Diplomarbeit

Effiziente Berechnung der Tate Paarung

Anika Frischwasser

Mai 2008

Erstprüfer: Prof. Dr. Florian Heß

Institut für Mathematik der Technischen Universität Berlin

Die selbständige und eigenhändige Anfertigung versichere ich an Eides statt.

Unterschrift

Berlin, den 22. Mai 2008

Inhaltsverzeichnis

Notationsverzeichnis

Schreibweise	
K	Körper
$\overline{K}$	Algebraischer Abschluss eines Körpers K
$K^\times$	$K \setminus \{0\}$
E, C	Elliptische bzw. hyperelliptische Kurve
$E(L)$, $C(L)$	L-rationale Punkte der jeweiligen Kurve
g	Geschlecht einer Kurve
π_q	q-Potenz Frobenius-Endomorphismus
	$P := (x_P, y_P) \mapsto (x_P^q, y_P^q)$
$K[C]$	Assoziierter Koordinatenring zu C
$K(C)$	$=$ Quot$(K[C])$,
	Funktionenkörper der Kurve C
$\mathrm{ord}_P(f)$	Ordnung eines Punktes $P \in C$ an einer rationalen Funktion f
Div_C	Divisorgruppe auf der Kurve C
$\mathrm{Div}_C(K)$	Divisorgruppe auf der Kurve C über einem Körper K
$D \in \mathrm{Div}_C$	Divisor $D = \sum_{P_i \in C} n_i(P_i)$,
	mit $n_i \in \mathbb{Z}$, wobei fast alle $n_i = 0$ sind,
	Formale Summe von Punkten
$\deg(D)$	Grad eines Divisors D
Div_C^0	Gruppe der Divisoren vom Grad 0
$\mathrm{div}(f)$, (f)	Divisor einer rationalen Funktion $f \in K(C)^*$
Princ_C	Gruppe der Hauptdivisoren
Pic_C	Picard Gruppe, bezeichnet $\mathrm{Div}_C/\mathrm{Princ}_C$
Pic_C^0	Picard Gruppe vom Grad 0,
	bezeichnet $\mathrm{Div}_C^0/\mathrm{Princ}_C$
$\overline{D}$, $[D]$	Divisorklasse des Divisors D
$\rho(\overline{D})$, $\rho([D])$	Eindeutiger reduzierter Divisor der Divisorklasse $\overline{D}$ bzw. $[D]$
$\epsilon(\overline{D})$, $\epsilon([D])$	Effektiver Teil von $\rho(\overline{D})$ bzw. $\rho[D]$
$f_{s,P}$	Rationale Miller-Funktion,
	mit Divisor $(f_{s,P}) = s(P) - ([s]P) - (s-1)(O)$
$f_{s,P}^{\mathrm{norm}}$	Normalisierte Miller-Funktion,
$\hat{e}(\cdot,\cdot)$	Bilineare, nichtdegenerierte Abbildung
$e(\cdot,\cdot)$	Reduzierte Tate Paarung auf elliptischen Kurven,
	definiert als $e(P,Q) = f_{r,P}^{\frac{(q^k-1)}{r}}(Q)$
$T_r(\cdot,\cdot)^{\frac{(q^k-1)}{r}}$	Reduzierte Tate Paarung auf hyperelliptischen Kurven,
	definiert als $T_r(\overline{D_1}, \overline{D_2}) = f_{r,\overline{D_1}}^{\frac{(q^k-1)}{r}}(\overline{D_2})$

Einleitung

Die Ermöglichung einer effizienten Durchführung identitätsbasierter Kryptographie hat Paarungen einen Verwendungszweck im positiven Sinne geschaffen. In der identitätsbasierten Kryptographie ist der öffentliche Schlüssel dem Nutzer eindeutig über eine Information seiner Identität zuordbar. Beispielsweise kann diese Information die nutzereigene E-Mail Adresse sein, die eindeutig vergeben ist. Damit ist es innerhalb eines solchen Systems nicht mehr notwendig für einen öffentlichen Schlüssel ein Zertifikat ausstellen zu lassen. Statt einer Instanz, die diese Zertifizierungen durchführt, ist lediglich eine vertrauenswürdige Instanz zur Berechnung des geheimen Schlüssels aus den Daten des öffentlichen Schlüssels in diesem System einzusetzen.
Lange Zeit waren Paarungen nur ein Werkzeug der Kryptoanalyse und wurden zur Analyse der Sicherheit von Verschlüsselungsverfahren verwendet. Paarungen sind dabei bilineare Abbildungen, die nicht für jedes Argumentpaar (P, Q) einen trivialen Wert liefern, diese Eigenschaft bezeichnen wir fortan als *Nichtdegeneriertheit*.

Die Tate Paarung ist neben der Weil Paarung die bekannteste dieser Art von bilinearen, nichtdegenerierten Abbildungen, die für kryptographische Zwecke eingesetzt werden können. Die vorliegende Arbeit betrachtet die Berechnung dieser Paarung auf elliptischen und hyperelliptischen Kurven. Diese zugrundeliegenden Kurven sind interpretierbar als Polynome in den Variablen x, y und die Menge der Punkte einer solchen Kurve ist die Menge von Nullstellen des definierenden Polynoms.
Auf der Punktgruppe im Fall der elliptischen Kurven beziehungsweise auf der Gruppe formaler Summen von Punkten für hyperelliptische Kurven werden wir uns mit der Theorie der Tate Paarung auseinandersetzen.

Neben der klassischen Berechnung der Tate Paarung über den sogenannten *Miller-Algorithmus* zeigen wir die bekannten effizienten Implementierungstechniken auf und diskutieren effizent berechenbare Variationen der Tate Paarung wie beispielsweise die *Eta* und *Ate Paarungen*. Diese beiden Paarungen sind besitzen somit eine enge Relationzur Tate Paarung und bieten die Möglichkeit einer effizienten Berechnung.
Für Anwendungen in der Kryptographie ist es von besonderer Wichtigkeit eine effiziente Berechenbarkeit einer Paarung in Kombination mit der schwierigen Invertierbarkeit derselben zu besitzen. Diese Arbeit soll einen Überblick bezüglich der existierenden Möglichkeiten geben und neue Ansätze zur Konstruktion effizienter Paarungen aufzeigen.

Den Aspekt der paarungsbasierten Kryptographie wollen wir anhand verschiedener Protokolle verdeutlichen. Neben der konkreten Angabe wollen wir auch deren gewährleis-

tete Sicherheit betrachten, wobei die Sicherheit der Public-Key Kryptographie auf der angenommenen Berechnungsschwierigkeit mathematischer Probleme und der Klassifikation ihrer Komplexität beruht.

Die vorliegende Arbeit über die effiziente Berechnung der Tate Paarung ist wie folgt strukturiert. Kapitel 1 erläutert neben den Grundlagen elliptischer und hyperelliptischer Kurven, deren Arithmetik. In diesem Zusammenhang greifen wir die Theorie von Divisoren auf, welche wir als formale Summen von Punkten einführen. Mit der Theorie der Paarungen legen wir in Kapitel 2 den Grundstein für die Betrachtungen der effizienten Berechenbarkeit der Tate Paarung. Innerhalb dieses Kapitels führen wir sowohl die Tate Paarung als auch die Weil Paarung auf elliptischen und hyperelliptischen Kurven ein. In Kapitel 3 betrachten wir die Möglichkeiten der effizienten Implementierung und Variation der Tate Paarung. Als Variationen geben wir die Eta und Ate Paarungen an. Ebenfalls werden wir verschiedene Modfikationen und Kombinationen der Ate Paarung angeben und diskutieren. Mit der expliziten Konstruktion einer neuen Paarung auf speziellen elliptischen Kurven und einigen Beispielen beschließen wir dieses Kapitel.
In Kapitel 4 gehen wir auf verschiedene Anwendungsgebiete von Paarungen in der Kryptographie ein. Dieses Kapitel beinhaltet konkret ausformulierte kryptographische Protokolle und beleuchtet die zugrundeliegenden mathematischen Probleme auf denen diese Anwendungen basieren. Wir schließen die vorliegende Arbeit mit einem Fazit und weiterführenden Fragestellungen in Kapitel 5 ab.

Alle Implementierungen und notwendigen Rechnungen wurden mit dem Computeralgebrasystem **Magma** auf einem Intel®Core^{TM}2 Duo E6850@3.00GHz und 4GB RAM durchgeführt.
Dieses System wurde entwickelt, um eine Softwareumgebung für die Berechnungen mit Strukturen, welche in den Bereichen Algebra, Zahlentheorie, algebraische Geometrie und (algebraischer) Kombinatorik auftreten, bereitzustellen.

1 Grundlagen (hyper-)elliptischer Kurven und Divisoren

Dieses einführende Kapitel dient der inhaltlichen Aufbereitung der Grundzüge über elliptische und hyperelliptische Kurven, welche wir als Polynome in zwei Variablen auffassen und deren Punkte die Nullstellen dieses Polynoms sind. Wir gehen dabei auf die Grundlagen der Divisortheorie ein und betrachten darauf aufbauend die Arithmetik (hyper-)elliptischer Kurven.
Abschließen werden wir das Kapitel mit einigen Anmerkungen über Abbildungen auf und zwischen Kurven.

1.1 Elliptische Kurven

Dieser Abschnitt soll einen Einblick in die notwendige Theorie elliptischer Kurven geben, ohne dabei näher auf die zu Grunde liegenden Strukturen der algebraischen Geometrie einzugehen. Für detaillierte Informationen bezüglich dieser Grundlagen und Zusammenhänge verweisen wir auf die Literaturquellen [CF06], [Sil86] bzw. [Hul02].

Definition 1. Eine *elliptische Kurve* über einem Körper K ist eine durch die Gleichung

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K. \tag{1.1}$$

beschriebene Punktmenge. Dies sind die Nullstellen in $\overline{K} \times \overline{K}$ des Polynoms $g(x, y)$, welches durch Gleichung (1.1) als $g(x, y) = y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6$ bestimmt ist. Die in (1.1) angegebene Gleichung bezeichnen wir als *Weierstraßgleichung*.

Diese in Definition 1 beschriebene simultane Nullstellenmenge notieren wir als die Menge $E(\overline{K}) := \left\{(x_P, y_P) \in \overline{K} \times \overline{K} \mid g(x_P, y_P) = 0\right\} \cup \{O\}$. Der Punkt O heißt der *Punkt im Unendlichen* und diesen verwenden wir als neutrales Element der Addition. Betrachten wir einen Erweiterungskörper L von K, so bezeichnen wir die Menge der Nullstellen, deren Koordinaten in $L \times L$ liegen, als die Menge der *L-rationalen Punkte* der elliptischen Kurve und schreiben $E(L)$. Im Folgenden sei $E := E(\overline{K})$ für den algebraischen Abschluss $\overline{K}$ von K.
Eine elliptische Kurve heißt *glatt*, falls es keinen Punkt in $E(\overline{K})$ gibt für den die beiden partiellen Ableitungen $\frac{\partial g}{\partial x}$ und $\frac{\partial g}{\partial y}$ verschwinden. Das heißt eine glatte Kurve besitzt keine singulären Punkte und wir nennen eine Kurve dann auch nichtsingulär.

Im Folgenden betrachten wir Körper der Charakteristik $\neq 2, 3$. Unter diesen Voraussetzungen ist es möglich mittels linearer Substitution die Weierstraßgleichung (1.1) wesentlich zu vereinfachen.

Kurze Normalform und Invarianten

Sei E eine elliptische Kurve über K und $\mathrm{char}(K) \neq 2$. Dann kann unter Verwendung der Substitution $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ Gleichung (1.1) zu

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \quad \text{mit } b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3 \text{ und } b_6 = a_3^2 + 4a_6 \tag{1.2}$$

vereinfacht werden. Schließen wir für die Körpercharakteristik zusätzlich $\mathrm{char}(K) = 3$ aus, gilt also insgesamt $\mathrm{char}(K) \neq 2,\ 3$, so ist stets der Übergang zu einer noch einfacheren Weierstraßgleichung möglich. Diese Darstellung wird *kurze Weierstraßform* (oder auch *kurze Weierstraßgleichung*) genannt und wir schreiben

$$E : y^2 = x^3 + ax + b, \quad a \text{ und } b \in K. \tag{1.3}$$

Wenden wir nach der Transformation von Gleichung (1.1) in (1.2) noch die Substitutionen $x \mapsto \frac{x-3b_2}{36}$ und $y \mapsto \frac{y}{108}$ an, so wird der Term mit x^2 eliminiert und wir erhalten explizit die Gleichung $y^2 = x^3 + ax + b$ mit Koeffizienten $a = -27(b_2^2 - 24b_4)$ und $b = -54(-b_2^3 + 36b_2b_4 - 216b_6)$.
Weitere Fälle in denen eine Vereinfachung der Gleichung (1.1) erreicht werden kann, sind in [Sil86] eingehend behandelt, einige Vereinfachungen listen wir in Tabelle 1.1 auf.

In manchen Fällen ist es möglich, statt einer gegebenen Kurve mit komplizierter Gleichung, eine einfacher zuhandhabende, isomorphe Kurve zu betrachten. Allerdings müssen wir uns in diesem Zusammenhang zunächst die Frage „*Wann sind zwei gegebene elliptische Kurven isomorph zueinander?*“ stellen. Die Antwort führt direkt zu den Begriffen der Diskriminante und der j-Invariante einer elliptischen Kurve.
Dabei legt die *j-Invariante* die Isomorphieklasse der Kurve über dem algebraischen Abschluss fest und wir nennen zwei elliptische Kurven E, E' genau dann isomorph zueinander, wenn für ihre j-Invarianten Gleichheit gilt, also $j_E = j_{E'}$ erfüllt ist. Das heißt für zwei elliptische Kurven mit derselben j-Invariante existiert ein Isomorphismus $E \to E'$.
Bevor wir die j-Invariante betrachten, führen wir den Begriff der Diskriminante einer elliptischen Kurve ein. Über diesen Begriff kann die Bedingung der Nichtsingularität einer Kurve dahingehend überführt werden, dass die Diskriminante der Gleichung von E ungleich null ist. Die Diskriminante ist hierbei ein Polynom in den Koeffizienten a_i. Speziell im Fall einer kurzen Weierstraßgleichung (1.3) mit $f(x) := x^3 + ax + b$ ist die Diskriminante leicht hinzuschreiben.

Definition 2. Die Diskriminante Δ_E einer durch Gleichung (1.3) beschriebenen elliptischen Kurve E ist gleich der Diskriminante des Polynoms f, welche (bis auf Vorzeichen) ein Produkt von Differenzen der Nullstellen von f ist:

$$\Delta_E = -16(4a^3 + 27b^2).$$

Werden elliptische Kurven über einem Körper beliebiger Charakteristik betrachtet, so ist anzumerken, dass die Diskriminante eine wesentlich komplexere Gestalt hat. Dies soll uns hier nicht weiter beschäftigen und eine Definition mit weiteren diesbezüglichen Anmerkungen findet sich in [Sil86, §1] oder [Wer02, Abschnitt 2.3].

Definition 3. Die *j-Invariante* (auch als *absolute Invariante* bezeichnet) j_E von E ist definiert durch

$$j_E = 12^3 \frac{-4a^3}{\Delta_E}.$$

Tabelle 1.1: Kurze Weierstraßformen elliptischer Kurven und ihre Invarianten [Sil86]

char(K)	elliptische Kurve E	Diskriminante Δ_E	j-Invariante j_E
$\neq 2, 3$	$y^2 = x^3 + a_4x + a_6$	$-16(4a_4^3 + 27a_6^2)$	$-12^3(4a_4)^3/\Delta$
3	$y^2 = x^3 + a_2x^2 + a_6$	$-a_2^3a_6$	$-a_2^3/a_6$
3	$y^2 = x^3 + a_4x + a_6$	$-a_4^3$	0
2	$y^2 + xy = x^3 + a_2x^2 + a_6$	a_6	$1/a_6$
2	$y^2 + a_3y = x^3 + a_4x + a_6$	a_3^4	0

Zu dem jetzigen Zeitpunkt ist es uns möglich elliptische Kurven in einer möglichst einfachen Form zu betrachten. Wir können Entscheidungen über spezielle Eigenschaften von elliptischen Kurven treffen. Bevor wir uns in Abschnitt 1.4.1 weiterführend mit den Punkten dieser Kurven, deren Arithmetik, Anzahl und daraus resultierenden Aussagen über die Kurve beschäftigen, definieren wir die zweite, uns in dieser Arbeit beschäftigende, Art von Kurven.

1.2 Hyperelliptische Kurven

Innerhalb dieses Abschnittes bseschäftigen uns Verallgemeinerungen elliptischer Kurven.

Definition 4. Eine *hyperelliptische Kurve C vom Geschlecht g über K* ist definiert als eine, durch eine Gleichung der Form

$$C : y^2 + h(x)y = f(x), \text{ mit } h, f \in K[x], \deg(f) = 2g + 1, \deg(h) \leq g, \tag{1.4}$$

beschriebene, Punktmenge, falls kein Punkt $P = (x_P, y_P) \in \overline{K} \times \overline{K}$ den drei Gleichungen

$$C : y_P^2 + h(x_P)y_P = f(x_P) \ \wedge \frac{\partial C}{\partial y} : 2y_P + h(x_P) = 0 \ \wedge \frac{\partial C}{\partial x} : f'(x_P) - h'(x_P)y_P = 0$$

genügt.

Die Bemerkung über die partiellen Ableitungen stellt hierbei sicher, dass die Kurve C nichtsingulär ist.

Nach Definition 4 können wir elliptische Kurven als spezielle hyperelliptische Kurven des Geschlechts eins mit

$$C : y^2 + h(x)y = f(x), \text{ mit } h, f \in K[x], \deg(f) = 3, \deg(h) \leq 1$$

auffassen.
Für einen Erweiterungskörper L von K definieren wir die Menge der *L-rationalen Punkte auf C* als $C(L) = \left\{(x_P, y_P) \in L \times L \mid y_P^2 + h(x_P)y_P = f(x_P)\right\} \cup \{O\}$, wobei O den Punkt im Unendlichen bezeichnet. Schreiben wir im Folgenden C, so meinen wir damit $C(\overline{K})$.
Als das Negative eines Punktes $P = (x_P, y_P)$ bezeichnen wir das Bild von P bezüglich der natürlich gegebenen *Involution* ι, d. h. einer selbstinversen Abbildung, für die wir das Bild als $-P := \iota(P) = (x_P, -y_P - h(x_P))$ definieren. Die fixen Punkte unter dieser so genannten *hyperelliptischen* Involution nennen wir *Weierstraß-Punkte*. Sprechen wir fortlaufend in dieser Arbeit über hyperelliptische Kurven, so meinen wir Kurven mit genau einem Weierstraß-Punkt, dieser sei der Punkt im Unendlichen für den $\iota(O) = O$ gilt.

Kurze Weierstraßgleichungen

Ist die Charakteristik des Körpers ungleich zwei, so kann die definierende Gleichung einer durch (1.4) gegebenen Kurve mittels einer Transformation in eine Kurve der Form

$$C : y^2 = f(x), \text{ mit } f \in K[x] \text{ und } \deg(f) = 2g + 1 \tag{1.5}$$

überführt werden. Eine solche Kurve C ist genau dann nichtsingulär, falls kein Punkt den partiellen Ableitungen

$$\frac{\partial C}{\partial y} : 2y = 0 \quad \text{und} \tag{1.6}$$

$$\frac{\partial C}{\partial x} : 0 = f'(x) \tag{1.7}$$

genügt. Jene Punkte, für die Gleichung (1.6) gilt, sind von der Form $P_i = (x_i, 0)$. Ausserdem müssen diese Punkte $f(x_i) = 0$ erfüllen, da anderenfalls der Punkt nicht auf der Kurve liegt.
Für singuläre Punkte muss zudem die partielle Ableitung (1.7) verschwinden, also muss

$f'(x_i) = 0$ gelten. Damit liegt an x_i eine doppelte Nullstelle von f vor und wir stellen fest, dass die durch (1.5) beschriebene Kurve C nichtsingulär ist, falls f nur einfache Nullstellen über dem algebraischen Abschluss besitzt.

Für den Fall der Charakteristik zwei nehmen wir vorab $h(x) = 0$ an, das heißt wir könnten (1.4) ebenso wie im Fall zuvor als $y^2 = f(x)$ schreiben. Die partiellen Ableitungen sind wiederum durch (1.6) und (1.7) gegeben. Für jede der Nullstellen x_i von f' erhalten wir einen Punkt (x_i, y_i), der sowohl die Gleichung $y_i^2 = f(x_i)$ als auch die beiden partiellen Ableitungen erfüllt. Falls x_i eine Nullstelle der Funktion f ist, gilt $y_i^2 = 0$ und es folgt, dass dann gerade $y = 0$ erfüllt ist.
Die Annahme $h(x) = 0$ führt also sofort zu einem singulären Punkt und somit muss $h(x) \neq 0$ gelten.

Bevor wir die Arithmetik der erläuterten Kurven betrachten können, müssen wir auf die Theorie der Divisoren als formale Summen von Punkten eingehen.

1.3 Divisortheorie

Dieser Abschnitt legt die, für die Angabe der Arithmetik auf (hyper-)elliptischen Kurven, fehlenden Grundbausteine. Mittels der Betrachtung von Divisoren als *formale Summen von Punkten* ist es uns auf eine sehr nützliche Art und Weise möglich die Null- und Polstellen von rationalen Funktionen zu beschreiben.
Zunächst geben wir einige grundlegende Definitionen an.

Der *Koordinatenring von C über K* ist der Quotientenring $K[C] := K[x, y]/(y^2 + h(x)y - f(x))K[x, y]$.
Analog definieren wir $\overline{K}[C] := \overline{K}[x, y]/(y^2 + h(x)y - f(x))\overline{K}[x, y]$ als *Koordinatenring von C über* $\overline{K}$. Die Elemente von $\overline{K}[C]$ heißen *Polynomfunktionen*. Da $y^2 + h(x)y - f(x)$ über dem algebraischen Abschluss $\overline{K}$ irreduzibel ist, ist der Koordinatenring $\overline{K}[C]$ ein Integritätsring[1]. Die Ordnung $\mathrm{ord}_Q(p)$ einer solchen Polynomfunktion p an einem Punkt Q der Kurve ist entweder

- Null, falls $Q \neq \mathcal{O}$ und $p(Q) \neq 0$,
- die Vielfachheit der Nullstelle, falls $Q \neq \mathcal{O}$ und $p(Q) = 0$
- oder der negierte Grad der Polynomfunktion, falls $Q = \mathcal{O}$.

Den Quotientenkörper zu $K[C]$ nennen wir *Funktionenkörper von C über K* und notieren diesen mit $K(C)$. Analog definieren wir $\overline{K}(C)$. Die in $\overline{K}(C)$ enthaltenen Elemente

[1] Ein kommutativer Ring R heißt *Nullteilerfrei* oder *Integritätsring*, wenn $R \neq \{0\}$ und R nur 0 als Nullteiler besitzt. Ein Element a eines Ringes R heißt Nullteiler, wenn ein $b \in R \setminus \{0\}$ mit $ab = 0$ oder $ab = 0$ existiert. [Bos06]

heißen *rationale Funktionen auf C* und wir definieren die Ordnung $\mathrm{ord}_P(q)$ einer solchen Funktion $q = \frac{p_Z}{p_N}$, mit $p_Z, p_N \in \overline{K}[C]$, an einem Punkt P der Kurve als

$$\mathrm{ord}_P(q) := \mathrm{ord}_P(p_Z) - \mathrm{ord}_P(p_N).$$

Wir nennen eine rationale Funktion u ein uniformisierendes Element, falls $\mathrm{ord}_P(u) = 1$ für einen Punkt P gilt. Weiterhin ist u eine rationale Funktion, die das maximale Ideal der in P regulären Funktionen f mit $f(P) = 0$ erzeugt.

An dieser Stelle haben wir die nötigen Begriffe erklärt und beginnen mit der Theorie über Divisoren.

Definition 5. Die *Divisorgruppe* Div_C *von C* ist die freie abelsche Gruppe über den Punkten der Kurve C. Ein Element $D \in \mathrm{Div}_C$ heißt *Divisor* und ist gegeben durch die formale Summe

$$D = \sum_{P_i \in C} n_i(P_i), \text{ mit } n_i \in \mathbb{Z}, \text{ und } n_i = 0 \text{ für fast alle } i.$$

Diese Gruppe schreiben wir additiv und es gilt für die (kommutative) Addition zweier Divisoren $D = \sum_{P_i \in C} n_i(P_i)$, $E = \sum_{P_i \in C} m_i(P_i) \in \mathrm{Div}_C$

$$D + E = \sum_{P_i \in C} n_i(P_i) + \sum_{P_i \in C} m_i(P_i) = \sum_{P_i \in C} (n_i + m_i)(P_i).$$

Analog gilt $D - E = \sum_{P_i \in C} n_i(P_i) - \sum_{P_i \in C} m_i(P_i) = \sum_{P_i \in C} (n_i - m_i)(P_i)$ für die Differenz zweier Divisoren.
Als *Träger* eines Divisors D bezeichnen wir jene Menge von Punkten P_i, deren Koeffizienten n_i nicht Null sind, also $\mathrm{supp}(D) := \{P_i \in C \mid n_i \neq 0\}$ und definieren den *Grad* $\deg(D)$ *eines Divisors D* als Abbildung

$$D \mapsto \deg(D) := \sum_{P_i \in C} n_i \in \mathbb{Z}.$$

Ein Divisor wird *effektiv* genannt, sofern für alle Koeffizienten $n_i \geq 0$ gilt. Ist die Divisordifferenz $E - D = \sum_{P_i \in C} (m_i - n_i)(P_i)$ für zwei Divisoren $D = \sum_{P_i \in C} n_i(P_i)$ und $E = \sum_{P_i \in C} m_i(P_i)$ effektiv, so schreiben wir $E \geq D$ und erhalten eine Halbordnung auf der Menge der Divisoren.
Wir können jeden Divisor $D \in \mathrm{Div}_C$ in zwei effektive Divisoren zerlegen, wobei wir den Anteil der Punkte, deren Koeffizienten größer oder gleich Null sind, mit D_0 bezeichnen und D_∞ für den Anteil der Punkte mit negativem Koeffizienten schreiben. Wir definieren

$$D_0 = \sum_{P_i \in C,\, n_i \geq 0} n_i(P_i) \quad \text{und} \quad D_\infty = \sum_{P_i \in C,\, n_i < 0} -n_i(P_i), \tag{1.8}$$

so dass D der Differenz zwischen D_0 und D_∞ entspricht, d.h. $D = D_0 - D_\infty$.

Innerhalb dieser Arbeit betrachten wir meist Divisoren vom Grad Null. Diese bilden eine Gruppe, welche wir mit Div_C^0 notieren. Besondere Aufmerksamkeit widmen wir dabei den Divisoren rationaler Funktionen, den so genannten *Hauptdivisoren*, welche wir über Definition 6 charakterisieren.

Definition 6. Sei $f \in \overline{K}(C)^\times$. Der *Divisor einer rationalen Funktion* f ist definiert durch die Abbildung

$$\begin{aligned} \mathrm{div} : \overline{K}(C)^\times &\to \mathrm{Div}_C \\ f &\mapsto (f) := \mathrm{div}(f) = \sum_{P_i \in C} \mathrm{ord}_{P_i}(f)(P_i). \end{aligned} \tag{1.9}$$

Ein Divisor D mit $D = (f)$ für eine Funktion $f \in \overline{K}(C)^\times$ heißt *Hauptdivisor* und der Grad eines solchen ist stets Null [CF06, Proposition 4.104]. Ein ausführlicher Beweis dieser Eigenschaft ist in [Hul02, Kapitel *VI*. Abschnitt 2] zu finden. Die Menge der Hauptdivisoren bildet eine Untergruppe von Div_C^0 und wir bezeichnen diese mit Princ_C.

Analog zu der Zerlegung in (1.8) können wir auch für Divisoren von Funktionen eine Darstellung als Differenz von effektiven Divisoren erklären.

$$(f) = \sum_{P_i \in C,\, \mathrm{ord}_{P_i}(f) \geq 0} \mathrm{ord}_{P_i}(f)(P_i) - \sum_{P_i \in C,\, \mathrm{ord}_{P_i}(f) < 0} -\mathrm{ord}_{P_i}(f)(P_i) =: (f)_0 - (f)_\infty.$$

Die in $(f)_0$ auftretenden Punkte mit Koeffizienten ungleich Null heißen *Nullstellen von* f. In $(f)_\infty$ auftretende nennen wir *Pole*.

Für eine Funktion f und einen Divisor $D \in \mathrm{Div}_C^0$ mit $\mathrm{supp}((f)) \cap \mathrm{supp}(D) = \{O\}$, d.h. die Träger sind disjunkt voneinander, definieren wir die Auswertung von f an D als $f(D) = \prod_P f(P)^{n_P}$. Sind f und D über einem Körper K definiert, so liegt auch $f(D)$ in K.

Auf die Arithmetik von Divisoren gehen wir hier nicht weiter ein, merken jedoch an, dass wir für Hauptdivisoren die folgenden Rechenregeln häufiger verwenden.
Seien f und g rationale Funktionen. Das Produkt dieser beiden Funktionen ist dann wieder rational und wir können den entsprechenden Hauptdivisor als $(fg) = (f) + (g)$ angeben.
Und analog erhalten wir für den Hauptdivisor des Quotienten $\frac{f}{g}$ dann $(\frac{f}{g}) = (f) - (g)$ [BSSC05, Abschnitt *IX*.2].
Mehrfache Anwendung liefert für $j \in \mathbb{Z} \setminus \{0\}$ dementsprechend $(f^j) = j(f)$.

Um zwei Divisoren D_1 und D_2 aus Div_C klassifizieren zu können, nennen wir D_1 und D_2 *linear äquivalent* zueinander, in Zeichen: $D_1 \sim D_2$, sofern sie sich nur um einen Hauptdivisor unterscheiden:

$$D_1 \sim D_2 \Leftrightarrow \text{ es existiert eine Funktion } f \in K(C)^\times \text{ mit } D_1 = D_2 + (f).$$

Als die *Divisorklassengruppe von C* bezeichnen wir die Faktorisierung der Gruppe der Divisoren nach den Hauptdivisoren: $\mathrm{Div}_C/\mathrm{Princ}_C$. Diese wird mit Pic_C (*Picardgruppe von C*) bezeichnet.
Die *Picardgruppe vom Grad Null von C* ist analog definiert als $\mathrm{Div}_C^0/\mathrm{Princ}_C$ und wir bezeichnen diese mit Pic_C^0.
Für Divisoren D_1, $D_2 \in \mathrm{Div}_C^0$ gilt

$$D_1 \sim D_2 \Leftrightarrow D_1 - D_2 \in \mathrm{Princ}_C \Leftrightarrow \overline{D_1} = \overline{D_2} \text{ in } \mathrm{Pic}_C^0.$$

Weiterhin nennen wir einen Divisor D *semireduziert*, falls eine Darstellung der Form

$$D = \sum_{i=1}^{l} (P_i) - l(O)$$

existiert, wobei die Punkte P_i in $C \setminus O$ enthalten sind und zudem $P_i \neq -P_j$ für $i \neq j$ erfüllen.

Definition 7 ([CF06])**.** Enthält der Träger von D höchstens geschlechtviele Punkte, das heißt $l \leq g$, so wird D als *reduzierter Divisor* bezeichnet.

Für elliptische Kurven spezifizieren wir die vorangestellte Definition 7.
Reduzierte Divisoren sind in diesem Fall für einen Punkt P der Kurve von der Form $D = (P) - (O)$. Diese Darstellungsform erhalten wir aus den Eigenschaften, dass der Träger eines reduzierten Divisors $l \leq g$ Punkte enthalten soll und für elliptische Kurven $g = 1$ gilt.

Sei C eine (hyper-)elliptische Kurve über einem Körper K, $P = (x_P, y_P) \in C$ und σ ein Automorphismus von $\overline{K}$ über K. Dann ist $P^\sigma := (\sigma(x_P), \sigma(y_P))$ ebenfalls ein Punkt der Kurve C. Wir nennen einen Divisor *definiert über K* oder auch *K-rational*, falls $D^\sigma := \sum n_i P_i^\sigma = D$ für alle Automorphismen σ von $\overline{K}$ über K.

Wir sind in der elementaren Theorie der Kurven und Divisoren so weit fortgeschritten, dass wir an dieser Stelle die Arithmetik auf (hyper-)elliptischen Kurven konkretisieren. Im Anschluss schieben wir einen Exkurs über Abbildungen auf und zwischen Kurven ein. Als grundlegende Literatur verwenden wir dazu [CF06] und [Sil86].

1.4 Arithmetik (hyper-)elliptischer Kurven

Zunächst erklären wir die Arithmetik elliptischer Kurven, wofür wir die Kenntnisse über Divisoren noch nicht benötigen. Im Anschluss wenden wir die in Abschnitt 1.3 gewonnenen Kenntnisse auf die Grundzüge der Arithmetik hyperelliptischer Kurven an.

Dem Titel dieser Arbeit entsprechend ist die effiziente Berechnung der Tate Paarung auf (hyper-)elliptischen Kurven das Kernthema. Für die Auswertung dieser Paarung muss

eine sogenannte Miller-Funktion f_{m,g_1} an einem Element g_2 einer abelschen Gruppe evaluiert werden. Der durch eine solche Miller-Funktionen definierte Hauptdivisor lässt sich in der einfachen Form

$$\begin{aligned}(f_{m,g_1}) &= m((g_1) - (O)) - (([m]g_1) - (O)) \\ &= m(g_1) - ([m]g_1) - (m-1)(O)\end{aligned}$$

schreiben. Die zugrundeliegenden abelschen Gruppen basieren auf den Punktgruppen der betrachteten Kurve.
Eine der arithmetisch teueren Operationen, welche innerhalb der Paarungsberechnung verwendet wird, ist die Multiplikation eines Skalaren m mit einem Punkt P, also die Berechnung von $[m]P$ bzw. von mD für einen Divisor D. Dies gibt Anlass dazu verschiedene Techniken zur effizienten Auswertung zu finden und anzuwenden.
Eine ausführliche Aufbereitung der Grundlagen über Paarungen geben wir in Abschnitt 2.1 auf elliptischen und hyperelliptischen Kurven.

1.4.1 Arithmetik auf elliptischen Kurven

Statten wir die Menge der Punkte einer Kurve E mit einer Addition und geeigneter Inversenbildung aus, so bilden die Punkte der elliptischen Kurve eine abelsche Gruppe und die betrachtete Addition wird als *Tangent-And-Chord*-Methode bezeichnet.
Für die Angabe der expliziten Formeln betrachten wir den folgenden Satz.

Satz 1 ([Wer02])**.** *Sei E eine elliptische Kurve der Form (1.3) über einem Körper K und $P = (x_1, y_1), Q = (x_2, y_2)$ zwei Punkte der Kurve E. Dann gilt*

1. *Für $P \in E$ ist $-P = (x_1, -y_1)$ das additive Inverse.*
2. *Falls $x_1 = x_2$ und $y_1 + y_2 = 0$ gilt, so ist $P + Q = O$ (demnach ist $Q = -P$).*
3. *Falls 1. und 2. nicht gelten, so liegt $R := P + Q$ in E mit $R = (x_3, y_3)$ und*

$$\left.\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1, \end{aligned}\right\} \quad \text{wobei} \quad \lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{, für } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{, für } P = Q \end{cases}.$$

Der Beweis dieses Satzes ist äußerst rechenaufwändig und wird in [Wer02], zusammen mit der geometrischen Deutung der *Tangent-And-Chord*-Methode, explizit durchgeführt.

Mit der in Satz 1 erklärten Punktaddition ist es leicht die Definition der Multiplikation mit einem Skalar einzuführen. Für $m \in \mathbb{Z}$ und $P \in E$ ist die Multiplikation mit m gegeben durch:

$$\begin{aligned} P \mapsto [m]P &= \underbrace{P + P + \ldots + P}_{m-\text{Mal}} \quad \text{für} \quad m > 0, \\ P \mapsto [m]P &= [- \mid m \mid]P = [\mid m \mid](-P) = -([\mid m \mid]P) \quad \text{für} \quad m < 0. \end{aligned}$$

Es gilt insbesondere $[0]P = \mathcal{O}$.

Zu Beginn dieses Abschnittes haben wir die Skalar-Punkt-Multiplikation als arithmetisch teuere Operation beschrieben, da für die Vervielfachung eines Punktes P m teuere Punktadditionen nötig sind. Für ein großes m ist dies ineffizient. In Implementierungen werden diese Berechnungen unter der Verwendung des Horner-Schemas in Kombination mit der Binärdarstellung der Zahl m beschleunigt.

Diese Idee wollen wir beispielhaft an der Berechnung von $[m]P$ für $m = 10^6$ erläutern [Sma99] und konkret den zugehörigen *Double-And-Add* Algorithmus angeben.

Beispiel 1. Die Binärdarstellung für m ist gegeben durch $(11110100001001000000)_2$. Die naive Rechenanweisung ist

$$[m]P = [2^{19}]P + [2^{18}]P + [2^{17}]P + [2^{16}]P + [2^{14}]P + [2^9]P + [2^6]P.$$

Die Verwendung des Horner-Schemas in Kombination mit der Binärentwicklung ergibt die effizientere Berechnung als

$$[m]P = [2^6](P + [2^3](P + [2^5](P + [2^2](P + [2](P + [2](P + [2]P)))))).$$

Wollen wir dieses Vorgehen systematisch anhand eines Algorithmus beschreiben, so erhalten wir den sehr einfachen *Double-And-Add* Algorithmus 1.

Algorithmus 1 : Double-And-Add Algorithmus

Input : Die Zahl $m = (m_{l-1} \dots m_0)_2$ mit $m_{l-1} = 1$, ein Punkt P.
Output : Der Punkt $[m]P$

```
1 V ← P;
2 for i = l − 2 to 0 do
3     V ← 2V;
4     if r_i = 1 then
5         V ← V + P;
6     end
7 end
8 return V
```

Eine weitere effiziente Vorgehensweise zur Berechnung von $[m]P$ ist die Verwendung effizient berechenbarer Endomorphismen wie zum Beispiel in [Tak07] verwendet oder auch die Frobenius-Entwicklung der Zahl m [Sma99].
Die Idee der effizienten Endomorphismen beschreiben wir eingehender in Abschnitt 3.2.4 und geben eine Anwendungsmöglichkeit zur Evaluation einer Paarung an. Die Frobenius-Entwicklung behandeln wir im Anschluss an diesen Abschnitt..
Zunächst jedoch geben wir einige weiterführende Bemerkungen bezüglich elliptischer Kurven, deren Punkten und damit zusammenhängenden Eigenschaften an.

