Effiziente Berechnung der Tate-Paarung

Peter Schwabe

Lehrstuhl für Theoretische Informationstechnik

RWTH AACHEN

6.6.2007

AG Kommunikationstheorie

Überblick

Rückblick

Millers Algorithmus

Verbesserungen für Spezialfälle

Die Ate-Paarung

Weitere Aspekte

Die Tate Paarung

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

Die Tate Paarung

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

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

Die Tate Paarung

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

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

- Dann ist die Tate Paarung definiert durch:

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

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

Die Tate Paarung in der Kryptographie

- Abschließende Potenzierung mit $\frac{q^k-1}{r}$
- Isomorphismus von $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$ nach μ_r.

Die Tate Paarung in der Kryptographie

- Abschließende Potenzierung mit $\frac{q^k-1}{r}$
- Isomorphismus von $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$ nach μ_r.
- Einschränken der Argumente auf $\ker(\pi_q - [1]) \times \ker(\pi_q - [q]) = E(\mathbb{F}_q)[r] \times \ker(\pi_q - [q])$.

Die Tate Paarung in der Kryptographie

- Abschließende Potenzierung mit $\frac{q^k-1}{r}$
- Isomorphismus von $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$ nach μ_r.
- Einschränken der Argumente auf $\ker(\pi_q - [1]) \times \ker(\pi_q - [q]) = E(\mathbb{F}_q)[r] \times \ker(\pi_q - [q])$.
- Zu berechnende Funktion ist

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

Bestimmung des Divisors D

- Gegeben: $P, Q \in E[r]$.
- Gesucht: $D \in \mathrm{Div}^0(E)$ mit $D \sim (Q) - (\mathcal{O})$ und $\mathrm{supp}(D) \cap \{P, \mathcal{O}\} = \emptyset$.

Bestimmung des Divisors D

- Gegeben: $P, Q \in E[r]$.
- Gesucht: $D \in \mathrm{Div}^0(E)$ mit $D \sim (Q) - (\mathcal{O})$ und $\mathrm{supp}(D) \cap \{P, \mathcal{O}\} = \emptyset$.
- Wähle $S \in E[r]$ zufällig und setze $D = (Q + S) - (S)$.

Bestimmung der Funktion f

- Gegeben: $P \in E(\mathbb{F}_q)[r]$.
- Gesucht: $f \in \mathbb{F}_q(E)$ mit $\mathrm{div}(f) = r(P) - r(\mathcal{O})$.

Bestimmung der Funktion f

- Gegeben: $P \in E(\mathbb{F}_q)[r]$.
- Gesucht: $f \in \mathbb{F}_q(E)$ mit $\mathrm{div}(f) = r(P) - r(\mathcal{O})$.
- Idee: Definiere f_i durch $\mathrm{div}(f_i) = i(P) - ([i]P) - (i-1)(\mathcal{O})$

Bestimmung der Funktion f

- Gegeben: $P \in E(\mathbb{F}_q)[r]$.
- Gesucht: $f \in \mathbb{F}_q(E)$ mit $\operatorname{div}(f) = r(P) - r(\mathcal{O})$.
- Idee: Definiere f_i durch $\operatorname{div}(f_i) = i(P) - ([i]P) - (i-1)(\mathcal{O})$
- Berechne dann $f_r = f$ durch Rekursion:

$$f_1 = 1$$

$$f_{i+j} = f_i f_j \frac{l}{v}$$

wobei l und v die in der Punktaddition $[i]P + [j]P$ verwendeten Geraden sind.

