

Mathematical Foundations of Elliptic Curve Cryptography

Diplomarbeit

Clemens Koppensteiner

TU Wien – Institut für diskrete Mathematik und Geometrie
Betreuer: Michael Drmota

9. Juni 2009

Wieso *elliptic curve* cryptography?

Diffie-Hellman, RSA

Diffie-Hellman, RSA

Subexponentielle Algorithmen zur Lösung des zugrundeliegenden Problems!

Diffie-Hellman, RSA

Subexponentielle Algorithmen zur Lösung des zugrundeliegenden Problems!

Was tun?

Idee: verwende eine andere Gruppe für DH

Idee: verwende eine andere Gruppe für DH

Nur welche?

Mögliche Quelle für Gruppen:

Jacobivarietäten algebraischer Kurven

Mögliche Quelle für Gruppen:
Jacobivarietäten algebraischer Kurven

Algorithmisch brauchbar?

Mögliche Quelle für Gruppen:
Jacobivarietäten algebraischer Kurven

Algorithmisch brauchbar?

Ja.

Zumindest von elliptischen und hyperelliptischen Kurven.

Mögliche Quelle für Gruppen:
Jacobivarietäten algebraischer Kurven

Algorithmisch brauchbar?

Ja.

Zumindest von elliptischen ~~und hyperelliptischen~~ Kurven.

Was sind *elliptische Kurven*?

Definition

Eine elliptische Kurve ist eine **glatte algebraische Kurve mit Geschlecht 1** mit einem ausgezeichneten Punkt.

Definition

Eine elliptische Kurve ist eine glatte Kurve, gegeben durch eine Gleichung

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

in $\mathbb{P}^2(\bar{K})$, wobei der Punkt $\mathcal{O} = [0 : 1 : 0]$ ausgezeichnet ist.

Warum sind elliptische Kurven interessant?

Warum sind elliptische Kurven interessant?

Die elliptische Kurve ist **ihre eigene Jacobi-Varietät!**

Warum sind elliptische Kurven interessant?

Die elliptische Kurve ist ihre eigene Jacobi-Varietät!

Die Gruppenelemente lassen also sich einfach darstellen
(und speichern).

Die Jacobi-Varietät induziert eine **effizient berechenbare Gruppenstruktur** auf der elliptischen Kurve.

Die Jacobi-Varietät induziert eine effizient berechenbare Gruppenstruktur auf der elliptischen Kurve.

- **geometrisch**: Addition ist mit Zirkel und Lineal möglich.

Die Jacobi-Varietät induziert eine effizient berechenbare Gruppenstruktur auf der elliptischen Kurve.

- geometrisch: Addition ist mit Zirkel und Lineal möglich.
- **arithmetisch**: Koordinaten der Summe als rationale Funktion in den Summanden.

Noch ein Problem.

Wie groß ist $E(\mathbb{F}_q)$?

Wie groß ist $E(\mathbb{F}_q)$ **ungefähr**?

Wie groß ist $E(\mathbb{F}_q)$ ungefähr?

Theorem (Satz von Hasse)

$$|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}.$$

Wie groß ist $E(\mathbb{F}_q)$?

Theorem (Folgerung aus den Weil-Vermutungen)

Sei E definiert über \mathbb{F}_q .

Wenn man $\#E(\mathbb{F}_q)$ kennt, kennt man auch $\#E(\mathbb{F}_{q^n})$.

- Naive Methoden

Algorithmen zur Bestimmung von $\#E(\mathbb{F}_q)$

- Naive Methoden
- **Schoofs Algorithmus**
 - Berechne $\#E(\mathbb{F}_q) \bmod \ell$ für $\ell < \log q$ prim.
 - Verwende den chinesischen Restsatz.
 - Mit Verbesserungen: SEA-Algorithmus.

