

Kryptographie - eine mathematische Einführung

Rosa Freund <rosa@pool.math.tu-berlin.de>

04. September 2005

Überblick

- RSA
- Diskretes Logarithmusproblem (DLP) / ElGamal
- DLP auf elliptischen Kurven

Kurze Wiederholung

Folgende Konzepte, die wir gestern kennengelernt haben, benötigen wir heute für die Algorithmen:

- Mathematische Strukturen: Gruppe, Ring, Körper, insb. endliche Körper
- Chinesischer Restsatz, kleiner Satz von Fermat

RSA 1

- Rivest, Shamir und Adleman, 1977
- p, q Primzahlen, $n = pq$
- Wähle d mit $1 < d < (p - 1)(q - 1) =: m$ und $\text{ggT}(d, m) = 1$
- Wähle e mit $1 < e < (p - 1)(q - 1)$ und $ed \equiv 1 \pmod{m}$
- n, d ist öffentlicher Schlüssel
- e ist geheimer Schlüssel

RSA 2

- $encrypt(x) \equiv x^d \pmod{n}$
- $decrypt(y) \equiv y^e \pmod{n}$
- **Wir zeigen nun:** $decrypt(encrypt(x)) = x$
- $decrypt(encrypt(x)) \equiv x^{de} \pmod{n}$, also zeige $x^{de} = x$ für $x \in \mathbb{F}_n$
- Es ist $ed = 1 + km = 1 + l(p - 1)$ nach Konstruktion

RSA 3

- Also $x^{ed} = xx^{l(p-1)} = x(x^{p-1})^l = x$ für $x \in \mathbb{F}_p$ (kleiner Satz von Fermat)
- Analog $x^{ed} = x$ für $x \in \mathbb{F}_q$
- Also auch $x^{ed} = x$ für $x \in \mathbb{F}_{pq} = \mathbb{F}_n$ (Chinesischer Restsatz)

RSA 4

- Sicherheit von RSA beruht auf der Schwierigkeit des Faktorisierens von großen ganzen Zahlen n
- In polynomieller Zeit lösbar (Algorithmus 2004 veröffentlicht): Ist n Primzahl?
- Vermutlich nicht in polynomieller Zeit lösbar: Was sind die Primfaktoren von n ?

Diskretes Logarithmus Problem - DLP

- Wieder Rechnen in Restklassen
- Gegeben: g aus einer zyklischen Gruppe, $x \in \mathbb{Z}$. Gesucht: e mit $g^e = x$
- z.B. \mathbb{F}_{11} : Suche $e \in \mathbb{F}_{11}$ mit $7^e \equiv 1 \pmod{11}$. Lösung: 8.
- Verfahren z.B. ElGamal
- Mathematische Fragestellungen: In welchen Gruppen ist das DLP „besonders schwer“?