Als die *Ordnung* eines Punktes $P \in E$ bezeichnen wir die kleinste $n \in \mathbb{N} \setminus \{0\}$, für die $[n]P = O$ gilt. Existiert eine solche Zahl nicht, so sagen wir der Punkt hat unendliche Ordnung. Punkte endlicher Ordnung nennen wir *Torsionspunkte*.
Für jeden m-Torsionspunkt P aus E gilt stets $[m]P = O$ und ein Punkt P ist genau dann ein m-Torsionspunkt, falls dessen Ordnung m teilt. Die Untergruppe, welche gerade die m-Torsionspunkte enthält, wird mit $E[m] := \{P \in E \mid [m]P = O\}$ bezeichnet.

Für Paarungen und deren zugehörige Anwendungen werden endliche Körper $\mathbb{F}_q$, für eine Primzahlpotenz $q = p^l$ verwendet. Daher gehen wir an dieser Stelle auf einige wichtige Aspekte über endliche Körper ein.

Die Anzahl der Elemente eines endlichen Körpers entspricht der Primzahlpotenz p^l mit $l \geq 1$. Umgekehrt gibt es zu jeder Primzahlpotenz $q = p^l$ bis auf Isomorphie genau einen endlichen Körper $\mathbb{F}_q$.
Körpererweiterungen eines endlichen Körpers, haben stets die Form $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ und solch eine Körpererweiterung ist galoissch mit zyklischer Galoisgruppe der Ordnung n. Die Galoisgruppe wird erzeugt von dem *Frobenius-Automorphismus* $x \mapsto x^q$.
Der algebraische Abschluss von $\mathbb{F}_q$ ist die Vereinigung $\overline{\mathbb{F}_q} = \bigcup_n \mathbb{F}_{q^n}$ und wir schreiben $\mathbb{F}_q = \{x \in \overline{\mathbb{F}_q} \mid x^q = x\}$.
Die Menge der *Einheiten von* $\mathbb{F}_q$ sind $\mathbb{F}_q^\times = \{x \in \overline{\mathbb{F}_q} \mid x^{q-1} = 1\} = \mu_{q-1}$.

Um die Anzahl der Punkte einer elliptischen Kurve über einem endlichen Körper $\mathbb{F}_q$ anzugeben, betrachten wir zunächst die Anzahl von $E(\mathbb{F}_p)$ für $\mathbb{F}_p$ mit p prim. Nach dem Satz von Hasse [Sil94, Kapitel V, Theorem 1.1] gilt für die Anzahl $\#E(\mathbb{F}_p)$ der Punkte der elliptischen Kurve:

$$\#E(\mathbb{F}_p) = p + 1 - t \text{ mit } \mid t \mid \leq 2\sqrt{p}.$$

Betrachten wir einen endlichen Körper $\mathbb{F}_q$ (mit q als Potenz einer Primzahl $p > 3$), so gilt bezüglich der Anzahl der Punkte in $E(\mathbb{F}_q)$ der folgende Satz [CF06, Abschnitt 13.1.8].

Satz 2. *Sei $q = p^l$ eine p-Potenz für eine ganze positive Zahl l. Es existiert genau dann eine elliptische Kurve E über $\mathbb{F}_q$ mit $\#E(\mathbb{F}_q) = q + 1 - t$, falls eine der angegebenen Bedingungen erfüllt ist.*

1. $t \not\equiv 0 \pmod{p}$ *und* $t^2 \leq 4q$.
2. *l ist ungerade und es gilt entweder*
   - $t = 0$ *oder*
   - $p = 2$ *und* $t^2 = 2q$ *oder*
   - $p = 3$ *und* $t^2 = 3q$.
3. *l ist gerade und es gilt entweder*
   - $t^2 = 4q$ *oder*
   - $p \not\equiv 1 \pmod{3}$ *und* $t^2 = q$ *oder*

- $p \not\equiv 1 \pmod 4$ *und* $t = 0$.

Beweis. Siehe [Wat69].

Mit $\#E(\mathbb{F}_q)$ bezeichnen wir die *Ordnung einer elliptischen Kurve* und die Zahl t nennen wir *Spur des Frobenius* der Kurve E. Eine eng mit dieser Zahl verknüpfte Eigenschaft, die eine elliptische Kurve E besitzen kann, ist die *Supersingularität*. Wir nennen eine Kurve *supersingulär*, falls die Charakteristik p von $\mathbb{F}_q$ die Zahl t teilt, das heißt wenn $t \equiv 0 \pmod p$ gilt. Anderenfalls bezeichnen wir eine Kurve als ordinär oder nichtsupersingulär.
Es ist zu beachten, dass Supersingularität nicht in direktem Zusammenhang mit der Singularität einer Kurve steht. Über einem beliebigen Grundkörper ist eine elliptische Kurve stets nichtsingulär, diese Kurve kann zusätzlich supersingulär sein oder nicht.

Weiterführendes auf dem Gebiet elliptischer Kurven, deren Bedeutung in der algebraischen Geometrie und deren Anwendungen ist in [CF06], [Sil86] bzw. [Sil94] nachzulesen.

1.4.2 Arithmetik auf hyperelliptischen Kurven

Ähnlich der Assoziation der abelschen Punktgruppe einer elliptischen Kurve zu der Kurve selbst können wir zu einer hyperelliptischen Kurve ebenso eine Gruppe assoziieren. Im Gegensatz zu elliptischen Kurven ist das Gruppengesetz nicht für die Kurvenpunkte selbst definiert, sondern auf einer Konstruktion von Divisoren. Diese abelsche Gruppe nennen wir die *Jacobische $\mathcal{J}_C$ von C*. Die Jacobische einer Kurve besitzt für jede Körpererweiterung $\mathcal{K}$ von K die Eigenschaft isomorph zur Picardgruppe vom Grad Null zu sein, das heißt es gilt $\mathcal{J}_C(\mathcal{K}) \cong \mathrm{Pic}_C^0(K)$. Anders formuliert bedeutet dies, dass $\mathcal{J}_C(\mathcal{K})$ die Menge der Divisorklassen ist, die einen über $\mathcal{K}$ definierten Divisor enthalten.

Für elliptische Kurven ergibt sich die Isomorphie zwischen der Punktgruppe $E(K)$ und der Grad-Null-Picardgruppe $\mathrm{Pic}_C^0(K)$.
Im Folgenden verwenden wir stets $E(K) \cong \mathrm{Pic}_C^0(K) \cong \mathcal{J}_E(K)$ [Sil86, Seite 295]und schreiben nur noch $E(K)$ bzw. im eindeutigen Kontext E.

Eine der Darstellungsmöglichkeiten der Elemente der Jacobischen von C kann über reduzierte Divisoren formuliert werden [BSSC05]. Zur Erinnerung verweisen wir auf Abschnitt 1.3.

Zur Implementierung der Arithmetik ist diese Darstellung über Divisoren reduzierter Form jedoch nicht geeignet und aus diesem Grund gehen wir zur sogenannten *Mumford-Darstellung* über [CF06].
Eine kompakte Darstellung für jede nichttriviale Divisorklasse über K erhalten wir über ein eindeutiges Paar von Polynomen $u(x)$, $v(x)$ mit $u,\ v \in K[x]$ mit den Eigenschaften

1. u ist normiert,

2. $\deg v < \deg u \leq g$,
3. $u \mid (u^2 + vh - f)$.

Eine Divisorklasse lässt sich der Mumford-Darstellung entsprechend als $\overline{D} = [u, v]$ angeben. Der Algorithmus von Cantor implementiert das Gruppengesetz auf der Jacobischen einer Kurve beliebigen Geschlechts und über einem beliebigen Körper. Die Addition zweier solcher Klassen ergibt, dem Algorithmus von Cantor nach, einen eindeutigen reduzierten Divisor als Klassenrepräsentant.
Da die Addition zweier Divisoren aus Pic_C^0 bzw. $\mathcal{J}_C$ eine sehr technische Angelegenheit ist, verweisen wir für detaillierte Ausführungen und die Angabe des Algorithmus auf [CF06].

Um die Notation in nachfolgenden Abschnitten zu vereinfachen, betrachten wir, den Bezeichnungen von [GHO+07] folgend, zwei Abbildungen auf $\mathcal{J}_C$ für deren Bildmengen sich leicht Gruppengesetze definieren lassen.

Nach Definition 7 nennen wir einen Divisor reduziert, falls dieser eine Summe von Punkten abzüglich eines Vielfachen des Punktes $\mathcal{O}$ ist und wir schreiben einen solchen reduzierten Divisor in der Form $\sum_{i=1}^{l} (P_i) - l(\mathcal{O})$, mit $P_i \in C(\mathbb{F}_{q^k})$, $P_i \neq \mathcal{O}$ und $P_i \neq -P_j$ für $i \neq j$ mit $l \leq g$.
Für eine Divisorklasse $[D]$ bezeichne $\rho([D])$ im Folgenden den eindeutigen reduzierten Divisor einer Divisorklasse. Mit $\epsilon([D])$ bezeichnen wir den effektiven Teil von $\rho([D])$. Somit gilt $\rho([D]) = \epsilon([D]) - \deg(\epsilon([D]))(\mathcal{O})$. Zur Betrachtung der Bildmengen der beiden Abbildungen $\rho : \mathrm{Pic}_C(K) \to \mathrm{Div}_C(K)$ und $\epsilon : \mathrm{Pic}_C(K) \to \mathrm{Div}_C(K)$ als Gruppen, spezifizieren wir das Gruppengesetz $\oplus$ für Divisoren D_1, D_2:

$$\rho([D_1]) \oplus \rho([D_2]) := \rho([D_1] + [D_2])$$

und ebenso für den effektiven Anteil

$$\epsilon([D_1]) \oplus \epsilon([D_2]) := \epsilon([D_1] + [D_2]).$$

Einen Spezialfall dieser Vorgehensweise haben wir innerhalb der Betrachtungen bezüglich der Arithmetik auf der Punktgruppe einer elliptischen Kurve in Abschnitt 1.4.1 bereits kennengelernt.

Für tiefergehende Informationen verweisen wir auf das grundlegend für diese Arbeit verwendete Buch [CF06] bzw. auf die Originalarbeit aus dem Jahr 1987 [Can87] und darauf Aufbauendes. Ein Überblick kann auch in [GHV07b] gewonnen werden.

1.5 Abbildungen auf und zwischen Kurven

In praxisrelevanten Anwendungen von Paarungen werden häufig Eigenschaften von Abbildungen auf Kurven ausgenutzt, um beispielsweise Berechnungen zu beschleunigen oder zu vereinfachen.

Einige Anwendungsgebiete werden wir in dieser Arbeit aufzeigen:

1. Die beschleunigte Berechnung der Skalar-Punkt-Multiplikation auf elliptischen Kurven mit effizient berechenbaren Endomorphismen (zu finden in der Anwendung auf Paarungen Abschnitt 3.2.4).
2. Die Eliminierung von Divisionen innerhalb der Paarungsevaluation unter Verwendung von Verzerrungsabbildungen (zusammen mit weiteren Anmerkungen zu diesem Bereich siehe Abschnitt 3.2.1).
3. Die Verwendung des Frobenius-Endomorphismus für die Ate Paarung (siehe Abschnitt 3.2.3).

Wir werden im Schriftbild häufig nicht unterscheiden, ob eine Abbildung auf einer oder zwischen zwei (verschiedenen) Kurven operiert und verwenden die Notation „auf (einer) Kurve(n)“.

Eine rationale Abbildung ϕ heißt *Morphismus*, falls diese in jedem Punkt P definiert ist, d. h. es gibt Polynomfunktionen ϕ_1, ϕ_2 mit $\phi = \frac{\phi_1}{\phi_2}$ und $\phi_2(P)$ für jeden Punkt P.
Zwischen zwei Kurven C_1 und C_2 über K ist eine rationale Funktion ϕ entweder konstant oder surjektiv [Sil86]. Sprechen wir im Folgenden von Abbildungen zwischen Kurven, dann sei stets ein Morphismus auf Kurven gemeint.

Für nichtkonstante, rationale Abbildungen ϕ können wir die durch Komposition mit ϕ gegebene Injektion von Funktionenkörpern, welche K fix lässt, betrachten

$$\begin{aligned} \phi^* : \overline{K}(C_2) &\to \overline{K}(C_1) \\ f &\mapsto \phi^* f := \phi^*(f) = f \circ \phi. \end{aligned} \tag{1.10}$$

Dieses Zurückziehen von Funktionen liefert uns einen engen Zusammenhang zwischen den rationalen Abbildungen ϕ und den zugehörigen Funktionenkörpern der Kurven auf denen ϕ^* agiert.
Einerseits ist für nichtkonstantes ϕ der Funktionenkörper $\overline{K}(C_1)$ eine endliche Körpererweiterung von $\phi^*\overline{K}(C_2)$. Andererseits existiert für eine Injektion $\iota : \overline{K}(C_2) \to \overline{K}(C_1)$, welche K fix lässt, eine eindeutige nichtkonstante Abbildung $\phi : C_1 \to C_2$ mit $\phi^* = \iota$. Aus diesen Beziehungen heraus können wir die Definition des Grades einer Abbildung ϕ leicht erklären.

Definition 8. Ist ϕ konstant, so definieren wir den *Grad von* ϕ $\deg(\phi)$ als 0. Ansonsten sagen wir ϕ ist *endlich* und definieren den Grad als

$$\deg(\phi) = [K(C_1) : \phi^* K(C_2)].$$

Die Eigenschaften der Seperabilität bzw. der Inseparabilität übertragen sich von der Körpererweiterung auf die Abbildung.

Nachdem wir das Wichtigste zusammengetragen haben, richten wir die Aufmerksamkeit auf eine sehr spezielle Abbildung: dem *Frobenius-Endomorphismus*.

1.5.1 Der Frobenius-Endomorphismus

Sei die Charakteristik des Grundkörpers K eine Primzahl $p > 0$ und q eine Potenz von p. Der q-Potenz Frobenius-Endomorphismus ist dann eine Abbildung, welche wir durch (1.11) beschreiben.

$$\begin{aligned} \pi_q &: C \to C \\ P = (x_P, y_P) &\mapsto \pi_q(P) = \pi_q(x_P, y_P) = (x_P^q, y_P^q) \end{aligned} \tag{1.11}$$

Wir werden drei grundlegende Eigenschaften der Frobenius-Abbildung für einen vollkommenen Körper K charakterisieren. Wobei ein Körper *vollkommen* heißt, falls jede algebraische Körpererweiterung F separabel ist. Da für unsere Zwecke nur endliche Körpern interessant sind und jeder endliche Körper vollkommen ist, werden wir uns nicht weiter mit anderen Eigenschaften auseinandersetzen. Für die durch (1.11) definierte Abbildung π_q gilt:

- π_q ist rein inseparabel
- $\deg(\pi_q) = q$.

Der zughörige Beweis und weitere Aussagen sind in [Sil86, Proposition 2.11] zu finden.

In Abschnitt 1.4.1 haben wir die Ordnung einer elliptischen Kurve definiert. Mit Hilfe dieser Definition werden wir weitere Eigenschaften des Frobenius-Endomorphismus für elliptische Kurven charakterisieren. Für Punkte $P \in E(\overline{\mathbb{F}_q})$ gilt die folgende Äquivalenz:

$$P \in \ker(\pi_q - 1) \Leftrightarrow (\pi_q - 1)P = 0 \Leftrightarrow \pi_q P = P \Leftrightarrow P \in E(\mathbb{F}_q)$$

und wir folgern analog

$$P \in \ker(\pi_q - q) \Leftrightarrow (\pi_q - q)P = 0 \Leftrightarrow \pi_q P = [q]P.$$

Einige dieser charakteristischen Besonderheiten werden wir im Folgenden verwenden. Abschließend wenden wir uns der effizienten Skalarmultiplikation unter Verwendung des Frobenius-Endomorphismus zu.

Frobenius-Entwicklung Die hier vorgestellte Technik gestaltet die Berechnung von $[m]P$ für eine Zahl $m \in \mathbb{Z}$ und einen Kurvenpunkt P durch eine spezielle Entwicklung der Darstellung des Skalars m wesentlich effizienter. Dieser Ansatz wurde von V. Müller im Jahre 1998 [Mül98] für „kleine“ Körper der Charakteristik zwei veröffentlicht. Kurze Zeit später in 1999 wird diese Technik von N. Smart [Sma99] auf „kleine“ Körper ungerader Charakteristik verallgemeinert.
Mit klein meinen wir in diesem Zusammenhang die Tatsache, dass wir Körper $\mathbb{F}_q$ betrachten, für die q eine p-Potenz p^l zu einem kleinen Exponenten l ist.

Nachfolgend fassen wir die Idee und Anwendung der Frobenius-Entwicklung einer ganzen Zahl $m \in \mathbb{Z}$ kurz zusammen. Dabei halten wir uns inhaltlich nah an [Sma99].

Sei also E eine elliptische Kurve der Form (1.3) mit Koeffizienten in $\mathbb{F}_q$, wobei q eine kleine Potenz von p ist. Weiterhin teile p nicht die Spur des Frobenius t. Die Kurve E ist demnach ordinäre (nichtsupersinguläre) Kurven.

Wir betrachten den Ring $\mathbb{Z}[\pi_q]$, dessen Elemente wir darstellen können als $S = Q\pi_q + R$ mit eindeutig bestimmten Zahlen $R \in \{-(q-1)/2, \ldots, (q-1)/2\}$ und $Q \in \mathbb{Z}[\pi_q]$.
Diese Darstellung können wir als Analogon der Division mit Rest innerhalb des Euklidischen Algorithmus auffassen. Führen wir diese Zerlegung mehrfach hintereinander durch, erhalten wir für ein Element $S \in \mathbb{Z}[\pi_q]$ die Schreibweise als Summe von Potenzen des Frobenius-Endomorphismus mit ganzzahligen Koeffizienten.

$$S = \sum_{i=0}^{r} s_i \pi_q^i \quad \text{mit } s_i \in \{-(q-1)/2, \ldots, (q-1)/2\}$$
$$\text{und } r \leq \left\lceil 2 \log_q \left(\sqrt{N_{\mathbb{Z}[\pi_q]/\mathbb{Z}}(s)} \right) + 3 \right\rceil$$

Beweis. Die Existenz und Konstruktion wird in [Mül98] bzw. [Sma99] gezeigt.

Wobei wir die Norm $N_{L/K}(a)$ eines Elementes $a \in L$ einer endlichen Körpererweiterung L von K definieren als die Determinante des K-Vektorraumendomorphismus von L

$$\varphi_a : L \to L,\ x \mapsto ax,\ \text{d. h.} \quad N_{L/K}(a) = \det(\varphi_a) \text{ [Bos06].}$$

Betrachten wir dieses Entwicklungsschema für die Zahl m, so erhalten wir für die Berechnung von $[m]P$ die Vorschrift $[m]P = \sum_{i=0}^{r} s_i \pi_q^i(P)$, welche sich wiederum unter Verwendung des Horner-Schemas effizient berechnen lässt als

$$[m]P = \pi_q(\ldots \pi_q([s_r]\pi_q(P) + [s_{r-1}]P) + \ldots + [s_1]P) + [s_0]P.$$

Diese Berechnungsvorschrift ersetzt die vielen, in der binärbasierten *Double-And-Add* Methode benötigten, teueren arithmetischen Operationen durch deutlich weniger Operationen und einige Potenzierungen innerhalb des endlichen Köpers $\mathbb{F}_q$. Diese Potenzierungen entsprechen den Anwendungen des Frobenius-Endomorphismus.
Um dies zu verdeutlichen, führen wir das folgende Zahlenbeispiel an, welches wir ebenfalls [Sma99] entnommen haben.

Beispiel 2. Sei $\mathcal{E}$ eine elliptische Kurve über $\mathbb{F}_{23}$ mit Spur $t = -1$. Zu berechnen sei $[m]P$ für einen Punkt $P \in \mathcal{E}$ und $m = 10^6$, wie schon in unserem Zahlenbeispiel zur skalaren Multiplikation.
Die Binärdarstellung von m war gegeben durch $(11110100001001000000)_2$ und der klassische Berechnungsweg war

$$[m]P = [2^6](P + [2^3](P + [2^5](P + [2^2](P + [2](P + [2](P + [2]P)))))), \tag{1.12}$$

wobei wir sechs Additionen und 19 Punktverdopplungen benötigen. Im Gegensatz hierzu berechnet sich $[m]P$ unter Anwendung der Frobenius-Entwicklung als

$$[m]P = \pi_q(\ldots(\pi_q(-\pi_q(P) + [2]P) + [7]P) - [3]P) - [9]P) - [5]P) - [4]P - [8]P) + [6]P. \tag{1.13}$$

Werden vorberechnete Werte von $[l]P$ mit l aus $\{1, \ldots, (q-1)/2\}$ verwendet, dann sind neun Additionen und neun Anwendungen des Frobenius zu berechnen. Das ist ein deutlicher Vorsprung der Frobenius-Entwicklung (1.13) gegenüber der üblichen Multiplikation zwischen Skalar und Punkt (1.12).

In diesem Kapitel haben wir uns zu gleichen Teilen der Einführung elliptischer und hyperelliptischer Kurven, deren Funktionenkörpern und Abbildungen als auch der Theorie der Divisoren gewidmet. Wir fahren im nächsten Kapitel mit den Grundlagen über Paarungen fort.

2 Theorie der Paarungen

Die Kryptographie auf elliptischen Kurven besitzt gegenüber den als Standard verwendeten Algorithmen einen großen Vorteil. Die heutzutage verwendeten Algorithmen benötigen für eine akzeptable Sicherheit Mindestschlüssellängen von 1024 Bit, elliptische Kurven auf einem vergleichbare Sicherheitslevel nur ca. 160 Bit [Tak07]. Dieser Hintergrund treibt die Untersuchungen auf diesem Gebiet voran. Immer effizientere Tricks und Kniffe werden gesucht, um elliptische Kurven und Paarungen attraktiv für die Praxis werden zu lassen.
Ob diese Kryptographie auf elliptischen Kurven und die paarungsbasierte Kryptographie eine Alternative zu den Anwendungen der Algorithmen von Rivest, Shamir und Adleman (RSA) oder des *Advanced Encryption Standard* (AES)[1] werden können, bleibt in dieser Arbeit unbeantwortet.

Dieses Kapitel soll einen Überblick über die bisher bekannten Paarungen und deren Berechnung geben. Auf den nächsten Seiten erläutern wir zunächst die Grundlagen über Paarungen, um im Folgenden dann im Speziellen die Entwicklung der Tate Paarung, effiziente Implementierungstechniken und einige wichtige Aspekte der kryptographischen Sicherheit zu betrachten.

2.1 Paarungen

Seien $\mathbb{G}_1$, $\mathbb{G}_2$ endliche abelsche (additive) Gruppen mit Exponent $n \in \mathbb{N}$. Ist weiterhin eine zyklische multiplikative Gruppe $\mathbb{G}_3$ der Ordnung n gegeben, dann ist eine Paarung definiert als eine bilineare und nichtdegenerierte Abbildung $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_3$. Für diese Abbildung gilt:

1. Wohldefiniertheit: $\hat{e}(P, O_{\mathbb{G}_2}) = e(O_{\mathbb{G}_1}, Q) = 1_{\mathbb{G}_3}$
2. Bilinearität: $\hat{e}([j]P, Q) = \hat{e}(P, Q)^j = \hat{e}(P, [j]Q)$ für alle $j \in \mathbb{Z}$, explizit gilt dann auch

$$\hat{e}(-P, Q) = \hat{e}(P, Q)^{-1} = \hat{e}(P, -Q)$$

[1] AES - Seit Oktober 2000 vom National Institute of Standards and Technology (NIST) als Standard eingesetzt

Weitere Eigenschaften sind in [BSSC05] zu finden.

In Anbetracht der praktischen Anwendungen betrachten wir zyklische Untergruppen primer Ordnung r. Den Schwerpunkt der Betrachtungen legen wir dabei auf die Paarungstheorie elliptischer Kurven, geben jedoch in den meisten Fällen auch die Verallgemeinerung auf hyperelliptische Kurven an.

Diese Reihenfolge- und Schwerpunktswahl basiert zum einen auf der ausgereifteren Arithmetik und Implementierung elliptischer Kurven, zum anderen sind die Fragen bezüglich der Berechnungsgeschwindigkeit auf vergleichbaren Sicherheitsleveln für hyperelliptische Kurven des Geschlechts zwei oder höher und der Schnelligkeit der Skalarmultiplikation auf diesen Kurven ungeklärt. Daher beschränken wir uns innerhalb dieser Arbeit darauf die Thematik für elliptische Kurven detailliert zu beleuchten und immer wieder Verbindungen zu hyperelliptischen Kurven höheren Geschlechts aufzuzeigen.

Zunächst gilt unsere Aufmerksamkeit der Einführung von Notationen und grundlegenden Sätzen, die wir ohne Beweis aus [BSSC05] zitieren.

2.2 Die Tate Paarung

Beginnen werden wir die Betrachtung der Tate Paarung bezüglich elliptischer Kurven. Das heißt die Gruppen $\mathbb{G}_1$ und $\mathbb{G}_2$ sind Untergruppen der Gruppe der Kurvenpunkte.

2.2.1 Die Tate Paarung auf der Punktgruppe elliptischer Kurven

Bevor wir die Definion der Tate Paarung angeben, wiederholen wir einige Inhalte der Divisortheorie.
Im Folgenden seien die betrachteten elliptischen Kurven E über $\mathbb{F}_q$ definiert. Die Punktgruppe der Kurve E enthalte stets mindestens einen Punkt der Ordnung r.

Satz 3. *Sei $D = \sum_P n_P(P)$ ein Divisor mit $\deg(D) = 0$ auf E.*
Der Divisor D ist genau dann ein Hauptdivisor, d. h. es existiert eine Funktion f mit $D = (f)$, wenn $\sum_P [n_P]P = O$ auf E gilt.

Für eine Funktion f und einen Divisor $D \in \mathrm{Div}_E^0$ mit $\mathrm{supp}((f)) \cap \mathrm{supp}(D) = O$ haben wir die Auswertung von f an D als $f(D) = \prod_P f(P)^{n_P}$ definiert. Sind f und D über $\mathbb{F}_q$ definiert, so liegt auch $f(D)$ in $\mathbb{F}_q$.

Definition 9. Die Tate Paarung ist definiert als Abbildung

$$\begin{aligned}\langle \cdot, \cdot \rangle : E[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) &\to \mathbb{F}_{q^k}^{\times}/(\mathbb{F}_{q^k}^{\times})^r \\ (P, Q) &\mapsto \langle P, Q \rangle_r = f_P(D_Q).\end{aligned}$$

Das Element Q ist Repräsentant einer Äquivalenzklasse in $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ und wir können den Divisor $D_Q = (Q+R)-(R)$ für einen zufälligen Punkt R aus $E(\mathbb{F}_{q^k})$ auswählen.

Den Wert $f_P(D_Q)$ dieser Paarung konstruieren wir sukzessive mit Hilfe sogenannter *Miller-Funktionen* und bezeichnen diese rationalen Funktionen im Folgenden mit $f_{s,P}$. Der Divisor einer solchen Funktion lässt sich für jede ganze, positive Zahl s in der einfachen Form $(f_{s,P}) = s(P) - ([s]P) - (s-1)(O)$ schreiben.
Für negative Zahlen s wird der Divisor definiert als $(f_{s,P}) = -(f_{-s,P}) - (v_{[s]P})$, wobei $v_{[s]P}$ die vertikale Gerade durch den Punkt $[s]P$ beschreibt.
Somit gilt in diesem Fall $f_{s,P} = \frac{1}{f_{-s,P} v_{[s]P}}$.
Algorithmus 2 liefert die Konstruktion dieser Funktionen, indem bezüglich der Binärdarstellung der Zahl r ein *Double-And-Add*-Algorithmus angewendet wird. Als Ausgabe erhalten wir den Wert der Miller-Funktion $f_{r,P} = f_P$ ausgewertet an dem Divisor D_Q. Diesen Algorithmus bezeichnen wir als den *Miller*-Algorithmus.
Für das Verständnis des Algorithmus notieren wir mit $l_{P,Q}$ die durch P und Q verlaufende Gerade und der Einfachheit der Notation wegen sei v_P die Gerade, welche durch P und $-P$ verläuft. Für alle $a, b \in \mathbb{Z}$ definieren wir

$$f_{a+b,P}(Q) = f_{a,P}(Q) f_{b,P}(Q) \cdot l_{aP,bP}(Q) / v_{(a+b)P,-(a+b)P}(Q)$$

und betrachten Algorithmus 2.

Algorithmus 2 : *Miller*-Algorithmus

Input : Punkt $P \in E[r]$ und $Q \in E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ und $(r_l, \ldots, r_0)_2$ sei die Binärdarstellung von r

Output : Die Tate Paarung $e(P, Q)$ auf einer elliptischen Kurve E

Wähle einen geeigneten Punkt $R \in \mathbb{F}_{q^k}$;
$l \leftarrow \lfloor \log_2(r) \rfloor - 1$, $f \leftarrow 1$;
$Q' \leftarrow Q + R$ und $V \leftarrow P$;
for $i = l$ **to** 0 **do**
    $f \leftarrow f^2 \frac{l_{V,V}(Q') v_{2V}(R)}{v_{2V}(Q') l_{V,V}(R)}$;
    $V \leftarrow 2V$;
    if $r_i = 1$ **then**
        $f \leftarrow f^2 \frac{l_{V,P}(Q') v_{V+P}(R)}{v_{V+P}(Q') l_{V,P}(R)}$;
        $V \leftarrow V + P$;
    end
    return $f^{\frac{(q^k-1)}{r}}$;
end

Werden Paarungen unter kryptographischen Aspekten betrachtet, so darf nicht der wesentliche Gesichtspunkt der Sicherheit vernachlässigt werden. Diesem Themenbereich

wenden wir uns in Abschnitt 4.2.1 ausführlicher zu. In enger Verbindung zu diesem Gebiet steht der sogenannte Tate Einbettungsgrad.

Definition 10. Jene Zahl k, welche als kleinster ganzzahliger Exponent von q definiert ist, so dass die Ordnung r den Wert $(q^k - 1)$ teilt, wird als der *Tate Einbettungsgrad* k_t bezüglich r bezeichnet, das heißt $k_t := \min_{l \in \mathbb{N}} \left\{ r \mid (q^l - 1) \right\}$.

Bemerkung 1. Nach Definition 9 liefert die Tate Paarung auf elliptischen Kurven als Wertemenge Klassen modulo r-ter Potenzen. Um eindeutige Elemente der Ordnung r in $\mathbb{F}_{q^k}$ zu erhalten, potenzieren wir den Wert der Paarung mit $\frac{(q^k-1)}{r}$ und bezeichnen dies als die *reduzierte* Tate Paarung.

$$e(\cdot,\cdot) : E[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mu_r$$
$$(P, Q) \mapsto e(P, Q) := \langle P, Q \rangle_r^{\frac{(q^k-1)}{r}} = f_P(D_Q)^{\frac{(q^k-1)}{r}} \tag{2.1}$$

Somit erhalten wir eine primitive r-te Einheitswurzel in $\mu_r = \{u \in \mathbb{F}_{q^k} \mid u^r = 1\}$, wobei $k := k_t$ der in Definition 10 eingeführte Tate Einbettungsgrad bezüglich r ist.
Häufig ist der Einbettungsgrad k größer als eins. Ist dies gegeben so kann, statt mit dem Divisor D_Q, auch mit dem divisordefinierenden Punkt Q gearbeitet werden [BKLS02]. Wir erhalten somit die einfache Definition $e(P, Q) = f_{r,P}(Q)^{\frac{(q^k-1)}{r}}$. Zudem können wir die Zahl r durch eine ganze Zahl N ersetzen, für die $r \mid N \mid (q^k - 1)$ gilt und schreiben für die reduzierte Tate Paarung $e(P, Q) = f_{N,P}(Q)^{\frac{(q^k-1)}{N}}$ [GHS02].

Entsprechend der zeitlichen Erscheinungsreihenfolge haben wir einführend die Tate Paarung auf elliptischen Kurven betrachtet und gehen nun auf die Tate Paarung auf hyperelliptischen Kurven bzw. deren auf Jacobischen ein.

2.2.2 Die Tate Paarung auf der Jacobischen hyperelliptischer Kurven

Sei C eine hyperlliptische Kurve des Geschlechts g über einem endlichen Körper $\mathbb{F}_q$ mit einem Weierstraß-Punkt gegeben.

Definition 11. (Notation nach [GHV07b]) Wir bezeichnen die nichtdegenerierte, bilineare Abbildung

$$T_r : \mathrm{Pic}_C^0(\mathbb{F}_{q^k})[r] \times \mathrm{Pic}_C^0(\mathbb{F}_{q^k})/r\mathrm{Pic}_C^0(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^\times/(\mathbb{F}_{q^k}^\times)^r \tag{2.2}$$
$$(\overline{D_1}, \overline{D_2}) \mapsto T_r(\overline{D_1}, \overline{D_2}) \tag{2.3}$$

als *Tate-Lichtenbaum Paarung*.
Als Repräsentanten der Divisorklassen $\overline{D_1} \in \mathrm{Pic}_C^0(\mathbb{F}_{q^k})[r]$ bzw. $\overline{D_2} \in \mathrm{Pic}_C^0(\mathbb{F}_{q^k})$ wählen wir D_1 für die Klasse $\overline{D_1}$ und den Divisor $D_2 = \sum_{P \in C(\mathbb{F}_{q^k})} n_P(P)$ für die Klasse $\overline{D_2}$, so

dass die Träger dieser zwei Divisoren disjunkt voneinander sind. Erfüllen zwei Divisoren $\text{supp}(D_1) \cap \text{supp}(D_2) = \{O\}$, so nennen wir diese *koprim*.
Da $\overline{D_1}$ eine Divisorklasse der Ordnung r ist, existiert eine $\mathbb{F}_{q^k}$-rationale Funktion f_{r,D_1} deren Divisor sich schreiben lässt als $(f_{r,D_1}) = rD_1$. Die Auswertung $T_r(\overline{D_1}, \overline{D_2})$ ist definiert als

$$T_r(\overline{D_1}, \overline{D_2}) \equiv f_{r,D_1}(D_2) = \prod_{P \in C(\mathbb{F}_{q^k})} f_{r,D_1}(P)^{n_P}. \tag{2.4}$$

Einen Nachweis der Wohldefiniertheit, der Nichtdegeneriertheit und der Bilinearität ist in [Rue99] zu finden.

Den Ausführungen in Abschnitt 1.4.2 nach ist es uns möglich $\mathcal{J}_C(\mathbb{F}_{q^k})$ und $\text{Pic}^0_C(\mathbb{F}_{q^k})$ miteinander zu identifizieren. Die Elemente in $\mathcal{J}_C(\mathbb{F}_{q^k})$ oder alternativ auch die Divisorklassen $\overline{D}$ in $\text{Pic}^0_C(\mathbb{F}_{q^k})$ können wir mittels Divisoren der Form $D - g(O)$ mit einem effektiven Divisor D vom Grad g darstellen. Demnach erhalten wir die Tate-Lichtenbaum Paarung auf der Jacobischen der Kurve C als Abbildung

$$T_r : \mathcal{J}_C(\mathbb{F}_{q^k})[r] \times \mathcal{J}_C(\mathbb{F}_{q^k})/r\mathcal{J}_C(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}^\times_{q^k}/(\mathbb{F}^\times_{q^k})^r. \tag{2.5}$$

Je nach Anwendungsgebiet in der Kryptographie sind unterschiedliche Anforderungen an den Definitionsbereich der Paarung zu stellen; diese können zu einer Vereinfachung und unter Umständen zu einer effizienteren Berechnung der Paarung führen.
In [CF06, Seite 390] sind einige explizite Herleitungen mit den entsprechenden Annahmen für solche Vereinfachungen erklärt.

Weiterführende Informationen finden sich in [CF06, Kapitel 6]. Für einen sehr guten Überblick bezüglich der Paarungen auf hyperelliptischen Kurven empfehlen wir die Arbeit von Galbraith, Heß und Vercauteren [GHV07b]

Implementierung der Tate-Lichtenbaum Paarung

An dieser Stelle skizzieren wir die Implementierung dieser Paarung. Konkrete Algorithmen oder detaillierte Beschreibungen geben wir nicht an. Für Ausführlicheres verweisen wir auf [CF06, Kapitel 16].

In vielen kryptographischen Protokollen ist die Eindeutigkeit der Repräsentanten notwendig, um eine Durchführung zu ermöglichen. Wollen Alice und Bob miteinander kommunizieren, so müssen sie sich auf einen gemeinsamen Schlüssel einigen. Um diesen zu bestimmen, führen beide unterschiedliche Berechnungen durch, sollen jedoch denselben Wert als Ergebnis erhalten. Daher werden häufig zwei Vereinbarungen getroffen.

Erstere ist die Annahme, dass die Jacobische $\mathcal{J}_C(\mathbb{F}_{q^k})$ keine Elemente der Ordnung r^2 enthält. Dies ermöglicht die Identifikation von $\mathcal{J}_C(\mathbb{F}_{q^k})[r]$ mit $\mathcal{J}_C(\mathbb{F}_{q^k})/r\mathcal{J}_C(\mathbb{F}_{q^k})$ über

die Abbildung $\overline{D_2} \mapsto \overline{D_2} + r\mathcal{J}_C(\mathbb{F}_{q^k})$.
Die zweite Vereinbarung ist die Potenzierung des Resultats mit $(q^k - 1)/r$, um in die Untergruppe μ_r abzubilden und damit eindeutige r-te Einheitswurzeln zu erhalten.
Die *reduzierte Tate Paarung* ist dann gegeben als

$$(\overline{D_1}, \overline{D_2}) \mapsto t_r(\overline{D_1}, \overline{D_2}) := T_r(\overline{D_1}, \overline{D_2})^{\frac{(q^k-1)}{r}}$$

Für die Divisorklassen $\overline{D_1}$ und $\overline{D_2}$ ist folgendes gegeben:

1. $\overline{D_1}$ wird repräsentiert über einen $\mathbb{F}_{q^k}$-rationalen Divisor D_1 vom Grad 0.
2. Da $\overline{D_1}$ eine Divisorklasse des Grades r ist, existiert eine Funktion f_{r,D_1} auf C, so dass $(f_{r,D_1}) = r(D_1)$ gilt.
3. $\overline{D_2}$ wird repräsentiert über einen Divisor D_2 vom Grad 0, dessen Träger disjunkt von D_1 sei.
4. Demnach berechnen wir $T_r(\overline{D_1}, \overline{D_2} + r\mathcal{J}_C(\mathbb{F}_{q^k})) = f_{r,D_1}(D_2)$.

