Einführung in die Elliptic Curve Cryptography

Mathias Schmalisch · Dirk Timmermann

Universität Rostock

Dipl.-Ing. Mathias Schmalisch
mathias.schmalisch@e-technik.uni-rostock.de

Übersicht

- **Elliptische Kurven**
- Punktoperationen
- Körper
- Beispiel
- Zusammenfassung

Dipl.-Ing. Mathias Schmalisch
mathias.schmalisch@e-technik.uni-rostock.de

Elliptische Kurven

- Weierstrass Normalform:

  $E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad x,y,a_i \in K$

- $char(K) \neq 2,3$

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

- $char(K) = 2$

  $E_1: y^2 + xy = x^3 + a_2x^2 + a_6$

  $E_2: y^2 + a_3y = x^3 + a_4x + a_6$

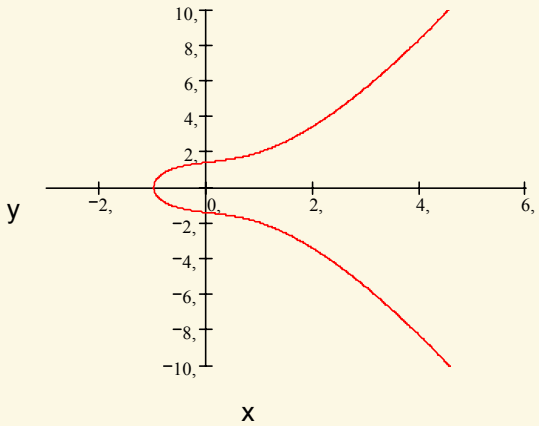
Dipl.-Ing. Mathias Schmalisch
mathias.schmalisch@e-technik.uni-rostock.de

Elliptische Kurven

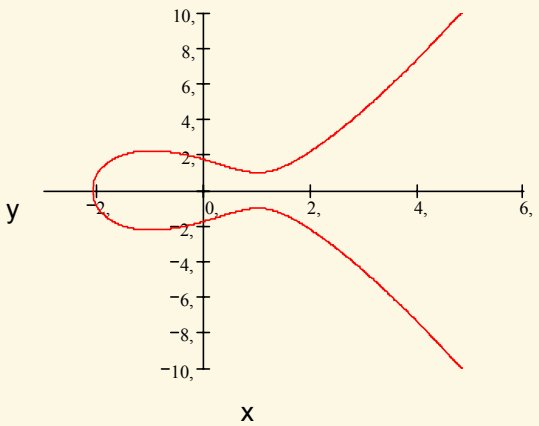
- Kurve E/K, mit K = **R** (reelle Zahlen)

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

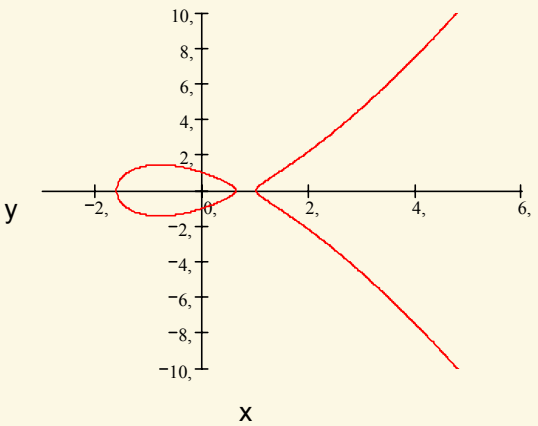
- Koeffizienten a, b müssen ganze Zahlen sein
- Kurven mit einer oder drei Nullstellen



