

# Paarungen in der Kryptographie

Osmanbey Uzunkol

Fakultät für Mathematik  
Technische Universität Berlin

18.01.2006

# Outline

- 1 Grundlagen**
  - Bilineare Paarungen
  - Elliptische Kurven
  - Divisorentheorie
- 2 Tate Paarung**
  - Definition
  - Berechnung
  - Anwendung
- 3 Einbettungsgrad**
  - Kurven mit kleinem Einbettungsgrad
  - Supersingulare Kurven
  - MNT Kurven
- 4 Distortionsabbildungen**
  - Definition
  - Modifizierte Tate Paarung

# Outline

- 1 Grundlagen**
  - Bilineare Paarungen
  - Elliptische Kurven
  - Divisorentheorie
- 2 Tate Paarung
  - Definition
  - Berechnung
  - Anwendung
- 3 Einbettungsgrad
  - Kurven mit kleinem Einbettungsgrad
  - Supersingulare Kurven
  - MNT Kurven
- 4 Distortionsabbildungen
  - Definition
  - Modifizierte Tate Paarung

# Definition

## Was brauchen Wir?

- Seien  $G_1$ ,  $G_2$  sind zwei additive Gruppen der Ordnung  $n$  und  $G_3$  eine zyklische multiplikative Gruppe der Ordnung  $n$ .
- Eine *Paarung* ist eine Abbildung

$$e : G_1 \times G_2 \rightarrow G_3$$

- Die Paarungen, die wir betrachten werden besitzen die folgende Eigenschaften

## Bilinearität

Für alle  $P, P' \in G_1$  und  $Q, Q' \in G_2$  haben wir

$$e(P + P', Q) = e(P, Q)e(P', Q) \text{ und}$$

$$e(P, Q + Q') = e(P, Q)e(P, Q')$$

## Nicht-ausgeartet

- Für alle  $P \in G_1$  mit  $P \neq 0$  existiert ein  $Q \in G_2$  so dass  $e(P, Q) \neq 1$
- Für alle  $Q \in G_2$  mit  $Q \neq 0$  existiert ein  $P \in G_1$  so dass  $e(P, Q) \neq 1$

## Bilinearität

Für alle  $P, P' \in G_1$  und  $Q, Q' \in G_2$  haben wir

$$e(P + P', Q) = e(P, Q)e(P', Q) \text{ und}$$

$$e(P, Q + Q') = e(P, Q)e(P, Q')$$

## Nicht-ausgeartet

- Für alle  $P \in G_1$  mit  $P \neq 0$  existiert ein  $Q \in G_2$  so dass  $e(P, Q) \neq 1$
- Für alle  $Q \in G_2$  mit  $Q \neq 0$  existiert ein  $P \in G_1$  so dass  $e(P, Q) \neq 1$

## Lemma

Seien  $e$  eine bilineare Abbildung und  $P \in G_1$ ,  $Q \in G_2$ . Dann

- 1  $e(P, 0) = e(0, Q) = 1$ .
- 2  $e(-P, Q) = e(P, Q)^{-1} = e(P, -Q)$ .
- 3  $e([j]P, Q) = e(P, Q)^j = e(P, [j]Q)$  für alle  $j \in \mathbb{Z}$ .

# Definition

## Weierstrassche Gleichung

Seien  $K$  ein Körper und  $\overline{K}$  der algebraische Abschluss von  $K$ . Sei weiter  $F(X, Y, Z)$  ein glattes homogenes Polynom definiert über  $\mathbb{P}^2(\overline{K})$  und gegeben durch

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

- Eine *elliptische Kurve*  $E$  ist die Menge der Nullstellen eines solchen Polynoms  $F$ .
- Es existiert genau ein Punkt  $\mathcal{O} = (0 : 1 : 0)$  in  $E$  mit  $Z = 0$ . Dieser Punkt heisst *Punkt auf unendlichen*.
- Man kann die folgende Gleichung erhalten, wenn  $Z \neq 0$  ist

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

## Die Lösung

Man kann die folgende Gleichung erhalten, wenn  $Z \neq 0$  ist

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

wobei  $x = \frac{X}{Z}$  und  $y = \frac{Y}{Z}$ .

## Forderungen

Wenn  $\text{char}(K) \neq 2, 3$  ist, dann ist jede elliptische Kurve isomorph zu

$$y^2 = x^3 + ax + b.$$

## Die Lösung

Man kann die folgende Gleichung erhalten, wenn  $Z \neq 0$  ist

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

wobei  $x = \frac{X}{Z}$  und  $y = \frac{Y}{Z}$ .

## Forderungen

Wenn  $\text{char}(K) \neq 2, 3$  ist, dann ist jede elliptische Kurve isomorph zu

$$y^2 = x^3 + ax + b.$$

## Punktgruppe einer elliptischen Kurve

- Die Punkten einer elliptischen Kurve bilden eine additive Gruppe mit Nullelement  $\mathcal{O}$ , die mittels *tangent-and-chord-method* beschrieben werden kann.
- Man kann explizit die Addition zweier Punkte geben. Wir geben die Summe falls  $\text{char}(K) > 3$  ist:

• Eingabe  $P = (x_1, y_1) \neq \mathcal{O}$ ,  $Q = (x_2, y_2) \neq \mathcal{O}$

$$P + Q = \left( x_3, y_3 \right) = \left( x_1 + x_2 + \frac{y_1^2 - y_2^2}{x_1 - x_2}, y_3 \right)$$

$$y_3 = -y_1 - y_2 + \frac{y_1^2 - y_2^2}{x_1 - x_2} \left( x_1 + x_2 + \frac{y_1^2 - y_2^2}{x_1 - x_2} \right)$$

$$\text{falls } P = Q \text{ (Tangentenmethode)}$$

$$P + P = \left( x_3, y_3 \right) = \left( x_1 + \frac{2y_1^2}{x_1^2 - y_1^2}, y_3 \right)$$

$$y_3 = -y_1 + \frac{2y_1^2}{x_1^2 - y_1^2} \left( x_1 + \frac{2y_1^2}{x_1^2 - y_1^2} \right)$$

- Man kann auch dann skalare Multiplikation folgendermassen definieren

$$[m]P = P + \dots + P \text{ (} m\text{-mal) für } m > 0 \text{ und}$$

$$[0]P = \mathcal{O}, \text{ und } [-m]P = [m](-P) \text{ für } m < 0$$

## Punktgruppe einer elliptischen Kurve

- Die Punkten einer elliptischen Kurve bilden eine additive Gruppe mit Nullelement  $\mathcal{O}$ , die mittels *tangent-and-chord-method* beschrieben werden kann.
- Man kann explizit die Addition zweier Punkte geben. Wir geben die Summe falls  $\text{char}(K) > 3$  ist:
  - Eingabe**  $P = (x_1, y_1) \neq \mathcal{O}$ ,  $Q = (x_2, y_2) \neq \mathcal{O}$
  - Ausgabe**  $P + Q = (x_3, y_3)$
  - $x_3 = \lambda^2 - x_1 - x_2$  und  $y_3 = \lambda(x_1 - x_3) - y_1$ , wobei
 
$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{falls } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{falls } P = Q \end{cases}$$
- Man kann auch dann skalare Multiplikation folgendermassen definieren

$$[m]P = P + \cdots + P \quad (m\text{-mal}) \quad \text{für } m > 0 \quad \text{und}$$

$$[0]P = \mathcal{O}, \quad \text{und} \quad [-m]P = [m](-P) \quad \text{für } m < 0$$

## Punktgruppe einer elliptischen Kurve

- Die Punkten einer elliptischen Kurve bilden eine additive Gruppe mit Nullelement  $\mathcal{O}$ , die mittels *tangent-and-chord-method* beschrieben werden kann.
- Man kann explizit die Addition zweier Punkte geben. Wir geben die Summe falls  $\text{char}(K) > 3$  ist:
  - Eingabe**  $P = (x_1, y_1) \neq \mathcal{O}$ ,  $Q = (x_2, y_2) \neq \mathcal{O}$
  - Ausgabe**  $P + Q = (x_3, y_3)$
  - $x_3 = \lambda^2 - x_1 - x_2$  und  $y_3 = \lambda(x_1 - x_3) - y_1$ , wobei
 
$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{falls } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{falls } P = Q \end{cases}$$
- Man kann auch dann skalare Multiplikation folgendermassen definieren

$$[m]P = P + \cdots + P \quad (m\text{-mal}) \quad \text{für } m > 0 \quad \text{und}$$

$$[0]P = \mathcal{O}, \quad \text{und} \quad [-m]P = [m](-P) \quad \text{für } m < 0$$

