_1-r_1)-p_2$. (3) Sei nun $p_1 = q_1$ und $p_2 \neq q_2$ dann ist die Gerade vertikal und schneidet E am Punkt ∞. Man setzt in dem Fall $P+Q=\infty$. (4) Im letzten Fall $P=Q$ legt man eine Tangente an E an: Ohne Einschränkung sei $p_2 \neq 0$, sonst setze wieder $R := \infty$ (die Tangente ist vertikal). Implizites ableiten[12] ergibt

$$E' : 2y\frac{dy}{dx} = 3x^2 + a \implies m = \frac{dy}{dx} = \frac{3p_1^2+a}{2p_2}$$

p_1 ist diesmal eine doppelte Nullstelle, weil die Tangente die elliptische Kurve berührt. Wie oben folgt $r_1 := m^2 - 2p_1$ und wieder $r_2 := m(p_1-r_1)-p_2$ und $P+Q := R = (r_1, r_2)$.

Theorem 4.2.3 (Zusammenfassung der Gruppeneigenschaft bis auf Assoziativität). Das *neutrale Element* sei $e = \infty$ und man setze $P^{-1} := (p_1, -p_2)$ als das *inverse Element*. Die *Abgeschlossenheit* und die *Kommutativität* folgen aus der Konstruktion oben[13]

$$P+Q := \begin{cases} \infty, q_1 = p_1, q_2 \neq q_2 \\ Q, P = \infty \\ P, Q = \infty \\ R, \text{ sonst} \end{cases} , R := \begin{cases} \begin{pmatrix} m^2 - q_1 - p_1 \\ m(2p_1 + q_1 - m^2) - p_2 \end{pmatrix}, m := \frac{q_2-p_2}{q_1-p_1}, p_1 \neq q_1 \\ \begin{pmatrix} m^2 - 2p_1 \\ m(3p_1 - m^2) - p_2 \end{pmatrix}, m := \frac{3p_1^2+a}{2p_2}, P = Q \end{cases}$$

□

[12] Differenzierbarkeit auf allgemeinen Körpern ist nicht trivial. Ggf. reicht es aus, die Formel als axiomatische Definition zu betrachten.

[13] Alternativ kann man direkt den Satz von Bézout anwenden, wenn nicht die Weierstrass Form vorliegt: Aus der Glattheit folgt nämlich, dass die Schnittzahl immer Eins ist, und somit muss ein dritter Punkt existieren. vgl. [Stoll 2020] Satz 9.1

4.3 Beweis der Assoziativität

Für die Kryptographie reicht es, die Eigenschaften der Gruppenoperation mit einem Computeralgebraprogramm zu verifizieren. Das passiert im Kapitel 6. Im Folgenden wird aber ein rein mathematischer Beweis mit dem Lemma vom neunten Punkt geführt, das auf einer vereinfachten Version des Satzes von Bézout beruht. Weil die Abgeschlossenheit im ursprünglichen Körper bereits gezeigt wurde, kann man für den Beweisen Körper ohne Einschränkung erweitern. Sei also K algebraisch abgeschlossen.

Proposition 4.3.1 (Stoll 2020, Lemma 9.2, Lemma vom neunten Punkt). Seien G_i, G'_j, $i, j = 1, 2, 3$ paarweise verschiedene projektive Graden, sodass die neun Schnittpunkte P_{ij} paarweise verschieden sind. Sei weiter C eine ebene projektive Varietät vom Grad 3, die die acht Punkte P_{ij} mit $(i, j) \neq (3, 3)$ enthält. *Dann* enthält C auch P_{33}.

