DE LA RECHERCHE À L'INDUSTRIE

cea

www.cea.fr

leti & list

Les courbes elliptiques en cryptographie

Christine HENNEBERT

Fil rouge

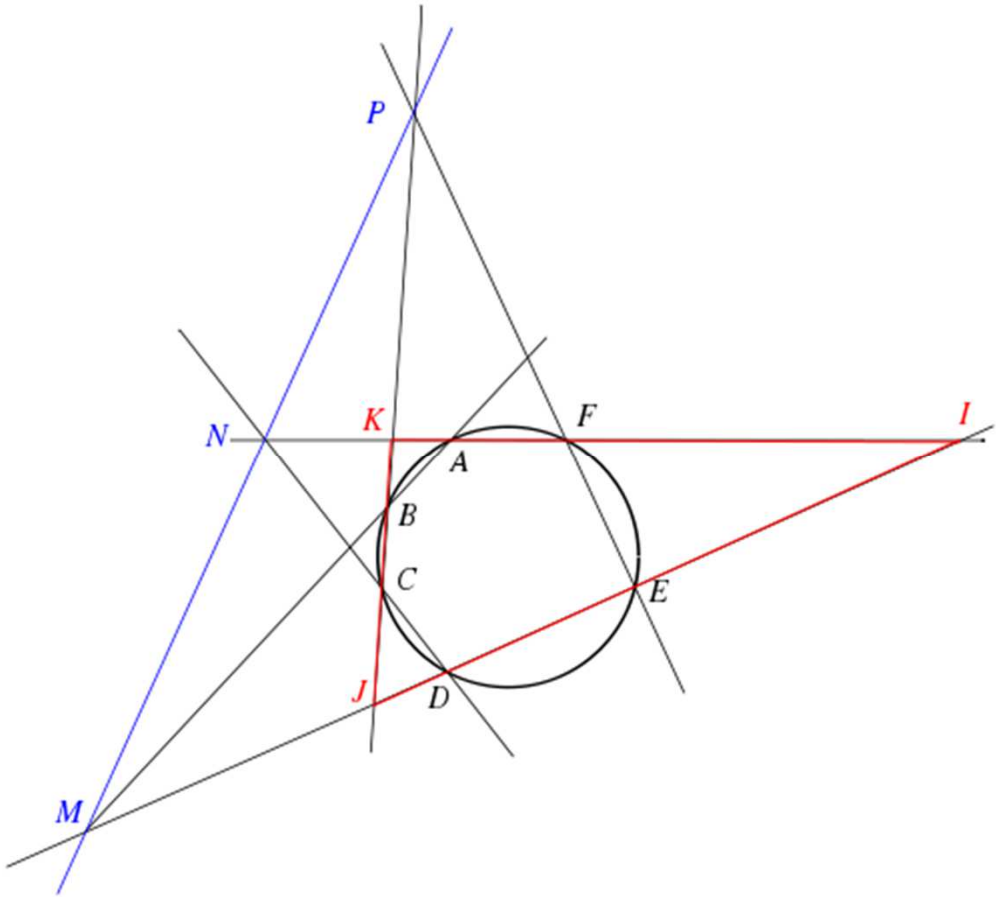
- Un peu de géométrie…
- Et la cryptographie dans tout ça ?
- Est-ce bien « secure » ?

UN PEU DE GÉOMÉTRIE…

CONSTRUCTION D'UNE COURBE ELLIPTIQUE

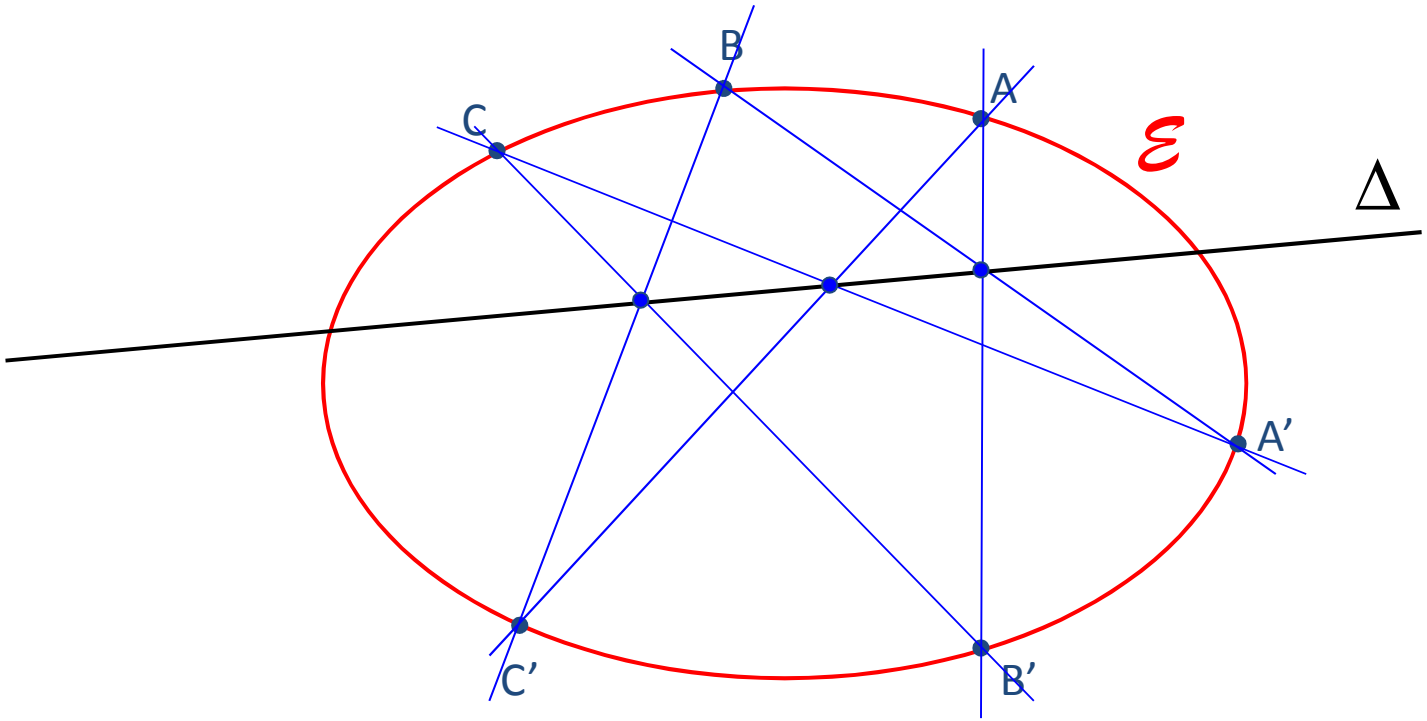
Le théorème de Pascal

- Étant donné un hexagone inscrit dans une ellipse, les intersections des côtés opposés sont alignées



