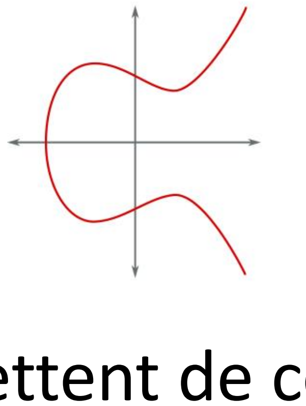
Partie « cryptog
courbes elliptiq

Alexandre Guitt

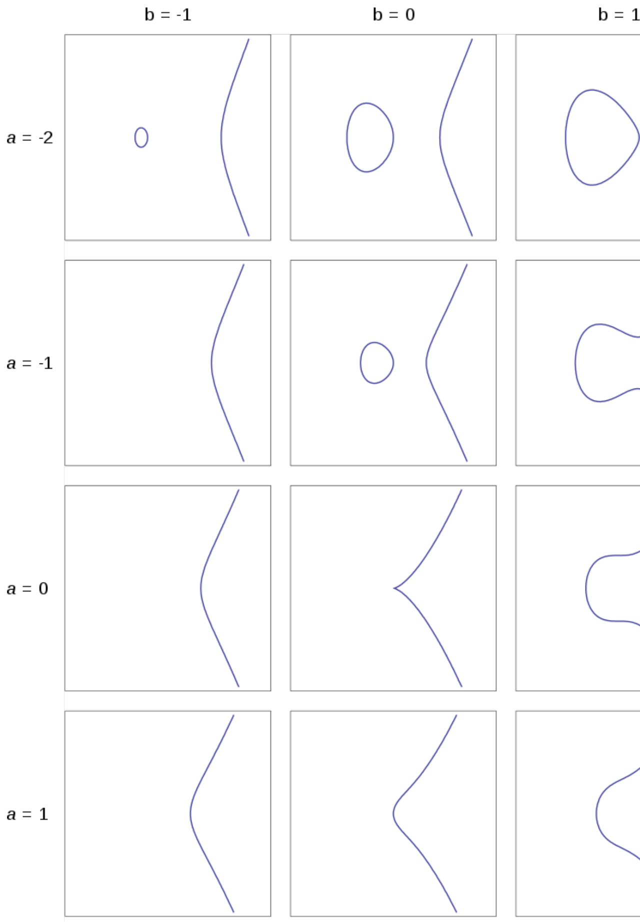
Introduction brève

- Les courbes elliptiques sont des courbes mathématiques intéressantes



- Les courbes elliptiques permettent de c cryptographiques asymétriques efficace
  - Avec des clés plus petites que les protocole qui se basent sur l'arithmétique modulaire

Plusieurs exemples de cour



Rappel sur les protocoles a

- Dans un protocole cryptographique asy
  clé publique et une clé privée
- Confidentialité (ex : RSA)
  - La clé publique sert à chiffrer, la clé privée
  - RSA étant lent, il sert davantage pour la sig
    chiffrement
- Intégrité (ex : RSA et fonction de hachag
  - La clé privée sert à signer, la clé publique s
- Echange de secret (ex : Diffie-Hellman)
  - Les deux partenaires échangent des inform
    publique, et calculent un secret partagé en

Efficacité de RSA

- En 2021, la taille des clés RSA recomman
  - Pour information, le record de factorisation
    soit un nombre à factoriser de 250 chiffres
    https://en.
- Cela signifie que toutes les opérations q
  chiffrement, déchiffrement, signature, e
  - C’est long… surtout pour les ordinateurs ay
    téléphones portables, montres connectées
- Pourquoi faut-il des clés aussi longues ?
- Comment concevoir un protocole plus e

Pourquoi faut-il des clés au
RSA ? (1/2)

- Une clé RSA valide est un produit de deu
  certains nombres ne sont pas des clés v
  - Par exemple, 2021 est une clé RSA valide (2
  - Mais, 2022 n’est pas une clé RSA valide (20
- Donc, le nombre de clés RSA valides est
  de la clé RSA
  - Par exemple, si la clé RSA faisait 8 bits, il n’
    2^8=256 entiers. Un algorithme de cryptana
    clés pour trouver la bonne.
  - Si la clé RSA faisait 16 bits, il n’y aurait qu’à
    nombres)

