

Kryptographie mit Elliptischen Kurven

Diplomarbeit

Clemens Koppensteiner

26. Juni 2009

Wieso *elliptic curve* cryptography?

Diffie-Hellman, RSA

Diffie-Hellman, RSA

Subexponentielle Algorithmen zur Lösung der zugrundeliegenden Probleme!

Diffie-Hellman, RSA

Subexponentielle Algorithmen zur Lösung der zugrundeliegenden Probleme!

Was tun?

Idee: verwende eine andere Gruppe für DH

Idee: verwende eine andere Gruppe für DH

Nur welche?

Mögliche Quelle für Gruppen:

Jacobi-Varietäten algebraischer Kurven

Mögliche Quelle für Gruppen:
Jacobi-Varietäten algebraischer Kurven

Algorithmisch brauchbar?

Mögliche Quelle für Gruppen:
Jacobi-Varietäten algebraischer Kurven

Algorithmisch brauchbar?

Ja.

Zumindest von elliptischen und hyperelliptischen Kurven.

Mögliche Quelle für Gruppen:
Jacobi-Varietäten algebraischer Kurven

Algorithmisch brauchbar?

Ja.

Zumindest von elliptischen ~~und hyperelliptischen~~ Kurven.

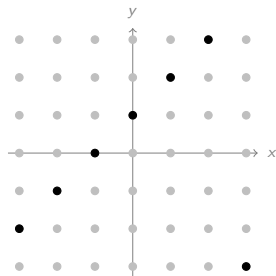
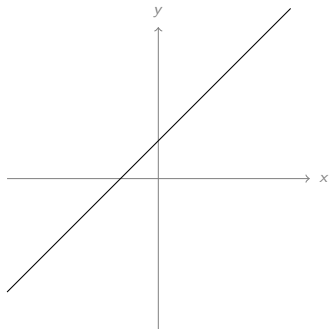
Exkurs: Jacobi-Varietäten

Definition

Eine **ebene affine algebraische Kurve** über eine Körper K ist die Nullstellenmenge eines Polynomes aus $K[x, y]$.

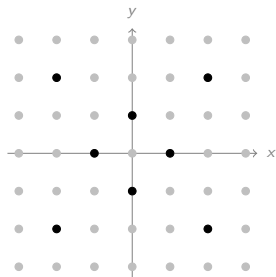
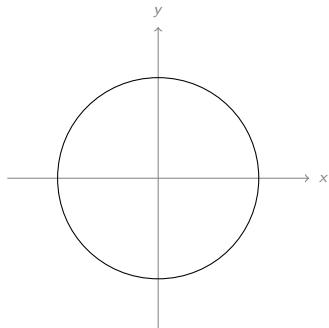
Beispiele algebraischer Kurven (über \mathbb{R} und \mathbb{F}_7)

$$f(x, y) = x - y + 1$$



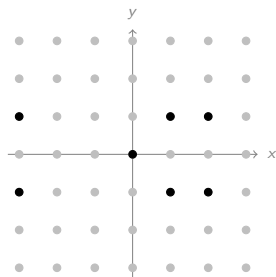
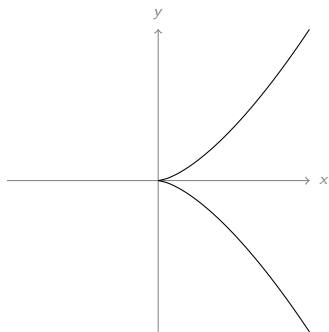
Beispiele algebraischer Kurven (über \mathbb{R} und \mathbb{F}_7)

$$f(x, y) = x^2 + y^2 - 1$$



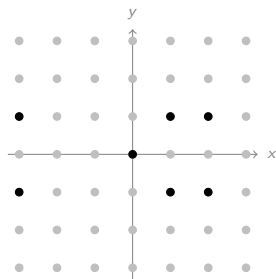
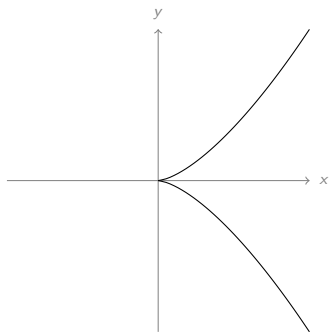
Beispiele algebraischer Kurven (über \mathbb{R} und \mathbb{F}_7)

$$f(x, y) = y^2 - x^3$$



Beispiele algebraischer Kurven (über \mathbb{R} und \mathbb{F}_7)

$$f(x, y) = y^2 - x^3$$



$$\frac{\partial f}{\partial x} = 3x^2$$

$$\frac{\partial f}{\partial y} = 2y$$

Wir betrachten

- glatte Kurven
- im projektiven Raum.