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



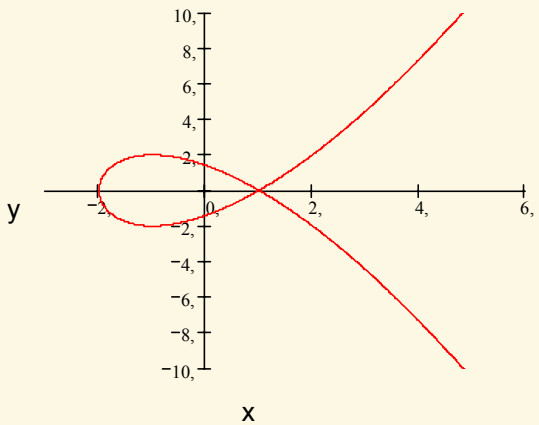
$y^2 = x^3 - 3x + 3$



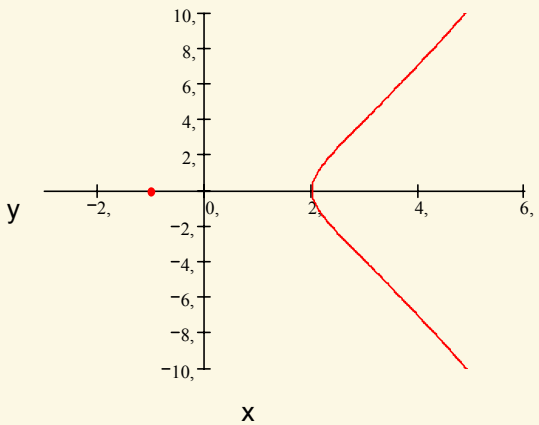
$y^2 = x^3 - 2x + 1$

Elliptische Kurven

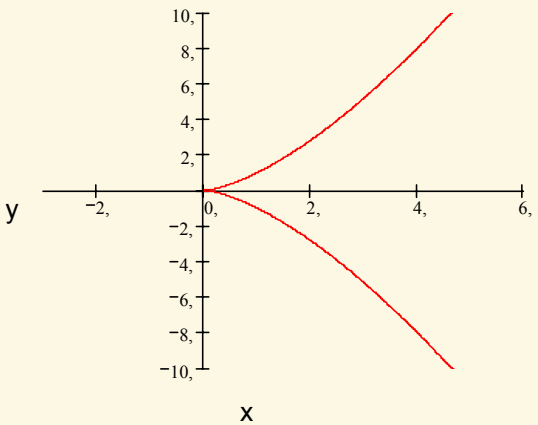
- Kurven mit doppelten Nullstellen
- werden auch singuläre Kurven genannt
- Punktoperationen sind auf diesen Kurven nicht definiert



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



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



$y^2 = x^3$

Diskriminante Δ

- mit der Diskriminante Δ kann eine singuläre Kurve ermittelt werden
- bei singulären Kurven ist $\Delta = 0$
- $\text{char}(K) \neq 2,3$

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

  $\Delta = -16\,(4a_4^3 + 27a_6^2)$

- $\text{char}(K) = 2$

  $E_1: y^2 + xy = x^3 + a_2x^2 + a_6$

  $\Delta = a_6$

  $E_2: y^2 + a_3y = x^3 + a_4x + a_6$

  $\Delta = a_3^4$

Übersicht

- Elliptische Kurven
- **Punktoperationen**
- Körper
- Beispiel
- Zusammenfassung

Dipl.-Ing. Mathias Schmalisch
mathias.schmalisch@e-technik.uni-rostock.de

Punktoperationen

Punkte auf einer Kurve E bilden eine abelsche Gruppe

für alle Punkte $P, Q \in E$ gilt:

1. $0 + P = P$ und $P + 0 = P$ (0 ist das neutrale Element)
2. $-0 = 0$
3. wenn $P = (x_1, y_1) \neq 0$, dann $-P = (x_1, -y_1 - a_1 x_1 - a_3)$
4. wenn $Q = -P$, dann $P + Q = 0$
5. $P + Q = R, R \in E$