## Punktgruppe einer elliptischen Kurve

- Die Punkten einer elliptischen Kurve bilden eine additive Gruppe mit Nullelement  $\mathcal{O}$ , die mittels *tangent-and-chord-method* beschrieben werden kann.
- Man kann explizit die Addition zweier Punkte geben. Wir geben die Summe falls  $\text{char}(K) > 3$  ist:
  - Eingabe**  $P = (x_1, y_1) \neq \mathcal{O}$ ,  $Q = (x_2, y_2) \neq \mathcal{O}$
  - Ausgabe**  $P + Q = (x_3, y_3)$
  - $x_3 = \lambda^2 - x_1 - x_2$  und  $y_3 = \lambda(x_1 - x_3) - y_1$ , wobei
 
$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{falls } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{falls } P = Q \end{cases}$$
- Man kann auch dann skalare Multiplikation folgenermasse definieren

$$[m]P = P + \cdots P \quad (m\text{-mal}) \quad \text{für } m > 0 \quad \text{und}$$

$$[0]P = \mathcal{O}, \quad \text{und} \quad [-m]P = [m](-P) \quad \text{für } m < 0$$

## Punktgruppe einer elliptischen Kurve

- Die Punkten einer elliptischen Kurve bilden eine additive Gruppe mit Nullelement  $\mathcal{O}$ , die mittels *tangent-and-chord-method* beschrieben werden kann.
- Man kann explizit die Addition zweier Punkte geben. Wir geben die Summe falls  $\text{char}(K) > 3$  ist:
  - Eingabe**  $P = (x_1, y_1) \neq \mathcal{O}$ ,  $Q = (x_2, y_2) \neq \mathcal{O}$
  - Ausgabe**  $P + Q = (x_3, y_3)$
  - $x_3 = \lambda^2 - x_1 - x_2$  und  $y_3 = \lambda(x_1 - x_3) - y_1$ , wobei
 
$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{falls } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{falls } P = Q \end{cases}$$
- Man kann auch dann skalare Multiplikation folgendermassen definieren

$$[m]P = P + \cdots + P \quad (m\text{-mal}) \quad \text{für } m > 0 \text{ und}$$

$$[0]P = \mathcal{O}, \text{ und } [-m]P = [m](-P) \text{ für } m < 0$$

## Punktgruppe einer elliptischen Kurve

- Die Punkten einer elliptischen Kurve bilden eine additive Gruppe mit Nullelement  $\mathcal{O}$ , die mittels *tangent-and-chord-method* beschrieben werden kann.
- Man kann explizit die Addition zweier Punkte geben. Wir geben die Summe falls  $\text{char}(K) > 3$  ist:
  - Eingabe**  $P = (x_1, y_1) \neq \mathcal{O}$ ,  $Q = (x_2, y_2) \neq \mathcal{O}$
  - Ausgabe**  $P + Q = (x_3, y_3)$
  - $x_3 = \lambda^2 - x_1 - x_2$  und  $y_3 = \lambda(x_1 - x_3) - y_1$ , wobei
 
$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{falls } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{falls } P = Q \end{cases}$$
- Man kann auch dann skalare Multiplikation folgenermasse definieren

$$[m]P = P + \dots + P \quad (m\text{-mal}) \quad \text{für } m > 0 \quad \text{und}$$

$$[0]P = \mathcal{O}, \quad \text{und} \quad [-m]P = [m](-P) \quad \text{für } m < 0$$

## Torsionspunkte

- Wenn  $[n]P = \mathcal{O}$  für  $P \in E$ , dann heisst  $P$  ein  $n$ -Torsionspunkt.
- Die Untergruppe  $E[n]$  der  $n$ -Torsionspunkte ist gegeben durch

$$E[n] = \{P \in E : [n]P = \mathcal{O}\} \text{ bzw. } E(K)[n] = \{P \in E(K) : [n]P = \mathcal{O}\}$$

## Hasse

Sei  $E$  eine elliptische Kurve über  $\mathbb{F}_q$ .

- *Spur von Frobenius* ist die Zahl  $t$  mit

$$|E(\mathbb{F}_q)| = q + 1 - t$$

- **Satz von Hasse**  $|t| \leq 2\sqrt{q}$ .

## Torsionspunkte

- Wenn  $[n]P = \mathcal{O}$  für  $P \in E$ , dann heisst  $P$  ein  $n$ -Torsionspunkt.
- Die Untergruppe  $E[n]$  der  $n$ -Torsionspunkte ist gegeben durch

$$E[n] = \{P \in E : [n]P = \mathcal{O}\} \text{ bzw. } E(K)[n] = \{P \in E(K) : [n]P = \mathcal{O}\}$$

## Hasse

Sei  $E$  eine elliptische Kurve über  $\mathbb{F}_q$ .

- *Spur von Frobenius* ist die Zahl  $t$  mit

$$|E(\mathbb{F}_q)| = q + 1 - t$$

- **Satz von Hasse**  $|t| \leq 2\sqrt{q}$ .

## Bemerkungen

- **Silverman** Wenn  $(n, q) = 1$  dann

$$E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

- Nach Silverman wenn  $(n, q) = 1$  ist, dann ist die Zahl der  $E[n]$  gleich  $n^2$ . Ferner wenn  $n$  prim ist, dann ist  $E[n]$  erzeugt von zwei linear unabhängigen  $n$ -Torsionspunkte.
- Eine rationale Abbildung von  $E$  nach  $E$  heisst *Endomorphismus*. Die ist auch ein Gruppenhomomorphismus, z.B. Multiplikation bei  $m$ . Für die Kurven definiert über  $\mathbb{F}_q$  haben wir auch der sogenannte *Frobenius Endomorphismus*  $\Phi$ , der den Punkt  $(x, y)$  zu  $(x^q, y^q)$  zuschickt. Dann ist es einfach zu sehen

$$P \in E(\mathbb{F}_q) \text{ genau dann, wenn } \Phi(P) = P.$$

## Bemerkungen

- **Silverman** Wenn  $(n, q) = 1$  dann

$$E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

- Nach Silverman wenn  $(n, q) = 1$  ist, dann ist die Zahl der  $E[n]$  gleich  $n^2$ . Ferner wenn  $n$  prim ist, dann ist  $E[n]$  erzeugt von zwei linear unabhängigen  $n$ -Torsionspunkte.
- Eine rationale Abbildung von  $E$  nach  $E$  heisst *Endomorphismus*. Die ist auch ein Gruppenhomomorphismus, z.B. Multiplikation bei  $m$ . Für die Kurven definiert über  $\mathbb{F}_q$  haben wir auch der sogenannte *Frobenius Endomorphismus*  $\Phi$ , der den Punkt  $(x, y)$  zu  $(x^q, y^q)$  zuschickt. Dann ist es einfach zu sehen

$$P \in E(\mathbb{F}_q) \text{ genau dann, wenn } \Phi(P) = P.$$

## Bemerkungen

- **Silverman** Wenn  $(n, q) = 1$  dann

$$E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

- Nach Silverman wenn  $(n, q) = 1$  ist, dann ist die Zahl der  $E[n]$  gleich  $n^2$ . Ferner wenn  $n$  prim ist, dann ist  $E[n]$  erzeugt von zwei linear unabhängigen  $n$ -Torsionspunkte.
- Eine rationale Abbildung von  $E$  nach  $E$  heisst *Endomorphismus*. Die ist auch ein Gruppenhomomorphismus, z.B. Multiplikation bei  $m$ . Für die Kurven definiert über  $\mathbb{F}_q$  haben wir auch der sogenannte *Frobenius Endomorphismus*  $\Phi$ , der den Punkt  $(x, y)$  zu  $(x^q, y^q)$  zuschickt. Dann ist es einfach zu sehen

$$P \in E(\mathbb{F}_q) \text{ genau dann, wenn } \Phi(P) = P.$$

## Divisoren

- Für unser Zweck, ist ein *Divisor* eine formale Summe auf der Kurve  $E(\mathbb{F}_{q^m})$ ,  $m > 0$ , d. H.

$$\mathcal{A} = \sum_{P \in E} a_P(P).$$

- Grad der divisor  $\mathcal{A}$  ist  $\deg(\mathcal{A}) = \sum_{P \in E} a_P$ .
- Die Menge der Divisoren bildet eine abelsche Gruppe.
- Seien  $f : E(\mathbb{F}_{q^k}) \rightarrow E(\mathbb{F}_{q^k})$  eine Funktion auf der Kurve und  $\mathcal{A} = \sum_{P \in E} a_P(P)$  ein Divisor vom Grad 0. Dann definieren wir

$$f(\mathcal{A}) = \prod_P f(P)^{a_P}$$

- Weil  $\sum_P a_P = 0$  ist, haben wir  $f(\mathcal{A}) = (cf)(\mathcal{A})$  für alle  $c \in \mathbb{F}_{q^k}^*$

