La cryptographie du futur

Abderrahmane NITAJ

Laboratoire de Mathématiques Nicolas Oresme
Université de Caen, France

Rabat, 16 juin 2011

الرباط

CONTENU

1. Le passé
2. Le présent
3. Le futur
4. Conclusion

CONTENU

1 Le passé

2 Le présent

3 Le futur

4 Conclusion

Le passé

L'antiquité (1)

- L'écriture hiéroglyphique égyptienne date de 4 000 ans et peut être considérée comme la première manifestation de la cryptographie.

Le passé

L'antiquité (1)

- L'écriture hiéroglyphique égyptienne date de 4 000 ans et peut être considérée comme la première manifestation de la cryptographie.

=Cryptographie

Le passé

L'antiquité (1)

- L'écriture chinoise, à base de pictogrammes date de 3500 ans et a longtemps servi comme procédé cryptographique.

=?

Le passé

L'antiquité (1)

- L'écriture chinoise, à base de pictogrammes date de 3500 ans et a longtemps servi comme procédé cryptographique.

=**Marguerite**

Le passé

La deuxième guerre mondiale

- Pendant la deuxième guerre mondiale, les américains avaient utilisé la langue des Indiens Navajos pour communiquer.

La saga des Indiens Navajos fut transformé en film

Le passé

La deuxième guerre mondiale

- Pendant la deuxième guerre mondiale, les américains avaient utilisé la langue des Indiens Navajos pour communiquer.

Le passé

L'antiquité (2)

- Le chiffre de César : Il s'agit de décaler les lettres de l'alphabet de quelques rangs vers la droite ou la gauche.

Jules César

A	B	C	D	E	F	...	W	X	Y	Z
↓	↓	↓	↓	↓	↓	...	↓	↓	↓	↓
D	E	F	G	H	I	...	Z	A	B	C

Le passé

Le moyen âge (1)

- L'analyse fréquentielle : il s'agit de comparer la fréquence d'apparition d'une lettre dans dans un texte codé et dans l'alphabet utlisé.
- Découverte par Al Kindi (801-873)

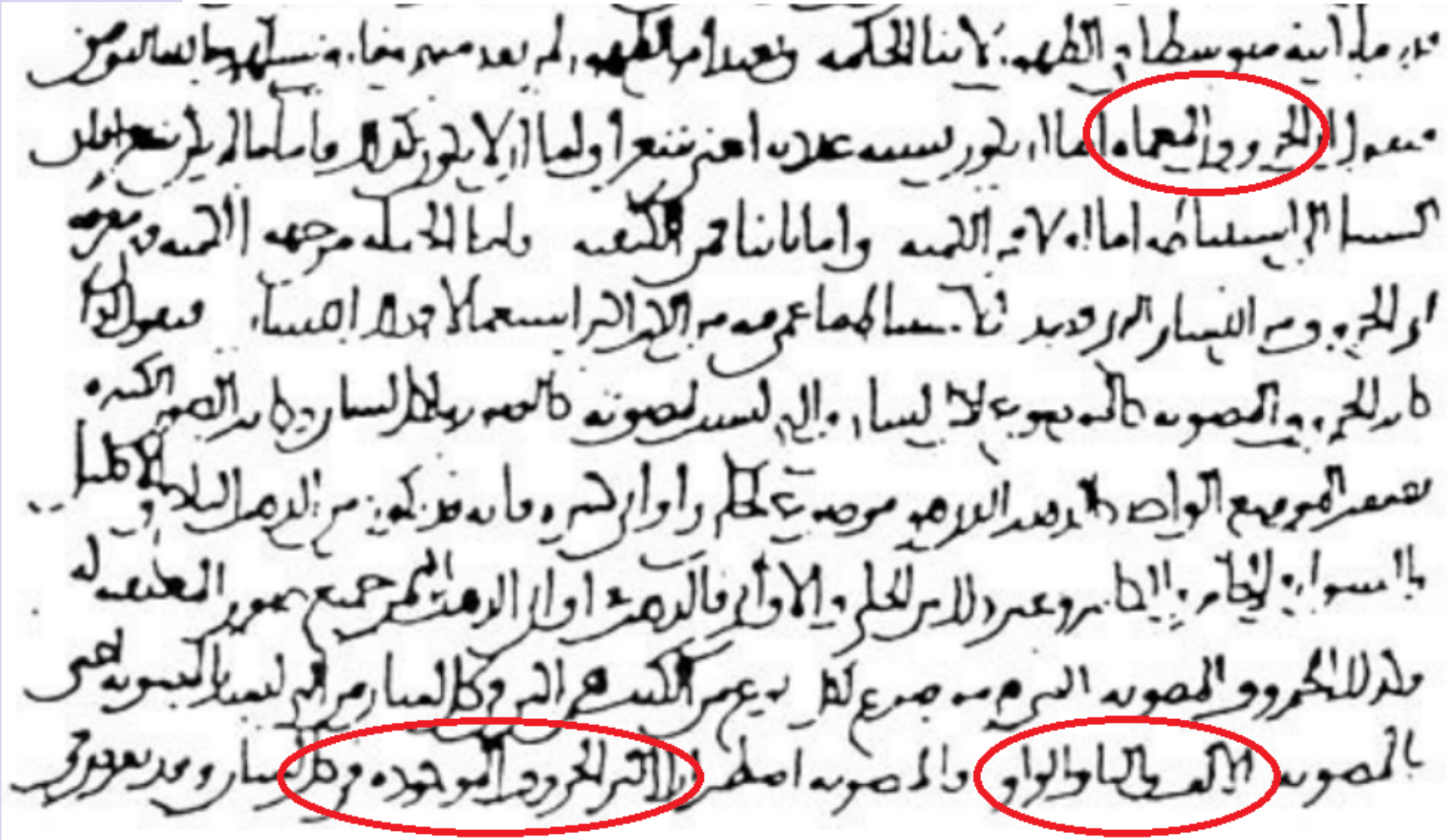
ابُو يُوسُف يَعقُوب إِبنُ إِسحَاق الكِندي

- En français, les principales fréquences sont les uivantes :

E	A	S	I	...	K	W
16	9.5	8	7.5	...	0.1	0

ابُو يُوسُف يَعقُوب إِبنُ إِسحَاق الكِندي Al Kindi

ابُو يُوسُف يَعقُوب إِبنُ إِسحَاق الكِندي Al Kindi



Le passé

Le moyen âge (2)

- Le chiffre de Vigenère (1523-1596) : Il s'agit de décaler les lettres de l'alphabet de en utlisant une clé composée de lettres avec les translations avec A$\longrightarrow +0$, B$\longrightarrow +1$, C$\longrightarrow +2$,..., Z$\longrightarrow +25$.

Vigenère

- Décrypté par Charles Babbage en 1846.

Le passé

Le moyen âge (2)

- Le chiffre de Vigenère (1523-1596).
- Exemple :
  Texte = CRYPTOGRAPHIE A RABAT.
  Clé = CASA.

	CRYP	TOGR	APHI	E	A	RABA	T
+	CASA	CASA	CASA	C	C	CASA	C
=	ERQP	VOYR	CPZI	G	C	TATA	V

Le passé

La deuxième guerre mondiale (1)

- Enigma : inventée en 1919 par Arthur Scherbius, cette machine a été intensivement utilisée par les allemands pendant la deuxième guerre mondiale.
- La dernière machine fut décryptée par Alan Turing en 1943.

La machine enigma

Alan Turing

CONTENU

1 Le passé

2 Le présent

3 Le futur

4 Conclusion

Le présent

La cryptographie moderne

Quelques dates importantes.

- 1883 : Les principes de Kerckhoffs :
  "Le système doit être matériellement, sinon mathématiquement, indéchiffrable; ".
- 1976 : Les principes de la cryptographie à clé publique de Diffie et Hellman.
- 1978 : Invention du cryptosystème RSA par Rivest, Shamir et Adleman.
- 1978 : Invention du cryptosystème McElliece.
- 1982 : Invention de l'algorithme LLL par Lenstra, Lenstra et Lovasz.

Le présent

La cryptographie moderne

Quelques dates importantes.

- 1883 : Les principes de Kerckhoffs : "Le système doit être matériellement, sinon mathématiquement, indéchiffrable; ".
- 1976 : Les principes de la cryptographie à clé publique de Diffie et Hellman.
- 1978 : Invention du cryptosystème RSA par Rivest, Shamir et Adleman.
- 1978 : Invention du cryptosystème McElliece.
- 1982 : Invention de l'algorithme LLL par Lenstra, Lenstra et Lovasz.

Le présent

La cryptographie moderne

Quelques dates importantes.

- 1883 : Les principes de Kerckhoffs : "Le système doit être matériellement, sinon mathématiquement, indéchiffrable; ".
- 1976 : Les principes de la cryptographie à clé publique de Diffie et Hellman.
- 1978 : Invention du cryptosystème RSA par Rivest, Shamir et Adleman.
- 1978 : Invention du cryptosystème McElliece.
- 1982 : Invention de l'algorithme LLL par Lenstra, Lenstra et Lovasz.

Le présent

La cryptographie moderne

Quelques dates importantes.

- 1883 : Les principes de Kerckhoffs : "Le système doit être matériellement, sinon mathématiquement, indéchiffrable; ".
- 1976 : Les principes de la cryptographie à clé publique de Diffie et Hellman.
- 1978 : Invention du cryptosystème RSA par Rivest, Shamir et Adleman.
- 1978 : Invention du cryptosystème McElliece.
- 1982 : Invention de l'algorithme LLL par Lenstra, Lenstra et Lovasz.

Le présent

La cryptographie moderne

Quelques dates importantes.

- 1883 : Les principes de Kerckhoffs : "Le système doit être matériellement, sinon mathématiquement, indéchiffrable; ".
- 1976 : Les principes de la cryptographie à clé publique de Diffie et Hellman.
- 1978 : Invention du cryptosystème RSA par Rivest, Shamir et Adleman.
- 1978 : Invention du cryptosystème McElliece.
- 1982 : Invention de l'algorithme LLL par Lenstra, Lenstra et Lovasz.

Le présent

La cryptographie moderne

Quelques dates importantes.

- 1984 : Ebauche de la cryptographie quantique par Bennett et Brassard.
- 1985 : Invention du cryptosystème El Gamal par T. El Gamal.
- 1985 : Invention de la cryptographie basée sur les courbes elliptiques ECC indépendamment par Koblitz et Miller.
- 1994 : Algorithme de Shor pour la factorisation par les ordinateurs quantiques.
- 1996 : Invention de NTRU par Hoffstein, Pipher et Silverman.

Le présent

La cryptographie moderne

Quelques dates importantes.

- 1984 : Ebauche de la cryptographie quantique par Bennett et Brassard.
- 1985 : Invention du cryptosystème El Gamal par T. El Gamal.
- 1985 : Invention de la cryptographie basée sur les courbes elliptiques ECC indépendamment par Koblitz et Miller.
- 1994 : Algorithme de Shor pour la factorisation par les ordinateurs quantiques.
- 1996 : Invention de NTRU par Hoffstein, Pipher et Silverman.

Le présent

La cryptographie moderne

Quelques dates importantes.

- 1984 : Ebauche de la cryptographie quantique par Bennett et Brassard.
- 1985 : Invention du cryptosystème El Gamal par T. El Gamal.
- 1985 : Invention de la cryptographie basée sur les courbes elliptiques ECC indépendamment par Koblitz et Miller.
- 1994 : Algorithme de Shor pour la factorisation par les ordinateurs quantiques.
- 1996 : Invention de NTRU par Hoffstein, Pipher et Silverman.

Le présent

La cryptographie moderne

Quelques dates importantes.

- 1984 : Ebauche de la cryptographie quantique par Bennett et Brassard.
- 1985 : Invention du cryptosystème El Gamal par T. El Gamal.
- 1985 : Invention de la cryptographie basée sur les courbes elliptiques ECC indépendamment par Koblitz et Miller.
- 1994 : Algorithme de Shor pour la factorisation par les ordinateurs quantiques.
- 1996 : Invention de NTRU par Hoffstein, Pipher et Silverman.