Definition

Ein **Divisor** einer Kurve C ist eine formale Summe

$$D = \sum_{P \in C} n_P(P)$$

mit $n_P \in \mathbb{Z}$ und fast alle $n_P = 0$. Die Menge aller Divisoren wird mit $\text{Div}(C)$ bezeichnet.

Definition

Ein Divisor einer Kurve C ist eine formale Summe

$$D = \sum_{P \in C} n_P(P)$$

mit $n_P \in \mathbb{Z}$ und fast alle $n_P = 0$. Die Menge aller Divisoren wird mit $\text{Div}(C)$ bezeichnet.

Addition:
$$\sum_{P \in C} n_P(P) + \sum_{P \in C} m_P(P) = \sum_{P \in C} (n_P + m_P)(P).$$

Definition

Ein Divisor einer Kurve C ist eine formale Summe

$$D = \sum_{P \in C} n_P(P)$$

mit $n_P \in \mathbb{Z}$ und fast alle $n_P = 0$. Die Menge aller Divisoren wird mit $\text{Div}(C)$ bezeichnet.

$$\text{Addition: } \sum_{P \in C} n_P(P) + \sum_{P \in C} m_P(P) = \sum_{P \in C} (n_P + m_P)(P).$$

fancy: $\text{Div}(C)$ ist die **von C frei erzeugte abelsche Gruppe**.

Definition

Der **Grad** eines Divisors

$$D = \sum_{P \in C} n_P(P)$$

ist

$$\deg(D) = \sum_{P \in C} n_P \in \mathbb{Z}.$$

Definition

Der Grad eines Divisors

$$D = \sum_{P \in C} n_P(P)$$

ist

$$\deg(D) = \sum_{P \in C} n_P \in \mathbb{Z}.$$

Die **Divisoren von Grad 0** bilden eine Untergruppe von $\text{Div}(C)$, die mit $\text{Div}^0(C)$ bezeichnet wird.

Sei f eine *rationale Funktion* auf C .

Sei f eine *rationale Funktion* auf C .

Definition

Der **Divisor von f** ist

$$\operatorname{div}(f) = \sum_{P \in C} \operatorname{ord}_P(f)(P) \in \operatorname{Div}(C).$$

Sei f eine *rationale Funktion* auf C .

Definition

Der Divisor von f ist

$$\operatorname{div}(f) = \sum_{P \in C} \operatorname{ord}_P(f)(P) \in \operatorname{Div}(C).$$

Theorem

Sei K *algebraisch abgeschlossen*.

$$\deg \operatorname{div}(f) = 0.$$

Die Picard-Gruppe

Zwei Divisoren D_1, D_2 heißen linear äquivalent, wenn es eine rationale Funktion f gibt mit

$$D_1 = D_2 + \operatorname{div}(f).$$

Die Picard-Gruppe

Zwei Divisoren D_1, D_2 heißen linear äquivalent, wenn es eine rationale Funktion f gibt mit

$$D_1 = D_2 + \operatorname{div}(f).$$

Definition

Die Gruppe der Divisoren von $D \in \operatorname{Div}^0(C)$ modulo linearer Äquivalenz heißt Grad-0-Teil der **Picard-Gruppe** von C , $\operatorname{Pic}^0(C)$.

$$\begin{aligned} & \text{„Pic}^0(C) \\ & + \\ & \text{geometrische Struktur} \\ & = \\ & \text{Jacobi-Varietät von } C \end{aligned}$$

Zurück zu elliptischen 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?

$$\begin{aligned}\mathrm{Pic}^0(E) &\xrightarrow{\cong} E \\ [(P) - (\mathcal{O})] &\mapsto P\end{aligned}$$

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

Warum sind elliptische Kurven interessant?

$$\begin{aligned} \text{Pic}^0(E) &\xrightarrow{\cong} E \\ [(P) - (\mathcal{O})] &\mapsto P \end{aligned}$$

Die elliptische Kurve ist ihre eigene Jacobi-Varietät!