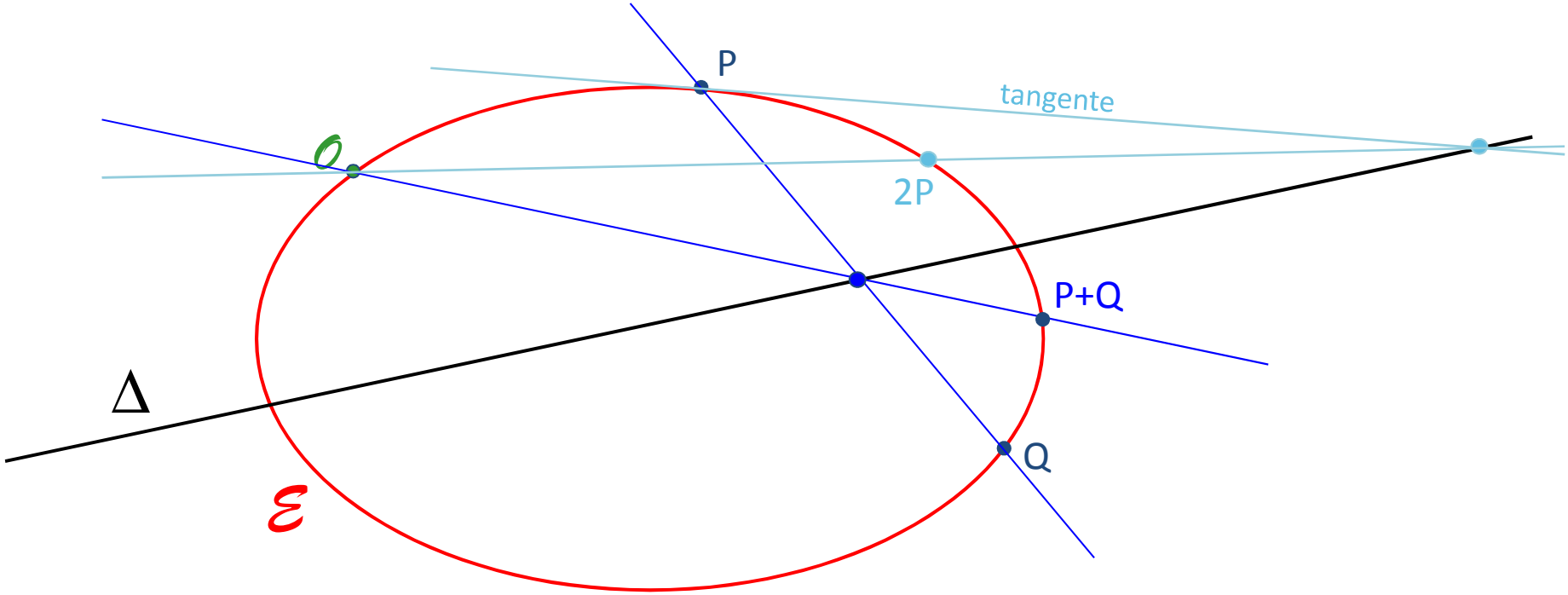
Corollaire du théorème de Pascal

- Considérons une ellipse



Autour du théorème de Pascal

- Soit une ellipse $\mathcal{E}$ et une droite Δ privées de leurs intersections
- Soit $\mathcal{O}$ un point de l'ellipse