Pourquoi faut-il des clés au
RSA ? (2/2)

- De plus, l'algorithme actuel le plus rapic
est assez efficace
  - Il s'appelle le crible généralisé du corps des
  - Sa complexité est $\exp\left(\left(\sqrt[3]{\frac{64}{9}} + o(1)\right)(\ln n)^{\frac{1}{3}}(\ln \ln$

https://en.wik

  - Pour une clé de 1024 bits, il faut 2^{86} opérat
  - Pour une clé de 2048 bits, il faut 2^{116} opéra
bits
- (Remarque : dans les algorithmes de chi
DES ou AES, une clé de 128 bits fournit

Vers un protocole plus effic

- L'attaque principale de RSA est liée à la f
  faut trouver un nouveau protocole qui r
  factorisation des nombres entiers
- Et on doit trouver une fonction qui est :
  - Facile à calculer dans un sens (c'était l'expo
  - Difficile à calculer dans l'autre sens (c'était
  - Qui possède une faille (c'était la connaissan
    permet une énorme simplification du calcu

Les courbes elliptiques

- Les courbes elliptiques sont des fonctio
  particulières
  - Elles correspondent à des équations de la f
  - … avec quelques contraintes supplémentai
- La cryptographie sur courbes elliptiques
  - Que l'opération de multiplication (voir plus
  - Que l'opération inverse (appelée « logarith
    elliptiques ») est très difficile à calculer
  - Que l'opération inverse possède une faille
    possède certaines informations

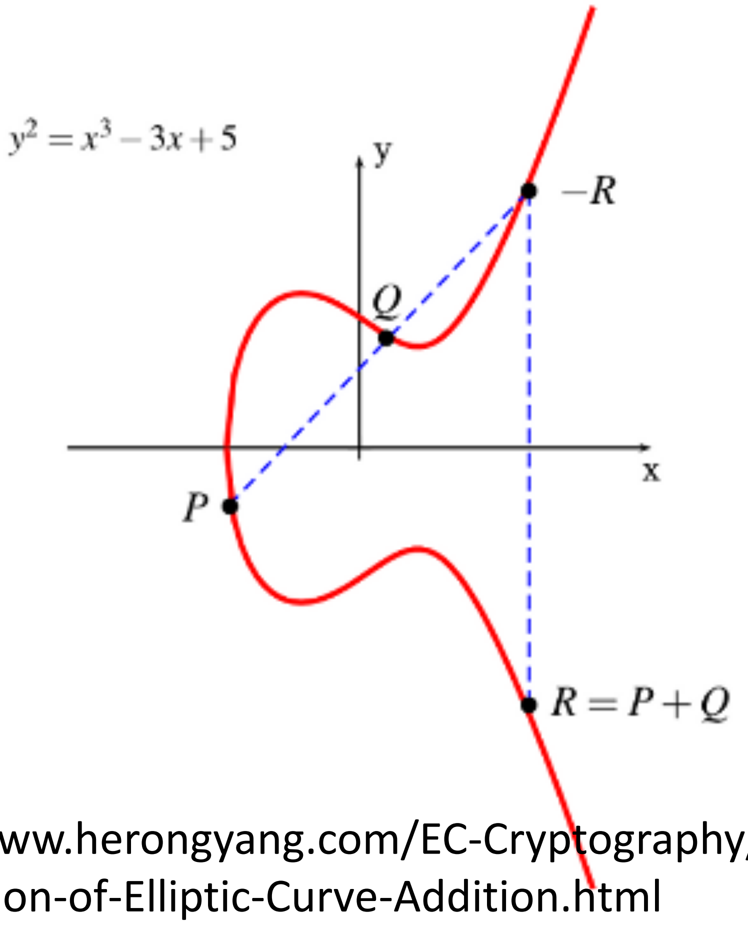
Préalable : les groupes cycl

- Les courbes elliptiques se basent sur la not
  cyclique (cette notion est d'ailleurs très pré
- En algèbre, un groupe cyclique est un grou
  monogène
  - La loi « + » doit être interne (pour tous a et b d
  - La loi « + » est associative (pour tous a, b et c,
  - La loi « + » possède un élément neutre noté e
  - La loi « + » possède un symétrique (pour tout a
    notera –a
  - Le nombre d'éléments de G est fini
  - G possède un élément g tel que tout élément d
- Un (sous-)groupe cyclique G est donc égal a

