Kryptographie und elliptische Kurven - oder: Wie macht man Mathematikern das Leben schwer?

Harold Gutch
logix@foobar.franken.de

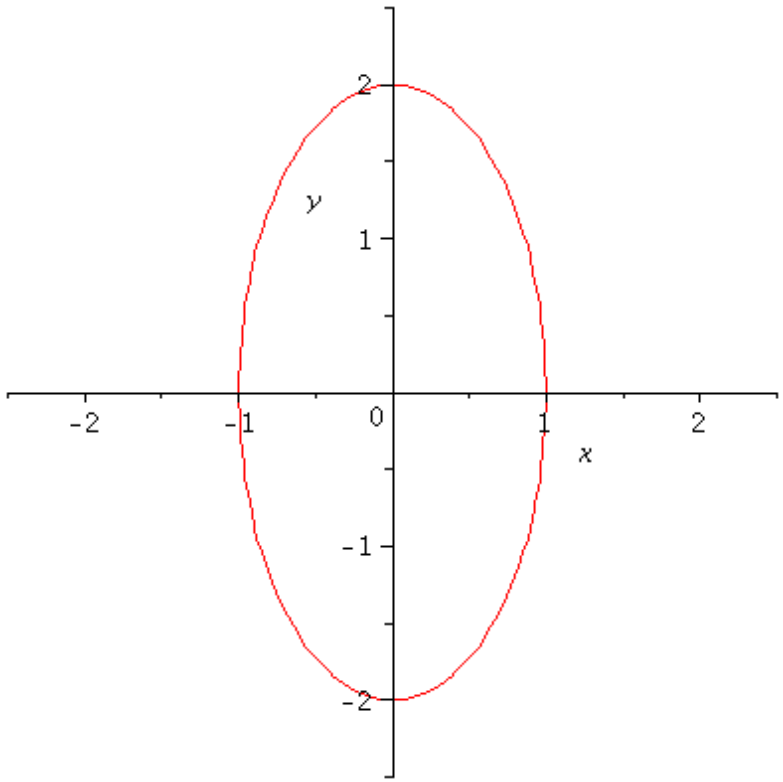
KNF Kongress 2007, 25. 11. 2007

Outline

Was ist Kryptographie?

- Darstellung einer Nachricht durch Folge von Zahlen (Klartext)
- Verschlüsselung = Berechnen anderer Zahlen aus dem Klartext (Chiffretext)
- Entschlüsselung = Berechnen des Klartextes aus dem Chiffretext
- Kryptographiealgorithmen: Verschlüsselung, Entschlüsselung, Signatur, Schlüsselaustausch, ...
- Klassische Zahlen: $0, 1, 2, \ldots, \infty, -1, -2, \ldots, -\infty$
- In der Kryptographie: meistens zugrunde liegenden Zahlen in der Form $\{0..N\}$ (Rechnen modulo N)
- Elliptische Kurven: Anderes Zahlensystem; die Kryptographiealgorithmen sind i.W. dieselben

Was sind elliptische Kurven nicht?

