Paarungen und Identitätsbasierte Kryptographie

Peter Schwabe

Lehrstuhl für Theoretische Informationstechnik

RWTHAACHEN

10.05.2007

AG Kommunikationstheorie

Motivation

RWTH AACHEN UNIVERSITY TIplain theme

Ziel: Identitätsbasierte Kryptographie auf mobilen Endgeräten

Motivation

Ziel: Identitätsbasierte Kryptographie auf mobilen Endgeräten

- Public Key Verfahren
- Öffentlicher Schlüssel ist die Identität des Benutzers (E-Mail-Adresse, Rufnummer,...)

Motivation

Ziel: Identitätsbasierte Kryptographie auf mobilen Endgeräten

- Public Key Verfahren
- Öffentlicher Schlüssel ist die Identität des Benutzers (E-Mail-Adresse, Rufnummer,...)
- Benötigt Trusted Authority zur Generierung und Verteilung privater Schlüssel

Motivation

RWTH AACHEN UNIVERSITY TIplain theme

Ziel: Identitätsbasierte Kryptographie auf mobilen Endgeräten

- Public Key Verfahren
- Öffentlicher Schlüssel ist die Identität des Benutzers (E-Mail-Adresse, Rufnummer,...)
- Benötigt Trusted Authority zur Generierung und Verteilung privater Schlüssel
- Effiziente Implementierung (in Hard- und Software)

Motivation

Ziel: Identitätsbasierte Kryptographie auf mobilen Endgeräten

- Public Key Verfahren
- Öffentlicher Schlüssel ist die Identität des Benutzers (E-Mail-Adresse, Rufnummer,...)
- Benötigt Trusted Authority zur Generierung und Verteilung privater Schlüssel

- Effiziente Implementierung (in Hard- und Software)
- Voraussetzung: Genaue Kenntnis der Algorithmen und mathematischen Strukturen

Überblick

Definition

Seien G_1, G_2 abelsche Gruppen mit Exponent r und sei G_3 eine zyklische Gruppe der Ordnung r. Eine Abbildung

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

heißt Paarung, wenn sie bilinear und nicht-degeneriert ist.

Paarungen

Definition

Seien G_1, G_2 abelsche Gruppen mit Exponent r und sei G_3 eine zyklische Gruppe der Ordnung r. Eine Abbildung

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

heißt Paarung, wenn sie bilinear und nicht-degeneriert ist.

- G_1 und G_2 werden üblicherweise additiv, G_3 multiplikativ geschrieben.

Identitätsbasierte Kryptographie

`BasicIdent` (Boneh, Franklin, 2001)

TIplain theme

- Die TA legt die folgenden Systemparameter fest:
  - Gruppen $G_1 = \langle P \rangle$, $G_2 = \langle Q \rangle$ und G_3
  - Eine Paarung $e : G_1 \times G_2 \to G_3$
  - $P_{pub} = [s]P$, hierbei ist $s \in Z_r^*$ der geheime Master-Schlüssel
  - Kryptographische Hashfunktionen $H_1 : \{0,1\}^* \to G_2^*$ und $H_2 : G_3 \to \{0,1\}^m$
    m bezeichne die Länge von Klartext-Nachrichten

Identitätsbasierte Kryptographie

BasicIdent (Boneh, Franklin, 2001)

- Die TA legt die folgenden Systemparameter fest:
  - Gruppen $G_1 = \langle P \rangle$, $G_2 = \langle Q \rangle$ und G_3
  - Eine Paarung $e : G_1 \times G_2 \to G_3$
  - $P_{pub} = [s]P$, hierbei ist $s \in Z_r^*$ der geheime Master-Schlüssel
  - Kryptographische Hashfunktionen $H_1 : \{0,1\}^* \to G_2^*$ und $H_2 : G_3 \to \{0,1\}^m$
    m bezeichne die Länge von Klartext-Nachrichten
- Jeder Teilnehmer A erhält von der TA seinen privaten Schlüssel $S_A = [s]Q_A = [s]H_1(ID_A)$.

