Kryptographie - eine mathematische Einführung

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

28. Dezember 2004

Überblick

- Grundlegende Fragestellungen
- Symmetrische Verschlüsselung: Blockchiffren, Hashfunktionen
- asymmetrische Verschlüsselung: RSA, Diskretes Logarithmus Problem (DLP), DLP auf elliptischen Kurven

Grundlegende Fragestellungen

- Eine Nachricht soll nur vom vorgesehenen Empfänger gelesen werden können. Es geht nicht darum, das Lauschen zu verhindern, sondern darum, daß Lauscher die Nachricht nicht entschlüsseln können

- Die Signatur einer Nachricht soll es jedem ermöglichen, die Identität des Absenders zu verifizieren. Gleichzeitig soll es unmöglich sein, eine gefälschte Nachricht mit gültiger Signatur zu erstellen

Allgemeines

Zum verschlüsselten Kommunizieren benötigen die Parteien

- ein Verschlüsselungsverfahren, mit dem ver- und entschlüsselt wird (z.B. PGP, SSL)
- einen Schlüssel, d.h. den Variablen, die das Verfahren benötigt, müssen Werte zugeordnet werden
- z.B. Verschlüsselungsverfahren Cäsarchiffre, Schlüssel ist die Zahl, um die das Alphabet verschoben wird

Symmetrische Verfahren

- Die kommunizierenden Parteien teilen sich einen geheimen Schlüssel (secret key)
- z.B. Blockchiffren, Stromchiffren, Hashfunktionen
- Problem: Schlüsseltausch

Asymmetrische Verfahren 1

- Diffie und Hellman, 1976: *New Directions in Cryptography*
- Es gibt einen öffentlichen sowie einen geheimen Schlüssel (public key, private key), der geheime ist schwer oder garnicht aus dem öffentlichen berechenbar
- Um verschlüsselte Nachrichten erhalten bzw. Nachrichten signieren zu können, generiert A sich einen öffentlichen und einen geheimen Schlüssel
- Wie der Name sagt, muß A ihren geheimen Schlüssel (private key) geheimhalten, den öffentlichen (public key) jedoch veröffentlichen

Asymmetrische Verfahren 2

- Beim Verschlüsseln nutzt B den öffentlichen Schlüssel von A, um eine Nachricht an A zu verschlüsseln. A entschlüsselt die Nachricht mit ihrem geheimen Schlüssel

- Beim Signieren signiert A die Nachricht mit ihrem geheimen Schlüssel. B benutzt As öffentlichen Schlüssel, um die Signatur zu verifizieren

Asymmetrische Verfahren 3

- Sicherheit beruht meist auf algorithmischen Problemen mit hoher (bzw. ungeklärter) Komplexität
- Mathematisch geht insbesondere algebraische Zahlentheorie ein (z.B. diskreter Logarithmus, elliptische Kurven)
- Häufig zum Austausch von Schlüsseln für symmetrische Verfahren genutzt (z.B. SSL), da weniger effizient als symmetrische Verfahren

Kerckhoff-Prinzip

- Auguste Kerckhoff, 1883: *La Cryptographie militaire*
- Sicherheit eines kryptographischen Systems sollte nur auf der Geheimhaltung des Schlüssels beruhen, nicht jedoch auf Geheimhaltung des Verfahrens selbst
- Vorteile: die Qualität des Verfahrens kann intensiver untersucht werden

Blockchiffren

- symmetrisch
- Jede Nachricht wird in gleichlange Blöcke aufgeteilt, die Blöcke werden separat und unterschiedlich verschlüsselt. Der letzte Block wird ggf. mit Bits gepadded
- z.B. DES (1977), AES / Rijndael (2001)

Hashfunktionen

- Berechnet für Inputs beliebiger Länge Hashwerte von vorgegebener (meist kurzer) Länge
- Geringe Änderung des Inputs führt zu stark geändertem Hashwert
- Unix-Paßworte werden als Hashes gespeichert
- Aber: Dictionary-Attacke

Rechnen in Restklassen

- $\mathbb{Z}/q\mathbb{Z} := \{x + q\mathbb{Z} | x \in \mathbb{Z}\}$, bzw. $\mathbb{F}_q := \{0, 1, ..., q-1\}$
- Gerechnet wird modulo q, etwa wie bei einer Uhr (modulo 12)
- q ist hier prim
- $\mathbb{F}_q$ ist ein Körper (d.h. Struktur mit +,-,*,/)

RSA 1

- Rivest, Shamir und Adleman, 1977
- p, q Primzahlen, $n = pq$
- n, d ist öffentlicher Schlüssel
- e ist geheimer Schlüssel
- $encrypt(x) \equiv x^d \mod n$
- $decrypt(y) \equiv y^e \mod n$

RSA 2

Zu zeigen: $decrypt(encrypt(x)) = x$

- Wähle d mit $1 < d < (p-1)(q-1) =: m$ und $ggT(d, m) = 1$
- Wähle e mit $1 < e < (p-1)(q-1)$ und $ed \equiv 1 \mod m$
- $decrypt(encrypt(x)) \equiv x^{de} \mod n$, also zeige $x^{de} = x$ für $x \in \mathbb{Z}/n\mathbb{Z}$
- Es ist $ed = 1 + km = 1 + l(p-1)$ nach Konstruktion
- Ferner gilt $x^{p-1} = 1$ für $x \in \mathbb{Z}/p\mathbb{Z}$ (Fermats kleiner Satz)