Zur Berechnung der Tate-Lichtenbaum Paarung auf Kurven beliebigen Geschlechts g müssen wir zunächst die Funktion f_{r,D_1} konstruieren und anschliessend an D_2 auswerten. Der grundlegende Schritt ist das Lösen der folgenden Aufgabe:

Finde zu gegebenen, effektiven Divisoren A, A' des Grades g, einen effektiven Divisor B desselben Grades und eine Funktion G auf der Kurve C, so dass $A + A' - B - gO = (G)$ erfüllt wird.

Basierend auf dieser Aufgabe ist eine Verallgemeinerung des *Miller*-Algorithmus, welchen wir schon in Abschnitt 2.2.1 diskutiert haben, zur Anwendung auf hyperelliptische Kurven möglich. Hierzu erfolgt die Konstruktion der Funktion f_{r,D_1} über einen *Double-And-Add*-Algorithmus mit Zwischenschritten der Form

$$f_{a+b,D} = f_{a,D} \cdot f_{b,D} \cdot g_{aD,bD},$$

wie wir sie schon für die Tate Paarung auf elliptischen Kurven gesehen haben. Die Implementierung der verwendeten Divisoren erfolgt über die in Abschnitt 1.4.2 bereits eingeführte Mumford-Darstellung als reduzierte Divisoren.
Die Funktionen $f_{n,D}$ haben Divisoren der Form $(f_{n,D}) = nD - \rho(n\overline{D})$, wobei $\rho(n\overline{D})$ den zu nD äquivalenten, eindeutigen, reduzierten Divisor beschreibt. (Vgl. Abschnitt 1.4.2)
Analog geben wir für die Funktion $g_{aD,bD}$ den Divisor als $(g_{aD,bD}) = D_a + D_b - \rho(\overline{D_a} + \overline{D_b})$ an. Den Algorithmus im Detail und weitere Ausführung finden sich in [GHV07b].

Obwohl das Thema dieser Arbeit die effiziente Berechnung der Tate Paarung ist, nehmen wir uns an dieser Stelle die Zeit eine kurze Unterbrechung einzufügen und die in engem Zusammenhang stehende Weil Paarung zu betrachten. Den Fall der hyperelliptischen Kurven betrachten wir dabei nicht. Dieser ist in [CF06, §16.1] zu finden.

2.3 Die Weil Paarung

Diese Paarung ist die zeitlich gesehen ältere der beiden Paarungen Tate und Weil. Die erstmalige Anwendung der Weil Paarung war innerhalb des von Menenzes, Okamoto und Vanstone entwickelten Verfahrens zur Reduktion des diskreten Logarithmus Problem (DLP) für eine ellitpische Kurve auf das DLP in $\mathbb{F}_{q^l}$ für ein $l \geq 1$. Dieses Verfahren ist auch bekannt als der *MOV*-Algorithmus [MOV91].
In Abschnitt 4.1.1 gehen wir auf das DLP ein und erläutern konkret die Fragestellung und Schwierigkeit.

Die Weil Paarung auf der Punktgruppe elliptischer Kurven Ähnlich zu der Tate Paarung verwenden wir für die Weil Paarung die Torsionsgruppe $E[r]$ auf der elliptischen Kurve E. Der Unterschied ist, dass zur Weil Paarung beide Argumente aus $E[r]$ gewählt und über die Grad-Null Divisoren $D_P \sim (P)-(O)$ und $D_Q \sim (Q)-(O)$ dargestellt werden. Nach Satz 3 bilden $r(P) - r(O)$, ebenso wie $r(Q) - r(O)$ für die Punkte P und Q Hauptdivisoren. Für diese Divisoren finden wir daher rationale Funktionen f_P und f_Q mit Divisor $(f_P) = rD_P$ bzw. $(f_Q) = rD_Q$. Unter der Annahme, dass die Träger $\mathrm{supp}(D_P)$ und $\mathrm{supp}(D_Q)$ voneinander disjunkt sind, erhalten wir die Weil Paarung als

$$w_r(\cdot,\cdot) : E[r] \times E[r] \to \mu_r$$
$$(P, Q) \mapsto w_r(P, Q) = \frac{f_P(D_Q)}{f_Q(D_P)}.$$

Diese Paarung besitzt, zusätzlich zu Bilinearität und Nichtdegeneriertheit, die folgenden Eigenschaften:

- $w_r(P, P) = 1$ und damit $w_r(P, Q) = w_r(Q, P)^{-1}$ (*Alternierend*)
- Ist $P \in E[nr]$ und $Q \in E[r]$, dann gilt $w_{nr}(P, Q) = w_r([n]P, Q)$. (*Kompatibilität*)

Die Weil Paarung bildet, im Gegensatz zur Tate Paarung, direkt in die Menge der r-ten Einheitswurzeln μ_r ab. Analog zum Tate Einbettungsgrad definieren wir den sogenannten *Weil Einbettungsgrad*. Dieser ist die kleinste Zahl k_w, so dass $E[r] \subseteq E(\mathbb{F}_{q^{k_w}})$ gilt. Ein weiterer Effekt, der sich aus der Definition der Weil Paarung ergibt, ist das folgende Korollar, welches wir ohne Angabe des Beweises aus [BSSC05] zitieren.

Korollar 1. *Sei E eine elliptische Kurve über einem Körper K und r eine Primzahl. Seien P und Q in $E[r]$ mit $P \neq O$. Dann liegt Q genau dann in der von P erzeugten Untergruppe, wenn $w_r(P, Q) = 1$.*

Somit kann die Unabhängigkeit bzw. die Abhängigkeit zweier Punkte voneinander durch die Auswertung der Weil Paarung leicht getestet werden. Hierbei nennen wir zwei Punkte P_1, P_2 einer abelschen Gruppe *unabhängig*, falls $P_1 \notin \langle P_2 \rangle$ und $P_2 \notin \langle P_1 \rangle$ gilt.

Eine spezielle Form der Weil Paarung auf elliptischen Kurven, die sogenannte *r-adische Weil Paarung*, findet sich in [Sil86]. Die Weil Paarung kann analog zum elliptischen Fall auf der Jacobischen einer hyperelliptischen Kurve C definiert werden. Eine solche Definition ist in [CF06] zu finden.

Diese zwei Paarungen, Tate und Weil Paarung, sind die bekanntesten ihrer Art, wobei beide sowohl in konstruktiver als auch in destruktiver Weise genutzt werden können. In destruktiver Weise trat die Weil Paarung 1993 zur Reduktion des diskreten Logarithmus Problems zum ersten Mal in Erscheinung. Eine Verwendung im positiven Sinne als Verschlüsselungsystem stellen Boneh und Franklin im Jahre 2001 bzw. eine Erweiterung in 2003 [BF03] vor und setzen eine Reihe von Forschungsarbeiten in Gang. Ein Überblick über existierende Kryptosysteme ist in [DBS04] zu finden.

Wir wollen im Folgenden auf einige Unterschiede und Gemeinsamkeiten dieser beiden Paarungen eingehen. Dabei sehen wir, dass für die Tate Paarung, im Gegensatz zur Weil Paarung, über einem relativ kleinen endlichen Körper gearbeitet werden kann. Die Größe dieses endlichen Körpers hängt von dem Einbettungsgrad ab.

Ein offensichtlicher Unterschied liegt in der Anzahl der Berechnungen. Nach Definition der Weil Paarung sind zwei Auswertungen von Miller-Funktionen nötig, eine für $f_P(D_Q)$ und eine zweite für $f_Q(D_P)$, wogegen für die Tate Paarung lediglich $f_P(D_Q)$ ausgewertet wird. Diese Differenz kann jedoch, durch eine geschickte Wahl der Gruppen sowie eine sehr effiziente Implementierung, auf ein Minimum reduziert werden.

Als weiteren Aspekt betrachten wir die Gruppen aus denen die Punkte P und Q stammen. Zur Weil Paarung müssen zwei voneinander unabhängige r-Torsionspunkte gefunden werden, da ansonsten das Resultat für einen Punkt Q, welcher in der von P erzeugten Untergruppe liegt, trivial ist. Zur Konstruktion eines geeigneten Punktes Q wird häufig ein zufälliges Element aus $E(\mathbb{F}_{q^k})$ gewählt und mit $\#E(\mathbb{F}_{q^k})/r$ multipliziert, was der finalen Potenzierung der Tate Paarung entspricht.

Analog zum eben angegebenen, offensichtlichen Unterschied, sind wir auch in der Lage eine dementsprechende Gemeinsamkeit aufzuzeigen. Betrachten wir die Definition der Weil Paarung in der Formulierung des elliptischen Falles, so ist der Wert dargestellt als Quotient zweier Miller-Funktionen f_P, f_Q. Diese können wir bis auf r-te Potenzen jeweils mit einer Tate Paarung identifizieren und erhalten als Relation zwischen Weil und Tate Paarung

$$w_r(P, Q) = \frac{e(P, Q)}{e(Q, P)}.$$

Um weitere Gemeinsamkeiten aufzugreifen, betrachten wir die Einbettungsgrade der Tate und Weil Paarungen und erläutern in Abschnitt 4.2 die Besonderheiten im Zusammenhang zur kryptographischen Sicherheit.

Zunächst nur so viel, dass sich die Sicherheit der paarungsbasierten Kryptographie sich durch ein Tupel (kF, G) beschreiben lässt. Hierbei bezeichne F die Bitlänge von q, dies entspricht in etwa $\log_2(q)$ und G analog die Bitlänge von r, also ungefähr $\log_2(r)$.

Die Werte F und G sind bekannt, woher jedoch erhält man die Zahl k?

Diese Frage wollen wir in dem folgenden Abschnitt beantworten. Ebenso erläutern wir in welchen Relationen diese Zahl k bezüglich der Tate bzw. der Weil Paarung steht.

2.4 Der Einbettungsgrad

Sowohl die Definition der Tate als auch die der Weil Paarung verwenden eine Körpererweiterung des Grundkörpers $\mathbb{F}_q$, so dass wir in beiden Fällen den jeweiligen Einbettungsgrad k_t bzw. k_w definiert haben.
In diesem Abschnitt beleuchten wir den Fall der elliptischen Kurven eingehender und erklären den Zusammenhang der verschiedenen Einbettungsgrade.

Der Einbettungsgrad der Tate Paarung ist definiert als $k_t = \min_{l\in\mathbb{N}} \left\{r \mid (q^l - 1)\right\}$ und für die Weil Paarung gilt $k_w = \min_{l\in\mathbb{N}} \left\{E[r] \subseteq E(\mathbb{F}_{q^l})\right\}$.
Wollen wir die überleitend gestellte Frage nach der Herkunft der Zahl k beantworten, so müssen wir uns für die Antwort tiefergehend mit dem Einbettungsgrad beschäftigen, da dieser den Körper, über dem wir die Punktgruppe der elliptischen Kurve betrachten, bestimmt. Oft wird der Einbettungsgrad in der englischen Literatur (bspw. [Sco05] oder [BLS01]) daher als „Securitymultiplier“ bezeichnet, was so viel wie die Sicherheit vervielfachen meint.

Um letztendlich das Verhältnis der unterschiedlichen Einbettungsgrade beschreiben zu können, untersuchen wir (gemeinsame) untere Schranken an die Zahlen k_t und k_w.

2.4.1 Eine gemeinsame untere Schranke der Einbettungsgrade

Eine untere Schranke an die beiden Einbettungsgrade k_t und k_w ist gegeben durch eine Zahl k, welche für die Bedingungen

$$\mu_r \subseteq \mathbb{F}_{q^k}^{\times} \text{ und } \mu_r \not\subseteq \mathbb{F}_{q^l}^{\times} \text{ für } l < k$$

minimal ist. Hierzu betrachten wir zunächst das [BSSC05] entnommene Lemma ohne weitere Angaben des Beweises.

Lemma 1. *Sei $r > 0$. Die Menge der r-ten Einheitswurzeln ist genau dann vollständig in $\mathbb{F}_{q^k}^{\times}$ enthalten, wenn r ein Teiler von $(q^k - 1)$ ist.*

Demnach gilt für den Wert der unteren Schranke k: $r \mid (q^k - 1)$ und $r \nmid (q^l - 1)$ für $0 < l < k$.

Notwendigerweise erhalten wir also $k_t \geq k$ und $k_w \geq k$. Es stellt sich die Frage, wann tritt der Fall $k_t = k_w$ auf bzw. nur $k_t = k$ (oder $k_w = k$)? Dies betrachten wir zunächst getrennt für die jeweilige Paarung, um anschließend einen Zusammenhang herzustellen.

Tate Paarung Der Input der Tate Paarungs ist ein r-Torsionspunkt und ein Punkt der Quotientengruppe $E(\mathbb{F}_{q^{k_t}})/rE(\mathbb{F}_{q^{k_t}})$. Für $k_t \geq 1$ existiert immer sowohl ein solcher Punkt in $E[r]$ als auch ein nichttrivialer Repräsentant der Quotientengruppe. Die Bedingung an die untere Schranke der Tate Paarung ist demzufolge auch ein hinreichendes Kriterium für diese und es gilt stets der Optimalwert $k_t = k$.

Weil Paarung Um die Nichttrivialität der Weil Paarung zu garantieren, sind zwei voneinander linear unabhängige r-Torsionspunkte zur Eingabe notwendig.
Sind r und q relativ prim zueinander, gilt also $\gcd(r, q) = 1$, so ist $E[r] \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ (siehe [Sil86]). Demzufolge wird $E[r]$ von zwei linear unabhängigen Punkten erzeugt und die gesamte r-Torsionsgruppe muss notwendig auf der Kurve über $\mathbb{F}_{q^{k_w}}$ liegen. Damit ist die Forderung $E[r] \subseteq E(\mathbb{F}_{q^{k_w}})$ nicht hinreichend, sondern nur notwendig.

Den Zusammenhang der unteren Schranke zwischen Tate und Weil Einbettungsgrad stellt uns ein fundamentales Resultat von Balasubramanian und Koblitz in [BK98] her. Teilt r die Anzahl der Punkte auf E über $\mathbb{F}_q$ und gilt $r \nmid (q-1)$, was $k > 1$ impliziert, so gilt folgende Äquivalenz.

$$E[r] \subseteq E(\mathbb{F}_{q^k}) \;\Leftrightarrow\; r \mid (q^k - 1)$$

Mit anderen Worten bedeutet dies, dass falls r kein Teiler von $(q-1)$ ist, also explizit der Einbettungsgrad k größer als eins ist, so erreichen wir stets den Optimalwert $k_w = k$.

Für den in der Praxis häufig auftretenden Fall $k > 1$ haben demnach Tate und Weil Paarung denselben Einbettungsgrad $k_t = k_w = k$.
Der Fall $k = 1$ wird beispielsweise in [Maa04] ausführlich behandelt.

Paarungsfreundliche Kurven Wir thematisieren innerhalb dieser Arbeit die effiziente Berechnung der Tate Paarung und Variationen dieser Paarung, welche wir im folgenden Kapitel 3 ausführlich diskutieren. Im Rahmen kryptographischer Protokolle sprechen wir stets von *paarungsfreundlichen Kurven*. Damit meinen wir Kurven, für die wir einen „geeignet großen“ Einbettungsgrad k und eine große prime Untergruppenordnung r erreichen können.
Mit einem geeignet großen Einbettungsgrad beschreiben wir einerseits die Forderung nach einem großen Einbettungsgrad (zur Gewährleistung der Sicherheit in dem Körper $\mathbb{F}_{q^k}$) und anderseits die unerlässliche Vorgabe einer effizienten Arithmetik in $\mathbb{F}_{q^k}$.
Ein breit gefächerter Überblick über paarungsfreundliche Kurven ist [FST06b] zu finden.

3 Effiziente Implementierung und Abwandlungen der Tate Paarung

Dieses Kapitel behandelt im ersten Teil verschiedene Techniken zur effizienten Gestaltung der Implementierung der klassischen Tate Paarung, wie wir sie in Abschnitt 2.2 kennengelernt haben. Im zweiten Teil diskutieren wir Abwandlungen der Tate Paarung und gehen auf die systematische Konstruktion neuer Paarungen ein.

Im Folgenden betrachten wir Paarungen über Körpern $\mathbb{F}_q$ bzw. $\mathbb{F}_{q^k}$. Die Punktordnung r sei stets prim.

3.1 Effiziente Implementierung

Sei E im Folgenden stets eine elliptische Kurve über $\mathbb{F}_q$ mit Einbettungsgrad $k > 1$, so dass $r \mid (q^k - 1)$. Wir wollen die reduzierte Tate Paarung $e(P, Q) = \langle P, Q \rangle_r^{\frac{(q^k-1)}{r}}$ für P in $E[r]$ und Q in $E(\mathbb{F}_{q^k})$ berechnen.
Für alle folgenden Berechnungen ist anzumerken, dass der Körper $\mathbb{F}_{q^k}$ wesentlich größer ist als der Grundkörper $\mathbb{F}_q$. Daher empfiehlt es sich, so oft wie möglich die arithmetischen Operationen über dem kleineren Körper auszuführen. Die zur Berechnung effizienteste Darstellung von $\mathbb{F}_{q^k}$ erhalten wir durch die Interpretation von $\mathbb{F}_{q^k}$ als Erweiterungskörper von $\mathbb{F}_q$ mit einer geeigneten Basis [CF06, §11.3].

Es gibt mittlerweile sehr viele Ansätze die Berechnung der klassischen Tate Paarung effizienter zu gestalten und somit zu beschleunigen. Wir wollen an dieser Stelle die wichtigsten Ideen herausarbeiten und verweisen für ein detaillierteres Studium dieser Techniken auf die Basisliteratur dieser Arbeit [CF06, Kapitel 16]. Weitere sehr interessante Arbeiten in diesem Kontext sind [GHS02], [BKLS02] und [BSSC05]. Aus letzterer Quellenangabe sind die folgenden Verbesserungen entnommen.

1. Wo immer möglich sollten Berechnungen in einer kleinen Untergruppe ($r \approx 2^{160}$) von $E(\mathbb{F}_q)$ durchgeführt werden.
   Vorteilhaft ist auch ein kleines Hamminggewicht der Gruppenordnung, das heißt die Summe $\sum b_i$ über die Koeffizienten der Binärdarstellung $(b_l, \ldots, b_0)_2$ von r soll klein sein, um möglichst wenig Additionsschritte im Miller-Algorithmus durchzuführen.

2. Das Arbeiten über dem kleineren Körper $\mathbb{F}_q$ meint im Besonderen, dass die Funktion f mit Divisor $(f) = r(P) - r(O)$ über $\mathbb{F}_q$ definiert ist und somit auch die Geraden $l_{P,Q}$ und v_P innerhalb des Miller-Algorithmus.

3. Arithmetik für $\mathbb{F}_q$, $\mathbb{F}_{q^k}$ so effizient wie möglich implementieren [CF06, §11].

4. Divisionen sollten in $\mathbb{F}_{q^k}$ soweit wie möglich vermieden werden. Beispielsweise kann das Aufspalten der Funktion f in eine Zählerfunktion f_1 und eine Nennerfunktion f_2 genutzt werden. Zum Ende des Algorithmus wird lediglich noch eine Division f_1/f_2 durchgeführt.

5. Die finale Potenzierung zu Abschluss des Algorithmus sollte effizient gestaltet werden. Für Exponenten einer speziellen Form kann unter Umständen die Linearität der q-Potenz Frobenius-Abbildung verwendet werden.
   In manchen Anwendungen ist es möglich mehrere Potenzierungen gleichzeitig auszuführen.

6. Für einen Einbettungsgrad größer eins und primer Punktordnung r gilt für jedes Element x aus $\mathbb{F}_q^\times$ die Relation $x^{(q^k-1)/r} = 1$. Somit kann jeder innerhalb des Miller-Algorithmus auftretende und in einem Element aus $\mathbb{F}_{q^k}$ resultierende Term vernachlässigt werden. Beispielsweise sind in der Verwendung für den Miller-Algorithmus 2 die Geraden $l_{P,Q}$, v_P und der Punkt R über $\mathbb{F}_q$ definiert, dann sind die Werte $l_{P,Q}(R)$ und $v_P(R)$ trivial. Unter diesen Voraussetzungen kann in Zeile 1 $Q' = Q$ gesetzt werden und der Punkt R wird nicht weiter benötigt.

7. Eine weitere Möglichkeit Divisionen zu vermeiden, ist die Verwendung geeigneter nichtrationaler Endomorphismen. Über diese Technik können alle Nenner, die im Laufe des Miller-Algorithmus von Nöten sind, eliminiert werden [BKLS02].

Diese sieben Ansätze betreffen direkt die Implementierung der Paarung. Nehmen wir jedoch an, dass der Punkt P mehrfach verwendet werden kann bzw. mehrfach verwendet werden soll, so ist es möglich Vorberechnungen anzustellen und diese zur Wiederverwendung abzuspeichern. Allerdings ist die Zahl der benötigten Vorberechnungen recht hoch und es ist genau abzuwägen, ob dies in Relation zum Nutzen akzeptabel erscheint.

Nachdem wir einige Ansätze der effizienten Implementierung der klassischen Tate Paarung betrachtet haben, gehen wir auf spezielle Paarungen ein, welche der Tate Paarung sehr ähnlich und zudem äußerst effizient sind.

3.2 Abwandlungen der Tate Paarung

Der Abschnitt 3.1 zeigt in welchen Bereichen die Implementierung der Tate Paarung verbesserungsfähig ist. Dies kann einerseits durch die Wahl der Eingabeparameter, beispielsweise durch eine spezielle Wahl der betrachteten Kurve oder der Zahl q geschehen.

Andererseits kann dies auch auf Programmierebene durch effiziente Techniken erreicht werden.

Wir wollen an dieser Stelle fortfahren und auf effiziente Abwandlungen, der bis hierhin diskutierten Tate Paarung, betrachten. Dabei ist die Zielsetzung dieser Betrachtungen die Berechnungsdauer, in Abhängigkeit der Eingabeparameter, für die Auswertung einer Paarung so gering wie möglich zu halten. Konkret bedeutet dies den Grad der auszuwertenden Miller-Funktion $f_{s,P}$ klein zu halten.

Innerhalb dieser Diskussion greifen wir die Verwendung effizient berechenbarer Endomorphismen, die η Paarung und die Ate Paarung auf.

3.2.1 Paarungen unter Verwendung spezieller Endomorphismen

In einigen Paarungsanwendungen sind die Gruppen $\mathbb{G}_1, \mathbb{G}_2$ identische Untergruppen von $E[r]$. Betrachten wir für diese Anwendungen die Weil Paarung, so ist festzustellen, dass diese auf $\mathbb{G}_1 \times \mathbb{G}_1$ nach Konstruktion stets trivial ist. Um, sowohl für die Tate als auch die Weil Paarung, trotzdem kryptographische Protokolle betrachten zu können, gehen wir auf diesen Sachverhalt näher ein.

Selbst Paarungen Wie einleitend erwähnt ist eine der Eigenschaften der Weil Paarung, dass für jeden mit sich selbst gepaarten Punkt P diese Paarung in der trivialen Einheitswurzel resultiert. (Vgl. hierzu Abschnitt 2.3)
Daher beschränken wir uns zur Betrachtung der Selbst Paarung auf die Tate Paarung und müssen zunächst untersuchen, wann diese trivial ist.

Einerseits ist die Verschiedenheit der beiden zugrundeliegenden Gruppen $E(\mathbb{F}_{q^k})[r]$ und $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ zu betrachten. Ist der Schnitt dieser beiden Gruppen nicht leer[1], so gilt für diese im Schnitt enthaltenen Punkte $e(P,P) = 1$. Andererseits gilt für einen Punkt $P \in E(\mathbb{F}_q)$ primer Ordnung und $k > 1$ ebenfalls stets $e(P,P) = 1$.
Diesen Zusammenhang halten wir in dem folgenden Lemma [BSSC05] ohne Angabe des Beweises fest.

Lemma 2. *Sei E eine elliptische Kurve über $\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$ ein Punkt mit primer Ordnung r. Sei k der Einbettungsgrad mit $r \mid (q^k - 1)$. Dann ist $e(P,P) = 1$, falls $k > 1$ oder $P \in rE(\mathbb{F}_q)$.*

Der Vollständigkeit halber verweisen wir für den in kryptographischen Anwendungen selten auftretenden Fall $k = 1$ auf [BSSC05]. Stattdessen widmen wir uns den Verzerrungsabbildungen, welche sowohl für die Tate als auch für die Weil Paarung anwendbar sind. Damit weiten wir die Technik der Selbst Paarung aus, um diese praktikabler zu gestalten.

[1] wobei wir mit leer meinen, dass der Schnitt $E(\mathbb{F}_{q^k})[r] \cap rE(\mathbb{F}_{q^k})$ nur den Punkt im Unendlichen $\mathcal{O}$ enthält

Verzerrungsabbildungen In der kryptographischen Praxis sind die gegebenen Voraussetzungen im Allgemeinen jene, für welche das Lemma 2 einen trivialen Wert liefert, das heißt es gilt $P \in E(\mathbb{F}_q)$ und der Einbettungsgrad k ist größer als eins.
Verwenden wir für die Paarung im zweiten Argument statt desselben Punktes P einen verzerrten Punkt $\varphi(P)$, welchen wir über eine sogenannte Verzerrungsabbildung

$$\varphi : E(\mathbb{F}_q) \to E(\mathbb{F}_{q^k})$$

erhalten, so liefert uns das folgende Lemma [BSSC05] unter bestimmten Voraussetzungen einen nichttrivialen Paarungswert.

Lemma 3. *Sei $P \in E(\mathbb{F}_q)$ mit primer Ordnung r und sei $k > 1$. $E(\mathbb{F}_{q^k})$ enthalte keine Punkte der Ordnung r^2 und sei φ ein nichtrationaler Endomorphismus auf E. Dann ist für $\varphi(P) \notin E(\mathbb{F}_q)$ der Wert der Paarung $e(P, \varphi(P)) \neq 1$.*

Beweis. Da φ ein Endomorphimus ist, folgt sofort, dass der Punkt $\varphi(P)$ von der Ordnung 1 oder r ist. Der Fall der Ordnung gleich eins kann jedoch, wegen der Voraussetzung $\varphi(P) \notin E(\mathbb{F}_q)$, nicht eintreten. Die Ordnung des Punktes $\varphi(P)$ ist somit r.
Da P ebenfalls ein Punkt der Ordnung r ist und unabhängig von $\varphi(P)$, bilden diese beiden Punkte eine Basis der r-Torsionsgruppe auf E. Nach Voraussetzung enthält $E(\mathbb{F}_{q^k})$ keine r^2-Torsionspunkte und es gilt $\varphi(P) \notin rE(\mathbb{F}_{q^k})$. Nach Lemma 2 folgt $e(P, P) = 1$ und somit gilt $e(P, \varphi(P)) \neq 1$. □

Dieser Endomorphismus φ, der von $E(\mathbb{F}_q)$ nach $E(\mathbb{F}_{q^k})$ abbildet und den wir eine Verzerrungsabbildung nennen, bildet demnach einen Punkt P auf einen von diesem Punkt unabhängigen Punkt $\varphi(P)$ ab.

Die Frage, welche wir uns nach dieser Einführung stellen müssen, ist die folgende: „*Wann existiert solch eine Verzerrungsabbildung?*“

Wird von der Existenz eines Endomorphismus φ auf einer elliptischen Kurve mit dieser Eigenschaft ausgegangen, so kann gezeigt werden, dass diese Kurve dann notwendig supersingulär ist [Ver01]. Dies impliziert, dass für eine ordinäre Kurve keine Verzerrungsabbildung existiert.
Praktisch bedeutet dies, dass diese Technik nur für supersinguläre Kurven mit Einbettungsgrad ≤ 6 in Betracht gezogen werden kann [MOV91]. Um eine ausreichende Sicherheit zu gewährleisten, muss dann z.B. q als eine relativ große Zahl gewählt werden. Dies soll die folgenden Abschnitte motivieren, in denen wir die η (Eta) Paarung und die Ate Paarung vorstellen, um eine Balance zwischen praktischer Sicherheit und effizienter Berechenbarkeit zu erlangen.
Die Eta Paarung ist eine Paarung, für die Verzerrungsabbildungen verwendet werden.

3.2.2 Die Eta Paarung auf elliptischen Kurven

Für die von Duursma und Lee in [DL03] diskutierten Ideen bezüglich der effizienten Paarungsberechnung auf supersingulären Kurven der speziellen Form $y^2 = x^p - x + d$ über

$\mathbb{F}_{p^l}$ mit $p \geq 3$ und ggT$(l, 2p)$ gelingt es Barreto *et al.* in ihrer 2004 veröffentlichten Arbeit [BGhS04] die verschiedenen Ansätze in vier unabhängige Bereiche zu unterteilen.

1. Die Wahl einer geeigneten Funktion um qD in der Divisorklassengruppe zu berechnen.
2. Die Definition einer Paarung auf Kurvenpunkten (für $g > 1$). Das heißt eher auf reduzierten statt allgemeinen Divisoren.
3. Eine kürzere Schleifenlänge erreichen als der Gruppenordnung nach zu erwarten ist.
4. Die Verwendung von Frobenius-Operationen innerhalb der Berechnung.

Dem Ansatz 3. folgend ist die η Paarung (gesprochen „Eta“) eine der ersten konkreten Veränderungen und damit nahe mit der Tate Paarung verwandt.

Für diese Paarung setzen wir in dieser Arbeit elliptische Kurven E voraus, für die wir die Existenz einer Verzerrungsabbildung annehmen. Damit ist die Supersingularität der Kurve und somit ein Einbettungsgrad ≤ 6 vorausgesetzt. Die durch die Supersingularität garantierte Existenz einer Verzerrungsabbildung ψ ermöglicht uns Nennereliminierungen. Das heißt falls $P \in E(\mathbb{F}_q)$ ist, dann liegt die x-Koordinate des verzerrten Punktes $\psi(P) \in E(\mathbb{F}_{q^k})$ in $\mathbb{F}_{p^{\frac{k}{2}}}$.

Die Betrachtung dieser Paarung über hyperelliptischen Kurven ist ebenfalls möglich und wird inklusive des hier behandelten Falles in [BGhS04] thematisiert.

Nutzen wir den Sachverhalt über supersinguläre Kurven, dass die Multiplikation mit p bzw. einer p-Potenz sehr spezielle Formen annehmen kann und interpretieren diese Multiplikation als Wirkung eines Automorphismus γ auf der Kurve, so führt diese wichtige Beobachtung zur Eta Paarung. Für eine Primzahlpotenz $q = p^l$ und eine prime Zahl r betrachten wir Punkte $P \in E(\mathbb{F}_q)[r]$ und $Q \in E(\mathbb{F}_{q^k})[r]$. Wir definieren die $\eta_{\mathcal{T}}$ Paarung für $\mathcal{T} \in \mathbb{Z}$ als

$$\eta_{\mathcal{T}}(P, Q) = f_{\mathcal{T},P}(\psi(Q)) \tag{3.1}$$

für eine Verzerrungsabbildung ψ auf E. Im Allgemeinen ist diese Paarung jedoch weder bilinear noch nichtdegeneriert. Um diese Eigenschaften zu garantieren, stellen wir den Zusammenhang zur Tate Paarung, welche die geforderten Attribute aufweist, her und halten dies in dem folgenden Theorem fest.

Theorem 1. *[BGhS04] Sei E eine supersinguläre elliptische Kurve über $\mathbb{F}_q$ mit Verzerrungsabbildung ψ und Einbettungsgrad $k \leq 6$.*
Sei $r \mid N \mid (q^k - 1)$, $M = \frac{(q^k-1)}{N}$ und $\mathcal{T} \in \mathbb{Z}$.
Gilt weiterhin

1. *$\mathcal{T} D \equiv \gamma(D)$ in der Divisorklassengruppe für den Divisor $D \approx (P) - (O)$.*
2. *ψ und γ erfüllen $\gamma\psi^q(R) = \psi(R)$ für jeden Punkt $R \in E(\mathbb{F}_q)$.*

3. $\mathcal{T}^a + 1 = LN$ *für ein geeignetes* $a \in \mathbb{N}$ *und* $L \in \mathbb{Z}$.

4. $\mathcal{T} = q + cN$ *für ein geeignetes* $c \in \mathbb{Z}$.

Dann erhalten wir den Zusammenhang von Eta und Tate Paarung als

$$e(P, \psi(Q))^L = (\eta_{\mathcal{T}}(P, Q)^M)^{a\mathcal{T}^{a-1}} \tag{3.2}$$

und die $\eta_{\mathcal{T}}$ *Paarung ist in diesem Fall bilinear und nichtdegeneriert.*

Auf einen Beweis verzichten wir an dieser Stelle, da wir in dem nachfolgenden Abschnitt über die Ate Paarung einen sehr ähnlich strukturierten Beweis vollständig angeben. Der Beweis des Theorems 1 ist in allgemeiner Version auf (hyper-)elliptischen Kurven in [BGhS04] zu finden.
Aus der Verallgemeinerung der Duursma-Lee Technik [DL03], welche wir als Spezialfall $\mathcal{T} = q$ der Eta Paarung verifizieren können, erhalten Barreto *et al.* [BGhS04] unter der Voraussetzung $\mathcal{T} = q - N = \mp t - 1$ eine Größenordnung der Laufzeit der Berechnung der Eta Paarung von $O(\log_2(t))$.
Unter der Annahme, dass die Spur des Frobenius t von der Größenordnung $\sqrt{q}$ ist, erhalten wir $O(\log_2(\sqrt{q}))$. Die klassische Tate Paarung kann über den *Miller*-Algorithmus in $O(\log_2(r))$ berechnet werden.

Ihren Namen verdankt Eta Paarung der engen Relation zur Tate Paarung (3.2) und der Eigenschaft der verkürzten Schleifenlänge des *Miller*-Algorithmus. Diese Anzahl der Schleifendurchläufe gilt als Aufwandsmaß der Berechnung einer Paarung.
Diese Beschleunigung wird erreicht, indem auf die Forderung $[\mathcal{T}]P = O$ verzichtet wird. Der Algorithmus beerechnet nur noch die Funktion $f_{\mathcal{T},P}$, deren Divisor wir angeben können als $(f_{\mathcal{T},P}) = \mathcal{T}(P) - ([\mathcal{T}]P) - (\mathcal{T} - 1)(O)$.

Der aktuelle Stand der Forschung ist die Entwicklung der sogenannten *Ate Paarung*. Auch hier lässt der Name schon die nahe Verwandtschaft zu Tate und Eta Paarung vermuten.

3.2.3 Die Ate Paarung

Zur Namensgebung zitieren wir die äußerst treffende Beschreibung aus [HSV06].

> „We call our new pairing the Ate pairing, pronounced eight. This is for two reasons, firstly it is like the Tate pairing, but faster (hence the missing „*T*"), it is also like the Eta pairing but it reverses the order of the arguments (and Ate is Eta spelled backwards)."

Ein Nachteil der Eta Paarung ist, dass diese ausschließlich für supersinguläre Kurven verwendbar ist. Für diese Kurven gilt die Einschränkung bezüglich des Einbettunsgrades $k \leq 6$. Deren Gegenpart, die ordinären Kurven lassen einen größeren Einbettungsgrad zu und dieser steht in direktem Zusammenhang mit der Sicherheit paarungsbasierter,

kryptographischer Protokolle.
Der Einbettungsgrad sollte aus Effizienzgründen jedoch nicht zu groß werden, da dann die im Körper $\mathbb{F}_{q^k}$ auszuführenden Operationen arithmetisch zu teuer sind.

Die Ate Paarung auf der Punktgruppe elliptischer Kurven

Den Schritt von supersingulären zu ordinären Kurven finden wir detailliert in [HSV06] beschrieben. Wir betrachten diese Paarung im Folgenden sehr ausführlich.

Als Eingabeargumente der Tate Paarung auf elliptischen Kurven gelten im Allgemeinen die Punkte $P \in E(\mathbb{F}_q)$ und $Q \in E(\mathbb{F}_{q^k})$. In der Praxis beschränkt sich die Berechnung meist auf spezifische Untergruppen und wir erhalten daraus eine relevante Beschleunigung. Für die Ate Paarung betrachten wir folgenden Gruppen

- $\mathbb{G}_1 = E(\mathbb{F}_q)[r]$
- $\mathbb{G}_2 = E(\mathbb{F}_{q^k})[r] \cap \ker(\pi_q - [q])$

Hierbei bezeichnen wir mit π_q den Frobenius-Endomorphismus. Das heißt jenen Endomorphismus $\pi_q : E \to E$, der einen Punkt (x, y) auf (x^q, y^q) abbildet und die Eigenwerte 1 und q besitzt.

Sei $f_{s,R}$ eine Miller-Funktion für einen Punkt $R \in E(\mathbb{F}_{q^k})$. Im Folgenden betrachten wir die normalisierte Funktion $f_{s,R}^{\text{norm}}$. Sei dazu $z \in \mathbb{F}_q(E)$ ein uniformisierendes Element an O, das heißt es gilt $\text{ord}_O(z) = 1$.
Wir definieren $\text{lc}_O(f_{s,R}) = z^{-\text{ord}_O(f_{s,R})} f_{s,R}(O)$ und $f_{s,R}^{\text{norm}} = f_{s,R}/\text{lc}_O(f_{s,R})$. Die Funktion $f_{s,R}^{\text{norm}}$ ist dann über dem Defintionsbereich von R und (bis auf s-Potenzen) eindeutig durch s und R bestimmt.

Die erstmals in 2006 vorgestellte Ate Paarung auf $\mathbb{G}_2 \times \mathbb{G}_1$ ist wie im folgend zitierten Theorem 2 erklärt.

Theorem 2. *[HSV06] Sei E eine ordinäre, elliptische Kurve über $\mathbb{F}_q$, $r \geq 5$ eine große Primzahl, so dass $r \mid \#E(\mathbb{F}_q)$. Die Zahl t sei die Frobenius-Spur zu $\#E(\mathbb{F}_q) = q - t + 1$. Für $T = t - 1$, $Q \in \mathbb{G}_2$ und $P \in \mathbb{G}_1$ gilt dann das Folgende.*

- *Die Abbildung $a_T(Q, P) := f_{T,Q}^{\text{norm}}(P)$ definiert eine bilineare Paarung, welche wir elliptische Ate Paarung nennen.*
- *Sei $N = \gcd(T^k - 1, q^k - 1)$ und $T^k - 1 = LN$, mit Einbettungsgrad k, dann gilt*

$$e(Q, P)^L = f_{T,Q}^{\text{norm}}(P)^{c(q^k-1)/N}, \text{ wobei } c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv kq^{k-1} \mod r. \quad (3.3)$$

- *Teilt r nicht L, falls also $r \nmid L$ gilt, so ist die Ate Paarung nichtdegeneriert.*

Beweis. Ist vollständig in [HSV06] zu finden.

