Seminar Kryptographie

Elliptische Kurven in der Kryptographie

Prusoth Vijayakumar

Sommersemester 2011

Inhaltsverzeichnis

1 Motivation

In diesem Vortrag werden wir uns verschiedene Kryptosysteme anschauen, die auf den Elliptischen Kurven basieren. Einige Verfahren, die wir uns anschauen werden, werden uns bekannt vorkommen als klassische Systeme aus der Kryptographie. Also stellt sich die Frage warum auf den Elliptischen Kurven?
Zunächst einmal sind die Verfahren auf Elliptischen Kurven, die meist asymmetrisch sind, genauso sicher wie die klassischen Systeme, da die Methoden ebenfalls auf der Schwierigkeit mathematischer Probleme beruhen wie zum Beispiel dem Diskreten Logarithmus Problem oder das Faktorisierungsproblem. Der Vorteil dabei ist, dass die Verfahren auf Elliptischen Kurven wesentlich schneller sind, da sie mit kürzeren Schlüssellängen auskommen.

Beispiel:
Schlüssellänge RSA ohne Elliptische Kurven: 4096 bits
Schlüssellänge RSA mit Elliptische Kurven: 313 bits

Das heißt in der Praxis, dass die Implementierung einfacher wird, kleinere Chipgrößen benötigt werden und der Aufwand insgesamt geringer wird.

Bezeichnungen

Wir verwenden wie in der Kryptographie üblich die Personen

- Alice als Nachrichtenempfängerin
- Bob als Nachrichtenempfänger
- Eve als Unbefugte, die Nachrichten abfangen/manipulieren will

2 Verfahren

2.1 Diffie-Hellman-Schlüsselaustausch

Das erste Verfahren beschäftigt sich mit einem Schlüsselaustausch, das heißt Alice und Bob einigen sich hierüber auf einen gemeinsamen Schlüssel mittels dem sie ihre Daten austauschen wollen.

Algorithmus:

- 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

Die Sicherheit dieses Verfahrens beruht auf dem Diffie-Hellman Problem:

Gegeben seien die Punkte P, aP, bP auf $E(F_q)$. Bestimme daraus abP.

bzw dem zugehörigen 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.

Das heißt dieses Verfahren kann nur geknackt werden, wenn man das Diskrete Logarithmus Problem hierin löst.

2.2 Massey-Omura-Schema

Bei diesem Verfahren haben wir nun folgende Situation gegeben: Alice will eine Nachricht an Bob versenden, allerdings ist noch kein Schlüssel vereinbart.

Algorithmus

- 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_AM 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

Bleibt zu zeigen, dass $M_4 = m_B^{-1}\ m_A^{-1}\ m_B\ m_A$ = M gilt.

Dazu müssen wir zunächst zeigen, dass m_A^{-1}, welches eine ganze Zahl und die Inverse zu m_A mod N ist, und m_A sich aufheben.
Wir betrachten $m_A^{-1}\ m_A \equiv 1$ mod N, also $m_A^{-1}\ m_A$=1+kN für ein k $\in$ Z. Die Gruppe $E(F_q)$ hat Ordnung N, dann impliziert Lagranges Theorem, dass NR=∞ $\forall$ R$\in$ $E(F_q)$. Daher ergibt sich $m_A^{-1}\ m_A$R=(1+kN)R=R+kNR=R+k∞=R.
Setzen für R=m_BM :
M_3=$m_A^{-1}\ m_B\ m_A$M=m_BM .
Analog gilt dies für m_B^{-1} und m_B :
M_4= $m_B^{-1}\ M_3$=$m_B^{-1}\ m_B$M=M.

Veranschaulicht kann man sich das so vorstellen, dass Alice ihre Nachricht in eine Box schließt und ihr Schloss daran hängt. Sobald die Box zu Bob gelangt, hängt dieser wiederum sein Schloss daran und sendet diese zurück. Alice entfernt danach ihr Schloss und sendet letztendlich die Box an Bob. Dieser kann nun sein Schloss entfernen und die Nachricht entnehmen.

Eve kennt E, m_AM, m_BM und m_B m_AM.
Mit a=m_A^{-1}, b=m_B^{-1} und P=m_A m_BM gibt uns das Diffie-Hellman Problem wieder die Sicherheit für das Verfahren.

2.3 Elgamal Verschlüsselung

Als nächstes schauen wir uns ein asymmetrisches Verschlüsselungsverfahren an, dessen Idee wir aus der klassischen Methode kennen.