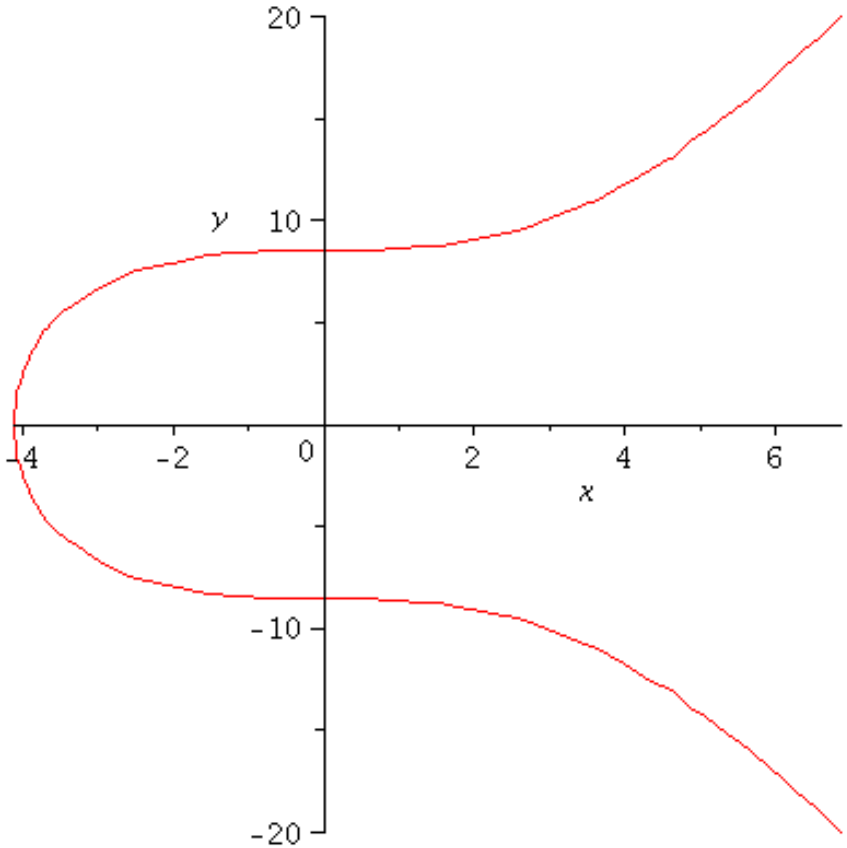


Elliptische Kurven sind nicht Ellipsen

Erinnerung:

- Punktmenge eines Kreises: $x^2 + y^2 = r^2$
- Punktmenge einer Ellipse: $Ax^2 + By^2 = C$

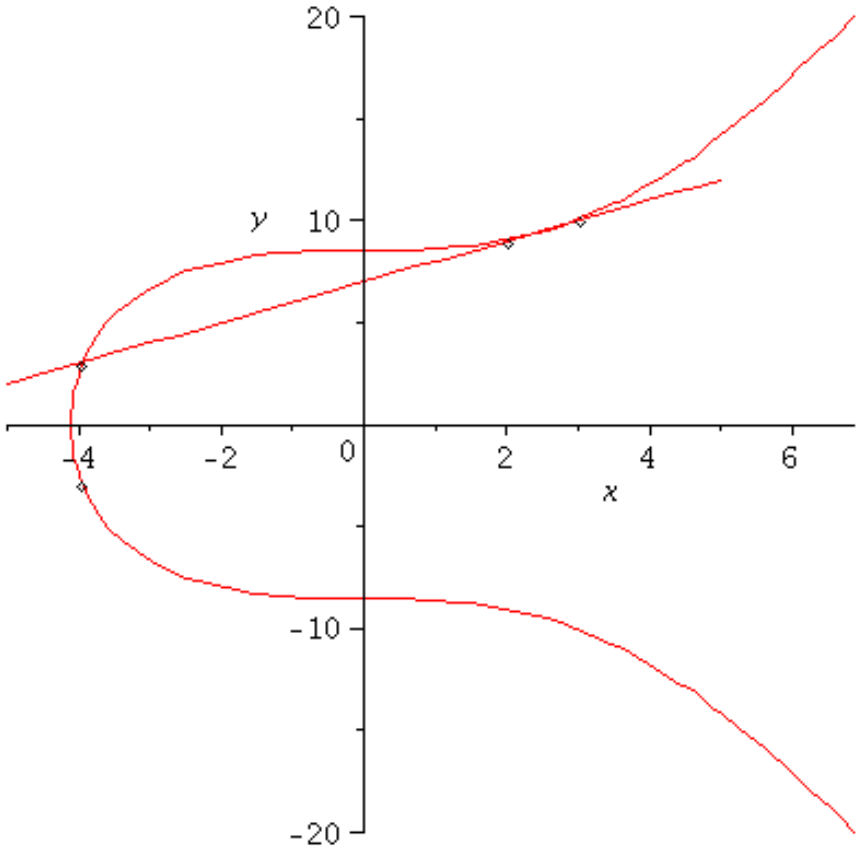
Was sind elliptische Kurven?



Punktmenge einer elliptischen Kurve: $y^2 = x^3 + ax^2 + b$ (hier: $a = 0$, $b = 73$; $y^2 = x^3 + 73$)