In Theorem 2 ist die Ate Paarung über Gleichung (3.3) bestimmt und mit dem Exponenten $c(q^k - 1)/N$ versehen. Wollen wir denselben Exponenten erreichen, den wir für die reduzierte Tate Paarung in (2.1) verwenden, so ist die folgend definierte Paarung

$$\begin{aligned} a_T : \mathbb{G}_2 \times \mathbb{G}_1 &\to \mu_r \\ (Q, P) &\mapsto a_T(Q, P) = f_{T,Q}(P)^{(q^k-1)/r}, \end{aligned}$$

wegen $r \mid N$ und $r \nmid c$ stets bilinear und genau dann nichtdegeneriert, falls $s^k \not\equiv 1 \mod r^2$ gilt.

Betrachten wir die Ate Paarung auf $\mathbb{G}_1 \times \mathbb{G}_2$ so definiert dies im Allgemeinen keine bilineare Paarung. Für ordinäre elliptische Kurven, welche einen eindeutigen Twist vom Grad $m = \gcd(k, \#\mathrm{Aut}(E))$ zulassen, kann die *getwistete Ate Paarung* definiert werden [HSV06].
Wir nennen eine elliptische Kurve E' über $\mathbb{F}_q$ einen *Twist vom Grad d von E*, wenn es einen Isomorphismus $\psi : E' \to E$ gibt, der über $\mathbb{F}_{q^d}$ mit d minimal definiert ist.
Ist E ordinär, $k = ed$ und besitzt E einen Twist über $\mathbb{F}_{q^e}$ vom Grad $d > 1$, so können E' und ψ so gewählt werden, dass $E'(\mathbb{F}_{q^e})[r] = \langle \psi^{-1}(Q) \rangle$ gilt [Hes06].

Diese Paarung ist in einer optimierten Version, welche durch die Ersetzung der Zahl T durch ein S mit $S \equiv q \mod r$ erreicht wird, in [MKHO07] publiziert worden. Der eben eingeführte Fall $T = t - 1$ ist hierbei als Spezialfall in der optimierten Aussage inbegriffen, da die Zahl $t - 1$ die Kongruenz $t - 1 \equiv q \mod r$ ebenfalls erfüllt.

Ein Resultat der vorliegenden Arbeit ist der folgende Satz. Wir formulieren mit diesem eine weiterführende und das Ergebnis aus [MKHO07] verallgemeinernde, optimierte Version der Ate und der getwisteten Ate Paarung.

Satz 4. *Für eine ordinäre elliptische Kurve E sei $r \geq 5$ ein großer primer Teiler der Kurvenordnung $\#E(\mathbb{F}_q) = q + 1 - t$. Sei S_i eine ganze Zahl mit $S_i \equiv q^i \mod r$ mit minimalem Exponenten α_i, so dass die Kongruenz $S_i^{\alpha_i} \equiv 1 \mod r$ erfüllt ist.*
Für $Q \in \mathbb{G}_2$ und $P \in \mathbb{G}_1$ gilt dann das Folgende.

- *Die Abbildung $a_{S_i} := f_{S_i,Q}(P)$ definiert eine bilineare Paarung, welche wir Ate$_i$ Paarung nennen.*
- *Sei $N_i = \gcd(S_i^{\alpha_i} - 1, q^k - 1)$ und $L_i N_i = (S_i^{\alpha_i} - 1)$, dann gilt*

$$\begin{aligned} e(Q, P)^{L_i} &= f_{S_i,Q}(P)^{c_{S_i}(q^k-1)/N_i}, \qquad (3.4) \\ \text{wobei } c_{S_i} &= \sum_{j=0}^{\alpha_i - 1} S^{\alpha_i - 1 - j}(q^i)^j \equiv \alpha_i q^{\alpha_i - 1} \mod r. \end{aligned}$$

- *Falls r nicht L_i teilt, also $r \nmid L_i$ gilt, so ist die Ate$_i$ Paarung nichtdegeneriert.*

Gilt $k \mid \#Aut(E)$, so definiert

$$a_{S_i}^{Twist} : (P, Q) \mapsto f_{S_i,P}(Q)^{c_{S_i}(q^k-1)/N_i}$$
$$mit\ c_{S_i} = \sum_{j=0}^{\alpha_i-1} S^{\alpha_i-1-j}(q^i)^j \equiv \alpha_i q^{\alpha_i-1} \mod r$$

ebenfalls eine bilineare Paarung und diese ist genau dann nichtdegeneriert, wenn $r \nmid L_i$.

Die grundsätzliche Vorgehensweise des Beweises entspricht der aus den [HSV06] bzw. [MKHO07]. Dieser Konstruktion folgend erarbeiten wir drei Lemmata, deren Aussagen wir zum Beweis des Satzes 4 verwenden.

Lemma 4. *Mit den Bezeichnungen aus Satz 4 gilt*

$$e(Q, P)^{L_i} = f_{S_i^{\alpha_i},Q}(P)^{(q^k-1)/N_i}$$

Beweis. Die reduzierte Tate Paarung ist nach Abschnitt 2.2.1 definiert als

$$e(Q, P) = f_{r,Q}(P)^{(q^k-1)/r} = f_{N,Q}(P)^{(q^k-1)/N} \tag{3.5}$$

für jedes $N \in \mathbb{N}$ mit $r \mid N \mid (q^k - 1)$. Mit den Konstruktionen aus Satz 4 erhalten wir mit $N_i = \gcd(S_i^{\alpha_i} - 1, q^k - 1)$ und $L_i N_i = (S_i^{\alpha_i} - 1)$, wonach offensichtlich $r \mid N_i \mid (q^k - 1)$ gilt, die folgende Gleichheit.

$$\begin{aligned} e(Q, P)^{L_i} &= f_{N_i,Q}(P)^{L_i(q^k-1)/N_i} \\ &= f_{L_iN_i,Q}(P)^{(q^k-1)/N_i} \\ &= f_{S_i^{\alpha_i}-1,Q}(P)^{(q^k-1)/N_i} \\ &= f_{S_i^{\alpha_i},Q}(P)^{(q^k-1)/N_i}. \end{aligned} \tag{3.6}$$

Hierbei verwenden wir die durch Konstruktion erhaltenen Eigenschaften.
Letztere Gleichheit in (3.6) kann durch einfaches Nachrechnen von $(f_{S_i^{\alpha_i}-1,Q}) = (f_{S_i^{\alpha_i},Q})$ gezeigt werden.

$$\begin{aligned} (f_{S_i^{\alpha_i}-1,Q}) &= (S_i^{\alpha_i} - 1)(Q) - ([S_i^{\alpha_i} - 1]Q) - (S_i^{\alpha_i} - 1 - 1)(O) \\ &\overset{(*)}{=} S_i^{\alpha_i}(Q) - ([S_i^{\alpha_i}]Q) - (S_i^{\alpha_i} - 1)(O) \\ &= (f_{S_i^{\alpha_i},Q}) \end{aligned}$$

Wobei wir in $(*)$ ausnutzen, dass $S_i^{\alpha_i} \equiv 1 \mod r$ gilt. Aufgrund der gezeigten Gleichheit der Divisoren können wir ohne Einschränkung die Gleichheit der Funktionen in (3.6) annehmen und vervollständigen damit den Beweis des Lemma 4. □

Lemma 5. *Mit den Bezeichnungen aus Satz 4 können wir $f_{S_i^{\alpha_i},Q}$ so wählen, dass*

$$f_{S_i^{\alpha_i},Q} = f_{S_i,Q}^{S_i^{\alpha_i-1}} \cdot f_{S_i,S_iQ}^{S_i^{\alpha_i-2}} \cdot \ldots \cdot f_{S_i,S_i^{\alpha_i-1}Q}. \tag{3.7}$$

Beweis. Wir betrachten die zu zeigende Gleichung (3.7) ausgehend von der rechten Seite (gekennzeichnet mit (r. S.)) und überführen diese in die linke.
Um die Gleichheit der Funktionen zu erhalten, genügt es die Gleichheit für die zugehörigen Divisoren zu zeigen.

$$\left(f_{S_i^{\alpha_i},Q}\right) = \left(f_{S_i,Q}^{S_i^{\alpha_i-1}} \cdot f_{S_i,S_iQ}^{S_i^{\alpha_i-2}} \cdot \ldots \cdot f_{S_i,S_i^{\alpha_i-1}Q}\right).$$

Dies lässt sich leicht nachrechnen.

$$\begin{aligned}
\text{(r. S.)} &= \left(\prod_{j=0}^{\alpha_i-1} f_{S_i,[S_i^j]Q}^{S_i^{\alpha_i-1-j}}\right) \\
&= \sum_{j=0}^{\alpha_i-1} S_i^{\alpha_i-1-j}\left\{\left(f_{S_i,[S_i^j]Q}\right)\right\} \\
&= \sum_{j=0}^{\alpha_i-1} S_i^{\alpha_i-1-j}\left\{S_i([S_i^j]Q) - ([S_i \cdot S_i^j]Q) - (S_i-1)(O)\right\} \\
&= \sum_{j=0}^{\alpha_i-1} S_i^{\alpha_i-1-j}\left\{S_i([S_i^j]Q) - ([S_i^{j+1}]Q)\right\} - \sum_{j=0}^{\alpha_i-1} S_i^{\alpha_i-1-j}(S_i-1)(O) \\
&= \underbrace{\sum_{j=0}^{\alpha_i-1}\left\{S_i^{\alpha_i-j}([S_i^j]Q) - S_i^{\alpha_i-1-j}([S_i^{j+1}]Q)\right\}}_{(S1)} - \underbrace{\sum_{j=0}^{\alpha_i-1}(S_i^{\alpha_i-j} - S_i^{\alpha_i-1-j})(O)}_{(S2)} \\
&\overset{(**)}{=} S_i^{\alpha_i}(Q) - ([S_i^{\alpha_i}]Q) - (S_i^{\alpha_i}-1)(O)
\end{aligned}$$

Die Gleichung $(**)$ folgt durch Auflösen der beiden Summen. Für je zwei aufeinanderfolgende Indizes l und $l+1$ gilt für $(S1)$

$$\begin{aligned}
&\left\{S_i^{\alpha_i-l}([S_i^l]Q) - S_i^{\alpha_i-1-l}([S_i^{l+1}]Q)\right\} + \left\{S_i^{\alpha_i-(l+1)}([S_i^{l+1}]Q) - S_i^{\alpha_i-1-(l+1)}([S_i^{(l+1)+1}]Q)\right\} \\
&= S_i^{\alpha_i-l}([S_i^l]Q) - S_i^{\alpha_i-l}([S_i^{l+2}]Q).
\end{aligned}$$

Analoges gilt für die Summe $(S2)$. Daher bleiben nur die Summanden zu den Indizes für $j = 0$ und $j = \alpha_i - 1$ stehen:

$$\begin{aligned}
&\left\{S_i^{\alpha_i-0}([S_i^0]Q) - S_i^{\alpha_i-1-(\alpha_i-1)}([S_i^{(\alpha_i-1)+1}]Q)\right\} - \left\{(S_i^{\alpha_i-0} - S_i^{\alpha_i-1-(\alpha_i-1)})(O)\right\} \\
&= S_i^{\alpha_i}(Q) - ([S_i^{\alpha_i}]Q) - (S_i^{\alpha_i}-1)(O),
\end{aligned}$$

wobei wir $S_i^{\alpha_i} \equiv 1 \mod r$ ausnutzen.

Die überbleibenden Terme entsprechen gerade dem Divisor der linken Seite und wir erhalten ohne Einschränkung die Behauptung (3.7). □

Lässt sich jeder Faktor $f_{S_i,[S_i^j]Q}^{S_i^{\alpha_i-1-j}}$ der rechten Seite von (3.7) vollständig durch Terme in $f_{S_i,Q}$ ausdrücken, so sind wir in der Lage den Beweis des Satzes 4 anzugeben.

Für diesen Schritt können wir die Beziehung $\pi_{q^i}^j(Q) = [q^{ij}]Q = [S_i^j]Q$ des Frobenius-Endomorphismus für Punkte $Q \in \mathbb{G}_2$ verwenden und es genügt $f_{S_i,[S_i^j]Q}$ und $f_{S_i,Q}$ für $0 \leq j \leq (\alpha_i - 1)$ miteinander in Relation zu setzen. Diese Verbindung liefert das folgende Lemma.

Lemma 6. *Für alle $Q \in \mathbb{G}_2$ können wir $f_{S_i,[S_i^j]Q} = f_{S_i,Q}^{\sigma^{ij}}$ schreiben, wobei σ der q-Potenz Frobenius-Automorphismus auf $\overline{\mathbb{F}}_q$ ist.*

Beweis. Zunächst definieren wir den Homomorphismus $F^* : \mathrm{Div}_E \to \mathrm{Div}_E$, der für eine nichtkonstante rationale Abbildung $F : E \to E$ erklärt ist als

$$F^*((Q)) := \sum_{F(R)=Q} e_F(R) \cdot (R), \tag{3.8}$$

wobei $e_F(R)$ der *Verzweigungsindex von F an R* heißt und über $e_F(R) = \mathrm{ord}_R(u \circ F)$ mit einem uniformisierenden Element $u \in \mathbb{F}_q(E)$ definiert ist. Ist F ein Endomorphismus, so ist $e_F(P)$ konstant für alle P und wir bezeichnen den Verzweigungsindex in diesem Fall mit e_F. Weiterhin gilt für eine rationale Funktion h die folgende Identität für die durch $h \circ F$ und h erklärten Hauptdivisoren:

$$(h \circ F) = F^*(h). \tag{3.9}$$

Weiterhin definieren wir den Homomorphismus $F_* : \mathrm{Div}_E \to \mathrm{Div}_E$, der für eine nichtkonstante rationale Abbildung $F : E \to E$ erklärt ist als

$$F_*((R)) := (F(R)). \tag{3.10}$$

Das obige Lemma 6 können wir mit diesen Ausführungen wie folgt beweisen.

Nach Definition gilt $(f_{S_i,[S_i^j]Q}) = S_i([S_i^j]Q) - ([S_iS_i^j]Q) - (S_i - 1)(O)$. Da π_{q^i} ein rein inseparabler Endomorphismus vom Grad q^i bzw. $\pi_{q^i}^j$ vom Grad q^{ij} ist, gilt

$$\begin{aligned}
(\pi_{q^i}^j)^*\left((f_{S_i,[S_i^j]Q})\right) &= (\pi_{q^i}^j)^*\left((f_{S_i,\pi_{q^i}^j(Q)})\right) \\
&= (\pi_{q^i}^j)^*(S_i([S_i^j]Q) - ([S_i^{j+1}]Q) - (S_i - 1)(O)) \\
&= S_i \cdot (\pi_{q^i}^j)^*([S_i^j]Q) - (\pi_{q^i}^j)^*([S_i^{j+1}]Q) - (S_i - 1) \cdot (\pi_{q^i}^j)^*(O) \\
&= q^{ij}S_i(Q) - q^{ij}([S_i](Q)) - q^{ij}(S_i - 1)(O) \\
&= q^{ij}(S_i(Q) - ([S_i]Q) - (S_i - 1)(O)) \\
&= (f_{S_i,Q}^{q^{ij}}).
\end{aligned}$$

Weiterhin gilt nach (3.9) gerade $(\pi_{q^i}^j)^*((f_{S_i,\pi_{q^i}^j(Q)})) = (f_{S_i,\pi_{q^i}^j(Q)} \circ \pi_{q^i}^j)$ und wir können wegen der Gleichheit von $(\pi_{q^i}^j)^*((f_{S_i,[S_i^j]Q})) = (f_{S_i,Q}^{q^{ij}})$ die Funktionen ohne Einschränkung so wählen, dass

$$f_{S_i,\pi_{q^i}^j(Q)} \circ \pi_{q^i}^j = f_{S_i,Q}^{q^{ij}}$$

gilt. Nach Umformulieren von $f_{S_i,Q}^{q^{ij}}$ zu $f_{S_i,Q}^{\sigma^{ij}} \circ \pi_{q^i}^j$ erhalten wir die Behauptung. □

An dieser Stelle haben wir das für den Beweis von Satz 4 nötige Handwerkszeug beisammmen und geben diesen an.

Beweis. Sei $\psi = \pi_{q^i}$ im Falle der Ate$_i$ Paarung und $\psi = \gamma^l \pi_{q^i}$ für die getwistete Ate$_i$ Paarung. Wobei $\gamma \in \mathrm{Aut}(E)$ ein Automorphismus der Ordnung k mit $(\gamma^l \pi_{q^i})(Q) = Q$ und $(\gamma^l \pi_{q^i})(P) = [q^i]P$ für ein l ist.
Nach Konstruktion gilt in beiden Fälle $\psi(P) = P$ und $\psi(Q) = [q^i]Q$. Analog zur Ate$_i$ Paarung ist demnach $f_{S_i,Q}(P)^{c_{S_i}(q^k-1)/N_i}$ zu betrachten. Infolgedessen können wir dies in einem gemeinsamen Beweis abhandeln, indem wir stets mit der Abbildung ψ arbeiten. Die Aussagen und Beweise für die Lemma 4, 5 und 6 sind übertragbar.

Es gilt $\psi^j(Q) = [q^{ij}]Q$ und $\psi^j(P) = P$. Kombinieren wir $f_{S_i{}^{\alpha_i},Q}(P)$ mit den Ergebnissen aus Lemma 5 sowie denen aus Lemma 6 so erhalten wir

$$\begin{aligned} f_{S_i{}^{\alpha_i},Q}(P) &= f_{S_i,Q}^{S_i{}^{\alpha_i-1}}(P) \cdot f_{S_i,[S_i]Q}^{S_i{}^{\alpha_i-2}}(P) \cdot \ldots \cdot f_{S_i,[S_i{}^{\alpha_i-1}]Q}(P) \\ &= f_{S_i,Q}^{S_i{}^{\alpha_i-1}\cdot(q^i)^0}(P) \cdot f_{S_i,Q}^{S_i{}^{\alpha_i-2}\cdot(q^i)^1}(P) \cdot \ldots \cdot f_{S_i,Q}^{S_i{}^{0}\cdot(q^i)^{\alpha_i-1}}(P) \\ &= f_{S_i,Q}(P)^{\sum_{j=0}^{\alpha_i-1} S_i{}^{\alpha_i-1-j}(q^i)^j}. \end{aligned} \tag{3.11}$$

Die Substitution der Gleichheit (3.11) in das Resultat (3.6) aus Lemma 4 ergibt

$$e(Q,P)^{L_i} = f_{S_i,Q}(P)^{c_{S_i}(q^k-1)/N_i}. \tag{3.12}$$

Die Gleichung (3.12) zeigt, dass die Paarungen in Satz 4 bilinear und genau dann nichtdegeneriert sind, falls $r \nmid L_i$. □

Im Vergleich zur Tate Paarung kann die Ate Paarung also die Auswertung von $f_{T,Q}(P)$ mittels des *Miller*-Algorithmus 2 in einer Schleifenlänge von $\lfloor \log_2 | T | \rfloor$ berechnet werden. Für den oben angegeben Fall der Ate$_i$ Paarung in Satz 4 kann dies in $\lfloor \log_2 | S_i | \rfloor$ geschehen. Zur Wahl eines geeigneten S_i verweisen wir auf [ZZH07], worin auch einige Betrachtungen der Effizienz zu finden sind.

Die Ate Paarung auf der Jacobischen hyperelliptischer Kurven

Auch die, in Theorem 2 definierte, Ate Paarung kann auf hyperelliptische Kurven des Geschlechts g übertragen werden.

Für eine hyperelliptische Kurve C sei $r \mid \#\mathrm{Pic}^0_C(\mathbb{F}_q) = q^g + a_1(q^{g-1}+1) + \ldots + a_g$. Ist $r \approx \#\mathrm{Pic}^0_C(\mathbb{F}_q)$, so ist die Bitlänge von q schon g-mal kürzer als die Bitlänge von r. Wir geben für die hyperelliptische Ate Paarung eine dem Theorem 2 ähnliche Version für $T = q$ an. Die betrachteten Gruppen sind in diesem Fall

- $\mathbb{G}_1 = \mathrm{Pic}^0_C(\mathbb{F}_q)[r]$
- $\mathbb{G}_2 = \mathrm{Pic}^0_C(\mathbb{F}_{q^k})[r] \cap \ker(\pi_q - [q])$.

Die paarungsdefinierende Miller-Funktion sei wiederum normalisiert und wir schreiben $f^{\mathrm{norm}}_{s,D} = f_{s,D}/\mathrm{lc}_O(f_{s,D})$.
Zu jeder Divisorklasse $[D]$ bezeichnen wir, nach Abschnitt 1.4.2, mit $\rho([D])$ den eindeutigen reduzierten Divisor der Äquivalenzklasse. Mit $\epsilon([D])$ notieren wir den effektiven Teil von $\rho([D])$. Damit gilt $\rho([D]) = \epsilon([D]) - d(O)$.
Eine hyperelliptische Kurve nennen wir *superspezial*, falls die Jacobische der Kurve $\mathcal{J}_C$ isomorph zu E^g, für eine supersinguläre, elliptische Kurve E, ist. Das heißt es existiert ein Isomorphismus $\mathcal{J}_C \to E^g$.

Theorem 3. *[GHO+07] Mit den voranstehenden Notationen und Annahmen definiert*

$$\begin{aligned} a &: \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r \\ ([D_2], [D_1]) &\mapsto f^{\mathrm{norm}}_{q,\rho([D_2])}(\epsilon([D_1])) \end{aligned} \tag{3.13}$$

eine nichtdegenerierte, bilineare Paarung. Die über (3.13) erklärte Paarung heißt hyperelliptische Ate Paarung.
Ist C eine superspezielle Kurve und ist $d = \gcd(k, q^k - 1)$, so definiert

$$\begin{aligned} \hat{a} &: \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r \\ ([D_1], [D_2]) &\mapsto f^{\mathrm{norm}}_{q,\rho([D_1])}(\epsilon([D_2]))^d \end{aligned}$$

ebenfalls eine nichtdegenerierte, bilineare Paarung.
Gilt für eine der beiden Paarungen $\mathrm{supp}(\epsilon([D_i])) \cap \mathrm{supp}(\rho([D_j])) \neq \emptyset$, so muss $\epsilon([D_i])$ durch einen Divisor $D \in [D_i]$ mit $\mathrm{supp}(D) \cap \mathrm{supp}(\rho([D_j])) = \emptyset$ ersetzt werden.

Die Verhältnisse zur Tate Paarung lassen sich angeben als

$$t_r([D_2], [D_1]) = a([D_2], [D_1])^{kq^{k-1}} \text{ und } t_r([D_1], [D_2]) = \hat{a}([D_1], [D_2])^{\frac{k}{d}q^{k-1}}.$$

Beweis. Ist vollständig in [GHO+07] zu finden.

Der folgende Satz zeigt, dass die in Theorem 3 angenommenen Voraussetzung für die Definition der hyperelliptischen Ate Paarungen zu stark sind. Wir zeigen im Folgenden, dass die Existenz eines Automorphismus der Ordnung k genügt.
Wir betrachten zunächst allgemeine Untergruppen $\mathbb{G}_1, \mathbb{G}_2 \subset \mathrm{Pic}^0_C(\mathbb{F}_{q^k})[r]$, so dass die Tate Paarung auf diesen Gruppen nichtdegeneriert ist.

Satz 5. *Sei C eine hyperelliptische Kurve über dem Körper $\mathbb{F}_q$ vom Geschlecht $g \geq 2$. Seien die Gruppen $\mathbb{G}_1, \mathbb{G}_2 \subset \mathrm{Pic}^0_C(\mathbb{F}_{q^k})[r]$ gegeben. Sei s eine primitive m-te Einheitswurzel modulo r, d.h $s^m \equiv 1 \mod r$.*
Für $[D_2] \in \mathbb{G}_2$, $[D_1] \in \mathbb{G}_1$, $c_s = \sum_{i=0}^{k-1} s^{m-1-i} q^i$, $N = \gcd(q^k - 1, s^m - 1)$ und $LN = s^m - 1$ gilt dann das Folgende.
Die Abbildung

$$\begin{aligned}\tilde{a} : \mathbb{G}_1 \times \mathbb{G}_2 &\to \mu_r \\ ([D_1], [D_2]) &\mapsto f_{s,D_1}(D_2)^{c_s(q^k-1)/N}\end{aligned}$$

definiert eine nichtdegenerierte, bilineare Paarung, falls r nicht L teilt, d.h. $r \nmid L$.

Die grundsätzliche Vorgehensweise des Beweises entspricht der des Satzes 4.

Beweis. Für die Ausführung nehmen wir die Existenz einer rein inseperablen Abbildung $\psi : C \to C$ an. Diese habe im Weiteren die folgenden Eigenschaften auf den Untergruppen $\mathbb{G}_1, \mathbb{G}_2 \subset \mathrm{Pic}^0_C(\mathbb{F}_{q^k})[r]$.
Es existieren Erzeuger $[D_1]$, $[D_2]$ der Gruppen $\mathbb{G}_1$ bzw. $\mathbb{G}_2$, so dass $\psi([D_1]) = s[D_1]$ und $\psi([D_2]) = [D_2]$. Weiterhin gelte $\psi(D_2) = D_2$. Nehmen wir die Reduziertheit von $\psi^i(D_1)$ für $0 \leq i \leq m-1$ an, so gilt $\rho(\psi^i([D_1])) = \psi^i(\rho([D_1]))$ für $0 \leq i \leq m-1$.
Im Anschluss an den Beweis des Satzes 5 werden wir die konkrete Wahl der Parameter angeben.

Sei q^n der Grad der Abbildung ψ. N und L seien wie in Satz 5 gewählt. Der Divisor einer Miller-Funktion ist definiert als $(f_{n,D}) = nD - \rho([nD])$.
Dann gilt für die Tate Paarung

$$t_r([D_1], [D_2])^L = f_{r,D_1}(D_2)^{L(q^k-1)/r} = f_{N,D_1}(D_2)^{L(q^k-1)/N}.$$

Weiterhin gilt wegen $N \equiv 0 \mod r$ für den Divisor

$$\begin{aligned}(f^L_{N,D_1}) &= L(f_{N,D_1}) = L(ND_1 - \rho([ND_1])) \\ &= L(ND_1) = LND_1 \\ &= LND_1 - \rho([LND_1])) \\ &= (f_{LN,D_1})\end{aligned}$$

und damit

$$t_r([D_1], [D_2])^L = f_{LN,D_1}(D_2)^{(q^k-1)/N} = f_{s^m-1,D_1}(D_2)^{(q^k-1)/N}. \tag{3.14}$$

Für f_{s^m-1,D_1} können wir o.B.d.A. die Gleichheit zu f_{s^m,D_1} annehmen, da für die Divisoren Gleichheit gilt.

$$\begin{aligned}(f_{s^m-1,D_1}) &= (s^m - 1)D_1 - \rho([(s^m - 1)D_1]) \\ &= s^m D_1 - D_1 = s^m D_1 - \rho([D_1]) \\ &= (f_{s^m,D_1})\end{aligned}$$

Betrachten wir die Funktion f_{s^m,D_1} genauer, so stellen wir das Folgende fest:

$$\begin{aligned}(f_{s^m,D_1}) &= s^m D_1 - \rho([D_1]) \\ &= s(s^{m-1}D_1) - s\rho([s^{m-1}D_1]) + s\rho([s^{m-1}D_1]) - \rho([D_1]) \\ &= s(f_{s^m-1,D_1}) + (f_{s,\rho([s^{m-1}D_1])}) \\ &= (f^s_{s^m-1,D_1} f_{s,\rho([s^{m-1}D_1])})\end{aligned}$$

Und somit gilt nach mehrfacher Anwendung

$$(f_{s^m,D_1}) = (\prod_{i=0}^{m-1} f^{s^i}_{s,\rho([s^{m-1-i}D_1])}). \tag{3.15}$$

Die Abbildung ψ vom Grad q^n operiert auf der Gruppe $\mathrm{Div}_C(\mathbb{F}_{q^k})$ über

$$\psi(\sum_j \lambda_j P_j) = \sum_j \lambda_j \psi(P_j)$$

und auf $\mathrm{Pic}^0_C(\mathbb{F}_{q^k})$ mittels $\psi[D] = [\psi(D)]$.
Gilt $\psi(\rho([nD])) = \rho(\psi([nD]))$, so folgt

$$(f_{s,\rho([s^iD_1])}) = (f_{s,\rho([\psi^i(D_1)])}) = (f_{s,\rho(\psi^i([D_1]))}) = (f_{s,\psi^i(\rho([D_1]))}). \tag{3.16}$$

Für einen Divisor $D \in \mathrm{Div}_C(\mathbb{F}_{q^k})$ betrachten wir

$$\begin{aligned}(f_{n,\psi(D)}) &= n\psi(D) - \rho([n\psi(D)]) \\ &= \psi(nD) - \rho([\psi(nD)]) \\ &= \psi(nD) - \rho(\psi([nD])) = \psi(nD) - \psi(\rho([nD])) \\ &= \psi(nD - \rho([nD])) = (\psi_*(f_{n,D})),\end{aligned}$$

wobei wir die in (3.10) erklärte $_*$-Abbildung verwenden. Des Weiteren gilt $\psi^*(f) = f \circ \psi$ und $(\psi^* \circ \psi_*)(f) = f^{q^n}$ für eine rationale Abbildung f und wir erhalten

$$(f_{n,\psi(D)} \circ \psi) = (\psi_*(f_{n,D}) \circ \psi) = ((\psi^* \circ \psi_*)(f_{n,D})) = (f^{q^n}_{n,D}). \tag{3.17}$$

Wenden wir dies auf (3.16) an, so ergibt sich mit den vorangestellten Erläuterungen

$$(f_{s,\rho([s^iD_1])} \circ \psi^i) = (f^{q^{ni}}_{s,\rho(D_1)}) = (f^{q^{ni}}_{s,D_1}).$$

Damit gilt

$$\begin{aligned} f_{s^m,D_1}(D_2) &\overset{(3.15)}{=} \prod_{i=0}^{m-1} f_{s,\rho([s^{m-1-i}D_1])}^{s^i}(D_2) \\ &= \prod_{i=0}^{m-1} f_{s,\rho([s^iD_1])}^{s^{m-1-i}}(D_2) \\ &\overset{(*)}{=} \prod_{i=0}^{m-1} f_{s,\rho([s^iD_1])}^{s^{m-1-i}}(\psi^i(D_2)) \\ &= \prod_{i=0}^{m-1} (f_{s,\rho([s^iD_1])}^{s^{m-1-i}} \circ \psi^i)(D_2) \\ &\overset{(3.17)}{=} \prod_{i=0}^{m-1} f_{s,D_1}^{s^{m-1-i}q^{ni}}(D_2) \\ &= f_{s,D_1}(D_2)^{\sum_{i=0}^{m-1} s^{m-1-i}q^{ni}}. \end{aligned} \tag{3.18}$$

In $(*)$ nutzen wir $\psi(D_2) = D_2$. Substituieren wir (3.18) in Gleichung (3.14) und schreiben $c_s = \sum_{i=0}^{m-1} s^{m-1-i}q^{ni}$, dann folgt

$$t_r([D_1], [D_2])^L \overset{(3.14)}{=} f_{s^m,D_1}(D_2)^{(q^k-1)/N} \overset{(3.18)}{=} f_{s,D_1}(D_2)^{c_s(q^k-1)/N}.$$

Gelten die zu Beginn dieses Beweises aufgestellten Annahmen, so ist die in Satz 5 definierte Paarung nichtdegeneriert und bilinear, falls $r \nmid L$. □

Zur Existenz geeigneter Parameter Sei ψ eine rein inseperable Abbildung vom Grad q^n. Es existiert ein $\mathbb{F}_{q^k}$-rationaler Automorphismus $\alpha \in \mathrm{Aut}_{\mathbb{F}_{q^k}}(C)$ auf C, so dass $\psi = \pi_q^n \circ \alpha$ erfüllt ist.
Betrachten wir den Frobenius-Endomorphismus π_q auf $\mathrm{Pic}_C(\overline{\mathbb{F}_q})[r]$, so zerlegt die normalisierte Spurabbildung $\mathrm{Pic}_C(\overline{\mathbb{F}_q})[r] \to \mathrm{Pic}_C(\mathbb{F}_q)[r]$ die Inklusion von $\mathrm{Pic}_C(\mathbb{F}_q)[r]$ in $\mathrm{Pic}_C(\overline{\mathbb{F}_q})[r]$. Wir können daher $\mathrm{Pic}_C(\overline{\mathbb{F}_q})[r]$ schreiben als

$$\mathrm{Pic}_C(\overline{\mathbb{F}_q})[r] = \mathrm{Pic}_C(\mathbb{F}_q)[r] \oplus V.$$

Im Weiteren verwenden wir für $\mathrm{Pic}_C(\mathbb{F}_q)[r]$ die Notation $V_1 := \mathrm{Pic}_C(\mathbb{F}_q)[r]$. V_1 ist der Eigenraum des Frobenius-Endomorphismus zum Eigenwert 1. Weiterhin gilt ür V $\pi_q(V) = V$.

Analog notieren wir V_q für den Eigenraum des Frobenius-Endomorphismus zum Eigenwert q. Wir können somit V als direkte Summe der beiden Unterräume V_q und $\mathcal{V}$ schreiben.
Weiterhin gilt das folgende Lemma.

Lemma 7. *Für alle $x \in V_1$ und $v \in \mathcal{V}$ gilt*

$$t_r(x, v) = 1.$$

Beweis. Sei $\nu_1, \ldots, \nu_n$ eine Basis von $\mathcal{V}$. Seien $\lambda_{i,j} \in \mathbb{F}_r$, so dass

$$(\pi_q(\nu_1), \ldots, \pi_q(\nu_n)) = (\nu_1, \ldots, \nu_n)(\lambda_{i,j})_{i,j}$$

erfüllt ist. Einerseits gilt dann

$$(t(x, \pi_q(\nu_1)), \ldots, t(x, \pi_q(\nu_n))) = (t(x, \nu_1), \ldots, t(x, \nu_n))(\lambda_{i,j})_{i,j} \tag{3.19}$$

und andererseits gilt

$$(t(x, \pi_q(\nu_1)), \ldots, t(x, \pi_q(\nu_n))) = (t(x, \nu_1), \ldots, t(x, \nu_n))qI_n. \tag{3.20}$$

Die Subtraktion (3.19)−(3.20) ergibt

$$(t(x, \nu_1), \ldots, t(x, \nu_n))((\lambda_{i,j})_{i,j} - qI_n) = 0$$

Das charakteristische Polynom von π_q auf $\mathcal{V}$ ist gegeben durch $\det((\lambda_{i,j})_{i,j} - tI_n)$. Damit ist q keine Nullstelle dieses Polynoms und es gilt $\det((\lambda_{i,j})_{i,j} - qI_n) \neq 0$. Demnach muss $(t(x, \nu_1), \ldots, t(x, \nu_n))$ trivial sein und wir erhalten die Behauptung. □

Aufgrund der Nichtdegeneriertheit der Tate Paarung muss zu jedem $x \in V_1$ ein $y \in V_q$ existieren, so dass $t_r(x, y) \neq 1$ gilt. Genauer gesagt, bedeutet dies, dass die Abbildung $V_1 \to \mathrm{Hom}(V_q, \mathbb{F}_r)$ injektiv ist und somit gilt $\dim(V_1) \leq \dim(V_q)$. Weiterhin können wir zeigen, dass $V_q \to \mathrm{Hom}(V_1, \mathbb{F}_r)$ ebenfalls injektiv ist.
Sei hierzu $Q \in V_q$ und $P \in V_1 \oplus V_q \oplus \mathcal{V}$.
Das Element P lässt sich schreiben als $P = P_1 \oplus P_q \oplus \mathcal{P}$ und wir erhalten

$$\begin{aligned} t_r(P, Q) &= t_r(P_1 \oplus P_q \oplus \mathcal{P}, Q) \\ &= t_r(P_1, Q) \underbrace{t_r(P_q, Q)}_{=1} \underbrace{t_r(\mathcal{P}, Q)}_{=1}. \end{aligned}$$

Wobei wir die Trivialität von $t_r(P_q, Q)$ aufgrund der Galois-Invarianz der Paarung erhalten:

$$t_r(P_q, Q)^q = t_r(\pi_q(P_q), \pi_q(Q)) = t_r(P_q, Q)^{q^2} \Leftrightarrow t_r(P_q, Q) = 1.$$

Analoges kann für $t_r(\mathcal{P}, Q)$ gezeigt werden und demnach muss $t_r(P_1, Q) \neq 1$ gelten. Damit gilt $\dim(V_1) = \dim(V_q)$
Ist das charakteristische Polynom χ von π_q auf der Jacobischen $\mathcal{J}_C$ quadratfrei modulo r, so gilt $\dim(V_1) = \dim(V_q) = 1$.

Die Wirkung eines Automorphismus $\alpha \in \mathrm{Aut}(C)$ auf $V_1 \oplus V_q \oplus \mathcal{V}$ beschreibt der folgende Satz.

Satz 6. *Sei das Geschlecht der betrachteten Kurve $g \geq 2$. Die Gruppe $Aut_{\mathbb{F}_{q^k}}(C)$ operiert treu auf jeder zyklischen Untergruppe der Ordnung r von* $\mathrm{Pic}_C(\mathbb{F}_{q^k})$.

Beweis. Die Gruppe $\mathrm{Aut}_{\mathbb{F}_{q^k}}(C)$ operiert treu auf $\mathrm{Pic}_C(\overline{\mathbb{F}_q})$. Daher existiert ein Monomorphismus $\iota : \mathrm{Aut}(C) \to \mathrm{End}(\mathcal{J}_C)$.
Sei $\alpha \in \mathrm{Aut}(C)$, dann ist die Ordnung von α gegeben als $\mathrm{ord}(\alpha) = O(g^4)$ und damit ist der Grad $\deg(\iota(\alpha) - 1)$ in $\mathrm{End}(\mathcal{J}_C)$ eine von r unabhängige Zahl, beschränkt durch die Kardinalität von $\ker(\iota(\alpha) - 1)$.
Würde α trivial auf einer zyklischen Untergruppe der Ordnung r operieren, so wäre $\deg(\iota(\alpha) - 1)$ durch r teilbar. Da r jedoch sehr gross ist, kann dies nicht möglich sein und wir erhalten die Behauptung. □

Satz 6 zeigt, dass eins für hinreichend großes r kein Eigenwert von α auf der direkten Summe $V_1 \oplus V_q \oplus \mathcal{V}$ sein kann. Da α von nicht durch r teilbarer, endlicher Ordnung ist, müssen alle Eigenwerte von α primitive Einheitswurzeln $\mu_{\mathrm{ord}(\alpha)}$ der Vielfachheit eins sein.
Nehmen wir $\alpha \in \mathrm{Aut}_{\mathbb{F}_q}(C)$ an, dann erhalten wir $\alpha(V_1) = V_1$ und $\alpha(V_1 \oplus V_q) = V_1 \oplus V_q$ ebenso wie auch $\pi_q(V_1 \oplus V_q) = V_1 \oplus V_q$. Damit gilt $\alpha \circ \pi_q = \pi_q \circ \alpha$ und α, π_q sind simultan diagonalisierbar auf $V_1 \oplus V_q$ über $\overline{\mathbb{F}}_r$.
Gilt weiterhin $\mathrm{ord}(\alpha) \mid (r-1)$, so sind die Eigenwerte von α modulo r in $\mathbb{F}_r$ enthalten und α ist diagonalisierbar auf V_1, V_q über $\mathbb{F}_r$.