Algorithmus :

- 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-sM_1

Hier gilt es zu überprüfen, dass M_2-sM_1 die urspüngliche Nachricht M ist.
M_2-sM_1=(M+kB)-s(kp)=M+k(sP)-skp=M.

Auch hier gibt uns das DLP die Sicherheit, denn Eve muss s berechnen mittels P und B, damit sie M_2-sM_1 bestimmen kann oder sie muss k berechnen mittels P und M_2, damit sie M_2-kB bestimmen kann.

Beachten muss man hierbei, dass Alice für jede weitere Nachricht jeweils ein anderes k nehmen muss.
Denn sei $M \neq M'$, dann gilt M_1=M_1'. Daraus ergibt sich M_2'-M_2=M'-M.
Sobald also Eve irgendwann eine Nachricht M kennt, kennt sie auch M' durch M'=M-M_2+M_2'.

2.4 Digitale Signaturen mit ElGamal

Nun haben wir folgende Situation gegeben: Alice will ein elektronisches Dokument unterzeichnen, sodass ihre digitale Unterschrift nicht kopiert und von Eve für andere Dokumente wiederverwendet werden kann. Die Unterschrift muss also als gültig verifiziert werden können und eindeutig sein. Dazu verwendet man unter anderem folgendes Signaturverfahren:

Algorithmus :

- 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 α und berechnet B=αA
- 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- α f(R)) mod N

- Sie signiert die Nachricht mit (m, R, s)

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

Zu zeigen ist hier dass, V_1=V_2 gilt.
Dazu betrachten wir zunächst s≡ k^{-1}(m-αf(R)) mod N, also sk=m-αA f(R)+zN für ein z∈Z.
Daher gilt: skA=(m-α f(R))A+zNA= (m-αf(R))A+z∞=(m-α f(R))A.
Somit ergibt sich für V_1=f(R)B+sR=f(R)αA+skA=f(R)αA+(m-αf(R))A = mA = V_2

Die Sicherheit gibt uns wieder das DLP.
Eve müsste α berechnen mittels A und B oder k berechnen mittels A und R um mit s,f(R) und m das α zu erhalten.

Auch hier muss Alice verschiedene k für jeweils verschiedene Signaturen verwenden.

Angenommen Alice unterschreibt zwei Dokumente m und m' mit demselben k als (m,R,s) und (m',R,s'), dann bemerkt Eve, dass bei beiden Dokumenten dasselbe k benutzt wurde durch das gleiche R in der Signatur.
Mit den beiden Gleichungen
sk ≡ m-αf(R) mod N und
s'k ≡ m'-αf(R) mod N
erhalten wir durch Subtraktion k(s-s')≡m-m' mod N.
Sei d=ggT(s-s',N). Dann gibt es genau d verschiedene Möglichkeiten für k.
Eve probiert dann diese d Möglichkeiten aus bis sie ein k findet, das R=kA erfüllt.

2.5 DSA: Digital Signature Algorithm

Hier wird ein weiteres Signaturverfahren vorgestellt.

Algorithmus :

- 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 α und berechnet Q=αG

- Sie veröffentlicht q, E, r, G und Q
- Sie wählt ein k<r und bestimmt R=kG=(x,y)
- Sie bestimmt s=k^{-1}(m+αx) mod r und signiert mit (m,R,s)

Verifizierung:

- Bob berechnet u_1=s^{-1}m mod r und u_2=s^{-1}x mod r
- Er bestimmt V= u_1G+u_2Q
- Falls V=R ist die Signatur gültig

Zu überprüfen gilt es ob V=R.

V=u_1G+u_2Q=s^{-1}mG+s^{-1}xQ=s^{-1}(mG+xαG) = kG = R

Der wesentliche Unterschied zur vorherigen Methode liegt im Verifizierungsprozess. Während im Elgamal System 3 Berechnungen angestellt werden müssen, nämlich f(R)*B,s*R und m*A, müssen hier im Verifizierungsteil nur 2 Berechnungen, nämlich u_1*G und u_2*Q durchgeführt werden.
Da dieser Teil der aufwändigste Teil des Algorithmus ist und da oft mehrere Verifikationen durchgeführt werden müssen, erweist sich dieses Signaturverfahren als effizienter.

2.6 Koyama-Maurer-Okamoto-Vanstone

Im Anschluss an alle Verfahren, die auf dem DLP beruhen wollen wir uns zu guter Letzt ein Verfahren anschauen das auf dem Faktorisierungsproblem basiert und die Grundidee des RSA-Verfahrens verwendet.