Le présent

La cryptographie moderne

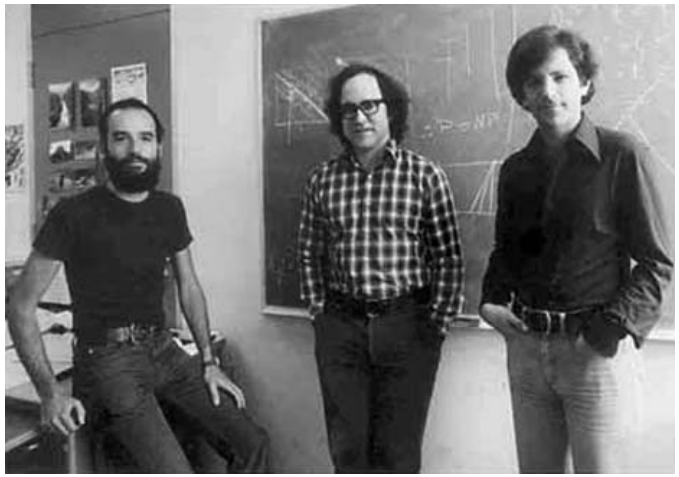
Quelques dates importantes.

- 1984 : Ebauche de la cryptographie quantique par Bennett et Brassard.
- 1985 : Invention du cryptosystème El Gamal par T. El Gamal.
- 1985 : Invention de la cryptographie basée sur les courbes elliptiques ECC indépendamment par Koblitz et Miller.
- 1994 : Algorithme de Shor pour la factorisation par les ordinateurs quantiques.
- 1996 : Invention de NTRU par Hoffstein, Pipher et Silverman.

Le présent

RSA

- Inventé en 1978 par Rivest, Shamir et Adleman.



- Problème difficile

Factorisation :

Soit $N = pq$ où p et q sont deux grands nombres premiers. Factoriser N.

Le présent

RSA

- Inventé en 1978 par Rivest, Shamir et Adleman.

- Problème difficile

Factorisation :

Soit $N = pq$ où p et q sont deux grands nombres premiers. Factoriser N.

Le présent

RSA

- Inventé en 1978 par Rivest, Shamir et Adleman.

- Problème difficile

Factorisation :

Soit $N = pq$ où p et q sont deux grands nombres premiers. Factoriser N.

RSA

L'arithmétique de RSA

- p, q des nombres premiers, $N = pq$.
- $\varphi(N) = (p-1)(q-1)$, $(e, \varphi(N)) = 1$, $ed \equiv 1 \pmod{\varphi(N)}$.
- Les opérations consistent en des exponentiations.

$$c \equiv m^e \pmod{N}, \qquad m \equiv c^d \pmod{N}.$$

- Complexité de l'exponentiation: $\mathcal{O}(\log(N))$.

Problème difficile : La factorisation

Soit $N = pq$ où p et q sont deux grands nombres premiers, factoriser N.

RSA

L'arithmétique de RSA

- p, q des nombres premiers, $N = pq$.
- $\varphi(N) = (p-1)(q-1)$, $(e, \varphi(N)) = 1$, $ed \equiv 1 \pmod{\varphi(N)}$.
- Les opérations consistent en des exponentiations.

$$c \equiv m^e \pmod{N}, \qquad m \equiv c^d \pmod{N}.$$

- Complexité de l'exponentiation: $\mathcal{O}(\log(N))$.

Problème difficile : La factorisation

Soit $N = pq$ où p et q sont deux grands nombres premiers, factoriser N.

Le présent

El Gamal

- Inventé en 1985 par T. El Gamal طَاهِر الجَمَال

http://www.youtube.com/watch?v=vsgsSb5DGPg&feature=related

- Problème difficile

Logarithme discret (DLP)

Soient g et b des nombres entiers et p un nombre premier. Déterminer un entier a tel que $g^a \equiv b \pmod{p}$.

Le présent

El Gamal

- Inventé en 1985 par T. El Gamal طَاهِر الجَمَال

http://www.youtube.com/watch?v=vsgsSb5DGPg&feature=related

- Problème difficile

Logarithme discret (DLP)

Soient g et b des nombres entiers et p un nombre premier. Déterminer un entier a tel que $g^a \equiv b \pmod{p}$.

El Gamal

L'arithmétique d'El Gamal

- p un nombre premier, g un générateur de $\mathbb{F}_p^*$.
- Les opérations consistent en des exponentiations.

$$b \equiv g^a \pmod{p}, \quad \gamma \equiv g^k \pmod{p},$$
$$\delta \equiv mb^k \pmod{p} \quad m \equiv \gamma^{-a}\delta \pmod{p}.$$

- Complexité de l'exponentiation $g^n \pmod{p}$: $\mathcal{O}(\log(n))$.

- **Problème difficile: Le logarithme discret (DLP)**

Soient g et b des nombres entiers et p un nombre premier, déterminer un entier a tel que $g^a \equiv b \pmod{p}$.

El Gamal

L'arithmétique d'El Gamal

- p un nombre premier, g un générateur de $\mathbb{F}_p^*$.
- Les opérations consistent en des exponentiations.

$$b \equiv g^a \pmod{p}, \quad \gamma \equiv g^k \pmod{p},$$
$$\delta \equiv mb^k \pmod{p} \quad m \equiv \gamma^{-a}\delta \pmod{p}.$$

- Complexité de l'exponentiation $g^n \pmod{p}$: $\mathcal{O}(\log(n))$.

- **Problème difficile: Le logarithme discret (DLP)**

Soient g et b des nombres entiers et p un nombre premier, déterminer un entier a tel que $g^a \equiv b \pmod{p}$.

Le présent

ECC

- ECC (Elliptic Curve Cryptography), inventé en 1985 par Koblitz et Miller.

- Problème difficile

Logarithme discret elliptique :

Soient P et Q deux points d'une courbe elliptique E. Déterminer un entier n tel que $nP = Q$.

Le présent

ECC

- ECC (Elliptic Curve Cryptography), inventé en 1985 par Koblitz et Miller.

- Problème difficile

Logarithme discret elliptique :

Soient P et Q deux points d'une courbe elliptique E. Déterminer un entier n tel que $nP = Q$.

Les courbes elliptiques : Equation de Weierstrass

- $\mathbb{K}$ est un corps ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$,...), $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$.
- Une courbe elliptique sur $\mathbb{K}$ est définie par :
  - Une équation de Weierstrass (forme projective)

$$E: \quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

  - Un discriminant $\Delta \neq 0$.
  - Le point $\mathcal{O} = [0, 1, 0]$ est appelé point à l'infini.
- Pour $Z \neq 0$, on peut écrire $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, et l'équation de Weierstrass devient (forme affine)

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

- L'ensemble des points $\mathbb{K}$ rationnels est

$$E(K) = \{(x, y) \in \mathbb{K}^2, y^2 \cdots = \cdots + a_6\} \cup \{\mathcal{O}\}.$$

Les courbes elliptiques : Equation de Weierstrass

- $\mathbb{K}$ est un corps ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$,...), $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$.
- Une courbe elliptique sur $\mathbb{K}$ est définie par :
  - Une équation de Weierstrass (forme projective)

$$E: \quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

  - Un discriminant $\Delta \neq 0$.
  - Le point $\mathcal{O} = [0, 1, 0]$ est appelé point à l'infini.
- Pour $Z \neq 0$, on peut écrire $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, et l'équation de Weierstrass devient (forme affine)

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

- L'ensemble des points $\mathbb{K}$ rationnels est

$$E(K) = \{(x, y) \in \mathbb{K}^2, y^2 \cdots = \cdots + a_6\} \cup \{\mathcal{O}\}.$$

Les courbes elliptiques : Equation de Weierstrass

- $\mathbb{K}$ est un corps ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$,...), $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$.
- Une courbe elliptique sur $\mathbb{K}$ est définie par :
  - Une équation de Weierstrass (forme projective)

$$E: \quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

  - Un discriminant $\Delta \neq 0$.
  - Le point $\mathcal{O} = [0, 1, 0]$ est appelé point à l'infini.
- Pour $Z \neq 0$, on peut écrire $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, et l'équation de Weierstrass devient (forme affine)

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

- L'ensemble des points $\mathbb{K}$ rationnels est

$$E(K) = \{(x, y) \in \mathbb{K}^2, y^2 \cdots = \cdots + a_6\} \cup \{\mathcal{O}\}.$$

Les courbes elliptiques : Equation de Weierstrass

- $\mathbb{K}$ est un corps ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$,...), $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$.
- Une courbe elliptique sur $\mathbb{K}$ est définie par :
  - Une équation de Weierstrass (forme projective)

$$E: \quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

  - Un discriminant $\Delta \neq 0$.
  - Le point $\mathcal{O} = [0, 1, 0]$ est appelé point à l'infini.
- Pour $Z \neq 0$, on peut écrire $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, et l'équation de Weierstrass devient (forme affine)

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

- L'ensemble des points $\mathbb{K}$ rationnels est

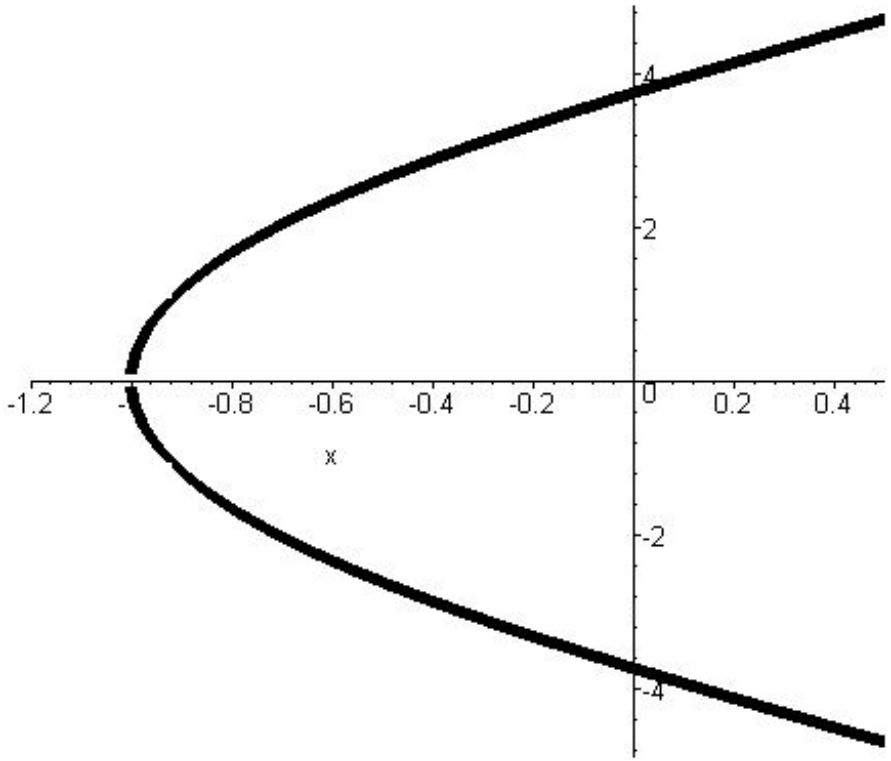
$$E(K) = \left\{(x, y) \in \mathbb{K}^2, y^2 \cdots = \cdots + a_6\right\} \cup \{\mathcal{O}\}.$$

Les courbes elliptiques : Représentation graphique

Exemple 1 :