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

Rechnen auf elliptischen Kurven

$$P_1 \quad + \quad P_2 \quad =$$

Rechnen auf elliptischen Kurven

$$\begin{array}{ccc} P_1 & + & P_2 & = \\ \downarrow \text{wavy} & & \downarrow \text{wavy} & \\ (P_1) - (\mathcal{O}) & + & (P_2) - (\mathcal{O}) & \end{array}$$

Rechnen auf elliptischen Kurven

$$\begin{array}{ccccc} P_1 & + & P_2 & = & \\ \downarrow \text{wavy} & & \downarrow \text{wavy} & & \\ (P_1) - (\mathcal{O}) & + & (P_2) - (\mathcal{O}) & = & (P_1) + (P_2) - 2(\mathcal{O}) \end{array}$$

Rechnen auf elliptischen Kurven

$$\begin{array}{ccccc} P_1 & + & P_2 & = & ? \\ \downarrow \text{wavy} & & \downarrow \text{wavy} & & \uparrow \text{wavy} \\ (P_1) - (\mathcal{O}) & + & (P_2) - (\mathcal{O}) & = & (P_1) + (P_2) - 2(\mathcal{O}) \end{array}$$

Rechnen auf elliptische Kurven

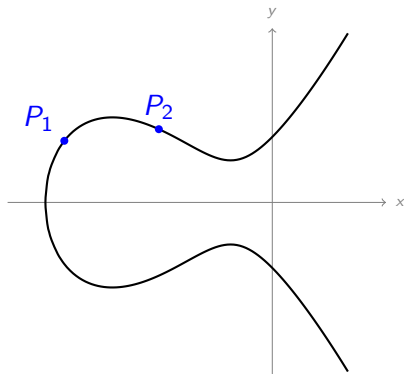
Die Jacobi-Varietät induziert eine **effizient berechenbare Gruppenstruktur** auf der elliptischen Kurve.

