Institut für Informatik
Seminar Kryptographie
SoSe 2005

Präsentation
Ingo Grebe

1. Einleitung

2. Elliptische Kurven über reellen Zahlen

3. Elliptische Kurven über Körpern

4. Public-Key Verfahren

5. Elliptische Kurven im Allgemeinen

6. Vergleich ECC RSA

7. Schlussbetrachtung

8. Literaturverzeichnis

Elliptische Kurven

in der Kryptographie

Institut für Informatik
Seminar Kryptographie
SoSe 2005

Präsentation
Ingo Grebe

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Gliederung

- Einleitung
- Elliptische Kurven über reellen Zahlen
- Elliptische Kurven über Körper
- Public-Key Verfahren mittels elliptischer Kurven
- Elliptische Kurven im Allgemeinen
- Vergleich ECC und RSA
- Schlussbetrachtung
- Literaturverzeichnis

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Elliptische Kurven in der Kryptographie (ECC)

Im Jahre 1986 gelang es Neal Koblitz und Victor Miller unabhängig von einander, **elliptische Kurven** im Bereich der **Public Key Kryptographie** einzusetzen.

Mit **elliptischen Kurven** lassen sich **asymmetrische** Krypto-Verfahren realisieren.

„Im Herzen von **ECC** steht die Tatsache, dass man auf einer **elliptischen Kurve** eine **abelsche Gruppe** definieren kann und dass in dieser Gruppe das **diskrete Logarithmus Problem** extrem schwer zu lösen ist.“

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

ECC in Standards

- **IEEE [P1363] (Institute of Electrical and Electronics Engineers)**
  - **Public-Key Verfahren**
  - **geeignete Parameter**
  - **Schlüsselerzeugung, Schlüsselaustausch**
- **FIPS [186-2] (Federal Information Processing Standard)**
  - **NIST (National Institute of Standards and Technologie)**
  - **ECDSA Signaturverfahren**
- **Standards der IETF (Internet Engineering Task Force)**
  - SSL/TLS, IPSEC, PKIX, S/MIME, WAP-Protokoll

Institut für Informatik
Seminar Kryptographie
SoSe 2005

Präsentation
Ingo Grebe

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

ECC in der Praxis

Smartcards

- enthält privaten Schlüssel
- beschränkter Speicherplatz
- RSA benötigt >1024 Bit, ECC benötigt 160 Bit
- ECC ist schneller beim signieren

Kryptographie-Plugin „cv act s/mail“

- entwickelt von Cryptovision
- eingesetzt vom Bundesamt für Wehrtechnik und Beschaffung
- Plugin für eMail-Clients
  - Verschlüsselung
  - digitale Signatur
  - kompatibel zu IBM Lotus Notes, Novel GroupWise, Microsoft Outlook

Universität Potsdam
Institut für Informatik
Seminar Kryptographie
SoSe 2005

Präsentation
Ingo Grebe

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

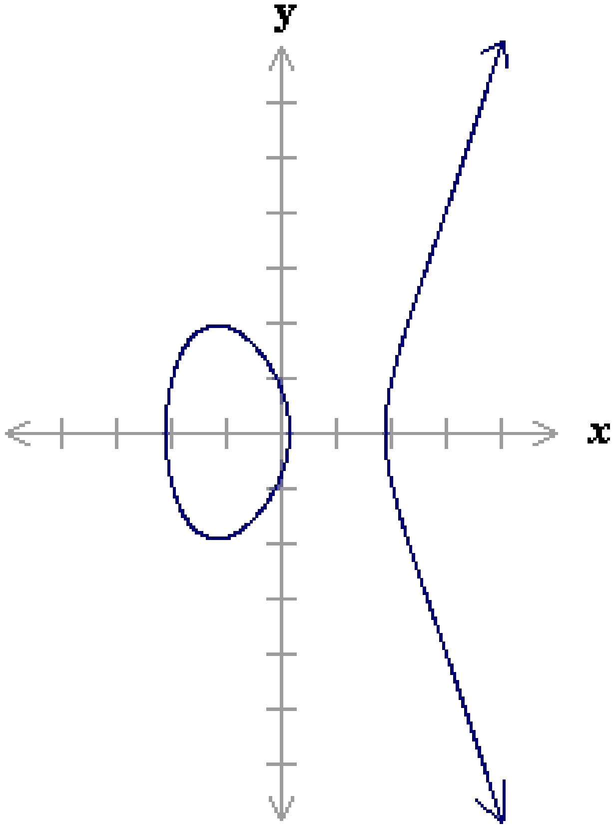
Elliptische Kurven über reellen Zahlen

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

$a = -4$

$b = 0.67$

$y^2 = x^3 - 4x + 0.67$



1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Abelsche Gruppe $[y^2 = x^3 + ax + b]$

Bedingung: $4a^3 + 27b^2 \neq 0$

Gleichung: $y^2 = x^3 + ax + b$

Punkt **O**, der Punkt im „unendlichen“

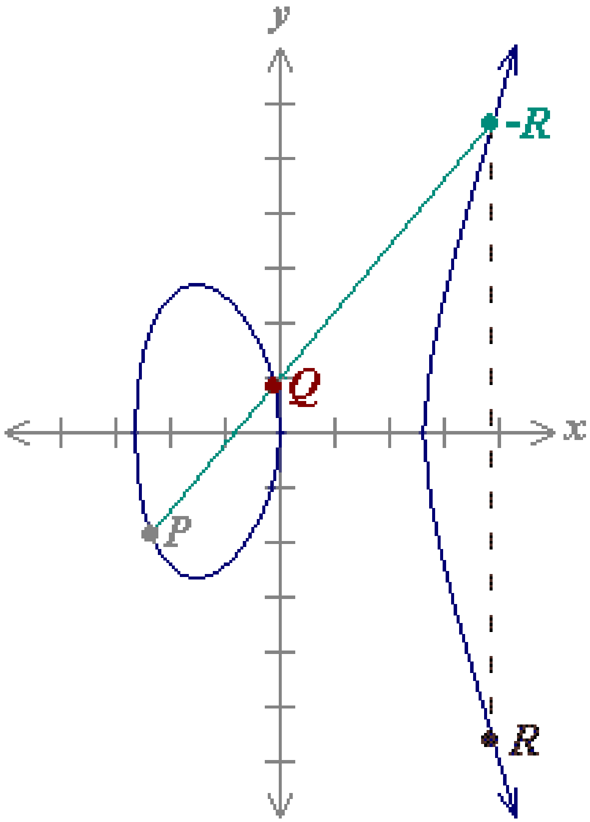
$P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, $R = (x_R, y_R)$