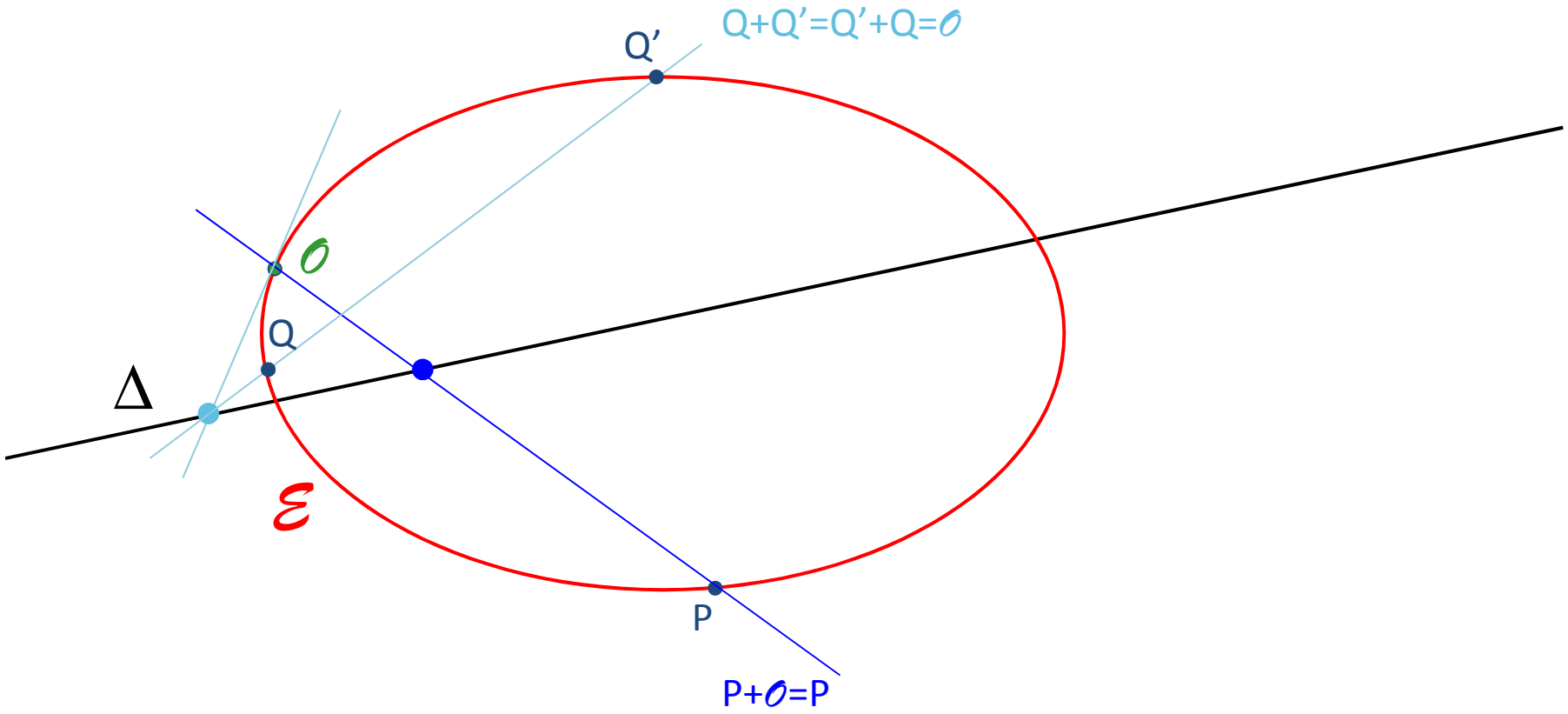
1) Opérateur + : P+Q

2) Opérateur 2P : P+P

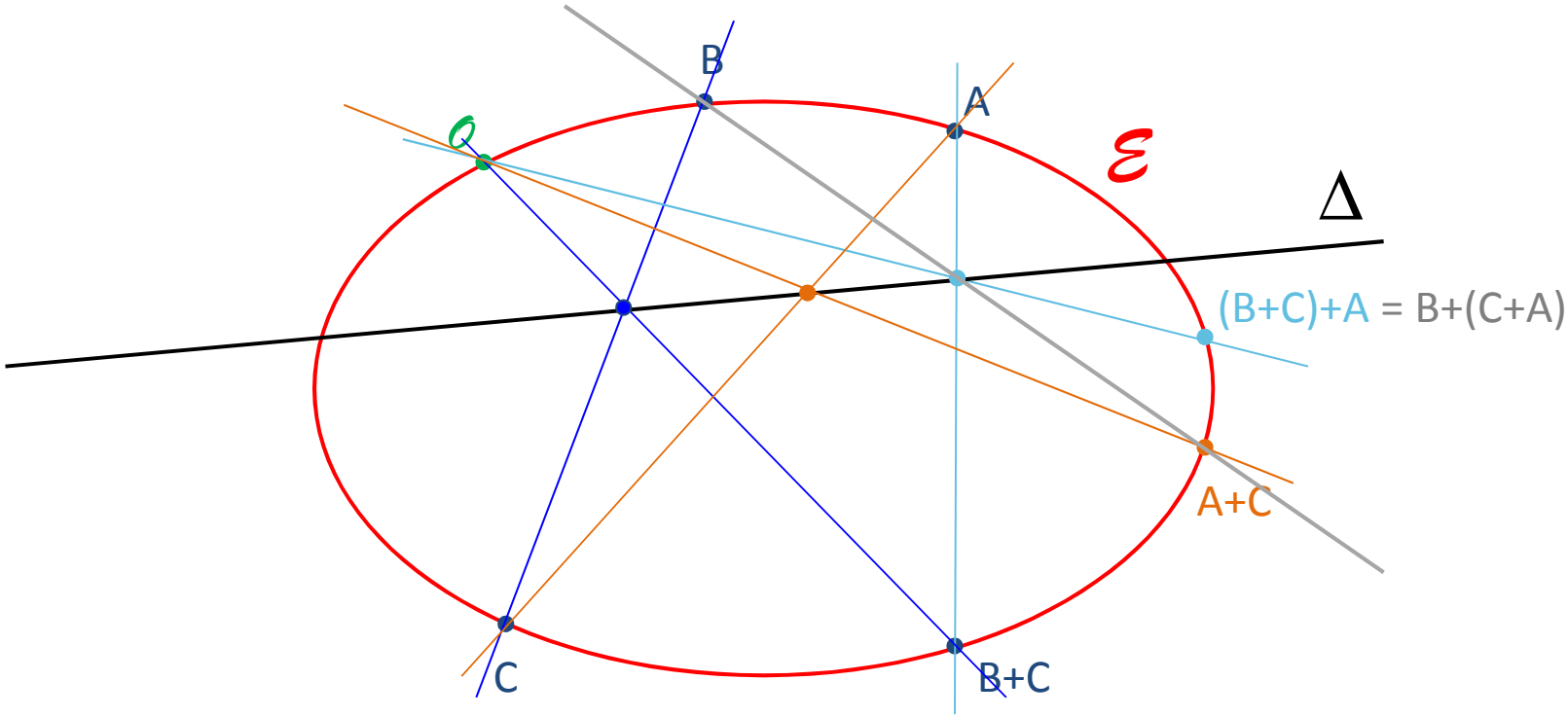
De la géométrie à l'algèbre

- Définition d'un groupe
  - Un ensemble E
  - Une opération interne $\star$ dans E qui vérifie :
    - Associativité : $(x \star y) \star z = x \star (y \star z)$
    - Existence d'un élément neutre e : $\forall x \in \mathrm{E}$, $x \star e = e \star x = x$
    - Existence d'un inverse : $\forall x \in \mathrm{E}, \exists x'$ tel que $x \star x' = x' \star x = e$
- On va montrer que :
  - $\mathcal{E} \setminus \Delta$, muni de la loi +, est un groupe commutatif
  - L' élément neutre est $\mathcal{O}$
    - $\mathcal{O}$+P = P
    - Q+Q' = Q'+Q = $\mathcal{O}$
    - A+(B+C) = (A+B)+C
    - Commutativité : A+B = B+A

Elément neutre & Inverse



Associativité



Mise en équation…

Théorème : $\mathcal{E} \setminus \Delta$, muni de la loi +, est un groupe commutatif dont l' élément neutre est $\mathcal{O}$

Pour montrer ce résultat, on a utilisé la réunion $\mathcal{E} \cup \Delta$ de la courbe et de la droite :

$$\mathcal{E} = \{(x, y) \in \mathbb{R}^2 \mid P_2(x, y) = 0\}$$

$$\Delta = \{(x, y) \in \mathbb{R}^2 \mid P_1(x, y) = 0\}$$

où P_i est un polynôme de degré total i .

Donc :

$$\mathcal{E} \cup \Delta = \{(x, y) \in \mathbb{R}^2 \mid P_1(x, y)P_2(x, y) = 0\}.$$

C'est une **cubique** !

On a aussi utilisé le point à l'infini…

Quelques notions de géométrie

Droite : $a\,x + b\,y + c = 0$

Conique : $a\,x^2 + b\,xy + c\,y^2 + d\,x + e\,y + f = 0$

L'ellipse est une conique

Cubique : polynôme de degré 3

$a\,x^3 + b\,x^2y + c\,xy^2 + d\,y^3 + e\,x^2 + f\,xy + g\,y^2 + h\,x + i\,y + j = 0$

Courbe elliptique : cubique irréductible sans point singulier

irréductible : polynôme non factorisable

point singulier: point où la dérivée partielles en x et en y s'annulent simultanément

Équation de Weierstrass…

Equation de Weierstrass

Une courbe elliptique $\mathcal{E}$, définie sur un corps **K**, est une cubique irréductible, non singulière (ou lisse), définie dans le plan projectif $\mathbb{P}^2(\mathbf{K})$ comme l'ensemble des solutions (X, Y, Z) de l'équation de **Weierstrass** homogène :

$$\mathcal{E} : Y^2Z + a_1 XYZ + a_3 Y Z^2 = X^3 + a_2 X^2Z + a_4 XZ^2 + a_6 Z^3$$

La courbe $\mathcal{E}$ n'admet qu'un point de coordonnée Z=0, le point P=(0, 1, 0) qui est appelé point à l'infini et noté $\mathcal{O}$.

On utilise généralement la représentation affine de cette équation en faisant correspondre à tout point P = (X, Y, Z) solution de l'équation homogène, le point p(x, y) = p($\frac{X}{Z}$, $\frac{Y}{Z}$) solution de l'équation affine :

$$\mathcal{E} = \{ (x, y) \in \mathbf{K}^2 \mid y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \} \cup \{ \mathcal{O} \}$$

Equation d'une courbe elliptique

Par changements de variable successifs, on peut simplifier l'équation $\mathcal{E}$.

On obtient l'équation de la courbe utilisée en cryptographie pour les champs premiers (définie sur $\mathbb{Z}/p\mathbb{Z}$ avec p premier) :

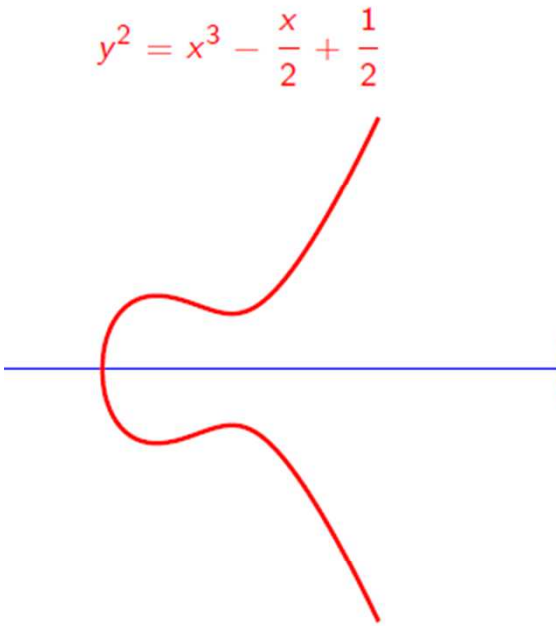
$$\mathcal{E} : y^2 = x^3 + a\,x + b \;\cup\; \mathcal{O}$$