Dipl.-Ing. Mathias Schmalisch
mathias.schmalisch@e-technik.uni-rostock.de

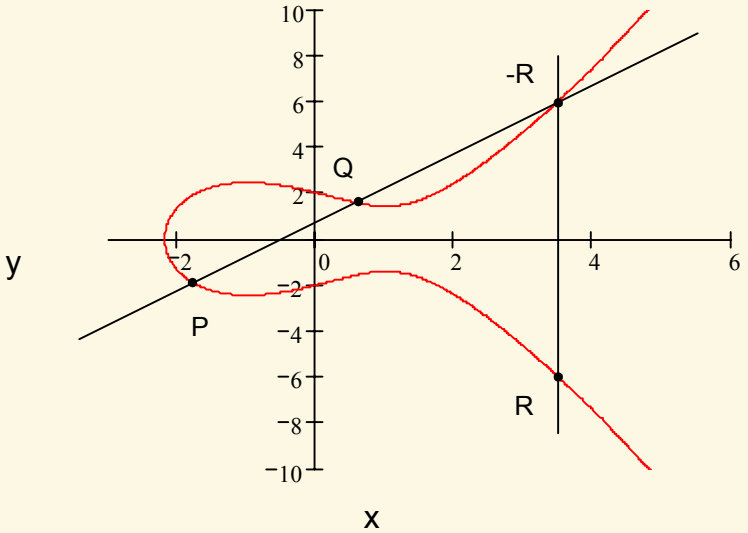
Punktaddition

- $P \neq Q$
- Line durch P und Q

$$y = \lambda x + \beta$$

$$\lambda = (y_2 - y_1) / (x_2 - x_1)$$

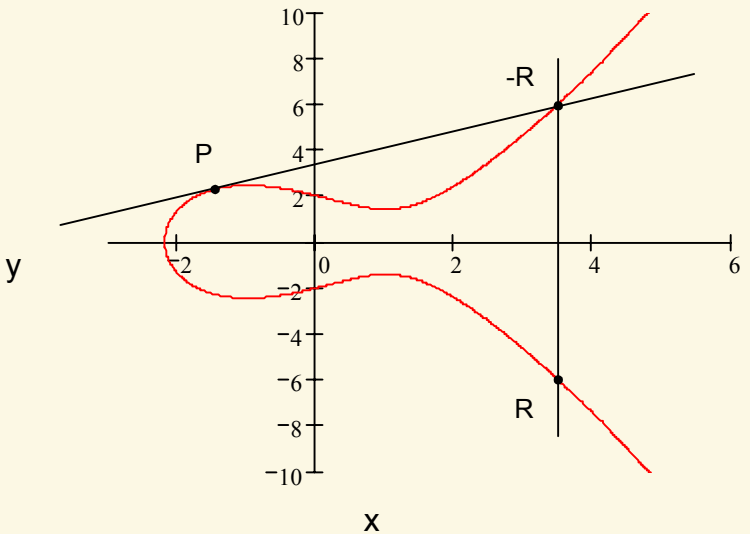
$$\beta = y_1 - \lambda x_1$$



Punktverdopplung

- P = Q
- Tangente an P
- Steigung entspricht erste Ableitung von E im Punkt P

$$\lambda = (3x_1^2 + 2a_2x_1 + a_4 - a_1y_1) / (2y_1 + a_1x_1 + a_3)$$
$$\beta = y_1 - \lambda x_1$$



Punktoperationen

- Berechnung von R

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

für $y = \lambda x + \beta$ einsetzen $F(x, \lambda x + \beta)$

$$F(x, \lambda x + \beta) = (x - x_1)(x - x_2)(x - x_3)$$

Koeffizientenvergleich

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

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

Skalarmultiplikation

- Multiplizieren mit einem Skalar

  $k * P = P + P + P + ... + P$

- Vereinfachung (z.B. k = 9)

  $2P = P + P$ (Punktverdopplung)

  $4P = 2P + 2P$

  $8P = 4P + 4P$

  $9P = 8P + P$ (Punktaddition)

Dipl.-Ing. Mathias Schmalisch
mathias.schmalisch@e-technik.uni-rostock.de

Übersicht

- Elliptische Kurven
- Punktoperationen
- **Körper**
- Beispiel
- Zusammenfassung