Sei $[D_1] \in V_1$, $[D_2] \in V_q$ mit $D_1 \in \mathrm{Div}_C(\mathbb{F}_q)$, $D_2 \in \mathrm{Div}_C(\mathbb{F}_{q^k})$. Wir haben mit den vorangestellten Ausführungen gezeigt, dass wir Divisoren D_1 D_2 wählen können, so dass diese koprim sind, $t_r([D_1], [D_2]) \neq 1$ gilt und $[D_1]\,[D_2]$ Eigenvektoren von α sind. Dies erhalten wir durch die Auswahl von $[D_1]$ als einen beliebigen Eigenvektor und die Wahl von $[D_2]$ als einen der Vektoren der Eigenbasis von V_q bezüglich α.
Gilt $\alpha([D_1]) = \lambda[D_1]$ und $\alpha([D_2]) = \mu[D_2]$, so folgt einerseits

$$t_r(\alpha([D_1])\,\alpha([D_2])) = t_r([D_1]\,[D_2])$$

und andererseits

$$t_r(\alpha([D_1])\,\alpha([D_2])) = t_r(\lambda[D_1]\,\mu[D_2]) = t_r([D_1]\,[D_2])^{\lambda\mu}.$$

Es muss daher $\lambda\mu \equiv 1 \mod r$ gelten.

Zur Wahl geeigneter Parameter Wir haben ausgeführt unter welchen Annahmen die in Satz 5 definierte Paarung nichtdegeneriert und bilinear ist. Weiterhin haben wir die Existenz geeigneter Paramter gezeigt. Dieser Abschnitt gibt die konkrete Wahl der Parameter an und zeigt, dass diese die Annahmen erfüllen.

Um Forderungen zur Erfüllung von $\psi(D_2) = D_2$ zu stellen, formulieren wir den folgenden Satz.

Satz 7. *Sei C eine hyperelliptische Kurve des Geschlechts $g \geq 2$. Existiert ein Punkt im Unendlichen $O \in C$ mit $\psi(O) = O$ für eine rein inseperable Abbildung ψ, so wählen wir für die Reduktionsabbildung ρ für eine Divisorklasse $[D] \in V_q$ die Standardreduktion über*

$$\rho([D]) = \epsilon([D]) - \deg(\epsilon([D]))(O).$$

mit einem effektiven Divisor $\epsilon([D])$ minimalen Grades.
Dann gilt $\psi \circ \rho = \rho \circ \psi$ und damit $\psi(D) = D$.

Beweis. Seien die Voraussetzungen des Satzes erfüllt.
Dann ist $\dim(\epsilon([D])) = 1$ und die Äquivalenzklasse $[\epsilon([D])]$ enthält genau einen effektiven Divisor. Dieser ist gerade $\epsilon([D])$.
Demnach folgt

$$\begin{aligned}\rho(\psi([D])) &= \rho([D]) = \epsilon([D]) - \deg(\epsilon([D]))(O) \\ &= \psi(\epsilon([D])) - \deg(\epsilon([D]))(O) \\ &= \psi(\epsilon([D])) - \deg(\epsilon([D]))\psi(O) \\ &= \psi(\epsilon([D]) - \deg(\epsilon([D]))(O)) = \rho(\psi([D]))\end{aligned}$$

und wir erhalten $\psi \circ \rho = \rho \circ \psi$ auf V_q. Wegen der Einzigartigkeit des effektiven Divisors $\epsilon([D])$ in $[\epsilon([D])]$ folgt dann auch $\psi(D) = D$. □

Sei $\alpha \in \mathrm{Aut}_{\mathbb{F}_q}(C)$ von der Ordnung k. Dann hat α ebenfalls die Ordnung k auf V_q und es existiert ein j, so dass $\alpha^j(\pi_q^i([D_2])) = [D_2]$ und $\alpha^j(\pi_q^i([D_1])) = q^i[D_1]$.

Für die Wahl der Abbildung ψ gibt es die zwei folgenden möglichen Fälle:

1. Sei $\psi := \pi_q^i$. Diese Abbildung ist rein inseperabel vom Grad q^i.
   Dann gilt $\psi[D_1]) = [D_1]$ und $\psi([D_2]) = q^i[D_2]$. Weiterhin gilt wegen $\pi_q(O) = O$

   $$\begin{aligned}\psi([D_1]) &= \psi(\epsilon([D_1]) - \deg(\epsilon([D_1]))(O)) \\ &= \psi(\epsilon([D_1])) - \deg(\epsilon([D_1]))(O) \stackrel{!}{=} \epsilon([D_1]) - \deg(\epsilon([D_1])) = [D_1]\end{aligned}$$

   gerade die Gleichheit $\pi_q^i(D_1) = D_1$.
   Wobei wir verwenden, dass $\dim(\epsilon([D_1])) = 1$ ist und daher die Äquivalenzklasse $[\epsilon([D_1])]$ genau einen effektiven Divisor besitzt. Dieser ist gerade $\epsilon([D_1])$.

2. Sei $\psi := \alpha^j \circ \pi_q^i$. Dann gilt $\psi([D_1])) = q^i[D_1]$ und $\psi([D_2]) = [D_2]$. Gilt nun $\psi(O) = O$ für $O \in C$, so gilt gerade die Gleichheit $\psi(D_2) = D_2$. Wiederum nutzen wir hierfür, dass $\dim(\epsilon([D_2])) = 1$ gilt.

Wählen wir in beiden Fällen $s = q$ und $m = k$, so erhalten wir das Gewünschte.

Satz 8. *Seien die geeigneten Untergruppen, der Konstruktion zur Existenz der Parameter folgend, die Eigenräume* $\mathbb{G}_1 = \mathrm{Pic}^0_C(\mathbb{F}_q)[r]$ *und* $\mathbb{G}_2 = \mathrm{Pic}^0_C(\mathbb{F}_{q^k})[r] \cap \ker(\pi_q - q)$. *Die hyperelliptischen Ate Paarungen sind dann für die Parameter* $s = q$ *und* $m = k$ *mit* $c_s = \sum_{j=0}^{m-1} s^{m-1-j} q^{nj}$, $N = \gcd(q^k - 1, s^m - 1)$ *und* $LN = s^m - 1$ *gegeben als*

$$\begin{aligned} a : \mathbb{G}_2 \times \mathbb{G}_1 &\to \mu_r \\ ([D_2], [D_1]) &\mapsto f_{s,D_2}(D_1)^{c_s(q^k-1)/N} \end{aligned} \tag{3.21}$$

und, falls ein $\alpha \in Aut_{\mathbb{F}_q}(C)$ *von der Ordnung k existiert,*

$$\begin{aligned} \hat{a} : \mathbb{G}_1 \times \mathbb{G}_2 &\to \mu_r \\ ([D_1], [D_2]) &\mapsto f_{s,D_1}(D_2)^{c_s(q^k-1)/N}. \end{aligned} \tag{3.22}$$

Diese Paarungen sind nach Satz 5 bilinear und nichtdegeneriert, wenn r nicht L teilt.

Zur Konstruktion der Gruppen $\mathbb{G}_1$, $\mathbb{G}_2$ Um die Paarungen (3.21) bzw. (3.22) zu implementieren, müssen die beiden Untergruppen von $\mathrm{Pic}^0_C(\mathbb{F}_{q^k})[r]$ explizit konstruiert werden. Wir geben in diesem Abschnitt eine Möglichkeit an, diese Untergruppen zu erzeugen.

Wir wählen zunächst ein zufälliges Element $\tilde{Q} \in \mathrm{Pic}^0_C(\mathbb{F}_{q^k})[r] = V_1 \oplus V_q \oplus \mathcal{V}$.
Die normalisierte Spur von $\tilde{Q}$ ist definiert als $\mathrm{Tr}(\tilde{Q}) := c \sum_{i=0}^{k-1} \pi_q^i(\tilde{Q})$ für eine Konstante c mit $ck \equiv 1 \mod r$.
Damit gilt für die Verknüpfung der Spurabbildung $\mathrm{Tr} : V_1 \oplus V_q \oplus \mathcal{V} \to V_1$ mit der Inklusion $\iota : V_1 \to V_1 \oplus V_q \oplus \mathcal{V}$ die Identität $\mathrm{Tr} \circ \iota = \mathrm{id}_{V_1}$ auf V_1.

Als Erzeuger der Gruppe $\mathbb{G}_1$ können wir das Element $P := \mathrm{Tr}(\tilde{Q}) \in V_1 = \mathrm{Pic}^0_C(\mathbb{F}_q)[r]$ auswählen.

Setzen wir $Q' := \tilde{Q} - P$, so gilt $\tilde{Q} = P \oplus Q_q \oplus Q$ und $Q' = Q_q \oplus Q$. Gilt weiterhin für das Element $Q \in \mathcal{V}$ gerade

$$\pi_q(Q) = \zeta Q \text{ für ein } \zeta \neq 1 \text{ mit } \zeta^k \equiv 1 \mod r, \tag{3.23}$$

so kann der Erzeuger der Gruppe $\mathbb{G}_2$ als das Element

$$\begin{aligned} Q := \tilde{\mathrm{Tr}}(Q') := c \sum_{i=0}^{k-1} (q^{-1} \mod r)^i \underbrace{\pi_q^i(Q')}_{= \pi_q^i(Q_q) \oplus \pi_q^i(Q)} \\ = c \sum_{i=0}^{k-1} (q^{-1} \mod r)^i (q^i Q_q \oplus \zeta^i Q) \\ \overset{(*)}{=} c(kQ_q \oplus O) = Q_q \end{aligned}$$

gewählt werden. In $(*)$ nutzen wir aus, dass für jede k-te primitive Einheitswurzel $\xi \neq 1$ modulo r gilt :$\sum_{i=0}^{k-1} \xi^i \equiv 0 \mod r$.

Der Konstruktion nach können wir die Untergruppen als $\mathbb{G}_1 := \langle P \rangle$ und $\mathbb{G}_2 := \langle Q \rangle$ wählen.

Ist die Eigenschaft (3.23) nicht für das Element $Q \in \mathcal{V}$ erfüllt, so ist die Konstruktion der Gruppen $\mathbb{G}_1$, $\mathbb{G}_2$ komplizierter. Wir wollen die dann gegebene Vorgehensweise nur skizzenhaft angeben, da die zugrundeliegende mathematische Theorie in dieser Arbeit nicht behandelt wird.
In diesem Fall fassen wir $\mathrm{Pic}^0_C(\mathbb{F}_{q^k})[r] = V_1 \oplus V_q \oplus \mathcal{V}$ als $\mathbb{F}_r[X]$-Modul auf. Andererseits ist der $\mathbb{F}_r[X]$-Modul auch ein Vektorraum, wenn man die Multiplikation auf den Körper $\mathbb{F}_r \subset \mathbb{F}_r[X]$ einschränkt. Die Linksmultiplikation mit X induziert einen Vektorraumendomorphismus $\tilde{L} : V \to V, v \mapsto Xv$. Wir werden im Folgenden $Xv := \pi_q(v)$ betrachten.
Wir schreiben dann $V := \prod_i \mathbb{F}_r[X]/f_i(X)\mathbb{F}_r[X]$ mit irreduziblen f_i. Das Produkt der f_i ist dann $f = \prod_i f_i(X) = X^k - 1$ und die Spur eines Elementes $Q \in V$ ist dann $Tr(Q) = \frac{(X^k-1)}{(X-1)}Q$. Der Erzeuger der Gruppe $\mathbb{G}_1$ ist dann analog zu berechnen.
Für den Erzeuger der Gruppe $\mathbb{G}_2$ ist wiederum eine Reduktion über eine variierte Spurabbildung notwendig. Auf diesen Sachverhalt gehen wir an dieser Stelle jedoch nicht weiter ein, da dies über die hier behandelten mathematischen Zusammenhänge hinaus geht.

Die Ate Paarung haben wir jetzt in der elliptischen und hyperelliptischen Variante erklärt. Für den elliptischen Fall konnten wir eine Verallgemeinerung der Ate Paarung auf die Kongruenzen $S_i \equiv q^i \mod r$ aufzeigen. Auf hyperelliptischen Kurven konnten wir die Voraussetzungen für die Definition der hyperelliptischen Ate Paarung abschwächen. Diese abgeschwächte Formulierung haben wir in Satz 8 ausgeführt.

Wir setzen diesen Abschnitt über die direkten Abwandlungen der Tate Paarung mit der Berechnung dieser Paarung unter Verwendung effizient berechenbarer Endomorphismen fort. Den abschließenden Abschnitt dieses Kapitels widmen wir der systematischen Konstruktion neuer Paarungen. Da diese meist aus der Ate Paarung gewonnen werden, behandeln wir diese Thematik nicht im aktuellen Abschnitt, sondern trennen diese gedanklich voneinander.

3.2.4 Berechnung der Tate Paarung mit effizienten Endomorphismen

Neben der Idee der Berechnungsbeschleunigung aufgrund der Variation der Paarung stellen wir in dieser Arbeit einen weiteren Ansatz vor. Dieser basiert auf den Forschungsergebnissen im Bereich der schnellen Skalar-Punkt Multiplikation unter Verwendung effizient berechenbarer Endomorphismen. Diese Effizienzsteigerung haben wir schon in dem einführenden Abschnitt 1.5 diskutiert. Wir setzen uns mit der grundlegenden Idee auseinander und betrachten einige Aspekte der Praktikabilität. Detaillierte Angaben zu den Grundlagen und den Sicherheitsaspekten finden sich in [Sco05] und [Tak07].

Ausgangspunkt dieser Technik ist das von Boneh und Franklin entwickelte identitätsbasierte Verschlüsselungsschema (im Folgenden *IBE* Schema genannt) auf supersingulären elliptischen Kurven über dem Körper $\mathbb{F}_p$ [BF03].

Betrachten wir elliptische Kurven der Form

$$y^2 = x^3 + Ax \quad p \equiv 3 \mod 4, \tag{3.24}$$

$$y^2 = x^3 + B \quad p \equiv 2 \mod 3, \tag{3.25}$$

so sind diese für die Auswahl der Primzahl p stets supersingulär. Die Existenz von Verzerrungsabbildungen ist somit garantiert. Für Kurven der Form (3.24) ist eine Verzerrungsabbildung definiert als $\psi_1 : (x, y) \mapsto (-x, \alpha y)$, wobei $\alpha = \sqrt{-1}$ modulo p. Für Kurven der Form (3.25) erhalten wir $\psi_2 : (x, y) \mapsto (\beta x, y)$ für eine nichttriviale kubische Einheitswurzel β modulo p.

Betrachten wir diese Kurven jedoch für andere Primzahlen p mit

$$y^2 = x^3 + Ax \quad p \equiv 1 \mod 4, \tag{3.26}$$

$$y^2 = x^3 + B \quad p \equiv 1 \mod 3, \tag{3.27}$$

so verlieren die Kurven $y^2 = x^3 + Ax$ und $y^2 = x^3 + B$ ihre Supersingularität und damit auch den garantierten Besitz einer Verzerrungsabbildung. Die Abbildungen ψ_1, ψ_2 erweisen sich jedoch weiterhin als nutzbringend verwendbar, da diese effizient berechenbare Endomorphismen ϕ_1, ϕ_2 auf den ordinären Kurven (3.26), (3.27) beschreiben. Um die Wirkung dieser Endomorphismen zu erklären, betrachten wir beispielhaft Kurven der Form (3.27).

Zur Berechnung der klassischen Tate Paarung ist die skalare Multiplikation eines Punktes mit seiner Ordnung r, im Allgemeinen eine sehr große Primzahl, erforderlich. Um dies zu beschleunigen haben wir bereits in Abschnitt 1.5 einige Ansätze betrachtet.
Hinzukommen soll die Verwendung effizient berechenbarer Endomorphismen. Die Idee dieser Technik ist die Aufteilung der Skalarmultiplikation in zwei Teile, so dass der erste Teil leicht aus dem ursprünglich verwendeten Punkt errechnet und auf den zweiten Teil angewendet werden kann. Dieses Vorgehen wollen wir anhand einer Kurve der Form (3.27) mit gegebener Verzerrungsabbildung ϕ_2 erläutern.

Sei also ein Punkt $P = (x, y)$ einer solchen Kurve (3.27) der Ordnung r gegeben. Finden wir eine Zahl λ, so dass die Bedingung $\lambda^2 + \lambda + 1 \equiv 0 \mod r$ erfüllt ist, so trägt der Punkt $[\lambda]P$ die Koordinaten $(\beta x, y)$ für eine nichttriviale kubische Einheitswurzel β (modulo p). Ist beispielsweise r als ein großer Primteiler von $\lambda^2 + \lambda + 1$ für ein festes λ gegeben, so können wir von dieser Situation ausgehend $[\lambda]([\lambda]P + P) + P$ effizient unter Verwendung von ϕ_2 berechnen.

Betrachten wir das in [Sco05] gegebene Beispiel einer im Voraus gewählten Zahl λ mit kleinem Hamminggewicht.

Beispiel 3. Wählen wir $\lambda = 2^n$ mit $n = 87$ und die Punktordnung als den Primteiler $r = ((2^{87})^2 + 2^{87} + 1)/73$, dann wird zur Auswertung der Tate Paarung $2^n(2^nP + P) + P$ berechnet. Verwenden wir den Endomorphismus ϕ_2, so berechnen wir zunächst $2^nP + P$, dessen Wert wir sofort als $P' := \phi_2(P) + P = (\beta x, y) + (x, y) = (-(\beta + 1)x, -y)$ angeben können.
Somit sind alle weiteren in der Berechnung benötigten Schritte implizit bekannt und wir müssen $2^nP' + P$ berechnen. Verwenden wir die Berechnungen der ersten n Iterationen des Algorithmus innerhalb der zweiten n wieder, so können wir die Kosten dieser Iterationen mit jeweils einer Multiplikation im Körper angeben.
Den zu diesem Beispiel gehörigen Algorithmus 4 [Sco05] wollen wir zur Übersicht mit einer ausgelagerten Methode (Algorithmus 3) zur Auswertung der Geraden l angeben.

Algorithmus 3 : Auswertung der Funktion $l(\cdot, \cdot, \cdot, \cdot)$

Input : Punkte A, B und Q, Index i

1 $x_i, y_i \leftarrow A$;
2 $x_Q, y_Q \leftarrow Q$;
3 $m_i \leftarrow$ Tangentensteigung in $A + B$;
4 Speichere $-y_Q - y_i - m_i(\beta x_Q - x_i)$ in einem Arrayelement $s[i]$;
5 **return** $y_Q - y_i - m_i(x_Q - x_i)$;

Algorithmus 4 : Berechnung der Paarung $e(P, Q)$ für eine ordinäre Kurve (3.27), $k = 2$, $\lambda = 2^{87}$, $r = ((2^{87})^2 + 2^{87} + 1)/73$

Input : Punkte P und Q
Output : $e(P, Q)$

1 $A \leftarrow P$, $f \leftarrow 1$;
2 **for** $i = 1$ **to** 87 **do**
3 $\quad f \leftarrow f^2 \cdot l(A, A, Q, i)$;
4 **end**
5 $f \leftarrow f \cdot l(A, P, Q, -)$;
6 **for** $i = 1$ **to** 87 **do**
7 $\quad f \leftarrow f^2 \cdot s[i]$;
8 **end**
9 **return** $f^{\frac{(p+1)(p-1)}{r}}$;

Die Übertragung auf andere Hamminggewichte und die algorithmischen Ideen, sowie die Beeinflussbarkeit des Sicherheitslevels über diese Technik kann in den Artikeln [Sco05] und [Tak07] nachgelesen werden.

Der letzte Teil dieses Kapitels beinhaltet das systematische Suchen und Finden neuer

effizienter Konstruktionen der Ate und Ate$_i$ Paarungen und greift die Forschungsergebnisse dieses Gebietes der letzten Monate auf.

3.3 Konstruktionen optimierter Ate Paarungen

In den Abschnitten 3.1, 3.2.2 und 3.2.3 haben wir verschiedene Techniken und verwandte Paarungen eingeführt, die effiziente Möglichkeiten bereitstellen die Tate Paarung bzw. ihre verwandte Paarung zu berechnen.

An dieser Stelle wollen wir Paarungen betrachten, deren definierende Funktionen möglichst kleinen Grad besitzen. Parallel zur Bearbeitungszeit der vorliegenden Arbeit sind im Januar 2008 von Lee *et al.* [LLP08], Anfang März 2008 von F. Vercauteren [Ver08] und Mitte März 2008 von F. Heß [Hes08] Artikel erschienen, deren Ideen und Resultate wir vorstellen und im Kontext des thematischen Rahmens zur Konstruktion weiterer effizienter Paarungen dieser Arbeit verwerten.
Die Veröffentlichung von Lee *et al.* [LLP08] geht auf eine Verallgemeinerung der Ate und Ate$_i$ Paarungen ein, welche die Autoren als R-Ate Paarung bezeichnen. Eine kurze Abhandlung dieses Artikels werden wir in Abschnitt 3.3.1 angeben.
Einen weiteren Ansatz optimale Ate Paarungen zu konstruieren, macht die Arbeit von Vercauteren „Optimal Pairings“. Diese Idee behandeln wir in Abschnitt 3.3.2 und skizzieren das inhaltliche Vorgehen, um anschließend den Bogen zu den von F. Heß konstruierten Paarungsgittern zu schließen.

3.3.1 R-Ate Paarungen

Diesen Namen verdanken die R-Ate Paarungen ihrer Konstruktion als Quotient zweier Paarungen, wobei das R abgeleitet von dem englischen Wort *ratio* = Quotient ist. Die R-Ate Paarungen sind eine logische Konsequenz der Fortsetzung des Gedankens, dass die Ate$_i$ Paarungen aus der Variation der Parameter (q, r) entstehen und mit dieser Beobachtung ergeben sich für die Verfasser von [LLP08] durch Kombination der Werte r, q und $(S_i \equiv q^i \mod r)$ neue bilineare Paarungen.

Zunächst geben wir das Grundgerüst dieser Paarungen an und konkretisieren dieses in Theorem 4.

Definition 12. Für $A, B, a, b \in \mathbb{Z}$ mit $A = aB + b$ definieren wir die *R-Ate Paarung* als

$$R_{A,B}(D, E) = f_{a,BD}(E) \cdot f_{b,D}(E) \cdot G_{aBD,bD}(E). \tag{3.28}$$

Im Allgemeinen definiert uns das in (3.28) definierte $R_{A,B}$ noch keine nichtdegenerierte, bilineare Paarung. Dies kann aber durch geschickte Parameterwahl von A und B erreicht werden, wie das folgende Theorem zeigt. Wir formulieren dieses Theorem in der Form

für nichtsinguläre elliptische Kurven. Die Originalversion des Artikels [LLP08] behandelt den allgemeineren Fall der (hyper-)elliptischen Kurven.

Theorem 4. *Sei E eine nichtsinguläre Kurve über $\mathbb{F}_q$ und r ein großer Primteiler von $\#E(\mathbb{F}_q)$). Seien P und Q Punkte der Kurve E mit einer r teilenden Ordnung.*
Seien A, B ganze Zahlen, so dass

1. *$A = aB + b$ für $a, b \in \mathbb{Z}$*
2. *$f_{a,P}(Q)$ und $f_{B,P}(Q)$ nichtdegenerierte, bilineare Paarungen mit den folgenden Relationen zur Tate Paarung für $L_i, M_i \in \mathbb{Z}$, $i \in \{1, 2\}$ sind.*

$$e(P, Q)^{L_1} = f_{A,P}(Q)^{M_1}, \quad e(P, Q)^{L_2} = f_{B,P}(Q)^{M_2}$$

Sei weiterhin $M = lcm(M_1, M_2)$, $d_1 = \frac{M}{M_1}$, $d_2 = \frac{M}{M_2}$ und $l = d_1L_1 - ad_2L_2$. Teilt r nicht L, dann ist die R-Ate Paarung $R_{A,B}(P, Q)$ nichtdegeneriert und bilinear. Für das Verhältnis zur Tate Paarung gilt

$$e(P, Q)^L = R_{A,B}(P, Q)^M. \tag{3.29}$$

Beweis. Für den Beweis müssen einige leichte Rechnungen für den Divisor der Funktion $f_{aB,P}$ und die Umformung der Funktion $f_{A,P}$ angestellt werden, worauf wir an dieser Stelle jedoch verzichten und auf [LLP08] verweisen. □

Eine offensichtlich auftretende Fragestellung an dieser Stelle ist: „*Welche Tupel (A, B) definieren effizient berechenbare R-Ate Paarungen?*“
Als Antwort betrachten wir die in [LLP08, Korollar 3.3] angeführten Beispiele in einer zusammengestellten Tabelle.
Hierbei sei E eine nichtsinguläre Kurve über $\mathbb{F}_q$ mit Einbettungsgrad k bezüglich des Primteilers r von $\#E(\mathbb{F}_q)$. Analog zur Ate Paarung betrachten wir die speziellen Gruppen $\mathbb{G}_1 = E[r] \cap \ker(\pi_q - [1])$ beziehungsweise $\mathbb{G}_2 = E[r] \cap \ker(\pi_q - [q])$ und die Punkte $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$.
Weiterhin sei

- $S_i \equiv q^i \mod r$ für $1 \leq i < k$ und α_i sei die Ordnung von S_i modulo r, das heißt die kleinste Zahl für die $S_i^{\alpha_i} \equiv 1 \mod r$ gilt,
- $N_i = \gcd(S_i^{\alpha_i} - 1, q^k - 1)$ und $S_i^{\alpha_i} - 1 = N_iL_i$,
- $c_i = \sum_{j=0}^{\alpha_i - 1} S_i^{\alpha_i - 1 - j} q^{ij} \mod N_i$ und $M_i = \frac{(q^k - 1)}{N_i}$.

Für jede Wahl der Parameter (A, B) mit $A = aB + b$ erhalten wir nach Theorem 4 die Relation $e(Q, P)^L = R_{A,B}(Q, P)^M$. Die von Lee *et al.* [LLP08] gewählten Parameterpaare für die effiziente Konstrukttion der R-Ate Paarung geben wir in Tabelle 3.1 mit den zugehörigen Paarungen und deren definierenden Paarungsfunktionen an.

Tabelle 3.1: Effiziente R-Ate Paarungen [LLP08, Korollar 3.3]

• R-Ate Paarung • $L,\ M$
• $(\boldsymbol{q^i, r})$ mit $R_{q^i,r}(Q,P) = f_{S_i,Q}(P)$ • $L = iq^{i-1}\frac{(q^k-1)}{r} - akq^{k-1}, \quad M = kq^{k-1}\frac{(q^k-1)}{r}$ • $(\boldsymbol{q, S_1})$ für $q > S_1$ mit $R_{q,S_1}(Q,P) = f^q_{a,Q}(P) \cdot f_{b,Q}(P) \cdot G_{aS_1Q,bQ}(P)$ • $L = M_1 - aL_1, \quad M = c_1M_1$ • $(\boldsymbol{S_i, S_j})$ mit $R_{S_i,S_j}(Q,P) = f^{q^j}_{a,Q}(P) \cdot f_{b,Q}(P) \cdot G_{aS_jQ,bQ}(P)$ • $L = d_iM_1 - ad_jL_j, \quad M = \mathrm{lcm}(c_iM_i, c_j, M_j) = d_ic_iM_i = d_jc_jM_j$ • $(\boldsymbol{r, S_j})$ mit $R_{r,S_j}(Q,P) = f^{q^j}_{a,Q}(P) \cdot f_{b,Q}(P) \cdot G_{aS_jQ,bQ}(P)$ • $L = d_0 - ad_jL_j, \quad M = \mathrm{lcm}(\frac{(q^k-1)}{r}, c_j, M_j) = d_0\frac{(q^k-1)}{r} = d_jc_jM_j$

Den Beweis dieser Abhängigkeiten, einen entsprechenden Algorithmus zur Berechnung der R-Ate Paarung, Untersuchungen von Effizienzkriterien und einige konkrete Beispiele sind ebenfalls in [LLP08] zu finden. Wir wenden uns dem nicht weiter zu. Stattdessen beschäftigen wir uns als nächstes mit der Konstruktion optimaler Ate Paarungen von F. Vercauteren.

3.3.2 Optimale Ate Paarungen

Das Konzept der optimalen Paarungen verspricht eine Berechnung über nur $\log_2 \frac{r}{\varphi(k)}$ Iterationen des Miller-Algorithmus und einen Algorithmus, um zu jeder parametrisierten Familie von paarungsfreundlichen elliptischen Kurven optimale Ate Paarungen zu konstruieren.
Sei r die Untergruppenordnung und $\varphi(k)$ die *Euler-Phi Funktion* ausgewertet für den Einbettungsgrad k.
Die Euler-Phi Funktion gibt die Anzahl der, zu einer Zahl n, teilerfremden Zahlen $z \leq n$ an und ist definiert als $\varphi(n) := \mid \{1 \leq z \leq n \mid \gcd(z,n) = 1\} \mid$.

Bevor wir die Vorgehensweise zur Konstruktion angeben, halten wir zunächst fest, dass zu Ate Paarungen mit rationalen Miller-Funktionen $f_{S_i,Q}$ für $S_i \equiv q^i \mod r$

$$r \mid \Phi_{k/d}(S_i), \quad \text{mit } d = \gcd(i,k) \tag{3.30}$$

gilt. Mit Φ_n, für $n \in \mathbb{N} \setminus \{0\}$, bezeichnen wir das *n-te Kreisteilungspolynom*, dass für einen Körper K mit $\mathrm{char}(K) \nmid n$ definiert ist als $\Phi_n := \prod_{j=1}^{\varphi(n)} (x - \zeta_j)$, wobei $\zeta_1, \ldots, \zeta_{\varphi(n)}$

die n-ten primitiven Einheitswurzeln in $\overline{K}$ sind [Bos06]. Der Grad dieses Polynoms ist $\varphi(n)$.
Die Gleichung (3.30) liefert uns implizit einen Minimalwert von ungefähr $r^{1/\varphi(\frac{k}{d})}$ für S_i. Für den Fall, dass der größte gemeinsame Teiler der Zahlen i und k gleich eins ist, erhalten wir die kleinste untere Schranke von $r^{1/\varphi(k)}$.

Um den Begriff der Optimalität einer Paarung in Abhängigkeit von der Laufzeit des *Miller*-Algorithmus zu spezifizieren, betrachten wir die folgende Definition.

Definition 13. Sei $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ eine nichtdegenerierte, bilineare Paarung mit Gruppenkardinalitäten $\mid \mathbb{G}_1 \mid = \mid \mathbb{G}_2 \mid = \mid \mathbb{G}_T \mid = r$, wobei der Grundkörper von $\mathbb{G}_T$ der Körper $\mathbb{F}_{q^k}$ ist.
Dann heißt $e(\cdot,\cdot)$ eine *optimale Paarung*, falls die Paarung in $\log_2 \frac{r}{\varphi(k)} + \epsilon(k)$ Miller-Iterationen mit $\epsilon(k) \leq \log_2 k$ berechenbar ist.

Eine der Hauptideen zur Reduktion der Anzahl der Schleifendurchläufe des *Miller*-Algorithmus haben wir in den Abschnitten 3.2.2, 3.2.3 als das Ausnutzen von effizient berechenbaren Endomorphismen diskutiert. Diese Endomorphismen können z. B. Potenzen des Frobenius-Endomorphismus π_q^i für $i = 0, \ldots, k-1$ sein, welche zur Zerlegung eines Vielfachen λ der Zahl r in eine Summe dieser Frobenius-Potenzen $\lambda = mr = \sum_{i=0}^{l} c_i q^i$ genutzt werden.
Da $\Phi_k(q)$ kongruent zu Null modulo r ist, wirken höhere Potenzen $j \geq \varphi(k)$ in $\mathbb{G}_2$ wie Linearkombinationen mit kleinen Koeffizienten der $\varphi(k)$ Endomorphismen π_q^i für $i = 0, \ldots, \varphi(k) - 1$. Aus diesem Blickwinkel betrachtet der Autor von [Ver08] nur diese letzteren Potenzen als „unabhängig“, da sich die Größe der Koeffizienten einer Linearkombination der π_q^j für $j \geq \varphi(k)$ nur wenig modulo der Reduktion bezüglich Φ_k verändert.
Wie man aus diesen Frobenius-Entwicklungen bilineare Paarungen erhält, zeigt Theorem 1 in [Ver08], welches wir an dieser Stelle zitieren.

Theorem 5. *Sei $\lambda = mr$ mit $r \nmid m$ und wir schreiben $\lambda = \sum_{i=0}^{l} c_i q^i$. Dann definiert*

$$a_{[c_0,\ldots,c_l]} : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r$$

$$(Q,P) \mapsto \left(\prod_{i=0}^{l} f_{c_i,Q}^{q^i}(P) \cdot \prod_{i=0}^{l-1} \frac{l_{[s_{i+1}]Q,[c_i q^i]Q}(P)}{v_{[s_i]Q}(P)} \right)^{\frac{(q^k-1)}{r}} \tag{3.31}$$

mit $s_i = \sum_{j=1}^{l} c_j q^j$ eine bilineare Paarung. Gilt weiterhin

$$mkq^{k-1} \not\equiv \frac{(q^k-1)}{r} \cdot \sum_{i=0}^{l} i c_i q^{i-1} \mod r,$$

so ist die in Gleichung (3.31) definierte Paarung nichtdegeneriert.

Beweis. Siehe [Ver08]. □

Der Algorithmus zur genauen Konstruktion dieser Paarungen basiert auf dem Suchen und Finden von kurzen Vektoren in dem $\varphi(k)$-dimensionalen Gitter L, welches aufgespannt wird durch die Zeilen der Matrix

$$\begin{pmatrix} r & 0 & 0 & \dots & 0 \\ -q & 1 & 0 & \dots & 0 \\ -q^2 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \ddots & \\ -q^{\varphi(k)-1} & 0 & \dots & 0 & 1 \end{pmatrix}. \tag{3.32}$$

Das Volumen dieses Gitters ist r und nach dem ersten Satz von Minkowski existiert ein kurzer Vektor $v \in L$ mit $\| v \|_\infty \leq r^{1/\varphi(k)}$, wobei die Norm $\| \cdot \|_\infty$ gegeben ist durch $\| v \|_\infty = \max_i | v_i |$.

Beispiel 4. Für eine spezielle Wahl elliptischer Kurven wollen wir ein Beispiel angeben. Diese nennen wir *Barreto-Nährig Kurve* mit den folgenden Eigenschaften.

Sei E also eine Barreto-Nährig Kurve. Diese haben die Form $E : y^2 = x^3 + b$ über einem Körper $\mathbb{F}_q$ für eine Primzahl q. Die Parameter q, r und t sind durch Polynome in $\mathbb{Z}[x]$ bestimmt, es gilt $r := \#E(\mathbb{F}_q) = q + 1 - t$ und der Einbettungsgrad dieser Kurven ist 12.

$$q = 36x^4 + 36x^3 + 24x^2 + 6x + 1 \quad \text{prim} \tag{3.33}$$

$$r = 36x^4 + 36x^3 + 18x^2 + 6x + 1 \quad \text{prim} \tag{3.34}$$

$$t = 6x^2 + 1 \tag{3.35}$$

Betrachten wir das nach (3.32) definierte Gitter für die Parametrisierung der Kurve, so sind die bezüglich der euklidischen Norm kürzesten Vektoren gegeben durch

$$V_1(x) = [x + 1, x, x, -2x] \quad \text{bzw.} \quad V_2(x) = [2x, x + 1, -x, x].$$

Die $c_i(x)$ sind hier sehr einfach und die Funktionen $f_{c_i(x),Q}$ können jeweils durch $f_{x,Q}$ dargestellt werden. Suchen wir alternativ nach kürzesten Vektoren mit einer minimalen Anzahl an Koeffizienten der Größe x so gilt

$$W(x) = [6x + 2, 1, -1, 1].$$

Die Paarung $a_{[6x+2,1,-1,1]}$ geben wir an als

$$a_{[6x+2,1,-1,1]}(Q, P) = (f_{6x+2,Q} l_{Q_3,-Q_2} l_{-Q_2+Q_3,Q_1} l_{Q_1-Q_2+Q_3,[6x+2]Q})^{\frac{(q^{12}-1)}{r}}(P) \tag{3.36}$$

mit $Q_i = [q^i]Q$.

Wir wollen an dieser Stelle nicht weiter auf diese Thematik eingehen und verweisen für die detaillierte Diskussion und Angabe von Beispielen für verschiedene Familien paarungsfreundlicher elliptischer Kurven auf [Ver08]. Auf das Beipiel 4 gehen wir in Abschnitt 3.3.4 ein weiteres Mal ein.

Stattdessen beschäftigen wir uns eingehender mit der Konstruktion von Paarungsgittern und arbeiten die Inhalte von [Hes08] auf. Anschließend stellen wir ein weiteres erarbeitetes Resultat der vorliegenden Arbeit vor.

3.3.3 Paarungsfunktionen kleinsten Grades

Wir haben die verschiedenen Abwandlungen der klassischen Tate Paarung betrachtet und gehen mit diesem Abschnitt auf den heutigen Stand der Forschung ein. Wir haben die Idee der Konstruktion von Paarungen aus Produkten von Tate und Ate Paarungen nach den Ausführungen von [LLP08] diskutiert und sind auf die Ansätze in [Ver08] zur Konstruktion optimaler Ate Paarungen eingegangen. In diesem Abschnitt beschäftigt uns die konstruktive und systematische Weiterentwicklung von Paarungen unter Verwendung von Gittern [Hes08]. Damit schaffen wir einen geeigneten mathematischen Rahmen, welcher im Wesentlichen alle auf der Tate Paarung basierenden, bekannten Paarungsfunktionen umfaßt.