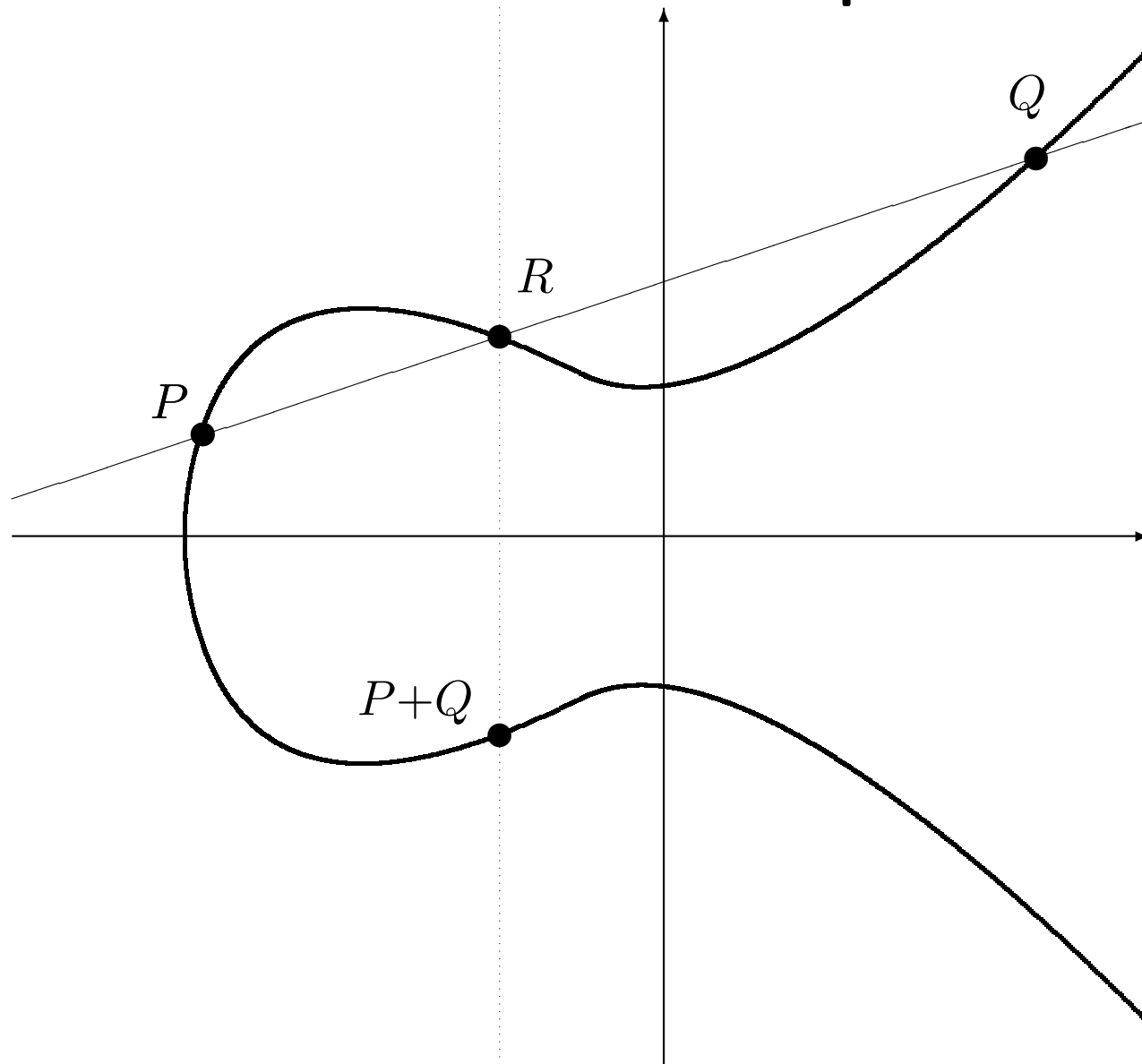
ElGamal Verschlüsselung

- Sei $\#G = l$, G zyklisch mit $G = \langle g \rangle$, $x \in \mathbb{Z}$ mit $0 \leq x \leq l$. Sei $y := g^x$
- private key: x , public key: y
- $encrypt(m) = (u, v)$ mit $u = g^r$, $v = my^r$, $r \in \mathbb{Z}$ zufällig
- $decrypt(u, v) = vu^{-x}$, da: $my^r(g^r)^{-x} = my^r(g^{-x})^r = my^r(y^{-1})^r = m$

DLP auf elliptischen Kurven 1

- Auf Punktgruppen von (hyper-)elliptischen Kurven ist das DLP „besonders schwer“
- $E : y^2 = x^3 + ax + b$, Punktmenge $\{(x, y) \in K \mid y^2 = x^3 + ax + b\}$, K Körper
- Die Punktmenge, die die Gleichung erfüllt, ist eine Gruppe (Punktgruppe), und zwar mit einer speziellen Punktaddition und dem neutralem Element "O" (s. Bild)
- Für kryptographische Zwecke werden Kurven über endlichen Körpern \mathbb{F}_q betrachtet

Punktaddition auf elliptischen Kurven



DLP auf elliptischen Kurven 2

Mathematische Fragestellungen z.B.

- Wieviel Punkte enthält E (über endlichen Körpern)?
- Für welche Gruppen und welche speziellen E ist das DLP nicht schwer bzw. besonders schwer?

Also:

- RSA und ElGamal werden z.B. bei PGP eingesetzt.
- ECC (Elliptic Curve Cryptosystems) kommen bei „gleicher“ Sicherheit mit deutlich kürzerem Schlüssel aus. Anwendung also z.B. bei Smartcards.
- **Jetzt:** Aufgaben!

Literatur

Bruce Schneier: Applied Cryptography. (Die Krypto-Bibel, sehr umfassend und allgemeinverständlich, allerdings etwas veraltet).

Ansonsten findet ihr alles Wissenswerte, und weitere Literaturtips hier:
http://de.wikipedia.org/wiki/Wikipedia:WikiProjekt_Kryptologie