Beweis. Seien G_i und G'_j Varietäten gegeben durch lineare Polynome L_i, L_j. Es gibt 10 Monome vom Grad 3 in drei Variablen. Die Bedingung $P_{ij} \in C$ liefert eine homogene lineare Gleichung für die zehn Koeffizienten von C. Der Raum der homogenen Polynome vom Grad 3, die in den acht gegebenen Punkten verschwinden ist also mindestens 2-dimensional. In diesem Fall liegen die Polynome $L = L_1L_2L_3$ und $L' = L'_1L'_2L'_3$ in diesem Raum und sind linear Unabhängig. Im Folgenden wird durch Kontraposition gezeigt, dass die Dimension genau 2 ist. D. h. der Raum wird von L, L' aufgespannt. Angenommen dim ≥ 3, dann existieren $P_{ij} \neq A, B \in C$ so dass $A \in G_1$ und $B \notin G_1, G_2, G_3$. Sei $C : F(X, YZ) = 0$ eine Varietät vom Grad 3, die alle P_{ij} und P, Q enthält. Da G_1 diese Varietät in den vier Punkten P_{ij}, P schneidet folgt mit den Satz von Bézout dass L_1 ein Teiler von F ist. Es gilt $F = L_1F'$ mit einem homogenen Polynom F' vom Grad 2. Für F' gilt des weiteren $F \cap G_2 = \{P_{2j}, j = 1, 2, 3\}$. Folglich muss L_2 ein Teiler von F' sein: $F' = L_2F''$. Letztlich gilt noch $F'' \cap G_3 = \{P_{31}, P_{32}\}$, die Graden sind identisch, d. h. $F = cL, c \in K$. Das ist aber ein Widerspruch zu $Q \in C$.

Sei nun $C : F = 0$ eine Kurve vom Grad 3 durch die acht Punkte. Wie oben gezeigt gilt $F = cL + c'L', c, c\prime \in K$. Da die rechte Seite in P_{33} verschwindet (P_{33} liegt ja auf den Graden) ist das Lemma bewiesen □

Theorem 4.3.3 (Stoll 2020, Satz 9.1, Assoziativität auf elliptischen Kurven) Es gilt

$$(P+Q)+R = P+(Q+R)$$

Beweis. Wichtig sind die folgenden Objekte:
G_1 sei die Gerade durch P und Q (von nun an geschrieben $\overline{PQ}$);
X sei ihr dritter Schnittpunkt mit $E(K)$
$G_1' := \overline{\infty X}$; und
$P+Q$ der dritte Schnittpunkt mit $E(K)$;
$G_2' := \overline{QR}$; und
Y der dritte Schnittpunkt mit $E(K)$;
$G_2 := \overline{\infty Y}$; und
$Q+R$ der dritte Schnittpunkt mit $E(K)$;
$G_3 := \overline{(P+Q)R}$; und
Z_1 der dritte Schnittpunkt mit $E(K)$;
$G_3' := \overline{(Q+R)P}$; und
Z_2 der dritte Schnittpunkt mit $E(K)$;
letztlich sei Z der Schnittpunkt von G_3 und G_3'.

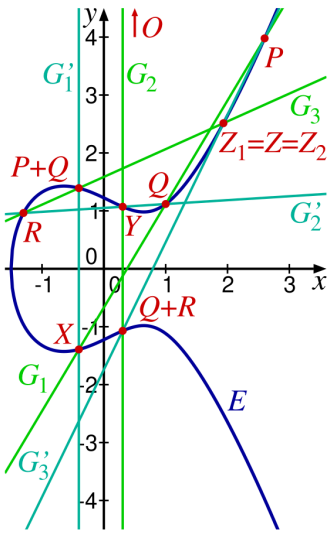

Abbildung 8: Graden-Gitter auf der elliptischen Kurve. Hier wird $O := \infty$ notiert.

Hier ist zu Bemerken, dass sich zwei beliebige Graden genau einmal Schneiden, und es genau 3 Schnittpunkte (respektive Multiplizität) von $E(K)$ und einer beliebigen Graden gibt (Satz von Bézout). Hier ist Z per Konstruktion assoziativ. Es bleibt zu zeigen, dass Z der gesuchte Punkt ist. Angenommen dass die Punkte $\infty, P, Q, R, X, Y, P+Q, Q+R, Z$ paarweise verschieden sind. Man wendet nun das *Lemma von neunten Punkt* an, und sieht dass $Z \in E(K)$, was zu zeigen war.