- Operation: **+** mit $P + Q = R$
  - Assoziativität: $P + (Q + R) = (P + Q) + R$
  - Kommutativität: $P + Q = Q + P$
- neutrales Element: **O** mit $P + O = O + P = P$
- Inverses Element: **(x,-y)** mit $P + -P = -P + P = O$

Geometrische Betrachtung $[y^2 = x^3 + ax + b]$

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

$P + Q = R, \quad P \neq Q$



$y^2 = x^3 - 7x$

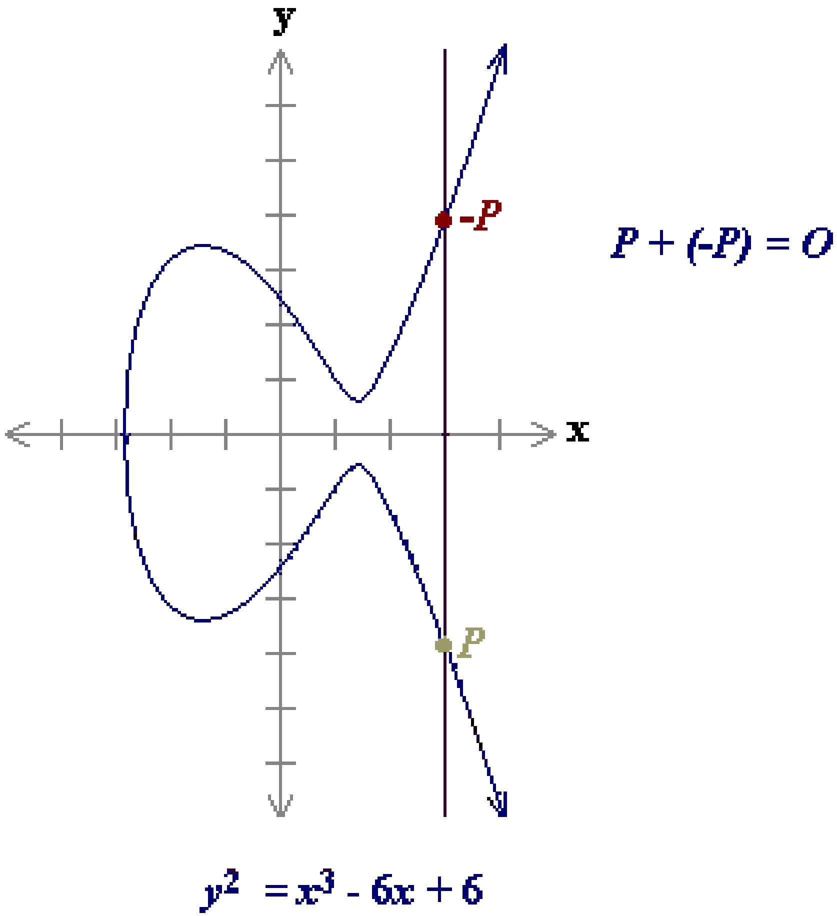
P (-2.35, -1.86)
Q (-0.1, 0.836)
$-R$ (3.89, 5.62)
R (3.89, -5.62)

$P + Q = R = (3.89, -5.62)$.

Geometrische Betrachtung $[y^2 = x^3 + ax + b]$

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

P + -P = O

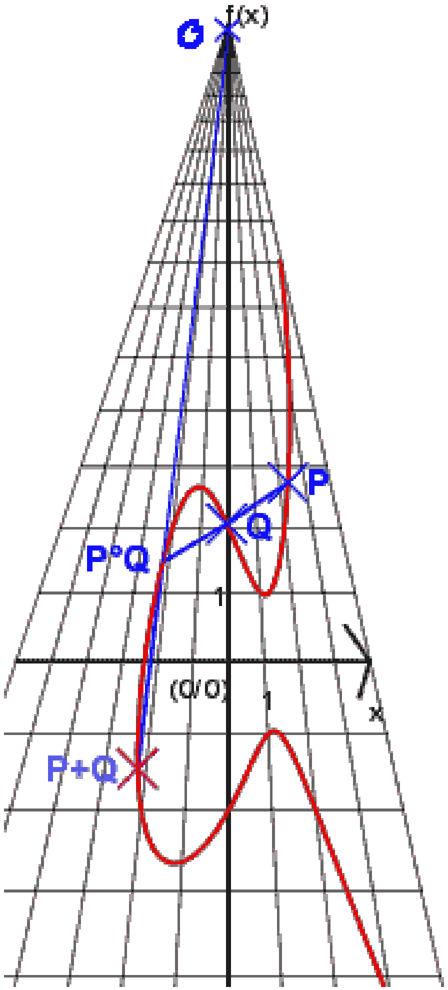


O wird auch der „Punkt im Unendlichen“ genannt

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Geometrische Betrachtung $[y^2 = x^3 + ax + b]$

