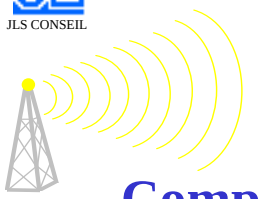
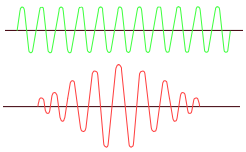
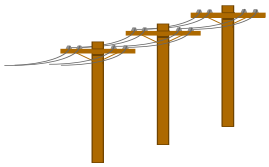
JLS CONSEIL







Compléments et révisions

Jean-Luc Stehlé

Bases mathématiques pour la sécurité informatique

EPITA

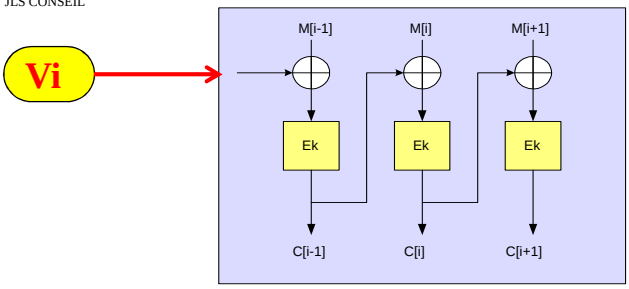
28 mai 2014

Jean-Luc.Stehle@NormaleSup.org

JLS CONSEIL

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

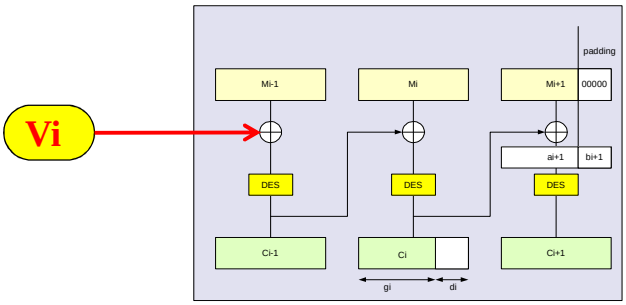
Communication de type « stream »
Chiffrage de supports séquentiels (bande magnétique de sauvegarde)
Messages séparés indépendants les uns des autres
Disques chiffrés avec accès direct

Chaînage secteur par secteur
Vi dépendant du N° de secteur

JLS CONSEIL

Mode chaîné CTS (Ciffer Text 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))

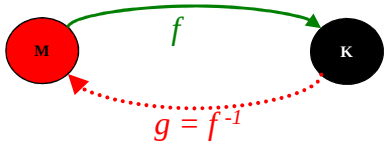
  CT[n] = PT[n] ⊕ Masque[n]

- **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 a et $f(x) = a^x$**

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, x très grand)**
- **Logarithme de base a dans G : retrouver x connaissant a et f(x)**

JLS CONSEIL

Compléments d'algèbre : Les polynômes

On travaille sur un corps 𝕂

Attention : les propriétés ne sont pas toujours celles auxquelles nous étions habitués sur ℝ ou sur ℂ .

Se méfier de son intuition

Exemples de corps :

- Les entiers modulo p (p premier)
- Le corps à 256 éléments utilisé dans AES

Racine cubique de 2 : Équation $x^3 - 2 = 0$

- Dans $\mathbb{Q}$: Pas de racines
- Dans $\mathbb{R}$: Une seule racine $\sqrt[3]{2}$
- Dans $\mathbb{C}$: Trois racines : $\sqrt[3]{2}$; $\sqrt[3]{2} \cdot j$; $\sqrt[3]{2} \cdot j^2$
  avec $j = 1/2 + \sqrt{3}/2\, i$ racine cubique de l'unité dans $\mathbb{C}$
- Dans $\mathbb{Z}/3\mathbb{Z}$: Une seule racine : $x=2$ $x^3 = 8 \equiv 2$
- Dans $\mathbb{Z}/5\mathbb{Z}$: Une seule racine : $x=3$ $x^3 = 27 \equiv 2$
- Dans $\mathbb{Z}/7\mathbb{Z}$: Pas de racines
- Dans $\mathbb{Z}/31\mathbb{Z}$: Trois racines : $4^3=64\equiv 2$; $7^3=343\equiv 2$; $20^3=8000\equiv 258\times31+2\equiv 2$

JLS CONSEIL
Compléments d'algèbre : Les polynômes

Équation $x^3 + x + 2 = 0$

- Dans $\mathbb{Q}$ et dans $\mathbb{R}$: Une seule racine $x = -1$
  $x^3 + x + 2 = (x+1)(x^2-x+2)$
- Dans $\mathbb{C}$: Trois racines : $x = -1$ et $x = (1 \pm i\sqrt{7}) / 2$
- Dans $\mathbb{Z}/5\mathbb{Z}$: Une seule racine : $x=4$ $64 + 4 + 2 = 70$
- Dans $\mathbb{Z}/7\mathbb{Z}$: Deux racines : $x=4$ et $x=6$
- Dans $\mathbb{Z}/11\mathbb{Z}$: Trois racines : $x=5$, $x=7$, $x=10$

Compléments d'algèbre : Les polynômes

Deux polynômes premiers entre eux n'ont pas de racine commune

Réciproque **vraie** dans $\mathbb{C}$, **fausse** dans $\mathbb{R}$:

Contre-exemple : $(x-3)(x^2+x+1)$ et $(x-4)(x^2+x+1)$

JLS CONSEIL

Compléments d'algèbre : Les polynômes

Recherche des zéros d'un polynôme dans un corps $\mathbb{K}$

(Résultats valables que soit le corps de base $\mathbb{K}$)

- On peut toujours se ramener au cas où le coefficient du terme de plus haut degré est 1.
- Un polynôme du premier degré a toujours un et un seul zéro.
- Si le polynôme non nul P[X] s'annule pour X=a, alors il est divisible par (X-a)