Algorithmen zur Bestimmung von $\#E(\mathbb{F}_q)$

- Naive Methoden
- Schoofs Algorithmus
 - Berechne $\#E(\mathbb{F}_q) \bmod \ell$ für $\ell < \log q$ prim.
 - Verwende den chinesischen Restsatz.
 - Mit Verbesserungen: SEA-Algorithmus.
- **Satohs Algorithmus**
 - Lifte E/\mathbb{F}_q zu \mathcal{E}/\mathbb{Q}_q (kanonischer Lift).
 - Benutze Eigenschaften des kanonischen Lifts.

Elliptic Curve Cryptography

Verwende Diffie-Hellman Varianten in einer zyklischen Untergruppe von $E(\mathbb{F}_q)$:

- Schlüsselaustausch: EC-DH, ECMQV
- Verschlüsselung: ECIES
- Signaturen: ECDSA

Elliptic Curve Diffie-Hellman Problem

Gegeben die Punkte P , $[n]P$ und $[m]P$, finde $[nm]P$.

Elliptic Curve Diffie-Hellman Problem

Gegeben die Punkte P , $[n]P$ und $[m]P$, finde $[nm]P$.

Elliptic Curve Discrete Logarithm Problem

Gegeben die Punkte P und $[n]P$, finde n .

Diskreter Logarithmus: Klassische Algorithmen

$Q = [m]P$, $n = \text{ord } P$; gesucht: m .

- Pohlig-Hellman reduction: Nur der größte Primteiler von n zählt.
- Baby-step giant-step, Pollard- ρ , u.a.: $O(\sqrt{n})$.

$Q = [m]P$, $n = \text{ord } P$; gesucht: m .

- Pohlig-Hellman reduction: Nur der größte Primteiler von n zählt.
- Baby-step giant-step, Pollard- ρ , u.a.: $O(\sqrt{n})$.
- **Index Calculus auf elliptischen Kurven nicht anwendbar.**

Diskreter Logarithmus: Algorithmen für elliptische Kurven

$Q = [m]P$, $n = \text{ord } P$; gesucht: m .

Diskreter Logarithmus: Algorithmen für elliptische Kurven

$Q = [m]P$, $n = \text{ord } P$; gesucht: m .

Idee: Übertrage das DLP von der elliptischen Kurve in eine Gruppe, in der effizientere Methoden bekannt sind (\mathbb{F}_q , hyperelliptische Kurven).

Diskreter Logarithmus: Algorithmen für elliptische Kurven

$Q = [m]P$, $n = \text{ord } P$; gesucht: m .

Idee: Übertrage das DLP von der elliptischen Kurve in eine Gruppe, in der effizientere Methoden bekannt sind (\mathbb{F}_q , hyperelliptische Kurven).

Funktioniert nur bei speziellen Kurven.

Wähle ein *pairing*

$$e: E[n] \times E[n] \rightarrow \mu_n(\overline{\mathbb{F}}_q) \subseteq \mathbb{F}_{q^k}$$

bilinear und nicht degeneriert. ($E[n] = \{P \in E : [n]P = \mathcal{O}\}$)

Wähle ein *pairing*

$$e: E[n] \times E[n] \rightarrow \mu_n(\overline{\mathbb{F}}_q) \subseteq \mathbb{F}_{q^k}$$

bilinear und nicht degeneriert. ($E[n] = \{P \in E : [n]P = \mathcal{O}\}$)

Wähle S fest mit $e(P, S)$ primitiv.

$$e(Q, S) = e([m]P, S) = e(P, S)^m.$$

Wähle ein *pairing*

$$e: E[n] \times E[n] \rightarrow \mu_n(\bar{\mathbb{F}}_q) \subseteq \mathbb{F}_{q^k}$$

bilinear und nicht degeneriert. ($E[n] = \{P \in E : [n]P = \mathcal{O}\}$)

Wähle S fest mit $e(P, S)$ primitiv.

$$e(Q, S) = e([m]P, S) = e(P, S)^m.$$

$\mathbb{F}_{q^k}^*$ -DLP

$\mathbb{F}_{q^k}^*$ -DLP

Subexponentiell in $k \log q$

$$\mathbb{F}_{q^k}^* \text{-DLP}$$

Subexponentiell in $k \log q$

Für supersinguläre Kurven: $k \leq 6$.

$$\mathbb{F}_{q^k}^* \text{-DLP}$$

Subexponentiell in $k \log q$

Für supersinguläre Kurven: $k \leq 6$.

sonst: k meist sehr groß.