TIplain theme

Identitätsbasierte Kryptographie

`BasicIdent` (Boneh, Franklin, 2001)

- Die TA legt die folgenden Systemparameter fest:
  - Gruppen $G_1 = \langle P \rangle$, $G_2 = \langle Q \rangle$ und G_3
  - Eine Paarung $e : G_1 \times G_2 \to G_3$
  - $P_{pub} = [s]P$, hierbei ist $s \in Z_r^*$ der geheime Master-Schlüssel
  - Kryptographische Hashfunktionen $H_1 : \{0,1\}^* \to G_2^*$ und $H_2 : G_3 \to \{0,1\}^m$
    m bezeichne die Länge von Klartext-Nachrichten
- Jeder Teilnehmer A erhält von der TA seinen privaten Schlüssel $S_A = [s]Q_A = [s]H_1(ID_A)$.
- Verschlüsselung einer Nachricht M: Wähle zufälliges $t \in Z_r^*$

$$C = (U, V) = ([t]P, M \oplus H_2(e(P_{pub}, Q_A)^t))$$

Identitätsbasierte Kryptographie

`BasicIdent` (Boneh, Franklin, 2001)

- Die TA legt die folgenden Systemparameter fest:
  - Gruppen $G_1 = \langle P \rangle$, $G_2 = \langle Q \rangle$ und G_3
  - Eine Paarung $e : G_1 \times G_2 \to G_3$
  - $P_{pub} = [s]P$, hierbei ist $s \in Z_r^*$ der geheime Master-Schlüssel
  - Kryptographische Hashfunktionen $H_1 : \{0,1\}^* \to G_2^*$ und $H_2 : G_3 \to \{0,1\}^m$
    m bezeichne die Länge von Klartext-Nachrichten
- Jeder Teilnehmer A erhält von der TA seinen privaten Schlüssel $S_A = [s]Q_A = [s]H_1(ID_A)$.
- Verschlüsselung einer Nachricht M: Wähle zufälliges $t \in Z_r^*$

$$C = (U, V) = ([t]P, M \oplus H_2(e(P_{pub}, Q_A)^t))$$

- Entschlüsselung:

$$M = V \oplus H_2(e(U, S_A))$$

Die Tate Paarung

TIplain theme

Die Tate-Paarung ist eine Abbildung der Form

$$\begin{aligned} \langle \cdot, \cdot \rangle_r : G_1 \times G_2 &\to G_3, \\ (P, Q) &\mapsto \langle P, Q \rangle_r. \end{aligned}$$

Die Tate Paarung

TIplain theme

Die Tate-Paarung ist eine Abbildung der Form

$$\begin{aligned} \langle \cdot, \cdot \rangle_r : {\color{red} G_1} \times G_2 &\to G_3, \\ (P, Q) &\mapsto \langle P, Q \rangle_r. \end{aligned}$$

r-Torsionspunkte

- Sei E elliptische Kurve über $\mathbb{F}_q$ definiert durch eine Gleichung der Form

$$E : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

r-Torsionspunkte

- Sei E elliptische Kurve über $\mathbb{F}_q$ definiert durch eine Gleichung der Form

$$E : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

- Sei $r \in \mathbb{N}$ prim, mit $r \mid \#E(\mathbb{F}_q)$ und $r^2 \nmid \#E(\mathbb{F}_q)$

r-Torsionspunkte

- Sei E elliptische Kurve über $\mathbb{F}_q$ definiert durch eine Gleichung der Form
$$E : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$
- Sei $r \in \mathbb{N}$ prim, mit $r \mid \#E(\mathbb{F}_q)$ und $r^2 \nmid \#E(\mathbb{F}_q)$
- Sei weiter $r \neq \mathrm{char}(\mathbb{F}_q)$.