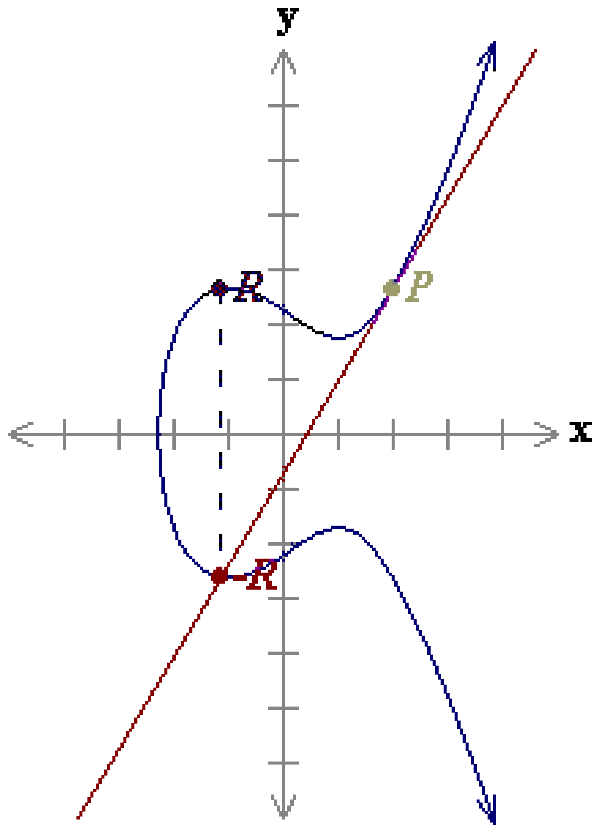
O wir auch der „Punkt im Unendlichen“ genannt



1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Geometrische Betrachtung [$y^2 = x^3 + ax + b$]

P + P = 2P = R



P (2, 2.65)

$-R$ (-1.11, -2.64)

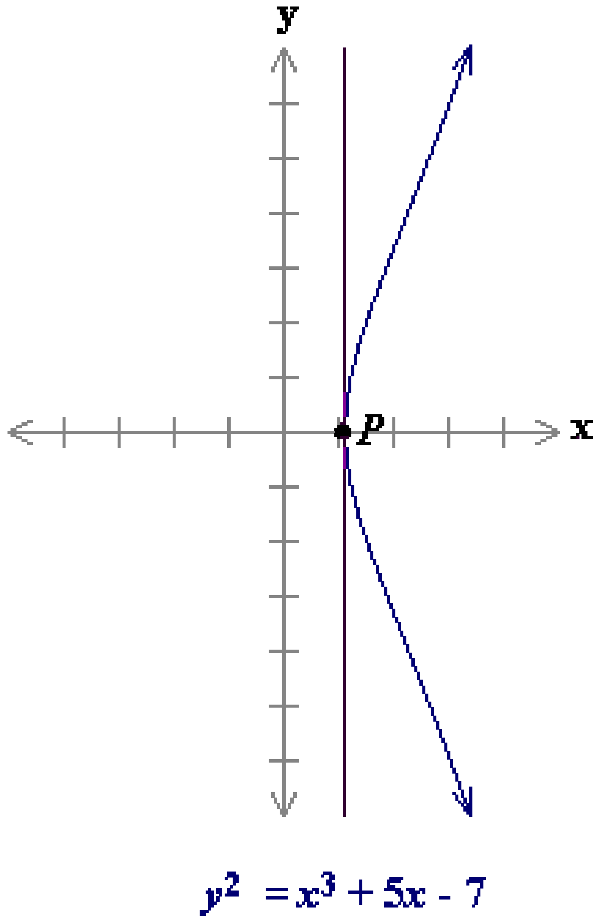
R (-1.11, 2.64)

$2P = R = (-1.11, 2.64)$.

$y^2 = x^3 - 3x + 5$

Geometrische Betrachtung $[y^2 = x^3 + ax + b]$

$P + P = 2P = R,\ y_p = 0$



P+O=P, 2P=P, 3P=2P+P=O+P=P, 4P=O, …

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

1. Einleitung

2. Elliptische Kurven über reellen Zahlen

3. Elliptische Kurven über Körpern

4. Public-Key Verfahren

5. Elliptische Kurven im Allgemeinen

6. Vergleich ECC RSA

7. Schlussbetrachtung

8. Literaturverzeichnis

Algebraische Betrachtung $[y^2 = x^3 + ax + b]$

$P + Q = R$, $P=(x_P,y_P)$, $Q=(x_Q,y_Q)$, $R=(x_R,y_R)$, $P \neq Q$

$s = (y_P - y_Q) / (x_P - x_Q)$

$x_R = s^2 - x_P - x_Q$

$y_R = -y_P + s\cdot(x_P - x_R)$

s: Steigung der Geraden durch P und Q

$P + P = 2P = R$, $P=(x_P,y_P)$, $R=(x_R,y_R)$, $y_P \neq 0$

$s = (3x_P^2 + a) / (2y_P)$

$x_R = s^2 - 2x_P$

$y_R = -y_P + s\cdot(x_P - x_R)$

s: Tangente am Punkt P

a: Parameter der Kurve

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Beispiele

1. Definiert die Gleichung $y^2 = x^3 - 7x - 6$ eine Elliptische Kurve?

   Ja! $4a^3 + 27b^2 = 4\cdot(-7)^3 + 27\cdot(-6)^2 = -400 \neq 0$

2. Ist P=(4,7) ein Punkt auf der Elliptischen Kurve $y^2 = x^3 - 5x + 5$?

   Ja! $7^2 = 4^3 - 5\cdot 4 + 5$

   $49 = 64 - 20 + 5$

   $49 = 49$

- Berechne P+Q=R für P=(0,-4) und Q=(1,0) auf $y^2 = x^3 - 17x + 16$!

  $s = (y_P - y_Q) / (x_P - x_Q) = (-4 - 0) / (0 - 1) = 4$

  $x_R = s^2 - x_P - x_Q = 4^2 - 0 - 1 = 15$

  $y_R = -y_P + s\cdot(x_P - x_R) = -(-4) + 4\cdot(0 - 15) = -56$

  $\Rightarrow P + Q = R = (15,-56)$

- Berechne 2P=R für P=(4,√20) auf $y^2 = x^3 - 17x + 16$!