Falls $\text{ggT}(q, n) > 1$, gibt es kein solches pairing.

Falls $\text{ggT}(q, n) > 1$, gibt es kein solches pairing.

Idee: verwende Kurven mit $n = q$.

Falls $\text{ggT}(q, n) > 1$, gibt es kein solches pairing.

Idee: verwende Kurven mit $n = q$.

Aber: In diesem Fall existiert ein Isomorphismus

$$E(\mathbb{F}_q) \rightarrow \mathbb{F}_q^+.$$

Falls $\text{ggT}(q, n) > 1$, gibt es kein solches pairing.

Idee: verwende Kurven mit $n = q$.

Aber: In diesem Fall existiert ein Isomorphismus

$$E(\mathbb{F}_q) \rightarrow \mathbb{F}_q^+.$$

DLP ist in **linearer Zeit** lösbar.

Theorem (Weil restriction)

Es gibt eine abelsche Varietät A der Dimension k und einen Isomorphismus

$$E(\mathbb{F}_{q^k}) \rightarrow A(\mathbb{F}_q).$$

Theorem (Weil restriction)

Es gibt eine abelsche Varietät A der Dimension k und einen Isomorphismus

$$E(\mathbb{F}_{q^k}) \rightarrow A(\mathbb{F}_q).$$

Einfacherer Körper aber kompliziertere Varietät.

Theorem (Weil restriction)

Es gibt eine abelsche Varietät A der Dimension k und einen Isomorphismus

$$E(\mathbb{F}_{q^k}) \rightarrow A(\mathbb{F}_q).$$

Einfacherer Körper aber kompliziertere Varietät.

Manchmal: DLP lässt sich in A einfacher lösen.
Insbesondere für k klein und $k \geq 3$.

- Keinen allgemeinen Algorithmus um ECDLP schnell zu lösen.

- Keinen allgemeinen Algorithmus um ECDLP schnell zu lösen.
- Vermeide Kurven mit besonders schöner Struktur (supersinguläre, anomale).

- Keinen allgemeinen Algorithmus um ECDLP schnell zu lösen.
- Vermeide Kurven mit besonders schöner Struktur (supersinguläre, anomale).
- Vermeide \mathbb{F}_{p^k} mit k zusammengesetzt.

- Keinen allgemeinen Algorithmus um ECDLP schnell zu lösen.
- Vermeide Kurven mit besonders schöner Struktur (supersinguläre, anomale).
- Vermeide \mathbb{F}_{p^k} mit k zusammengesetzt.
- Dann: ECC liefert höhere Sicherheit bei kleinerer Schlüsselgröße.

- Keinen allgemeinen Algorithmus um ECDLP schnell zu lösen.
- Vermeide Kurven mit besonders schöner Struktur (supersinguläre, anomale).
- Vermeide \mathbb{F}_{p^k} mit k zusammengesetzt.
- Dann: ECC liefert höhere Sicherheit bei kleinerer Schlüsselgröße.

- Keinen allgemeinen Algorithmus um ECDLP schnell zu lösen.
- Vermeide Kurven mit besonders schöner Struktur (supersinguläre, anomale).
- Vermeide \mathbb{F}_{p^k} mit k zusammengesetzt.
- Dann: ECC liefert höhere Sicherheit bei kleinerer Schlüsselgröße.

- Keinen allgemeinen Algorithmus um ECDLP schnell zu lösen.
- Vermeide Kurven mit besonders schöner Struktur (supersinguläre, anomale).
- Vermeide \mathbb{F}_{p^k} mit k zusammengesetzt.
- Dann: ECC liefert höhere Sicherheit bei kleinerer Schlüsselgröße.