Millers Algorithmus

Eingabe:
$P \in \ker(\pi_q - [1]), Q \in \ker(\pi_q - [q]), S \in E[r], r = (r_m, \ldots, r_0)_2$
Ausgabe: $\langle P, Q \rangle_r$
$Q' \leftarrow Q + S$
$R \leftarrow P$
for $(i \leftarrow m - 1; i \geq 0; i - -)$ **do**
  Calculate lines l and v for doubling R
  $R \leftarrow [2]R$
  $f \leftarrow f^2 \frac{l(Q')v(S)}{v(Q')l(S)}$
  if $(r_i = 1)$ **then**
    Compute lines l and v for adding P and R
    $R \leftarrow R + P$
    $f \leftarrow f \frac{l(Q')v(S)}{v(Q')l(S)}$
  end if
end for
return f

Punkte statt Divisoren

Was geschieht durch die abschließende Potenzierung?

Alle in der Miller-Schleife auftretenden Faktoren, die in einem echten Teilkörper von $\mathbb{F}_{q^k}$ liegen, werden in der abschließenden Potenzierung auf 1 abgebildet.

Punkte statt Divisoren

Was geschieht durch die abschließende Potenzierung?

Alle in der Miller-Schleife auftretenden Faktoren, die in einem echten Teilkörper von $\mathbb{F}_{q^k}$ liegen, werden in der abschließenden Potenzierung auf 1 abgebildet.

Idee

Wähle in der Konstruktion von D den Punkt S aus $E(\mathbb{F}_q)$. Dann sind $v(S), l(S) \in \mathbb{F}_q$.

Punkte anstatt von Divisoren

Eingabe: $P, S \in \ker(\pi_q - [1]), Q \in \ker(\pi_q - [q]), r = (r_m, \dots, r_0)_2$
Ausgabe: $\langle P, Q \rangle_r$

```
Q' ← Q + S
R ← P
for (i ← m − 1; i ≥ 0; i − −) do
    Calculate lines l and v for doubling R
    R ← [2]R
    f ← f^2 · l(Q')/v(Q')
    if (r_i = 1) then
        Compute lines l and v for adding P and R
        R ← R + P
        f ← f · l(Q')/v(Q')
    end if
end for
return f
```

Punkte anstatt von Divisoren

Eingabe: $P, S \in \ker(\pi_q - [1]), Q \in \ker(\pi_q - [q]), r = (r_m, \dots, r_0)_2$
Ausgabe: $\langle P, Q \rangle_r$

```
R ← P
for (i ← m − 1; i ≥ 0; i − −) do
    Calculate lines l and v for doubling R
    R ← [2]R
    f ← f^2 · l(Q)/v(Q)
    if (r_i = 1) then
        Compute lines l and v for adding P and R
        R ← R + P
        f ← f · l(Q)/v(Q)
    end if
end for
return f
```

$R \leftarrow P$
for $(i \leftarrow m-1; i \geq 0; i--)$ **do**
  Calculate lines l and v for doubling R
  $R \leftarrow [2]R$
  $f \leftarrow f^2 \frac{l(Q)}{v(Q)}$
  if $(r_i = 1)$ **then**
    Compute lines l and v for adding P and R
    $R \leftarrow R + P$
    $f \leftarrow f \frac{l(Q)}{v(Q)}$
  end if
end for
return f

Nenner eliminieren

- Die Gerade v ist von der Form $x - c = 0$.
- Idee: Ist die x-Koordinate von Q' Element eines echten Teilkörpers von $\mathbb{F}_{q^k}$, so muss man keinen Nenner berechnen.

Nenner eliminieren

Eingabe: $P, S \in \ker(\pi_q - [1]) Q \in \ker(\pi_q - [q]), r = (r_m, \ldots, r_0)_2$
Ausgabe: $\langle P, Q \rangle_r$

$R \leftarrow P$
for $(i \leftarrow m-1; i \geq 0; i--)$ **do**
  Calculate lines l and v for doubling R
  $R \leftarrow [2]R$
  $f \leftarrow f^2 l(Q)$
  if $(r_i = 1)$ **then**
    Compute lines l and v for adding P and R
    $R \leftarrow R + P$
    $f \leftarrow f l(Q)$
  end if
end for
return f

Ein Blick auf BN-Kurven

- Es sei $E : y^2 = x^3 + b$ eine BN-Kurve über $\mathbb{F}_p$

Ein Blick auf BN-Kurven

- Es sei $E : y^2 = x^3 + b$ eine BN-Kurve über $\mathbb{F}_p$
- Es existiert $\xi \in \mathbb{F}_{p^2}$ so dass $X^6 - \xi$ irreduzibel über $\mathbb{F}_{p^2}$.