## Divisoren

- Für unser Zweck, ist ein *Divisor* eine formale Summe auf der Kurve  $E(\mathbb{F}_{q^m})$ ,  $m > 0$ , d. H.

$$\mathcal{A} = \sum_{P \in E} a_P(P).$$

- Grad der divisor  $\mathcal{A}$  ist  $\deg(\mathcal{A}) = \sum_{P \in E} a_P$ .
- Die Menge der Divisoren bildet eine abelsche Gruppe.
- Seien  $f : E(\mathbb{F}_{q^k}) \rightarrow E(\mathbb{F}_{q^k})$  eine Funktion auf der Kurve und  $\mathcal{A} = \sum_{P \in E} a_P(P)$  ein Divisor vom Grad 0. Dann definieren wir

$$f(\mathcal{A}) = \prod_P f(P)^{a_P}$$

- Weil  $\sum_P a_P = 0$  ist, haben wir  $f(\mathcal{A}) = (cf)(\mathcal{A})$  für alle  $c \in \mathbb{F}_{q^k}^*$

## Divisoren

- Für unser Zweck, ist ein *Divisor* eine formale Summe auf der Kurve  $E(\mathbb{F}_{q^m})$ ,  $m > 0$ , d. H.

$$\mathcal{A} = \sum_{P \in E} a_P(P).$$

- Grad der divisor  $\mathcal{A}$  ist  $\deg(\mathcal{A}) = \sum_{P \in E} a_P$ .
- Die Menge der Divisoren bildet eine abelsche Gruppe.
- Seien  $f : E(\mathbb{F}_{q^k}) \rightarrow E(\mathbb{F}_{q^k})$  eine Funktion auf der Kurve und  $\mathcal{A} = \sum_{P \in E} a_P(P)$  ein Divisor vom Grad 0. Dann definieren wir

$$f(\mathcal{A}) = \prod_P f(P)^{a_P}$$

- Weil  $\sum_P a_P = 0$  ist, haben wir  $f(\mathcal{A}) = (cf)(\mathcal{A})$  für alle  $c \in \mathbb{F}_{q^k}^*$

## Divisoren

- Für unser Zweck, ist ein *Divisor* eine formale Summe auf der Kurve  $E(\mathbb{F}_{q^m})$ ,  $m > 0$ , d. H.

$$\mathcal{A} = \sum_{P \in E} a_P(P).$$

- Grad der divisor  $\mathcal{A}$  ist  $\deg(\mathcal{A}) = \sum_{P \in E} a_P$ .
- Die Menge der Divisoren bildet eine abelsche Gruppe.
- Seien  $f : E(\mathbb{F}_{q^k}) \rightarrow E(\mathbb{F}_{q^k})$  eine Funktion auf der Kurve und  $\mathcal{A} = \sum_{P \in E} a_P(P)$  ein Divisor vom Grad 0. Dann definieren wir

$$f(\mathcal{A}) = \prod_P f(P)^{a_P}$$

- Weil  $\sum_P a_P = 0$  ist, haben wir  $f(\mathcal{A}) = (cf)(\mathcal{A})$  für alle  $c \in \mathbb{F}_{q^k}^*$

## Divisoren

- Für unser Zweck, ist ein *Divisor* eine formale Summe auf der Kurve  $E(\mathbb{F}_{q^m})$ ,  $m > 0$ , d. H.

$$\mathcal{A} = \sum_{P \in E} a_P(P).$$

- Grad der divisor  $\mathcal{A}$  ist  $\deg(\mathcal{A}) = \sum_{P \in E} a_P$ .
- Die Menge der Divisoren bildet eine abelsche Gruppe.
- Seien  $f : E(\mathbb{F}_{q^k}) \rightarrow E(\mathbb{F}_{q^k})$  eine Funktion auf der Kurve und  $\mathcal{A} = \sum_{P \in E} a_P(P)$  ein Divisor vom Grad 0. Dann definieren wir

$$f(\mathcal{A}) = \prod_P f(P)^{a_P}$$

- Weil  $\sum_P a_P = 0$  ist, haben wir  $f(\mathcal{A}) = (cf)(\mathcal{A})$  für alle  $c \in \mathbb{F}_{q^k}^*$

## Bemerkungen

- Divisor einer Funktion  $f$  ist

$$(f) \equiv \sum_P \text{ord}_P(f)(P).$$

- $\text{ord}_P(f)$  ist die Ordnung von Null- und Polstellen von  $f$  auf  $P$ .
- Ein Divisor  $\mathcal{A}$  heißt *Hauptdivisor*, wenn  $\mathcal{A} = (f)$  für eine  $f$ .  
 $\sum_P a_P(P)$  ist genau dann Hauptdivisor, wenn  $\deg(\mathcal{A}) = 0$  und  $\sum_P a_P P = \mathcal{O}$  sind.
- Die Divisoren  $\mathcal{A}$  und  $\mathcal{B}$  sind *äquivalent*,  $\mathcal{A} \sim \mathcal{B}$ , wenn  $\mathcal{A} - \mathcal{B}$  ein Hauptdivisor ist. Dann für  $P \in E[n]$ ,  $(n, q) = 1$ , und für  $\mathcal{A}_P$  äquivalent zu  $(P) - (\mathcal{O})$ , dann existiert nach Definition  $(f_P) = n\mathcal{A}_P$  ein Hauptdivisor

## Bemerkungen

- Divisor einer Funktion  $f$  ist

$$(f) \equiv \sum_P \text{ord}_P(f)(P).$$

- $\text{ord}_P(f)$  ist die Ordnung von Null- und Polstellen von  $f$  auf  $P$ .
- Ein Divisor  $\mathcal{A}$  heißt *Hauptdivisor*, wenn  $\mathcal{A} = (f)$  für eine  $f$ .  
 $\sum_P a_P(P)$  ist genau dann Hauptdivisor, wenn  $\deg(\mathcal{A}) = 0$  und  $\sum_P a_P P = \mathcal{O}$  sind.
- Die Divisoren  $\mathcal{A}$  und  $\mathcal{B}$  sind *äquivalent*,  $\mathcal{A} \sim \mathcal{B}$ , wenn  $\mathcal{A} - \mathcal{B}$  ein Hauptdivisor ist. Dann für  $P \in E[n]$ ,  $(n, q) = 1$ , und für  $\mathcal{A}_P$  äquivalent zu  $(P) - (\mathcal{O})$ , dann existiert nach Definition  $(f_P) = n\mathcal{A}_P$  ein Hauptdivisor

## Bemerkungen

- Divisor einer Funktion  $f$  ist

$$(f) \equiv \sum_P \text{ord}_P(f)(P).$$

- $\text{ord}_P(f)$  ist die Ordnung von Null- und Polstellen von  $f$  auf  $P$ .
- Ein Divisor  $\mathcal{A}$  heißt *Hauptdivisor*, wenn  $\mathcal{A} = (f)$  für eine  $f$ .  
 $\sum_P a_P(P)$  ist genau dann Hauptdivisor, wenn  $\deg(\mathcal{A}) = 0$  und  $\sum_P a_P P = \mathcal{O}$  sind.
- Die Divisoren  $\mathcal{A}$  und  $\mathcal{B}$  sind *äquivalent*,  $\mathcal{A} \sim \mathcal{B}$ , wenn  $\mathcal{A} - \mathcal{B}$  ein Hauptdivisor ist. Dann für  $P \in E[n]$ ,  $(n, q) = 1$ , und für  $\mathcal{A}_P$  äquivalent zu  $(P) - (\mathcal{O})$ , dann existiert nach Definition  $(f_P) = n\mathcal{A}_P$  ein Hauptdivisor

## Bemerkungen

- Divisor einer Funktion  $f$  ist

$$(f) \equiv \sum_P \text{ord}_P(f)(P).$$

- $\text{ord}_P(f)$  ist die Ordnung von Null- und Polstellen von  $f$  auf  $P$ .
- Ein Divisor  $\mathcal{A}$  heißt *Hauptdivisor*, wenn  $\mathcal{A} = (f)$  für eine  $f$ .  
 $\sum_P a_P(P)$  ist genau dann Hauptdivisor, wenn  $\deg(\mathcal{A}) = 0$  und  $\sum_P a_P P = \mathcal{O}$  sind.
- Die Divisoren  $\mathcal{A}$  und  $\mathcal{B}$  sind *äquivalent*,  $\mathcal{A} \sim \mathcal{B}$ , wenn  $\mathcal{A} - \mathcal{B}$  ein Hauptdivisor ist. Dann für  $P \in E[n]$ ,  $(n, q) = 1$ , und für  $\mathcal{A}_P$  äquivalent zu  $(P) - (\mathcal{O})$ , dann existiert nach Definition  $(f_P) = n\mathcal{A}_P$  ein Hauptdivisor

# Outline

- 1 Grundlagen
  - Bilineare Paarungen
  - Elliptische Kurven
  - Divisorentheorie
- 2 Tate Paarung**
  - Definition
  - Berechnung
  - Anwendung
- 3 Einbettungsgrad
  - Kurven mit kleinem Einbettungsgrad
  - Supersingulare Kurven
  - MNT Kurven
- 4 Distortionsabbildungen
  - Definition
  - Modifizierte Tate Paarung

## Definition

- Sei  $l \in \mathbb{N}$  mit  $(l, q) = 1$ . Die *Tate Paarung* der Ordnung  $l$  ist die Abbildung

$$e_l : E(\mathbb{F}_q)[l] \times : E(\mathbb{F}_{q^k})[l] \rightarrow \mathbb{F}_{q^k}^*,$$

definiert durch

$$e_l(P, Q) = f_P(\mathcal{A}_Q)^{(q^k-1)/l}.$$

- Eigenschaften**

$e_l$  ist wohldefiniert!