Soit $E/\mathbb{R}$ définie par

$$E : \quad y^2 = (x^2 + x + 14)(x + 1) = x^3 + 2x^2 + 15x + 14.$$

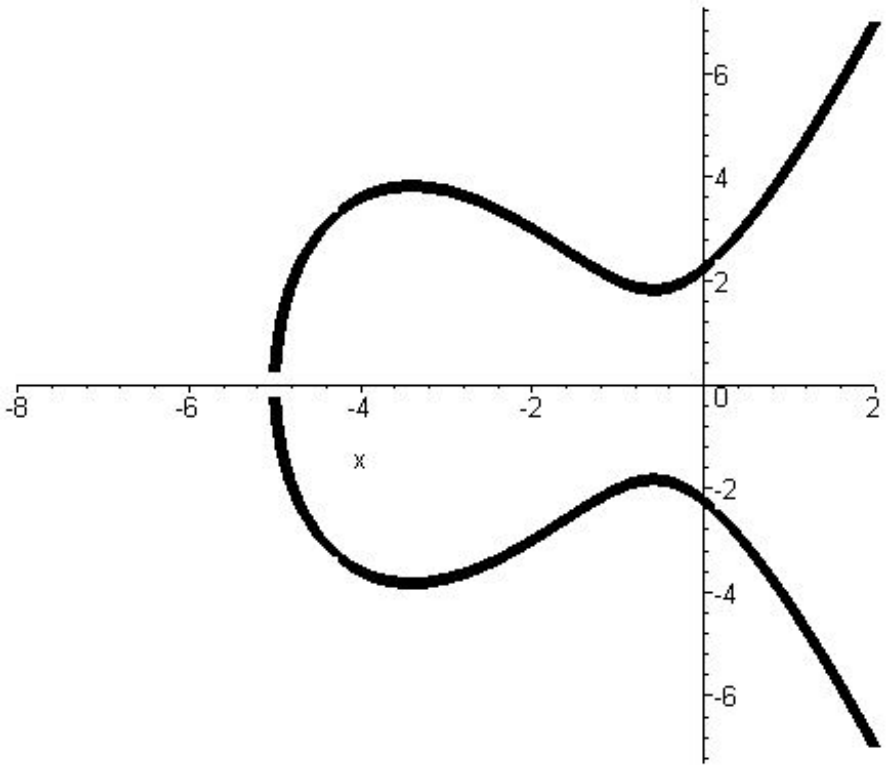


Les courbes elliptiques : Représentation graphique

Exemple 2 :

Soit $E/\mathbb{R}$ définie par

$$E : \quad y^2 = (x^2 + x + 1)(x + 5) = x^3 + 6x^2 + 6x + 5.$$

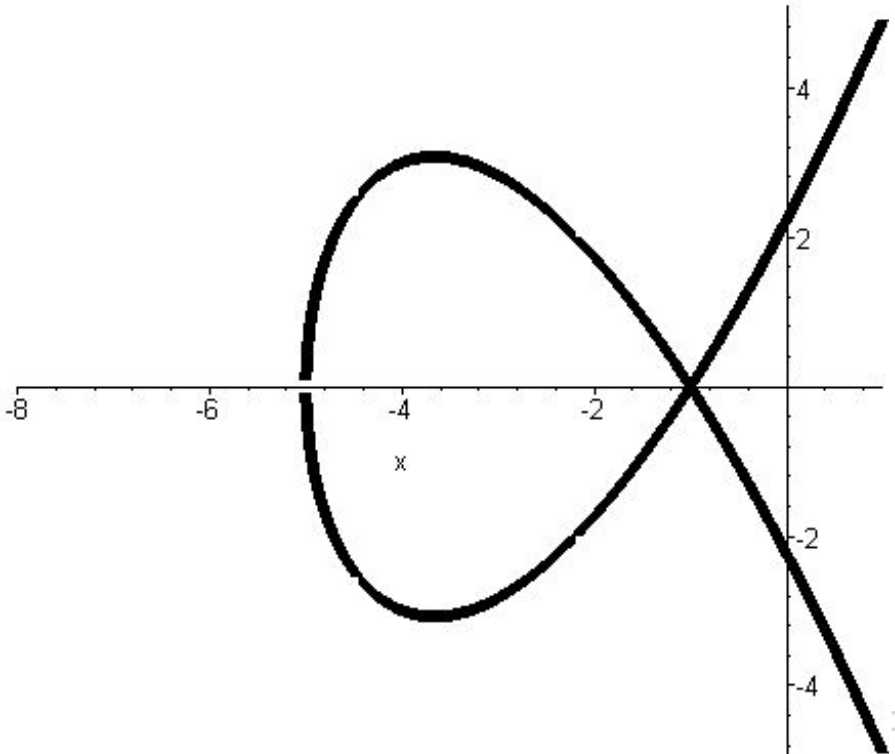


Les courbes elliptiques : Représentation graphique

Exemple 3 :

Soit $E/\mathbb{R}$ définie par E : $y^2 = (x+1)^2(x+5)$.

Ceci n'est pas une courbe elliptique car $\Delta = 0$.

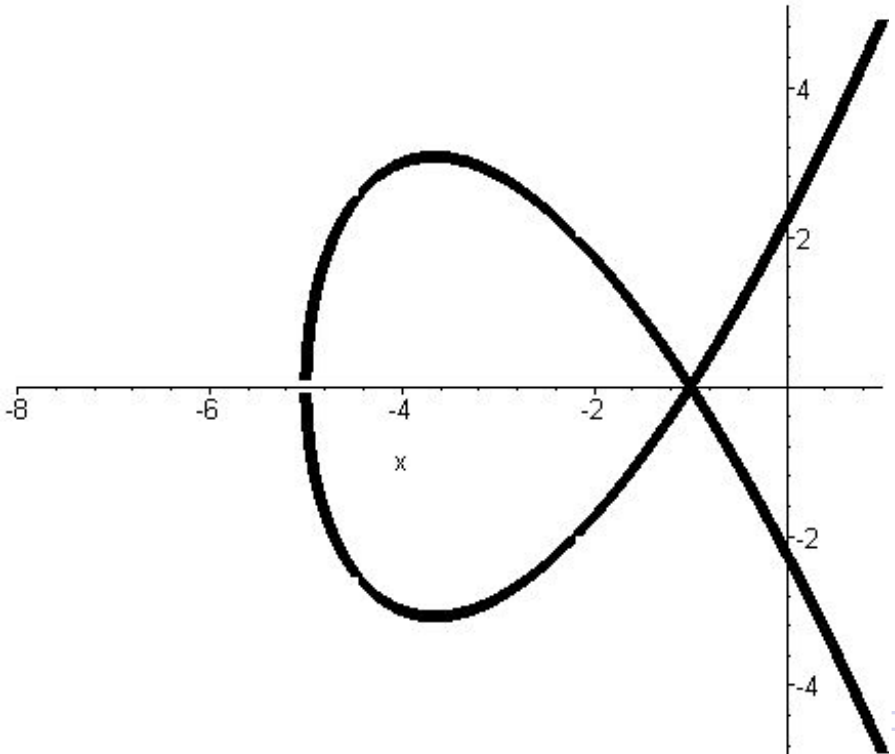


Les courbes elliptiques : Représentation graphique

Exemple 3 :

Soit $E/\mathbb{R}$ définie par E : $y^2 = (x+1)^2(x+5)$.

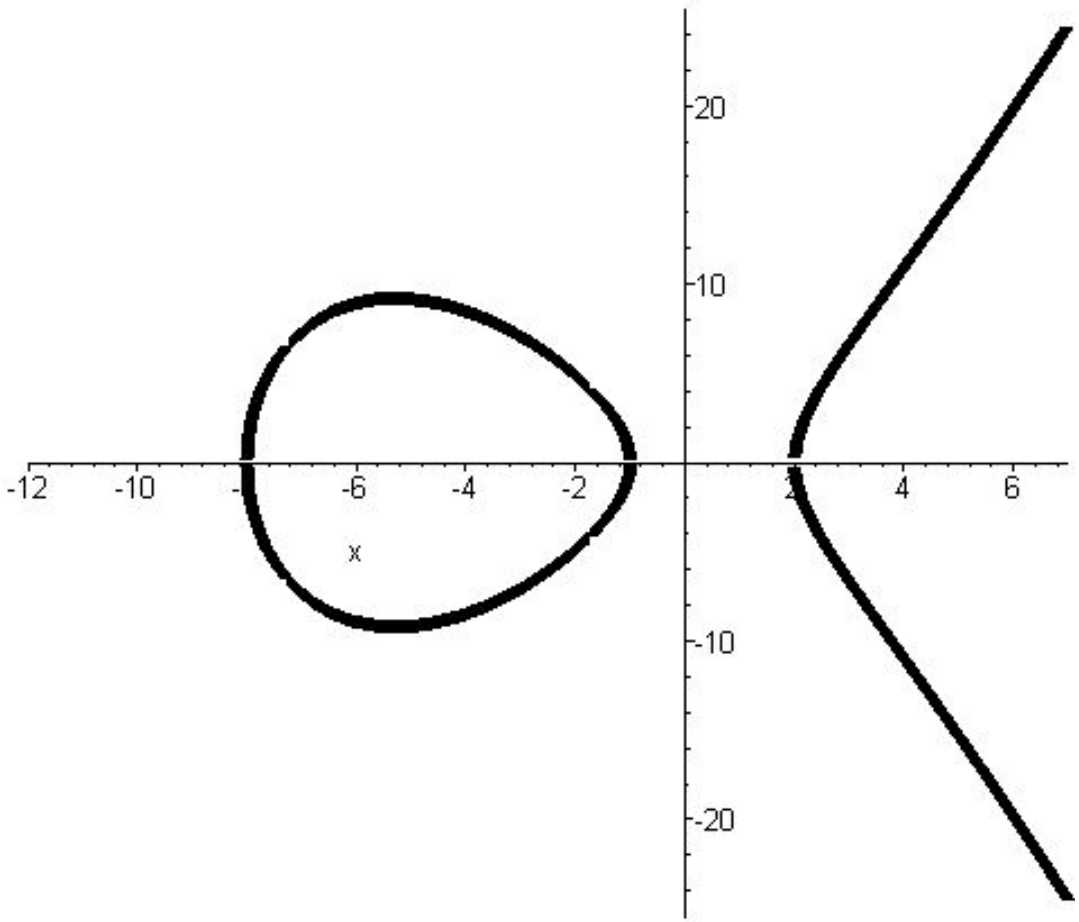
Ceci n'est pas une courbe elliptique car $\Delta = 0$.



Les courbes elliptiques : Représentation graphique

Exemple 4 :

Soit $E/\mathbb{R}$ définie par E : $y^2 = (x+8)(x+1)(x-2)$.

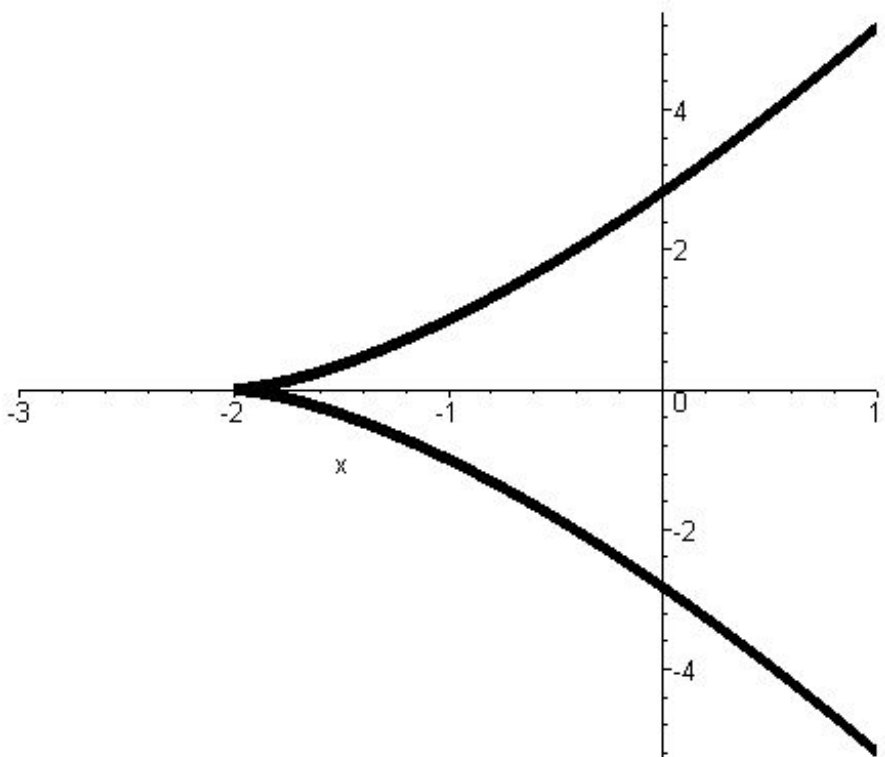


Les courbes elliptiques : Représentation graphique

Exemple 3 :

Soit $E/\mathbb{R}$ définie par E : $y^2 = (x+2)^3$.