Dipl.-Ing. Mathias Schmalisch
mathias.schmalisch@e-technik.uni-rostock.de

Körper

- K ist eine nichtleere Menge
- auf K sind zwei Operanden definiert (+,*) für die gilt:

1. Assoziativgesetz

   $a + (b + c) = (a + b) + c$ $\qquad$ $a * (b * c) = (a * b) * c$

2. Kommutativgesetz

   $a + b = b + a$ $\qquad$ $a * b = b * a$

3. Distributivgesetz

   $$a * (b + c) = a * b + a * c$$

4. neutrales Element

   0, mit $a + 0 = a$ $\qquad$ 1, mit $a * 1 = a$

5. inverses Element

   $-a$, mit $a + (-a) = 0$ $\qquad$ a^{-1}, mit $a * a^{-1} = 1$

Körper

- K kann kein Körper sein über:
  - **Z** – ganze Zahlen (kein inverses Element für *)
  - **N** – natürliche Zahlen (kein inverses Element für *)

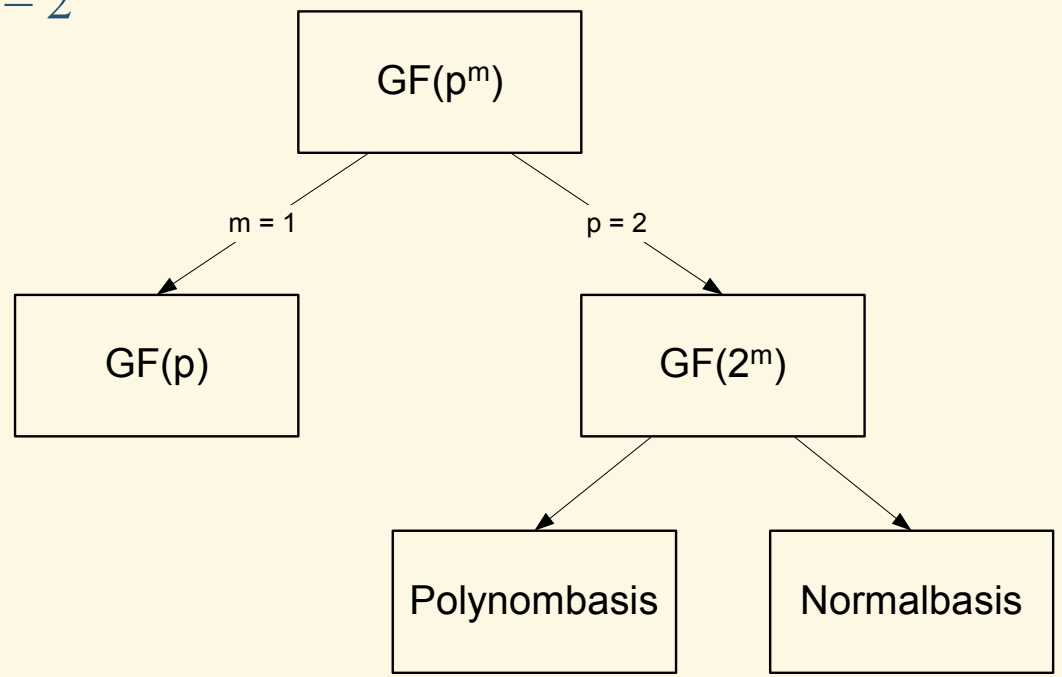
- K kann ein Körper sein über:
  - **R** – reelle Zahlen
  - **C** – komplexe Zahlen
  - **Q** – irrationale Zahlen
  - $\mathbf{F}_q$ – endlicher Körper (Galois Feld GF(q)) mit q Elementen

Dipl.-Ing. Mathias Schmalisch
mathias.schmalisch@e-technik.uni-rostock.de

endlicher Körper GF(q)

