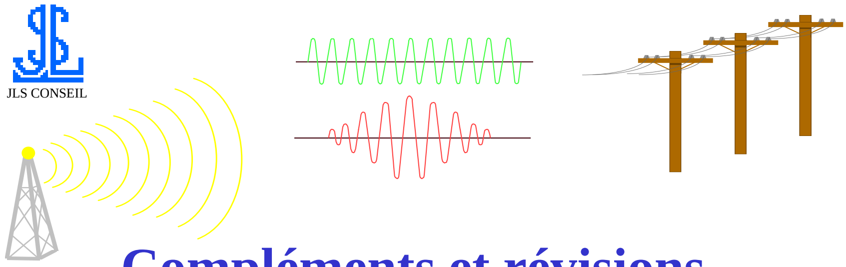


# Compléments et révisions

*Jean-Luc Stehlé*

*Bases mathématiques pour la sécurité informatique*

*EPITA*

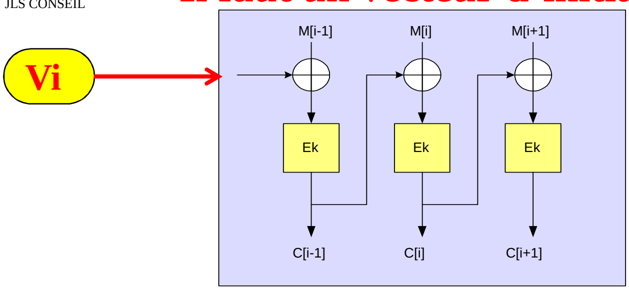
*13 juin 2013*

Jean-Luc.Stehle@NormaleSup.org



## Mode chaîné CBC (ciffer block chaining)

## Il faut un vecteur d'initialisation




**VI n'est pas nécessairement confidentiel.**
**Est là pour assurer que le même bloc n'est jamais codé de la même façon**

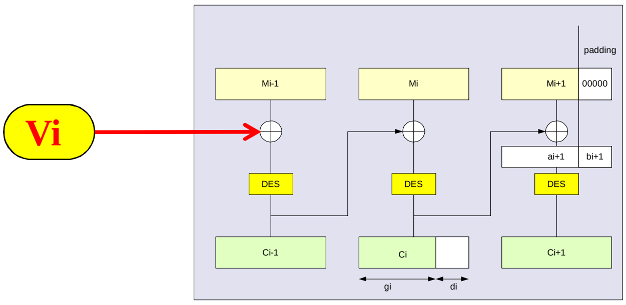
**Communication de type « stream »**
**Chiffrage de supports séquentiels (bande magnétique de sauvegarde)**
**Messages séparés indépendants les uns des autres**
**Disques chiffrés avec accès direct**

**Chaînage secteur par secteur**
**VI dépendant du N° de secteur**

JLS CONSEIL

# Mode chaîné CTS (ciffer block stealing)

## Cas des tout petits messages




**Il faut transmettre au moins un bloc**



JLS CONSEIL

# Mode CTR et vecteur d'initialisation

- **On chiffre un compteur, le résultat du chiffrement est XORé avec le texte à chiffrer/déchiffrer**
  - **Chiffrement = déchiffrement**
  - **Pratique pour le chiffrement de supports à accès direct**
    - ***Inutile de tout lire pour déchiffrer un secteur***

  **Masque[n] = $DES_K$( f(n))**

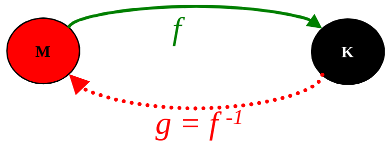
  **CT[n] = PT[n] ⊕ Masque[n]**

- **Utilisable même pour des messages très courts**

- **Nécessité d'une initialisation** **Masque[n] = $DES_K$( f(n+INI))**
  **pour ne pas toujours utiliser le même masque**

JLS CONSEIL

## Recherche de bonnes fonctions à sens unique




**Exemple dans Z/NZ :**

- **Exponentiation modulaire : f(x) = $a^x$**
- **Logarithme discret : retrouver x connaissant y = $a^x$**