$e_l$  ist eine bilineare Paarung  $f_P$  ist die  $l$ -te Potenzfunktion

$f_P(x) = x^l$

- Kompatibilität:** Sei  $l = hl'$ . Wenn  $P \in E(\mathbb{F}_q)[l]$  und  $Q \in E(\mathbb{F}_q)[l']$ , dann  $e_{l'}(hP, Q) = e_l(P, Q)^h$ .
- Bemerkung:** Weil  $P \in E(\mathbb{F}_q)$  ist, ist  $f_P$  eine rationale Funktion mit Koeffizienten in  $\mathbb{F}_q$ .

## Definition

- Sei  $l \in \mathbb{N}$  mit  $(l, q) = 1$ . Die *Tate Paarung* der Ordnung  $l$  ist die Abbildung

$$e_l : E(\mathbb{F}_q)[l] \times : E(\mathbb{F}_{q^k})[l] \rightarrow \mathbb{F}_{q^k}^*,$$

definiert durch

$$e_l(P, Q) = f_P(\mathcal{A}_Q)^{(q^k-1)/l}.$$

- Eigenschaften**

- $e_l$  ist wohldefiniert!

- $e_l$  ist eine bilieare Paarung, d. H.  $e_l$  ist bilinear und nicht-ausgeartet.

- Kompatibilität:** Sei  $l = hl'$ . Wenn  $P \in E(\mathbb{F}_q)[l]$  und  $Q \in E(\mathbb{F}_q)[l']$ , dann  $e_{l'}(hP, Q) = e_l(P, Q)^h$ .

- Bemerkung:** Weil  $P \in E(\mathbb{F}_q)$  ist, ist  $f_P$  eine rationale Funktion mit Koeffizienten in  $\mathbb{F}_q$ .

## Definition

- Sei  $l \in \mathbb{N}$  mit  $(l, q) = 1$ . Die *Tate Paarung* der Ordnung  $l$  ist die Abbildung

$$e_l : E(\mathbb{F}_q)[l] \times : E(\mathbb{F}_{q^k})[l] \rightarrow \mathbb{F}_{q^k}^*,$$

definiert durch

$$e_l(P, Q) = f_P(\mathcal{A}_Q)^{(q^k-1)/l}.$$

- **Eigenschaften**

- 1  $e_l$  ist wohldefiniert!

- 2  $e_l$  ist eine bilieare Paarung, d. H.  $e_l$  ist bilinear und nicht-ausgeartet.

- **Kompatibilität:** Sei  $l = hl'$ . Wenn  $P \in E(\mathbb{F}_q)[l]$  und  $Q \in E(\mathbb{F}_q)[l']$ , dann  $e_{l'}(hP, Q) = e_l(P, Q)^h$ .

- **Bemerkung:** Weil  $P \in E(\mathbb{F}_q)$  ist, ist  $f_P$  eine rationale Funktion mit Koeffizienten in  $\mathbb{F}_q$ .

## Definition

- Sei  $l \in \mathbb{N}$  mit  $(l, q) = 1$ . Die *Tate Paarung* der Ordnung  $l$  ist die Abbildung

$$e_l : E(\mathbb{F}_q)[l] \times : E(\mathbb{F}_{q^k})[l] \rightarrow \mathbb{F}_{q^k}^*,$$

definiert durch

$$e_l(P, Q) = f_P(\mathcal{A}_Q)^{(q^k-1)/l}.$$

- Eigenschaften**

- $e_l$  ist wohldefiniert!
  - $e_l$  ist eine bilieare Paarung, d. H.  $e_l$  ist bilinear und nicht-ausgeartet.
- Kompatibilität:** Sei  $l = hl'$ . Wenn  $P \in E(\mathbb{F}_q)[l]$  und  $Q \in E(\mathbb{F}_q)[l']$ , dann  $e_{l'}(hP, Q) = e_l(P, Q)^h$ .
  - Bemerkung:** Weil  $P \in E(\mathbb{F}_q)$  ist, ist  $f_P$  eine rationale Funktion mit Koeffizienten in  $\mathbb{F}_q$ .

## Definition

- Sei  $l \in \mathbb{N}$  mit  $(l, q) = 1$ . Die *Tate Paarung* der Ordnung  $l$  ist die Abbildung

$$e_l : E(\mathbb{F}_q)[l] \times : E(\mathbb{F}_{q^k})[l] \rightarrow \mathbb{F}_{q^k}^*,$$

definiert durch

$$e_l(P, Q) = f_P(\mathcal{A}_Q)^{(q^k-1)/l}.$$

- Eigenschaften**

- $e_l$  ist wohldefiniert!
  - $e_l$  ist eine bilieare Paarung, d. H.  $e_l$  ist bilinear und nicht-ausgeartet.
- Kompatibilität:** Sei  $l = hl'$ . Wenn  $P \in E(\mathbb{F}_q)[l]$  und  $Q \in E(\mathbb{F}_q)[l']$ , dann  $e_{l'}(hP, Q) = e_l(P, Q)^h$ .
  - Bemerkung:** Weil  $P \in E(\mathbb{F}_q)$  ist, ist  $f_P$  eine rationale Funktion mit Koeffizienten in  $\mathbb{F}_q$ .

## Definition

- Sei  $l \in \mathbb{N}$  mit  $(l, q) = 1$ . Die *Tate Paarung* der Ordnung  $l$  ist die Abbildung

$$e_l : E(\mathbb{F}_q)[l] \times : E(\mathbb{F}_{q^k})[l] \rightarrow \mathbb{F}_{q^k}^*,$$

definiert durch

$$e_l(P, Q) = f_P(\mathcal{A}_Q)^{(q^k-1)/l}.$$

- **Eigenschaften**

- 1  $e_l$  ist wohldefiniert!

- 2  $e_l$  ist eine bilieare Paarung, d. H.  $e_l$  ist bilinear und nicht-ausgeartet.

- **Kompatibilität:** Sei  $l = hl'$ . Wenn  $P \in E(\mathbb{F}_q)[l]$  und  $Q \in E(\mathbb{F}_q)[l']$ , dann  $e_{l'}(hP, Q) = e_l(P, Q)^h$ .

- **Bemerkung:** Weil  $P \in E(\mathbb{F}_q)$  ist, ist  $f_P$  eine rationale Funktion mit Koeffizienten in  $\mathbb{F}_q$ .