Ein Blick auf BN-Kurven

- Es sei $E : y^2 = x^3 + b$ eine BN-Kurve über $\mathbb{F}_p$
- Es existiert $\xi \in \mathbb{F}_{p^2}$ so dass $X^6 - \xi$ irreduzibel über $\mathbb{F}_{p^2}$.
- Weiter existiert eine Kurve $E' : y^2 = x^3 + b\xi^{-1}$ über $\mathbb{F}_{p^2}$ mit $E'(\mathbb{F}_{p^{12}}) \cong E(\mathbb{F}_{p^{12}})$.

Ein Blick auf BN-Kurven

- Es sei $E : y^2 = x^3 + b$ eine BN-Kurve über $\mathbb{F}_p$
- Es existiert $\xi \in \mathbb{F}_{p^2}$ so dass $X^6 - \xi$ irreduzibel über $\mathbb{F}_{p^2}$.
- Weiter existiert eine Kurve $E' : y^2 = x^3 + b\xi^{-1}$ über $\mathbb{F}_{p^2}$ mit $E'(\mathbb{F}_{p^{12}}) \cong E(\mathbb{F}_{p^{12}})$.
- Isomorphismus $\psi : E' \to E, (x, y) \mapsto (z^2x, z^3y)$, für eine Nullstelle $z \in \mathbb{F}_{p^{12}}$ von $X^6 - \xi$

Ein Blick auf BN-Kurven

- Es sei $E : y^2 = x^3 + b$ eine BN-Kurve über $\mathbb{F}_p$
- Es existiert $\xi \in \mathbb{F}_{p^2}$ so dass $X^6 - \xi$ irreduzibel über $\mathbb{F}_{p^2}$.
- Weiter existiert eine Kurve $E' : y^2 = x^3 + b\xi^{-1}$ über $\mathbb{F}_{p^2}$ mit $E'(\mathbb{F}_{p^{12}}) \cong E(\mathbb{F}_{p^{12}})$.
- Isomorphismus $\psi : E' \to E, (x, y) \mapsto (z^2 x, z^3 y)$, für eine Nullstelle $z \in \mathbb{F}_{p^{12}}$ von $X^6 - \xi$
- Es ist $\psi(E'(\mathbb{F}_{p^2})[r]) = \ker(\pi_p - p)$

Ein Blick auf BN-Kurven

- Es sei $E : y^2 = x^3 + b$ eine BN-Kurve über $\mathbb{F}_p$
- Es existiert $\xi \in \mathbb{F}_{p^2}$ so dass $X^6 - \xi$ irreduzibel über $\mathbb{F}_{p^2}$.
- Weiter existiert eine Kurve $E' : y^2 = x^3 + b\xi^{-1}$ über $\mathbb{F}_{p^2}$ mit $E'(\mathbb{F}_{p^{12}}) \cong E(\mathbb{F}_{p^{12}})$.
- Isomorphismus $\psi : E' \to E, (x, y) \mapsto (z^2 x, z^3 y)$, für eine Nullstelle $z \in \mathbb{F}_{p^{12}}$ von $X^6 - \xi$
- Es ist $\psi(E'(\mathbb{F}_{p^2})[r]) = \ker(\pi_p - p)$
- Es ist $z^2 \in \mathbb{F}_{p^6}$ und $z^3 \in F_{p^4}$