Aus Theorem 3.6.12 folgt, dass, wenn die Gleichung $\psi(S) = T$ für alle bis auf endlich viele $S \in E(K)$ gilt, ψ konstant ist, und die Gleichung folglich für alle $S \in E(K)$ gilt. Dafür muss die Kurve lediglich genug Punkte enthalten.
Beweis. Seien nun $P, R \neq \infty$, $P \neq R$ (sonst folgt die Assoziativität aus der Kommutativität). Dann folgt, dass es nur endlich viele Q geben kann, für die Q, R, P nicht paarweise verschieden sind (der Fall dass sie verschieden sind wurde bewiesen). Des weiteren gilt $\tilde{P} - \tilde{Q} = \infty \iff \tilde{P} = \tilde{Q}$. Der Morphismus

$$\phi_{P,R} : Q \mapsto ((P+Q)+R) - (P+(Q+R))$$

verschwindet demnach alle für fast alle $Q \in E(K)$. Es folgt $\phi_{P,R}$ konstant und die Assoziativität ist bewiesen. □

5 Technische Bemerkungen

5.1 Das Diffie Hellman Protokoll auf elliptischen Kurven

Statt $\mathbb{Z}/q\mathbb{Z}$ kann man auch $E(\mathbb{F}_p)$ für den Diffie-Hellman-Schlüsselaustausch verwenden. Man nennt das dann Elliptic-Curve-Diffie-Hellman ($ECDH$). Im Vergleich zum regulären Diffie-Hellman ermöglichen die elliptischen Kurven eine geringere Schlüssellänge bei gleicher Sicherheit[14].

5.2 Das Double-And-Add Verfahren

Bemerkung 5.2.1. Um das Diffie-Hellman-Protokoll mit elliptischen Kurven auszuführen, muss man offenbar $[d]P, d \in \mathbb{N}, P \in E(K)$ berechnen. Ein naiver Ansatz hat die Zeitkomplexität $O(d)$, weil etwa die Additionsformeln aus Algorithmus 3.3.2 d-mal ausgeführt werden. Das ist für große d ungünstig; Eine wesentliche Laufzeitverbesserung folgt jedoch aus der Gruppenassoziativität:

Proposition 5.2.2 (Schnellere Berechnung von Skalaren). Schreibe

$$d = \sum_{k=0}^{n} a_k \cdot 2^k, n \geq \log_2(d), a_i \in \{0, 1\}$$

(also in Binärdarstellung). Dann berechne $2^k P$, in dem P immer wieder verdoppelt wird ($P_{k+1} = 2P_k, P_0 = P$), und addiere diejenigen P_k für die $a_k \neq 0$ ist:

$$[d]P = \sum_{k=0}^{n} a_k \cdot P_k$$

Der neue Ansatz läuft mit $O(\log_2(d))$ und ist damit praxistauglich.

Bemerkung 5.2.3 (Sidechannel Angriffe). Unter einem Sidechannel-Angriff versteht man Angriffe auf Kryptosysteme, die das System nicht algorithmisch oder mathematisch lösen, sondern Umgebungsaffekte ausnutzen, wie z. B. den Leistungsverbrauch eines Prozessors. Der naive Double-And-Add-Algorithmus genau dafür anfällig[15]: Bei der Iteration wird nur dann eine Multiplikation durchgeführt, wenn das Bit im Schlüssel 1 ist. Wenn ein Angreifer nun den Leistungsverbrauch überwacht, kann dieser erhöhte Spannungen ablesen und auf den geheimen Schlüssel rekonstruieren. Ein Verfahren dazu ist die Simple Power Analysis (SPA), das in Abbildung 9 demonstriert wird.

5.3 Die Montgomery-Ladder

Die Montgomery-Ladder ist ein Additionsalgorithmus der gegen SPA resistent ist[16]. Es wird garantiert, das unabhängig vom Schlüssel immer eine der gleiche Typ von Operation durchgeführt wird, was den Sidechannel-Angriff erschwert.