## Die Idee

- Seien  $U, V \in E(\mathbb{F}_{q^k})$  und  $g_{U,V}$  die rationale Funktion gegeben durch die Geradengleichung  $g_{U,V} : l_1y + l_2x + l_3 = 0$ , wobei die Gerade die Punkten  $U$  und  $V$  enthält. Wenn  $U = V$  ist, dann ist  $G_{U,U}$  gegeben durch die tangente Gerade an  $U$ . Ferner bezeichnen wir  $g_{U,-U} = g_U$ .
- **Miller Formula:** Seien  $P \in E(\mathbb{F}_{q^k})$  und  $f_c$  eine rationale Funktion so dass  $(f_c) = c(P) - ([c]P - (c-1))(\mathcal{O})$  für  $c \in \mathbb{Z}$ . Dann für alle  $a, b \in \mathbb{Z}$  gilt die folgende Gleichung

$$f_{a+b} = f_a \cdot f_b \cdot g_{[a]P, [b]P} / g_{[a+b]P}$$

## Die Idee

- Seien  $U, V \in E(\mathbb{F}_{q^k})$  und  $g_{U,V}$  die rationale Funktion gegeben durch die Geradengleichung  $g_{U,V} : l_1y + l_2x + l_3 = 0$ , wobei die Gerade die Punkten  $U$  und  $V$  enthält. Wenn  $U = V$  ist, dann ist  $G_{U,U}$  gegeben durch die tangente Gerade an  $U$ . Ferner bezeichnen wir  $g_{U,-U} = g_U$ .
- **Miller Formula:** Seien  $P \in E(\mathbb{F}_{q^k})$  und  $f_c$  eine rationale Funktion so dass  $(f_c) = c(P) - ([c]P - (c-1))(\mathcal{O})$  für  $c \in \mathbb{Z}$ . Dann für alle  $a, b \in \mathbb{Z}$  gilt die folgende Gleichung

$$f_{a+b} = f_a \cdot f_b \cdot g_{[a]P, [b]P} / g_{[a+b]P}$$

## Rekursive Formula

- Nach Miller's Formula haben wir für  $D = (Q + Q') - Q$  (beachte, dass  $D \sim (Q) - (\mathcal{O})$  ist)

1

$$f_{a+1}(D) = f_{a+1}(Q+Q')/f_{a+1}(Q') = f_a(D) \cdot \frac{g_{[a]P,P}(Q+Q')g_{[a+1]P}(Q')}{g_{[a+1]P}(Q+Q')g_{[a]P,P}(Q')}$$

2

$$f_{2a}(D) = f_{2a}(Q+Q')/f_{2a}(Q') = f_a(D)^2 \frac{g_{[a]P,[a]P}(Q+Q')g_{[2a]P}(Q')}{g_{[2a]P}(Q+Q')g_{[a]P,[a]P}(Q')}$$

## Rekursive Formula

- Nach Miller's Formula haben wir für  $D = (Q + Q') - Q$  (beachte, dass  $D \sim (Q) - (\mathcal{O})$  ist)

1

$$f_{a+1}(D) = f_{a+1}(Q+Q')/f_{a+1}(Q') = f_a(D) \cdot \frac{g_{[a]P,P}(Q+Q')g_{[a+1]P}(Q')}{g_{[a+1]P}(Q+Q')g_{[a]P,P}(Q')}$$

2

$$f_{2a}(D) = f_{2a}(Q+Q')/f_{2a}(Q') = f_a(D)^2 \frac{g_{[a]P,[a]P}(Q+Q')g_{[2a]P}(Q')}{g_{[2a]P}(Q+Q')g_{[a]P,[a]P}(Q')}$$

## Rekursive Formula

- Nach Miller's Formula haben wir für  $D = (Q + Q') - Q$  (beachte, dass  $D \sim (Q) - (\mathcal{O})$  ist)

1

$$f_{a+1}(D) = f_{a+1}(Q+Q')/f_{a+1}(Q') = f_a(D) \cdot \frac{g_{[a]P,P}(Q+Q')g_{[a+1]P}(Q')}{g_{[a+1]P}(Q+Q')g_{[a]P,P}(Q')}$$

2

$$f_{2a}(D) = f_{2a}(Q+Q')/f_{2a}(Q') = f_a(D)^2 \frac{g_{[a]P,[a]P}(Q+Q')g_{[2a]P}(Q')}{g_{[2a]P}(Q+Q')g_{[a]P,[a]P}(Q')}$$

## Miller's Algorithmus

- 1 Wähle ein zufälliger Punkt  $Q' \in E(\mathbb{F}_{q^k})$  und berechne  $S = Q + Q' \in E(\mathbb{F}_{q^k})$ .
- 2 Setze  $t = \lfloor \log_2(l) \rfloor$ , und sei  $l = (l_t, \dots, l_1)_2$  die Binärdarstellung von  $l$
- 3 For  $i = t - 1$  to 0 do
- 4 Return  $f$ .

## Miller's Algorithmus

- 1 Wähle ein zufälliger Punkt  $Q' \in E(\mathbb{F}_{q^k})$  und berechne  $S = Q + Q' \in E(\mathbb{F}_{q^k})$ .
- 2 Setze  $t = \lfloor \log_2(l) \rfloor$ , und sei  $l = (l_t, \dots, l_1)_2$  die Binärdarstellung von  $l$
- 3 For  $i = t - 1$  to 0 do
  - Setze  $V = f'(x_{S,y(S)}, y(S)) / (y_{S,y(S)} - y_{Q',y(Q')})$  und  $V = [2]V$ .
  - Wenn  $l_{i+1} = 1$  dann  $V = [2]V + [1]Q'$ .
- 4 Return  $f$ .

## Miller's Algorithmus

- 1 Wähle ein zufälliger Punkt  $Q' \in E(\mathbb{F}_{q^k})$  und berechne  $S = Q + Q' \in E(\mathbb{F}_{q^k})$ .
- 2 Setze  $t = \lfloor \log_2(l) \rfloor$ , und sei  $l = (l_t, \dots, l_1)_2$  die Binärdarstellung von  $l$
- 3 For  $i = t - 1$  to 0 do
  - Setze  $f = f^2(g_{V,V}(S)g_{[2]V}(Q')) / (g_{[2]V}(S)g_{V,V}(Q'))$  und  $V = [2]V$ .
  - Wenn  $l_i = 1$ , dann setze  $f = f(g_{V,P}(S)g_{V+P}(Q')) / (g_{V+P}(S)g_{V,P}(Q'))$  und  $V = V + P$ .
- 4 Return  $f$ .

## Miller's Algorithmus

- 1 Wähle ein zufälliger Punkt  $Q' \in E(\mathbb{F}_{q^k})$  und berechne  $S = Q + Q' \in E(\mathbb{F}_{q^k})$ .
- 2 Setze  $t = \lfloor \log_2(l) \rfloor$ , und sei  $l = (l_t, \dots, l_1)_2$  die Binärdarstellung von  $l$
- 3 For  $i = t - 1$  to 0 do
  - Setze  $f = f^2(g_{V,V}(S)g_{[2]V}(Q')) / (g_{[2]V}(S)g_{V,V}(Q'))$  und  $V = [2]V$ .
  - Wenn  $l_i = 1$ , dann setze  $f = f(g_{V,P}(S)g_{V+P}(Q')) / (g_{V+P}(S)g_{V,P}(Q'))$  und  $V = V + P$ .
- 4 Return  $f$ .

## Miller's Algorithmus

- 1 Wähle ein zufälliger Punkt  $Q' \in E(\mathbb{F}_{q^k})$  und berechne  $S = Q + Q' \in E(\mathbb{F}_{q^k})$ .
- 2 Setze  $t = \lfloor \log_2(l) \rfloor$ , und sei  $l = (l_t, \dots, l_1)_2$  die Binärdarstellung von  $l$
- 3 For  $i = t - 1$  to 0 do
  - Setze  $f = f^2(g_{V,V}(S)g_{[2]V}(Q')) / (g_{[2]V}(S)g_{V,V}(Q'))$  und  $V = [2]V$ .
  - Wenn  $l_i = 1$ , dann setze  $f = f(g_{V,P}(S)g_{V+P}(Q')) / (g_{V+P}(S)g_{V,P}(Q'))$  und  $V = V + P$ .
- 4 Return  $f$ .

## Miller's Algorithmus

- 1 Wähle ein zufälliger Punkt  $Q' \in E(\mathbb{F}_{q^k})$  und berechne  $S = Q + Q' \in E(\mathbb{F}_{q^k})$ .
- 2 Setze  $t = \lfloor \log_2(l) \rfloor$ , und sei  $l = (l_t, \dots, l_1)_2$  die Binärdarstellung von  $l$
- 3 For  $i = t - 1$  to 0 do
  - Setze  $f = f^2(g_{V,V}(S)g_{[2]V}(Q')) / (g_{[2]V}(S)g_{V,V}(Q'))$  und  $V = [2]V$ .
  - Wenn  $l_i = 1$ , dann setze  $f = f(g_{V,P}(S)g_{V+P}(Q')) / (g_{V+P}(S)g_{V,P}(Q'))$  und  $V = V + P$ .
- 4 Return  $f$ .

## Frey-Rück Angriff gegen DLP

- **Eingabe:**  $P \in E(\mathbb{F}_q)$ ,  $l$  die Ordnung von  $P$  und  $Q \in \langle P \rangle$ , d. H.  $Q = [\lambda]P$  für  $\lambda \in \mathbb{N}$ .
- **Ausgabe:** Diskreter Logarithmus  $\lambda$  von  $Q$  zur Basis  $P$ .

- 1 Konstruiere den Körper  $\mathbb{F}_{q^k}$  so dass  $r \mid (q^k - 1)$ .
- 2 Finde einen Punkt  $S \in E(\mathbb{F}_{q^k})$  so dass  $e_l(P, S) \neq 1$ .
- 3  $\zeta_1 \leftarrow e_l(P, S)$ .
- 4  $\zeta_2 \leftarrow e_l(Q, S)$ .
- 5 Finde  $\lambda$  so dass  $\zeta_1^\lambda = \zeta_2$  in  $\mathbb{F}_{q^k}^*$  z. B. mit Hilfe von Index-Calculus Algorithmus.
- 6 Return  $\lambda$ .