Ceci n'est pas une courbe elliptique car $\Delta = 0$.

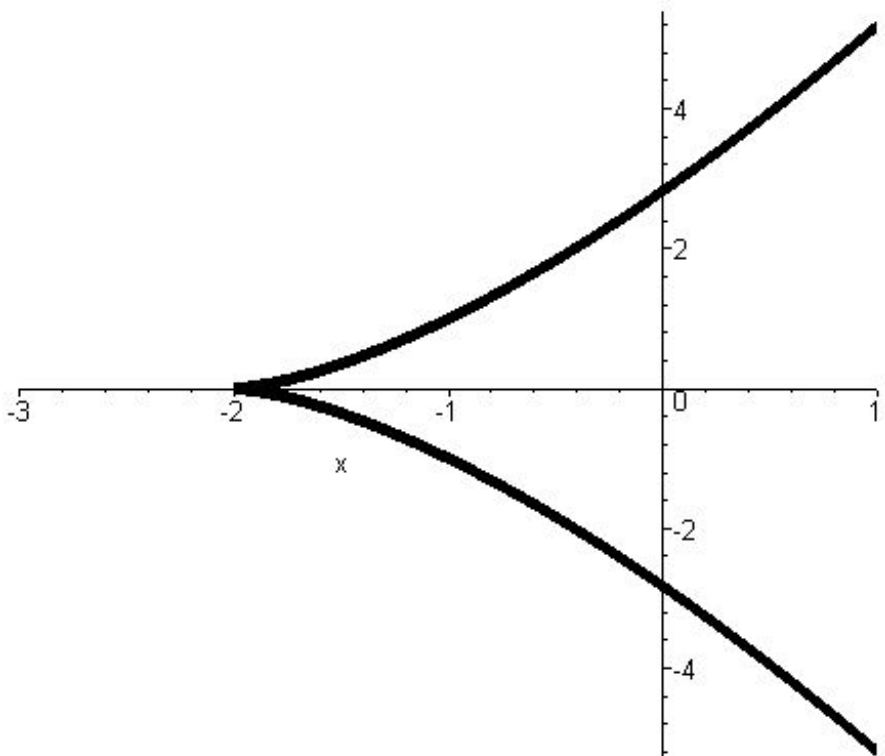


Les courbes elliptiques : Représentation graphique

Exemple 3 :

Soit $E/\mathbb{R}$ définie par E : $y^2 = (x+2)^3$.

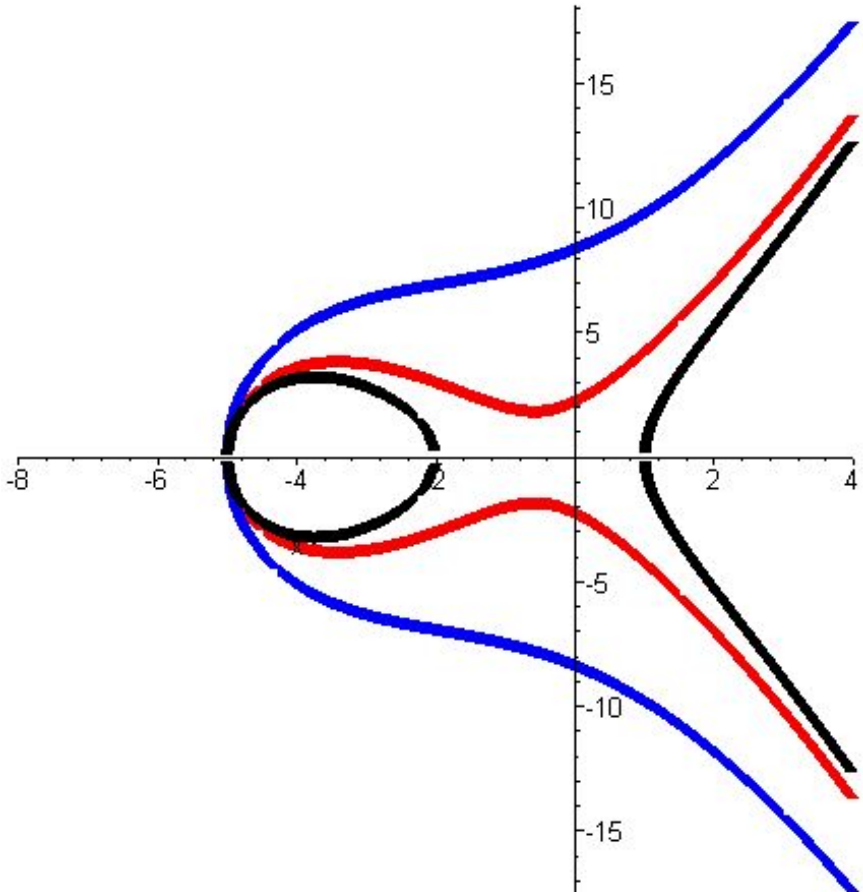
Ceci n'est pas une courbe elliptique car $\Delta = 0$.



Les courbes elliptiques : Représentation graphique

Exemple 5 :

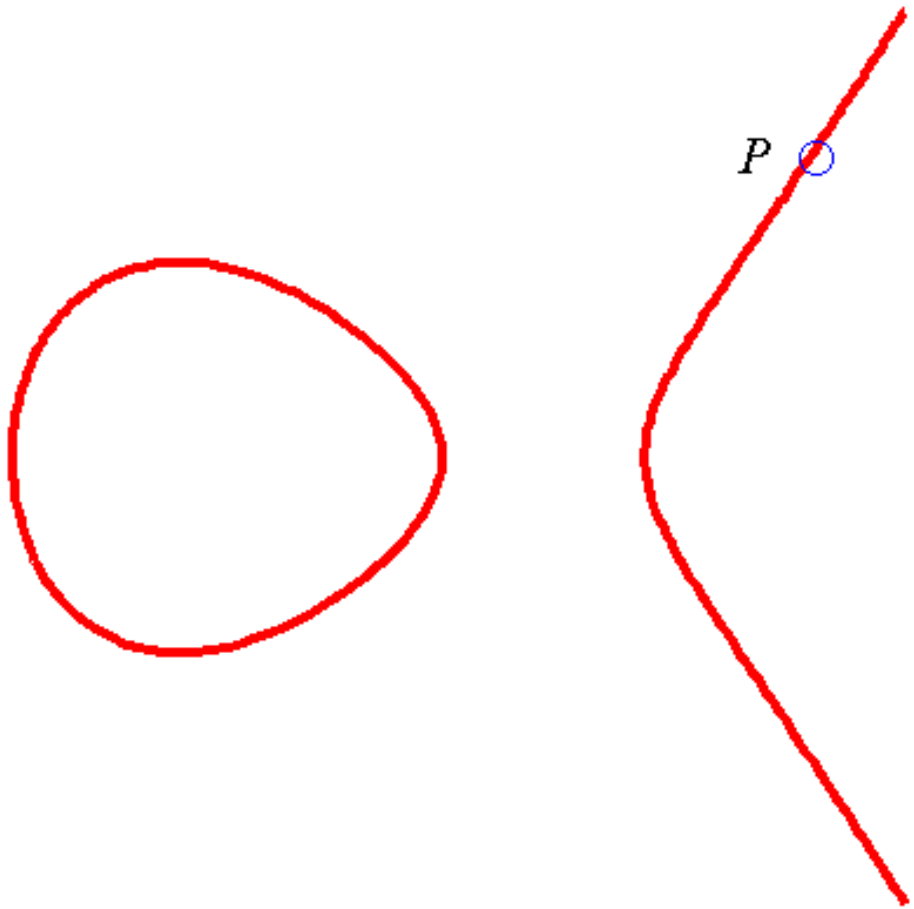
Soit $E/\mathbb{R}$ définie par E : $y^2 = (x-1)(x+2)(x+5), (x^2+x+14)(x+5), (x^2+x+1)(x+5)$.



Les courbes elliptiques : L'opposé d'un point

Pour placer le point $-P$.

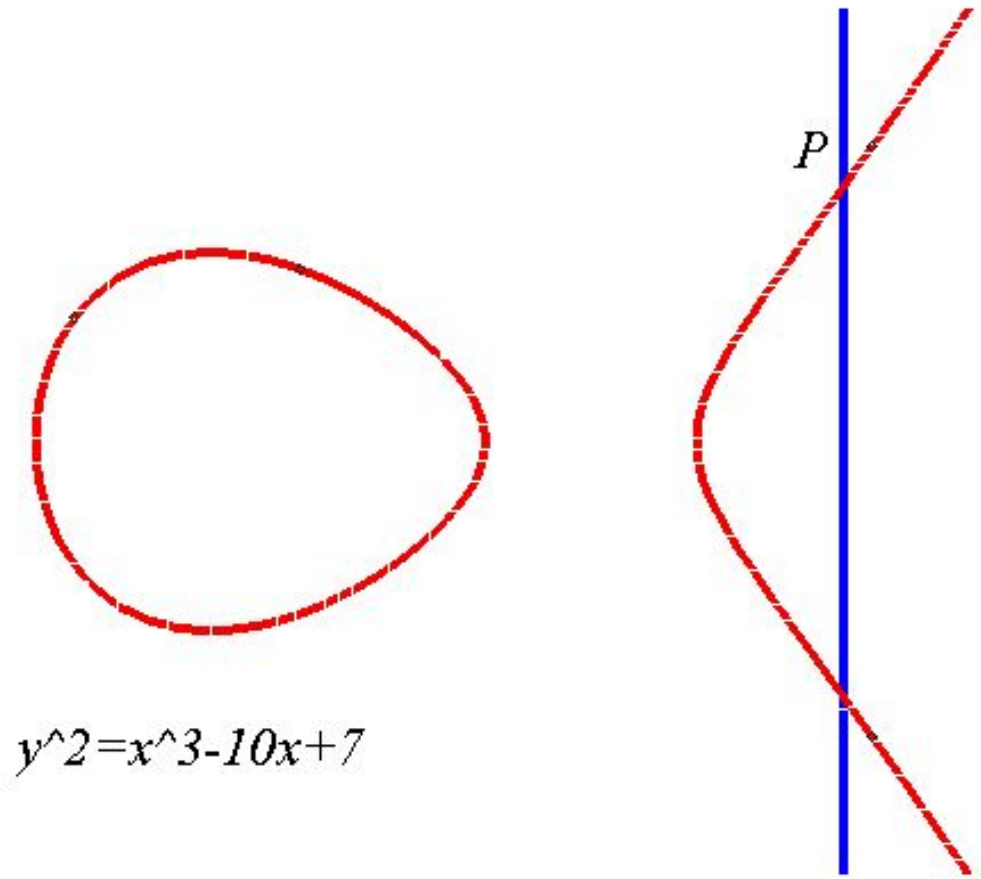
P est un point de la courbe.



Les courbes elliptiques : L'opposé d'un point

Pour placer le point $-P$.