Sei s eine ganze Zahl. Für ein Polynom $h = \sum_{i=0}^{d} h_i x^i \in \mathbb{Z}[x]$ mit $h(s) \equiv 0 \mod r$ sei die Funktion $f_{s,h,R}$ für $R \in E(\mathbb{F}_{q^k})[r]$, die eindeutig bestimmte normierte Funktion, deren Divisor

$$(f_{s,h,R}) = \sum_{i=0}^{d} h_i(([s^i]R) - (O)) \tag{3.37}$$

erfüllt. Die Einsnorm $\| \cdot \|_1$ definieren wir als $\| h \|_1 = \sum_{i=0}^{d} | h_i |$. Ist die Zahl d kleiner als die Ordnung der Zahl s modulo r, so können wir den Grad der Funktion $f_{s,h,R}$ in die folgenden Schranken setzen

$$\frac{\| h \|_1}{2} \leq \deg(f_{s,h,R}) \leq \| h \|_1 \ . \tag{3.38}$$

Mit dem nachfolgenden Theorem 6 schaffen wir den Rahmen, in welchem wir uns in Abschnitt 3.3.4 bewegen werden.

Theorem 6. *[Hes08] Sei k die Ordnung der Zahl s modulo r. Dann existiert ein $h \in \mathbb{Z}[x]$ mit $h(s) \equiv 0 \mod r$, $\deg(h) \leq \varphi(k) - 1$ und $\| h \|_1 = O(r^{1/\varphi(k)})$, so dass*

$$\begin{aligned} a_{s,h} : \mathbb{G}_2 \times \mathbb{G}_1 &\to \mu_r \\ (Q, P) &\mapsto f_{s,h,Q}^{\frac{(q^k-1)}{r}}(P) \end{aligned}$$

eine nichtdegenerierte, bilineare Paarung ist. Das Polynom h kann effizient berechnet werden und die entsprechende Relation zur Tate Paarung ist

$$a_{s,h}(Q, P) = e(Q, P)^{\frac{h(s)}{r}}.$$

Zu jedem Polynom $h \in \mathbb{Z}[x]$ mit $\deg(h) \leq k - 1$ für das $a_{s,h}$ eine nichtdegenerierte, bilineare Paarung definiert, erfüllt $\| h \|_1 \geq r^{1/\varphi(k)}$.

Beweis. Ist in [Hes08] zu finden. □

Der genannte Artikel [Hes08] geht noch über den Inhalt des zitierten Theorems hinaus auf erweiterte Ate Paarungen ein, welche eine etwas größere Menge an möglichen Werten für die Zahl s zulassen.
Wir wollen es bei der Angabe des Theorems 6 belassen und fahren mit der Konstruktion einer konkreten Paarung auf speziellen elliptischen Kurven, welche einen Einbettungsgrad $k = 12$ zulassen, fort.

3.3.4 Konstruktion von Paarungen auf Barreto-Nährig Kurven

Dieser Abschnitt bildet den Abschluss unserer theoretischen Betrachtungen von Paarungen (hyper-)elliptischer Kurven. Die angegebenen Paarungen (3.42) und (3.43) sind erarbeitete Ergebnisse der vorliegenden Arbeit. Inhaltlich beschäftigen wir uns mit der konstruktiven Suche nach Paarungen, welche sich als Linearkombinationen der Miller-Funktionen der Tate, Ate und der Ate_i Paarungen ergeben und effizient berechenbar sind.

Wir verwenden zur Konstruktion sogenannte *Barreto-Nährig* Kurven (BN-Kurven), da für diese speziellen Kurven der Einbettungsgrad $k = 12$ erreicht werden kann und deren Parameter q, r und t als Polynome mit ganzzahligen Koeffizienten (3.39), (3.40) und (3.41) beschreibbar sind. (Vgl. [BN05])
Für die notwendigen Berechnungen und experimentellen Implementierungen verwenden wir in dieser Arbeit das Computeralgebrasystem **Magma**.

Die BN-Kurven haben die Form $E : y^2 = x^3 + b$ und wir betrachten diese über einem Körper $\mathbb{F}_q$ für eine Primzahl q. Aufgrund der folgenden Parametrisierung gilt für die Ordnung einer BN-Kurve stets $r := \#E(\mathbb{F}_q) = q + 1 - t$. Die Parameter q, r und t sind durch Polynome in $\mathbb{Z}[x]$ bestimmt.

$$q = 36x^4 + 36x^3 + 24x^2 + 6x + 1 \quad \text{sei prim} \tag{3.39}$$

$$r = 36x^4 + 36x^3 + 18x^2 + 6x + 1 \quad \text{sei prim} \tag{3.40}$$

$$t = 6x^2 + 1 \tag{3.41}$$

Im Folgenden schreiben wir teilweise q, r und t in den Formen (3.39), (3.40) und (3.41). In diesem Fall sei x stets eine fixe, ganz, positive Zahl.

Für den Rest dieses Abschnittes seien die Zahlen S_i analog zu den Ate_i Paarungen als $S_i \equiv q^i \bmod r$ für $i = 1, \ldots, k-1$ und gegebene q und r definiert. Weiterhin bezeichne die Abbildung π_q den Frobenius-Endomorphismus auf der Kurve E.

Für diese parametrisierten Kurven wollen wir nichtdegenerierte, bilineare Abbildungen auf den Gruppen $\mathbb{G}_1 := E[r] \cap \ker(\pi_q - [1])$ und $\mathbb{G}_2 := E[r] \cap \ker(\pi_q - [q])$ konstruieren und diese auf $\mathbb{G}_2 \times \mathbb{G}_1$ betrachten. Für einen Punkt P aus $\mathbb{G}_1$ gilt stets $\pi_q(P) = P$. Die Punkte Q aus $\mathbb{G}_2$ erfüllen $\pi_q(Q) = [q]Q$.

Die Definition der konstruierten Paarungen geben wir getrennt nach den Restklassen der Zahl q modulo $\varphi(k)$ an und klassifizieren damit die folgenden Paarungen.
Für den Einbettungsgrad $k = 12$ betrachten wir q modulo $\varphi(k) = |\ \{1, 5, 7, 11\}\ | = 4$.

Der erste Fall sei $q \equiv 1 \bmod 4$.

$$e_1(Q,P) := g_1(P)^{(q^k-1)/r} \quad \text{mit} \tag{3.42}$$
$$(g_1) := (O) - a(Q) - a(\pi^2 Q) - b(\pi^3 Q) - a(\pi^5 Q) + a(\pi^6 Q) + a(\pi^8 Q) + a(\pi^9 Q) + a(\pi^{11} Q).$$

Als zweiten Fall geben wir $q \equiv 3 \bmod 4$ an.

$$e_3(Q,P) := g_3(P)^{(q^k-1)/r} \quad \text{mit} \tag{3.43}$$
$$(g_3) := -(O) - a(Q) - b(\pi^2 Q) - b(\pi^3 Q) - a(\pi^5 Q) + b(\pi^6 Q) + a(\pi^8 Q) + b(\pi^9 Q) + b(\pi^{11} Q).$$

Auf die Größe und exakte Bestimmung der Zahlen a und b gehen wir im Abschnitt über die Konstruktion dieser Paarungen ein.

Wegen der gegebenen Parametrisierung ist $q = 36x^4 + 36x^3 + 24x^2 + 6x + 1 \in \mathbb{Z}[x]$, welches für ein fixes x kongruent ist zu $2x^2 + 1 \pmod 4$ und wir erhalten somit als Divisionsreste stets 1 oder 3. Es gilt

$$36x^4 + 36x^3 + 24x^2 + 6x + 1 \equiv 2x^2 + 1 \mod \varphi(k) \equiv \begin{cases} 1 & \text{, falls } 2x^2 \equiv 0 \mod \varphi(k) \\ 3 & \text{, falls } 2x^2 \equiv 2 \mod \varphi(k) \end{cases}.$$

Daher genügt es die Paarungen in diese zwei Klassen zu unterteilen und wir wollen mit der genauen Vorgehensweise zur Konstruktion dieser Paarungen fortfahren.

Zur Konstruktion der Paarungen

Ausgehend von den bekannten Paarungsfunktionen der Tate und Ate$_i$ Paarungen, wollen wir Linearkombinationen dieser Paarungen bilden, mit dem Ziel eine nichtdegenerierte Paarung zu konstruieren. Inwiefern wir in diesem Kontext von Linearkombinationen sprechen können und was genau wir damit meinen, erklären wir in den nächsten Absätzen.

Zur Erinnerung und Festlegung der Notation rekapitulieren wir die Definitionen der Tate und Ate$_i$ Paarungen.

1. Die klassische Tate Paarung haben wir in Definition 9 als Funktion $f_{r,P}$ mit Divisor $(f_{r,P}) = r(P) - r(O)$ erklärt. Wir verwenden hier eine an die Ate Paarung angepasste Version $f_0 := f_{r,Q}$ mit $(f_{r,Q}) = r(Q) - r(O)$.

2. Die Ate$_i$ Paarungen haben wir mittels der Funktionen $f_i := f_{S_i,Q}$ mit Divisor $(f_{S_i,Q}) = S_i(Q) - ([S_i]Q) - (S_i - 1)(O)$ für alle $i = 1, \ldots, k-1$ eingeführt. Wobei wir durch die geschickte Gruppenwahl die Eigenschaft $[S_i]Q = \pi^i Q$ erhalten.

Um den Rechenaufwand zu minimieren sollen die Koeffizienten des Divisors der paarungsdefinierenden Funktion möglichst klein sein.
Das Problem geeignete Funktionen zu finden, deren Divisoren kleine ganzzahlige Koeffizienten besitzen, transformieren wir auf das Problem, kurze Vektoren innerhalb eines Gitters zu finden. Wir greifen dazu die Idee, auf den Paarungen basierende, Gitter zu konstruieren, welchen wir in Abschnitt 3.3.2 vorgestellt haben, auf.
Ein wichtiger Aspekt an dieser Stelle ist, dass im Gegensatz zu der Konstruktion der Gitter in [Ver08], alle Potenzen des Frobenius-Endomorphismus verwendet werden. Die Idee ist über ein höherdimensionales Gitter, das durch sehr speziell gewählte Vektoren erzeugt wird, kleinere Koeffizienten zu erreichen.

Untersuchen wir die Parametrisierung der BN-Kurven und betrachten die Relationen der S_i modulo der Kurvenordnung r in Abhängigkeit einer fixen positiven ganzen Zahl x näher, so stellen wir die folgende Regelmäßigkeit fest.

$$\begin{array}{lllllll}
q(x) & \bmod r(x) & \equiv & 6x^2 & \equiv & -q^7(x) & \bmod r(x), \\
q^2(x) & \bmod r(x) & \equiv & -36x^3 - 18x^2 - 6x - 1 & \equiv & -q^8(x) & \bmod r(x), \\
q^3(x) & \bmod r(x) & \equiv & -36x^3 - 24x^2 - 12x - 3 & \equiv & -q^9(x) & \bmod r(x), \\
q^4(x) & \bmod r(x) & \equiv & -36x^3 - 18x^2 - 6x - 2 & \equiv & -q^{10}(x) & \bmod r(x), \\
q^5(x) & \bmod r(x) & \equiv & -36x^3 - 30x^2 - 12x - 3 & \equiv & -q^{11}(x) & \bmod r(x), \\
q^6(x) & \bmod r(x) & \equiv & -1 & \equiv & -q^{12}(x) & \bmod r(x),
\end{array}$$

Interpretieren wir die Koeffizienten der Hauptdivisoren zu den f_i als Vektoreinträge $V_{i,j}$ mit $j = 1, 2, \ldots, k+1$ eines jeweiligen Vektors V_i, so können wir über diese Vektoren ein Gitter $\Lambda = \sum_{i=0}^{k-1} \mathbb{Z}V_i$ definieren. Dieses Gitter wird dann aus den folgenden zeilenweise gelesenen Vektoren V_i mit $i = 0, \ldots k-1$ erzeugt.

$$\begin{array}{lcccccccc}
 & & (O) & (Q) & (\pi(Q)) & (\pi^2(Q)) & \ldots & (\pi^{10}(Q)) & (\pi^{11}(Q)) & \\
V_0 & (& -r, & r, & 0, & 0, & \ldots, & 0, & 0 &) \\
V_1 & (& -(S_1-1), & S_1, & -1, & 0, & \ldots, & 0, & 0 &) \\
V_2 & (& -(S_2-1), & S_2, & 0, & -1, & & 0, & 0 &) \\
V_3 & (& -(S_3-1), & S_3, & 0, & 0, & \ddots & 0, & 0 &) \\
\vdots & & \vdots & \vdots & \vdots & \vdots & & & \vdots & \\
V_{k-2} & (& -(S_{10}-1), & S_{10}, & 0, & 0, & \ldots, & -1, & 0 &) \\
V_{k-1} & (& -(S_{11}-1), & S_{11}, & 0, & 0, & \ldots, & 0, & -1 &)
\end{array}$$

Für $\delta \in (1/4, 1]$ und $\eta \in [1/2, \sqrt{\delta})$ nennen wir d geordnete, linear unabhängige Vektoren $v_1, v_2, \ldots, v_d$ eines Gitters Λ dann (δ, η)-LLL-reduziert, wenn die folgenden zwei Bedingungen gelten.

1. Die $v_1, v_2, \ldots, v_d$ sind längenreduziert, das heißt für die Einträge der Transformationsmatrix des Gram-Schmidt-Verfahren $\mu_{i,j} = \frac{\langle v_j, v_i^* \rangle}{\langle v_i^*, v_i^* \rangle} = \frac{\langle v_j, v_i^* \rangle}{\|v_i^*\|^2}$ gilt $-\frac{1}{2} < \mu_{i,j} \leq \frac{1}{2}$ für $1 \leq i < j \leq d$ und $v_i^* \neq 0$. Hierbei ist v_i^* der i-te Vektor der Gram-Schmidt-Orthogonalisierung.
2. Für jedes $1 \leq i < d$ gilt $\delta \parallel v_i^* \parallel^2 \leq \parallel v_{i+1}^* + \mu_{i,i+1} v_{i+1}^* \parallel^2$.

Letztere Bedingung ist dabei äquivalent zu $(\delta - \mu_{i,i+1}^2) \parallel v_i^* \parallel^2 \leq \parallel v_{i+1}^* \parallel^2$.
Eine (δ, η)-LLL-reduzierte Basis $(b_1, b_2, \ldots, b_d)$ eines Gitters Λ besitzt die nachfolgenden Eigenschaften.

1. $\parallel b_1 \parallel \leq (\delta - \eta^2)^4 (\det L)^d$,

2. $\parallel b_1 \parallel \leq (\delta - \eta^2)^2 \min_{b \in L \setminus \{0\}} \parallel b \parallel$,

3. $\prod_{i=1}^{d} \parallel b_i \parallel \leq (\delta - \eta^2)^4 (\det L)$,

4. $\forall j < i, \parallel b_j^* \parallel \leq (\delta - \eta^2)^2 \parallel b_i^* \parallel$.

Die klassische LLL-Reduktion bezieht sich stets auf den Fall $\delta = 3/4$ und $\eta = 1/2$, da dies die ursprünglich angenommenen Zahlen in [LLL82] sind. Die Gitterbasis sollte jedoch, je näher δ und η an 1 bzw. $1/2$ sind, stärker reduziert sein. Die, von dem verwendeten Computeralgebrasystem **Magma**, per Default benutzten Werte sind $\delta = 0.75$ und $\eta = 0.501$, so dass $(\delta - \eta^2)^4 < 1.190$ und $(\delta - \eta^2)^2 < 1.416$ gilt.

Die Idee des Ansatzes ist es Elemente einer LLL-reduzierten Basis eines Gitters Λ und die zugehörgen Funktionen zu betrachten. Die relevanten, in dieser Arbeit betrachteten Vektoren der LLL-reduzierten Basis sind für $q \equiv 1 \mod \varphi(k)$ von der Form (i) bzw. für $q \equiv 3 \mod \varphi(k)$ von der Form (ii). Um diesen Abschnitt überschaubar zu halten, betrachten wir nie alle möglichen Vektoren, sondern uns stets an die in (i),(ii) exemplarisch gewählten halten. Die Vektoreinträge sind für $q \equiv 1 \mod \varphi(k)$ in der Menge

$$\left\{0, \pm\frac{1}{2}x, \pm(\frac{1}{2}x + 1)\right\}$$

und für $q \equiv 3 \mod \varphi(k)$ in

$$\left\{0, \pm\frac{1}{2}(x-1), \pm\frac{1}{2}(x+1)\right\},$$

für die in der Parametrisierung der Kurve erhaltene fixe Zahl $x \in \mathbb{N} \setminus \{0\}$, enthalten.
Ähnliche Vektoren und daüber folgend ähnliche Paarungen können über analoge Kon-

struktionen für $x \in \mathbb{Z} \setminus \mathbb{N}$ gefunden werden.

$$(i) \quad \begin{pmatrix} 1 \\ -\frac{1}{2}x \\ 0 \\ -\frac{1}{2}x \\ -(\frac{1}{2}x+1) \\ 0 \\ -\frac{1}{2}x \\ \frac{1}{2}x \\ 0 \\ \frac{1}{2}x \\ \frac{1}{2}x \\ 0 \\ \frac{1}{2}x \end{pmatrix} \quad \text{und } (ii) \quad \begin{pmatrix} -1 \\ -\frac{1}{2}(x-1) \\ 0 \\ -\frac{1}{2}(x+1) \\ -\frac{1}{2}(x+1) \\ 0 \\ -\frac{1}{2}(x-1) \\ \frac{1}{2}(x+1) \\ 0 \\ \frac{1}{2}(x-1) \\ \frac{1}{2}(x+1) \\ 0 \\ \frac{1}{2}(x+1) \end{pmatrix}$$

Wollen wir die zu diesen Vektoren korrespondierenden Hauptdivisoren untersuchen, so müssen wir zunächst sicherstellen, dass der Grad der jeweiligen Divisoren null ist. Zu (i) zeigen wir dies durch die Rechnung

$$1 - \frac{1}{2}x - \frac{1}{2}x - (\frac{1}{2}x+1) - \frac{1}{2}x + \frac{1}{2}x + \frac{1}{2}x + \frac{1}{2}x + \frac{1}{2}x = 0. \checkmark$$

Mit einer analogen Rechnung erhalten wir dasselbe Ergebnis für (ii).

Um die Notation noch einfacher zu gestalten, ersetzen wir die Vektoreinträge und somit die Koeffizienten der Hauptdivisoren durch die Buchstaben a und b.
Für den Fall $q \equiv 1 \mod 4$ definieren wir $a := \frac{1}{2}x$ und $b := \frac{1}{2}x + 1$. Im Fall $q \equiv 3 \mod 4$ definieren wir die Werte als $a := \frac{1}{2}(x-1)$ und $b := \frac{1}{2}(x+1)$.
Eine in beiden Fällen gültige, weitere mögliche Beschreibung der Werte von a und b geben wir als $a = \left\lfloor \sqrt{\frac{t}{24}} \right\rfloor$ und $b = \left\lceil \sqrt{\frac{t}{24}} \right\rceil$ für die Spur des Frobenius t an.

Die Herangehensweise zur Konstruktion dieser Paarung und die der Werte a und b haben wir erläutert und geben im nächsten Abschnitt einen konkreten Algorithmus zur Berechnung der Paarung e_1 an.
Abschließend wenden wir uns den mathematischen Betrachtungen bezüglich der Bilinearität, der Nichtdegeneriert und des Grades der Funktionen g_1, g_2 zu.

Der Algorithmus

Die Idee des Algorithmus ist die Schrittweise Vereinfachung und Zusammenfassung des aus der Konstruktion gegebenen Hauptdivisors. Sukzessive erhalten wir rationale Funktionen, die zusammengesetzt die gesuchte Funktion g_i mit $i = 1, 3$ ergeben.

Für jede der Paarungen erhalten wir aus der Konstruktion einen Hauptdivisor der Form $D = \sum \alpha_i(P_i) = \sum \alpha_i((P_i) - (\mathcal{O}))$, wobei jeder dieser Summanden linear äquivalent zu

einem eindeutig bestimmten Divisor der Form $(P_i') - (\mathcal{O})$ ist. Wir bezeichnen diese Darstellung $(P_i') - (\mathcal{O}) + (h_i)$ als *kanonische Form*. Damit gilt

$$D = \sum \alpha_i(P_i) = \sum \alpha_i((P_i) - (\mathcal{O})) \overset{Miller}{=} \sum (\alpha_i P_i) - (\mathcal{O}) + (h_i). \tag{3.44}$$

Die Addition zweier solcher Divisoren $D_1 := (R) - (\mathcal{O}) + (r)$ und $D_2 := (S) - (\mathcal{O}) + (s)$ für rationale Funktionen $r,\ s$ mit $R + S = T$ ist definiert als

$$\begin{aligned} D_1 + D_2 &= (R) + (S) - 2 * (\mathcal{O}) + (r \cdot s) = (T) - (\mathcal{O}) + (l) - (v) + (r \cdot s) \\ &= (T) - (\mathcal{O}) + (\frac{r \cdot s \cdot l}{v}). \end{aligned}$$

Hierbei beschreibt $l_{R,S} : l_1 x + l_2 y + l_3 = 0$ die Gerade durch die Punkte R und S. Die Vertikale $v_T : x - x_3 = 0$ verläuft durch $T = (x_3, y_3)$ und $-T$. Für die Berechnung genügt es demnach den Punkt T und die rationale Funktion $\frac{r \cdot s \cdot l}{v}$ abzuspeichern.

Für die divisordefinierende Funktion g_1 berechnen wir das Folgende.

$$\begin{aligned} (g_1) = \ & (\mathcal{O}) - a(Q) - a(\pi^2 Q) - b(\pi^3 Q) - a(\pi^5 Q) + a(\pi^6 Q) + a(\pi^8 Q) + a(\pi^9 Q) + a(\pi^{11} Q) \\ = \ & a[[(\pi^6 Q) + (\pi^8 Q) + (\pi^9 Q) + (\pi^{11} Q) - 4(\mathcal{O})] - [(Q) + (\pi^2 Q) + (\pi^3 Q) + (\pi^5 Q) - 4(\mathcal{O})]] \\ & - ((\pi^3 Q) - (\mathcal{O})) \\ \overset{(*)}{=} \ & a[[(-Q - \pi^2 Q - \pi^3 Q - \pi^5 Q) - (\mathcal{O}) + (f_-)] - [(Q + \pi^2 Q + \pi^3 Q + \pi^5 Q) - (\mathcal{O}) + (f_+)]] \\ & - ((\pi^3 Q) - (\mathcal{O})) \\ = \ & a[(-(Q + \pi^2 Q + \pi^3 Q + \pi^5 Q)) - (\underbrace{Q + \pi^2 Q + \pi^3 Q + \pi^5 Q}_{=:P_s}) + (f_-) - (f_+)] - ((\pi^3 Q) - (\mathcal{O})) \\ = \ & a[(\underbrace{[-2]P_s}_{=:\tilde{P}}) - (\mathcal{O}) + (\underbrace{\frac{f_-}{f_+}\frac{l_{P_s,P_s}}{v_{[2]P_s}}}_{=:f})] - ((\pi^3 Q) - (\mathcal{O})) \\ = \ & a((\tilde{P}) - (\mathcal{O})) + (f^a) - ((\pi^3 Q) - (\mathcal{O})) \end{aligned} \tag{3.45}$$

Die Hilfsfunktionen f_- und f_+ seien definiert als

$$f_+ = \frac{l_{Q,\pi^2 Q}}{v_{Q+\pi^2 Q}} \frac{l_{\pi^3 Q,\pi^5 Q}}{v_{\pi^3 Q+\pi^5 Q}} \frac{l_{Q+\pi^2 Q,\pi^3 Q+\pi^5 Q}}{v_{Q+\pi^2 Q+\pi^3 Q+\pi^5 Q}},$$

$$f_- = \frac{l_{-Q,-\pi^2 Q}}{v_{-Q-\pi^2 Q}} \frac{l_{-\pi^3 Q,-\pi^5 Q}}{v_{-\pi^3 Q-\pi^5 Q}} \frac{l_{-Q-\pi^2 Q,-\pi^3 Q-\pi^5 Q}}{v_{-Q-\pi^2 Q-\pi^3 Q-\pi^5 Q}}.$$

Und wir bestimmen

$$f := \frac{f_-}{f_+}\frac{l_{P_s,P_s}}{v_{[2]P_s}} = \frac{l_{-Q,-\pi^2 Q}}{l_{Q,\pi^2 Q}} \frac{l_{-\pi^3 Q,-\pi^5 Q}}{l_{\pi^3 Q,\pi^5 Q}} \frac{l_{-Q-\pi^2 Q,-\pi^3 Q-\pi^5 Q}}{l_{Q+\pi^2 Q,\pi^3 Q+\pi^5 Q}} \frac{l_{P_s,P_s}}{v_{[2]P_s}}. \tag{3.46}$$

In $(*)$ geht in die Rechnung ein, dass für $j = 6, \ldots k - 1$ das Folgende gilt

$$\pi_q^j Q = [q^j]Q = [S_j]Q = [-S_{j-6}]Q = [-q^{j-6}]Q = -\pi_q^{j-6} Q.$$

Um die Bestimmung der Funktion g_1 zu vollenden, berechnen wir mit Hilfe des *Miller*-Algorithmus die Funktion h, so dass $a((\tilde{P}) - (O)) + (f^a) = ([a]\tilde{P}) - (O) + (f^a h)$ gilt. Diesen Übergang kennzeichnen wir mit $(**)$. Dann erhalten wir als Umformungsschritte für die Gleichung (3.45)

$$\begin{aligned} & a((\tilde{P}) - (O)) + (f^a) - ((\pi^3 Q) - (O)) \\ \overset{(**)}{=} \; & ([a]\tilde{P}) - (O) + (f^a h) - ((\pi^3 Q) - (O)) \\ \overset{(***)}{=} \; & (f^a h \frac{v_{[a]\tilde{P}}}{1}). \end{aligned}$$

Die Gleichheit $(***)$ erhalten wir aus $[a]\tilde{P} - \pi_q^3 Q = O$. Die Gerade $l_{[a]\tilde{P},-\pi^3 Q}$ im Zähler entspricht somit der Vertikalen $v_{[a]\tilde{P}}$. Diese verläuft durch den Punkte $[a]\tilde{P}$ und dem Negativen dieses Punktes $\hat{=} -\pi^3 Q$. Die Vertikale des Nenners wird zu eins gesetzt.

Für den Fall e_1 spezifizieren wir die Berechnung in Algorithmus 5. In jedem Schritt, in dem Geraden konstruiert werden, evaluieren wir diese aus Effizienzgründen sofort am Punkt P.

Algorithmus 5 : Berechnung der Paarung e_1

Input : Binärdarstellung von $a = \sum_{j=0}^{l} b_j 2^j$ mit $b_l = 1$, Punkte $\pi^i Q \in E(\mathbb{F}_q^k)$ mit $i = 0, \ldots k/2$ und $P \in E(\mathbb{F}_q^k)$

Output : Die Paarung $e_1(Q, P) = g_1(P)^{(q^k-1)/r}$

1 $\tilde{P} \leftarrow -(Q + \pi^2 Q + pi^3 Q + pi^5 Q)$;

2 $f_Z \leftarrow \left(l_{-Q,-\pi^2 Q}(P) \cdot l_{-\pi^3 Q,-\pi^5 Q}(P) \cdot l_{-(Q,+\pi^2 Q),-(\pi^3 Q+\pi^5 Q)}(P) \cdot l_{\tilde{P},\tilde{P}}(P)\right)^a$;

3 $f_N \leftarrow \left(l_{Q,\pi^2 Q}(P) \cdot l_{\pi^3 Q,\pi^5 Q}(P) \cdot l_{(Q,+\pi^2 Q),(\pi^3 Q+\pi^5 Q)}(P) \cdot v_{[2]P\tilde{P}}(P)\right)^a$;

`/* Verwende Algorithmus 2 für` $a(([2]\tilde{P}) - (Oh)) = ([2a]\tilde{P}) - (Oh) + (h)$ `*/`

`/*` T `ist dann der Punkt` $[2a]\tilde{P}$ `*/`

4 $h, T \leftarrow$ *Miller*-Algorithmus$([2]\tilde{P}, a)$;

5 $f \leftarrow \frac{f_Z \cdot h}{f_N}$;

`/* Durchführen des letzten Schrittes */`

6 $f \leftarrow \left(f \cdot v_{T-\pi^3 Q}(P)\right)^{\frac{(q^k-1)}{r}}$;

Laufzeitbetrachtungen Für die Analyse des Aufwands von Algorithmus 5 betrachten wir diesen zeilenweise. Hierfür vernachlässigen wir die Dauer der einzelnen arithmetischen Operationen und nehmen an, dass diese in konstanter Zeit $O(1)$ durchführbar sind.

Die Zeilen 1 bis 3 berechnen wir mit jeweiligem Aufwand in $O(1)$. Der Aufwand des durchlaufenen Miller-Algorithmus in Zeile 4 wird über die Länge der Binärdarstellung von a ermittelt und wir erhalten $O(\log_2 a)$. Für das in den Parametrisierungen (3.39),

(3.40) und (3.41) fixierte $x \in \mathbb{N} \setminus \{0\}$ erhalten wir über die Relation $a = \frac{1}{2}x$ einen Gesamtaufwand von $O(\log_2 x)$.
Betrachten wir in direktem Vergleich die klassische Tate Paarung mit einer Millerschleifenlänge von $\log_2 r$ und Gesamtaufwand von $O(\log_2 r) = O(\log_2 x^4)$ ist die Beschleunigung klar erkennbar.

Analog zu der Vorgehensweise zur Konstruktion von g_1, geben wir die Funktion g_3 an.

$$\begin{aligned}
(g_3) = \quad & -(O) - a(Q) - b(\pi^2 Q) - b(\pi^3 Q) - a(\pi^5 Q) + b(\pi^6 Q) + a(\pi^8 Q) + b(\pi^9 Q) + b(\pi^{11} Q) \\
\overset{(*)}{=} \quad & a[[(-Q - \pi^2 Q - \pi^3 Q - \pi^5 Q) - (O) + (f_-)] - [(Q + \pi^2 Q + \pi^3 Q + \pi^5 Q) - (O) + (f_+)]] \\
& + ((-Q) + (-\pi^3 Q) + (-\pi^5 Q) - 3(O)) - ((\pi^2 Q) + (\pi^3 Q) - 2(O)) \\
& \vdots \\
= \quad & a((\tilde{P}) - (O)) + (f^a) \\
& + ((-Q - \pi^3 Q - \pi^5 Q) - (O) + (h_-)) - ((\pi^2 Q + \pi^3 Q) - (O) + (h_+)) \\
\overset{(**)}{=} \quad & ([a]\tilde{P}) - (O) + (f^a h) \\
& + ((\underbrace{-(Q + \pi^2 Q + [2]\pi^3 Q + \pi^5 Q)}_{P'}) - (O) + (\frac{h_-}{h_+} \frac{l_{-(Q+\pi^3 Q+\pi^5 Q),-(\pi^2 Q+\pi^3 Q)}}{v_{-(Q+\pi^2 Q+[2]\pi^3 Q+\pi^5 Q)}})) \\
\overset{(***)}{=} \quad & (f^a h \frac{v_{[a]\tilde{P}}}{1}),
\end{aligned}$$

wobei die Funktion f wie in (3.46) definiert ist. Die Funktionen h_- und h_+ sind wie folgt beschrieben.

$$h_+ = \frac{l_{\pi^2 Q,\pi^3 Q}}{v_{\pi^2 Q+\pi^3 Q}},$$

$$h_- = \frac{l_{-Q,-\pi^3 Q}}{v_{-(Q+\pi^3 Q)}} \frac{l_{-(Q+\pi^3 Q),-\pi^5 Q}}{v_{-(Q+\pi^3 Q+\pi^5 Q)}}.$$

Die Übergänge $(*)$, $(**)$ und $(***)$ folgen mit analogen Argumenten wie in der Berechnung von g_1.

Mathematische Betrachtungen

Im Folgenden zeigen wir unter Verwendung des in Abschnitt 3.3.3 angegeben Theorems 6, dass die in dem vorangegangenen Abschnitt konstruierten Paarungen e_1 und e_3 stets bilinear und nichtdegeneriert sind.
Weiterhin geben wir einige Ausführungen bezüglich des Grades der paarungsdefinierenden Funktionen an.

Bilinearität und Nichtdegeneriertheit Um diese Eigenschaften für die über e_1, e_3 erklärten Paarungen zu zeigen halten wir zunächst das Folgende fest:

- Sei $s \equiv q \mod r$. Dann hat s die Ordnung $k \mod r$.
- Sei $h_1(X) = aX^{11} + aX^9 + aX^8 + aX^6 - aX^5 - bX^3 - aX^2 - a \in \mathbb{Z}[X]$.
  Dann gilt $h_1(s) \equiv 0 \mod r$.
  Beweis.

$$\begin{aligned}
h_1(s) = \; & as^{11} + as^9 + as^8 + as^6 - as^5 - bs^3 - as^2 - a \\
\overset{(*)}{\equiv} \; & a(-s^5) + a(-s^3) + a(-s^2) + a(-s^0) \\
& + a(-s^5) + b(-s^3) + a(-s^2) + a(-s^0) \mod r \\
\equiv \; & x(-s^5) + (x+1)(-s^3) + x(-s^2) - x \mod r \\
\equiv \; & x(36x^3 + 30x^2 + 12x + 3) + (x+1)(36x^3 + 24x^2 + 12x + 3) \\
& + x(36x^3 + 18x^2 + 6x + 1) - x \mod r \\
\equiv \; & 3 \cdot (\underbrace{36x^4 + 36x^3 + 18x^2 + 6x + 1}_{= r \text{ siehe (3.40)}}) \mod r \\
\equiv \; & 0 \mod r
\end{aligned}$$

  Wobei wir in $(*)$ die schon in der Konstruktion aufgezeigten und im Algorithmus verwendeten Kongruenzen modulo r

$$\pi_q^j Q = [q^j]Q \overset{s \equiv q \bmod r}{=} [s^j]Q = [-s^{j-6}]Q \overset{s \equiv q \bmod r}{=} [-q^{j-6}]Q = -\pi_q^{j-6} Q$$

  für $j = 6, \ldots k-1$ ausnutzen. □
- Es gilt $\| h_1 \|_1 = O(r^{1/\varphi(k)})$.
  Beweis. Für die Einsnorm $\| h_1 \|_1 = \sum_{i=0}^{k-1} | h_{1_i} |$ des Polynoms h_1 gilt
  $\| h_1 \|_1 = 8a + 1 = 4x + 1 \in O(\sqrt[4]{36x^4 + 36x^3 + 18x^2 + 6x + 1}) = O(r^{1/\varphi(k)})$. Wobei die Aussage

$$\exists_{c>0} \exists_{x_0 \in \mathbb{N}} \forall_{x \in \mathbb{N}, x > x_0} : 4x + 1 \leq c \cdot r^{1/\varphi(k)}$$

  durch Nachrechnen gezeigt werden kann. □

Unter diesen Voraussetzungen können wir Theorem 6 anwenden, da die Aussage des Theorems erfüllt ist, solange der Grad des Polynoms echt kleiner als die Ordnung der Zahl s ist. Somit erhalten wir die Bilinearität und Nichtdegeneriertheit der Paarung e_1. Analog kann für e_3 mit $s \equiv q \mod r$ gezeigt werden, dass für das Polynom

$$h_3(X) = bX^{11} + bX^9 + aX^8 + bX^6 - aX^5 - bX^3 - bX^2 - a \in \mathbb{Z}[X]$$

die Kongruenz $h_3(s) \equiv 0 \mod r$ erfüllt ist und $\| h_3 \|_1 = O(r^{1/\varphi(k)})$ gilt. Nach Anwendung des Theorems 6 erhalten wir ebenfalls die Bilinearität und Nichtdegeneriertheit der Paarung e_3.

Diese Ergebnisse halten wir in den beiden folgenden Sätzen fest.
Für den Fall $q \equiv 1 \mod \varphi(k)$ formulieren wir Satz 9.

Satz 9. *Sei E eine BN-Kurve mit den in (3.39), (3.40) und (3.41) für ein fixes $x \in \mathbb{N} \setminus \{0\}$ gegebenen Parametern q, r und t. Sei $s \equiv q \mod r$ und k der Einbettungsgrad bzgl. r. Dann ist für $h_1(X) = aX^{11} + aX^9 + aX^8 + aX^6 - aX^5 - bX^3 - aX^2 - a \in \mathbb{Z}[X]$*

$$\begin{aligned} e_1 : \mathbb{G}_2 \times \mathbb{G}_1 &\to \mu_r \\ (Q, P) &\mapsto g_1^{\frac{(q^k-1)}{r}}(P) \end{aligned}$$

eine nichtdegenerierte, bilineare Paarung.
Die entsprechende Relation zur Tate Paarung ist $e_1(Q, P) = e(Q, P)^{\frac{h_1(s)}{r}}$.

Beweis. Folgt aus den vorangegangenen Ausführungen bzw. aus Theorem 6. □

Analog zu Satz 9 formulieren wir für den Fall $q \equiv 3 \mod \varphi(k)$ Satz 10.

Satz 10. *Sei E eine BN-Kurve mit den in (3.39), (3.40) und (3.41) für ein fixes $x \in \mathbb{N} \setminus \{0\}$ gegebenen Parametern q, r und t. Sei $s \equiv q \mod r$ und k der Einbettungsgrad bzgl. r. Dann ist für $h_3(X) = bX^{11} + bX^9 + aX^8 + bX^6 - aX^5 - bX^3 - bX^2 - a \in \mathbb{Z}[X]$*

$$\begin{aligned} e_3 : \mathbb{G}_2 \times \mathbb{G}_1 &\to \mu_r \\ (Q, P) &\mapsto g_3^{\frac{(q^k-1)}{r}}(P) \end{aligned}$$

eine nichtdegenerierte, bilineare Paarung.
Die entsprechende Relation zur Tate Paarung ist $e_3(Q, P) = e(Q, P)^{\frac{h_3(s)}{r}}$.