  $s = (3x_P^2 + a) / (2y_P) = (3\cdot 4^2 + (-17)) / (2\cdot\sqrt{20}) = 4.475$

  $x_R = s^2 - 2x_P = 4.475^2 - 2\cdot 4 = 12.022$

  $y_R = -y_P + s\cdot(x_P - x_R) = -(\sqrt{20}) + 4.475\cdot(4 - 12.022) = -39{,}362$

  $\Rightarrow 2P = R = (12.022,-39.362)$

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Elliptische Kurven über dem Körper F_P

Wichtig für Kryptographie

- **endliche Gruppe (Diskreter Logarithmus)**
- **schnelle** und **präzise** Berechnungen

Elliptische Kurven über reellen Zahlen haben keine endliche Anzahl an Punkten, sind langsam in ihrer Berechnung und es treten Rundungsfehler auf.

Primzahlkörper F_P

- **p-1 Elemente, p ist Primzahl**
- **keine Rundungsfehler**
- $y^2 \bmod p = x^3 + ax + b \bmod p$, $a,b \in F_P$
- $4a^3 + 27b^2 \bmod p \neq 0$

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Beispiel $[y^2 = x^3 + x]$ über F_{23}

Körper F_{23}, $y^2 = x^3 + x$, $P = (9,5)$

$$y^2 \bmod p = x^3 + x \bmod p$$

$$25 \bmod 23 = 729 + 9 \bmod 23$$

$$2 = 2$$

$\Rightarrow$ Punkt $P=(9,5)$ erfüllt $y^2 = x^3 + x$

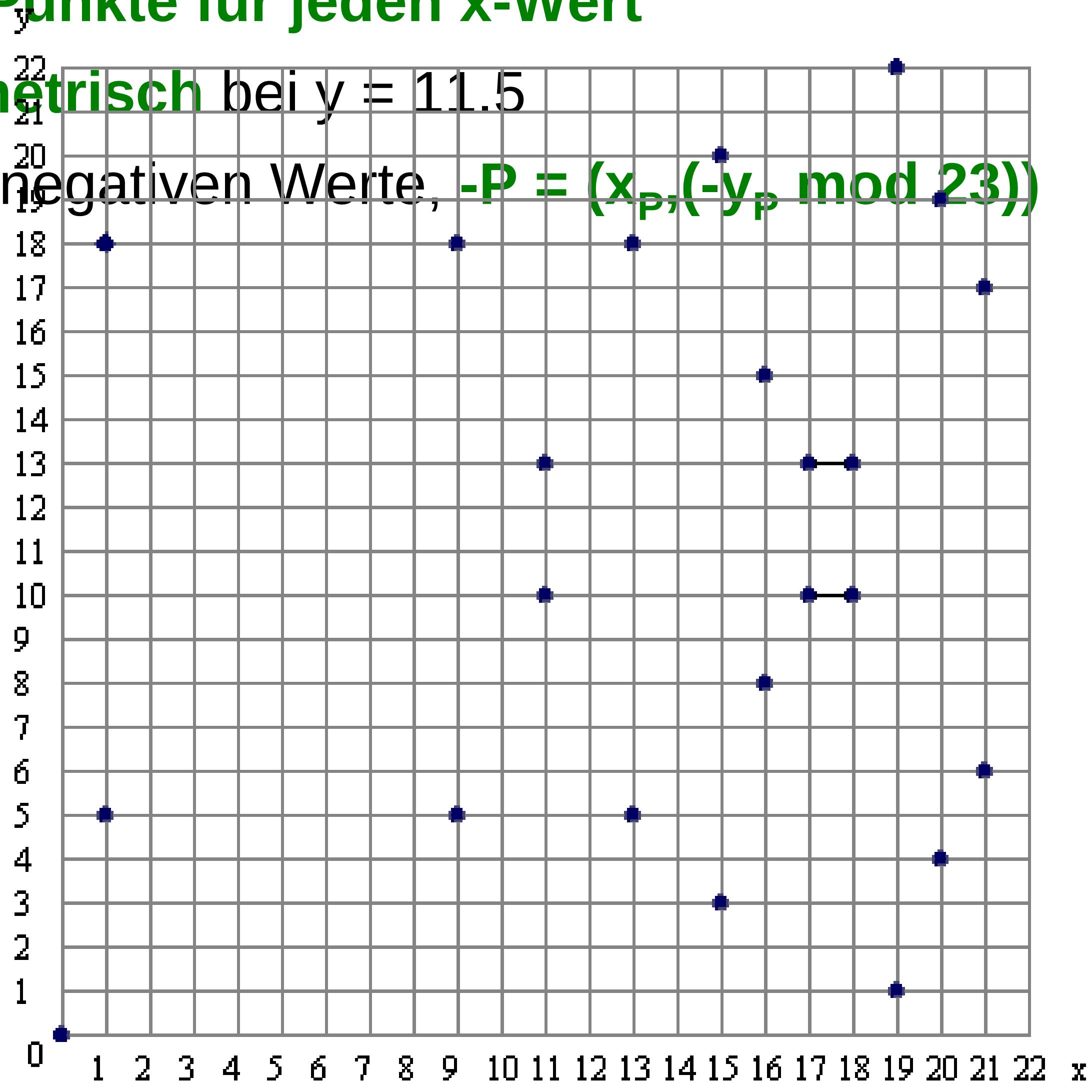
Es gibt insgesamt 23 Punkte auf der Kurve $y^2 = x^3 + x$:

(0,0)	(1,5)	(1,18)	(9,5)	(9,18)	(11,10)	(11,13)
(13,5)	(13,18)	(15,3)	(15,20)	(16,8)	(16,15)	(17,10)
(17,13)	(18,10)	(18,13)	(19,1)	(19,22)	(20,4)	(20,19)
(21,6)	(21,17)					

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Beispiel $[y^2 = x^3 + x]$ über F_{23}

- zwei Punkte für jeden x-Wert
- symmetrisch bei y = 11.5
- keine negativen Werte, $-P = (x_P, (-y_P \bmod 23))$



