Cryptographie à courbes elli

Annexe du cours de sécurité et ré

Logarithmes discrets et co
elliptiques

- Problème du logarithme discret
  - crible général de corps de nombres : alg
    plus efficace actuellement
  - complexité : *exp^(1.9.n^(1/3).log(n)^(2/3*
    taille en bits
  - complexité sous-exponentielle
- Pourquoi un nouvel outil ?
  - complexité polynômiale avec la clé
  - complexité exponentielle pour attaquer

Logarithmes discrets et co elliptiques

- Faille du problème du logarithme disc
  - la multiplication modulaire est proche de multiplication sur les entiers
- Force des courbes elliptiques
  - la multiplication sur des courbes elliptiq pas proche de la multiplication sur les e
  - raison : on manipule des courbes qui ne continues dans le plan

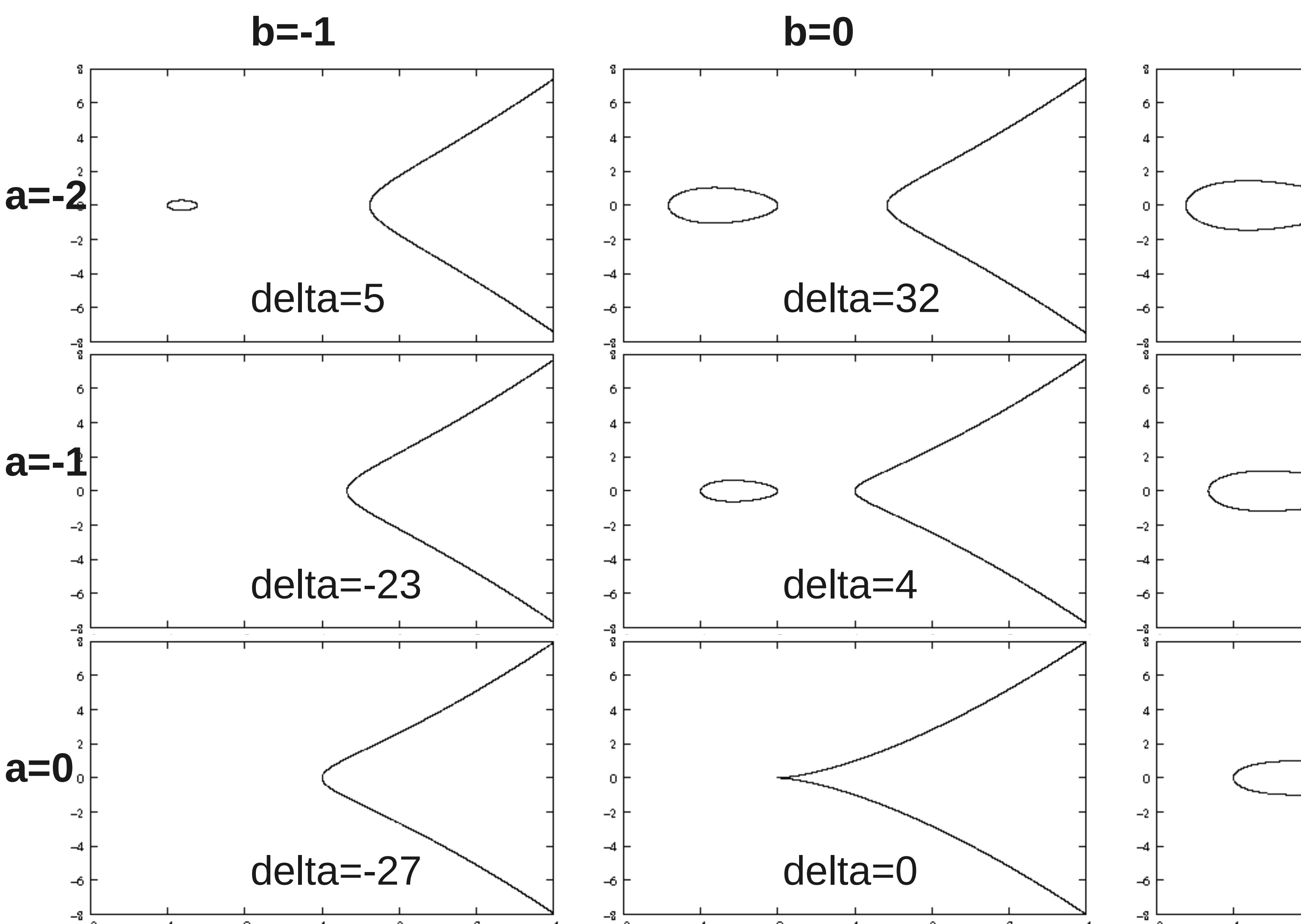
Robustesse

- Pour avoir 128 bits de sécurité, il faut
  - 3072 bits avec RSA
  - 256 bits avec une courbe elliptique
- Avril 2004 : 109 bits, 2600 machines
  17 mois (corps premier)
- Juillet 2009 : 112 bits, 200 machines
  3.5 mois (corps binaire)