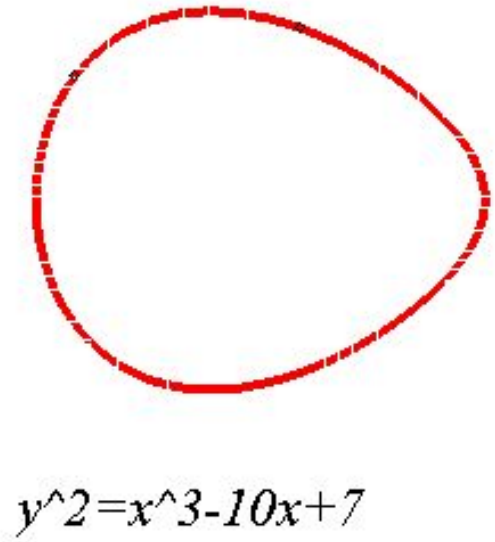
On trace la verticale qui passe par P.

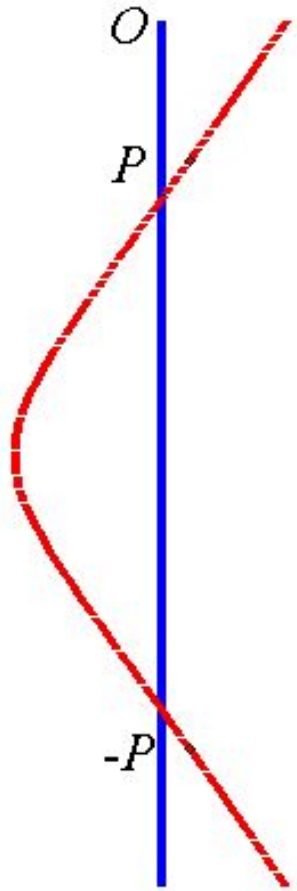


Les courbes elliptiques : L'opposé d'un point

Pour placer le point $-P$.

On obtient le point $-P$ à l'intersection avec la courbe.

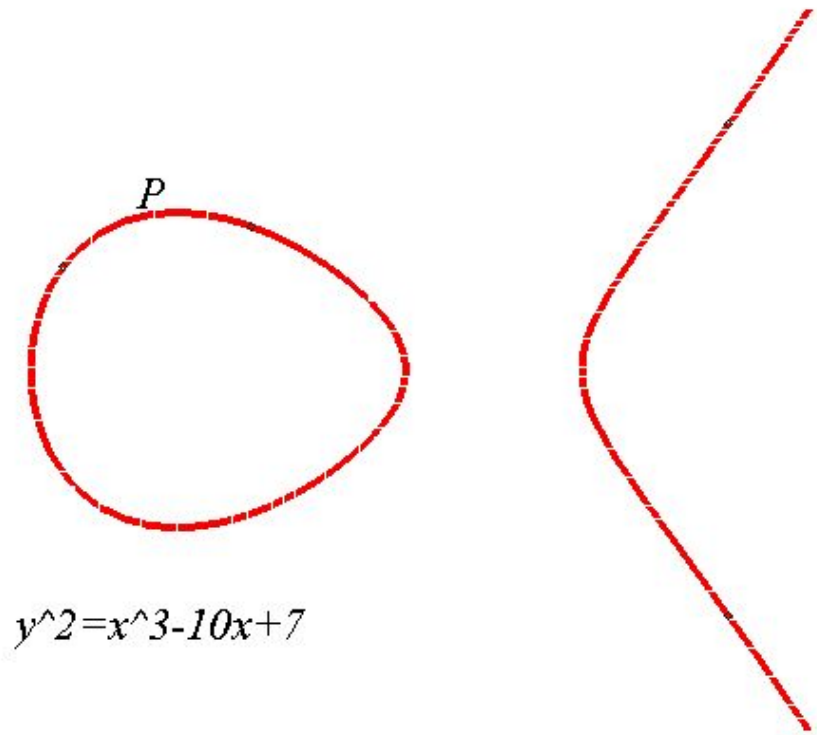




Les courbes elliptiques : Doubler un point

Soit $E/\mathbb{K}$ une courbe elliptique et $P \in E(\mathbb{K})$.

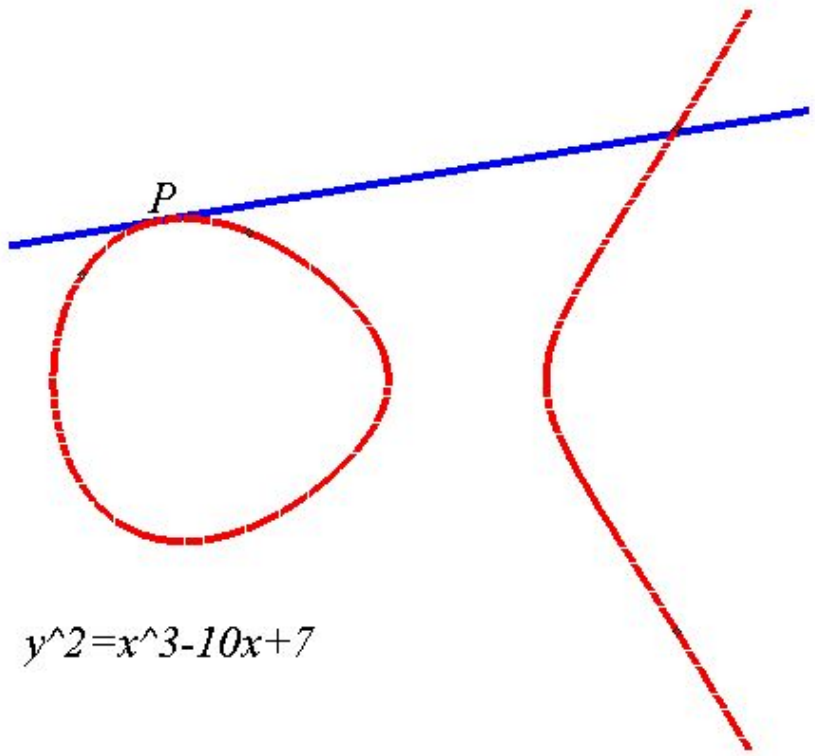
Comment placer le point $2P$ si $2y + a_1x + a_3 = 0 \neq 0$?



Les courbes elliptiques : Doubler un point

Pour placer le point $2P$ si $2y + a_1x + a_3 \neq 0$.

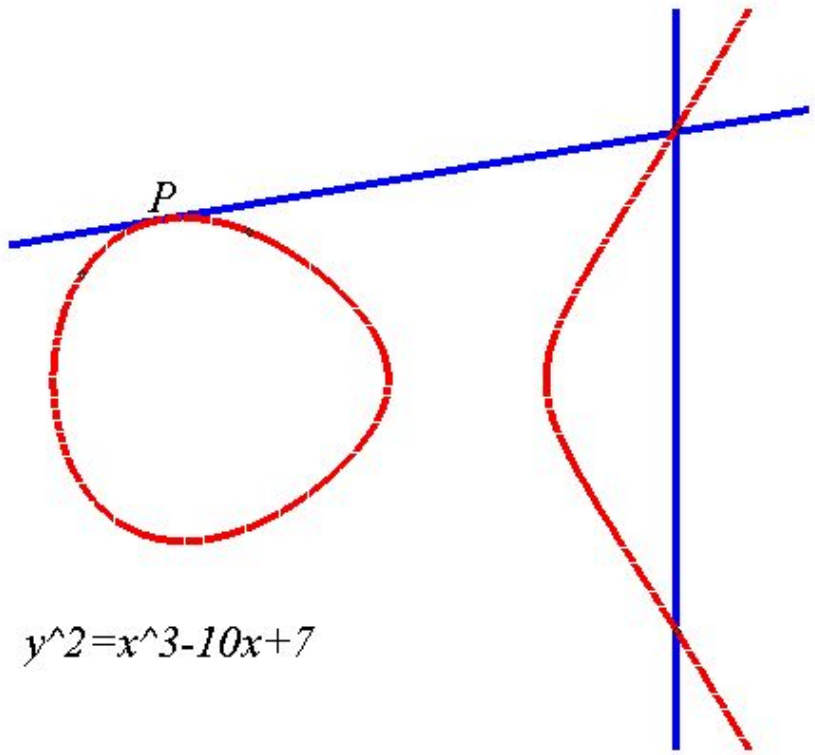
On trace la tangente en P.



Les courbes elliptiques : Doubler un point

Pour placer le point $2P$ si $2y + a_1x + a_3 \neq 0$.

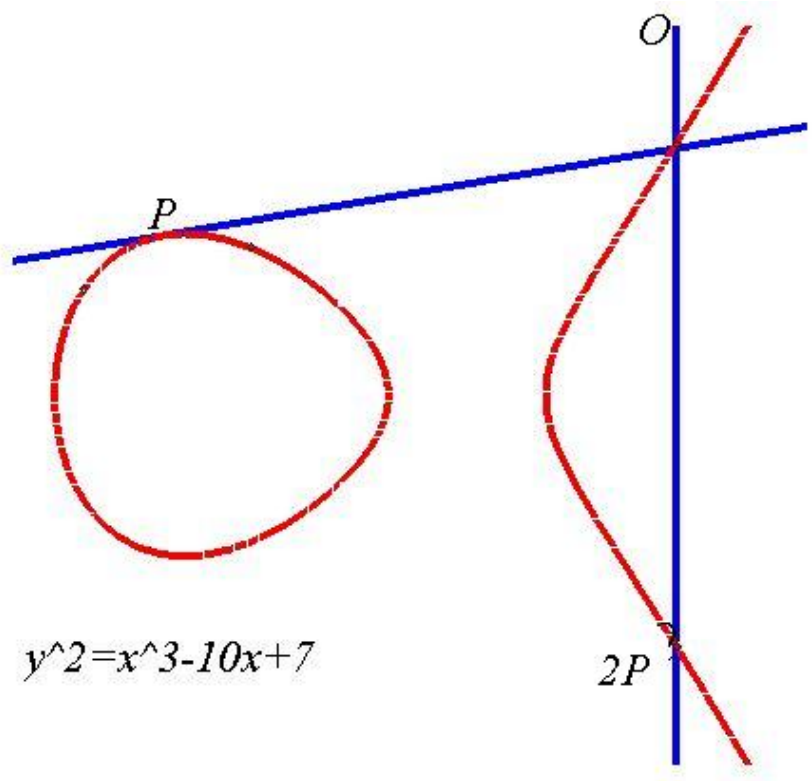
On trace la verticale.



Les courbes elliptiques : Doubler un point

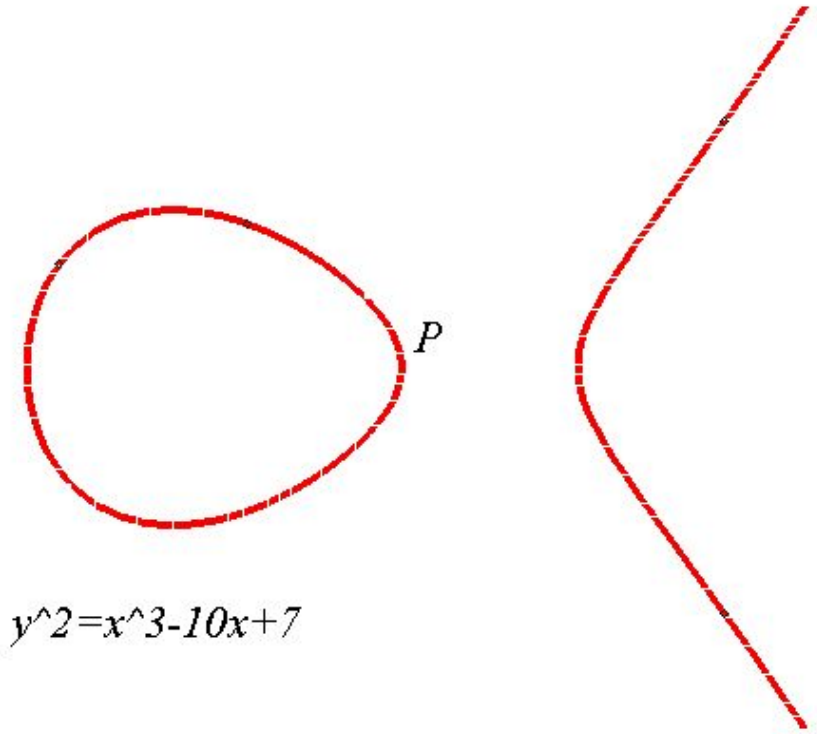
Pour placer le point $2P$ si $2y + a_1x + a_3 \neq 0$.