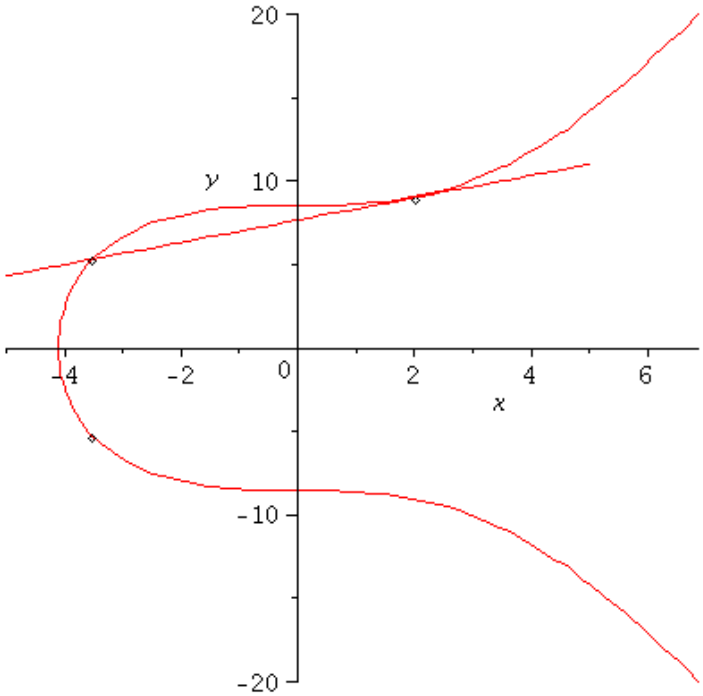
Ab jetzt: x und y immer $\mod p$

Geometrische Addition zweier (normaler) Punkte



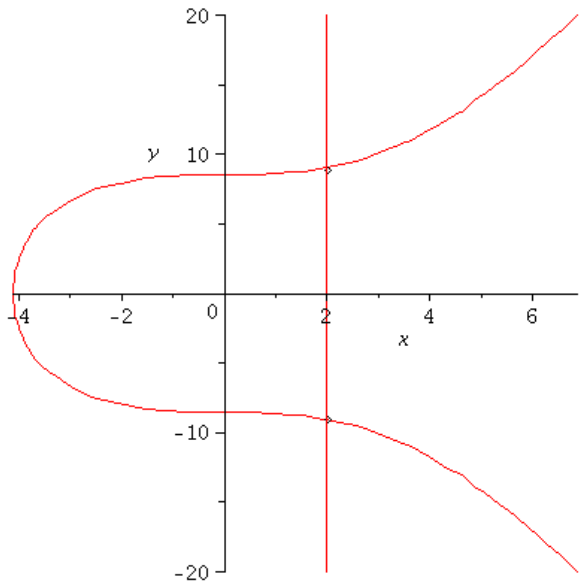
- Gerade durch die beiden Punkte P, Q; diese schneidet Kurve (meistens) in genau 1 weiterem Punkt
- Spiegelung dieses Punktes an x-Achse $= P + Q$

Besondere Additionen



- $P + P$: Tangente an Kurve benutzen
- Damit definiert: $2 \cdot P$
- Analog allgemein: $N \cdot P = (N-1) \cdot P + P = P + P + \cdots + P$

Ein besonderer Punkt



- $P+? = P$: Definition eines Nullpunktes (liegt nicht auf der gezeichneten Kurve)
- Gerade durch festes P und beliebigen anderen Punkt Q schneidet Gerade genau 1 weiteres Mal; Ausnahme: Q = Spiegelung von P an x-Achse
- Definition von $-P$ durch Spiegelung von P an x-Achse; Schnittpunkt liegt nicht auf der gezeichneten Kurve (= Nullpunkt)

Algebraische Addition

Wie berechnet man die Summe zweier Punkte P und Q?

$$P = (p_1, p_2)$$
$$Q = (q_1, q_2)$$

Was ist $(r_1, r_2) = P + Q$?
Sonderfälle betrachten ($P = 0$ oder $Q = 0$; $P = -Q$)
Ansonsten: wenn $P = Q$, dann $L = (3 \cdot p_1^2 + a)/(2 \cdot p_2)$, sonst $L = (p_2 - q_2)/(q_1 - p_1)$.

$$r_1 = L^2 - p_1 - q_1$$
$$r_2 = L \cdot (p_1 - r_1) - p_2$$

Eigenschaften der Addition

Für beliebige Punkte P, Q, R auf einer elliptischen Kurve gilt:

- $P + Q$ liegt wieder auf der elliptischen Kurve
- $P + Q = Q + P$ (Kommutativität)
- $(P + Q) + R = P + (Q + R)$ (Assoziativität)
- Existenz eines Punktes 0, mit der Eigenschaft $P + 0 = P$
- Existenz eines Punktes $-P$ mit der Eigenschaft $(-P) + P = 0$

Damit: Elliptische Kurve erfüllt die Eigenschaften einer Gruppe

Schlüsselaustausch

Diffie-Hellman Schlüsselaustausch auf elliptischen Kurven:

- Alice und Bob einigen sich auf eine elliptische Kurve (= wählen öffentlich bekannte Parameter a, b, p
- Alice und Bob einigen sich auf einen (öffentlichen) Punkt P auf der Kurve
- Beide wählen (geheime) ganze Zahlen a_k bzw. b_k
- Alice berechnet $A_k = a_k \cdot P$ und veröffentlicht dies
- Bob berechnet $B_k = b_k \cdot P$ und veröffentlicht dies
- Alice berechnet $a_k \cdot B_k$, Bob berechnet $b_k \cdot A_k$
- Beide kennen nun $a_k B_k = a_k(b_k P) = b_k(a_k P) = b_k A_k$ und können dies für z.B. klassische Verschlüsselung via AES benutzen

Sicherheit beruht auf der Schwierigkeit, aus P und kP den Wert k zu berechnen (diskreter Logarithmus)

Digitale Signaturen

- a_k, A_k wie oben
- $x(P)$ bezeichne die x-Koordinate von P
- Alice wählt zufälliges k
- Alice berechnet $r = x(kP) + H$ (wobei H der zu signierende Wert ist)
- Alice berechnet $s = k - a_k * r$
- Signatur: (r, s)
- Bob verifiziert Signatur durch: $H == r - x(sP + rA_k)$

Weitere Möglichkeiten: DSA, Schnorr-Signatur, andere Verfahren die auf Sicherheit des diskreten Logarithmus beruhen

Wahl von P

- Betrachtung von $P, 2P, 3P, \ldots$
- Kurve hat endlich viele Punkte, also irgendwann Wiederholung ($aP = bP$)
- Dann ist $(a - b)P = 0$
- Je größer das kleinste solche $(a - b)$ (= die Ordnung von P), desto sicherer ist Kombination aus Kurve und P
- Ist die Ordnung von P eine Primzahl der Länge n, so benötigt man ca. $2^{n/2}$ Operationen um k aus P und kP zu berechnen
- Bei gleicher Schlüssellänge deutlich komplexer als z.B. RSA

Vergleich mit herkömmlicher Kryptographie

- Bei gleicher Komplexität kürzer: ECC mit $p \approx 2^{1}63$ so möglich dass etwa gleich stark wie RSA-1024
- Sicherheit ähnlich hoch wie bei herkömmlicher Kryptographie
- Also: ECC benutzbar um gute Kryptographie in wenig(er) Platz unterzubringen
- ECC jünger, musste daher bisher weniger Angriffen Stand halten als herkömmliche Kryptographie
- Hintertüren in ECC-Verfahren? CRYPTO'07, Shumow/Ferguson: NIST SP800-90: DUAL_EC_DRBG

Was fehlt in diesem Vortrag?

- Angriffe auf ECC
- Komplexere Analyse von ECC
- Erwähnung von schwachen Kurven
- Daher: Bitte nicht anhand der hier gewonnen Erkenntnisse ECC implementieren und sämtliche Firmengeheimnisse anvertrauen
- ECC bietet unter der Haube noch viele Fallen die nur für Experten ersichtlich sind

Zusammenfassung

- Elliptische Kurven haben nicht direkt mit Kryptographie zu tun - sie sind vielmehr eine bestimmte Art zu rechnen
- Die Zahlen des Rechensystems sind Punkte auf bestimmten Kurven
- Man rechnet, indem man Geraden durch Punkte zieht und weitere Schnittpunkte von Gerade und Kurve betrachtet
- Aufbauend auf diesem Rechensystem lässt sich nun (wie auch auf anderen Rechensystemen) Kryptographie betreiben
- Vorteil: im Vergleich zur Größe der Zahlen besitzt Problem des diskreten Logarithmus hohe Komplexität
- (Bisher?) keine prinzipiellen gravierenden Nachteile bekannt

Empfehlenswerte Literatur

- Buchmann, J.: Einführung in die Kryptographie, Springer 2003
- Schneier, B: Angewandte Kryptographie, Pearson Studium 2005
- Singh, S.: Geheime Botschaften, Dtv 2001
- Beutelspacher, A.: Kryptographie in Theorie und Praxis, Vieweg 2005
- Linkliste von Franz Lemmermeyer: http://www.rzuser.uni-heidelberg.de/~hb3/ellc.html
- Wolfgang Ruppert, Vorlesung Sommersemester 2003; http://www.mi.uni-erlangen.de/~ruppert/