r-Torsionspunkte

- Sei E elliptische Kurve über $\mathbb{F}_q$ definiert durch eine Gleichung der Form

$$E : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

- Sei $r \in \mathbb{N}$ prim, mit $r \mid \#E(\mathbb{F}_q)$ und $r^2 \nmid \#E(\mathbb{F}_q)$
- Sei weiter $r \neq \mathrm{char}(\mathbb{F}_q)$.
- Einbettungsgrad k: Kleinstes $k \in \mathbb{N}$ mit $r \mid q^k - 1$

r-Torsionspunkte

- Sei E elliptische Kurve über $\mathbb{F}_q$ definiert durch eine Gleichung der Form

$$E : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

- Sei $r \in \mathbb{N}$ prim, mit $r \mid \#E(\mathbb{F}_q)$ und $r^2 \nmid \#E(\mathbb{F}_q)$
- Sei weiter $r \neq \mathrm{char}(\mathbb{F}_q)$.
- Einbettungsgrad k: Kleinstes $k \in \mathbb{N}$ mit $r \mid q^k - 1$
- Die Menge $\{P \in E \mid [r]P = \mathcal{O}\}$ bildet die Gruppe der r-Torsionspunkte, Bezeichnung: $E[r]$.

r-Torsionspunkte

- Sei E elliptische Kurve über $\mathbb{F}_q$ definiert durch eine Gleichung der Form

$$E : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

- Sei $r \in \mathbb{N}$ prim, mit $r \mid \#E(\mathbb{F}_q)$ und $r^2 \nmid \#E(\mathbb{F}_q)$
- Sei weiter $r \neq \mathrm{char}(\mathbb{F}_q)$.
- Einbettungsgrad k: Kleinstes $k \in \mathbb{N}$ mit $r \mid q^k - 1$
- Die Menge $\{P \in E \mid [r]P = \mathcal{O}\}$ bildet die Gruppe der r-Torsionspunkte, Bezeichnung: $E[r]$.
- Es ist $E[r] \subset E(\mathbb{F}_{q^k})$.

r-Torsionspunkte

- Sei E elliptische Kurve über $\mathbb{F}_q$ definiert durch eine Gleichung der Form
$$E : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$
- Sei $r \in \mathbb{N}$ prim, mit $r \mid \#E(\mathbb{F}_q)$ und $r^2 \nmid \#E(\mathbb{F}_q)$
- Sei weiter $r \neq \mathrm{char}(\mathbb{F}_q)$.
- Einbettungsgrad k: Kleinstes $k \in \mathbb{N}$ mit $r \mid q^k - 1$
- Die Menge $\{P \in E \mid [r]P = \mathcal{O}\}$ bildet die Gruppe der r-Torsionspunkte, Bezeichnung: $E[r]$.
- Es ist $E[r] \subset E(\mathbb{F}_{q^k})$.
- Es gilt $E[r] \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$.

Die Tate Paarung

Die Tate-Paarung ist eine Abbildung der Form

$$\begin{aligned} \langle \cdot, \cdot \rangle_r : E[r] \times G_2 &\to G_3, \\ (P, Q) &\mapsto \langle P, Q \rangle_r. \end{aligned}$$

Die Tate Paarung

Die Tate-Paarung ist eine Abbildung der Form

$$\begin{aligned}\langle\cdot,\cdot\rangle_r : E[r] \times G_2 &\to G_3,\\ (P,Q) &\mapsto \langle P,Q\rangle_r.\end{aligned}$$

Die Gruppe $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$

TIplain theme

- Betrachte weiter elliptische Kurve E über $\mathbb{F}_q$, r und k wie oben

Die Gruppe $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$

RWTH AACHEN UNIVERSITY TIplain theme

- Betrachte weiter elliptische Kurve E über $\mathbb{F}_q$, r und k wie oben
- $rE(\mathbb{F}_{q^k})$ ist Untergruppe von $E(\mathbb{F}_{q^k})$

Die Gruppe $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$

- Betrachte weiter elliptische Kurve E über $\mathbb{F}_q$, r und k wie oben
- $rE(\mathbb{F}_{q^k})$ ist Untergruppe von $E(\mathbb{F}_{q^k})$
- Die Quotientengruppe $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ hat Exponent r.