Rechnen auf elliptische Kurven

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

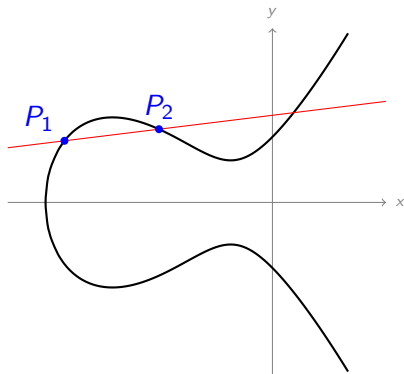
Rechnen auf elliptische Kurven

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



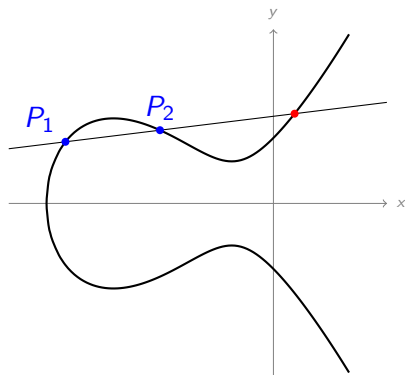
Rechnen auf elliptische Kurven

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



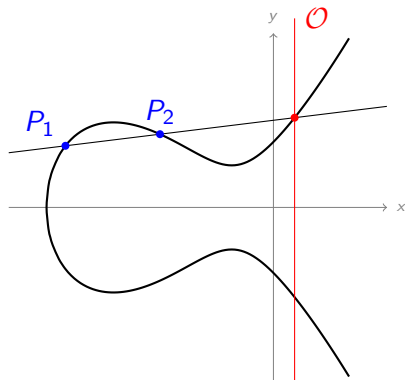
Rechnen auf elliptische Kurven

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



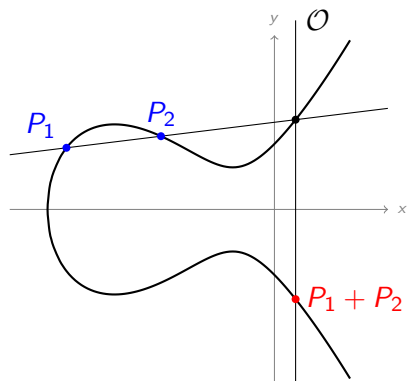
Rechnen auf elliptische Kurven

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



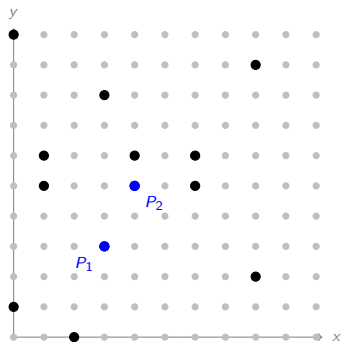
Rechnen auf elliptische Kurven

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



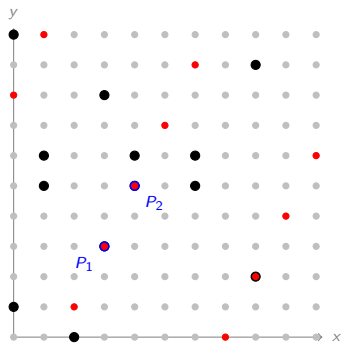
Rechnen auf elliptische Kurven

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



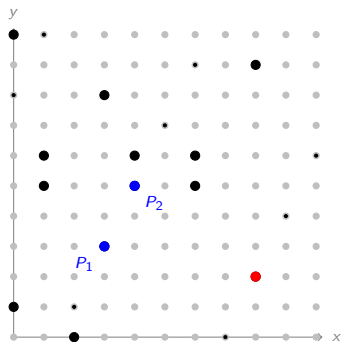
Rechnen auf elliptische Kurven

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



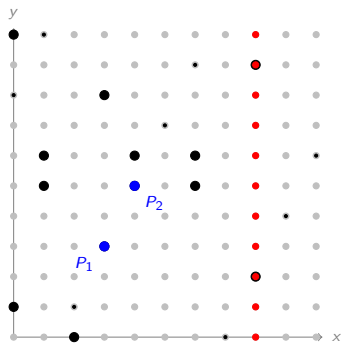
Rechnen auf elliptische Kurven

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



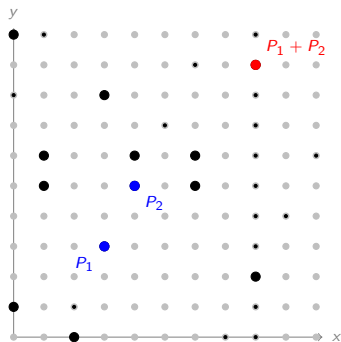
Rechnen auf elliptische Kurven

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



Rechnen auf elliptische Kurven

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



Rechnen auf elliptische Kurven

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

Rechnen auf elliptische Kurven

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

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

$$x_3 = \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2$$

$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3$$

Elliptic Curve Cryptography

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

domain parameters: E/\mathbb{F}_q , $P \in E(\mathbb{F}_q)$ und $n = \text{ord } P$

Elliptic Curve Diffie-Hellman

domain parameters: E/\mathbb{F}_q , $P \in E(\mathbb{F}_q)$ und $n = \text{ord } P$

Alice

$$d_A \in [0, n - 1]$$

Bob

$$d_B \in [0, n - 1]$$

Elliptic Curve Diffie-Hellman

domain parameters: E/\mathbb{F}_q , $P \in E(\mathbb{F}_q)$ und $n = \text{ord } P$

Alice

$$d_A \in [0, n-1]$$

$$Q_A = [d_A]P$$

Bob

$$d_B \in [0, n-1]$$

$$Q_B = [d_B]P$$

Elliptic Curve Diffie-Hellman

domain parameters: E/\mathbb{F}_q , $P \in E(\mathbb{F}_q)$ und $n = \text{ord } P$

Alice	Bob
$d_A \in [0, n - 1]$	$d_B \in [0, n - 1]$
$Q_A = [d_A]P$	$Q_B = [d_B]P$