## Frey-Rück Angriff gegen DLP

- **Eingabe:**  $P \in E(\mathbb{F}_q)$ ,  $l$  die Ordnung von  $P$  und  $Q \in \langle P \rangle$ , d. H.  $Q = [\lambda]P$  für  $\lambda \in \mathbb{N}$ .
  - **Ausgabe:** Diskreter Logarithmus  $\lambda$  von  $Q$  zur Basis  $P$ .
- 1 Konstruiere den Körper  $\mathbb{F}_{q^k}$  so dass  $r \mid (q^k - 1)$ .
  - 2 Finde einen Punkt  $S \in E(\mathbb{F}_{q^k})$  so dass  $e_l(P, S) \neq 1$ .
  - 3  $\zeta_1 \leftarrow e_l(P, S)$ .
  - 4  $\zeta_2 \leftarrow e_l(Q, S)$ .
  - 5 Finde  $\lambda$  so dass  $\zeta_1^\lambda = \zeta_2$  in  $\mathbb{F}_{q^k}^*$  z. B. mit Hilfe von Index-Calculus Algorithmus.
  - 6 Return  $\lambda$ .

## Frey-Rück Angriff gegen DLP

- **Eingabe:**  $P \in E(\mathbb{F}_q)$ ,  $l$  die Ordnung von  $P$  und  $Q \in \langle P \rangle$ , d. H.  $Q = [\lambda]P$  für  $\lambda \in \mathbb{N}$ .
- **Ausgabe:** Diskreter Logarithmus  $\lambda$  von  $Q$  zur Basis  $P$ .

- 1 Konstruiere den Körper  $\mathbb{F}_{q^k}$  so dass  $r \mid (q^k - 1)$ .
- 2 Finde einen Punkt  $S \in E(\mathbb{F}_{q^k})$  so dass  $e_l(P, S) \neq 1$ .
- 3  $\zeta_1 \leftarrow e_l(P, S)$ .
- 4  $\zeta_2 \leftarrow e_l(Q, S)$ .
- 5 Finde  $\lambda$  so dass  $\zeta_1^\lambda = \zeta_2$  in  $\mathbb{F}_{q^k}^*$  z. B. mit Hilfe von Index-Calculus Algorithmus.
- 6 Return  $\lambda$ .

## Frey-Rück Angriff gegen DLP

- **Eingabe:**  $P \in E(\mathbb{F}_q)$ ,  $l$  die Ordnung von  $P$  und  $Q \in \langle P \rangle$ , d. H.  $Q = [\lambda]P$  für  $\lambda \in \mathbb{N}$ .
  - **Ausgabe:** Diskreter Logarithmus  $\lambda$  von  $Q$  zur Basis  $P$ .
- 1 Konstruiere den Körper  $\mathbb{F}_{q^k}$  so dass  $r \mid (q^k - 1)$ .
  - 2 Finde einen Punkt  $S \in E(\mathbb{F}_{q^k})$  so dass  $e_l(P, S) \neq 1$ .
  - 3  $\zeta_1 \leftarrow e_l(P, S)$ .
  - 4  $\zeta_2 \leftarrow e_l(Q, S)$ .
  - 5 Finde  $\lambda$  so dass  $\zeta_1^\lambda = \zeta_2$  in  $\mathbb{F}_{q^k}^*$  z. B. mit Hilfe von Index-Calculus Algorithmus.
  - 6 Return  $\lambda$ .

## Frey-Rück Angriff gegen DLP

- **Eingabe:**  $P \in E(\mathbb{F}_q)$ ,  $l$  die Ordnung von  $P$  und  $Q \in \langle P \rangle$ , d. H.  $Q = [\lambda]P$  für  $\lambda \in \mathbb{N}$ .
  - **Ausgabe:** Diskreter Logarithmus  $\lambda$  von  $Q$  zur Basis  $P$ .
- 1 Konstruiere den Körper  $\mathbb{F}_{q^k}$  so dass  $r \mid (q^k - 1)$ .
  - 2 Finde einen Punkt  $S \in E(\mathbb{F}_{q^k})$  so dass  $e_l(P, S) \neq 1$ .
  - 3  $\zeta_1 \leftarrow e_l(P, S)$ .
  - 4  $\zeta_2 \leftarrow e_l(Q, S)$ .
  - 5 Finde  $\lambda$  so dass  $\zeta_1^\lambda = \zeta_2$  in  $\mathbb{F}_{q^k}^*$  z. B. mit Hilfe von Index-Calculus Algorithmus.
  - 6 Return  $\lambda$ .

## Frey-Rück Angriff gegen DLP

- **Eingabe:**  $P \in E(\mathbb{F}_q)$ ,  $l$  die Ordnung von  $P$  und  $Q \in \langle P \rangle$ , d. H.  $Q = [\lambda]P$  für  $\lambda \in \mathbb{N}$ .
  - **Ausgabe:** Diskreter Logarithmus  $\lambda$  von  $Q$  zur Basis  $P$ .
- 1 Konstruiere den Körper  $\mathbb{F}_{q^k}$  so dass  $r \mid (q^k - 1)$ .
  - 2 Finde einen Punkt  $S \in E(\mathbb{F}_{q^k})$  so dass  $e_l(P, S) \neq 1$ .
  - 3  $\zeta_1 \leftarrow e_l(P, S)$ .
  - 4  $\zeta_2 \leftarrow e_l(Q, S)$ .
  - 5 Finde  $\lambda$  so dass  $\zeta_1^\lambda = \zeta_2$  in  $\mathbb{F}_{q^k}^*$  z. B. mit Hilfe von Index-Calculus Algorithmus.
  - 6 Return  $\lambda$ .

# Outline

- 1 Grundlagen
  - Bilineare Paarungen
  - Elliptische Kurven
  - Divisorentheorie
- 2 Tate Paarung
  - Definition
  - Berechnung
  - Anwendung
- 3 Einbettungsgrad**
  - Kurven mit kleinem Einbettungsgrad
  - Supersingulare Kurven
  - MNT Kurven
- 4 Distortionsabbildungen
  - Definition
  - Modifizierte Tate Paarung

## Problem

- Die Tate Paarung ist eine bilineare Abbildung, die die Punkte auf  $E(\mathbb{F}_q)$  zur multiplikativen Gruppe  $\mathbb{F}_{q^k}^*$  abbildet. Je grösser der Einbettungsgrad  $k$  ist, desto aufwendiger ist die Paarung zu berechnen. Wir brauchen *klein*  $k$ .
- Andererseits hängt die Sicherheit der kryptographischen Anwendung nach Frey-Rück Angriff die Schwierigkeit des DLP in  $\mathbb{F}_{q^k}^*$  ab. Dafür brauchen wir *gross*  $k$ .
- Folgerung:**  $k$  muss 'klein' genug sein um die Paarung zu berechnen und 'gross' genug sein damit das DLP nicht einfach zu lösen ist. Wir brauchen  $k < (\log q)^2$  um die Paarung berechnen zu können.

## Problem

- Die Tate Paarung ist eine bilineare Abbildung, die die Punkte auf  $E(\mathbb{F}_q)$  zur multiplikativen Gruppe  $\mathbb{F}_{q^k}^*$  abbildet. Je grösser der Einbettungsgrad  $k$  ist, desto aufwendiger ist die Paarung zu berechnen. Wir brauchen *klein*  $k$ .
- Andererseits hängt die Sicherheit der kryptographischen Anwendung nach Frey-Rück Angriff die Schwierigkeit des DLP in  $\mathbb{F}_{q^k}^*$  ab. Dafür brauchen wir *gross*  $k$ .
- **Folgerung:**  $k$  muss 'klein' genug sein um die Paarung zu berechnen und 'gross' genug sein damit das DLP nicht einfach zu lösen ist. Wir brauchen  $k < (\log q)^2$  um die Paarung berechnen zu können.

## Problem

- Die Tate Paarung ist eine bilineare Abbildung, die die Punkte auf  $E(\mathbb{F}_q)$  zur multiplikativen Gruppe  $\mathbb{F}_{q^k}^*$  abbildet. Je grösser der Einbettungsgrad  $k$  ist, desto aufwendiger ist die Paarung zu berechnen. Wir brauchen *klein*  $k$ .
- Andererseits hängt die Sicherheit der kryptographischen Anwendung nach Frey-Rück Angriff die Schwierigkeit des DLP in  $\mathbb{F}_{q^k}^*$  ab. Dafür brauchen wir *gross*  $k$ .
- **Folgerung:**  $k$  muss 'klein' genug sein um die Paarung zu berechnen und 'gross' genug sein damit das DLP nicht einfach zu lösen ist. Wir brauchen  $k < (\log q)^2$  um die Paarung berechnen zu können.