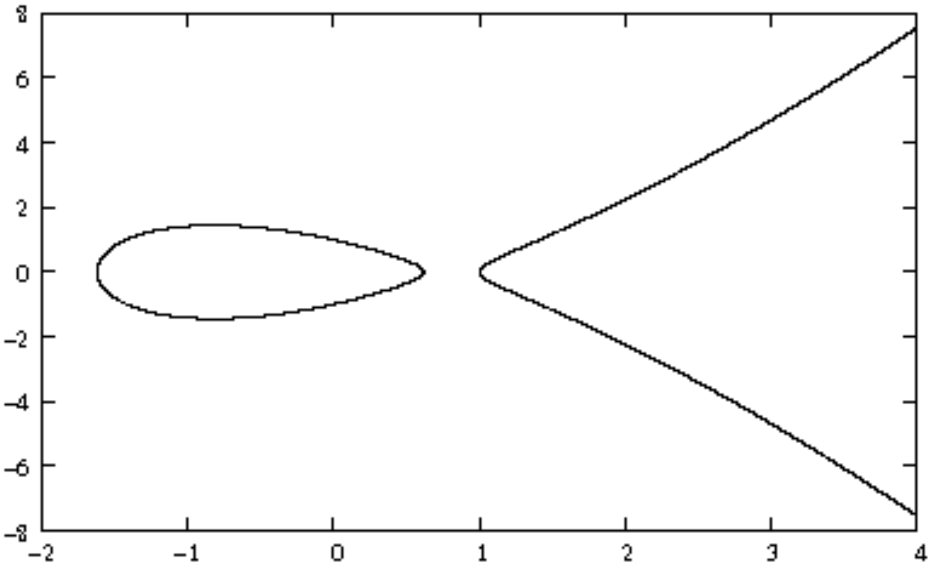
Définition

- Courbe elliptique $E(K)$
  - K corps de caractéristique différente de
    - le nombre d'éléments de K n'est pas 2^q o
    - utile pour les formules suivantes
  - courbe non singulière du type $y^2 = x^3$
  - Remarque : pour ax^3+bx^2+cx+d, $delt$
    $- 4ac^3 - 4b^3d - 27a^2.d^2 + 18.abcd$
  - discriminant de $x^3+a.x+b$: $delta = - 4.a$
  - courbe non singulière => $delta \neq 0$
  - $E(K)$ contient de plus un point spécial n

Exemples



Exemple avec *a*=-*2* et *b*

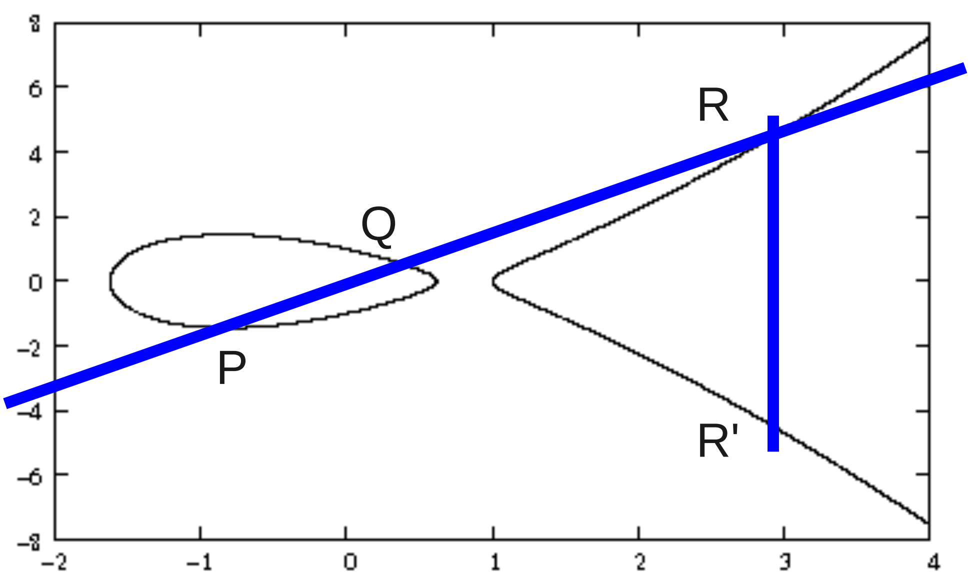


- Ne montre
point *Θ*
- *delta = 5*
- *delta* positi
courbe ave
composant
- *delta* négat
courbe ave
composant