Algorithmus :

- Bob wählt zwei große Primzahlen p, q mit p $\equiv$ q $\equiv$ 2 mod 3 und berechnet n=pq
- Er wählt e und d mit ed $\equiv$ 1 mod 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

Um hier zu zeigen, dass dC die ursprüngliche Nachricht M ist müssen wir etwas Vorarbeit leisten.

Definition: Eine Elliptische Kurve E über F_q der Charakteristik p heißt supersingulär, wenn p|t, wobei t=q+1- $\#E(F_q)$.

Propositon(ohne Beweis): Sei E eine Elliptische Kurve über F_q, wobei q eine Potenzzahl von der Primzahl p ist. Weiterhin sei a=q+1-$\#E(F_q)$. Dann ist E supersingulär $\Leftrightarrow$ a $\equiv$0 mod p $\Leftrightarrow$ $\#E(F_q)$ $\equiv$1 mod p.

Korollar: Sei p$\geq$5 eine Primzahl und E eine Elliptische Kurve über F_q. Dann ist E supersingulär $\Leftrightarrow$ $\#E(F_q)$=p+1.
Beweis: Wenn a=0, dann ergibt die vorherige Proposition, dass E supersingulär ist. Umgekehrt nehmen wir an, dass E supersingulär und a $\neq$0. Dann impliziert a$\equiv$0 mod p, dass |a|$\geq$p. Nach Hasses Theorem gilt |a|$\leq 2\sqrt{p}$, also folgt p$\leq 2\sqrt{p}$. Das bedeutet p$\leq$4.

Proposition: Sei q ungerade und q $\equiv$2 mod 3 und B $\in F_q^x$. Dann ist die Elliptische Kurve E: $y^2=x^3$ + b supersingulär.
Beweis: Sei ψ:$F_q^x \rightarrow F_q^x$ ein Homomorphismus definiert durch ψ(x)=x^3. Da q-1 kein Vielfaches von 3 ist gibt es keine Elemente der Ordnung 3 in F_q^x. Also ist der Kern von ψ trivial. Deswegen (ψ injektiv) muss ψ surjektiv sein, da es eine Abbildung von einer endlichen Gruppe auf sich selbst ist. Insbesondere hat jedes Element aus F_q eine Kubikwurzel in F_q.
Das heißt für jedes y$\in F_q$ existiert genau ein x$\in F_q$, sodass (x,y) auf der Kurve liegt. Also ist x die eindeutige Kubikwurzel von y^2-b. Da es q Werte von y gibt erhalten wir auch q Punkte. Mit dem Unendlich-Punkt ∞ folgt also $\#E(F_q)$=q+1. Somit ist E supersingulär.

Aus dem chinesichen Restsatz folgt, dass eine Zahl mod n, als ein Paar ganzer Zahlen angesehen werden kann. Das heißt jeder Punkt auf E in Z_n kann dargestellt werden als ganze Zahlen in E mop p und E mod q.
Also haben wir E(Z_n) = E(F_p) $\oplus$ E(F_q).
Weiterhin wissen wir ord E(Z_n) =# E(F_p)*#E(F_q).
Durch das Korollar wissen wir # E(F_p)=p+1 bzw #E(F_q)=q+1.
Daraus folgt (p+1)M $\equiv \infty$ mod p bzw (q+1)M $\equiv \infty$ mod p.
Wir haben nun alles zusammen um zu zeigen dass dC die ursprüngliche Nachricht ist.
de = 1+k(p+1)
dC=deM=(1+k(p+1))M=M+k(p+1)M=M+∞=M

Bemerkung: Das KMOV-Verfahren ist unabhängig von b.

Angenommen Bob wählt eine zufällige Kurve über Z. Dann muss Alice die Gruppenordnung bestimmen, zum Beispiel indem sie mit mod p oder mod q arbeitet. Falls p und q groß genug sind, ist dies schwer machbar. Wenn Bob eine Kurve fixiert, dann hat Alice es schwer Punkte auf der Kurve zu finden. Zum Beispiel könnte sie erst die x-Koordinate festlegen und dann y bestimmen. Dazu müsste sie aber die Quadratwurzel mod n berechnen, wovon wir wissen, dass das so hart wie das Faktorisierungsproblem ist. Wenn Bob a fixiert (in dem Fall a=0), erlaubt er Alice b zu wählen, sodass ihr Punkt auf der Kurve liegt. Dies erfordert, dass Bobs Wahl von e und d unabhängig von der Gruppenordnung von b ist, welches hier der Fall ist.