[14] vgl. z. B. [Bundesamt für Sicherheit in der Informationstechnik 2025]
[15] vgl. [Walter 2004]
[16] vgl. [Kocher 1996]

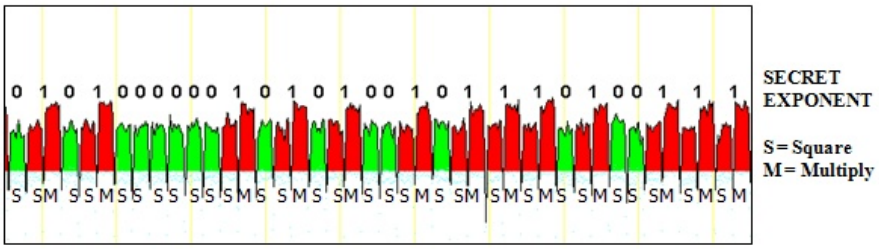

Abbildung 9: SPA eines RSA Systems mit Double-And-Add

Algorithmus 4: Montgomery-Ladder[17]

Input: g, $k = (k_{t-1}, \ldots, k_0)_2$
Output: $y = g^k$

$R_0 \leftarrow 1$
$R_1 \leftarrow g$
for $j = t - 1$ **to** 0 **do**
  if $k_j = 0$ **then**
    $R_1 \leftarrow R_0 \cdot R_1$
    $R_0 \leftarrow R_0^2$
  else
    $R_0 \leftarrow R_0 \cdot R_1$
    $R_1 \leftarrow R_1^2$
return R_0

6 Computer-assistierter Korrektheitsbeweis

Im Folgenden wird ein weiterer Beweisansatz vorgestellt, der diesmal nicht zur Intuition beitragen soll, sondern in der Praxis[18] dazu dient, (ggf. optimierte) Additionsformeln zu verifizieren. Dazu wird das Computeralgebrasystem (CAS) SageMath verwendet. Die hauptsächliche Schwierigkeit dieses Ansatzes besteht darin, dem CAS die Struktur der elliptischen Kurve effizient zu kommunizieren. Dazu werden weitere algebraische Grundlagen benötigt[19]. Insbesondere werden nun nicht mehr einzelne Punkte, sondern rationale Funktionen auf der elliptischen Kurve betrachtet. Dazu werden weitere algebraische Objekte definiert:

6.1 Ringe

Sei M eine nicht-leere Menge. Weiter seien $\oplus : M \times M \to M$ und $\otimes : M \times M \to M$ Abbildungen. $(M, \oplus, \otimes)$ heißt *Ring*, wenn gilt: $(M, \oplus)$ bilden eine Gruppe;

[17] vgl. [Kleppmann 2022]
[18] z. B. in der Explicit Formulas Database [Daniel J. Bernstein o. D.]
[19] Für die Definition von Ringen etc vgl. [Cox, Little und O'Shea 2015]

$\otimes$ ist abgeschlossen und assoziativ; Es gilt $(a \oplus b) \otimes c = a \otimes c \oplus b \otimes c$ und $a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c \forall a, b, c \in M$ (*Distributivgesetz*). Eine Teilmenge $I \subseteq R$ heißt *Ideal*, wenn $(I, \oplus)$ eine Teilgruppe von $(R, \oplus)$ ist, und I Multiplikationen absorbiert. D. h. falls $i \in I$ und $r \in R$ so gilt $i \cdot r \in I$ und auch $r \cdot i \in I$. Man schreibt $I \triangleleft R$. Ideale können durch eine endliche Menge $S \subseteq R$ generiert werden: $\langle S \rangle$ bezeichnet das kleinste Ideal, das S ganz enthält. Das ist die Menge der (endlichen) Linearkombinationen mit Koeffizienten in R: $\langle S \rangle = \{s_1 \cdot r_1 + \cdots + s_n \cdot r_n : r_i \in R, s_i \in S, n \in \mathbb{N}, i \in \{1, \dots n\}\}$. Die Menge der Polynome über einem Körper bildet mit Körper-Addition und -Multiplikation einen Ring.