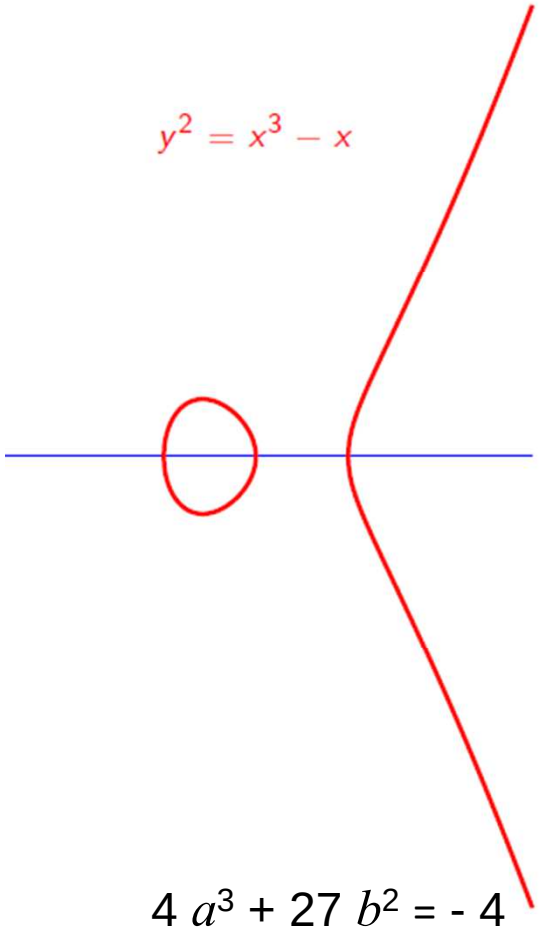
Parce que $\mathcal{E}$ est lisse et n'admet pas de racines double ni triple, a et b doivent vérifier la relation :

$$4\,a^3 + 27\,b^2 \neq 0$$

On peut remarquer que la courbe est symétrique par rapport à l'axe des abscisses...

Graphe d'une courbe elliptique





$a = b = 0$

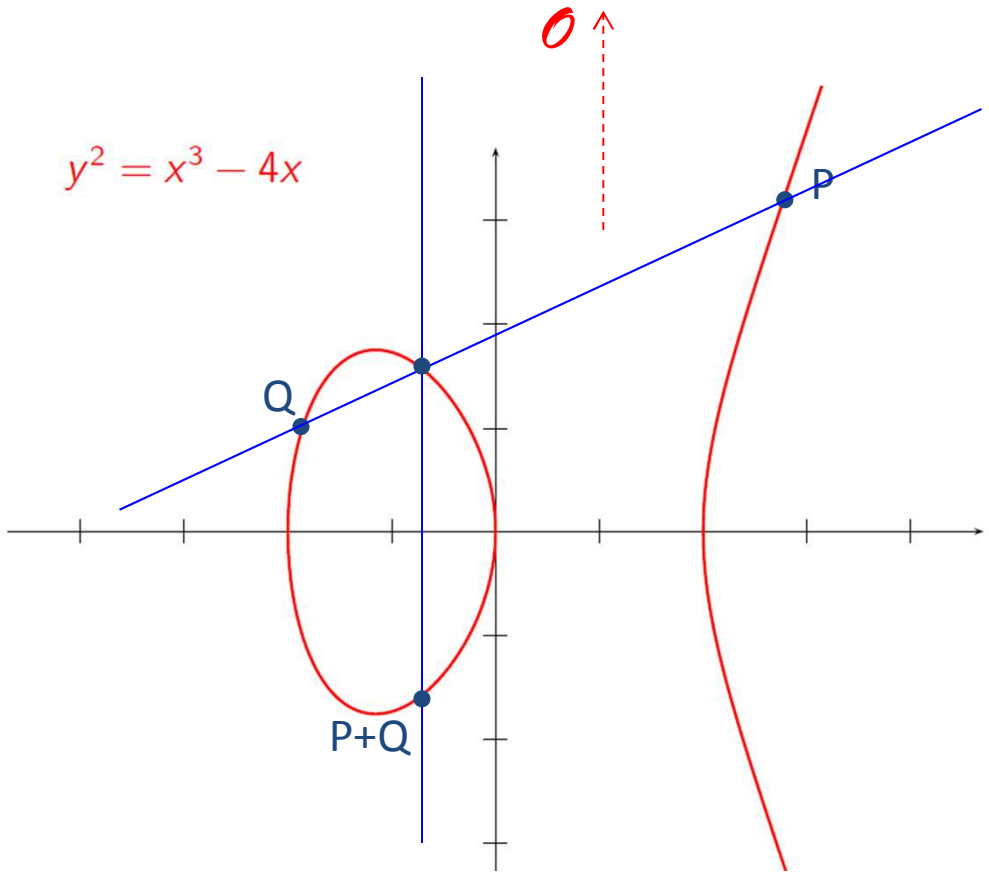
$4\,a^3 + 27\,b^2 = 6{,}25$

$4\,a^3 + 27\,b^2 = 0$

$4\,a^3 + 27\,b^2 = -4$

Propriétés d'une courbe elliptique

On munit $\mathcal{E}$ d'une structure de groupe commutatif + telle que $\mathcal{O}$ soit l'élément neutre…