Ein Blick auf BN-Kurven

- Es sei $E : y^2 = x^3 + b$ eine BN-Kurve über $\mathbb{F}_p$
- Es existiert $\xi \in \mathbb{F}_{p^2}$ so dass $X^6 - \xi$ irreduzibel über $\mathbb{F}_{p^2}$.
- Weiter existiert eine Kurve $E' : y^2 = x^3 + b\xi^{-1}$ über $\mathbb{F}_{p^2}$ mit $E'(\mathbb{F}_{p^{12}}) \cong E(\mathbb{F}_{p^{12}})$.
- Isomorphismus $\psi : E' \to E, (x, y) \mapsto (z^2x, z^3y)$, für eine Nullstelle $z \in \mathbb{F}_{p^{12}}$ von $X^6 - \xi$
- Es ist $\psi(E'(\mathbb{F}_{p^2})[r]) = \ker(\pi_p - p)$
- Es ist $z^2 \in \mathbb{F}_{p^6}$ und $z^3 \in F_{p^4}$
- Sei $(x, y) \in \ker(\pi_p - p)$, dann ist $(x, y) \in \mathbb{F}_{p^6} \times \mathbb{F}_{p^4}$

Ein Blick auf BN-Kurven

- Es sei $E : y^2 = x^3 + b$ eine BN-Kurve über $\mathbb{F}_p$
- Es existiert $\xi \in \mathbb{F}_{p^2}$ so dass $X^6 - \xi$ irreduzibel über $\mathbb{F}_{p^2}$.
- Weiter existiert eine Kurve $E' : y^2 = x^3 + b\xi^{-1}$ über $\mathbb{F}_{p^2}$ mit $E'(\mathbb{F}_{p^{12}}) \cong E(\mathbb{F}_{p^{12}})$.
- Isomorphismus $\psi : E' \to E, (x, y) \mapsto (z^2x, z^3y)$, für eine Nullstelle $z \in \mathbb{F}_{p^{12}}$ von $X^6 - \xi$
- Es ist $\psi(E'(\mathbb{F}_{p^2})[r]) = \ker(\pi_p - p)$
- Es ist $z^2 \in \mathbb{F}_{p^6}$ und $z^3 \in F_{p^4}$
- Sei $(x, y) \in \ker(\pi_p - p)$, dann ist $(x, y) \in \mathbb{F}_{p^6} \times \mathbb{F}_{p^4}$
- Eliminierung von Nennern ist bei BN-Kurven möglich.

Die Ate-Paarung

- Seien $P \in E(\mathbb{F}_q)$ und $Q \in \ker(\pi_q - q)$.

Die Ate-Paarung

- Seien $P \in E(\mathbb{F}_q)$ und $Q \in \ker(\pi_q - q)$.
- Sei $\#E(\mathbb{F}_q) = q + 1 - t$, setze $T = t - 1$.

Die Ate-Paarung

- Seien $P \in E(\mathbb{F}_q)$ und $Q \in \ker(\pi_q - q)$.
- Sei $\#E(\mathbb{F}_q) = q + 1 - t$, setze $T = t - 1$.
- Sei $f_{T,Q} \in \mathbb{F}_{q^k}(E)$ gegeben durch $\operatorname{div}(f_{T,Q}) = T(Q) - ([T]Q) - (T-1)(\mathcal{O})$.

Die Ate-Paarung

- Seien $P \in E(\mathbb{F}_q)$ und $Q \in \ker(\pi_q - q)$.
- Sei $\#E(\mathbb{F}_q) = q + 1 - t$, setze $T = t - 1$.
- Sei $f_{T,Q} \in \mathbb{F}_{q^k}(E)$ gegeben durch $\mathrm{div}(f_{T,Q}) = T(Q) - ([T]Q) - (T-1)(\mathcal{O})$.
- $f_{T,Q}(P)$ ist eine Paarung, die sog. Ate-Paarung.