6.2 Isomorphismen

Unter einer *isomorphen* oder strukturerhaltenden Abbildung versteht man eine Abbildung zwischen algebraischen Strukturen gleicher Klasse, die (1) bijektiv ist und (2) die algebraische Struktur erhält. Das heißt, dass sich die Abbildung linear bezüglich additiver oder multiplikativer Verknüpfungen verhält, also z. B. $\phi(x + ay) = \phi(x) + a\phi(y)$. Isomorphismen können z. B. zwischen Ringen und Gruppen definiert werden[20].

6.3 Quotientenringe

Es wurde bereits ein Quotientenraum behandelt, nämlich der projektive Raum. Gegeben sei ein Ring R und ein Ideal $I \triangleleft R$. Man erhält eine Äquivalenzrelation $\sim$ auf R mit $A \sim B \iff B - A \in I$ und damit den *Quotientenring* R/I. Für einen polynomialen Quotientenring gilt z. B. dass beliebige Linearkombinationen von Generator-Polynomen mit Null identifiziert werden.

Beispiel 6.3.1 (Restklassenring auf den ganzen Zahlen). Sei $R = \mathbb{Z}$ und $I = \langle p \rangle$ für eine Primzahl p. I enthält somit alle ganzzahlige Vielfache von p. Man schreibt auch $p\mathbb{Z}$. Betrachte $\mathbb{Z}/I = \mathbb{Z}/p\mathbb{Z}$: man erhält eine Struktur, in der alle ganzen Zahlen, die sich um ein vielfaches Unterscheiden identifiziert sind. Mit der Additiven Verknüpfung, die sich von R und I überträgt erhält man eine Gruppe, die sich ähnlich (isomorph) zur endlichen Gruppe auf $\{1, \dots, p\}$ mit Addition Modulo p verhält.

6.4 Beweis der Assoziativität

Der Idee ist die Folgende: Die Punkte Q, P, R werden als rationale Funktionen in zwei Variablen (insgesamt $P_x, P_y, Q_x, Q_y, R_x, R_y$) betrachtet, und jegliche Additionen genauso. Der Implementierung halber werden aber Polynome betrachtet, was ausreicht: rationale Funktionen sind offenbar genau dann identisch, wenn

$$ac = bd \iff \frac{a}{b} = \frac{c}{d}.$$

[20] Bemerkung. Silverman beweist die Assoziativität auf elliptischen Kurven, in dem die Existenz eines Isomorphismus zwischen der bekannten Verknüpfung auf E und der Picard-Gruppe $\mathrm{Pic}^0(E)$ gezeigt wird. vgl. [Silverman 2009], Proposition 3.4.

Statt den Polynomen in K sollen aber nur die Polynome auf $E(K)$ betrachtet werden. Um das zu erreichen werden genau die Polynome auf K gleichgesetzt, die auf $E(K)$ übereinstimmen. Dann wird die Identität der Additionen $P+(Q+R)$ und $(P+Q)+R$ in der Kurve kontrolliert, in dem SageMath die Ausdrücke algorithmisch vereinfacht. Um die Aussage auf beliebigen kurzen Weierstrass-Kurven zu zeigen, werden A und B als Variablen dazu genommen.

Proposition 6.4.1. Es werden drei Funktionen gleichzeitig betrachtet, daher sei $I = \langle P_y^2 - P_x^3 + AP_x + B, Q_y^2 - Q_x^3 + AQ_x + B, R_y^2 - R_x^3 + AR_x + B\rangle$. Um zu überprüfen, ob diese Funktionen auf der elliptischen Kurve identisch sind, wird der Quotientenring $K[P_x, P_y, Q_x, Q_y, R_x, R_y, A, B]/I$ betrachtet[21]. Dort sind Polynome identisch, wenn sie auf der Kurve identisch sind, was zu erreichen war. Genauso wie etwa $7 \equiv 2$ auf $\mathbb{Z}/\langle 5\rangle$ gilt, ist hier $P_y^2 \equiv P_x^3 + AP_x + B$. Insbesondere existiert ein Isomorphismus zwischen dem Quotientenring $K[X_1, \ldots, X_n]/I(E)$ und den Polynomen $E(K) \to K$ d. h. $K[X_1, \ldots, X_n]/I(E) \cong K[E]$ [22].