Points d’une courbe ellipti

- Une courbe elliptique est (presque) l’en
  l’équation suivante $y^2 = x^3 + ax + b$
  - On ajoute un point (que l’on peut imaginer
- On va ensuite définir deux opérations :
  - L’addition de deux points P et Q, notée « P
  - La multiplication d’un point P par un entier

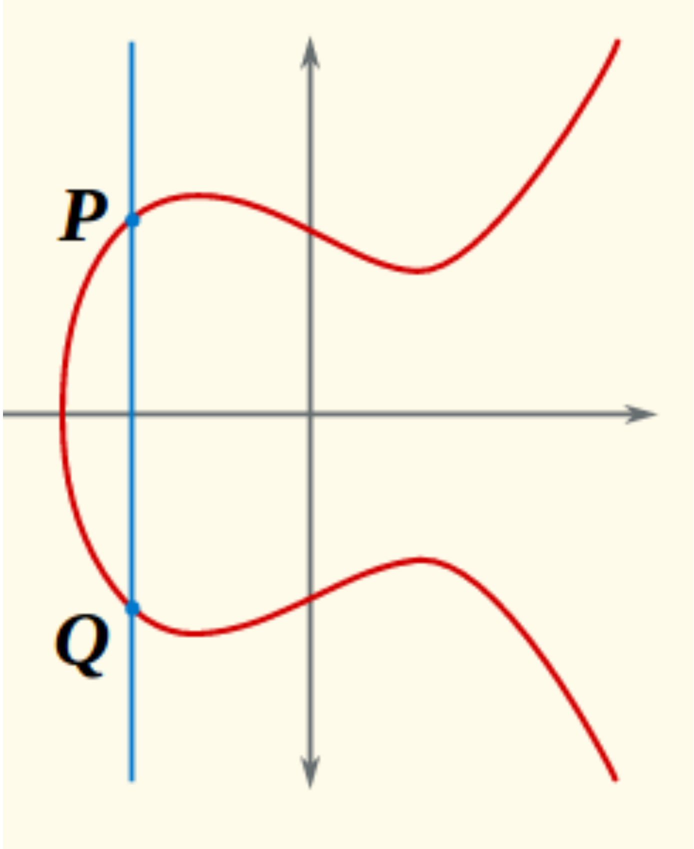
Addition de deux points P (



- Ap

http://www.herongyang.com/EC-Cryptography/Algebraic-Description-of-Elliptic-Curve-Addition.html