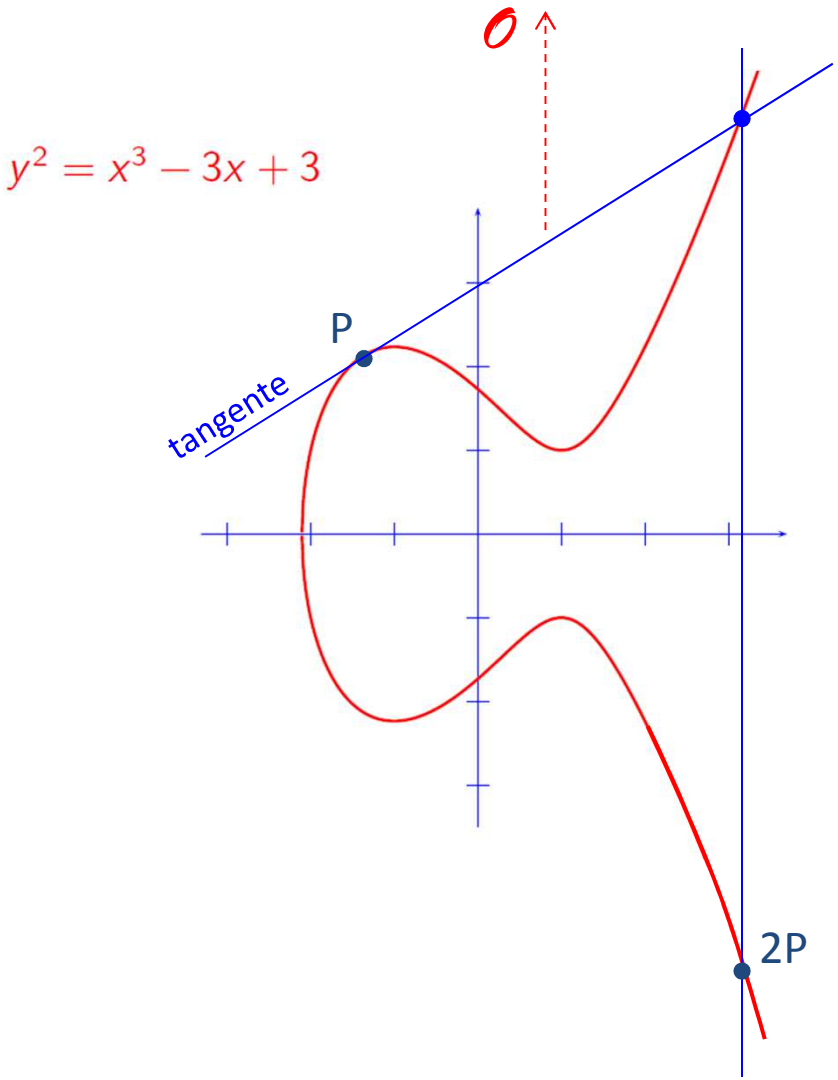


Du groupe au corps…

- Définition d'un corps
  - Un ensemble E
  - Une opération interne $+$ telle que $(\mathrm{E},+)$ forme un groupe commutatif dont l'élément neutre est O
  - Une opération interne $\times$ dans $\mathrm{E}^* = \mathrm{E} \setminus \{\mathrm{O}\}$ telle que $(\mathrm{E}, \times)$ forme un groupe
  - La loi $\times$ est distributive sur la loi $+$ soit : $x \times (y + z) = x \times y + x \times z$

- On va montrer que $\mathcal{E}$ est un corps :
  - $\mathcal{E}$ est un groupe commutatif pour la loi + dont l'élément neutre est $\mathcal{O}$
  - On munit $\mathcal{E} \setminus \{\mathcal{O}\}$, de la loi $\times$ telle que $(\mathcal{E}, \times)$ soit un groupe

Doublement d'un point



Formules analytiques

Calcul de l'inverse de P : $\boxed{\begin{cases} x_{-P} = x_P \\ y_{-P} = -y_P \end{cases}}$

Calcul de P + Q : $\boxed{\begin{cases} x_{P+Q} = \lambda^2 - x_P - x_Q \\ y_{P+Q} = \lambda(x_P - x_{P+Q}) - y_P \end{cases}}$ avec $\lambda = \frac{y_Q - y_P}{x_Q - x_P}$

Calcul du doublement [2]P : $\boxed{\begin{cases} x_{[2]P} = \lambda^2 - 2x_P \\ y_{[2]P} = \lambda(x_P - x_{[2]P}) - y_P \end{cases}}$ avec $\lambda = \frac{3x_P^2 + a}{2y_P}$

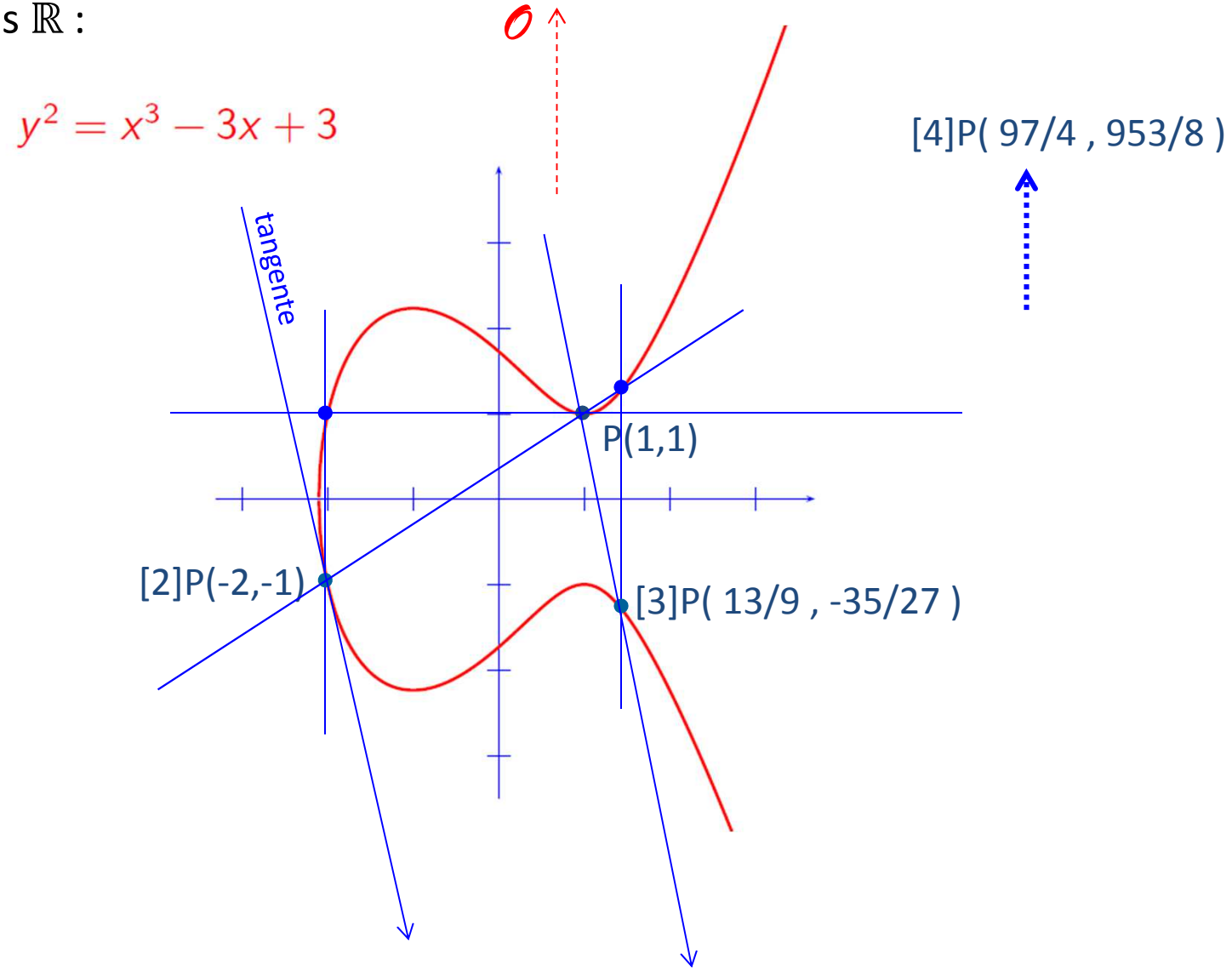
On peut travailler sur n'importe quel corps :

par exemple $\mathbb{Q}$ ou $\mathbb{R}$ ou $\mathbb{Z}/p\mathbb{Z}$ avec p premier

Il suffit de prendre P et Q dans ce corps

Multiple d'un point

Dans $\mathbb{R}$:



Point de torsion

Définition : Un point P est dit de **torsion** s'il existe un entier naturel non nul **m** tel que **[m]P = $\mathcal{O}$**

Dans $\mathbb{Z}/7\mathbb{Z}$ (corps fini premier) :

$\mathcal{E} : y^2 = x^3 - 3x + 3$

P = (1, 1)

[2]P = (-2, -1) mod 7 = (5, 6)

[3]P = (3, 0)