Theorem 6.4.2. Es folgt eine Implementierung in SageMath[23]. Hier werden Polynome mit über 500 Koeffizienten verglichen.

Listing 1: Verifizierung der Assoziativität von Elliptischen Kurven

```
RR.<Px,Py,Qx,Qy,Rx,Ry,A,B> = PolynomialRing(ZZ,8)
P=(Px,Py); Q=(Qx,Qy); R=(Rx,Ry)
I=RR.ideal(Py^2-Px^3-A*Px-B, Qy^2-Qx^3-A*Qx-B, Ry^2-Rx^3-A*Rx-B)
SS=RR.quotient(I)

def add(P,Q):
    x1=P[0]; y1=P[1]; x2=Q[0]; y2=Q[1];
    m = (y2-y1)/(x2-x1)
    x3 = m^2-x1-x2
    y3 = m*(x1-x3)-y1
    return (x3,y3)

def reduced_fractions_equal(p, q):
    return SS(p.numerator()*q.denominator()-p.denominator()*q.
        numerator()) == 0

def equal(P,Q):
    return reduced_fractions_equal(P[0],Q[0]) and
        reduced_fractions_equal(P[1],Q[1])

print("Confirmed associativity:", equal(add(add(P,Q),R),add(P,add(Q
    ,R))))
```

Um z. B. das Verfahren Curve25519 zu verifizieren, kann man `GF(2 ** 255 - 19)` statt `ZZ` einsetzen, um den endlichen Körper $\mathbb{F}_{2^{255}-19}$ zu nutzen auf dem Curve25519 basiert[24].

[21] vgl. [Friedl 2017]
[22] vgl. [Cox, Little und O'Shea 2015] Kap. 5, § 2, Theorem 7
[23] Der Quellcode ist eine Vereinfachung von [Sutherland 2021]. Man muss noch Sonderfälle betrachten.
[24] vgl. [Kleppmann 2022]

7 Ausblick

Das diskrete Logarithmus-Problem, und damit auch ECDH, gilt als quantenunsicher. Mit *Shors Algorithm* und einem hinreichend performanten Quantencomputer (d.h. ca. 2000 Qubits) kann das Problem in realistischer Zeit ($\mathcal{O}(n^2)$) gelöst werden[25]. Elliptische Kurven spielen in Isogenie basierten Kryptosystemen eine zentrale Rolle, die grundsätzlich für die Post-Quantum-Cryptography in Frage kommen[26].

[25] vgl. [Proos und Zalka 2004]
[26] siehe dazu z. B. [Feo 2017]

8 Quellen

Literatur

Bundesamt für Sicherheit in der Informationstechnik (2025). *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*. Accessed: 2025-04-11. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile.

Cox, David A., John Little und Donal O'Shea (2015). *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. 4. Aufl. Undergraduate Texts in Mathematics. Cham, Heidelberg, New York, Dordrecht, London: Springer. ISBN: 978-3-319-16720-6.

Daniel J. Bernstein, Tanja Lange (o. D.). *Explicit Formulas Database*. Accessed: 2025-04-11. URL: https://hyperelliptic.org/EFD/index.html.

Eklof, Paul C. (1973). „Lefschetz's Principle and Local Functors". In: *Proceedings of the American Mathematical Society* 37.2, S. 333–338. DOI: 10.1090/S0002-9939-1973-0325389-7. URL: https://www.ams.org/journals/proc/1973-037-02/S0002-9939-1973-0325389-7/S0002-9939-1973-0325389-7.pdf.