- $q = p^m$ und p muß eine Primzahl sein
- char(K) = p
- für Kryptographie von Interesse sind die Spezialfälle

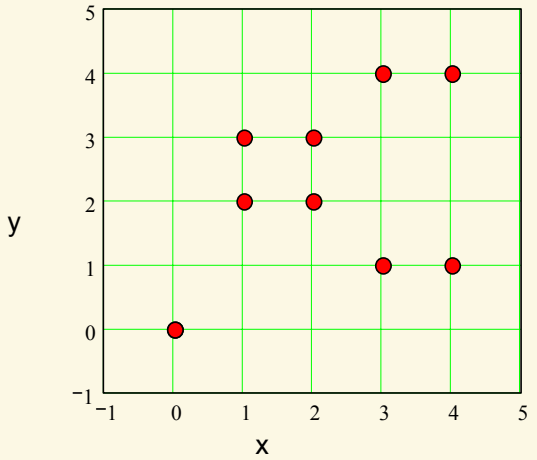
  m = 1 und p = 2



endlicher Körper GF(p)

- Modulare Mathematik
- Beispiel: $y^2 = x^3 + 3x$ über GF(5)

  $y^2 = x^3 + 3x \bmod 5$



- Addition

  $3 + 3 \bmod 5 = 1$
- Multiplikation

  $3 * 3 \bmod 5 = 4$
- Modulo Inverses (für Division)

  $x^{-1} \bmod p = 1$

  z.B. $3^{-1} \bmod 5 = 1$, $3^{-1} = 2$

endlicher Körper GF(2^m) Polynombasis

- es gilt im GF(2^m):
  - $a = -a$
  - $(a + b)^2 = a^2 + b^2$
- Verwendung eines irreduziblen Polynoms m(x)

  z.B. für $m = 8$, $m(x) = x^8 + x^4 + x^3 + x + 1$
- Addition
  - Addition der einzelnen Bitstellen mod 2 ($1 + 1 = 0$)

  z.B. $(x^6+x^4+x^2+x+1)+(x^7+x+1) = x^7+x^6+x^4+x^2$
- Multiplikation
  - Schieben und addieren, Reduktion mit irreduziblem Polynom

  z.B. $(x^6+x^4+x^2+x+1)(x^7+x+1) = x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1 \bmod m(x)$

  $= x^7+x^6+1$

endlicher Körper GF(2^m) Normalbasis

- es existiert immer eine Basis B = (β, β^2, β^{2^2}, ... , $\beta^{2^{m-1}}$)
- Nullelement (0, ... , 0), Einselement (1, ... , 1)

- Addition (wie bei Polynombasis)

  $(a_0, \dots, a_{m-1}) + (b_0, \dots, b_{m-1}) = (a_0+b_0, \dots, a_{m-1}+b_{m-1})$
- Multiplikation

  $(a_0, \dots, a_{m-1}) * (b_0, \dots, b_{m-1}) = (c_0, \dots, c_{m-1})$, mit $c_k = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i + k^{b_j} + k^{l_{ij}^{(0)}}$

  $l^{(0)}_{ij}$ hängt nur von der Basis ab
- Sonderfall Quadrierung x^2

  $(a_0, \dots, a_{m-1})^2 = (a_{m-1}, a_0, \dots, a_{m-2})$

Dipl.-Ing. Mathias Schmalisch
mathias.schmalisch@e-technik.uni-rostock.de

Übersicht

- Elliptische Kurven
- Punktoperationen
- Körper
- **Beispiel**
- Zusammenfassung

Dipl.-Ing. Mathias Schmalisch
mathias.schmalisch@e-technik.uni-rostock.de

Beispiel

- Diffie-Hellmann Schlüsselaustausch
- Alice wählt geheime Zahl a und Bob die Zahl b
- Alice und Bob einigen sich auf eine ell. Kurve E und Punkt F
- Alice berechnet PA = a * F
- Bob berechnet PB = b * F
- Punkte PB und PA werden ausgetauscht
- Alice berechnet Schlüssel x mit x =a * PB
- Bob berechnet Schlüssel x mit x = b * PA