**Applications : Diffie Hellman, Authentification par défi réponse, …**

**Trouver des groupes (G,• ) où l'exponentielle de base a∈G est une bonne fonction à sens unique**

- **Exponentiation dans G : f(x) = a•a •a •…. •a (x facteurs)**
- **Logarithme de base a dans G : retrouver x connaissant f(x)**




JLS CONSEIL

## Un peu de géométrie algébrique : Espaces projectifs

- **Plan : ensemble des points d'un espace vectoriel de dimension 2 avec coordonnées (x,y)**
- **Plan projectif : coordonnées (X,Y,Z)**
  - **Non tous trois simultanément nuls**
  - **Définis à une constante multiplicative près**

**(X,Y,Z) et ($\lambda$X, $\lambda$Y, $\lambda$Z), avec $\lambda \neq 0$ représentent le même point**

**Pour Z≠0, x=X/Z y=Y/Z**

**Pour Z=0, (X,Y,0) est le point à l'infini dans la direction (X,Y)**

**Le plan projectif apparaît comme un plan auquel on a rajouté une droite de l'infini**

**On travaille sur R, sur C ou sur un corps quelconque**

JLS CONSEIL

## Un peu de géométrie algébrique : Courbe algébrique

- **Ensemble des points (x,y) du plan vérifiant une équation f(x,y)=0 où f est un polynôme.**
- **Ensemble des points (X,Y,Z) du plan projectif, vérifiant une équation F(X,Y,Z)=0 ou F est un polynôme homogène.**

**Passage de f à F:**

| | | | |
|---|---|---|---|
| Hyperbole : | $f(x,y) = xy-1$ | $\leftrightarrow$ | $F(X,Y,Z) = XY - Z^2$ |
| | $f(x,y) = y^2-x^2-1$ | $\leftrightarrow$ | $F(X,Y,Z) = Y^2 - X^2 - Z^2$ |
| Cbe Elliptique: | $f(x,y) = y^2-x^3-px-q$ | $\leftrightarrow$ | $F(X,Y,Z) = Y^2Z - X^3 - pXZ^2 - Z^3$ |

Les points à l'infini sont les points (X,Y,Z) vérifiant Z=0 et F(X,Y,Z) =0

**On travaille sur R, sur C ou sur un corps quelconque**




JLS CONSEIL

## Un peu de géométrie algébrique : Fonction rationnelle sur une courbe algébrique

**Fonction R(X,Y,Z) = P(X,Y,Z)/Q(X,Y,Z),**

**Quotient de deux polynômes homogènes de même degré**

**On s'intéresse uniquement aux valeurs de la fonction sur l'ensemble $\Gamma$ des points de la courbe**

**Notion de zéro et de pôle.**

**On associe à un point de la courbe**

**0 si la fonction rationnelle est finie non nulle**

**1, 2, 3, … si c'est un zéro d'ordre 1, 2, 3, …**

**-1,-2,-3,…si c'est un pôle d'ordre 1, 2, 3, …**

**Fonction de $\Gamma$ à valeur dans Z, dont seul un nombre fini de points ont une valeur non nulle.**

**Cette fonction est appelée le Diviseur de la fonction R**

**On travaille sur R, sur C ou sur un corps quelconque**

# Un peu de géométrie algébrique :
## Diviseur sur une courbe algébrique

JLS CONSEIL

$$\Gamma = \{(X,Y,Z) : F(X,Y,Z) = 0\}$$

**F est un polynôme homogène, (X,Y,Z) sont définis à une constante multiplicative près**

- **Diviseur sur $\Gamma$ : Fonction $d$ de $\Gamma$ à valeur dans Z, dont seul un nombre fini de points ont une valeur non nulle.**
- **Les diviseurs forment un groupe abélien $\mathcal{D}$**
- **Ordre d'un diviseur : Somme de ses valeurs sur $\Gamma$**
- **La somme d'un diviseur d'ordre j et d'un diviseur d'ordre k est d'ordre j+k**
- **Les diviseurs d'ordre 0 forment un sous groupe $\mathcal{D}_0$ de $\mathcal{D}$**