On obtient le point $2P$.



Les courbes elliptiques : Doubler un point

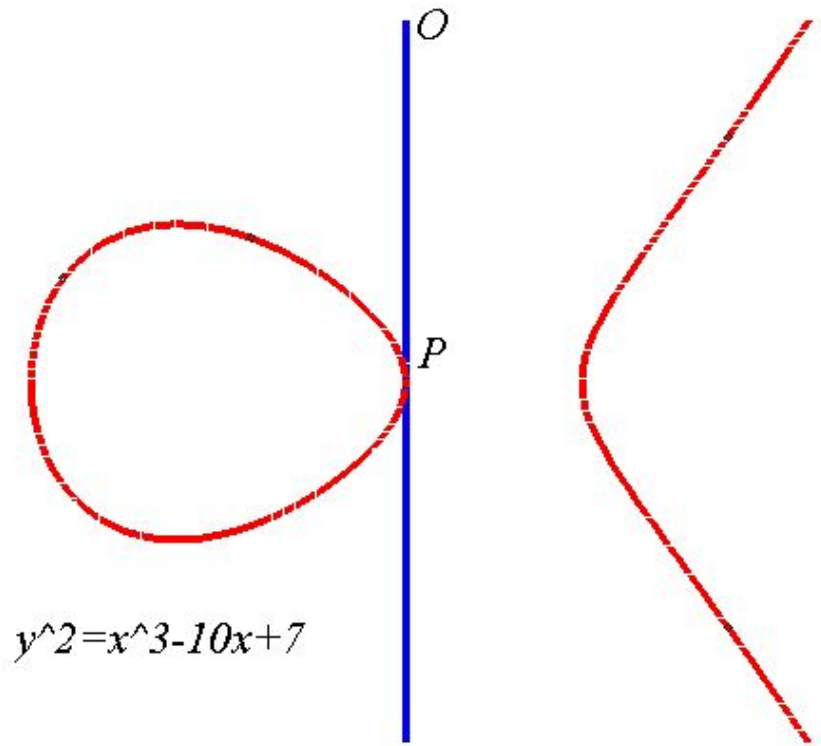
Comment placer le point $2P$ si $2y + a_1x + a_3 = 0$?



Les courbes elliptiques : Doubler un point

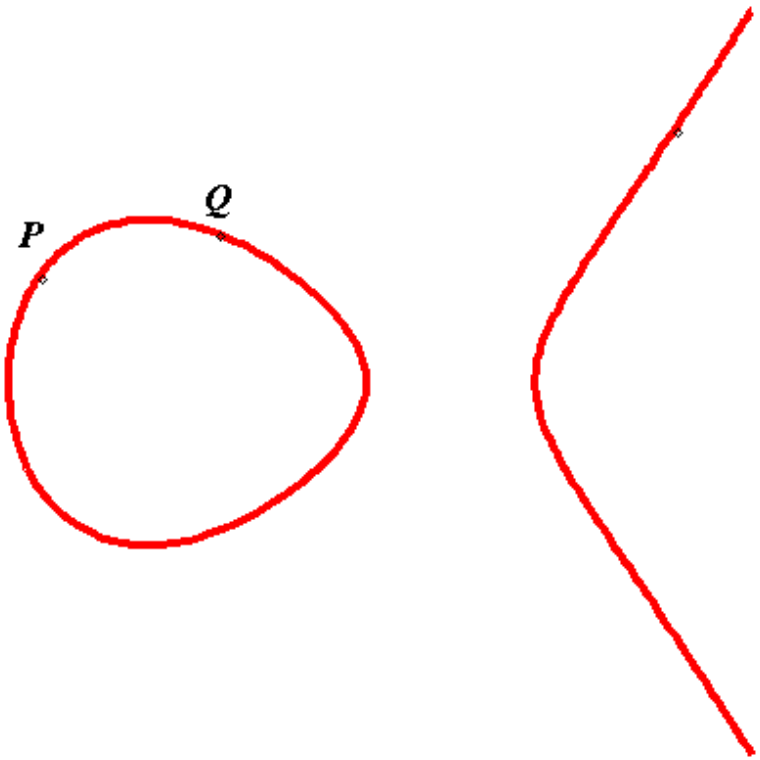
Pour placer le point $2P$ si $2y + a_1x + a_3 = 0$.

On trace la verticale en P. On obtient $2P = \mathcal{O}$.



Les courbes elliptiques : Additionner deux points différents

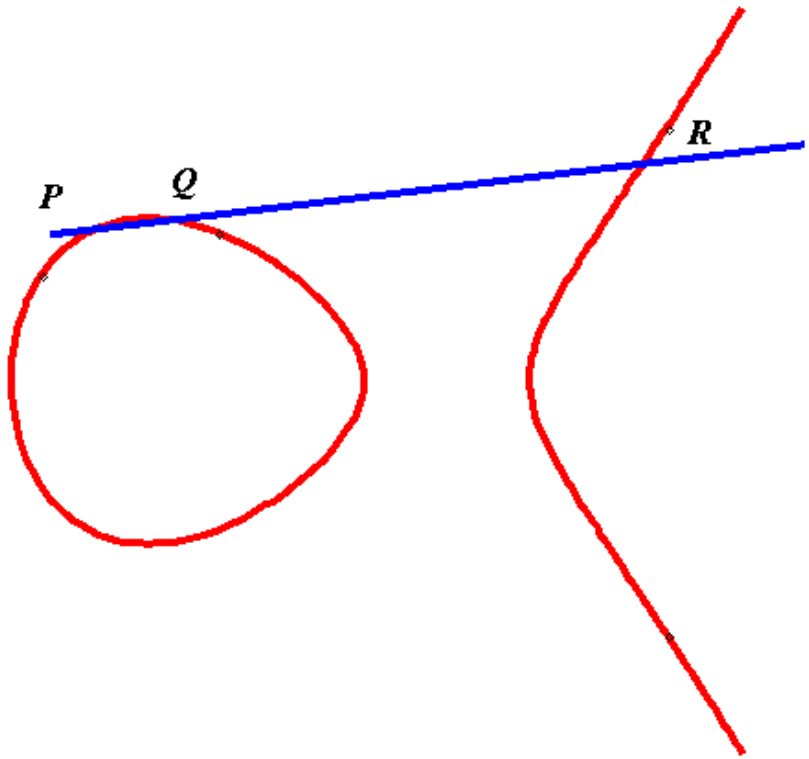
Comment placer le point $P+Q$?



Les courbes elliptiques : Additionner deux points différents

Pour placer le point $P + Q$.

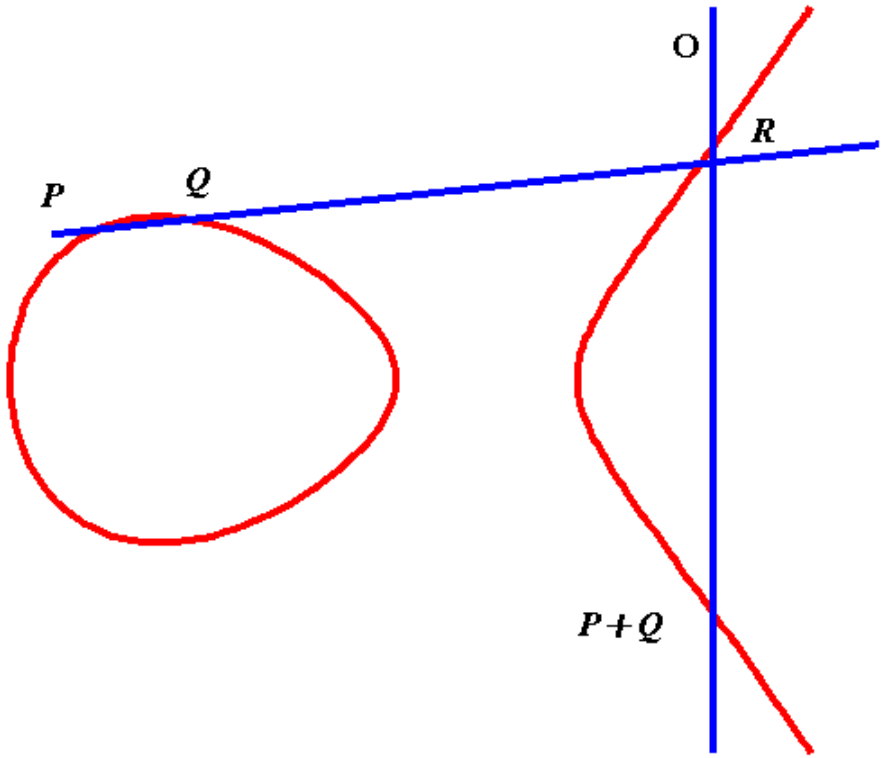
On trace la droite (PQ).



Les courbes elliptiques : Additionner deux points différents

Pour placer le point $P + Q$.

On trace la verticale au 3ème point d'intersection.



ECC

L'arithmétique de ECC

- E une courbe elliptique défine sur $\mathbb{F}_p$, P un générateur de $E(\mathbb{F}_p)$.
- Les opérations consistent en des exponentiations .

$$Q = kP, \quad P_1 + kP.$$

- Complexité de l'exponentiation $Q = kP$: $\mathcal{O}(\log(k))$.

- **Problème difficile: Le logarithme discret elliptic (ECDLP)**

Soient P et Q deux points d'une courbe elliptique E. Déterminer un entier n tel que $nP = Q$.

ECC

L'arithmétique de ECC

- E une courbe elliptique défine sur $\mathbb{F}_p$, P un générateur de $E(\mathbb{F}_p)$.
- Les opérations consistent en des exponentiations .

$$Q = kP, \quad P_1 + kP.$$

- Complexité de l'exponentiation $Q = kP$: $\mathcal{O}(\log(k))$.

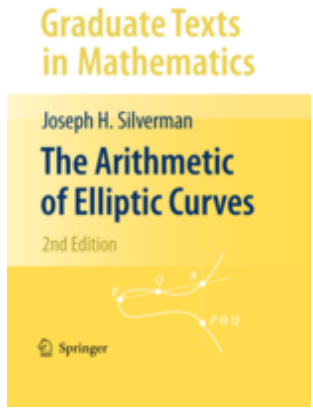
- **Problème difficile: Le logarithme discret elliptic (ECDLP)**

Soient P et Q deux points d'une courbe elliptique E. Déterminer un entier n tel que $nP = Q$.

Le présent et le futur

NTRU

- Inventé en 1996 par Hoffstein, Pipher et Silverman.



- Problème difficile

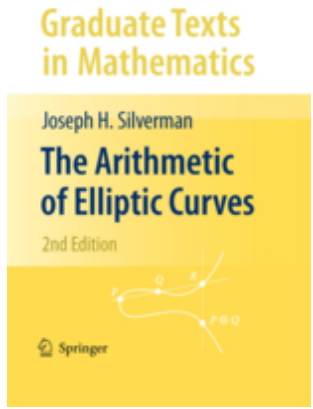
Problème du plus court vecteur (SVP):

Soit B une base d'un réseau L. Déterminer un vecteur non nul de L, le plus court possible pour la norme euclidienne.

Le présent et le futur

NTRU

- Inventé en 1996 par Hoffstein, Pipher et Silverman.