1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Algebraische Betrachtung $[y^2 = x^3 + ax + b]$ über F_P

$P + Q = R$, $P=(x_P,y_P)$, $Q=(x_Q,y_Q)$, $R=(x_R,y_R)$, $P \neq Q$

$s = (y_P - y_Q) / (x_P - x_Q)$ **mod p**

$x_R = s^2 - x_P - x_Q$ **mod p**

$y_R = -y_P + s \cdot (x_P - x_R)$ **mod p**

s: Steigung der Geraden durch P und Q

$P + P = 2P = R$, $P=(x_P,y_P)$, $R=(x_R,y_R)$, $y_P \neq 0$

$s = (3x_P^2 + a) / (2y_P)$ **mod p**

$x_R = s^2 - 2x_P$ **mod p**

$y_R = -y_P + s \cdot (x_P - x_R)$ **mod p**

s: Tangente am Punkt P

a: Parameter der Kurve

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Beispiele

1. Definiert die Gleichung $y^2=x^3+10x+5$ eine Elliptische Kurve über F_{17}?

   Nein! $4a^3 + 27b^2 \bmod p =$

2. Liegt P=(2,0) auf der Elli

   Ja! $0^2 \bmod 17 = 2^3 + 2 + 7 \bmod 17$

   $0 \bmod 17 = 17 \bmod 17$

   $0 = 0$

- Berechne P+Q=R für P=(2,0) und Q=(1,3) auf $y^2= x^3+x+7$ über F_{17}!

  $s = (y_P - y_Q) / (x_P - x_Q) \bmod p =$

  $x_R = s^2 - x_P - x_Q \bmod p =$

  $y_R = -y_P + s\cdot(x_P - x_R) \bmod$

  $\Rightarrow P + Q = R = (6,12)$

- Berechne 2P=R für P=(1,3) auf $y^2= x^3+x+7$ über F_{17}!

  $s = (3x_P^2 + a) / (2y_P) \bmod p =$

  $x_R = s^2 - 2x_P \bmod p =$

  $y_R = -y_P + s\cdot(x_P - x_R)$

  $\Rightarrow 2P = R = (6,5)$

Elliptische Kurven über dem Körper F_{2^m}

$$y^2 + xy = x^3 + ax^2 + b, \quad b \neq 0$$

- Bit Strings
- Addition mittels XOR-Funktion

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Verwendete Körper

Theoretisch

- jeder endliche Körper kann verwendet werden

Praktisch

- Primzahlkörper F_P mit Primzahl p
- F_{2^m} mit 2^m Elementen

Unterschiede zwischen F_P und F_{2^m}

- bisher noch keine Sicherheitsunterschiede
- F_P hat beim Softwareeinsatz Vorteile
- F_{2^m} hat beim Hardwareeinsatz Vorteile

Diskrete Logarithmus Problem (ECDLP)

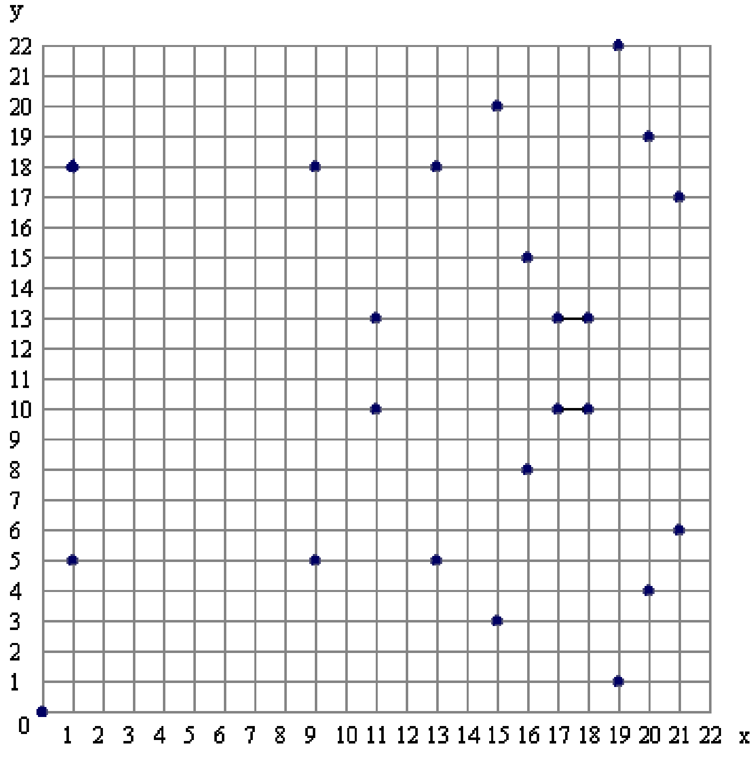
1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. **Public-Key Verfahren**
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Gegeben: zwei Punkte P und Q auf einer elliptischen Kurve über einer Gruppen mit einer ausreichend großen Gruppenordnung

Problem: Bestimme x, so dass Q = xP

$$xP = \underbrace{P+P+\ldots+P}_{\text{x-mal}}$$

Trägt man die Punkte einer elliptischen Kurve in ein Gitter ein, so erhält man eine „Punktwolke“. Die Addition von zwei Punkten entspricht dann einem scheinbar zufälligen Springen von Punkt zu Punkt. Dieses „Chaos“ drückt die Schwierigkeit des diskreten Logarithmusproblems auf einer elliptischen Kurve aus.