**On travaille sur R, sur C ou sur un corps quelconque**




# Un peu de géométrie algébrique :
## Groupe de Jacobi sur une courbe algébrique

JLS CONSEIL

$$\Gamma = \{(X,Y,Z) : F(X,Y,Z) = 0\}$$

- **Théorème : Soit R une fonction rationnelle sur $\Gamma$.**
  **Le diviseur de R est d'ordre 0**
  **R a autant de zéros que de pôles (en comptant les multiplicités) sur $\Gamma$**

- **Définition : Un diviseur sur $\Gamma$ est appelé un diviseur principal s'il existe une fonction rationnelle sur $\Gamma$ dont il est le diviseur.**
- **Théorème : Les diviseurs principaux forment un groupe $\mathcal{P}$ sous-groupe de $\mathcal{D}_0$**

- **Définition : Groupe de Jacobi : $\mathcal{J}$ est le groupe $\mathcal{D}_0/\mathcal{P}$**

**On travaille sur R, sur C ou sur un corps quelconque**

## Un peu de géométrie algébrique :
### Groupe de Jacobi sur une courbe algébrique

JLS CONSEIL

**L'exponentielle dans le groupe de Jacobi d'une courbe algébrique $\Gamma$ bien choisie peut être un très bon candidat pour une fonction à sens unique.**

- **$\Gamma$ sur K = Z/pZ avec p premier à 160 bits donne la même sécurité que l'exponentiation modulaire à 1024 ou 4096 bits**
  - **Calculs directs plus rapide / Calculs inverses plus longs**
  - **Difficultés de programmation, de représentation en machine des points de $\Gamma$**
- **Cas particulier des courbes elliptiques**



## Un peu de géométrie algébrique :
### Propriétés des courbes algébriques de degré 3

JLS CONSEIL

**Théorème : Un polynôme de degré 3 qui a deux racines en a toujours une troisième (quel que soit le corps de base)**

**Corollaire : Si une droite coupe une courbe de degré 3 en deux points, elle la recoupe en un troisième point**

**Théorème : La somme des trois racines (si elles existent) de $x^3+ax^2+bx+c=0$ est égale à $-a$ (quel que soit le corps de base)**

**Cela simplifie le calcul des coordonnées de ce troisième point**

JLS CONSEIL

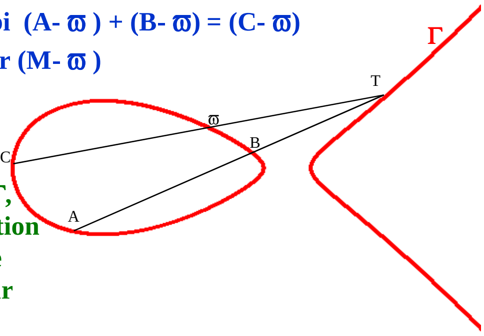
# Un peu de géométrie algébrique :
## Groupe de Jacobi d'une courbe elliptique

### A+B-C-ϖ est un diviseur principal

**C'est celui de P/Q ou P est l'équation de la droite AB et Q celle de la droite Cϖ**

**On a donc, dans le groupe de Jacobi (A- ϖ ) + (B- ϖ) = (C- ϖ)**
**Au point M∈Γ on associe le diviseur (M- ϖ )**

**Cette application réalise un bijection entre le groupe de Jacobi et l'ensemble des points de Γ, et un homomorphisme entre l'addition dans le groupe de Jacobi et la loi de groupe définie géométriquement sur les points de Γ.**