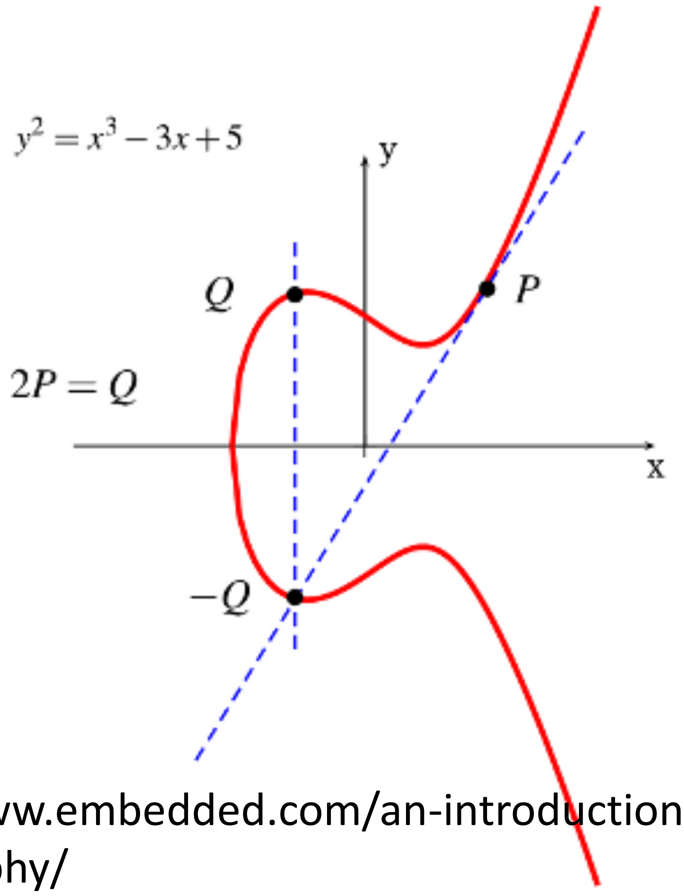
Addition de deux points P



https://electriccoin.co/blog/snark-explain7/

- Ap

Addition de deux points P (



https://www.embedded.com/an-introduction-to-elliptic-curve-cryptography/

- Ap
  -
  -
  -
  -

Multiplication d’un point P

- On cherche à calculer Q=k.P
  - On développe : Q=P+P+P+…+P (k fois)
  - On calcule P+P=2.P, puis (2.P)+P=3.P, puis (
- Remarque :
  - On peut aller plus rapidement en utilisant
  - Exemple : pour calculer 9.P, on peut calcule
    - 2.P => coûte une addition
    - Puis 4.P=2.P+2.P => coûte une addition
    - Puis 8.P=4.P+4.P => coûte une addition
    - Puis 9.P=8.P+P => coûte une addition

Signatures

- Elliptic Curve Digital Signature Algorithm
- Génération des clés :
  - Alice choisit une courbe elliptique (a, b, p,
  - Alice choisit un entier aléatoire s entre 1 et
  - La clé privée est s
  - La clé publique est Q=s.P
- Signature d'un message M par Alice :
  - Alice choisit un nombre aléatoire k entre 1
  - Alice envoie (i [n], k^{-1}(H(M)+s.i [n]))
- Vérification par Bob :
  - Bob calcule le point (H(M).y^{-1} [n]).P+(x.y^{-1} [

Echange de clés

- Elliptic Curve Diffie-Hellman (ECDH)
- Alice et Bob s’accordent sur une courbe
- Alice et Bob ont chacun leur clé privée,
  - Ces clés peuvent être créées pour l’occasio
- La clé partagée est : $\text{priv}_{\text{Alice}}.\text{priv}_{\text{Bob}}.P$
  - Alice la calcule avec $\text{priv}_{\text{Alice}}.\text{pub}_{\text{Bob}}$
  - Bob la calcule avec $\text{priv}_{\text{Bob}}.\text{pub}_{\text{Alice}}$

Complication…

- Malheureusement, ce n’est pas du tout
  courbes elliptiques définies sur des réel
    - Et la méthode géométrique n’est pas très p
    - On va donc utiliser des courbes elliptiques
    - Et on va aussi se limiter à des entiers codé
      on va travailler en arithmétique modulaire
    - L’équation devient : $y^2 = x^3 + ax + b$
- On va utiliser une approche analytique (

Méthode analytique pour points (1/3)

- Entrée :
  - Les valeurs de a, b et p dans : $y^2 = x^3 +$
  - Hypothèse : a et b sont tels que : $4a^3 + 2$
  - Les coordonnées du point générateur P so
- Exemple : p=17, a=2, b=2, P=(5,1), n=19 groupe cyclique

Méthode analytique pour
points (2/3)

- Addition de A et B, avec A et B différent
  - On calcule $s = (y_A-y_B).((x_A-x_B)^{-1})$ [p]
  - On a $x_C = s^2-(x_A+x_B)$ [p]
  - On a $y_C = s(x_A-x_C)-y_A$ [p]
- Addition de A et B, avec A=B
  - On calcule $s = (3x_A{}^2+a).((2y_A)^{-1})$ [p]
  - On a $x_C = s^2-2x_A$ [p]
  - On a $y_C = s(x_A-x_C)-y_A$ [p]
- Remarque : si on essaye de calculer 0^{-1} [