$\begin{matrix} \xrightarrow{Q_A} \\ \xleftarrow{Q_B} \end{matrix}$

Elliptic Curve Diffie-Hellman

domain parameters: E/\mathbb{F}_q , $P \in E(\mathbb{F}_q)$ und $n = \text{ord } P$

Alice	Bob
$d_A \in [0, n - 1]$	$d_B \in [0, n - 1]$
$Q_A = [d_A]P$	$Q_B = [d_B]P$
	$\xrightarrow{Q_A}$
	$\xleftarrow{Q_B}$
$K_A = [d_A]Q_B$	$K_B = [d_B]Q_A$

Elliptic Curve Diffie-Hellman

domain parameters: E/\mathbb{F}_q , $P \in E(\mathbb{F}_q)$ und $n = \text{ord } P$

Alice		Bob
$d_A \in [0, n - 1]$		$d_B \in [0, n - 1]$
$Q_A = [d_A]P$		$Q_B = [d_B]P$
	$\begin{array}{c} \xrightarrow{Q_A} \\ \xleftarrow{Q_B} \end{array}$	
$K_A = [d_A]Q_B$		$K_B = [d_B]Q_A$

$$K_A = [d_A]Q_B = [d_A][d_B]P = [d_B][d_A]P = [d_B]Q_A = K_B$$

gemeinsamer Schlüssel: $x(K_A) = x(K_B)$.

Noch ein Problem.

Wie groß ist $E(\mathbb{F}_q)$?

Wie groß ist $E(\mathbb{F}_q)$?

Etwas Theorie...

E/K eine elliptische Kurve, ℓ eine Primzahl ($\ell \neq \text{char}(K)$)

$$E[\ell] = \{P \in E(\bar{K}) : [\ell]P = \mathcal{O}\}.$$

E/K eine elliptische Kurve, ℓ eine Primzahl ($\ell \neq \text{char}(K)$)

$$E[\ell] = \{P \in E(\bar{K}) : [\ell]P = \mathcal{O}\}.$$

Definition (Tate Modul)

$$T_\ell(E) = \varprojlim_n E[\ell^n]$$

Tate Modul

E/K eine elliptische Kurve, ℓ eine Primzahl ($\ell \neq \text{char}(K)$)

$$E[\ell] = \{P \in E(\bar{K}) : [\ell]P = \mathcal{O}\}.$$

Definition (Tate Modul)

$$T_\ell(E) = \varprojlim_n E[\ell^n]$$

Theorem

$$T_\ell(E) \cong (\mathbb{Z}_\ell)^2 \text{ als } \mathbb{Z}_\ell\text{-Modul}$$

Theorem

Sei $\phi: E \rightarrow E$ ein **Endomorphismus**. Dann induziert ϕ eine kanonische \mathbb{Z}_ℓ -lineare Abbildung $T_\ell(E) \rightarrow T_\ell(E)$, also eine **Matrix** aus $\mathbb{Z}_\ell^{2 \times 2}$.

Die **Spur** dieser Matrix ist unabhängig von ℓ und wird mit $\text{tr } \phi$ bezeichnet.

Frobenius-Abbildungen

Aus der Theorie endlicher Körper: Die Abbildung

$$\begin{aligned}\phi_q: \mathbb{F}_q &\rightarrow \mathbb{F}_q \\ x &\mapsto x^q\end{aligned}$$

ist ein Isomorphismus.

Frobenius-Abbildungen

Aus der Theorie endlicher Körper: Die Abbildung

$$\begin{aligned}\phi_q: \mathbb{F}_q &\rightarrow \mathbb{F}_q \\ x &\mapsto x^q\end{aligned}$$

ist ein Isomorphismus.

Proposition

Sei E/\mathbb{F}_q eine elliptische Kurve. Die Abbildung

$$\begin{aligned}\phi_q: E &\rightarrow E \\ (x, y) &\mapsto (x^q, y^q)\end{aligned}$$

ist ein Endomorphismus von E .

Die Spur des Frobenius

ϕ_q induziert eine lineare Abbildung

$$(\mathbb{Z}_\ell)^2 \rightarrow (\mathbb{Z}_\ell)^2.$$

Die Spur dieser Abbildung wird mit $\text{tr } \phi_q$ bezeichnet.