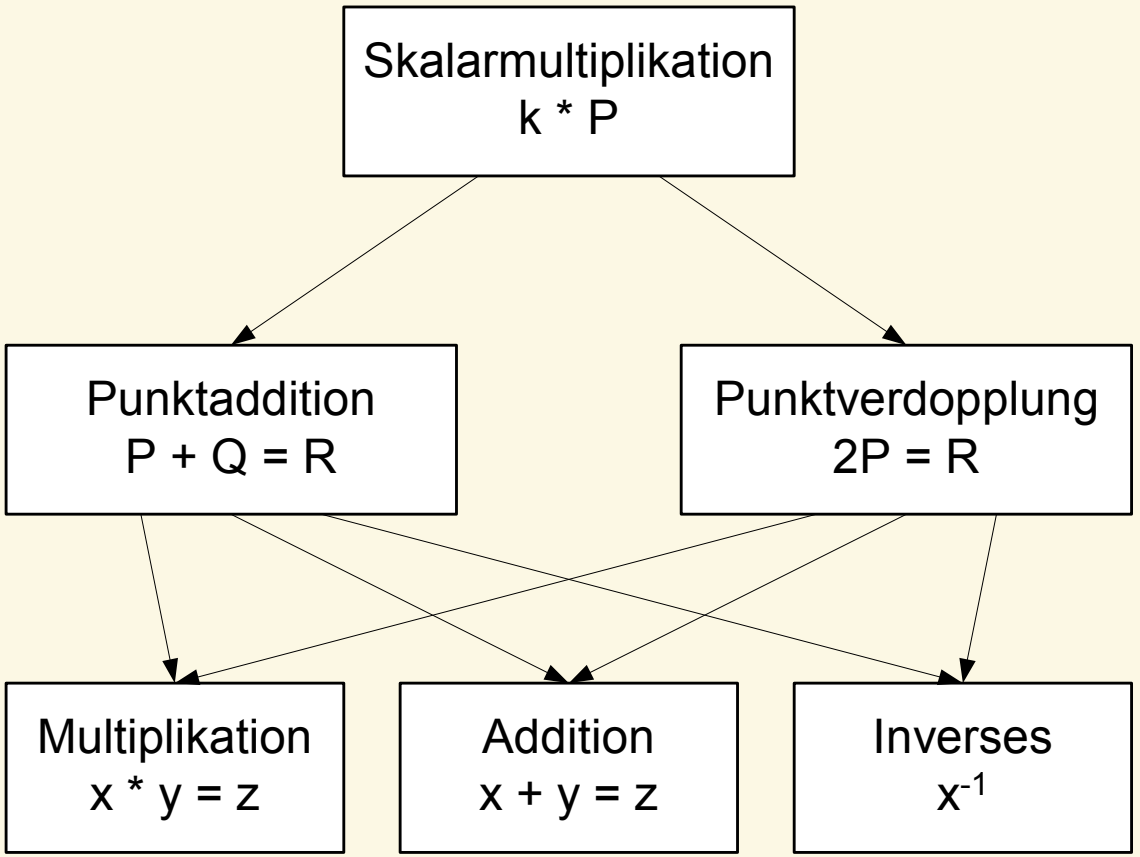
$$b * PA = b * (a * F) = b * (F * a) = (b * F) * a = a * PB$$

Übersicht

- Elliptische Kurven
- Punktoperationen
- Körper
- Beispiel
- **Zusammenfassung**