Méthode analytique pour points (3/3)

- Exemple 1 : Calcul de 2.P, avec p=17, a=2, b=2,
  - On doit calculer P+P
  - $s_1 = 3x_P{}^2+a$ [p] = 3.5^2+2 = 77 = 9 [17]
  - $s_2 = (2y_P)^{-1}$ [p] = $(2.1)^{-1} = 2^{-1}$ [17], et 2.9 = 18 = 1 [17]
  - $s = s_1.s_2$ [p] = 9.9 = 81 = 13 [17]
  - $x_{2.P} = s^2\text{-}2x_P$ [p] = 13^2-2.5 = 169-10 = 159 = 6 [17]
  - $y_{2.P} = s(x_P\text{-}x_{2.P})\text{-}y_P$ [p] = 13.(5-6)-1 = -14 = 3 [17]
- Exemple 2 : Calcul de 3.P
  - On doit calculer P+2.P
  - $s_1 = y_P\text{-}y_{2.P}$ [p] = 1-3 = -2 = 15 [17]
  - $s_2 = (x_P\text{-}x_{2.P})^{-1}$ [p] = $(5\text{-}6)^{-1} = (\text{-}1)^{-1} = 16^{-1}$ [17], et 16.1
  - $s = s_1.s_2$ [p] = 15.16 = 240 = 2 [17]
  - $x_{3.P} = s^2\text{-}(x_P+x_{2.P})$ [p] = 2^2-(5+6) = 4-11 = -7 = 10 [17]
  - $y_{3.P} = s(x_P\text{-}x_{3.P})\text{-}y_P$ [p] = 2.(5-10)-1 = -11 = 6 [17]

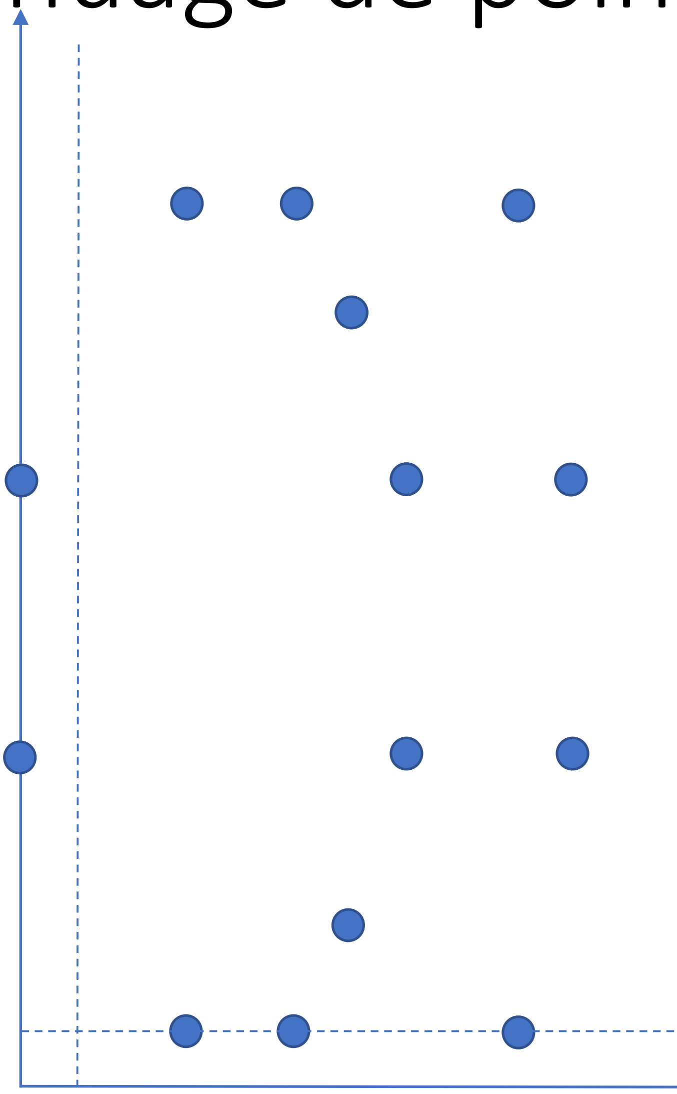
Rappel : calcul de l’inverse modulaire (1/2)

