# Elliptische Kurven in der Kryptographie

Prusoth Vijayakumar

06. 06. 2011

# Übersicht

- Motivation
- Verfahren

# Motivation

- Relativ sicher, da auf der Schwierigkeit mathematischer Probleme beruhend (z.B. Diskreter Logarithmus, Faktorisieren)
- Schnellere Verfahren (kürzere Schlüssellängen)
- Verfahren mit elliptischen Kurven sind asymmetrisch

# Verfahren

- Diffie-Hellman-Schlüsselaustausch
- Massey-Omura-Schema
- Elgamal Verschlüsselung
- Digitale Signaturen mit ElGamal
- DSA: Digital Signature Algorithm
- Koyama-Maurer-Okamoto-Vanstone

# Diffie-Hellman-Schlüsselaustausch

- Vereinbarung einer elliptischen Kurve E über einen endlichen Körper $F_q$, sodass das Problem des diskreten Logarithmus schwer lösbar ist in $E(F_q)$
- Wahl eines gemeinsamen Punktes P auf E, sodass dessen Ordnung r sehr groß und prim ist
- Alice wählt eine geheime Zahl a, berechnet aP und sendet diese an Bob
- Bob wählt eine geheime Zahl b, berechnet bP und sendet diese an Alice
- Alice und Bob berechnen nun baP = abP den gemeinsamen Schlüssel

# Diffie-Hellman-Schlüsselaustausch

- Vereinbarung einer elliptischen Kurve E über einen endlichen Körper $F_q$, sodass das Problem des diskreten Logarithmus schwer lösbar ist in $E(F_q)$
- Wahl eines gemeinsamen Punktes P auf E, sodass dessen Ordnung r sehr groß und prim ist
- Alice wählt eine geheime Zahl a, berechnet aP und sendet diese an Bob
- Bob wählt eine geheime Zahl b, berechnet bP und sendet diese an Alice
- Alice und Bob berechnen nun baP = abP den gemeinsamen Schlüssel

# Diffie-Hellman-Schlüsselaustausch

Diffie-Hellman Problem :
Gegeben seien die Punkte P, aP, bP auf $E(F_q)$.
Bestimme daraus abP.
Diffie-Hellman-Entscheidungsproblem :
Gegeben seien die Punkte P, aP, bP auf $E(F_q)$ sowie ein Punkt Q auf $E(F_q)$.
Finde heraus ob Q = abP.

# Massey-Omura-Schema

- Vereinbarung einer elliptischen Kurve E über $F_q$, sodass der diskrete Logarithmus schwer lösbar ist. Sei N=$\#E(F_q)$
- Alice stellt ihre Nachricht als Punkt M auf E dar
- Alice wählt eine geheime Zahl $m_A$ mit ggT($m_A$,N)=1 und berechnet $M_1 = m_A$M und sendet $M_1$ an Bob
- Bob wählt $m_B$ mit ggT($m_B$,N)=1, bestimmt $M_2 = m_B\ M_1$ und sendet $M_2$ an Alice
- Alice bildet $m_A^{-1}$ in $Z_n$ und berechnet $M_3 = m_A^{-1}\ M_2$ und sendet $M_3$ an Bob
- Bob berechnet $M_4 = m_B^{-1}\ M_3 =$ M

# Massey-Omura-Schema

- Vereinbarung einer elliptischen Kurve E über $F_q$, sodass der diskrete Logarithmus schwer lösbar ist. Sei N=$\#E(F_q)$
- Alice stellt ihre Nachricht als Punkt M auf E dar
- Alice wählt eine geheime Zahl $m_A$ mit ggT($m_A$,N)=1 und berechnet $M_1 = m_A$M und sendet $M_1$ an Bob
- Bob wählt $m_B$ mit ggT($m_B$,N)=1, bestimmt $M_2 = m_B\ M_1$ und sendet $M_2$ an Alice
- Alice bildet $m_A^{-1}$ in $Z_n$ und berechnet $M_3 = m_A^{-1}\ M_2$ und sendet $M_3$ an Bob
- Bob berechnet $M_4 = m_B^{-1}\ M_3 =$ M

# Massey-Omura-Schema

Eve kennt E, $m_A$M, $m_B$M und $m_B$ $m_A$M.
Mit a=$m_A^{-1}$, b=$m_B^{-1}$ und P=$m_A$ $m_B$M
führt dies wieder zum Diffie-Hellman Problem.

# Elgamal Verschlüsselung

- Bob wählt eine elliptische Kurve E über $F_q$ mit schwierigem DLP, einen Punkt P auf E, sowie eine geheime Zahl s. Damit bestimmt er B=sP und veröffentlicht E, P, B und $F_q$
- Alice drückt ihre Nachricht als einen Punkt M auf E aus.
- Mit einer geheimen Zahl k bestimmt sie $M_1$=kP und $M_2$=M+kB
- Sie sendet $M_1$ und $M_2$ an Bob
- Bob entschlüsselt M=$M_2$-s$M_1$

# Elgamal Verschlüsselung

- Bob wählt eine elliptische Kurve E über $F_q$ mit schwierigem DLP, einen Punkt P auf E, sowie eine geheime Zahl s. Damit bestimmt er B=sP und veröffentlicht E, P, B und $F_q$
- Alice drückt ihre Nachricht als einen Punkt M auf E aus.
- Mit einer geheimen Zahl k bestimmt sie $M_1$=kP und $M_2$=M+kB
- Sie sendet $M_1$ und $M_2$ an Bob
- Bob entschlüsselt M=$M_2$-s$M_1$