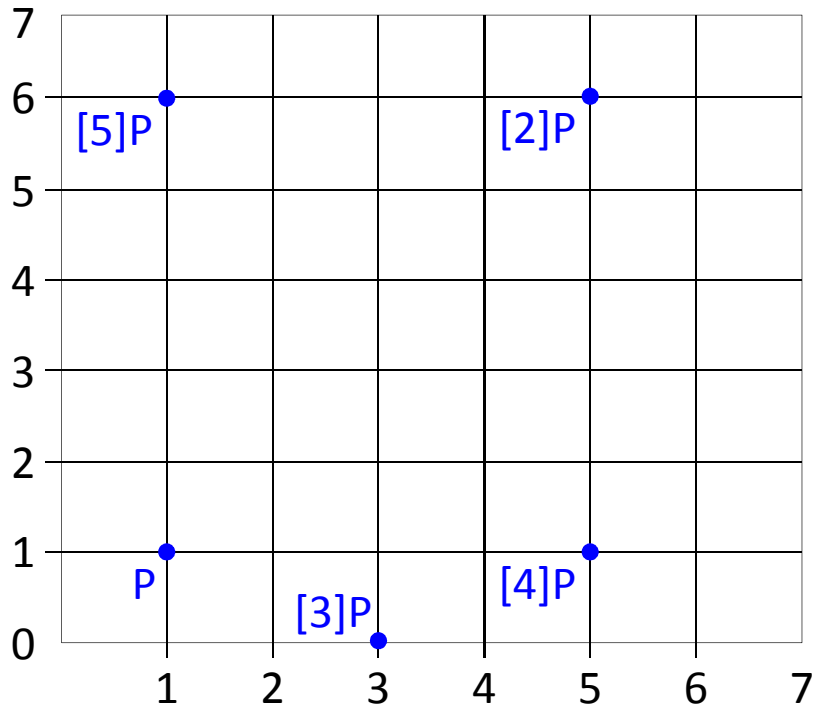
[4]P = (5, 1)

[5]P = (1, 6)

[6]P $\Rightarrow \lambda = \frac{y_{[5]P} - yP}{x_{[5]P} - xP}$ tend vers ∞

[6]P = $\mathcal{O}$

P est un point de torsion d'ordre 6
(qui engendre un groupe cyclique d'ordre 6)



Rang d'une courbe elliptique

Définition : On appelle **rang** de $\mathcal{E}$ le nombre de points d'ordre infini indépendants.

Le rang de la courbe est nul lorsque tous les points rationnels vérifiant son équation sont des points de torsion. Par conséquent, cet ensemble de points rationnel est fini.

Lorsque rang ≥ 1, l'ensemble des points rationnels vérifiant l'équation de la courbe est infini.

La détermination du rang est compliquée.

Le record est actuellement détenue par Noam Elkies, qui a trouvé en 2006 une courbe elliptique de rang 28 :

$$y^2 + xy + y = x^3 - x^2$$
$$- 20067762415575526585033208209338542750930230312178956502\ x$$
$$+ 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

Solution :

P_1 = [-212415009125438107329213746 3, 259854492051899599030515511070780628911531]
P_2 = [233450986603470175688475453 7, 188720041954944691808683165528036279315 31]
P_3 = [-167173605406236906387903866 3, 251709377261144287808506947241319126049131]
P_4 = [213913026013915666649298213 7, 366395091714397292024214596929412975275 31]
P_5 = [153470676446712072388547733 7, 854295853460176942890210328627810727995 31]
P_6 = [-273107948787567703334157506 3, 262521815484332191641284072623902143387531]
P_7 = [277572626684457164970545853 7, 128457554740140602488694876990826403699 31]
P_8 = [149438572932718895754183381 7, 884866055277334059861164945140492334114 51]
P_9 = [186843822862088735850906525 7, 592374032144377087127251403930593585891 31]
P_{10} = [200894510882574377486654253 7, 476906778801255528821517507815414247115 31]
P_{11} = [234836054091802516965163293 7, 174929300062005578573403324764488043635 31]
P_{12} = [-147208400709048117447000866 3, 246643450653503714199947441549759798469131]
P_{13} = [292412860770806121336328893 7, 283502644314888785014883564747673758995 31]
P_{14} = [537499389106606189329393453 7, 286188908427263386451175031916479893731531]
P_{15} = [170969076823335452333400855 7, 718988349746860894661597005292159809216 31]
P_{16} = [245095401135359314407259518 7, 444522817353263435704926255061071473653 1]
P_{17} = [296925470927355916746467493 7, 327668930753662708013336825431604696875 31]
P_{18} = [271191493494169260133288293 7, 206843661277838169865041398150659061353 1]
P_{19} = [200785860779968545287783289 37, 27796085411378066046560517256246240300915 31]
P_{20} = [215808245024073477431781069 7, 349943734019640268099696622418009012547 31]
P_{21} = [200464545824705902240322493 7, 480493297807046455224398669998884754675 31]
P_{22} = [297574945094799626494709133 7, 333989898260753223202089344101048578691 31]
P_{23} = [-210249046768628515014734786 3, 259576391459875789571677393171687203227531]
P_{24} = [311583179915063034902194537, 168104385229980603540109472915660153473931]
P_{25} = [277393100834186523144377181 7, 126321628346499210024141162737692758134 51]
P_{26} = [215658118814376840936346138 7, 351250929640229088970041505163751780873 31]
P_{27} = [386633049987241250881565913 7, 121197755655944226293036926715025847322531]
P_{28} = [223086828977357602377867873 7, 285587600305974856633870206007686400285 31]

ET LA CRYPTOGRAPHIE DANS TOUT ÇA ?

Lecture d'une norme

Standard for Efficient Cryptography
SEC 2: Recommended Elliptic Curve Domain Parameters
Certicom Research, September 2000

2.7.2 Recommended Parameters secp256r1

The verifiably random elliptic curve domain parameters over $\mathbb{F}_p$ `secp256r1` are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

p = FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF

$= 2^{224}(2^{32} - 1) + 2^{192} + 2^{96} - 1$

The curve E: $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ is defined by:

a = FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFC

b = 5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E 27D2604B

E was chosen verifiably at random as specified in ANSI X9.62 [1] from the seed:

S = C49D3608 86E70493 6A6678E1 139D26B7 819F7E90

The base point G in compressed form is:

G = 03 6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296

and in uncompressed form is:

G = 04 6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296 4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16 2BCE3357 6B315ECE CBB64068 37BF51F5

Finally the order n of G and the cofactor are:

n = FFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551

h = 01

- un nom
- 6 paramètres :
  - La dimension du champ fini
  - les coefficients a et b de l'équation $y^2 = x^3 + a\,x + b$
  - le point générateur $G(x, y)$ qui est un point de torsion
  - l'ordre n de G
  - le cofacteur h qui est : cardinalité / n soit 1
- la graine qui permet de vérifier que les paramètres de la courbe sont corrects (ANSI X9.62)

Cryptosystèmes recommandés

Parameters	Section	ANSI X9.62	ANSI X9.63	echeck	IEEE P1363	IPSec	NIST	WAP
secp112r1	2.2.1	-	-	-	c	c	-	r
secp112r2	2.2.2	-	-	-	c	c	-	c
secp128r1	2.3.1	-	-	-	c	c	-	c
secp128r2	2.3.2	-	-	-	c	c	-	c
secp160k1	2.4.1	c	r	c	c	c	-	c
secp160r1	2.4.2	c	c	c	c	c	-	r
secp160r2	2.4.3	c	r	c	c	c	-	c
secp192k1	2.5.1	c	r	c	c	c	-	c
secp192r1	2.5.2	r	r	c	c	c	r	c
secp224k1	2.6.1	c	r	c	c	c	-	c
secp224r1	2.6.2	c	r	c	c	c	r	c
secp256k1	2.7.1	c	r	c	c	c	-	c
secp256r1	2.7.2	r	r	c	c	c	r	c
secp384r1	2.8.1	c	r	c	c	c	r	c
secp521r1	2.9.1	c	r	c	c	c	r	c