Beweis. Folgt aus den vorangegangenen Ausführungen bzw. aus Theorem 6. □

Grad der Funktion Nach Abschnitt 3.3.3 können wir den Grad einer rationalen Funktion $f_{s,h,R}$ mit $(f_{s,h,R}) = \sum_{i=0}^{d} h_i(([s^i]R) - (O))$ beschränken durch

$$\frac{\| h \|_1}{2} \leq \deg(f_{s,h,R}) \leq \| h \|_1$$

für ein Polynom $h = \sum_{i=0}^{d} h_i X^i \in \mathbb{Z}[X]$ mit $h(s) \equiv 0 \mod r$ und $d < \mathrm{ord}(s) \mod r$. Betrachten wir dies für die Divisoren (g_1), (g_3) bzw. für die rationalen Funktionen g_1 und $_3$, so erhalten wir die Funktionen h_1, h_3 mit

$$\begin{aligned} h_1(X) &= aX^{11} + aX^9 + aX^8 + aX^6 - aX^5 - bX^3 - aX^2 - a \\ &= a(X^{11} + X^9 + X^8 + X^6 - X^5 - X^3 - X^2 - 1) - X^3 \end{aligned}$$

und

$$\begin{aligned} h_3(X) &= bX^{11} + bX^9 + aX^8 + bX^6 - aX^5 - bX^3 - bX^2 - a \\ &= a(X^{11} + X^9 + X^8 + X^6 - X^5 - X^3 - X^2 - 1) + X^{11} + X^9 + X^6 - X^3 - X^2 \end{aligned}$$

Wir rechnen leicht nach, dass die Divisoren der so definierten Funktionen $(f_{s,h_i,R})$ denen der Funktionen g_1 und g_3 entsprechen und in beiden Fällen gilt für $s \equiv q \mod r$ die Kongruenz $h_i(s) \equiv 0 \mod r$.
Da $\deg h_i < \mathrm{ord}(s) = k$ gilt, sind die folgenden Schranken an den Grad der Funktionen g_i gegeben.

$$\frac{\| h_i \|_1}{2} \leq \deg (f_{s,h_i,R}) \leq \| h_i \|_1 \tag{3.47}$$

Berechnen wir die Einsnorm von h_1 und h_3 so erhalten wir

$$\| h_1 \|_1 = 7a + b = 7\frac{1}{2}x + \frac{1}{2}x + 1 = 4x + 1$$

und

$$\| h_3 \|_1 = 3a + 5b = 3\frac{1}{2}(x-1) + 5\frac{1}{2}(x+1) = 2(2x+1)$$

Setzen wir diese Ergebnisse in (3.47) ein, gilt für den Grad der Funktionen

$$\frac{4x+1}{2} = 2x + \frac{1}{2} \leq \deg (f_{s,h_1,R}) \leq 4x + 1$$

und

$$\frac{2(2x+1)}{2} = 2x + 1 \leq \deg (f_{s,h_3,R}) \leq 2(2x+1).$$

Vergleichen wir diese Ergebnisse mit denen des Beispiels 4 aus [Ver08] in Abschnitt 3.3.2 zu denselben Kurven so erhalten wir die folgende Gegenüberstellung.

Tabelle 3.2: Tabelle der Paarungen zu BN-Kurven

Paarung	Polynom h	$\| h \|_1$
$a_{[6x+2,1,-1,1]}(Q,P)$	$X^3 - X^2 + X + (6x+2)$	$6x+3$
$e_1(Q,P)$	$aX^{11} + aX^9 + aX^8 + aX^6 - aX^5 - bX^3 - aX^2 - a$	$4x+1$
$e_3(Q,P)$	$bX^{11} + bX^9 + aX^8 + bX^6 - aX^5 - bX^3 - bX^2 - a$	$4x+2$

Beispiele

Bevor wir einige Beispiele der Berechnung der vorgestellten Paarungen e_1, e_2 inklusive zugehöriger Zeitmessungen angeben, müssen wir auf einige Besonderheiten innerhalb der **Magma**-Implementierung hinweisen.

Sei E eine Barreto-Nährig Kurve. Dann ist E von der Form $E : y^2 = x^3 + b$ über dem betrachteten Körper $\mathbb{F}_q$. Aufgrund der Parametrisierung der Zahl q in (3.39) gilt dann stets die Kongruenz $q \equiv 1 \mod 6$.
Für $\lambda \in \mathbb{F}_{q^2} \setminus (\mathbb{F}_{q^2})^3$ und $\mu \in \mathbb{F}_{q^2} \setminus (\mathbb{F}_{q^2})^2$ definiert die Kurve

$$E'\mu y^2 = \lambda x^3 + b$$

einen Twist vom Grad 6 und der Isomoprohismus, welcher den Twist E' in die Kurve E transformiert, können wir angeben als

$$\psi : E' \to E$$
$$(x, y) \mapsto (\lambda^{\frac{1}{3}} x, \mu^{\frac{1}{2}} y).$$

In Abschnitt 3.2.3 haben wir für eine ordinäre Kurve mit Einbettungsgrad $k = de$, die einen Twist über $\mathbb{F}_{q^e}$ vom Grad $d > 1$ besitzt, festgehalten, dass der Twist E' und ψ so gewählt werden können, so dass für die r-Torsionsgruppe des Twists über $\mathbb{F}_{q^e}$ $E'(\mathbb{F}_{q^e})[r] = \langle \psi^{-1}(Q) \rangle$ gilt.

Für Barreto-Nährig Kurven ist dies erfüllt. Zur Implementierung werden wir dies in sofern nutzen, dass wir den Körper $\mathbb{F}_{q^k}$ als Erweiterungskörper von $\mathbb{F}_q$ betrachten.
Die Konstruktion von $\mathbb{F}_{q^k}$ erfolgt dann über die folgenden Schritte:

1. Bilde die Körpererweiterung $\mathbb{F}_{q^2}$ und den zugehörigen univariaten Polynomring $\mathbb{F}_{q^2}[T]$.
2. Wähle $\lambda \in \mathbb{F}_{q^2}$, so dass $T^3 - \lambda \in \mathbb{F}_{q^2}[T]$ irreduzibel ist.
3. Bilde die Körpererweiterung $\mathbb{F}_{q^2}[\lambda]$ als $\mathbb{F}_{q^2}[T]/(T^3 - \lambda)$.
4. Wähle $\mu \in \mathbb{F}_{q^2}$, so dass $T^2 - \mu \in \mathbb{F}_{q^2}[T]$ irreduzibel ist.
5. Bilde Körpererweiterung $\mathbb{F}_{q^2}[\lambda, \mu]$ als $\mathbb{F}_{q^2}[T]/(T^2 - \mu)$.

Die Körpererweiterung $\mathbb{F}_{q^2}[\lambda, \mu]$ ist eine Körpererweiterung vom Grad 12 und entspricht damit $\mathbb{F}_{q^{12}}$. Über dem so konstruierten Körper sind die Punkte von der beschriebenen Form und die Berechnungen werden effizient ausgeführt.

Die in Tabelle 3.3 aufgeführten Beispiele geben die betrachteten BN-Kurven, die zugehörigen Parameter q, r, t und a an. Die angegebenen Laufzeiten werden mit den **Magma**-Befehlen `t := Cputime()` und `T := Cputime(t)` gemessen. `T` ist dann die seit `t` vergangene Cpuzeit in Sekunden.
Die Dauer der Kurvengenerierung ist nicht in den aufgeführten Zeiten enthalten. Es wird demnach die reine Rechenzeit der Paarungen gemessen.
Wir geben die Laufzeiten der Paarungsberechnungen für die folgenden Paarungen an:

- Die in dieser Arbeit konstruierten Paarungen $e_{q \mod \varphi(k)}(Q, P)$.
- Die Ate Paarung $a_S(Q, P)$ für $S \equiv q \mod r$.
- Die Tate Paarung $e(Q, P)$ und die klassischen Tate Paarung $e(P, Q)$.

Tabelle 3.3: Beispiele

$E : y^2 = x^3 + 6 \qquad q \equiv 1 \mod \varphi(k)$
q = 400648821621216256817698227300650550 1
r = 400648821621216256617536087791813050 1
t = 2001621395088375001
a = 288792125

$e_1(Q,P) : 0.190s / 0.130s$
$a_S(Q,P) : 0.260s / 0.150s$
$e(Q,P) : 0.360s / 0.120s \qquad e(P,Q) : 0.190s / 0.140s$

$E : y^2 = x^3 + 89 \qquad q \equiv 1 \mod \varphi(k)$
q = 98171843164767892965498361394767941927 61
r = 98171843164767892964507544342327837711 61
t = 99081705244010421601
a = 2031847530

$e_1(Q,P) : 0.250s / 0.170s$
$a_S(Q,P) : 0.340s / 0.190s$
$e(Q,P) : 0.480s / 0.170s \qquad e(P,Q) : 0.250s / 0.180s$

$E : y^2 = x^3 + 5 \qquad q \equiv 3 \mod \varphi(k)$
q = 124745987369944395442377822565283520 2203
r = 124745987369944395438845882767969178 7109
t = 35319397973143415095
a = 1213112353

$e_3(Q,P) : 0.250s / 0.180s$
$a_S(Q,P) : 0.350s / 0.200s$
$e(Q,P) : 0.470s / 0.180s \qquad e(P,Q) : 0.250s / 0.180s$

$E : y^2 = x^3 + 10 \qquad q \equiv 3 \mod \varphi(k)$
q = 439224231051039915852347663569466 23
r = 439224231051039913756579955303785 69
t = 209576770826568055
a = 93447126

$e_3(Q, P) : 0.190s / 0.130s$
$a_S(Q, P) : 0.240s / 0.140s$
$e(Q, P) : 0.350s / 0.130s \qquad e(P, Q) : 0.180s / 0.130s$

$E : y^2 = x^3 + 33 \qquad q \equiv 1 \mod \varphi(k)$
q = 122430571203180774650754349922350316381229331419543372175634002648898033576892 1
r = 122430571203180774650754349922350316381118683070616160082939895668278856075852 1
t = 110648348927212092694106980619177501040 1
a = 6789954250189886610

$e_1(Q, P) : 0.770s / 0.540s$
$a_S(Q, P) : 0.980s / 0.560s$
$e(Q, P) : 1.500s / 0.550s \qquad e(P, Q) : 0.770s / 0.560s$

$E : y^2 = x^3 + 5 \qquad q \equiv 1 \mod \varphi(k)$
q = 152328599816610099494549315160162948925899097139446605482151519066690950976 73
r = 152328599816610099494549315160162948924664882410087852044571644555769537592 09
t = 123421472935875343757987451092141338465
a = 2267721625845672293

$e_1(Q, P) : 0.640s / 0.450s$
$a_S(Q, P) : 0.860s / 0.480s$
$e(Q, P) : 1.220s / 0.440s \qquad e(P, Q) : 0.640s / 0.450s$

$E : y^2 = x^3 + 29 \qquad q \equiv 3 \mod \varphi(k)$
q = 443581609616126695091920250503401046555797354701807061714284168240477008556 59
r = 443581609616126695091920250503401046553691216981675430115626607713972702558 93
t = 210613772013163159865756052650430599767
a = 2962359504496677109

$e_3(Q, P) : 0.700s / 0.490s$
$a_S(Q, P) : 0.960s / 0.540s$
$e(Q, P) : 1.290s / 0.490s \qquad e(P, Q) : 0.690s / 0.490s$

$E : y^2 = x^3 + 7 \qquad q \equiv 3 \mod \varphi(k)$

q = 30629314290035893756735448254777661626501293400375920591073205764 62

r = 30629314290035893756735448254777661626483792167765034038504591157 52

t = 17501232610886552568614607101139754453 51

a = 8539426359267971092

$e_3(Q,P) : 0.750s / 0.530s$
$a_S(Q,P) : 1.020s / 0.580s$
$e(Q,P) : 1.420s / 0.530s \qquad e(P,Q) : 0.750s / 0.530s$

$E : y^2 = x^3 + 24 \qquad q \equiv 1 \mod \varphi(k)$

q = 13418208637671446577607541783118349524895754690697830067429998845217284390106947182951294545223051544080033868948929557016057545722021096245663744789040369 3

r = 13418208637671446577607541783118349524895754690697830067429998845217284390106910552078198655948878826420848661746385478217994600107527736442014212438718075 7

t = 36630873095889274172717659185207202544078798062945614493359803649532350322293 7

a = 12354296333645985617743004583381801369 6

$e_1(Q,P) : 2.740s / 1.960s$
$a_S(Q,P) : 3.800s / 2.170s$
$e(Q,P) : 5.170s / 1.920s \qquad e(P,Q) : 2.780s / 2.000s$

$E : y^2 = x^3 + 5 \qquad q \equiv 1 \mod \varphi(k)$

q = 25575313489536774704600969169757073828922338783129641967217077210728360267849725261299479072954006341522256114617917606534905503946922564633589459064418803 3

r = 25575313489536774704600969169757073828922338783129641967217077210728360267849674689258300634472171884760687109011663151988271242485773448286945815948761996 9

t = 50572041178438481834456761569005606254454546634261461149116346643643115656806 5

a = 14516088944460683288233518192467640320 0

$e_1(Q,P) : 2.750s / 1.970s$
$a_S(Q,P) : 3.660s / 2.170s$
$e(Q,P) : 5.230s / 1.960s \qquad e(P,Q) : 2.770s / 2.000s$

$E : y^2 = x^3 + 28 \qquad q \equiv 3 \mod \varphi(k)$

q = 387905190822916803129636454363320715384325893308557389025482772769605449537274
18489028611731404492866168318111880683582671791418252005737603772316807309072 3

r = 387905190822916803129636454363320715384325893308557389025482772769605449537273
56206993415142267732570235056820166889393765899260075329470116270561465509618 9

t = 62282035196589136760295933261291713794188905892158176676267487501755341799453 5

a = 161092668978382771667248663867529625600

$e_3(Q, P)$: 2.740s/ 1.960s
$a_S(Q, P)$: 3.750s/ 2.150s
$e(Q, P)$: 5.180s/ 1.960s $\qquad$ $e(P, Q)$: 2.740s/ 1.970s

---

$E : y^2 = x^3 + 6 \qquad q \equiv 3 \mod \varphi(k)$

q = 813863557176573011869180754994917801565676662839323870686046343349537455385174
29275047761767150087296223815551658024804609399983757997450713182304090609823

r = 813863557176573011869180754994917801565676662839323870686046343349537455385171
43992108002556695496253257276368489613491879538384390426452956111689708732649

t = 28528293975921045459104296653918316841131272986159936757099775707061438187717 5

a = 109026552530261035220652907861054062592

$e_3(Q, P)$: 2.740s/ 1.960s
$a_S(Q, P)$: 3.840s/ 2.140s
$e(Q, P)$: 5.150s/ 1.950s $\qquad$ $e(P, Q)$: 2.740s/ 1.970s

---

$E : y^2 = x^3 + 10 \qquad q \equiv 1 \mod \varphi(k)$

q = 580159088326370024512268501299217148866028955328305037066875107801227936069305
98359073778779593800315407999633599944856487517394689868065641555194056031595 8
56178577711013474772242032007611946854836894205836357786458570626619292421658 9
65107705458370875271446937772116121399332965473087697297168587995865622393

r = 580159088326370024512268501299217148866028955328305037066875107801227936069305
98359073778779593800315407999633599944856487517394689868065641555194056031588 2
39361077426724632933374947143911949954471504291888392255579218756650892894510 6
46540808161654144574316523234854667134799588727931358308989054372409240089

t = 761681750028428884183886708486369999690036538991394796553087935186996839952714
83185668972967167306971304145372614542645333767451563398981795336234563823 05

a = 178148083302958581604677471290051716721505311820319216780182604978187308892 16

$e_1(Q, P)$: 11.400s/ 8.540s
$a_S(Q, P)$: 15.930s/ 9.190s
$e(Q, P)$: 22.250s/ 8.490s $\qquad$ $e(P, Q)$: 11.800s/ 8.520s

---

$E : y^2 = x^3 + 3 \qquad q \equiv 3 \mod \varphi(k)$

q = 134023416371514802288518684832100354894135827305567675706961262859844147078955
859772609376760833342146166406139539799207351078421671514200983728858688086654
768589895454836417910564056197880482483901545246657813095512753613668057561752
605966214505343273028161921181279258334836297432086297235685991873914439403

r = 134023416371514802288518684832100354894135827305567675706961262859844147078955
859772609376760833342146166406139539799207351078421671514200983728858688086643
191741603647830005751153584277671460710891496690441550137432632526252017129054
734057763941493170308114336729190928438991919595760153936853379080691119509

t = 115768482918070064121594104719202090217730100485562162629580801210874160404326
978719084505638501027200475844520883298958443778363261432988326127932233198 95

a = 219628932252855050353889320790098426267785788780137619513004578721824159825 92

$e_3(Q, P) : 11.160s / 8.380s$
$a_S(Q, P) : 15.730s / 9.150s$
$e(Q, P) : 22.100s / 8.340s \qquad e(P, Q) : 11.610s / 8.370s$

Interpretation der Zeitmessungen Die Messungen in Tabelle 3.3 zeigen für die betrachteten Paarungen einen deutlichen Unterschied zwischen der Laufzeit für die Berechnung der reduzierten Tate Paarung $e(Q, P)$, der Ate Paarung $a_S(Q, P)$ und der Laufzeit für die Berechnung der Paarung $e_1(Q, P)$ bzw. $e_3(Q, P)$.

Im Durchschnitt über alle gerechneten Beispiele ergibt sich ein Faktor von $\approx 1,9$ zwischen der Laufzeit von $e_1(Q, P)$ bzw. $e_3(Q, P)$ und der Laufzeit der betrachteten Tate Paarung $e(Q, P)$. Damit können die Paarungen $e_1(Q, P)$ bzw. $e_3(Q, P)$ in der Hälfte der, zur Berechnung der Tate Paarung benötigten, Zeit berechnet werden.
Aufgrund der gemessenen Laufzeiten halten wir fest, dass die Auswertung der klassischen Tate Paarung $e(P, Q)$ ebenfalls doppelt so schnell möglich ist wie die Auswertung von $e(Q, P)$.

Zwischen den Laufzeiten für die Berechnung von $e_1(Q, P)$ bzw. $e_3(Q, P)$ und der Laufzeit der betrachteten Ate Paarung ergibt sich im Durchschnitt über alle gerechneten Beispiele ein Faktor von $\approx 1,4$.

Für die Berechnung der klassischen Tate Paarung $e(P, Q)$ über den *Miller*-Algoritmus und die Auswertung der Paarungen $e_1(Q, P)$ bzw. $e_3(Q, P)$ messen wir in etwa gleiche Laufzeiten.
Diesen geringen Unterschied bzw. die schnelle Berechnung von $e(P, Q)$ können wir darüber begründen, dass der Punkt P in der Gruppe $\mathbb{G}_1 = E[r] \cap \ker(\pi_q - [1])$ liegt. In Abschnitt 1.5.1 haben wir argumentiert, dass dann der Punkt P in $\mathbb{F}_q$-rational ist.
Dieser Punkt hat damit Koordinaten in $\mathbb{F}_q$ und in diesem Körper ist die Arithmetik schneller durchführbar als in dem Körper $\mathbb{F}_{q^k}$. Dies macht deutlich, dass es immer von Vorteil ist die Rechenoperationen in einem möglichst kleinen Körper durchzuführen.

4 Anwendungen

Um diese Arbeit nicht nur der reinen Theorie der Berechnung von Paarungen zu widmen, soll dieses Kapitel einen kleinen Einblick in die verschiedenen Anwendungsgebiete in der Kryptographie geben. Mit Kryptographie meinen wir dabei die Ver- und Entschlüsselung von Daten, welche zwischen Kommunikationsparteien ausgetauscht werden, ohne dass wir das Abfangen und illegitime Entschlüsseln betrachten. Um den Nutzen und die Rolle des Einsatzes von Kryptographie zu begründen, wollen wir wir das Bundesministerium für Sicherheit in der Informationstechnik (BSI)[1] zitieren.

> Daten werden verschlüsselt, um Sie (den Bürger) zu schützen. Die Verschlüsselung im Internet dient drei Zielen:
>
> 1. Schutz der **Vertraulichkeit**: Die Nachricht darf nur für den lesbar sein, für den sie bestimmt ist.
> 2. Schutz der **Authentizität**: Die Echtheit des Absenders soll gewahrt sein. Ist der Absender wirklich die Person, die als Absender angegeben wird?
> 3. Schutz der **Integrität**: Die Nachricht darf auf dem Weg vom Absender zum Empfänger nicht verändert werden.

Einen weiterer wichtiger Punkt in diesem Zusammenhang ist die **Verbindlichkeit / Nichtabstreitbarkeit**. Der Urheber der Daten oder Absender einer Nachricht soll nicht in der Lage sein seine Urheberschaft zu bestreiten, das heißt diese sollte sich gegenüber Dritten nachweisen lassen.

4.1 Paarungsbasierte Kryptographie

Wir werden verschiedene Protokolle kennenlernen und geben für die Verschlüsselung und die Signatur jeweils eine identitätsbasierte Modellierung an. Identitätsbasierte Kryptosysteme (im Folgenden ID basiert) haben die Eigenschaft, dass der öffentliche Schlüssel eines Nutzers sehr einfach über eine Hashfunktion aus einer eindeutig zum Nutzer gehörende, öffentlich zugängliche Information, die mit der Nutzeridentität verknüpft ist, berechnet werden kann. Beispielsweise kann dies der Hashwert der E-Mail Adresse oder Ähnliches sein. Die Zuordnung von Identitäten zu öffentlichen Schlüsseln ist eindeutig

[1] Das BSI für Bürger - `http://www.bsi-fuer-buerger.de/schuetzen/07_03.htm`

formuliert und die Notwendigkeit der Zertifizierung öffentlicher Schlüssel entfällt.
Der geheime Schlüssel wird für den Nutzer von einer vertrauenswürdigen Autorität, dem *private key generator (PKG)* mit Hilfe eines Mastergeheimnisses berechnet.
Systeme, welche identitätsbasierte Verschlüsselung verwenden, werden wir gemäß der englischen Übersetzung *identity based encryption* als IBE-Systeme bezeichnen. Dieses Schema kann aufgrund des Wegfallens der aufwändigen Konstruktion einer *zertifikatbasierten Public-Key Infrastrukturen* (PKI) eine Alternative zu den aktuell verwendeten Kryptosystemen werden. Vor allem dann, wenn ein effizientes Schlüsselmanagement und eine angemessene Sicherheit gefordert werden, da das Problem der Schlüsselvergabe in der ID basierten Kryptographie verschwindet.
Jedoch hat diese Art von Kryptosystemen auch Nachteile, auf die wir an dieser Stelle nicht weiter eingehen wollen und verweisen auf die, dies thematisierende, Veröffentlichung „Identitätsbasierte Kryptografie - Hindernisse auf dem Weg von der Theorie in die Praxis“ [FST06a]. Für weitere Informationen rund um das Thema Kryptographie und deren Verwendung verweisen wir für fundierte Informationen auf die Webseite des BSI (`http://www.bsi.de`) und auf die zahlreich vorhandene Literatur zu diesem Thema beispielsweise „Einführung in die Kryptographie“von J. Buchmann [Buc03] oder auch das populärwissenschaftliche Werk von S. Singh „Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet.“[Sin01].

Die grundlegenden Protokollmodelle der Verschlüsselung (*encryption*), der Signatur (*signature*) und der Schlüsselvereinbarung (*key agreement*) werden wir in dieser Arbeit vorstellen, um einen Einblick auf das zu gewähren was in der Praxis möglich ist. Weitere paarungsbasierte Protokollarten, teils eigenständiger Natur oder auch Mischungen der vorher genannten sind beispielsweise die *signcryption* oder das *key sharing*.
Eine große Sammlung verschiedener Anwendungen ist auf der Webseite „The Pairing-Based Crypto Lounge“ von P. Barreto [Bar] zu finden.

Um den Lese- und Verständnisfluss zu erhalten, werden wir im folgenden Abschnitt zunächst ein kleines Begriffswörterbuch zusammenstellen, die Fachworte erklären und im Zuge dessen auch auf die mathemathischen Begrifflichkeiten verschiedener Entscheidungsprobleme eingehen.

4.1.1 Kryptographische Begriffe und Grundlagen

In Kryptosystemen wird ein Paar zusammengehöriger Schlüssel verwendet. Einer davon wird als öffentlicher Schlüssel verwendet und ist eindeutig dem Besitzer zuzuordnen. Der andere ist der private Schlüssel, welcher vom Schlüsselinhaber geheim gehalten werden muss.
Ein solches System wird als asymmetrisch bezeichnet, da für die verschiedenen Vorgänge, beispielsweise Ver- und Entschlüsselung, unterschiedliche Schlüssel verwendet werden. Für jeden Teilnehmer ist somit nur ein einziges Schlüsselpaar von Nöten, da der

Besitz des öffentlichen Schlüssels die Sicherheit des privaten Schlüssels nicht gefährdet.

Die folgende Aufstellung stellt einen Ausschnitt der verschiedenen Protokollarten dar. (Vgl. [DBS04]) In den Abschnitten 4.1.3, 4.1.4 und 4.1.5 erklären wir einige Ausgewählte detaillierter. Den letzten Abschnitt 4.2 widmen wir den Sicherheitsbetrachtungen der vorgestellten Modelle.

Verschlüsselung Verschlüsselungen finden Verwendung um die Privatssphäre und Vertraulichkeit einer Nachricht zu garantieren. Will der User Alice eine Nachricht an einen weiteren User Bob senden, so verschlüsselt Alice diese Nachricht unter Verwendung des öffentlichen Schlüssels von Bob, der lediglich von den Identitätsinformationen von Bob abhängt.
Bob, der die verschlüsselte Botschaft empfangen und lesen soll, erhält den privaten (und damit geheimen) Schlüssel von einer dritten vertrauenswürdigen Partei (dem PKG) nachdem er sich dieser gegenüber authentifiziert hat und entschlüsselt Alice' Nachricht. Der geheime Schlüssel wird von dem PKG auf Bob's Anfrage hin aus seinem Masterschlüssel und seiner Identität generiert.

Signatur Die Signatur dient im Zeitalter der zunehmenden Digitalisierung von Dokumenten der adäquaten Abbildung von Unterschriften, wie sie beispielsweise bei gesetzlichen Schriftformerfordernissen oder zur beweiskräftigen Dokumentation von Willenserklärungen nötig ist. Diese soll der Authentifizierung des Unterzeichners dienen.
Im Gegensatz zur Verschlüsselung wird der private Schlüssel vom Absender Alice zur digitalen Unterschrift einer Nachricht genutzt. Diese Unterzeichnung wird von dem Empfänger Bob unter Verwendung des öffentlichen Schlüssels überprüft.

Schlüsselvereinbarung Wollen zwei oder mehr Parteien sichere Transaktionen miteinander durchführen, so muss zunächst ein sogenannter Schlüsselaustausch stattfinden, im Allgemeinen nennt man dies bei mehr als zwei Teilnehmern dann *conference keying*. Ein Angreifer, welcher nicht in Besitz des geheimen Schlüssels ist, wird die ausgetauschten Nachrichten nicht entschlüsseln können.

Schwellwert (Threshold) ***Shamirs Secret Sharing [Sha79]*** Die Idee dieser kryptographischen Technik basiert auf der Annahme, dass sich das Geheimnis G so in n Teile aufspalten lässt, dass es aus t beliebigen Teilgeheimnissen rekonstruierbar ist. Jedoch soll selbst die Kenntnis von $t-1$ solcher Teilstücke keine Informationen über das Geheimnis liefern. Dies ermöglicht die Konstruktion stabiler Schlüssel-Management Modelle für Systeme, die sicher und zuverlässig sind.

Signcryption Dieses Schema liefert eine effiziente Art und Weise geheime und vertrauliche Informationen zwischen zwei Parteien auszutauschen, indem Verschlüsselung mit der digitalen Unterschrift kombiniert wird. Innerhalb eines einzigen logischen Schrittes wird die Vertraulichkeit, die Integrität, die Autentizität und die Unleugbarkeit der Nachricht hergestellt und gesichert.

Identifikation Dieses Modell gibt einer Partei $\mathcal{P}$ die Möglichkeit die eigene Identität einer weiteren Partei gegenüber zu bestätigen, denn nur $\mathcal{P}$ kennt den geheimen Teil, welcher zu dem öffentlich bekannten Schlüssel korrespondiert.

Diese und einige mehr sind Anwendungsgebiete von Paarungen in der Kryptographie. Für einen kurzen Überblick empfehlen wir die Arbeit von Dutta *et al.* [DBS04] und für detaillierte Angaben zu Grundlagen und Realisierung das *Handbook of elliptic and hyperelliptic curve cryptography* [CF06]. Diese Literatur bildet die Grundlage dieses Kapitels und für einige der dort zusammengetragenen Protokolle wollen wir hier im Folgenden die Funktionsweise erläutern.

4.1.2 Bilineare Diffie-Hellman Probleme

Die Sicherheit der vorgestellten Kryptographiesysteme basiert auf der Unmöglichkeit der Entscheidbarkeit bzw. der effizienten Berechenbarkeit von sogenannten *bilinearen Diffie-Hellman Problemen*. Wir stellen die verschiedenen Probleme vor und untersuchen die Schwierigkeit in den Gruppen, welche den betrachteten Paarungen zugrundeliegen. Als Literatur verwenden wir [BF03].
Wir können solche Probleme in einen lockeren Verbund zusammenschließen und unterscheiden dann in die so genannten Entscheidungs- und Berechnungsprobleme. Dabei heißt ein Problem ein *Entscheidungsproblem*, falls die Problematik darin besteht zu entscheiden, ob eine Aussage bezüglich der vorliegenden Eingabe wahr oder falsch ist.
Ein Problem heißt ein *Berechnungsproblem*, falls danach gefragt wird eine spezifische Ausgabe aus einer Menge von Eingaben zu berechnen. Wir unterscheiden stets zwischen Entscheidungs- und Berechnungsproblemen des diskreten Logarithmus Problems (*DLP*). Das heißt zu gegebener Primzahl p und natürlichen Zahlen $a, b < p$ soll eine Zahl x gefunden werden, so dass $a^x \equiv b \mod p$ gilt. Dieses Problem ist mathematisch als schwierig einzustufen, da kein effizienter Algorithmus zur Lösung existiert. Auf dieser Basis ist eine weite Klasse kryptographischer Verfahren aufgebaut.
Die Algorithmen der Kryptographie, welche wir zu einem späteren Zeitpunkt betrachten wollen, stützen sich auf die eben angemerkte Schwierigkeit der Berechnung des *DLP* und somit auf die Komplexität dieser Berechnungen.

Für Gruppen $\mathbb{G}_1, \mathbb{G}_2$ der Ordnung r für ein großes primes r. Die in Kryptosystemen verwendete Abbildung e muss zur Verwendbarkeit die Eigenschaften der Bilinearität, Nichtdegeneriertheit und der effizienten Berechenbarkeit aufweisen. Abbildungen mit diesen Eigenschaften nennen wir *zulässig* und die in dieser Arbeit betrachteten Paarungen sind solch zulässige Abbildungen für die der *Miller*-Algorithmus eine effiziente Berechenbarkeit darstellt.
Aus der Existenz einer solchen Abbildung heraus betrachten wir die MOV-Reduktion [MOV91] und die Einfachheit des Diffie-Hellman Entscheidungsproblems.

Die MOV-Reduktion Diese Reduktion beschreibt die Transformation des DLP in $\mathbb{G}_1$ auf dasgleiche Problem in $\mathbb{G}_2$ und trägt den Namen der Autoren Menezes, Okamoto und

Vanstone.
Zur Reduktion betrachten wir $P,\ Q \in \mathbb{G}_1$ der Ordnung r als eine Instanz des DLP in $\mathbb{G}_1$ und die Aufgabe ist das Finden eines $\alpha \in \mathbb{Z}_q$, so dass $Q = [\alpha]P$ gilt.
Sei $g := e(P,P)$ und $h := e(P,Q)$. Aufgrund der Bilinearität gilt dann $h = g^\alpha$ und aus der Nichtdegeneriertheit von e folgt, dass die Ordnung der Elemente g, h in $\mathbb{G}_2$ r ist. Wir erhalten somit die Reduzierbarkeit eines DLP in $\mathbb{G}_1$ auf ein DLP in $\mathbb{G}_2$. Um die Schwierigkeit des DLP in $\mathbb{G}_1$ zu gewährleisten muss der Sicherheitsparameter so gewählt sein, dass das DLP in $\mathbb{G}_2$ schwer ist.

Einfachheit des Diffie-Hellman Entscheidungsproblems Das sogenannte Diffie-Hellman Entscheidungsproblem (DDH) in $\mathbb{G}_1$ ist die Frage nach der Unterscheidbarkeit zwischen den Tupeln $\langle P, [a]P, [b]P, [ab]P\rangle$ und $\langle P, [a]P, [b]P, [c]P\rangle$ für zufällig gewählte a, b, c aus $\mathbb{Z}_q^\times$.
Nach den Ausführungen von [JN01] ist das DDH in $\mathbb{G}_1$ leicht. Für gegebene Punkte $P, [a]P, [b]P, [c]P \in \mathbb{G}_1^\times$ haben wir die geltende Äquivalenz

$$c \equiv ab \mod r \Leftrightarrow e(P,[c]P) = e([a]P,[b]P),$$

welche das DLP auf $\mathbb{G}_1$ eine Kongruenzentscheidung reduziert.
Das zugehörige Diffie-Hellman Berechnungsproblem (CDH) kann in $\mathbb{G}_1$ immer noch schwer sein, da zu einem zufälligen Tupel $\langle P, [a]P, [b]P\rangle$ die Aufgabe das Finden von $[ab]P$ ist. In [JN01] sind Beispiele von Abbildungen e für diese Konstellation eines in $\mathbb{G}_1$ (vermutet) schweren CDH und leichten DDH zu finden.

Wie in den vorangegangenen Ausführungen gezeigt, ist das Diffie-Hellman Entscheidungsproblem in $\mathbb{G}_1$ leicht und auf Basis dieses Problems kann kein Kryptosystem entwickelt werden. Stattdessen betrachten wir für das vorgestellte IBE Protokoll eine Variante des CDH, welche wir *bilineare Diffie-Hellman Vermutung* nennen. Die genaue Formulierung führen wir an dieser Stelle nicht an, sondern geben nur die Definition des bilinearen Diffie-Hellman Problems (BDH) an.
Für Weiteres in diesem Kontext verweisen wir auf [BF03].

Das bilineare Diffie-Hellman Problem Sei e eine zulässige Abbildung und P ein Erzeuger von $\mathbb{G}_1$. Das BDH in $\langle \mathbb{G}_1, \mathbb{G}_2, e\rangle$ ist das Folgende:
Zu gegebenem Tupel $\langle P, [a]P, [b]P, [c]P\rangle$ für a, b, c aus $\mathbb{Z}_q^\times$ berechne $e(P,P)^{abc} \in \mathbb{G}_2$.
Ein Algorithmus $\mathcal{A}$ besitzt den Nutzen ϵ zur Lösung des BDH in $\langle \mathbb{G}_1, \mathbb{G}_2, e\rangle$, falls

$$\Pr[\mathcal{A}(P, [a]P, [b]P, [c]P) = e(P,P)^{abc}] \geq \epsilon$$

gilt.

Die Schwierigkeit des BDH und der zugehörigen Varianten bilden die Basis für die im Folgenden vorgestellten kryptographischen Protokolle.

4.1.3 ID basiertes Verschlüsselungsmodell FullIdent

Das von Boneh und Franklin, in [BF03] vorgestellte, IBE Schema ist für jede bilineare Abbildung $e : \mathbb{G}_1 \times \mathbb{G}_1 \mapsto \mathbb{G}_2$ zwischen zwei Gruppen $\mathbb{G}_1, \mathbb{G}_2$ erklärt, solange eine Variante des CDH Problems in $\mathbb{G}_1$ schwer ist. Die Tate Paarung ist eine dies erfüllende bilineare Abbildung für paarungsfreundliche Kurven.

Die ID basierte Verschlüsselung wird durch vier randomisierte Algorithmen, die einzelne Schritte abarbeiten, spezifiziert. Diese Schritte sind Setup, Extract, Verschlüsselung, Entschlüsselung.

Setup: Verwendet eine Zahl z, die als Sicherheitsparameter fungiert, als Grundlage für die Berechnungen der Systemparameter `params` und gibt diese Parameter und den Masterschlüssel zurück.
Die Systemparameter beinhalten eine Beschreibung eines endlichen Nachrichtenraumes $\mathcal{M}$ und eine Beschreibung eines endlichen Chiffreraumes C und sind systemweit zugängliche Informationen. Das Mastergeheimnis s hingegen ist nur dem PKG bekannt.

Extract: Dieser Schritt wird von einer vertrauenswürdige Partei (TA : *Trusted Authority*) ausgeführt, falls eine Anfrage auf einen identitätsabhängigen privaten Schlüssel stattfindet.
Verwendet als Eingabe die Systemparameter `params`, das Mastergeheimnis und eine beliebige `ID` $\in \{0,1\}^*$ und gibt einen geheimen Schlüssel d zurück.
Für identitätsbasierte Protokolle wird `ID` als öffentlicher Schlüssel verwendet und es ergibt sich das eindeutige Schlüsselpaar (ID, d). Der geheime Schlüssel wird wie der Name des Schrittes impliziert aus dem öffentlichen Schlüssel `ID` extrahiert.

Encrypt: Eingabe sind die Systemparameter `params`, die `ID` und die Nachricht $M \in \mathcal{M}$. Rückgabe ist die chiffrierte Nachricht $C \in C$.

Decrypt: Eingabe sind die Systemparameter `params`, das Geheimnis d und die Chiffre $C \in C$. Rückgabe ist die chiffrierte Nachricht $M \in \mathcal{M}$.

Jeder der obigen vier Schritte muss konsistent sein, das heißt für den in Extract erzeugten privaten Schlüssel d und die gegebene `ID` als öffentlichen Part, muss stets erfüllt sein, dass

$$\forall_{M \in \mathcal{M}} : \text{Decrypt}(\texttt{params}; C; d) = M \text{ mit } C = \text{Encrypt}(\texttt{params}; \texttt{ID}; M)$$

Für die Protokollbeschreibung von FullIdent sei $z \in \mathbb{N}$ der Sicherheitsparameter, welcher dem **Setup** übergeben wird. Die BDH Parameter seien durch $\mathcal{G}$ erzeugt. Dann ist das Protokoll das Folgende.

Setup (wird von der TA ausgeführt):
Schritt 1: Mittels $\mathcal{G}$ erzeuge aus der Eingabe z eine Primzahl r, zwei Gruppen $\mathbb{G}_1, \mathbb{G}_2$ der Ordnung r und eine geeignete bilineare Abbildung $e : \mathbb{G}_1 \times \mathbb{G}_1 \mapsto \mathbb{G}_2$. Weiterhin wählt die TA einen zufälligen Erzeuger P von $\mathbb{G}_1$.

Schritt 2: Wähle zufälliges $s \in \mathbb{Z}_q^\times$ und setze $P_{\text{pub}} = [s]P$.