- Problème difficile

Problème du plus court vecteur (SVP):

Soit B une base d'un réseau L. Déterminer un vecteur non nul de L, le plus court possible pour la norme euclidienne.

NTRU

L'arithmétique de NTRU

- N, p, q des entiers.
- $\mathcal{R} = \mathbb{Z}[X]/\left(X^N - 1\right)$.
- Les opérations ont lieu dans l'anneau $(\mathcal{R}, +, *)$.

$$
\begin{aligned}
f &= (f_0, f_1, \cdots, f_{N-1}) = \sum_{i=0}^{N-1} f_i X^i, \\
g &= (g_0, g_1, \cdots, g_{N-1}) = \sum_{i=0}^{N-1} g_i X^i, \\
f + g &= (f_0 + g_0, f_1 + g_1, \cdots, f_{N-1} + g_{N-1}), \\
f * g &= h = (h_0, h_1, \cdots, h_{N-1}), \quad h_k = \sum_{i+j \equiv k \mod N} f_i g_j.
\end{aligned}
$$

NTRU

L'arithmétique de NTRU

- **Problème difficile : Factorisation**

Soit $h \in \mathcal{R}$. Déterminer deux polynômes courts f et g tels que $f * h = g$.

- **Problème du plus court vecteur (SVP):**

Soit B une base d'un réseau L. Déterminer un vecteur non nul de L, le plus court possible pour la norme euclidienne.

NTRU

L'arithmétique de NTRU

- **Problème difficile : Factorisation**

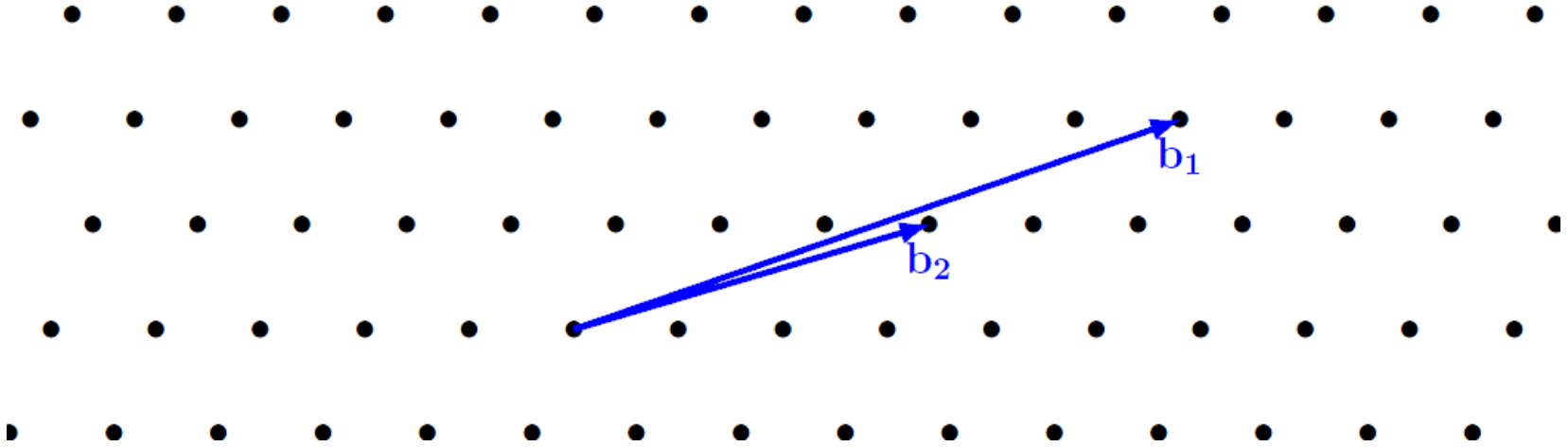
> *Soit $h \in \mathcal{R}$. Déterminer deux polynômes courts f et g tels que $f * h = g$.*

- **Problème du plus court vecteur (SVP):**

> *Soit B une base d'un réseau L. Déterminer un vecteur non nul de L, le plus court possible pour la norme euclidienne.*

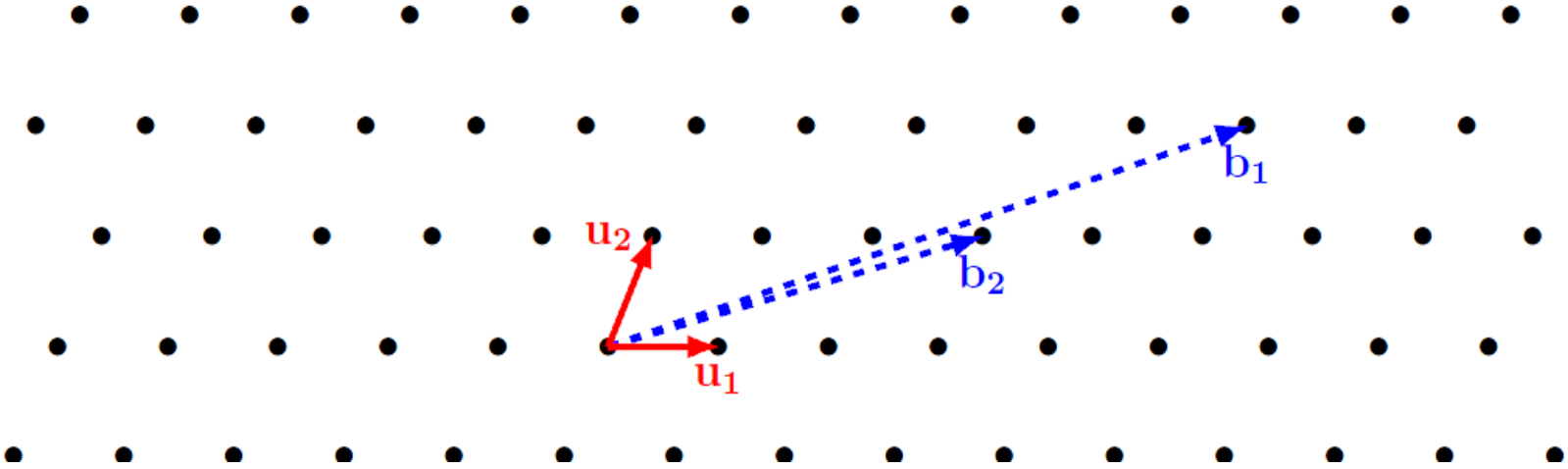
Le présent

Le problème SVP



Le présent

Le problème SVP



Le présent

Comparaisons des clés

Date limite	Symétrique	RSA	El Gamal	ECC
2012	80	1248	160	160
2020	96	1776	192	192
2030	112	2432	224	224
2040	128	3248	256	256
-	256	15424	512	512

Sources Ecrypt II, 2010

Le présent

Comparaisons des attaques

Cryptosystème	Méthode	Complexité
RSA	Number Field Sieve	Sous-Exponentielle
El Gamal	Index Calculus	Sous-Exponentielle
ECC	Rho de Pollard	Exponentielle
NTRU	LLL	Exponentielle

CONTENU

1 Le passé

2 Le présent

3 Le futur

4 Conclusion

Le futur

Post quantum cryptography

- Avec les ordinateurs quantiques, certains cryptosystèmes disparaîtront à cause de l'algorithme de Shor.
  1. RSA,
  2. El Gamal,
  3. ECC,
  4. Digital Signature Algorithm (DSA),
  5. Elliptic Curve Digital Signature Algorithm (ECDSA)...
- Certains cryptosystèmes peuvent subsister.

Le futur

Post quantum cryptography

- Avec les ordinateurs quantiques, certains cryptosystèmes disparaîtront à cause de l'algorithme de Shor.
  1. RSA,
  2. El Gamal,
  3. ECC,
  4. Digital Signature Algorithm (DSA),
  5. Elliptic Curve Digital Signature Algorithm (ECDSA)...
- Certains cryptosystèmes peuvent subsister.

Le futur

Post quantum cryptography

- Avec les ordinateurs quantiques, certains cryptosystèmes disparaîtront à cause de l'algorithme de Shor.
  1. RSA,
  2. El Gamal,
  3. ECC,
  4. Digital Signature Algorithm (DSA),
  5. Elliptic Curve Digital Signature Algorithm (ECDSA)...
- Certains cryptosystèmes peuvent subsister.

Le futur

Post quantum cryptography

- Avec les ordinateurs quantiques, certains cryptosystèmes disparaîtront à cause de l'algorithme de Shor.
  1. RSA,
  2. El Gamal,
  3. ECC,
  4. Digital Signature Algorithm (DSA),
  5. Elliptic Curve Digital Signature Algorithm (ECDSA)...
- Certains cryptosystèmes peuvent subsister.

Le futur

Post quantum cryptography

- Avec les ordinateurs quantiques, certains cryptosystèmes disparaîtront à cause de l'algorithme de Shor.
  1. RSA,
  2. El Gamal,
  3. ECC,
  4. Digital Signature Algorithm (DSA),
  5. Elliptic Curve Digital Signature Algorithm (ECDSA)...
- Certains cryptosystèmes peuvent subsister.

Le futur

Post quantum cryptography

- Avec les ordinateurs quantiques, certains cryptosystèmes disparaîtront à cause de l'algorithme de Shor.
  1. RSA,
  2. El Gamal,
  3. ECC,
  4. Digital Signature Algorithm (DSA),
  5. Elliptic Curve Digital Signature Algorithm (ECDSA)...
- Certains cryptosystèmes peuvent subsister.
  1. Cryptosystèmes basés sur les codes : McEliece, Niederreiter.

Le futur

Post quantum cryptography

- Avec les ordinateurs quantiques, certains cryptosystèmes disparaîtront à cause de l'algorithme de Shor.
  1. RSA,
  2. El Gamal,
  3. ECC,
  4. Digital Signature Algorithm (DSA),
  5. Elliptic Curve Digital Signature Algorithm (ECDSA)...
- Certains cryptosystèmes peuvent subsister.
  1. Cryptosystèmes basés sur les codes : McEliece, Niederreiter.
  2. Cryptosystèmes basés sur les réseaux : NTRU, GGH, LWE.
  3. Cryptosystèmes basés sur les équations quadratiques à plusieurs variables : HFEv, Sflash.
  4. Cryptosystèmes à clé secrète : AES.

Le futur

Post quantum cryptography

- Avec les ordinateurs quantiques, certains cryptosystèmes disparaîtront à cause de l'algorithme de Shor.
  1. RSA,
  2. El Gamal,
  3. ECC,
  4. Digital Signature Algorithm (DSA),
  5. Elliptic Curve Digital Signature Algorithm (ECDSA)...
- Certains cryptosystèmes peuvent subsister.
  1. Cryptosystèmes basés sur les codes : McEliece, Niederreiter.
  2. Cryptosystèmes basés sur les réseaux : NTRU, GGH, LWE.
  3. Cryptosystèmes basés sur les équations quadratiques à plusieurs variables : HFEv, Sflash.
  4. Cryptosystèmes à clé secrète : AES.

Le futur

Post quantum cryptography

- Avec les ordinateurs quantiques, certains cryptosystèmes disparaîtront à cause de l'algorithme de Shor.
  1. RSA,
  2. El Gamal,
  3. ECC,
  4. Digital Signature Algorithm (DSA),
  5. Elliptic Curve Digital Signature Algorithm (ECDSA)...
- Certains cryptosystèmes peuvent subsister.
  1. Cryptosystèmes basés sur les codes : McEliece, Niederreiter.
  2. Cryptosystèmes basés sur les réseaux : NTRU, GGH, LWE.
  3. Cryptosystèmes basés sur les équations quadratiques à plusieurs variables : HFEv, Sflash.
  4. Cryptosystèmes à clé secrète : AES.