Table 2: Status of Recommended Elliptic Curve Domain Parameters over $\mathbb{F}_p$

c paramètres conformes au standard

r paramètres recommandés par le standard

ANSI X9.62
standard for ECDSA
(signature numérique)

ANSI X9.63
standard for Key Establishment Schemes

echeck
electronic paiement mechanism

IEEE P1363
Standard Specifications for Public Key Cryptography

ANSI X9.62
Internet Protocol Security

WAP
Wireless Application Protocol

Comparaison avec RSA

Taille des clés RSA (bits)	Taille des clés ECC (bits)
1024	160
1536	**192**
2048	224
3072	**256**
7680	384
15360	521

Génération d'un couple de clés

La génération d'un couple de clés (**clé secrète/clé publique**) se déroule en 5 étapes :

1. Sélection de la courbe elliptique $\mathcal{E}$ sur un champ fini $E(\mathbb{F}_p)$
2. Sélection d'un point de la courbe $P(x, y) \in E(\mathbb{F}_p)$ d'ordre n
   Cela signifie que $[n]P = \mathcal{O}$
3. Sélection d'un nombre aléatoire d dans l'intervalle $[1, n - 1]$
   d sera la clé secrète
4. Calcul de $Q = [d]P \bmod n$
5. La clé publique est $(\mathcal{E}, P(x, y), Q(x, y))$

Calcul de la clé publique

$$Q = [d]P \bmod n$$

Souvenez-vous …

Addition :

$$\begin{cases} x_{P+Q} = \lambda^2 - x_P - x_Q \\ y_{P+Q} = \lambda(x_P - x_{P+Q}) - y_P \end{cases} \quad \text{avec } \lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

Doublement :

$$\begin{cases} x_{[2]P} = \lambda^2 - 2x_P \\ y_{[2]P} = \lambda(x_P - x_{[2]P}) - y_P \end{cases} \quad \text{avec } \lambda = \frac{3x_P^2 + a}{2y_P}$$

Ça fait beaucoup d'opérations, notamment des divisions et des réductions modulo.
Ce n'est pas simple en embarqué !

Exemple d'optimisation

Opération	Méthode	Complexité
Multiplication $Q=[k]P$	① Binary method	w additions & ℓ-1 doublements
	② M-ary method	Initialisation : m-2 doublements Puis : d additions & $(d-1)r$ doublements
Inversion dans $\mathbb{Z}/p\mathbb{Z}$	Algorithme d'Euclide étendu	Trouver trois entiers d, u et v tels que : $pgcd(a, b) = d = a.u + b.v$ L'inverse de a est u dans $\mathbb{Z}/p\mathbb{Z}$ (théorème de Bezout)
	Réduction de Montgoméry	Parallélisation du calcul de l'inverse
Réduction modulo p	Fast réduction	Basée sur la transformation de Montgoméry : décomposition de p en puissance de 2

① k : entier représenté sur ℓ bits

w : le nombre de '1' parmi les ℓ bits

② k : décomposé sur une base $m=2^r$ pour la binary method $r=1$

k : de longueur d dans la base m

Chiffrement

ECIES : Elliptic Curve Integrated Encryption System

ANSI X9.63, ISO 15946-3, IEEE P1363a

Soit :
- $\mathcal{E} = (p, a, b, P(x, y), n, h)$
- $Q=[d]P$ la clé publique (où d est la clé secrète)

Le **chiffrement** comporte 5 étapes :

1. Sélection d'un nombre aléatoire $k \in [1, n - 1]$
2. Calcul de $R = [k]P \bmod n$ et de $Z = [h][k]Q \bmod n$
   Si $Z = \mathcal{O}$ alors on revient à l'étape 1
3. Calcul de deux clés dérivées k_1 et k_2 telles que $(k_1, k_2) \leftarrow F_{hash}(x_Z, R)$
   avec x_Z abscisse du point Z
4. Calcul du chiffré $C = \mathbf{AES}_{k1}(m)$ et de $t = \mathbf{MAC}_{k2}(C)$.
5. La texte chiffré est ($R(x, y)$, C, t)

Déchiffrement

ECIES : Elliptic Curve Integrated Encryption System

ANSI X9.63, ISO 15946-3, IEEE P1363a

Soit :
- $\mathcal{E} = (p, a, b, P(x, y), n, h)$
- d la clé secrète

On a reçu $R(x, y)$, C, t

Le **déchiffrement** comporte 5 étapes :

1. Vérifier la validité de R *(embedded public key validation)*
2. Calcul de $Z = [h][d]R \bmod n$
   Si $Z = \mathcal{O}$ alors retourner ("Echec").
3. Calcul des deux clés dérivées k_1 et k_2 telles que $(k_1, k_2) \leftarrow F_{hash}(x_Z, R)$
   avec x_Z abscisse du point Z
4. Calcul de $t' = \mathbf{MAC}_{k2}(C)$. Si $t \neq t'$ retourner ("Echec")
5. Calcul du texte en clair $m = \mathbf{AES}^{-1}_{k1}(C)$

ECDSA : Elliptic Curve Digital Signature Algorithm

ANSI X9.62

Soit :
- $\mathcal{E} = (p, a, b, P(x, y), n, h)$
- d la clé secrète

Pour **signer** un message m, on déroule les étapes suivantes :

1. Choix d'une fonction de hashage $hash$ et d'une fonction $f : E(\mathbb{F}_p) \rightarrow \mathbb{Z}$ telle qu'à un élément de l'image de f ne corresponde que très peu d'antécédents. Par exemple : $f(x, y) = x$
2. Choix d'un nombre entier aléatoire k tel que $\text{pgcd}(k, n) = 1$
   Calcul de $R = [k]P = (x_R, y_R)$
3. Calcul de $s = k^{-1}(hash(m) - d.f(R)) \bmod n$
   Pour $f(x, y) = x$, cette relation devient : $s = k^{-1}(hash(m) - d.x_R) \bmod n$
4. Le document signé est (m, R, s)

Vérification de la signature

ECDSA : Elliptic Curve Digital Signature Algorithm

ANSI X9.62

Pour vérifier la signature (m, R, s), les éléments suivants doivent être rendus publiques :

- $(\mathcal{E}, P(x, y), n, Q(x, y))$ la clé publique
- la fonction de hashage $hash$ et la fonction $f : E(\mathbb{F}_p) \rightarrow \mathbb{Z}$

La procédure de **vérification** est la suivante :

1. On calcule $u_1 = s^{-1}\, hash(m) \bmod n$ et $u_2 = s^{-1}.f(R) \bmod n$
   Pour $f(x, y) = x$, on a $u_2 = s^{-1}.x_R \bmod n$
2. Calcul de $V = u_1 P + u_2 Q$
3. Si $V = R$, alors la signature est valide

Pour effectuer la vérification, le calcul du multiple d'un point de la courbe $[a]P$ est mené deux fois.