**On travaille sur R, sur C ou sur un corps quelconque**

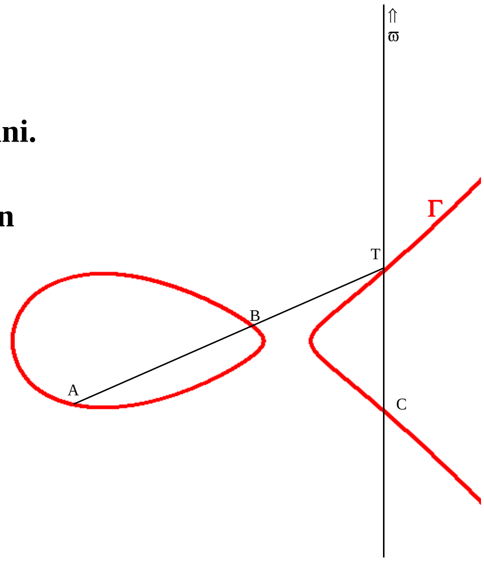



JLS CONSEIL

# Cryptographie en courbe elliptique

**Pour simplifier les calculs, on choisit pour ϖ le point à l'infini.**

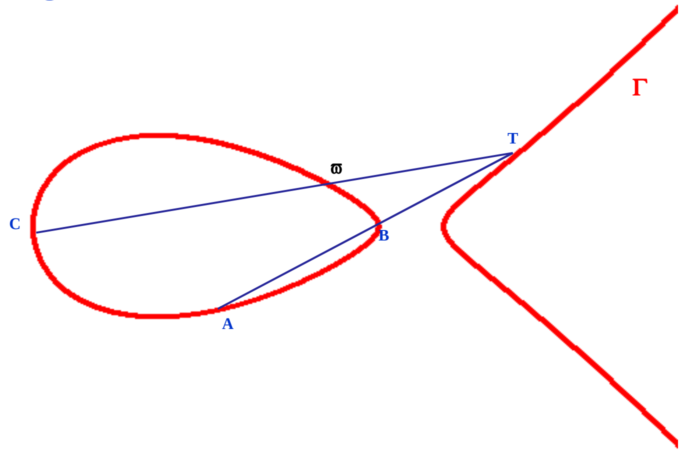
**Il n'y a donc plus à calculer qu'une seule fois l'intersection de Γ avec une droite.**



JLS CONSEIL

# Cryptographie en courbe elliptique
# Changement d'élément neutre

**C = A $+_{\varpi}$ B**







JLS CONSEIL

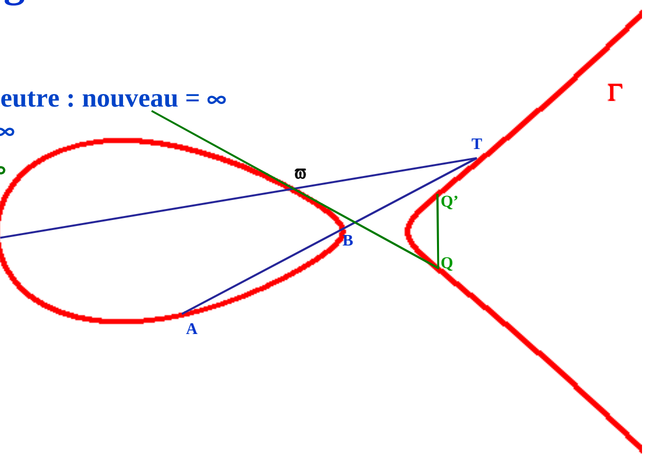
# Cryptographie en courbe elliptique
# Changement d'élément neutre

**C = A $+_{\varpi}$ B**

**Changer d'élément neutre : nouveau = ∞**

**Il faut calculer C $-_{\varpi}$ ∞**

**Q' est l'opposé $_{\varpi}$ de ∞**



# Cryptographie en courbe elliptique
# Changement d'élément neutre

JLS CONSEIL

**C = A $+_{\varpi}$ B**

**Changer d'élément neutre : nouveau = ∞**

**Il faut calculer C $-_{\varpi}$ ∞**

**Q' est l'opposé $_{\varpi}$ de ∞**

**Construire C $+_{\varpi}$ Q'**