Elliptic curve equation: $y^2 = x^3 + x$ over F_{23}

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

ECDH

- einfaches Protokoll für einen Schlüsselaustausch
- basiert auf Diffie-Hellman

Szenario

- Alice und Bob tauschen geheimen Schlüssel aus
- Lauscherin Eve

Vorraussetzungen

- Alice und Bob einigen sich auf gleiche ECC-Parameter
  - **E**: elliptische Kurve
  - **p**: Größe des Körpers F_P
  - **a**,**b**: Koeffizienten der elliptischen Kurve, $a,b \in F_P$
  - **G**: Punkt auf der elliptischen Kurve E
  - **n**: Ordnung des Punktes G, n muss Primzahl sein

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

ECDH - Prinzip

G: Punkt auf der elliptischen Kurve E
n: Ordnung des Punktes G, n ist Primzahl

Alice private Key $\mathbf{x_A}$: Zufallszahl, $1 < x_A < n$
public Key $\mathbf{Q_A}$: Punkt $Q_A = x_A G$

Bob private Key $\mathbf{x_B}$: Zufallszahl, $1 < x_B < n$
public Key $\mathbf{Q_B}$: Punkt $Q_B = x_B G$

geheimer Schlüssel $\mathbf{R} = R_A = R_B$

Alice holt sich Q_B Alice berechnet $R_A = x_A Q_B$
Bob holt sich Q_A Bob berechnet $R_B = x_B Q_A$.

$$\Rightarrow R_A = x_A Q_B = x_A x_B G = x_B x_A G = x_B Q_A = R_B$$

Eine Lauscherin Eve steht vor dem Problem aus G, Q_A und Q_B den Schlüssel R zu berechnen (≈ECDLP).

„Man in the Middle“-Attacke ist immer noch möglich.

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Elliptische Kurven allgemein

Polynom

$$F(x,y) := x^3 - a_1xy + a_2x^2 - a_3y + a_4x + a_6 - y^2$$

Eine elliptische Kurve **E** über einem Körper **K** ist eine **nicht-singuläre** Kurve, definiert als Menge aller Punkte (x,y), mit $x,y \in K$, für die gilt **F(x,y)=0** zusammen mit dem „Punkt in der Unendlichkeit" **O**.

elliptische Kurve (Weierstraßgleichung in Normalform)

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

nicht-singulär

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Polynom

$$F(x,y) := x^3 - a_1xy + a_2x^2 - a_3y + a_4x + a_6 - y^2$$

elliptische Kurve (Weierstraßgleichung in Normalform)

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

E(K) ist nicht-singulär

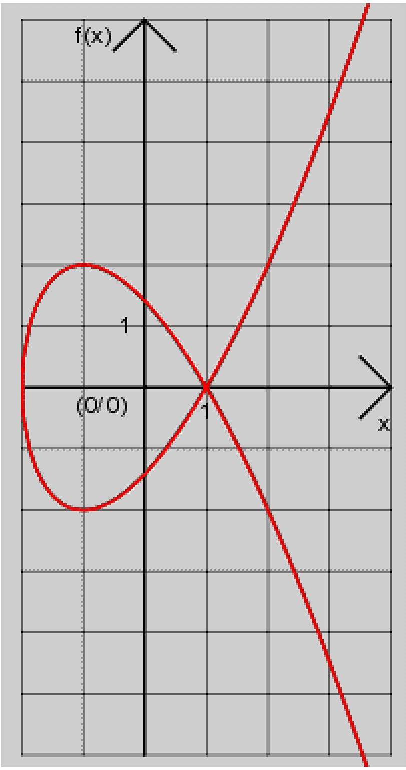
- keine Knoten, Spitzen oder Einsiedler

$$\Leftrightarrow \quad \frac{\partial F}{\partial x}(a,b) \neq 0 \quad \vee \quad \frac{\partial F}{\partial y}(a,b) \neq 0 \quad \text{mit } P(a,b) \in E$$

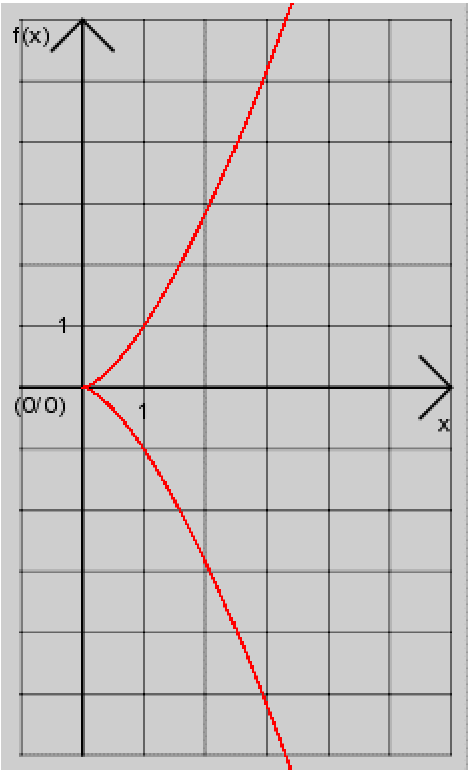
1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

E(K) ist nicht-singulär

- keine Knoten, Spitzen oder Einsiedler



E(K): $y^2 = x^3 - 3x + 2$



E(K): $y^2 = x^3$

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

nicht-singulär

char(K) = m

falls es eine kleinste natürliche Zahl *m* gibt, so dass

$$m1 = \underbrace{1+1+\ldots+1}_{\text{m-mal}} = 0$$

char(K) ≠ 2, 3

$$\boxed{E(K): y^2 = x^3 + ax + b}$$

E(K) ist nicht-singulär

beide Ableitungen ≠ 0 ⇔ Diskriminante von E ≠ 0

$$\frac{\partial F}{\partial x}(a,b) = -3x^2 - a_4 \neq 0 \quad \vee \quad \frac{\partial F}{\partial y}(a,b) = 2y \neq 0$$

$$\Downarrow$$

$$4a^3 + 27b^2 \neq 0, \quad \text{mit } a,b \in K$$

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

nicht-singulär

E(K) ist nicht-singulär

beide Ableitungen $\neq 0$ $\Leftrightarrow$ Diskriminante von E $\neq 0$

$$\frac{\partial F}{\partial x}(a,b) = -3x^2 - a \neq 0 \quad \vee \quad \frac{\partial F}{\partial y}(a,b) = 2y \neq 0$$