- Algorithme d’Euclide étendu, de comple
  - Entrée : a et b
  - Sortie : (r, u, v) tels que a*u+b*v=r, avec r=
  - (r, u, v, r’, u’, v’) ← (a, 1, 0, b, 0, 1)
  - Tantque r’<>0 faire
    - q ← r/r’
    - (r, u, v, r’, u’, v’) ← (r’, u’, v’, r-q*r’, u-q*u’, v-q*v
  - Retourner (r, u, v)

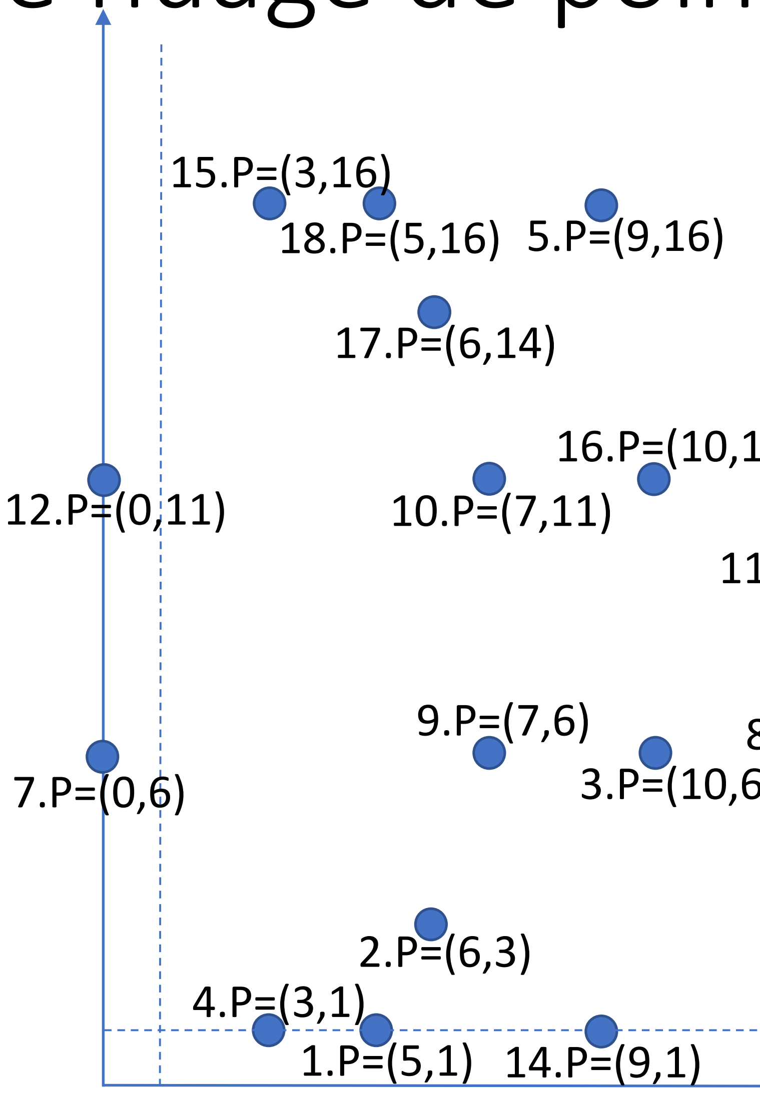
Rappel : calcul de l’inverse modulaire (2/2)