Le futur

Post quantum cryptography

- Avec les ordinateurs quantiques, certains cryptosystèmes disparaîtront à cause de l'algorithme de Shor.
  1. RSA,
  2. El Gamal,
  3. ECC,
  4. Digital Signature Algorithm (DSA),
  5. Elliptic Curve Digital Signature Algorithm (ECDSA)...
- Certains cryptosystèmes peuvent subsister.
  1. Cryptosystèmes basés sur les codes : McEliece, Niederreiter.
  2. Cryptosystèmes basés sur les réseaux : NTRU, GGH, LWE.
  3. Cryptosystèmes basés sur les équations quadratiques à plusieurs variables : HFEv, Sflash.
  4. Cryptosystèmes à clé secrète : AES.

Le futur

Post quantum cryptography

- Avec les ordinateurs quantiques, certains cryptosystèmes disparaîtront à cause de l'algorithme de Shor.
  1. RSA,
  2. El Gamal,
  3. ECC,
  4. Digital Signature Algorithm (DSA),
  5. Elliptic Curve Digital Signature Algorithm (ECDSA)...
- Certains cryptosystèmes peuvent subsister.
  1. Cryptosystèmes basés sur les codes : McEliece, Niederreiter.
  2. Cryptosystèmes basés sur les réseaux : NTRU, GGH, LWE.
  3. Cryptosystèmes basés sur les équations quadratiques à plusieurs variables : HFEv, Sflash.
  4. Cryptosystèmes à clé secrète : AES.

Le futur

L'algorithme de Shor, 1994

- **Entrée :** Un entier n.
  1. Choisir aléatoirement un entier x avec $2 \leq x \leq n-1$.
  2. Si $\gcd(x,n) \neq 1$, sortir $\gcd(x,n)$.
  3. Détermienr la période r de la suite $(x^a)_{a \geq 0} \pmod n$.
  4. Si r est impair ou si $x^{r/2} \equiv -1 \pmod n$, alors aller à l'étape 1.
  5. Sortir $\gcd\left(n, x^{r/2} \pm 1\right)$.
- **Sortie :** Un facteur de n.
- La partie quantique de l'algorithme est l'étape 3.

Le futur

L'algorithme de Shor, 1994

- **Entrée :** Un entier n.
  1. Choisir aléatoirement un entier x avec $2 \leq x \leq n-1$.
  2. Si $\gcd(x,n) \neq 1$, sortir $\gcd(x,n)$.
  3. Détermienr la période r de la suite $(x^a)_{a\geq 0} \pmod n$.
  4. Si r est impair ou si $x^{r/2} \equiv -1 \pmod n$, alors aller à l'étape 1.
  5. Sortir $\gcd\left(n, x^{r/2} \pm 1\right)$.
- **Sortie :** Un facteur de n.
- La partie quantique de l'algorithme est l'étape 3.

Le futur

L'algorithme de Shor, 1994

- **Entrée :** Un entier n.
  1. Choisir aléatoirement un entier x avec $2 \leq x \leq n-1$.
  2. Si $\gcd(x,n) \neq 1$, sortir $\gcd(x,n)$.
  3. Détermienr la période r de la suite $(x^a)_{a\geq 0} \pmod n$.
  4. Si r est impair ou si $x^{r/2} \equiv -1 \pmod n$, alors aller à l'étape 1.
  5. Sortir $\gcd\left(n, x^{r/2} \pm 1\right)$.
- **Sortie :** Un facteur de n.
- La partie quantique de l'algorithme est l'étape 3.

Le futur

L'algorithme de Shor, 1994

- **Entrée :** Un entier n.
  1. Choisir aléatoirement un entier x avec $2 \leq x \leq n-1$.
  2. Si $\gcd(x,n) \neq 1$, sortir $\gcd(x,n)$.
  3. Détermienr la période r de la suite $(x^a)_{a\geq 0} \pmod n$.
  4. Si r est impair ou si $x^{r/2} \equiv -1 \pmod n$, alors aller à l'étape 1.
  5. Sortir $\gcd\left(n, x^{r/2} \pm 1\right)$.
- **Sortie :** Un facteur de n.
- La partie quantique de l'algorithme est l'étape 3.

Le futur

L'algorithme de Shor, 1994

- **Entrée :** Un entier n.
  1. Choisir aléatoirement un entier x avec $2 \leq x \leq n-1$.
  2. Si $\gcd(x,n) \neq 1$, sortir $\gcd(x,n)$.
  3. Détermienr la période r de la suite $(x^a)_{a\geq 0} \pmod n$.
  4. Si r est impair ou si $x^{r/2} \equiv -1 \pmod n$, alors aller à l'étape 1.
  5. Sortir $\gcd\left(n, x^{r/2} \pm 1\right)$.
- **Sortie :** Un facteur de n.
- La partie quantique de l'algorithme est l'étape 3.

Le futur

L'algorithme de Shor, 1994

- **Entrée :** Un entier n.
  1. Choisir aléatoirement un entier x avec $2 \leq x \leq n-1$.
  2. Si $\gcd(x,n) \neq 1$, sortir $\gcd(x,n)$.
  3. Détermienr la période r de la suite $(x^a)_{a\geq 0} \pmod n$.
  4. Si r est impair ou si $x^{r/2} \equiv -1 \pmod n$, alors aller à l'étape 1.
  5. Sortir $\gcd\left(n, x^{r/2} \pm 1\right)$.
- **Sortie :** Un facteur de n.
- La partie quantique de l'algorithme est l'étape 3.

Le futur

L'algorithme de Shor, 1994

- **Entrée :** Un entier n.
  1. Choisir aléatoirement un entier x avec $2 \leq x \leq n-1$.
  2. Si $\gcd(x,n) \neq 1$, sortir $\gcd(x,n)$.
  3. Détermienr la période r de la suite $(x^a)_{a\geq 0} \pmod n$.
  4. Si r est impair ou si $x^{r/2} \equiv -1 \pmod n$, alors aller à l'étape 1.
  5. Sortir $\gcd\left(n, x^{r/2} \pm 1\right)$.
- **Sortie :** Un facteur de n.
- La partie quantique de l'algorithme est l'étape 3.

Ordinateur quantique en 2...?

Généralités

1. Deux états de base: $|0\rangle$ et $|1\rangle$.
2. Un qubit est de la forme $\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, avec $\alpha, \beta \in \mathbb{C}$ et $|\alpha|^2 + |\beta|^2 = 1$.
3. La mesure d'un qubit $\psi\rangle$ ne peut donner que $|0\rangle$ avec la probabilité $|\alpha|^2$ ou $|1\rangle$ avec la probabilité $|\beta|^2$.
4. La puissance est exponentielle en le nombre de qubits.
5. Le premier ordinateur quantique: 1996, IBM, avec 2 qubits.
6. 2007, D-Wave Systems, avec 16 qubits.

CONTENU

1 Le passé

2 Le présent

3 Le futur

4 Conclusion

Le futur

Le futur non quantique

- Le présent est pour RSA et El Gamal et très peu pour ECC et NTRU.
- Le futur proche peut être en faveur de ECC et NTRU.

Le futur quantique

- Le futur est pour les cryptosystèmes post quantiques : NTRU, McEliece, ...

- A moins que les cryptosystèmes du futur soit basés sur le calcul quantique: BB84.

Le futur

Le futur non quantique

- Le présent est pour RSA et El Gamal et très peu pour ECC et NTRU.
- Le futur proche peut être en faveur de ECC et NTRU.

Le futur quantique

- Le futur est pour les cryptosystèmes post quantiques : NTRU, McEliece, ...

- A moins que les cryptosystèmes du futur soit basés sur le calcul quantique: BB84.

Le futur

Le futur non quantique

- Le présent est pour RSA et El Gamal et très peu pour ECC et NTRU.
- Le futur proche peut être en faveur de ECC et NTRU.

Le futur quantique

- Le futur est pour les cryptosystèmes post quantiques : NTRU, McEliece, ...

- A moins que les cryptosystèmes du futur soit basés sur le calcul quantique: BB84.

Maroc Numeric 2013

http://www.egov.ma/Documents/MarocNumeric2013.pdf

- "Le Plan Maroc Numeric a été construit autour d'une vision et des ambitions claires pour le Maroc, visant à le positionner parmi les pays émergents dynamiques dans les Technologies de l'Information".
- "Le manque de confiance des usagers dans la sécurité des échanges électroniques constitue un frein majeur au développement des usages des TI".

Maroc Numeric 2013

http://www.egov.ma/Documents/MarocNumeric2013.pdf

- "Le Plan Maroc Numeric a été construit autour d'une vision et des ambitions claires pour le Maroc, visant à le positionner parmi les pays émergents dynamiques dans les Technologies de l'Information".
- "Le manque de confiance des usagers dans la sécurité des échanges électroniques constitue un frein majeur au développement des usages des TI".

Maroc Numeric 2013

http://www.egov.ma/Documents/MarocNumeric2013.pdf

- “Le Plan Maroc Numeric a été construit autour d’une vision et des ambitions claires pour le Maroc, visant à le positionner parmi les pays émergents dynamiques dans les Technologies de l’Information”.
- “Le manque de confiance des usagers dans la sécurité des échanges électroniques constitue un frein majeur au développement des usages des TI”.

Maroc Numeric 2013

http://www.egov.ma/Documents/MarocNumeric2013.pdf

- “La protection des échanges électroniques se réalise également par le développement des prestations de certification électronique et de cryptographie.
- “En liaison avec le Conseil National des Terchnologies de l’Information et de l’Economie Numérique, un comité de la sécurité des systèmes d’information sera créé et prendra en charge notamment l’élaboration de la politique relative à la protection des infrastructures critiques du Royaume”.

Maroc Numeric 2013

http://www.egov.ma/Documents/MarocNumeric2013.pdf

- "La protection des échanges électroniques se réalise également par le développement des prestations de certification électronique et de cryptographie.
- "En liaison avec le Conseil National des Terchnologies de l'Information et de l'Economie Numérique, un comité de la sécurité des systèmes d'information sera créé et prendra en charge notamment l'élaboration de la politique relative à la protection des infrastructures critiques du Royaume".

Maroc Numeric 2013

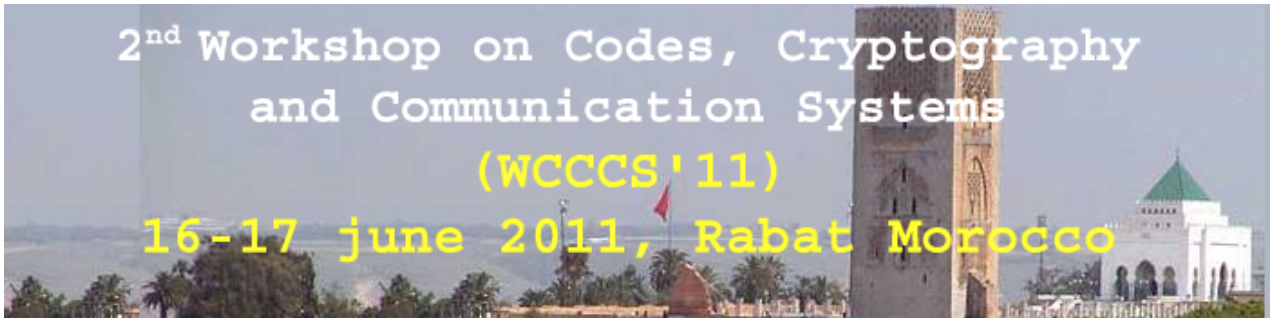
http://www.egov.ma/Documents/MarocNumeric2013.pdf

- “La protection des échanges électroniques se réalise également par le développement des prestations de certification électronique et de cryptographie.
- “En liaison avec le Conseil National des Terchnologies de l’Information et de l’Economie Numérique, un comité de la sécurité des systèmes d’information sera créé et prendra en charge notamment l’élaboration de la politique relative à la protection des infrastructures critiques du Royaume”.

Merci

شكرا

Centre National pour la Recherche Scientifique et Technique


2nd Workshop on Codes, Cryptography and Communication Systems
(WCCCS'11)
16-17 june 2011, Rabat Morocco