Die Ate-Paarung

- Seien $P \in E(\mathbb{F}_q)$ und $Q \in \ker(\pi_q - q)$.
- Sei $\#E(\mathbb{F}_q) = q + 1 - t$, setze $T = t - 1$.
- Sei $f_{T,Q} \in \mathbb{F}_{q^k}(E)$ gegeben durch $\operatorname{div}(f_{T,Q}) = T(Q) - ([T]Q) - (T-1)(\mathcal{O})$.
- $f_{T,Q}(P)$ ist eine Paarung, die sog. Ate-Paarung.
- Auch hier: Abschließende Potenzierung

Millers Algorithmus für die Ate-Paarung

Eingabe: $P \in E(\mathbb{F}_p)[r], Q \in \ker(\pi_q - q), 0 < T = (T_m, \ldots, T_0)_2$ mit $\#E(\mathbb{F}_q) = q - T$

Ausgabe: $f_{T,Q}(P)$

$R \leftarrow Q$

for $(i \leftarrow m-1; i \geq 0; i--)$ **do**

Calculate lines l and v for doubling R

$R \leftarrow [2]R$

$f \leftarrow f^2 \frac{l(P)}{v(P)}$

if $(r_i = 1)$ **then**

Compute lines l and v for adding P and R

$R \leftarrow R + Q$

$f \leftarrow f \frac{l(P)}{v(P)}$

end if

end for

return f

Ate vs. Tate

- Full Miller – Miller-Lite

Ate vs. Tate

- Full Miller – Miller-Lite
- Deutlich kürzere Miller-Schleife bei Ate ($T \approx \sqrt{r}$)

Ate vs. Tate

- Full Miller – Miller-Lite
- Deutlich kürzere Miller-Schleife bei Ate ($T \approx \sqrt{r}$)
- Abschätzung von Hess, Smart und Vercauteren (2006) passend für BN-Kurven:
  - Tate: 26880 Multiplikationen in $\mathbb{F}_p$
  - Ate: 15488 Multiplikationen in $\mathbb{F}_p$

Ate vs. Tate

- Full Miller – Miller-Lite
- Deutlich kürzere Miller-Schleife bei Ate ($T \approx \sqrt{r}$)
- Abschätzung von Hess, Smart und Vercauteren (2006) passend für BN-Kurven:
  - Tate: 26880 Multiplikationen in $\mathbb{F}_p$
  - Ate: 15488 Multiplikationen in $\mathbb{F}_p$
- Implementierung von Scott (2007):
  - Tate: 46,1 Millisekunden auf 3,4 GHz Pentium 4
  - Ate: 39,3 Millisekunden auf 3,4 GHz Pentium 4

Weitere Aspekte

- Implementierung der zugrunde liegenden Körper (Devigili, Ó hÉigeartaigh, Scott, Dahab, 2006)

Weitere Aspekte

- Implementierung der zugrunde liegenden Körper (Devigili, Ó hÉigeartaigh, Scott, Dahab, 2006)
- Effziente Berechnung der abschließenden Potenzierung

Weitere Aspekte

- Implementierung der zugrunde liegenden Körper (Devigili, Ó hÉigeartaigh, Scott, Dahab, 2006)
- Effziente Berechnung der abschließenden Potenzierung
- Ausnutzen des Twists bei der Berechnung der Ate-Paarung

Weitere Aspekte

- Implementierung der zugrunde liegenden Körper (Devigili, Ó hÉigeartaigh, Scott, Dahab, 2006)
- Effziente Berechnung der abschließenden Potenzierung
- Ausnutzen des Twists bei der Berechnung der Ate-Paarung
- Twisted Ate Pairing

Weitere Aspekte

- Implementierung der zugrunde liegenden Körper (Devigili, Ó hÉigeartaigh, Scott, Dahab, 2006)
- Effziente Berechnung der abschließenden Potenzierung
- Ausnutzen des Twists bei der Berechnung der Ate-Paarung
- Twisted Ate Pairing
- "Optimised Ate Pairing" (Matsuda, Kanayama, Hess, Okamoto, 2007)