- Application au cas de l’inverse de a mod
  - On cherche b tel que a*b+p*k=r, avec r=PG
- Exemple : on cherche l’inverse de a=2 m
  - (r, u, v, r’, u’, v’) ← (a, 1, 0, p, 0, 1) = (2, 1, 0
  - q ← r/r’ = 2/17 = 0
  - (r, u, v, r’, u’, v’) ← (17, 0, 1, 2-0*17, 1-0*0,
  - q ← r/r’ = 17/2=8
  - (r, u, v, r’, u’, v’) ← (2, 0, 1, 17-8*2, 0-8*1, 1
  - q ← r/r’ = 2/1 = 2
  - (r, u, v, r’, u’, v’) ← (1, -8, 1, 2-2*1, 0-2*(-8),
  - r’ vaut 0 donc la valeur recherchée est u =

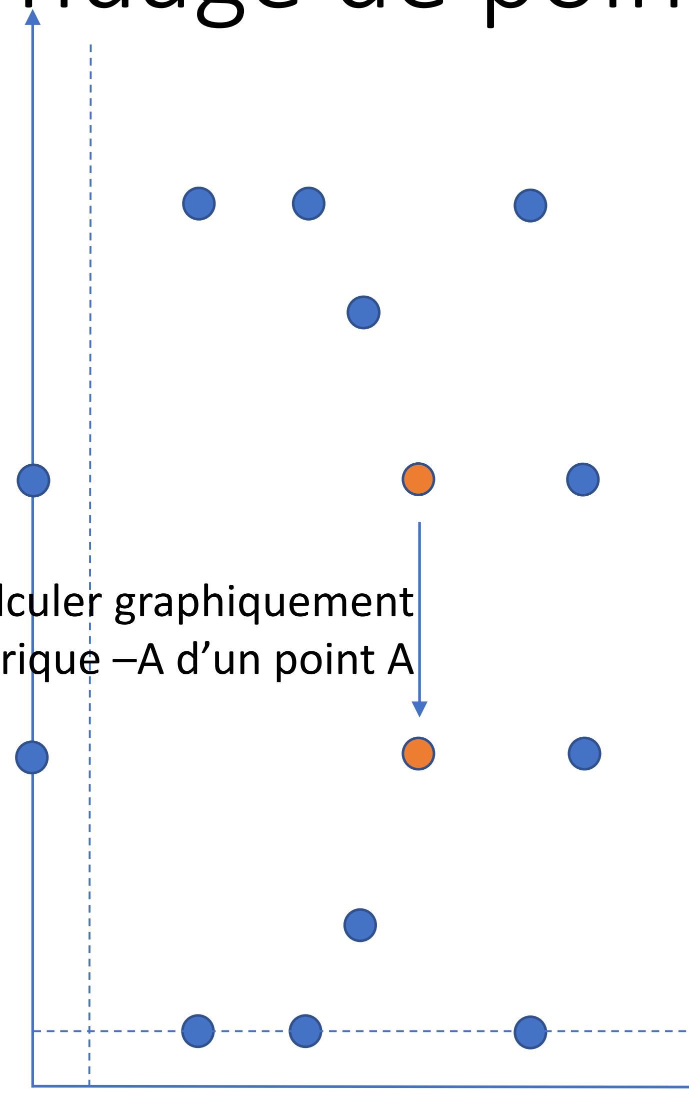
Exemple de nuage de point



Exemple de nuage de poin



Exemple de nuage de poin

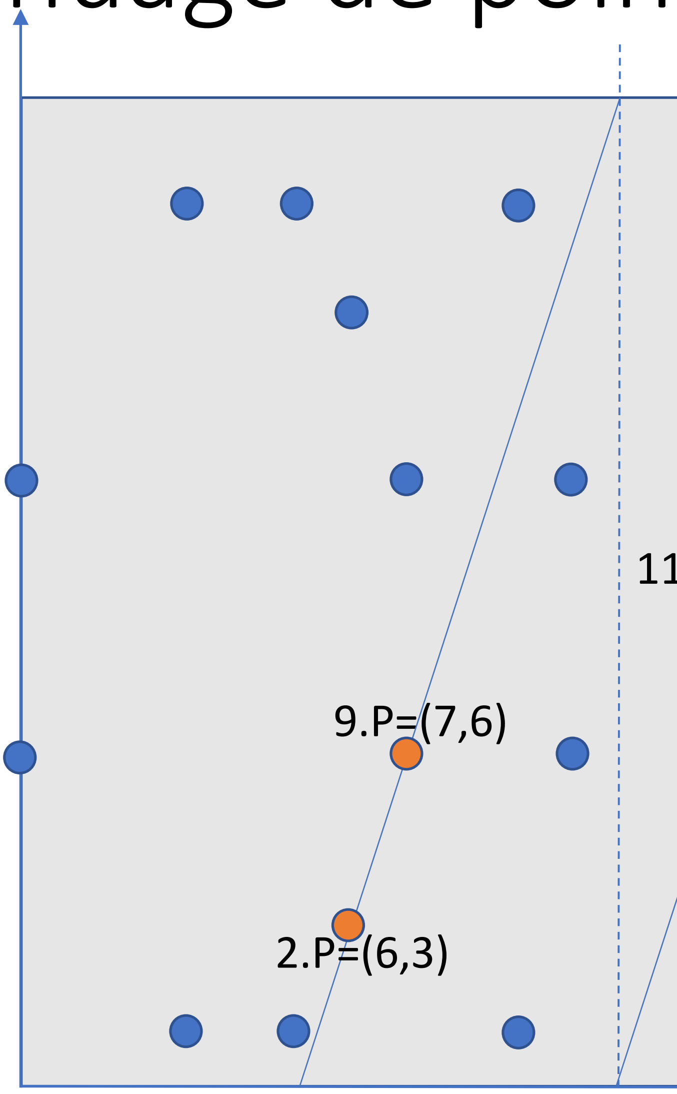


On peut toujours calculer graphiquement
le symétrique –A d'un point A

Exemple de nuage de poin

On peut toujours calculer graphiquement le point A+B, mais il faut « *wrapper* » la droite (AB)

Cette méthode reste peu précise



Attaques sur les courbes el

- Les seules attaques connues sur les cou
  attaques sur les groupes cycliques
  - Attaque *baby step giant step* [Shanks, 1971
    l’ordre du groupe
  - Attaque rho de Pollard [Pollard, 1978] : con
    du groupe
- Pour atteindre la même sécurité avec un
  RSA, on peut prendre une taille de clé p
  - Pour atteindre 80 bits de sécurité, il faut un
    sur 160 bits (la complexité pour cryptanaly