Die Tate Paarung

Die Tate-Paarung ist eine Abbildung der Form

$$\begin{aligned} \langle \cdot, \cdot \rangle_r : E[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) &\to G_3, \\ (P, Q) &\mapsto \langle P, Q \rangle_r. \end{aligned}$$

Darstellung der Elemente aus $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$

- Betrachte E und r mit $r^2 \parallel E(\mathbb{F}_{q^k})$

Darstellung der Elemente aus $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$

- Betrachte E und r mit $r^2 \parallel E(\mathbb{F}_{q^k})$
- Dann gilt:

$$E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \cong E[r] \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}.$$

Darstellung der Elemente aus $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$

- Betrachte E und r mit $r^2 \parallel E(\mathbb{F}_{q^k})$
- Dann gilt:

$$E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \cong E[r] \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}.$$

- Verwende in diesem Fall die Elemente aus $E[r]$ als Repräsentanten.

Die Tate Paarung

TIplain theme

Wenn $r^2 \parallel E(\mathbb{F}_{q^k})$ *betrachte* die Tate-Paarung als Abbildung der Form

$$\begin{aligned} \langle \cdot, \cdot \rangle_r : E[r] \times E[r] &\to G_3, \\ (P, Q) &\mapsto \langle P, Q \rangle_r. \end{aligned}$$

Die Tate Paarung

RWTH AACHEN UNIVERSITY TIplain theme

Wenn $r^2 \parallel E(\mathbb{F}_{q^k})$ *betrachte* die Tate-Paarung als Abbildung der Form

$$\begin{aligned} \langle \cdot, \cdot \rangle_r : E[r] \times E[r] &\to G_3, \\ (P, Q) &\mapsto \langle P, Q \rangle_r. \end{aligned}$$

Die Tate Paarung

Wenn $r^2 \parallel E(\mathbb{F}_{q^k})$ *betrachte* die Tate-Paarung als Abbildung der Form

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

Der Funktionenkörper von E

TIplain theme

- Der Koordinatenring von E ist der Quotientenring

$$\overline{\mathbb{F}_q}[E] = \overline{\mathbb{F}_q}[x,y]/_{(y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6)\overline{\mathbb{F}_q}[x,y]}$$

- Die Elemente aus $\overline{\mathbb{F}_q}[E]$ heißen Polynomfunktionen
- Der Quotientenkörper von $\overline{\mathbb{F}_q}[E]$ heißt Funktionenkörper von E, Bezeichnung: $\overline{\mathbb{F}_q}(E)$

Divisoren

TIplain theme

- Ein Divisor D ist eine formale Summe der Form

$$D = \sum_{P \in E} n_P P$$

mit $n_P \in \mathbb{Z}$ und $n_P = 0$ für alle, bis auf endlich viele $P \in E$.

Divisoren

RWTH AACHEN UNIVERSITY TIplain theme

- Ein Divisor D ist eine formale Summe der Form

$$D = \sum_{P \in E} n_P P$$

  mit $n_P \in \mathbb{Z}$ und $n_P = 0$ für alle, bis auf endlich viele $P \in E$.
- Die Menge der Divisoren einer Kurve E bildet die Gruppe $\mathrm{Div}(E)$.

Divisoren

RWTH AACHEN UNIVERSITY TIplain theme

- Ein Divisor D ist eine formale Summe der Form

$$D = \sum_{P \in E} n_P P$$

  mit $n_P \in \mathbb{Z}$ und $n_P = 0$ für alle, bis auf endlich viele $P \in E$.
- Die Menge der Divisoren einer Kurve E bildet die Gruppe $\mathrm{Div}(E)$.
- Der Grad eines Divisors D ist

$$\deg(D) = \sum_{P \in E} n_P.$$

Divisoren

- Ein Divisor D ist eine formale Summe der Form
$$D = \sum_{P \in E} n_P P$$
mit $n_P \in \mathbb{Z}$ und $n_P = 0$ für alle, bis auf endlich viele $P \in E$.
- Die Menge der Divisoren einer Kurve E bildet die Gruppe $\mathrm{Div}(E)$.
- Der Grad eines Divisors D ist
$$\deg(D) = \sum_{P \in E} n_P.$$
- Der Träger eines Divisors D ist
$$\mathrm{supp}(D) = \{P \in E \mid n_P \neq 0\}.$$

Hauptdivisoren

TIplain theme

- Idee: Einsetzen von Punkten $P \in E$ in eine Funktion $f \in \overline{\mathbb{F}_q}(E)$

Hauptdivisoren

- Idee: Einsetzen von Punkten $P \in E$ in eine Funktion $f \in \overline{\mathbb{F}_q}(E)$
- Hat f in P eine Nullstelle, so definiere $\mathrm{ord}_P(f)$ als deren Vielfachheit.