Dipl.-Ing. Mathias Schmalisch
mathias.schmalisch@e-technik.uni-rostock.de

Implementierung des ECC Verfahrens



Skalarmultiplikation

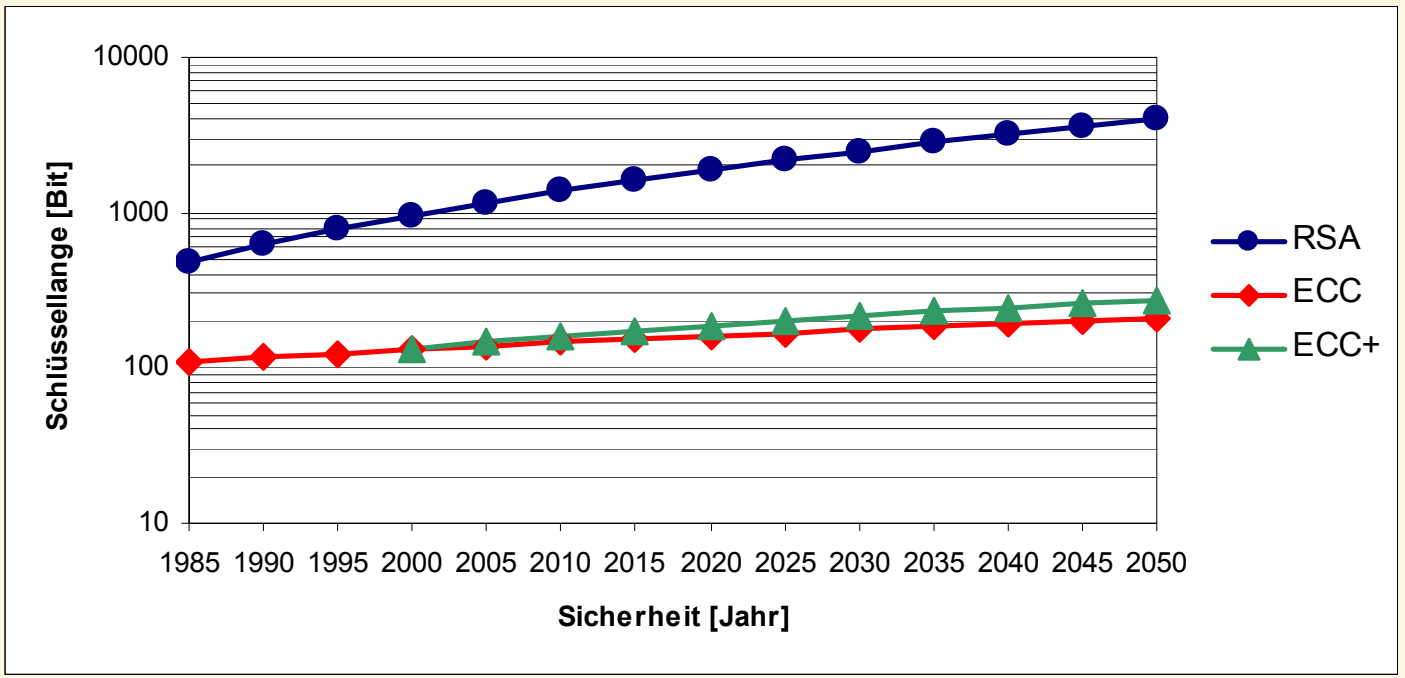
Punktoperationen auf der elliptischen Kurve

Operationen im endlichem Körper

Dipl.-Ing. Mathias Schmalisch
mathias.schmalisch@e-technik.uni-rostock.de

Vergleich mit RSA Verfahren

- Schlüssellänge wesentlich kürzer als bei RSA Verfahren
- RSA Schlüssellänge steigt schneller an
- bei kurzen Nachrichten (Schlüsselaustausch) viel Overhead



Zusammenfassung

- Elliptische Kurven über GF(2^m) sind für Hardwareimplementierung besonders gut geeignet
- Kürzere Schlüssellänge als bei anderen Verfahren (z.B. RSA)
- keine komplizierte Berechnung der Schlüssel notwendig, daher kann für jede Nachricht neuer Schlüssel gewählt werden
- Einarbeitung in Mathematik wesentlich aufwendiger als bei anderen Algorithmen