RSA 3

- Also $x^{ed} = xx^{l(p-1)} = x\big(x^{(p-1)}\big)^l = x$ für $x \in \mathbb{Z}/p\mathbb{Z}$
- Analog $x^{ed} = x$ für $x \in \mathbb{Z}/q\mathbb{Z}$
- Also auch $x^{ed} = x$ für $x \in \mathbb{Z}/pq\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$ (Chinesischer Restsatz: $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$)

RSA 4

- Sicherheit von RSA beruht auf der Schwierigkeit des Faktorisierens von großen ganzen Zahlen n
- In polynomieller Zeit ist lösbar: 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. $\mathbb{Z}/11\mathbb{Z}$: Suche $e \in \mathbb{Z}/11\mathbb{Z}$ mit $7^e \equiv 1 \mod 11$. Lösung: 8.
- Verfahren z.B. ElGamal
- Mathematische Fragestellungen: In welchen Gruppen ist das DLP "besonders schwer"?

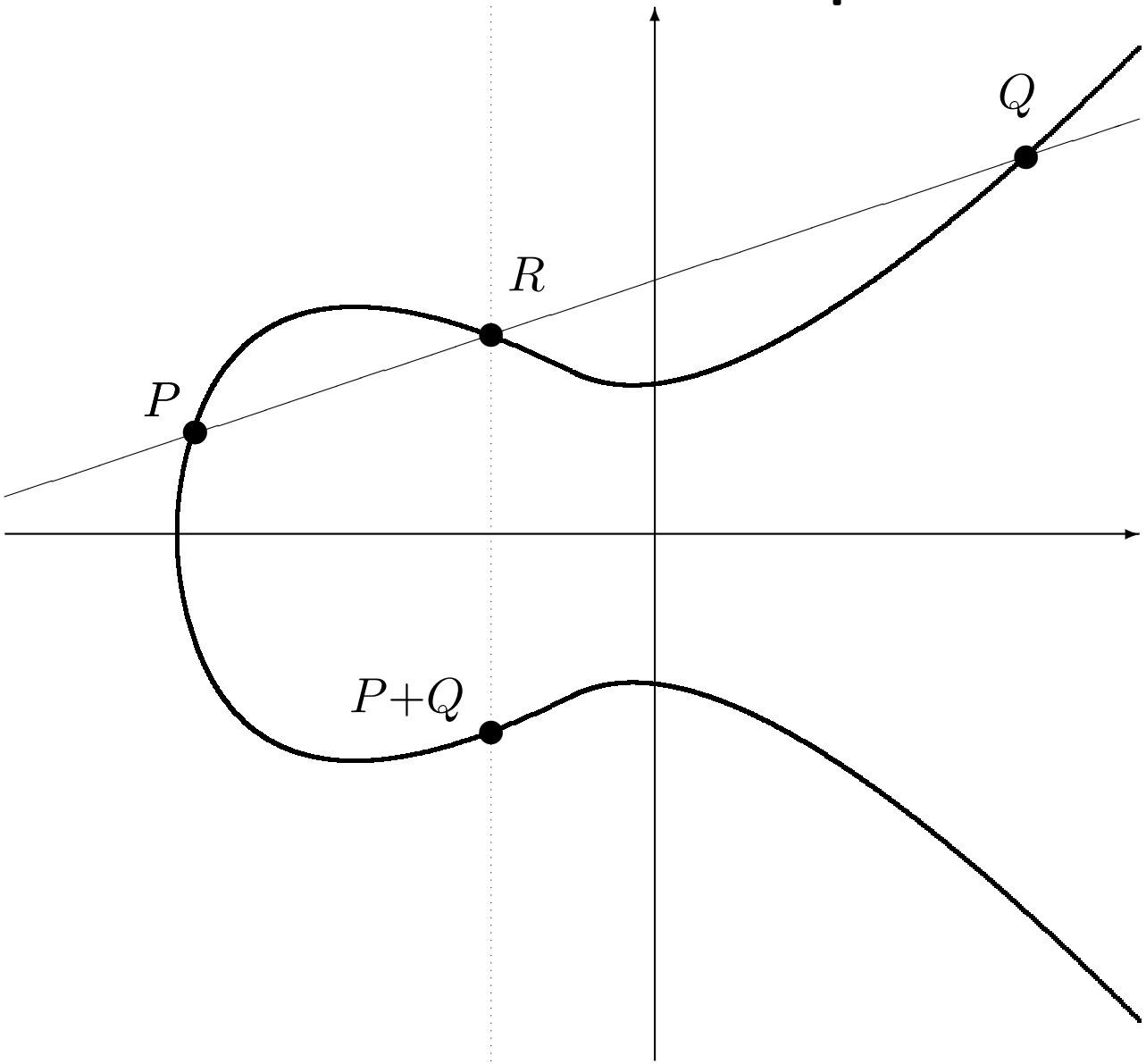
ElGamal Verschlüsselung

- Sei $\#G = l$, G zyklisch mit $G =< g >$, $x \in \mathbb{Z}$ 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 $\{(x, y) \in K | y^2 = x^3 + ax + b\}$, 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?

Literatur

http://de.wikipedia.org/wiki/Wikipedia:WikiProjekt_Kryptologie