# Elgamal Verschlüsselung

Angriffsmöglichkeiten:
Eve kennt $M_1$ und $M_2$
a)Wenn sie s herausfindet mittels P und B, kann sie $M_2$-s$M_1$ bestimmen
b)Wenn sie k herausfindet mittels P und $M_2$, kann sie $M_2$-kB bestimmen
Wichtig: Alice sollte verschiedene k wählen für verschiedene Nachrichten

# Elgamal Verschlüsselung

Angriffsmöglichkeiten:
Eve kennt $M_1$ und $M_2$
a)Wenn sie s herausfindet mittels P und B, kann sie $M_2$-s$M_1$ bestimmen
b)Wenn sie k herausfindet mittels P und $M_2$, kann sie $M_2$-kB bestimmen
Wichtig: Alice sollte verschiedene k wählen für verschiedene Nachrichten

# Digitale Signaturen mit ElGamal

- Alice wählt eine elliptische Kurve E über $F_q$, einen Punkt A auf E mit großer Ordnung N,eine beliebige Funktion f:$E(F_q)$ $\rightarrow$ Z, sowie ein $\alpha$ und berechnet B=$\alpha$A
- Alice veröffentlicht E, q, f, A und B
- Sie stellt das Dokument als ganze Zahl m dar und wählt ein beliebiges k mit ggT(k,N)=1 und bestimmt R=kA
- Sie berechnet s=$k^{-1}(m-\alpha f(R))$ mod N
- Sie signiert die Nachricht mit (m, R, s)

# Digitale Signaturen mit ElGamal

- Alice wählt eine elliptische Kurve E über $F_q$, einen Punkt A auf E mit großer Ordnung N,eine beliebige Funktion f:$E(F_q)$ $\rightarrow$ Z, sowie ein $\alpha$ und berechnet B=$\alpha$A
- Alice veröffentlicht E, q, f, A und B
- Sie stellt das Dokument als ganze Zahl m dar und wählt ein beliebiges k mit ggT(k,N)=1 und bestimmt R=kA
- Sie berechnet s=$k^{-1}(m-\alpha f(R))$ mod N
- Sie signiert die Nachricht mit (m, R, s)

# Digitale Signaturen mit ElGamal

Bob überprüft die Signatur folgendermaßen:

- Bob berechnet $V_1$=f(R)B+sR
- Bob berechnet $V_2$=mA
- Falls $V_1$=$V_2$ gilt die Signatur als gültig

# Digitale Signaturen mit ElGamal

Angriffsmöglichkeiten:
a) Wenn Eve $\alpha$ herausfindet mittels A und B, kann sie Alices Signatur für jede Nachricht verwenden
b) Wenn Eve k herausfindet mittels A und R, kann sie $\alpha$ bestimmen da sie s, f(R) und m kennt und ebenfalls Alices Signatur verwenden
Wichtig: Alice sollte verschiedene k für verschiedene Signaturen verwenden

# Digitale Signaturen mit ElGamal

Angriffsmöglichkeiten:
a) Wenn Eve $\alpha$ herausfindet mittels A und B, kann sie Alices Signatur für jede Nachricht verwenden
b) Wenn Eve k herausfindet mittels A und R, kann sie $\alpha$ bestimmen da sie s, f(R) und m kennt und ebenfalls Alices Signatur verwenden
Wichtig: Alice sollte verschiedene k für verschiedene Signaturen verwenden

# DSA: Digital Signature Algorithm

- Alice wählt m, E,$F_q$ so, dass #$E(F_q)$=fr, wobei r eine große Primzahl und f eine kleine ganze Zahl sein soll
- Sie wählt einen Punkt G auf E der Ordnung r aus, sowie eine geheime Zahl $\alpha$ und berechnet Q=$\alpha$G
- Sie veröffentlich q, E, r, G und Q
- Sie wählt ein k<r und bestimmt R=kG=(x,y)
- Sie bestimmt s=$k^{-1}(m+\alpha x)$ mod r und signiert mit (m,R,s)

# DSA: Digital Signature Algorithm

Verifizierung:

- Bob berechnet $u_1$=$s^{-1}$m mod r und $u_2$=$s^{-1}$x mod r
- Er bestimmt V= $u_1$G+$u_2$Q
- Falls V=R ist die Signatur gültig

# Koyama-Maurer-Okamoto-Vanstone

- Bob wählt zwei große Primzahlen p, q mit $p \equiv q \equiv 2 \bmod 3$ und berechnet n=pq
- Er wählt e und d mit $ed \equiv 1 \bmod kgV(p+1,q+1)$
- Er veröffentlicht n und e
- Alice stellt ihr Nachricht als Punkt M=($m_1$,$m_2$) der Kurve E:$y^2 = x^3$+b (mod n) dar (b ist frei wählbar)
- Sie berechnet C=eM
- Bob berechnet M=dC

# Koyama-Maurer-Okamoto-Vanstone

- Bob wählt zwei große Primzahlen p, q mit $p \equiv q \equiv 2 \bmod 3$ und berechnet n=pq
- Er wählt e und d mit $ed \equiv 1 \bmod kgV(p+1,q+1)$
- Er veröffentlicht n und e
- Alice stellt ihr Nachricht als Punkt M=($m_1$,$m_2$) der Kurve E:$y^2 = x^3$+b (mod n) dar (b ist frei wählbar)
- Sie berechnet C=eM
- Bob berechnet M=dC