## Definition und Eigenschaften

- Eine elliptische Kurve heisst *supersingular* über  $\mathbb{F}_q$ , wenn eine der folgenden Bedingungen erfüllt.
  - ①  $|E(\mathbb{F}_q)| \equiv 1 \pmod{p}$ .
  - ②  $E$  hat keinen Punkt der Ordnung  $p$  über  $\overline{\mathbb{F}_q}$ .
  - ③  $\text{End}(E)$  über  $\overline{\mathbb{F}_q}$  ist nicht kommutativ.
- **Satz** Sei  $E$  eine supersingulare elliptische Kurve. Dann  $k \leq 6$ .
- Eine supersingulare elliptische Kurve erreicht den maximalen Grad wenn  $\text{char}\mathbb{F}_q = 3$  ist.
- Supersingulare Kurven sind die Kurven mit kleinem Einbettungsgrad. Diese Kurven besitzen interessante Eigenschaften, die sowohl Vorteile als auch Nachteile für kryptographische Anwendungen haben.

## Definition und Eigenschaften

- Eine elliptische Kurve heisst *supersingular* über  $\mathbb{F}_q$ , wenn eine der folgenden Bedingungen erfüllt.
  - ①  $|E(\mathbb{F}_q)| \equiv 1 \pmod{p}$ .
  - ②  $E$  hat keinen Punkt der Ordnung  $p$  über  $\overline{\mathbb{F}_q}$ .
  - ③  $\text{End}(E)$  über  $\overline{\mathbb{F}_q}$  ist nicht kommutativ.
- **Satz** Sei  $E$  eine supersingulare elliptische Kurve. Dann  $k \leq 6$ .
- Eine supersingulare elliptische Kurve erreicht den maximalen Grad wenn  $\text{char}\mathbb{F}_q = 3$  ist.
- Supersingulare Kurven sind die Kurven mit kleinem Einbettungsgrad. Diese Kurven besitzen interessante Eigenschaften, die sowohl Vorteile als auch Nachteile für kryptographische Anwendungen haben.

## Definition und Eigenschaften

- Eine elliptische Kurve heisst *supersingular* über  $\mathbb{F}_q$ , wenn eine der folgenden Bedingungen erfüllt.
  - ①  $|E(\mathbb{F}_q)| \equiv 1 \pmod{p}$ .
  - ②  $E$  hat keinen Punkt der Ordnung  $p$  über  $\overline{\mathbb{F}_q}$ .
  - ③  $End(E)$  über  $\overline{\mathbb{F}_q}$  ist nicht kommutativ.
- **Satz** Sei  $E$  eine supersingulare elliptische Kurve. Dann  $k \leq 6$ .
- Eine supersingulare elliptische Kurve erreicht den maximalen Grad wenn  $char\mathbb{F}_q = 3$  ist.
- Supersingulare Kurven sind die Kurven mit kleinem Einbettungsgrad. Diese Kurven besitzen interessante Eigenschaften, die sowohl Vorteile als auch Nachteile für kryptographische Anwendungen haben.

## Definition und Eigenschaften

- Eine elliptische Kurve heisst *supersingular* über  $\mathbb{F}_q$ , wenn eine der folgenden Bedingungen erfüllt.
  - ❶  $|E(\mathbb{F}_q)| \equiv 1 \pmod{p}$ .
  - ❷  $E$  hat keinen Punkt der Ordnung  $p$  über  $\overline{\mathbb{F}_q}$ .
  - ❸  $End(E)$  über  $\overline{\mathbb{F}_q}$  ist nicht kommutativ.
- **Satz** Sei  $E$  eine supersingulare elliptische Kurve. Dann  $k \leq 6$ .
- Eine supersingulare elliptische Kurve erreicht den maximalen Grad wenn  $char\mathbb{F}_q = 3$  ist.
- Supersingulare Kurven sind die Kurven mit kleinem Einbettungsgrad. Diese Kurven besitzen interessante Eigenschaften, die sowohl Vorteile als auch Nachteile für kryptographische Anwendungen haben.

## Definition und Eigenschaften

- Eine elliptische Kurve heisst *supersingular* über  $\mathbb{F}_q$ , wenn eine der folgenden Bedingungen erfüllt.
  - ❶  $|E(\mathbb{F}_q)| \equiv 1 \pmod{p}$ .
  - ❷  $E$  hat keinen Punkt der Ordnung  $p$  über  $\overline{\mathbb{F}_q}$ .
  - ❸  $End(E)$  über  $\overline{\mathbb{F}_q}$  ist nicht kommutativ.
- **Satz** Sei  $E$  eine supersingulare elliptische Kurve. Dann  $k \leq 6$ .
- Eine supersingulare elliptische Kurve erreicht den maximalen Grad wenn  $char\mathbb{F}_q = 3$  ist.
- Supersingulare Kurven sind die Kurven mit kleinem Einbettungsgrad. Diese Kurven besitzen interessante Eigenschaften, die sowohl Vorteile als auch Nachteile für kryptographische Anwendungen haben.

## Definition und Eigenschaften

- Eine elliptische Kurve heisst *supersingular* über  $\mathbb{F}_q$ , wenn eine der folgenden Bedingungen erfüllt.
  - ❶  $|E(\mathbb{F}_q)| \equiv 1 \pmod{p}$ .
  - ❷  $E$  hat keinen Punkt der Ordnung  $p$  über  $\overline{\mathbb{F}_q}$ .
  - ❸  $End(E)$  über  $\overline{\mathbb{F}_q}$  ist nicht kommutativ.
- **Satz** Sei  $E$  eine supersingulare elliptische Kurve. Dann  $k \leq 6$ .
- Eine supersingulare elliptische Kurve erreicht den maximalen Grad wenn  $char\mathbb{F}_q = 3$  ist.
- Supersingulare Kurven sind die Kurven mit kleinem Einbettungsgrad. Diese Kurven besitzen interessante Eigenschaften, die sowohl Vorteile als auch Nachteile für kryptographische Anwendungen haben.

## Definition und Eigenschaften

- Eine elliptische Kurve heisst *supersingular* über  $\mathbb{F}_q$ , wenn eine der folgenden Bedingungen erfüllt.
  - ①  $|E(\mathbb{F}_q)| \equiv 1 \pmod{p}$ .
  - ②  $E$  hat keinen Punkt der Ordnung  $p$  über  $\overline{\mathbb{F}_q}$ .
  - ③  $End(E)$  über  $\overline{\mathbb{F}_q}$  ist nicht kommutativ.
- **Satz** Sei  $E$  eine supersingulare elliptische Kurve. Dann  $k \leq 6$ .
- Eine supersingulare elliptische Kurve erreicht den maximalen Grad wenn  $char\mathbb{F}_q = 3$  ist.
- Supersingulare Kurven sind die Kurven mit kleinem Einbettungsgrad. Diese Kurven besitzen interessante Eigenschaften, die sowohl Vorteile als auch Nachteile für kryptographische Anwendungen haben.

## Die Idee

- Bis 2001 gab es keine bekannte nicht-supersingulare Kurve, die kleinen Einbettungsgrad besitzen. Aber Miyaji, Nakabayashi und Takano haben eine Methode gefunden um diese Kurve zu konstruieren.
- Sei  $n = |E(\mathbb{F}_q)| = q + 1 - t$ . Fixiere ein  $k$  mit der Eigenschaft

$$n \mid q^k - 1, \text{ und } m \nmid q^t - 1 \text{ für } 0 < t < k.$$

- **Satz** Sei  $E/\mathbb{F}_q$  eine elliptische Kurve mit dem Spur  $t$ .

## Die Idee

- Bis 2001 gab es keine bekannte nicht-supersingulare Kurve, die kleinen Einbettungsgrad besitzen. Aber Miyaji, Nakabayashi und Takano haben eine Methode gefunden um diese Kurve zu konstruieren.
- Sei  $n = |E(\mathbb{F}_q)| = q + 1 - t$ . Fixiere ein  $k$  mit der Eigenschaft

$$n \mid q^k - 1, \text{ und } m \nmid q^t - 1 \text{ f\"ur } 0 < t < k.$$

- **Satz** Sei  $E/\mathbb{F}_q$  eine elliptische Kurve mit dem Spur  $t$ . Wenn  $(q, t)$  mit  $q = 12f^2 - 1$  und  $t = -1 \pm 6f$ ,  $f \in \mathbb{Z}$  repräsentiert werden kann, dann ist der Einbettungsgrad  $k = 3$ .