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

nicht-singulär

E(K) ist nicht-singulär

beide Ableitungen $\neq 0$ $\Leftrightarrow$ Diskriminante von E $\neq 0$

$$\frac{\partial F}{\partial x}(a,b) = -3x^2 - a \neq 0 \quad \vee \quad \frac{\partial F}{\partial y}(a,b) = 2y \neq 0$$

$$y^2 = x^3 + ax + b \quad \text{mit} \quad y = 0, \quad x = \pm\sqrt{-\frac{a}{3}}, \text{ für } a \leq 0$$

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

nicht-singulär

E(K) ist nicht-singulär

beide Ableitungen $\neq 0$ $\Leftrightarrow$ Diskriminante von E $\neq 0$

$$\frac{\partial F}{\partial x}(a,b) = -3x^2 - a \neq 0 \quad \vee \quad \frac{\partial F}{\partial y}(a,b) = 2y \neq 0$$

$$\Rightarrow \left(\sqrt{-\frac{a}{3}}\right)^3 + a\sqrt{-\frac{a}{3}} + b = 0$$

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

nicht-singulär

E(K) ist nicht-singulär

beide Ableitungen $\neq 0$ $\Leftrightarrow$ Diskriminante von E $\neq 0$

$$\frac{\partial F}{\partial x}(a,b) = -3x^2 - a \neq 0 \quad \vee \quad \frac{\partial F}{\partial y}(a,b) = 2y \neq 0$$

$$\Rightarrow -a\sqrt{-\frac{a}{3}} + 3a\sqrt{-\frac{a}{3}} + 3b = 0$$

Institut für Informatik
Seminar Kryptographie
SoSe 2005

Präsentation
Ingo Grebe

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

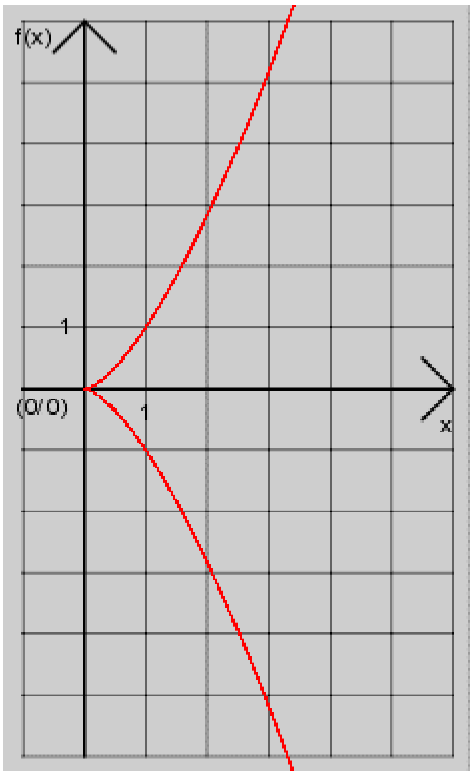
Beispiel

$P + Q = R, \ P=(x_P,y_P), \ Q=(x_Q,y_Q), \ R=(x_R,y_R), \ P \neq Q$

$s = (y_P - y_Q) / (x_P - x_Q)$

$xR = s^2 - x_P - x_Q$

$yR = -y_P + s\cdot(x_P - x_R)$



$E(K)$: $y^2 = x^3$

$P=(0,0), \ Q=(1,1), \ R=(x_R,y_R)$

$s = (0 - 1) / (0 - 1) = 1$

$x_R = 12 - 0 - 1 = 0$

$y_R = 0 + 0 - 0 = 0$

$P + Q = R = (0,0) = P$

$4a^3+27b^2 \neq 0, \ a,b \in K$

$4\cdot0^3 + 27\cdot0^2 = 0$

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Ordnung $\#E(F_P)$

Die Anzahl der Punkte einer elliptischen Kurve $E(F_P)$ heißt auch Ordnung $\#E(F_P)$.

Hasse-Schranke

- es gibt keine allgemeingültige Formel für $\#E(F_P)$
- Abschätzung mittels Theorem von Hasse

$$-2\sqrt{p} + p + 1 \leq \#E(F_P) \leq 2\sqrt{p} + p + 1$$

Beispiel

$$-2\sqrt{23} + 23 + 1 \leq \#E(F_{23}) \leq 2\sqrt{23} + 23 + 1$$

$$-2\cdot 4{,}795 + 24 \leq \#E(F_{23}) \leq 2\cdot 4{,}795 + 23 + 1$$

$$\approx 14 \leq \#E(F_{23}) \leq 33$$

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Untergruppen von $E(F_P)$

Untergruppe U_P

$U_P := \{kP \mid k \in Z\}$

ist die von P erzeugte zyklische Untergruppe von $E(F_P)$.

P ist Generator der Gruppe.

Ordnung von U_P

$$k_0 P = \underbrace{P + P + \ldots + P}_{k_0\text{-mal}} = O, \quad \text{mit } k_0 > 0$$

Da P Generator der Gruppe ist, spricht man auch von der Ordnung des Punktes P.

Wahl der elliptischen Kurve

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. **Elliptische Kurven im Allgemeinen**
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

- Kurven aus Standards
- eigene Kurven generieren

wichtigster Aspekt

- große Ordnung *n* der Punktegruppe
- in der Praxis ist *n* zumeist eine 160-Bit große Primzahl

  160-Bit = $2^{160} \approx 1{,}46 \cdot 10^{48}$

Testen

- Bestimmung der Kurvenordnung (Schoofs Algorithmus)

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Klassen schwacher Kurven

Geringe Ordnung der Kurve

Pohlig und Hellman haben gezeigt, wie das ECDLP in diesem Fall in kleinere Probleme unterteilt werden kann.

Gegenmittel: Kurve und einen Basispunkt benutzt, so dass die von diesem Punkt erzeugte Untergruppe von großer Primzahlordnung ist.

Anomale Kurven

- $\#E(F_P) = p$

Smart, Semaev, Satoh und Araki haben gezeigt, dass für diese Kurven ein Algorithmus mit linearer Laufzeit für das ECDLP existiert.