Hauptdivisoren

TIplain theme

- Idee: Einsetzen von Punkten $P \in E$ in eine Funktion $f \in \overline{\mathbb{F}_q}(E)$
- Hat f in P eine Nullstelle, so definiere $\mathrm{ord}_P(f)$ als deren Vielfachheit.
- Hat f in P eine Polstelle, so definiere $\mathrm{ord}_P(f)$ als das Negative deren Vielfachheit.

Hauptdivisoren

- Idee: Einsetzen von Punkten $P \in E$ in eine Funktion $f \in \overline{\mathbb{F}_q}(E)$
- Hat f in P eine Nullstelle, so definiere $\mathrm{ord}_P(f)$ als deren Vielfachheit.
- Hat f in P eine Polstelle, so definiere $\mathrm{ord}_P(f)$ als das Negative deren Vielfachheit.
- Sonst ist $\mathrm{ord}_P(f) = 0$

Hauptdivisoren

RWTH AACHEN UNIVERSITY TIplain theme

- Idee: Einsetzen von Punkten $P \in E$ in eine Funktion $f \in \overline{\mathbb{F}_q}(E)$
- Hat f in P eine Nullstelle, so definiere $\mathrm{ord}_P(f)$ als deren Vielfachheit.
- Hat f in P eine Polstelle, so definiere $\mathrm{ord}_P(f)$ als das Negative deren Vielfachheit.
- Sonst ist $\mathrm{ord}_P(f) = 0$
- Da jede Funktion $f \in \overline{\mathbb{F}_q}(E)$ nur endlich viele Nullstellen und Pole hat, ist
$$\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f) P$$
ein Divisor.

Hauptdivisoren

TIplain theme

- Ein Hauptdivisor $\mathrm{div}(f)$ bestimmt die Funktion f eindeutig bis auf einen konstanten Faktor $c \neq 0$.

Hauptdivisoren

TIplain theme

- Ein Hauptdivisor $\mathrm{div}(f)$ bestimmt die Funktion f eindeutig bis auf einen konstanten Faktor $c \neq 0$.
- Hauptdivisoren haben Grad 0.

Hauptdivisoren

- Ein Hauptdivisor $\mathrm{div}(f)$ bestimmt die Funktion f eindeutig bis auf einen konstanten Faktor $c \neq 0$.
- Hauptdivisoren haben Grad 0.
- Zwei Divisoren D_1 und D_2 sind äquivalent, wenn $D_1 = D_2 - \mathrm{div}(f)$ für ein $f \in \overline{\mathbb{F}_q}(E)$.

Hauptdivisoren

- Ein Hauptdivisor $\mathrm{div}(f)$ bestimmt die Funktion f eindeutig bis auf einen konstanten Faktor $c \neq 0$.
- Hauptdivisoren haben Grad 0.
- Zwei Divisoren D_1 und D_2 sind äquivalent, wenn $D_1 = D_2 - \mathrm{div}(f)$ für ein $f \in \overline{\mathbb{F}_q}(E)$.
- Divisorklassengruppe von E: Divisoren vom Grad 0 modulo Äquivalenz

Divisoren und Funktionen

Definition

Sei $f \in \overline{\mathbb{F}_q}(E)$ und sei $D = \sum_{P \in E} n_P P$ ein Divisor mit Grad 0.
Sei weiter $\mathrm{supp}(D) \cap \mathrm{supp}(\mathrm{div}(f)) = \emptyset$, dann definiert man:

$$f(D) = \prod_{P \in E} f(P)^{n_P} = \prod_{P \in \mathrm{supp}(D)} f(P)^{n_P}$$

- Gegeben $P, Q \in E[r]$
- Sei $f \in \mathbb{F}_{q^k}(E)$ gegeben durch $\mathrm{div}(f) = n(P) - n(\mathcal{O})$.