Schritt 3: Wähle zwei geeignete kryptographische Hashfunktionen $H_1 : \{0,1\}^* \to \mathbb{G}_1^\times$ und $H_2 : \mathbb{G}_2 \to \{0,1\}^n$, wobei n die Bitlänge der Nachrichten ist. Wähle weiterhin Hashfunktionen $H_3 : \{0,1\}^n \times \{0,1\}^n \to \mathbb{Z}_q^\times$ und $H_4 : \{0,1\}^n \to \{0,1\}^n$.
Dann ist $\mathcal{M} = \{0,1\}^n$ der Nachrichtenraum und $C = \mathbb{G}_1^\times \times \{0,1\}^n \times \{0,1\}^n$ der Raum der verschlüsselten Nachrichten.
Die Systemparameter sind $\texttt{params} := \langle r; \mathbb{G}_1; \mathbb{G}_2; e; n; P; P_{\text{pub}}; H_1; H_2; H_3; H_4 \rangle$, der Masterschlüssel ist die Zahl s und als öffentlichen Schlüssel verwende P_{pub}.

Extract (wird von der TA ausgeführt):
Für eine gegebene Identität $ID \in \{0,1\}^*$ berechne den öffentlichen Schlüssel als Bild eines beliebigen Strings $Q_{\texttt{ID}} = H_1(\texttt{ID}) \in G_1$ und hashe den String unter H_1 auf einen Punkt der Gruppe G_1.
Der private Schlüssel lässt sich aus dem Masterschlüssel als $S_{\texttt{ID}} = [s]Q_{\texttt{ID}}$ berechnen.

Encrypt:
Um eine Nachricht $M \in \mathcal{M}$ mit einem öffentlichen Schlüssel ID zu verschlüsseln, berechne zunächst $Q_{\texttt{ID}} = H_1(\texttt{ID})$. Wähle ein zufälliges $\sigma \in \{0,1\}^n$ und setze $u = H_3(\sigma, M)$, dann ist die verschlüsselte Nachricht C gegeben durch

$$C = \left\langle [u]P, \sigma \oplus H_2(g_{\texttt{ID}}^u), M \oplus H_4(\sigma) \right\rangle \text{ mit } g_{\texttt{ID}} = e(Q_{\texttt{ID}}, P_{\text{pub}}) \in \mathbb{G}_2$$

Decrypt:
Sei $C = \langle U, V, W \rangle \in C$ ein mit ID verschlüsselter Chifftretext gegeben. Ist $U \notin \mathbb{G}_1^\times$ so weise die Chiffre zurück, ansonsten entschlüssele unter Verwendung des geheimen Schlüssels $S_{\texttt{ID}} \in \mathbb{G}_1^\times$ und der folgenden Vorgehensweise.

1. Berechne $V \oplus H_2(e(S_{\texttt{ID}}, U)) = \sigma$.
2. Berechne $W \oplus H_4(\sigma) = M$.
3. Setze $u = H_3(\sigma, M)$ und überprüfe $U = [u]P$. Falls die Überprüfung $U \neq [u]P$ ergibt, so weise die Chiffre zurück.
4. Gib M als Entschlüsselung von C aus.

Die Korrektheit dieser Entschlüsselung prüfen wir über das Verifizieren von 1. nach:

$$\begin{aligned}
V \oplus H_2(e(S_{\texttt{ID}}, U)) &= (\sigma \oplus H_2(g_{\texttt{ID}}^u)) \oplus (H_2(e(S_{\texttt{ID}}, [u]P))) \\
&= (\sigma \oplus H_2(g_{\texttt{ID}}^u)) \oplus (H_2(e([s]Q_{\texttt{ID}}, [u]P))) \\
&= (\sigma \oplus H_2(e^u(Q_{\texttt{ID}}, P_{\text{pub}})) \oplus (H_2(e^{su}(Q_{\texttt{ID}}, P))) \\
&= (\sigma \oplus H_2(e^u(Q_{\texttt{ID}}, [s]P)) \oplus (H_2(e^{su}(Q_{\texttt{ID}}, P))) \\
&= (\sigma \oplus H_2(e^{su}(Q_{\texttt{ID}}, P)) \oplus (H_2(e^{su}(Q_{\texttt{ID}}, P))) \\
&= \sigma
\end{aligned}$$

Die ausführliche Sicherheitsanalyse, weitere Protokolle und eine konkrete Ausführung einer leicht variierten Form des BasicIdent anhand der Weil Paarung sind in [BF03] zu finden. Einige der Aspekte der kryptographischen Sicherheit werden wir in Abschnitt 4.2 behandeln. Das vorgestellte Schema ist Chosen Ciphertext sicher und bietet Nichtunterscheidbarkeit der chiffrierten Nachrichten (IND-ID-CCA) [BF03]. Ein Verschlüsselungssystem heißt Chosen Ciphertext sicher, falls sich ein Angreifer Chiffretexte aussuchen kann, die zugehörigen Klartexte erhält und der Angreifer mit diesen Informationen das System nicht umgehen kann.

Im folgenden Abschnitt geben wir einen Einblick in die Konstruktion von ID basierten Signaturmodellen. Anschließend betrachten wir ein Modell der Schlüsselvereinbarung inklusive eines Angriffes auf dieses Modell und zeigen somit Schwächen von nicht zertifizierten Schemata auf.

4.1.4 ID basiertes Modell für Signaturen

Die Sicherheit des von F. Heß in [Hes03] vorgestellten Signatur-Schemas basiert, wie das in Abschnitt 4.1.3 erklärte IBE Schema, auf einer Variante des BDH Problems in $\mathbb{G}_1$. Auch für dieses Protokoll verwenden wir als zulässige Abbildung eine Paarung e.

Die ID basierte Signatur wird analog zu der Verschlüsselung durch vier randomisierte Algorithmen, die einzelne Schritte abarbeiten, spezifiziert. Diese Schritte sind Setup, Extract, Signieren, Verifizieren. Die Funktionsweisen sind sehr ähnlich zu denen in Abschnitt 4.1.3.

Setup (wird von der TA ausgeführt):
Wähle zufälliges $s \in \mathbb{Z}_q^\times$ und setze $P_{\text{pub}} = [s]P$. Die Zahl s sei der Masterschlüssel und verwende P_{pub} als öffentlichen Schlüssel.
Wähle eine Hash-Funktion $H_1 : \{0,1\}^* \to \mathbb{G}_1^\times$, also eine auf die Punkte abbildende Hash-Funktion, und $H_2 : \{0,1\}^* \times \mathbb{G}_2 \to \mathbb{Z}_q^\times$ eine weitere Hash-Funktion.

Extract(wird von der TA ausgeführt):
Für eine gegebene Identität $ID \in \{0,1\}^*$ berechne den öffentlichen Schlüssel als Hashwert eines beliebigen Strings $Q_{\text{ID}} = H_1(ID) \in \mathbb{G}_1$ und den privaten Schlüssel als $S_{\text{ID}} = [s]Q_{\text{ID}}$.

Signieren:
Der Unterzeichner wählt einen beliebigen Punkt $P_1 \in \mathbb{G}_1^\times$, eine zufällig gewählte Zahl $z \in \mathbb{Z}_q^\times$ und berechnet für die Nachricht M die Signatur als Paar $\langle v, w\rangle \in \mathbb{G}_1 \times \mathbb{Z}_q^\times$.

1. $u = e(P_1, P)^z$
2. $w = H_2(M, u)$
3. $v = [w]S_{\text{ID}} + [z]P_1$

Verifizieren:
Mit Hilfe des öffentlichen Schlüssels P_{pub}, der Nachricht M und einer übersendeten Signatur $\langle v, w\rangle$ prüft der Empfänger das Folgende:

1. Berechne $u = e(v, P)e(Q_{\text{ID}}, -P_{\text{pub}})^w$.
2. Akzeptiere die Signatur genau dann, wenn $w = H_2(M, u)$ gilt.

Es ist leicht nachzurechnen, dass für eine gültige Signatur die Anweisungen des Verifizierens das Gewünschte liefern.

$$\begin{aligned} e(v, P)e(Q_{\text{ID}}, -P_{\text{pub}})^w &= e([w]S_{\text{ID}} + [z]P_1, P)e(Q_{\text{ID}}, -[s]P)^w \\ &= e([w][s]Q_{\text{ID}} + [z]P_1, P)e(Q_{\text{ID}}, -[s]P)^w \\ &= e([w][s]Q_{\text{ID}}, P)e([z]P_1, P)e(Q_{\text{ID}}, -[s]P)^w \\ &= e(Q_{\text{ID}}, P)^{sw}e(P_1, P)^z e(Q_{\text{ID}}, P)^{-sw} \\ &= e(Q_{\text{ID}}, P)^{sw-sw}e(P_1, P)^z \\ &= e(P_1, P)^z \\ &= u \end{aligned}$$

Auf die Betrachtung der Sicherheit dieses Protokolles gehen wir in dieser Arbeit nicht weiter ein. Diese Ausführungen, weitere Signaturprotokolle und Beispiele der angeführten Signaturschema sind in [Hes03] zu finden.

4.1.5 Modell für Schlüsselvereinbarungen

Die Sicherheit der von A. Joux in [Jou00] vorgestellten Schlüsselvereinbarung basiert, wie die in den Abschnitten 4.1.3 und 4.1.4 eingeführten Protokolle, auf einer Variante des BDH Problems in $\mathbb{G}_1$. Auch in diesem Abschnitt verwenden wir als zulässige Abbildung eine Paarung e.

Wir geben im Folgenden eine Protokollbeschreibung für eine tripartite Schlüsselvereinbarung an [Jou00] und demonstrieren über einen sogenannten *Man-in-the-middle*-Angriff [Shi03] die Anforderungen an die Sicherheit eines solchen Schemas.

Seien A, B und C jene drei Parteien mit jeweiligen geheimen Schlüsseln S_A, S_B und $S_C \in \mathbb{Z}_q^\times$, die miteinander kommunizieren wollen. Jede der einzelnen Parteien sendet das Produkt seines privaten Schlüssels und eines öffentlich bekannten Punktes P, also $P_i = [S_i]P$ $i \in \{A, B, C\}$ an die jeweils anderen beiden Parteien, das heißt

- A sendet $[S_A]P$ an B und C
- B sendet $[S_B]P$ an A und C
- C sendet $[S_C]P$ an A und B

Jede der Parteien berechnet anschließend die Paarung aus den zwei erhaltenen Punkten und potenziert diese mit dem eigenen privaten Schlüssel und erhält

- A berechnet $K_A = e(P_B, P_C)^{S_A}$
- B berechnet $K_B = e(P_A, P_C)^{S_B}$
- C berechnet $K_C = e(P_A, P_B)^{S_C}$

Aufgrund der Bilinearität der Paarung haben nun alle drei Parteien denselben gemeinsamen Wert als

$$K_{ABC} := K_A = K_B = K_C = e(P, P)^{S_A S_B S_C}$$

berechnet und jede der Parteien kann Nachrichten mit diesem Schlüssel chiffrieren und an die beiden anderen Kommunkationsparteien senden. Diese beiden können mit ihren geheimen Schlüsseln die gesendete Nachricht entschlüsseln.

Der Man-in-the-middle-Angriff kann auf dieses Schema der Schlüsselvereinbarung dann wie im Folgenden beschrieben ausgeführt werden. Ein Angreifer *Eve*, der sich in der „Mitte“des tripartiten Kommunikationsnetzes platziert, fängt die Produkte $P_i = [S_i]P$ $i \in \{A, B, C\}$ der einzelnen Parteien ab und erzeugt temporäre geheime Schlüssel S_X, S_Y und $S_Z \in \mathbb{Z}_q^\times$. *Eve* ersetzt die abgefangenen Produkte P_i durch die eigenen Produkte $P_j = [S_j]P$ mit $j \in \{X, Y, Z\}$ und sendet diese paarweise an A, B und C. Die einzelnen Parteien berechnen demnach

- A berechnet $K_A = e(P_Y, P_Z)^{S_A} = e(P, P)^{S_A S_Y S_Z}$
- B berechnet $K_B = e(P_X, P_Z)^{S_B} = e(P, P)^{S_B S_X S_Z}$
- C berechnet $K_C = e(P_X, P_Y)^{S_C} = e(P, P)^{S_C S_X S_Y}$

Dem Angreifer sind die Werte S_X, S_Y und S_Z als auch die einzelnen abgefangenen Produkte P_A, P_B, P_C bekannt. Eve kann aus der Kenntnis dieser Werte ebenso die Berechnungen der einzelnen Kommunikationsparteien anstellen und erhält

- $K_A = e(P_A, P_Z)^{S_A} = e(P, P)^{S_A S_Y S_Z}$
- $K_B = e(P_X, P_Z)^{S_B} = e(P, P)^{S_B S_X S_Z}$
- $K_C = e(P_X, P_Y)^{S_C} = e(P, P)^{S_C S_X S_Y}$

Sendet beispielsweise A eine mit K_A verschlüsselte Nachricht an B und C, so entschlüsselt *Eve* die Nachricht und verschlüsselt den Klartext mit den zu B bzw. C assoziierten K_B respektive K_C. Anschließend werden die so chiffrierten Nachrichten an die Empfänger versendet. Analog verfährt *Eve* mit den Nachrichten, die von B bzw. C versendet werden.
Während die Teilnehmer A, B und C an eine sichere Kommunikation glauben, kann *Eve* jede der gesendeten Nachricht abfangen und lesen.
Dieser Man-in-the-middle-Angriff ensteht aufgrund der fehlenden Authentifizierung der

Teilnehmer. Diese Beeinträchtigung kann durch die Verwendung zertifizierter, öffentlicher Schlüssel ausgeschlossen werden.
Eine authentifizierte, tripartite Schlüsselvereinbarung ist in [Shi03] zu finden.

Dieses Protokoll kann von dem hier angegebenen Schema für drei Teilnehmer auf eine Menge von N Parteien verallgemeinert werden und ist als *Multi Party Key Agreement* in [DBS03] zu finden.

4.2 Sicherheitsbetrachtungen der paarungsbasierten Kryptographie

In Abschnitt 4.1.2 haben wir Grundlagen bilinearer Diffie-Hellman Probleme betrachtet. Jedes der vorgestellten Kryptosysteme basiert auf einem dieser oder einer Variante der angebenen Probleme. Die angenommene Schwierigkeit zur Lösung eines dieser Probleme rechtfertigt stets die Existenzgrundlage der vorgestellten Schematas, wobei wir in Abschnitt 4.1.5 einen möglichen Angriff auf das vorgestellte System aufgezeigt haben.

Die Schwierigkeit paarungsbasierter Kryptosysteme basiert neben der Wahl der Sicherheitsparameter, wie in Abschnitt 4.1.2 beschrieben, auf der möglichst schwierigen Invertierbarkeit von Paarungen. Diese beiden Punkte behandeln die Abschnitte 4.2.1 und 4.2.2.

Im Folgenden betrachten wir Paarungen der Form $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Da sowohl $\mathbb{G}_1$ als auch $\mathbb{G}_2$ Untergruppen der Ordnung r von Pic_C sind, werden wir, um das Schriftbild durch die eigentlich nötige Unterscheidung von $\mathbb{G}_1$ und $\mathbb{G}_2$ einfacher zu gestalten, die Notation dahingehend einschränken stets nur $\mathbb{G}_1$ zu schreiben.

4.2.1 Sicherheit der Parameter

Um die Sicherheit paarungsbasierter Kryptosysteme zu gewährleisten, muss die Schwierigkeit des diskreten Logarithmus in $\mathbb{G}_1$ gegeben sein. Die Parameter der zugrundeliegenden Strukturen müssen so gewählt sein, dass das DLP in $\mathbb{G}_2$ schwer ist.
Für Paarungen bedeutet dies im Speziellen, dass das DLP auf der Jacobischen der betrachteten Kurve mit der Schwierigkeit des DLP innerhalb des endlichen Körpers $\mathbb{F}_{q^k}$ korreliert. Daher erhalten wir die Verknüpfung der Zahlen q, r und dem Einbettungsgrad k.

Die Sicherheit der paarungsbasierten Kryptographie ist beschrieben durch ein Tupel (kF, G). Hierbei bezeichnet F die Bitlänge von q und entspricht demnach $\approx \log_2(q)$. Die Größe G ist analog als die Bitlänge von r, also $\approx \log_2(r)$. Für das DLP in $\mathbb{F}_{q^k}^{\times}$ ist die Sicherheit durch kF und für das DLP auf den betrachteten Kurven durch G spezifiziert.

Jede der Paarungen, die wir behandelt haben, verwendet als Input Elemente der Jacobischen $\mathcal{J}_C(\mathbb{F}_q)$ einer, über dem Körper $\mathbb{F}_q$ definierten, (hyper-)elliptischen Kurve C und resultiert in einem Element des Körpers $\mathbb{F}_{q^k}$. Die Sicherheit der paarungsbasierten Kryptographie beruht auf der Unmöglichkeit der hinreichend effizienten Berechnung des diskreten Logarithmus Problems in der Jacobischen und der multiplikativen Gruppe $\mathbb{F}^{\times}_{q^k}$.
Die besten Algorithmen zur Lösung dieser Probleme sind einerseits der parallelisierte Pollard Rho Algorithmus [vW99, Tes00] mit einer Laufzeit von $O(\sqrt{r})$ für $\mathcal{J}_C(\mathbb{F}_q)$. Andererseits ist es der Index Calculus Angriff [Odl84] mit einer subexponentiellen Laufzeit in der Größe des endlichen Körpers für die Berechnung des DLPs in endlichen Körpern.

In beiden Gruppen wollen wir das gleiche Level an Sicherheit gewährleisten und müssen daher den deutlichen Unterschied zwischen der Größe q^k des Erweiterungskörpers und der Untergruppenordnung r fordern.
Das Verhältnis dieser beiden Größen zueinander wird beschrieben durch den Einbettungsgrad k und den Parameter $\rho = \frac{\log_2 q}{\log_2 r}$, der die Körpergröße in Relation zur Untergruppenordnung r setzt. In einigen Anwendungen, wie der Erzeugung kurzer Signaturen [BLS01], ist es wichtig das dieser Quotient ρ eins ist und somit die Größenordnungen von $\log_2 q$ und $\log_2 r$ gleich sind.
Für die in Abschnitt 3.3.4 verwendeten BN-Kurven gilt $\rho \approx 1$.

Dieser Zusammenhang erschwert die Auswahl der Parameter zur Konstruktion paarungsfreundlicher Kurven. Einerseits muss die Sicherheit bezüglich der betrachteten Kurve gewährleistet sein, das heißt eine große prime Untergruppenordnung r. Andererseits muss eine effiziente Berechnung der Paarung unter Verwendung des *Miller*-Algorithmus durchführbar sein. Dies setzt der Größe der Zahl q Grenzen und somit auch der Größe der Zahl r. Da r die betrachtete Untergruppenordnung ist, muss r ein Teiler der Ordnung der Kurve sein, das heißt $r \mid \#\mathcal{J}_C(\mathbb{F}_q)$.

Wir sind auf den Einbettungsgrad als einen der grundlegenden Sicherheitsparameter eingegangen. Unseren Ausführungen in Abschnitt 2.4 nach betrachten wir $\mathbb{F}_{q^k}$ als kleinsten Körper, der vollständig die Menge der r-ten Einheitswurzeln μ_r enthält.

Der Artikel [Hit07] diskutiert die in diesem Zusammenhang naheliegende Frage, nach der Existenz kleinerer Körper als $\mathbb{F}_{q^k}$, in die Paarungen abbilden. Das heißt, die Frage nach einem minimalen Körper, in dem die r-ten Einheitswurzeln μ_r enthalten sind.
Ein Resultat in [Hit07] ist das folgende Lemma über die Betrachtung des Einbettungsgrades. Mit $\mathrm{ord}_r(p)$ bezeichnen wir die kleinste, positive, ganze Zahl n mit $p^n \equiv 1 \mod r$.

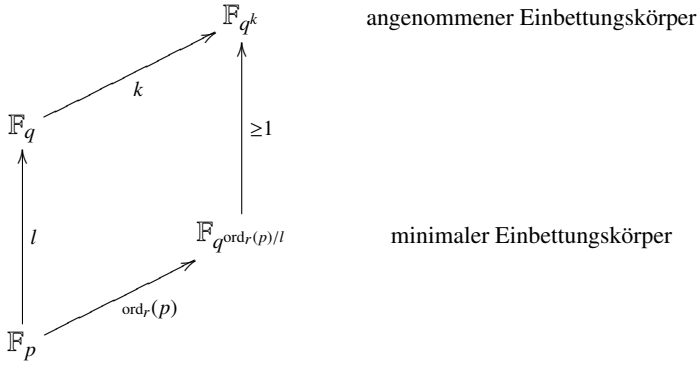
Lemma 8. *Sei $q = p^l$ für $p \in \mathbb{P}$ und $l \in \mathbb{N} \setminus \{0\}$. Sei weiterhin r prim mit* $\gcd(p, r) = 1$ *und sei k minimal mit $r \mid (q^k - 1)$. Dann gilt*

$$k = \frac{\mathrm{ord}_r(p)}{\gcd(\mathrm{ord}_r(p),\, l)}.$$

Beweis. Findet sich in [Hit07].

Betrachten wir die r-ten Einheitswurzeln μ_r näher, so liegen diese für $q = p^l$ im Speziellen in $\mathbb{F}^{\times}_{p^{\mathrm{ord}_r(p)}} = \mathbb{F}^{\times}_{p^{k \gcd(\mathrm{ord}_r(p), l)}} = \mathbb{F}^{\times}_{q^{\mathrm{ord}_r(p)/l}}$, nicht nur in $\mathbb{F}^{\times}_{q^k}$.

Die Auswertung einer Paarung lässt sich in μ_r einbetten und wir können diese multiplikative Gruppe als Erweiterung von $\mathbb{F}_p$ auffassen, welche nicht notwendig eine Erweiterung von $\mathbb{F}_q$ ist. Zur Verdeutlichung dieser möglichen Differenz zwischen den Körpergrößen betrachten wir das folgende Diagramm.



Um die Sicherheit kryptographischer Protokolle über den Einbettungsgrad genauer beschreiben zu können, sollte, statt nur den Einbettungsgrad k einzubeziehen, auch der Quotient $k' = \frac{\mathrm{ord}_r(p)}{lg}$ für (hyper-)elliptische Kurven des Geschlechts g betrachtet werden. Diese Betrachtungsweise beinhaltet die Größe der minimalen Körpererweiterung in der die r-ten Einheitswurzeln liegen. Für primes q besteht kein Unterschied zwischen $\mathbb{F}_{q^k}$ und $\mathbb{F}^{\times}_{q^{\mathrm{ord}_r(p)/l}}$.
Neben den eben angestellten Betrachtungen sind in [Hit07] einige konkrete Beispiele für (hyper-)elliptische Kurven angegeben, deren minimaler Einbettungskörper $\mathbb{F}^{\times}_{p^{\mathrm{ord}_r(p)}}$ nicht dem angenommenen $\mathbb{F}_{q^k}$ entspricht.

4.2.2 Invertierbarkeit von Paarungen

Für die Sicherheit paarungsbasierter Kryptographie muss, neben der Wahl einer paarungsfreundlichen Kurve, die Schwierigkeit der Invertierbarkeit der Paarung gewährleistet sein. Denn ist die Paarungsinvertierung zuverlässig für eine Klasse von Kurven lösbar, so kann das CDH in einer Klasse von Unterguppen endlicher Körper gelöst werden. Damit hat dies nicht nur Auswirkungen auf die Sicherheit paarungsbasierter Kryptographie, sondern zudem auf Potenzierungen basierende Kryptographie in endlichen Körpern [GHV07a].

Wir betrachten Paarungen der Form $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ und unterscheiden zwischen drei verschiedenen Umkehrbarkeiten [GHV07a].

1. Das Problem der Invertierung mit gegebenem ersten Argument *Fixed Argument Pairing Inversion* 1 *(FAPI-1)*: Berechne für ein gegebenes $\overline{D}_1 \in \mathbb{G}_1$ und ein $z \in \mathbb{G}_T$ ein $\overline{D}_2 \in \mathbb{G}_2$, so dass $e(\overline{D}_1, \overline{D}_2) = z$ gilt.

2. Das Problem der Invertierung mit gegebenem zweiten Argument *Fixed Argument Pairing Inversion* 2 *(FAPI-2)*: Berechne für ein gegebenes $\overline{D}_2 \in \mathbb{G}_2$ und ein $z \in \mathbb{G}_T$ ein $\overline{D}_1 \in \mathbb{G}_1$, so dass $e(\overline{D}_1, \overline{D}_2) = z$ gilt.

3. Das Problem der allgemeinen Paarungsinvertierung *Generalised Pairing Inversion (GPI)*: Finde für eine gegebene Paarung e und ein $z \in \mathbb{G}_T$ $\overline{D}_1 \in \mathbb{G}_1$ und $\overline{D}_2 \in \mathbb{G}_2$, so dass $e(\overline{D}_1, \overline{D}_2) = z$ gilt.

Innerhalb der Invertierung von Paarungen können wir zwei Schritte unterscheiden. Zum einen die Invertierung der finalen Potenzierung mit $\frac{(q^k-1)}{r}$ und zum anderen die Invertierung des *Miller*-Algorithmus. Diese Invertierungen sind unterschiedlich anspruchsvoll. Der Artikel [GHV07a] zeigt Familien von Parametern paarungsfreundlicher Kurven auf, für die das Problem der Miller-Invertierung in polynomieller Zeit gelöst werden kann. Weiterhin werden der Schwierigkeitsgrad der verschiedenen Invertierungen erläutert und Beispiele gegeben.
Wir wollen an dieser Stelle nicht tiefer auf diese Theorie eingehen. In [GHV07a] werden diese Aspekte und Probleme ausführlich diskutiert.

5 Zusammenfassung und Ausblick

Wir haben, zur Einführung in das Thema der Berechnung der Tate Paarung, zunächst die Grundlagen über (hyper-)elliptische Kurven betrachtet. Anschließend konnten wir die Paarungen Tate und Weil definieren. Fortführend haben wir unterschiedliche Möglichkeiten die Tate Paarung effizient zu berechnen aufgezeigt.
Wir sind von der Betrachtung der klassischen Tate Paarung auf effiziente Implementierungstechniken eingegangen, um die Berechnung der Tate Paarung über den *Miller*-Algorithmus zu beschleunigen.

Weiterhin haben wir uns mit verschiedenen, effizienten Abwandlungen der Tate Paarung befasst. In diesem Zusammenhang haben wir Paarungen unter der Verwendung von Verzerrungsabbildungen betrachtet. Als ein Beispiel für eine solche Paarung, die diese Effizienzsteigerung verwendet, haben wir die sogenannte Eta Paarung diskutiert.
Des Weiteren haben wir die sogenannte Ate Paarung als eine direkte Abwandlung der Tate Paarung untersucht und, die für $S \equiv q \mod r$ definierte, Ate Paarung auf den Fall $S_i \equiv q^i \mod r$ verallgemeinert.
Zur Definition der Ate Paarung auf hyperelliptischen Kurven haben wir gezeigt, dass die Forderung der Kurve superspeziell zu sein eine zu starke Anforderung war. In diesem Kontext haben wir die hyperelliptische Ate Paarung als Satz formuliert und haben gezeigt, dass diese Paarungen unter den angenommenen schwächeren Voraussetzungen bilinear und nichtdegeneriert ist.

Ausgehend von den Definitionen der Tate und den aufgezeigten Ate_i Paarungen sind wir auf die Konstruktion zusammengesetzter Paarungen eingegangen. Wir haben einerseits die R-Ate Paarung als Quotient zweier Paarungen betrachtet, andererseits haben wir uns mit Paarungen über Gitterkonstruktionen der Dimension $\varphi(k)$ beschäftigt.
Diesem Ansatz folgend haben wir für Barreto-Nährig Kurven die Konstruktion von bilinearen, nichtdegenerierten Paarungen untersucht. Wir haben Paarungen als Linearkombination der Tate und Ate_i definierenden, rationalen Funktionen konstruiert und die Bilinearität über die Konstruktion erhalten. Weiterhin haben wir die Nichtdegeneriertheit dieser Paarungen gezeigt. Neben der Angabe von Schranken für den Grad der Funktion haben wir eine geringe Laufzeit zur Berechnung dieser Paarungen erreicht. Die Berechnung verschiedener Beispiele hat, im Vergleich zur Berechnungsdauer für die Tate Paarung, eine Beschleunigung um den Faktor $\approx 1,9$ ergeben. Im Vergleich zur Ate Paarung mit $S \equiv q \mod r$ ergab sich ein Faktor von $\approx 1,4$.

Zum Abschluss dieser Arbeit haben wir einige Anwendungen und die sicherheitstheoretischen Aspekte betrachtet. Wir haben verschiedene kryptographische Protokolle, in

denen Paarungen zum Einsatz kommen, angegeben und die mathematischen Problemstellungen in Grundzügen untersucht. Die Sicherheit dieser Anwendungen haben wir auf die Auswahl der Parameter für paarungsfreundlichen Kurven und die Schwierigkeit der Paarungsinvertierungen zurückgeführt.

In dieser Arbeit haben sich Fragen ergeben, deren Untersuchung im Kontext der betrachteten Paarungen interessant ist.

- Ist eine weitergehende Verallgemeinerung, ähnlich der Erweiterung auf die Ate_i Paarung, für die hyperelliptische Ate Paarung möglich?
- Können die Gitterkonstruktionen analog für hyperelliptische Kurven übersetzt werden?
- Kann die Vorgehensweise der Verwendung aller Frobenius-Potenzen π_q^i, für Potenzen $i = 0, \ldots, k-1$ ebenso effizient auf andere Familien von parametrisierten, elliptischen Kurven verallgemeinert werden?

Weiterhin ist das Gebiet der Invertierungen von Paarungen ein bislang wenig untersuchtes Gebiet. Die Schwierigkeit dieses Problems ist jedoch eine wichtige Komponente der Sicherheit von paarungsbasierten Kryptosystemen.

Literaturverzeichnis

[Bar] Barreto, P.. – "http://paginas.terra.com.br/informatica/paulobarreto/pblounge.html"

[BF03] Boneh, D. ; Franklin, M.: Identity-Based Encryption from the Weil Pairing. In: *SIAM J. Comput.* 32 (2003), Nr. 3, S. 586–615

[BGhS04] Barreto, P. S. L. M. ; Galbraith, S. D. ; hEigeartaigh, C. O. ; Scott, M. *Efficient Pairing Computation on Supersingular Abelian Varieties*. Cryptology ePrint Archive, Report 2004/375. 2004

[BK98] Balasubramanian, R. ; Koblitz, N.: The Improbability That an Elliptic Curve Has Subexponential Discrete Log Problem under the Menezes-Okamoto-Vanstone Algorithm. In: *Journal of Cryptology* 11 (1998), Nr. 2, S. 141–145

[BKLS02] Barreto, P. S. L. M. ; Kim, H. Y. ; Lynn, B. ; Scott, M. *Efficient Algorithms for Pairing-Based Cryptosystems*. Cryptology ePrint Archive, Report 2002/008. 2002

[BLS01] Boneh, D. ; Lynn, B. ; Shacham, H.: Short Signatures from the Weil Pairing. In: *ASIACRYPT '01: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security*. London, UK : Springer, 2001, S. 514–532

[BN05] Barreto, P. S. L. M. ; Naehrig, M. *Pairing-Friendly Elliptic Curves of Prime Order*. Cryptology ePrint Archive, Report 2005/133. 2005

[Bos06] Bosch, S.: *Algebra*. Berlin : Springer, 2006

[BSSC05] Blake, I. ; Seroussi, G. ; Smart, N. ; Cassels, J. W. S.: *Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series)*. New York, NY, USA : Cambridge University Press, 2005

[Buc03] Buchmann, J.: *Einführung in die Kryptographie*. Berlin : Springer, 2003

[Can87] Cantor, D. G.: Computing in the Jacobian of a Hyperelliptic Curve. In: *Mathematics of Computation* 48 (1987), Nr. 177, S. 95–101

[CF06] Cohen, H. ; Frey, G.: *Handbook of elliptic and hyperelliptic curve cryptography*. Chapman & Hall/CRC, 2006

[DBS03] Dutta, R. ; Barua, R. ; Sarkar, P. *Extending Joux's Protocol to Multi Party Key Argeement*. Cryptology ePrint Archive, Report 2003/062. 2003

[DBS04] Dutta, R. ; Barua, R. ; Sarkar, P. *Pairing-Based Cryptographic Protocols : A Survey*. Cryptology ePrint Archive, Report 2004/064. 2004

[DL03] Duursma, I. ; Lee, H.: Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$. In: *Advances in Cryptology - ASIACRYPT 2003* Bd. 2894/2003, Springer, 2003, S. 111–123

[FST06a] Fay, B. ; Schweisgut, J. ; Tobias, C.: Identitätsbasierte Kryptografie - Hindernisse auf dem Weg von der Theorie in die Praxis. In: *Sicherheit*, 2006, S. 317–328

[FST06b] Freeman, D. ; Scott, M. ; Teske, E. *A taxonomy of pairing-friendly elliptic curves*. Cryptology ePrint Archive, Report 2006/372. 2006

[GHO+07] Granger, R. ; Hess, F. ; Oyono, R. ; Theriault, N. ; Vercauteren, F.: Ate Pairing on Hyperelliptic Curves. In: *Advances in Cryptology - EUROCRYPT 2007*, Springer, LNCS 4515, 2007, S. 430–447

[GHS02] Galbraith, S. D. ; Harrison, K. ; Soldera, D.: Implementing the Tate Pairing. In: *ANTS-V: Proceedings of the 5th International Symposium on Algorithmic Number Theory*, Springer, 2002, S. 324–337

[GHV07a] Galbraith, S. D. ; Hess, F. ; Vercauteren, F. *Aspects of Pairing Inversion*. Cryptology ePrint Archive, Report 2007/256. 2007

[GHV07b] Galbraith, S. D. ; Hess, F. ; Vercauteren, F.: Hyperelliptic Pairings. In: *Pairing* Bd. 4575, Springer, 2007, S. 108–131

[Hes03] Hess, F.: Efficient Identity Based Signature Schemes Based on Pairings. In: *SAC '02: Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography*, Springer, 2003, S. 310–324

[Hes06] Hess, F.: *Kryptographie mit elliptischen Kurven*. Computeralgebra Rundbrief. 2006. – `www.math.tu-berlin.de/hess/personal/ca-brief.pdf`

[Hes08] Hess, F. *Pairing Lattices*. Cryptology ePrint Archive, Report 2008/125. 2008

[Hit07] Hitt, L.: On the Minimal Embedding Field. In: Takagi, T. (Hrsg.) ; Okamoto, T. (Hrsg.) ; Okamoto, E. (Hrsg.) ; Okamoto, T. (Hrsg.): *Pairing* Bd. 4575, Springer, 2007, S. 294–301

[HSV06] Hess, F. ; Smart, N. P. ; Vercauteren, F. *The Eta Pairing Revisited*. Cryptology ePrint Archive, Report 2006/110. 2006

[Hul02] Hulek, K.: *Elementare Algebraische Geometrie*. Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, 2002

[JN01] Joux, A. ; Nguyen, K.: Separating Decision Diffie-Hellman from Diffie-Hellman in cryptographic groups. 2001 (2001/003). – Forschungsbericht

[Jou00] Joux, A.: A One Round Protocol for Tripartite Diffie-Hellman. In: *ANTS IV: Proceedings of the 4th International Symposium on Algorithmic Number Theory*, Springer, 2000, S. 385–394

[LLL82] Lenstra, A. K. ; Lenstra, H. W. ; Lovász, L.: Factoring polynomials with rational coefficients. In: *Mathematische Annalen* 261 (1982), Nr. 4, S. 515–534

[LLP08] Lee, E. ; Lee, H. ; Park, C. *Efficient and Generalized Pairing Computation on Abelian Varieties*. Cryptology ePrint Archive, Report 2008/040. 2008

[Maa04] Maas, M.: *Pairing-Based Cryptography*, Technische Universiteit Eindhoven, Diplomarbeit, 2004. – `http://www.win.tue.nl/~bdeweger/MTMartijnMaas.pdf`

[MKHO07] Matsuda, S. ; Kanayama, N. ; Hess, F. ; Okamoto, E. *Optimised versions of the Ate and Twisted Ate Pairings*. Cryptology ePrint Archive, Report 2007/013. 2007

[MOV91] Menezes, A. ; Okamoto, T. ; Vanstone, S.: Reducing elliptic curve logarithms to logarithms in a finite field. In: *STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing*, ACM, 1991, S. 80–89

[Mül98] Müller, V.: Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two. In: *Journal of Cryptology* 11 (1998), Nr. 4, S. 219–234

[Odl84] Odlyzko, A. M.: Discrete Logarithms in Finite Fields and Their Cryptographic Significance. In: *Theory and Application of Cryptographic Techniques*, 1984, S. 224–314

[Rue99] Rueck, H.: On the Discrete Logarithm in the Divisor Class Group of Curves. In: *Mathematics of Computation* 68 (1999), Nr. 226, S. 805–806

[Sco05] Scott, M.: Faster Pairings Using an Elliptic Curve with an Efficient Endomorphism. In: *INDOCRYPT*, 2005, S. 258–269

[Sha79] Shamir, A.: How to share a secret. In: *Commun. ACM* 22 (1979), Nr. 11, S. 612–613

[Shi03] Shim, K.: Efficient one round tripartite authenticated key agreement protocol from Weil pairing. In: *Electronics Letters* 39 (2003), Nr. 2, S. 208–209

[Sil86] Silverman, J. H.: *The arithmetic of elliptic curves*. Springer, 1986

[Sil94] SILVERMAN, J. H.: *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer, 1994

[Sin01] SINGH, S.: *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet.* DTV, 2001

[Sma99] SMART, N. P.: Elliptic Curve Cryptosystems over Small Fields of Odd Characteristic. In: *Journal of Cryptology* 12 (1999), Nr. 2, S. 141–151

[Tak07] TAKASHIMA, K.: Scaling Security of Elliptic Curves with Fast Pairing Using Efficient Endomorphisms. In: *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* E90-A (2007), Nr. 1, S. 152–159

[Tes00] TESKE, E. *On random walks for Pollard's rho method*. 2000

[Ver01] VERHEUL, E.: Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems. In: *EUROCRYPT '01: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques*. London, UK : Springer, 2001, S. 195–210

[Ver08] VERCAUTEREN, F. *Optimal Pairings*. Cryptology ePrint Archive, Report 2008/096. 2008

[vW99] VAN OORSCHOT, P. C. ; WIENER, M. J.: Parallel Collision Search with Cryptanalytic Applications. In: *Journal of Cryptology: the journal of the International Association for Cryptologic Research* 12 (1999), Nr. 1, S. 1–28

[Wat69] WATERHOUSE, W.C.: Abelian varieties over finite fields. (1969)

[Wer02] WERNER, A.: *Elliptische Kurven in der Kryptographie*. Berlin : Springer, 2002

[ZZH07] ZHAO, C. ; ZHANG, F. ; HUANG, J. *A Note on the Ate Pairing*. Cryptology ePrint Archive, Report 2007/247. 2007