    au lieu de 1024 bits dans RSA)

Attaque *baby step giant ste*

- On connaît P et Q tels que Q=k.P, et on
- On pose m=ceil(sqrt(n))
- On calcule i.P pour tout 0<=i<m
- On calcule Q-j.m.P pour tout 0<=j<m
- Dès qu'on trouve une correspondance e déduit que k=i+j.m
- La complexité est O(sqrt(n)) en nombre elliptique (c'est-à-dire, sans la recherche

Attaque *baby step giant ste*

- Exemple :
  - On connaît P=(5,1) et Q=(7,6), et on cherch
  - On pose m=ceil(sqrt(n))=ceil(sqrt(19))=5
  - On a 0.P = infinity, 1.P=(5,1), 2.P=(6,3), 3.P=
  - On a Q-0.m.P=Q=(7,6)
    Q-1.m.P=Q-5.P=Q+14.P=4.P=(3,1)
    Q-2.m.P=Q-10.P=Q+9.P=(5,16)
    Q-3.m.P=Q-15.P=(16,4)
    Q-4.m.P=Q-20.P=Q-P=(13,7)
  - La correspondance est entre i=4 (car 4.P=(3
    calcule k=4+1*5=9, ce qui est bien la valeu

Comment choisir les param
courbe elliptique ?

- Des courbes pré-calculées existent
  - Leurs paramètres a, b et p sont calculés po
ordre important
  - Ex : Curve25519 : a=486662, b=1, p=2^252
de sécurité
  - Ex : NIST P-256 : a=-3, b=410(…)291, p=2^2
fournissant 128 bits de sécurité
  - Pour calculer l'ordre du sous-groupe cycliq
l'algorithme de Schoof, qui donne l'ordre N
peut trouver assez facilement des sous-gro
un diviseur de N, ainsi que le point générat
  - Les paramètres sont choisis de manière à é