Die Tate Paarung

TIplain theme

- Gegeben $P, Q \in E[r]$
- Sei $f \in \mathbb{F}_{q^k}(E)$ gegeben durch $\mathrm{div}(f) = n(P) - n(\mathcal{O})$.
- Sei $D \in \mathrm{Div}(E)$ mit $\deg(D) = 0$ und $D \sim (Q) - (\mathcal{O})$ und

$$\mathrm{supp}(\mathrm{div}(f)) \cap \mathrm{supp}(D) = \emptyset$$

Die Tate Paarung

RWTH AACHEN UNIVERSITY TIplain theme

- Gegeben $P, Q \in E[r]$
- Sei $f \in \mathbb{F}_{q^k}(E)$ gegeben durch $\mathrm{div}(f) = n(P) - n(\mathcal{O})$.
- Sei $D \in \mathrm{Div}(E)$ mit $\deg(D) = 0$ und $D \sim (Q) - (\mathcal{O})$ und

$$\mathrm{supp}(\mathrm{div}(f)) \cap \mathrm{supp}(D) = \emptyset$$

- Dann ist die Tate Paarung definiert durch:

$$\langle P, Q \rangle_r = f(D).$$

Die Tate Paarung

- Gegeben $P, Q \in E[r]$
- Sei $f \in \mathbb{F}_{q^k}(E)$ gegeben durch $\mathrm{div}(f) = n(P) - n(\mathcal{O})$.
- Sei $D \in \mathrm{Div}(E)$ mit $\deg(D) = 0$ und $D \sim (Q) - (\mathcal{O})$ und

$$\mathrm{supp}(\mathrm{div}(f)) \cap \mathrm{supp}(D) = \emptyset$$

- Dann ist die Tate Paarung definiert durch:

$$\langle P, Q \rangle_r = f(D).$$

interpretiert als ein Element aus $\mathbb{F}_{q^k}^* / (\mathbb{F}_{q^k}^*)^r$.

2 letzte „Probleme“

TIplain theme

- Wie bekommt man einen eindeutigen Repräsentanten von $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$?

2 letzte „Probleme“

RWTH AACHEN UNIVERSITY TIplain theme

- Wie bekommt man einen eindeutigen Repräsentanten von $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$?
- Wir benötigen zyklische Gruppen G_1 und G_2, $E[r]$ ist aber nicht zyklisch.

2 letzte „Probleme“

- Wie bekommt man einen eindeutigen Repräsentaten von $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$?
- Wir benötigen zyklische Gruppen G_1 und G_2, $E[r]$ ist aber nicht zyklisch.

Die abschließende Potenzierung

TIplain theme

- Die Gruppen $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$ und $\mu_r := \{x \in \mathbb{F}_{q^k} \mid x^r = 1\}$ sind isomorph.

Die abschließende Potenzierung

- Die Gruppen $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$ und $\mu_r := \{x \in \mathbb{F}_{q^k} \mid x^r = 1\}$ sind isomorph.
- Idee: Wende auf das Ergebnis der Tate-Paarung einen Isomorphismus $\phi : \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \to \mu_r$ an.

Die abschließende Potenzierung

- Die Gruppen $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$ und $\mu_r := \{x \in \mathbb{F}_{q^k} \mid x^r = 1\}$ sind isomorph.
- Idee: Wende auf das Ergebnis der Tate-Paarung einen Isomorphismus $\phi : \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \longrightarrow \mu_r$ an.
- $\phi : \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \longrightarrow \mu_r, \quad x \cdot (\mathbb{F}_{q^k})^r \mapsto x^{\frac{q^k-1}{r}}$
  ist ein solcher Isomorphismus.