Feo, Luca De (2017). *Mathematics of Isogeny Based Cryptography*. arXiv: 1711.04062 [cs.CR]. URL: https://arxiv.org/abs/1711.04062.

Friedl, Stefan (2017). *An elementary proof of the group law for elliptic curves*. arXiv: 1710.00214 [math.AG]. URL: https://arxiv.org/abs/1710.00214.

Fulton, William (2008). *Algebraic Curves*. Accessed: 2025-05-11. URL: https://dept.math.lsa.umich.edu/~wfulton/CurveBook.pdf.

Hulek, Klaus (2012). *Elementare Algebraische Geometrie*. Springer Spektrum. ISBN: 978-3-8348-1964-2.

Jänich, Klaus (1990). *Topologie*. 3. Aufl. Springer.

Karpfinger, Christian (2024). *Algebra Gruppen – Ringe – Körper*. Springer Spektrum. ISBN: 978-3-662-68655-3.

Kleppmann, Martin (2022). *Implementing Curve25519/X25519: A Tutorial on Elliptic Curve Cryptography*. https://martin.kleppmann.com/papers/curve25519.pdf. Accessed: 2025-06-09.

Kocher, Paul C. (1996). „Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems". In: *Advances in Cryptology — CRYPTO '96*. Hrsg. von Neal Koblitz. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 104–113. ISBN: 978-3-540-68697-2.

Penrose, Roger (2004). *The Road to Reality*. London: Jonathan Cape. ISBN: 0-224-04447-8.

Proos, John und Christof Zalka (2004). *Shor's discrete logarithm quantum algorithm for elliptic curves*. arXiv: quant-ph/0301141 [quant-ph]. URL: https://arxiv.org/abs/quant-ph/0301141.

The Sage Developers (2025). *SageMath, the Sage Mathematics Software System (Version 10.5)*. https://www.sagemath.org.

Silverman, Joseph H. (2009). *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer-Verlag. ISBN: 978-0-387-09493-9.

Stoll, Michael (2020). *Elliptische Kurven*. Vorlesungsskript, Sommersemester 2020, Universität Bayreuth. Accessed: 2025-04-11. URL: https://www.mathe2.uni-bayreuth.de/stoll/teaching/ElliptischeKurven-SS2020/Skript-ElliptischeKurven-pub-screen.pdf.

Sutherland, Andrew (2021). *18.783 Elliptic Curves, Lecture #2*. MIT OpenCourseWare https://math.mit.edu/classes/18.783/2022/lectures.html. Accessed: 2025-06-21. URL: https://ocw.mit.edu.

Walter, Colin D. (2004). *Simple Power Analysis of Unified Code for ECC Double and Add*. Hrsg. von Marc Joye und Jean-Jacques Quisquater. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 191–204. ISBN: 978-3-540-28632-5.

Washington, Lawrence C. (2008). *Elliptic Curves Number Theory and Cryptography*. Taylor Francis Group, LLC. ISBN: 978-1-4200-7146-7.

Wätjen, Dietmar (2018). *Kryptographie Grundlagen, Algorithmen, Protolle*. Springer Vieweg. ISBN: 978-3-658-22473-8.

Abbildungen

Eidesstattliche Erklährung

Hiermit versichere ich, dass ich die Seminararbeit mit dem Titel

Korrektheit elliptischer Kryptosysteme und Fundierung in der algebraischen Geometrie

selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, alle Ausführungen, die anderen Schriften wörtlich oder sinngemäß entnommen wurden, kenntlich gemacht sind und die Arbeit in gleicher oder ähnlicher Fassung noch nicht Bestandteil einer Studien- oder Prüfungsleistung war. Ich verpflichte mich, ein Exemplar der Seminararbeit fünf Jahre aufzubewahren und auf Verlangen dem Prüfungsamt des Fachbereiches Medizintechnik und Technomathematik auszuhändigen.

Aachen, den 8. Juli 2025

Fabian Schuller