Super-singuläre Kurven

- ord(K) – #E(K) | char(K)

Menezes, Okamoto und Vanstone gezeigt, wie man das ECDLP auf das einfache DLP in Erweiterungskörpern von Z_P reduzieren kann. Es lässt sich aber sehr leicht feststellen, ob eine bestimmte Kurve super-singulär ist und sich dieser Angriff somit vermeiden.

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Andere Klassen spezieller Kurven

Jede Art von Kurve, die auf irgendeine Weise speziell ist, sollte gemieden werden, auch wenn bisher noch kein besonders effizienter Angriff entdeckt worden ist.

Zu dieser Klasse von Kurven gehören z.B. die Koblitz-Kurven über F_{2^m}, deren Kurvengleichungen nur die Koeffizienten „0“ und „1“ enthalten. Diese Kurven sind besonders interessant, da es für sie hoch effiziente Algorithmen für die Punktarithmetik auf ihnen gibt. Jedoch weiß man inzwischen, dass es möglich ist, das Lösen des ECDLP auf ihnen um einen Faktor *m* zu beschleunigen, was aber immer noch zu vernachlässigen ist.

Es gibt Verfahren, die es ermöglichen, Kurven mit einer bestimmten Punktordnung zu erzeugen. Für Kurven, die so erzeugt worden sind, besteht zwar bisher außer den allgemein anwendbaren und extrem langsamen Verfahren noch keine besondere Angriffsmöglichkeit, dennoch bilden sie eine „besondere“ Klasse von Kurven, so dass man solch eine Angriffsmöglichkeit in der Zukunft nicht ausschließen kann.

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Ein kurzer Vergleich zwischen RSA und ECC

Vergleichbare Schlüssellängen

Jahr	Schlüssellänge symmetrischer Verfahren	Asymmetrische Schlüssellänge (z.B. RSA)	Schlüssellängen von ECC	Erforderliche MIPS-Jahre	Erforderliche Jahre auf 450 Mhz PC
2000	70	952	132	$7.13 * 10^{9}$	$1.58 * 10^{7}$
2002	72	1028	137	$2.06 * 10^{10}$	$4.59 * 10^{7}$
2004	73	1108	141	$5.98 * 10^{10}$	$1.33 * 10^{8}$
2006	75	1191	145	$1.73 * 10^{11}$	$3.84 * 10^{8}$
2008	76	1279	149	$5.01 * 10^{11}$	$1.11 * 10^{9}$
2010	78	1369	153	$1.45 * 10^{12}$	$3.22 * 10^{9}$
2012	80	1464	157	$4.19 * 10^{12}$	$9.32 * 10^{9}$
2014	81	1562	162	$1.21 * 10^{13}$	$2.70 * 10^{10}$
2016	83	1664	166	$3.51 * 10^{13}$	$7.81 * 10^{10}$
2018	84	1771	170	$1.02 * 10^{14}$	$2.26 * 10^{11}$
2020	86	1881	175	$2.94 * 10^{14}$	$6.54 * 10^{11}$

Berechnungsaufwand eines privaten Schlüssels in Rechenzeiten für RSA und ECC

ECC ist erheblich schneller als RSA, da die benötigten Schlüssellängen bei gleichem Sicherheitsniveau für ECC deutlich kürzer sind als bei klassischen asymmetrischen Verfahren, wie RSA.

Ein kurzer Vergleich zwischen RSA und ECC

Einsatz des privaten Schlüssels

Dennoch liegt es in der Natur der beiden Systeme, dass ECC vor allem für die Aufgaben, die den Einsatz des privaten Schlüssels bedürfen, also digitales Signieren und Entschlüsseln, i.A. um wenigstens einen Faktor 4 schneller ist.

Bei der Überprüfung einer Signatur oder dem Verschlüsseln ist hingegen RSA um einen ähnlichen Faktor schneller. Dieser Unterschied rührt vor allem daher, dass der öffentliche RSA Exponent meist bewusst so gewählt wird, dass möglichst effektiv gerechnet werden kann, wohingegen der sich daraus ergebende private Exponent keine Geschwindigkeitsvorteile mit sich bringt.

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. Literaturverzeichnis

Schlussbetrachtung

Ziel dieser Folien ist es, einen Überblick über die Kryptographie basierend auf elliptischen Kurven zu geben.

Zu den hier gegebenen mathematische Ausführungen ist zu sagen, das elliptische Kurven und die zugrunde liegende Mathematik nicht annähernd vollständig erklärt worden sind.

So lässt sich beispielsweise der Punkt O in den projektiven Raum einbetten und hat somit auch konkrete Koordinaten und nicht nur die Hilfskonstruktion, die den Punkt im unendlich Fernen der perspektivischen Darstellung erscheinen lässt.

Elliptische Kurven lassen sich nicht nur zur Kryptographie verwenden, sondern es existieren auch Verfahren basieren auf elliptischen Kurven, die zur Faktorisierung oder zum Primzahlnachweis dienen.

Institut für Informatik
Seminar Kryptographie
SoSe 2005

Präsentation
Ingo Grebe

1. Einleitung
2. Elliptische Kurven über reellen Zahlen
3. Elliptische Kurven über Körpern
4. Public-Key Verfahren
5. Elliptische Kurven im Allgemeinen
6. Vergleich ECC RSA
7. Schlussbetrachtung
8. **Literaturverzeichnis**

Literaturverzeichnis

- „Elliptische Kurven in der Kryptographie“
  A. Werner, Springer, 2002
- „Cryptography: Theory and Practice“
  D. Stinson, Chapman&Hall/CRC, 2002
- „ECC Cryptography Tutorial“
  Certicom, http://www.certicom.com
- „ECC – Elliptic Curve Cryptography“
  Cryptovision GmbH, http://www.cryptovision.com
- „Krypto-Verfahren basierend auf elliptischen Kurven “
  T. Laubrock, http://www.laubrock.de, 1999