Die abschließende Potenzierung

RWTH AACHEN UNIVERSITY TIplain theme

- Die Gruppen $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$ und $\mu_r := \{x \in \mathbb{F}_{q^k} \mid x^r = 1\}$ sind isomorph.
- Idee: Wende auf das Ergebnis der Tate-Paarung einen Isomorphismus $\phi : \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \to \mu_r$ an.
- $\phi : \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \to \mu_r, \quad x \cdot (\mathbb{F}_{q^k})^r \mapsto x^{\frac{q^k-1}{r}}$
  ist ein solcher Isomorphismus.
- Betrachte also nun die Paarung

$$e : E[r] \times E[r] \to \mu_r, \quad (P,Q) \mapsto \langle P,Q \rangle_r^{\frac{q^k-1}{r}}$$

2 letzte „Probleme“

RWTH AACHEN UNIVERSITY TIplain theme

- Wie bekommt man einen eindeutigen Repräsentaten von $\mathbb{F}_{q^k}^* / (\mathbb{F}_{q^k}^*)^r$?
- Wir benötigen zyklische Gruppen G_1 und G_2, $E[r]$ ist aber nicht zyklisch.

Der Frobenius-Endomorphismus und $E[r]$

RWTH AACHEN UNIVERSITY TIplain theme

- Der Frobenius-Endomorphismus

$$\pi_q : E[r] \to E[r], (x, y) \mapsto (x^q, y^q)$$

hat Eigenwerte 1 und q.

Der Frobenius-Endomorphismus und $E[r]$

- Der Frobenius-Endomorphismus

$$\pi_q : E[r] \to E[r], (x, y) \mapsto (x^q, y^q)$$

  hat Eigenwerte 1 und q.
- Eigenraum zum Eigenwert 1 ist $\ker(\pi_q - [1]) = E(\mathbb{F}_q)[r]$.

Der Frobenius-Endomorphismus und $E[r]$

- Der Frobenius-Endomorphismus

$$\pi_q : E[r] \to E[r], (x, y) \mapsto (x^q, y^q)$$

  hat Eigenwerte 1 und q.
- Eigenraum zum Eigenwert 1 ist $\ker(\pi_q - [1]) = E(\mathbb{F}_q)[r]$.
- Idee: Schränke Paarung ein auf $E(\mathbb{F}_q)[r] \times E(\mathbb{F}_q)[r]$

Der Frobenius-Endomorphismus und $E[r]$

- Der Frobenius-Endomorphismus
$$\pi_q : E[r] \to E[r], (x, y) \mapsto (x^q, y^q)$$
hat Eigenwerte 1 und q.
- Eigenraum zum Eigenwert 1 ist $\ker(\pi_q - [1]) = E(\mathbb{F}_q)[r]$.
- Idee: Schränke Paarung ein auf $E(\mathbb{F}_q)[r] \times E(\mathbb{F}_q)[r]$
- Problem: “Dann kommt immer 1 raus”

Der Frobenius-Endomorphismus und $E[r]$

- Der Frobenius-Endomorphismus

$$\pi_q : E[r] \to E[r], (x, y) \mapsto (x^q, y^q)$$

  hat Eigenwerte 1 und q.
- Eigenraum zum Eigenwert 1 ist $\ker(\pi_q - [1]) = E(\mathbb{F}_q)[r]$.

- Schränke zweites Argument auf den anderen Eigenraum $\ker(\pi_q - [q])$ ein.

Die letzte Folie

Paarung für kryptographische Protokolle:

$$e : \ker(\pi_q - [1]) \times \ker(\pi_q - [q]) \to \mu_r, \quad (P, Q) \mapsto \langle P, Q \rangle_r^{\frac{q^k - 1}{r}}$$

Die letzte Folie

RWTH AACHEN UNIVERSITY TIplain theme

Paarung für kryptographische Protokolle:

$$e : E(\mathbb{F}_q)[r] \times \ker(\pi_q - [q]) \to \mu_r, \quad (P, Q) \mapsto \langle P, Q \rangle_r^{\frac{q^k - 1}{r}}$$

Ausblick

- Millers Algorithmus (Berechnung der Funktion f)
- Paarungsfreundliche Kurven
- Ate Paarung, twisted Ate Paarung
- Implementierung in Hardware