Démonstration

$$V = [u_1]P + [u_2]Q$$

$$= [s^{-1}.hash(m)]P + [s^{-1}.x_R]Q$$

$$= [s^{-1}]([hash(m)]P + [x_R][d]P)$$

$$= [s^{-1}] [hash(m) + x_R\, d] P$$

$$= [k]P$$

$$= R$$

Temps d'exécution

Processeur 32 bits ARM11 cadencé à 400MHz

	Génération d'une clé		Signature		Vérification	
	ECC	RSA	ECC	RSA	ECC	RSA
163 bits / 1024 bits	6,4 ms	164 ms	2,2 ms	4,5 ms	4,4 ms	0,007 ms
224 bits / 2048 bits	12,5 ms	**1,055 s**	4,4 ms	22,2 ms	5,2 ms	0,02 ms
256 bits / 3072 bits	12,7 ms	3,457 s	4,5 ms	53,5 ms	5,3 ms	0,3 ms
384 bits / 7680 bits	20,9 ms	92,61 s	7,4 ms	**609 ms**	8,8 ms	1,4 ms

30s sur un processeur 16 bits MSP430 cadencé à 16MHz

Négociation d'une clé de session

Protocole d'échange de clés de Diffie-Helmann (ECDH)

1. Alice et Bob choisissent une courbe elliptique $\mathcal{E}$ définie sur un corps $\mathbb{F}_p$ tel que le problème du logarithme discret soit difficile à résoudre. Ils choisissent un point de la courbe $P \in E(\mathbb{F}_p)$, tel que le sous-groupe généré par P ait un ordre de grande taille.

2. **Alice** choisit un nombre entier ***a*** qui restera secret. Elle calcule $P_a = [a]P$ et envoie $\boldsymbol{P_a}$ à Bob.

3. **Bob** choisit un nombre entier ***b*** qui restera secret. Il calcule $P_b = [b]P$ et envoie $\boldsymbol{P_b}$ à Alice.

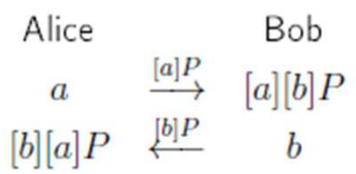
4. A la réception de $\boldsymbol{P_b}$, **Alice** calcule $\boldsymbol{[a]P_b = [a][b]P}$

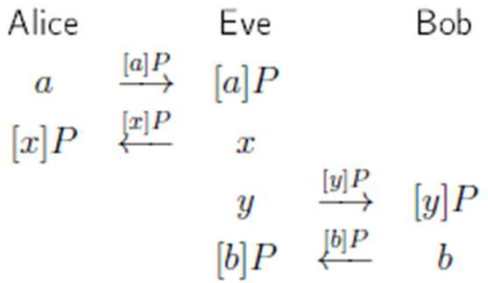
5. A la réception de $\boldsymbol{P_a}$, **Bob** calcule $\boldsymbol{[b]P_a = [b][a]P}$

6. **Alice** et **Bob** partagent désormais un secret consistant en un point de la courbe. Ils se mettent d'accord sur une fonction, par exemple une fonction de hashage, qu'ils appliquent à une des coordonnées de $\boldsymbol{[a][b]P}$ an d'obtenir une clé de session symétrique. Ils peuvent ensuite échanger des données en utilisant **la cryptographie symétrique**.

Attaque par man-in-the-middle

ECDH est vulnérable aux attaques par man-in-the-middle





Le problème de cet algorithme vient du fait que l'authentification de l'émetteur n'est pas assurée. Alice ne sait pas de qui provient la clé publique éphémère *[b]P*. Une façon d'assurer l'authentification est de signer les messages. Alice enverrait alors à Bob le message *([a]P, (r, s))* où *(r, s)* est la signature numérique.

EST-CE BIEN « SECURE » ?

Définition du problème

The elliptic curve discrete logarithm problem (ECDLP)

Est-ce qu'un adversaire peut réussir à calculer la clé secrète d connaissant les paramètres du domaine elliptique $(\mathcal{E}, P(x, y), Q(x, y))$ et la clé publique Q ?

	Attaque	Complexité	Contre-mesure
1	Naive Exhaustive Search	Teste les n points de la courbe	n grand
2	Polhig-Hellman Algorithm	Exploite la factorisation de n	n premier
3	Baby-Step Giant-Step	Compromis temps-mémoire Stockage de $\sqrt{n}$ points	n grand
4	Pollard's Rho Algorithm	Version aléatoire de Baby-Step Giant-Step – Complexité $\sqrt{\pi n}/2$	n grand
5	Parallelized Pollard's Rho	Parallélisation de Pollard's Rho sur r processeurs – Complexité $\sqrt{\pi n}/2r$	n grand
6	Pollard's Lambda method	Autre méthode de parallélisation moins efficace que Pollard's Rho (5)	n grand
7	Multiple Logarithms	Si une solution est trouvée, la 2ème sera trouvée en ($\sqrt{2}$-1)t	Aucune solution ne doit être trouvée
8	Supersingular Elliptic Curves	Courbes spéciales : la trace t de $\mathcal{E}$ est divisible par la caractéristique p de $\mathbb{F}_p$	Supersingular EC excluded
9	Prime-Field Anomalous Curves	Prime-Field anomalous if $\#E(\mathbb{F}_p) = p$	$\#E(\mathbb{F}_p) \neq p$
10	Curves defined over Small Field	L'algorithme Pollard's Rho peut être accéléré de $\sqrt{m}$ pour EC sur $\mathbb{F}_{2^m}$	Analyse de sécurité pour EC coef ∈ « small subfield »
11	Curves defined over $\mathbb{F}_{2^m}$, m composite	L'algorithme Pollard's Rho est résolu facilement qd m est divisible par k pt	Ne pas utiliser EC sur $\mathbb{F}_{2^m}$ avec m composite
12	Index-Calculus & Xedni-Calculus Attacks	résoud DLP and pb de facto des entiers	… une nouvelle menace !
13	Hyperelliptic Curves	Plus mauvais que (1)	Pas de menace

ECC challenge

L'attaque la plus efficace est l'algorithme de Pollard's Rho parallélisé

Challenge lancé par Certicom en 1997 sur trois catégories de courbes :

1. Courbes elliptiques définies sur $\mathbb{F}_p$ avec p premier générées à partir d'un nombre aléatoire
2. Courbes elliptiques définies sur $\mathbb{F}_{2^m}$ avec m premier générées à partir d'un nombre aléatoire
3. Courbes elliptiques de Koblitz définies sur $\mathbb{F}_{2^m}$ avec m premier

Résultats :

- La plus difficile instance de ECDLP a été résolue pour la courbe ECC sur $\mathbb{F}_p$ avec $p = 97$
- Pour cela, il a fallu utiliser 1200 machines de 16 pays différents et la réponse a été trouvée en 53 jours.
- On estime que le challenge peut être résolu pour ECC sur $\mathbb{F}_p$ avec $p = 109$ en 3 mois avec 50000 pentium PRO à 200MHz
- Attaque Hardware : On estime qu'une machine avec 330.000 processeurs peut résoudre le problème en 32 jours avec un coût de 10 millions de $

ANSI X9.63 indique que $n > 2^{160}$ pour que la courbe soit « secure »

Nouvelle attaque… en mai 2014

- **French team** (INRIA)
- Méthode basée sur l'algorithme Index-Calculus publiée en **mai 2014** à Eurocrypt'2014 (Amsterdam) :

  Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, Emmanuel Thomé, « A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic », Eurocrypt'2014, 11-15 mai 2014, Amsterdam
- Décompose le problème du log discret en un arbre hiérarchisé de polynômes
- Résout le problème sur les « small fields » $\mathbb{F}_{2^m}$
- Pas de **preuve formelle** pour l'instant mais fonctionne en pratique
- Les travaux se poursuivent pour appliquer la méthode aux « large fields » $\mathbb{F}_{2^m}$ et aux « prime fields » $\mathbb{F}_p$
- **Pas de menace** à court terme pour **secp256r1**
- **Exclue** les familles de courbes utilisées en **cryptographie basée sur l'identité**

Merci de votre attention