Die Spur des Frobenius

ϕ_q induziert eine lineare Abbildung

$$(\mathbb{Z}_\ell)^2 \rightarrow (\mathbb{Z}_\ell)^2.$$

Die Spur dieser Abbildung wird mit $\text{tr } \phi_q$ bezeichnet.

Theorem

$$\text{tr } \phi_q \in \mathbb{Z}$$

Die Spur des Frobenius

ϕ_q induziert eine lineare Abbildung

$$(\mathbb{Z}_\ell)^2 \rightarrow (\mathbb{Z}_\ell)^2.$$

Die Spur dieser Abbildung wird mit $\text{tr } \phi_q$ bezeichnet.

Theorem

$$\text{tr } \phi_q \in \mathbb{Z}$$

$$\#E(\mathbb{F}_q) = q + 1 - \text{tr } \phi_q$$

- Satz von Hasse:

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

Die Spur des Frobenius: Korollare

- Satz von Hasse:

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

- **Weil Vermutungen** (für elliptische Kurven):

$$\exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n}\right) = \frac{1 - \text{tr } \phi_q T + qT^2}{(1 - T)(1 - qT)}.$$

Die Spur des Frobenius: Korollare

- Satz von Hasse:

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

- Weil Vermutungen (für elliptische Kurven):

$$\exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n}\right) = \frac{1 - \text{tr } \phi_q T + qT^2}{(1 - T)(1 - qT)}.$$

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

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

- Naive Methoden

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

- Naive Methoden
- **Schoofs Algorithmus**
 - Berechne $\text{tr } \phi_q \bmod \ell$ 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 $\text{tr } \phi_q \bmod \ell$ 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 um $\text{tr } \phi_q$ zu berechnen.

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

- Generische Algorithmen: $O(\sqrt{n})$.

Diskreter Logarithmus: Klassische Algorithmen

- Generische Algorithmen: $O(\sqrt{n})$.
- Index Calculus auf elliptischen Kurven nicht anwendbar.

Diskreter Logarithmus: Algorithmen für elliptische Kurven

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

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

- **MOV/FR attack:** $E[n] \rightarrow \mu_n(\bar{\mathbb{F}}_q) \subseteq \mathbb{F}_{q^k}$.
 k meist sehr groß; bei supersingulären Kurven ≤ 6 .

Diskreter Logarithmus: Algorithmen für elliptische Kurven

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

- MOV/FR attack: $E[n] \rightarrow \mu_n(\bar{\mathbb{F}}_q) \subseteq \mathbb{F}_{q^k}$.
 k meist sehr groß; bei supersingulären Kurven ≤ 6 .
- **Anomale Kurven:** $E[n] \rightarrow \mathbb{F}_q^+$.

Diskreter Logarithmus: Algorithmen für elliptische Kurven

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

- MOV/FR attack: $E[n] \rightarrow \mu_n(\bar{\mathbb{F}}_q) \subseteq \mathbb{F}_{q^k}$.
 k meist sehr groß; bei supersingulären Kurven ≤ 6 .
- Anomale Kurven: $E[n] \rightarrow \mathbb{F}_q^+$.
- **Weil Descent**: Isomorphismus zu einer Varietät über einem kleineren Körper, aber mit höherer Dimension.

- Algebraische Geometrie in der Kryptographie. (Hilfe!)

Zusammenfassung: ECC

- Algebraische Geometrie in der Kryptographie. (Hilfe!)
- Aber: ECC liefert höhere Sicherheit bei kleinerer Schlüsselgröße.

Zusammenfassung: ECC

- Algebraische Geometrie in der Kryptographie. (Hilfe!)
- Aber: ECC liefert höhere Sicherheit bei kleinerer Schlüsselgröße.

Zusammenfassung: ECC

- Algebraische Geometrie in der Kryptographie. (Hilfe!)
- Aber: ECC liefert höhere Sicherheit bei kleinerer Schlüsselgröße.

Zusammenfassung: ECC

- Algebraische Geometrie in der Kryptographie. (Hilfe!)
- Aber: ECC liefert höhere Sicherheit bei kleinerer Schlüsselgröße.