Additions

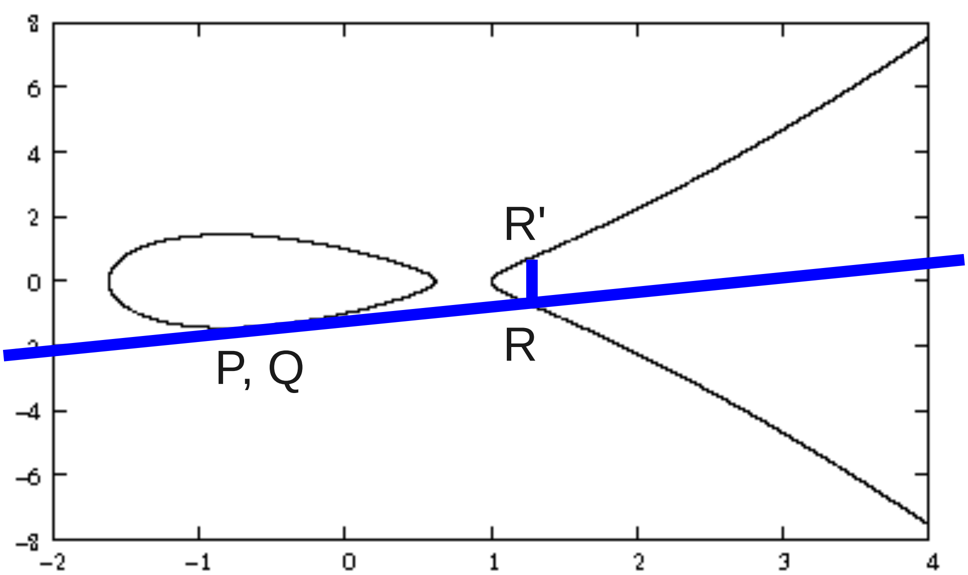
- Calculer $R = P + Q$
- Cas 1 : $P = \Theta$
  - $R = Q$
- Cas 2 : $Q = \Theta$
  - $R = P$

Additions (géométrique



- Cas 3 : $P \neq$
  $P \neq Q$
  - tracer la d
  - localiser le
    point d'int
  - calculer le
    R' par rap
    des abciss
  - $P+Q=R'$
  - (Θ est la t
    intersectio
    verticales)

Additions (géométrique



- Cas 4 : *P*≠
  P=*Q*
  - tracer la ta
    courbe en
  - localiser le
    point d'inte
  - calculer le
    R' par rap
    des abciss

Additions (analytiques

- Cas 3 : $P \neq \Theta$, $Q \neq \Theta$, $P \neq Q$
  - $x_R = lambda\hat{}2 - x_P - x_Q$
  - $y_R = lambda.(x_P - x_R) - y_P$
  - $lambda = (y_Q - y_P) / (x_Q - x_P)$
- Cas 4 : $P \neq \Theta$, $Q \neq \Theta$, $P = Q$
  - $x_R = lambda\hat{}2 - 2x_P$
  - $y_R = lambda.(x_P - x_R) - y_P$
  - $lambda = (3.x_P\hat{}2 + a) / (2.y_P)$

Multiplication scalaire

- Calculer $R = m.P$
  - pas la multiplication habituelle, puisque
    entier et P est dans K
  - utilisation du schéma de Horner
- Problème du logarithme discret sur c
  elliptique
  - P un point d'une courbe elliptique $E(K)$
  - Q un multiple de P sur $E(K)$
  - ordre de $E(K)$ est n (nombre d'éléments
  - trouver m tel que $Q = m.P$, avec $0 \leq m < n$

Paramètres pratiques do

- Cardinalité *q* du corps *K*
  - *K* est un corps premier ou un corps bina
  - corps premier : CG*(q)* avec *q* premier
  - corps binaire : *CG(2^r)*
    - caractéristique 2
    - formules précédentes non applicables
- Coefficients *a* et *b*
- Point de base *P* de *E(K)*, d'ordre *n*

Génération des clés

- Clé privée
  - d : entier aléatoire $1 \leq d < n$
- Clé publique
  - Q : point égal à $d.P$

Chiffrement et déchiffren

- Chiffrement
  - message M sur la courbe $E(K)$
  - choix d'un entier aléatoire $1 \leq k < n$
  - transmission du couple $(k.P, M + k.Q)=($
- Déchiffrement
  - P_2 - $d.P_1 = (M + k.Q) - d.k.P = M + k.d.$
    M

Signature

- Signer un message M avec deux fon
  hachage H et f
  - choisir un entier aléatoire $1 \leq k < n$
  - calculer $R = k.P$
  - $s = k^{-1} (h(M) - d.f(R))$ *modulo* n
- Vérifier la signature (R, s) d'un messa
  - $V_1 = f(R).Q + s.R$
  - $V_2 = h(M).P$
  - la signature est vérifiée si $V_1 = V_2$

Signature

- Preuve : une signature valide impliqu
  - $V_1 = f(R).Q + s.R$
    $= f(R).d.P + k^{-1}.(h(M) - d.f(R)).k.P$
    $= f(R).d.P + h(M).P - d.f(R).P$
    $= h(M).P$
    $= V_2$
- Preuve
  - il est difficile de trouver *s'* tel que *f(R).Q*
    h(M).P sans connaître *d* et *k*

Protocoles existants

- El Gamal sur des courbes elliptiques
  - utilise la cryptographie asymétrique pou
    des clés (plus sûr)
  - utilise la cryptographie symétrique pour
    communiquer (plus rapide)

Liens

- http://sage.mathematatik.uni-siegen.de
  home/pub/45/
- http://www.cc.gatech.edu/classes/AY
  cs8803g_spring/crypto17_1.ppt
- http://math.univ-bpclermont.fr/~reboll
  page-fichiers/projetMichael.pdf