## Die Idee

- Bis 2001 gab es keine bekannte nicht-supersingulare Kurve, die kleinen Einbettungsgrad besitzen. Aber Miyaji, Nakabayashi und Takano haben eine Methode gefunden um diese Kurve zu konstruieren.
- Sei  $n = |E(\mathbb{F}_q)| = q + 1 - t$ . Fixiere ein  $k$  mit der Eigenschaft

$$n \mid q^k - 1, \text{ und } m \nmid q^t - 1 \text{ für } 0 < t < k.$$

- **Satz** Sei  $E/\mathbb{F}_q$  eine elliptische Kurve mit dem Spur  $t$ .
  - Wenn  $(q, t)$  mit  $q = 12l^2 - 1$  und  $t = -1 \pm 6l, l \in \mathbb{Z}$  repräsentiert werden kann, dann ist der Einbettungsgrad  $k = 3$ .
  - Wenn  $(q, t)$  mit  $q = l^2 + l + 1$  und  $t = -l, l + 1, l \in \mathbb{Z}$  repräsentiert werden kann, dann ist der Einbettungsgrad  $k = 4$ .
  - Wenn  $(q, t)$  mit  $q = 4l^2 + 1$  und  $t = 1 \pm 2l, l \in \mathbb{Z}$  repräsentiert werden kann, dann ist der Einbettungsgrad  $k = 6$ .

## Die Idee

- Bis 2001 gab es keine bekannte nicht-supersingulare Kurve, die kleinen Einbettungsgrad besitzen. Aber Miyaji, Nakabayashi und Takano haben eine Methode gefunden um diese Kurve zu konstruieren.
- Sei  $n = |E(\mathbb{F}_q)| = q + 1 - t$ . Fixiere ein  $k$  mit der Eigenschaft

$$n \mid q^k - 1, \text{ und } m \nmid q^t - 1 \text{ für } 0 < t < k.$$

- **Satz** Sei  $E/\mathbb{F}_q$  eine elliptische Kurve mit dem Spur  $t$ .
  - Wenn  $(q, t)$  mit  $q = 12l^2 - 1$  und  $t = -1 \pm 6l, l \in \mathbb{Z}$  repräsentiert werden kann, dann ist der Einbettungsgrad  $k = 3$ .
  - Wenn  $(q, t)$  mit  $q = l^2 + l + 1$  und  $t = -l, l + 1, l \in \mathbb{Z}$  repräsentiert werden kann, dann ist der Einbettungsgrad  $k = 4$ .
  - Wenn  $(q, t)$  mit  $q = 4l^2 + 1$  und  $t = 1 \pm 2l, l \in \mathbb{Z}$  repräsentiert werden kann, dann ist der Einbettungsgrad  $k = 6$ .

## Die Idee

- Bis 2001 gab es keine bekannte nicht-supersingulare Kurve, die kleinen Einbettungsgrad besitzen. Aber Miyaji, Nakabayashi und Takano haben eine Methode gefunden um diese Kurve zu konstruieren.
- Sei  $n = |E(\mathbb{F}_q)| = q + 1 - t$ . Fixiere ein  $k$  mit der Eigenschaft

$$n \mid q^k - 1, \text{ und } m \nmid q^t - 1 \text{ für } 0 < t < k.$$

- **Satz** Sei  $E/\mathbb{F}_q$  eine elliptische Kurve mit dem Spur  $t$ .
  - Wenn  $(q, t)$  mit  $q = 12l^2 - 1$  und  $t = -1 \pm 6l, l \in \mathbb{Z}$  repräsentiert werden kann, dann ist der Einbettungsgrad  $k = 3$ .
  - Wenn  $(q, t)$  mit  $q = l^2 + l + 1$  und  $t = -l, l + 1, l \in \mathbb{Z}$  repräsentiert werden kann, dann ist der Einbettungsgrad  $k = 4$ .
  - Wenn  $(q, t)$  mit  $q = 4l^2 + 1$  und  $t = 1 \pm 2l, l \in \mathbb{Z}$  repräsentiert werden kann, dann ist der Einbettungsgrad  $k = 6$ .

## Die Idee

- Bis 2001 gab es keine bekannte nicht-supersingulare Kurve, die kleinen Einbettungsgrad besitzen. Aber Miyaji, Nakabayashi und Takano haben eine Methode gefunden um diese Kurve zu konstruieren.
- Sei  $n = |E(\mathbb{F}_q)| = q + 1 - t$ . Fixiere ein  $k$  mit der Eigenschaft

$$n \mid q^k - 1, \text{ und } m \nmid q^t - 1 \text{ für } 0 < t < k.$$

- **Satz** Sei  $E/\mathbb{F}_q$  eine elliptische Kurve mit dem Spur  $t$ .
  - Wenn  $(q, t)$  mit  $q = 12l^2 - 1$  und  $t = -1 \pm 6l, l \in \mathbb{Z}$  repräsentiert werden kann, dann ist der Einbettungsgrad  $k = 3$ .
  - Wenn  $(q, t)$  mit  $q = l^2 + l + 1$  und  $t = -l, l + 1, l \in \mathbb{Z}$  repräsentiert werden kann, dann ist der Einbettungsgrad  $k = 4$ .
  - Wenn  $(q, t)$  mit  $q = 4l^2 + 1$  und  $t = 1 \pm 2l, l \in \mathbb{Z}$  repräsentiert werden kann, dann ist der Einbettungsgrad  $k = 6$ .

## Konstruktion

- Um die Kurven, die die Eigenschaften in dem Satz erfüllen, zu konstruieren, benutzt man die sogenannte CM (komplexe Multiplikation) Methode für gegebene  $q$  und  $t$ .
- Aber man muss die CM-Gleichung lösen um die Kurven konstruieren zu können. Für  $k = 3, 4$  oder  $6$ , lässt sich die CM-Gleichung eine Pellische Gleichung reduzieren, die nach algebraischer Zahlentheorie lösbar ist.
- Barreto und Dupont haben eine andere methode für die Kurven mit Einbettungsgrad  $k > 6$ . Aber eine solche Reduzierung für CM-Gleichung in diesem Fall nicht möglich. Sie haben versucht für gegene partille Lösung eine CM-Gleichung zu finden und damit die Kurve konstruieren. Sie haben Kurvenbeispiele mit  $k = 7$  und  $12$  gegeben.

## Konstruktion

- Um die Kurven, die die Eigenschaften in dem Satz erfüllen, zu konstruieren, benutzt man die sogenannte CM (komplexe Multiplikation) Methode für gegebene  $q$  und  $t$ .
- Aber man muss die CM-Gleichung lösen um die Kurven konstruieren zu können. Für  $k = 3, 4$  oder  $6$ , lässt sich die CM-Gleichung eine Pellische Gleichung reduzieren, die nach algebraischer Zahlentheorie lösbar ist.
- Barreto und Dupont haben eine andere methode für die Kurven mit Einbettungsgrad  $k > 6$ . Aber eine solche Reduzierung für CM-Gleichung in diesem Fall nicht möglich. Sie haben versucht für gegene partille Lösung eine CM-Gleichung zu finden und damit die Kurve konstruieren. Sie haben Kurvenbeispiele mit  $k = 7$  und  $12$  gegeben.

## Konstruktion

- Um die Kurven, die die Eigenschaften in dem Satz erfüllen, zu konstruieren, benutzt man die sogenannte CM (komplexe Multiplikation) Methode für gegebene  $q$  und  $t$ .
- Aber man muss die CM-Gleichung lösen um die Kurven konstruieren zu können. Für  $k = 3, 4$  oder  $6$ , lässt sich die CM-Gleichung eine Pellische Gleichung reduzieren, die nach algebraischer Zahlentheorie lösbar ist.
- Barreto und Dupont haben eine andere methode für die Kurven mit Einbettungsgrad  $k > 6$ . Aber eine solche Reduzierung für CM-Gleichung in diesem Fall nicht möglich. Sie haben versucht für gegene partille Lösung eine CM-Gleichung zu finden und damit die Kurve konstruieren. Sie haben Kurvenbeispiele mit  $k = 7$  und  $12$  gegeben.

# Outline

- 1 Grundlagen
  - Bilineare Paarungen
  - Elliptische Kurven
  - Divisorentheorie
- 2 Tate Paarung
  - Definition
  - Berechnung
  - Anwendung
- 3 Einbettungsgrad
  - Kurven mit kleinem Einbettungsgrad
  - Supersingulare Kurven
  - MNT Kurven
- 4 **Distortionsabbildungen**
  - Definition
  - Modifizierte Tate Paarung

# Paarungen in der Kryptographie

**Vielen Dank**

<http://www.math.tu-berlin.de/~uzunkol>