Démonstration par la division euclidienne

$P[X] = (X-a)\,Q[X] + R[X]$ avec $\partial°(R[X]) < \partial°(X-a)$

donc R[X] = Constante, et, pour X=a, R[a]=0

donc R=0 et $\partial°(Q[X]) = \partial°(P[X])-1$

Compléments d'algèbre : Les polynômes

JLS CONSEIL

Recherche des zéros d'un polynôme dans un corps $\mathbb{K}$

(Résultats valables que soit le corps de base $\mathbb{K}$)

Définition : *On dit que a est une racine multiple d'ordre k si P[X] est divisible par $(X-a)^k$ et n'est pas divisible par $(X-a)^{k+1}$*

Si un polynôme de degré n a n-1 racines (en comptant les multiplicités), alors il en a une $n^{ième}$

Démonstration par divisions euclidiennes successives,:
on élimine ces n-1 racines et il restera un polynôme de degré 1.

Si l'équation $X^n + a X^{n-1} + \ldots = 0$ a n racines (en comptant les multiplicités), alors la somme des racines est égale à $-a$.

En particulier, si une équation du troisième degré a deux racines, elle en a automatiquement une troisième qui peut se calculer directement connaissant les deux autres et les coefficients des termes de degré 3 et 2 de du polynôme.

Compléments d'algèbre :

JLS CONSEIL

Dérivée d'un polynôme

La notion classique de dérivée
(pente de la tangente = limite d'une sécante qui…)
n'a aucun sens dans $\mathbb{Z}/N\mathbb{Z}$:
La notion de limite n'existe pas

Définition :

Si $P[X] = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$
on appelle polynôme dérivé de P[X] le polynôme
$P'[X] = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots + a_1$.

Définition purement algébrique, sans interprétation géométrique…

Compléments d'algèbre :

JLS CONSEIL

Dérivée d'un polynôme

Propriétés

- **Linéarité**
  - **dérivée d'une somme = somme des dérivées**
  - **dérivée de ×λ , avec λ scalaire = λ× dérivée)**
- **La dérivée d'un polynôme de degré n est un polynôme de degré n-1.**
- **La dérivée de (X-a) est le polynôme constant 1.**

Dérivée d'un produit de polynômes

$P[X] = \sum a_p X^p \quad Q[X] = \sum b_q X^q \quad R[X] = P[X]\times Q[X] = \sum c_r X^r$ avec $c_r = \sum_{p+q=r} a_p b_q$

Dérivée de X^r avec r=p+q donc $X^r = X^p X^q$: $r X^{r-1} = p X^{p-1} X^q : + q X^p X^{q-1}$:

Suite laissée en exercice au lecteur…

On retrouve les formules classiques $(PQ)' = P'Q + PQ'$ **et** $(P^2)' = 2PP'$

Compléments d'algèbre :

JLS CONSEIL

Racines multiples d'un polynôme

Théorème :

Si a est un zéro multiple de P[X] (zéro d'ordre au moins 2)
alors a est un zéro du polynôme dérivé P'[X]

Démonstration : $P[X] = (X-a)^2 Q[X] \quad P'[X] = (X-a)^2 Q'[X] + 2(X-a)Q[X]$

Corollaire :

Si a est un zéro multiple de P[X],
alors a est un zéro de R[X] = Pgcd(P[X],P'[X]).

Démonstration par Bezout : $\exists \lambda \mu : R[X] = \lambda P[X] + \mu P'[X])$

Compléments d'algèbre :

Racines multiples d'un polynôme

JLS CONSEIL

Cas particulier du degré 2

Calcul du Pgcd de (aX^2+bX+c) et $(2aX+b)$

$(aX^2+bX+c) = (2aX+b)(x/2 + b/4a) + c-b^2/4a$

- Si $b^2-4ac=0$, le Pgcd est $2aX+b$ (le polynôme est divisible par sa dérivée)
  Il y a une racine double $-b/2a$
- Sinon, le polynôme et sa dérivée sont premiers entre eux, pas de racine double.

Cas particulier du degré 3

Calcul du Pgcd de (X^3+pX+q) et $(3X^2+p)$

Par l'algorithme d'Euclide

$(X^3+pX+q) = (3X^2+p)\ (X/3) + (\ 2/3\ p\ X + q)$

$(3X^2+p) = (\ 2/3\ p\ X + q)\ (9/2p\ X - 27q/4p^2\ ) + p+27q^2/4p^2$

- Si $4p^3 + 27q^2 = 0$, le Pgcd est $(\ 2/3\ p\ X + q)$, et il y a une racine double $X = 3q/2p$
- Sinon, le polynôme et sa dérivée sont premiers entre eux, pas de racine double.

Un peu de géométrie algébrique : Espaces projectifs

JLS CONSEIL

- **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 $Z \neq 0$, $x=X/Z$ $y=Y/Z$

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 $\mathbb{R}$, sur $\mathbb{C}$ ou sur un corps $\mathbb{K}$ 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 où 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 $\mathbb{R}$, sur $\mathbb{C}$ ou sur un corps $\mathbb{K}$ 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 Γ 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 Γ 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 $\mathbb{R}$, sur $\mathbb{C}$ ou sur un corps $\mathbb{K}$ 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 Γ : Fonction $\mathcal{d}$ de Γ 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 Γ**
- **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 𝕂 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 Γ.**
  Le diviseur de R est d'ordre 0
  R a, sur Γ, autant de zéros que de pôles (en comptant les multiplicités et les valeurs de R sur les points à l'infini de Γ)

- **Définition : Un diviseur sur Γ est appelé un diviseur principal s'il existe une fonction rationnelle sur Γ 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 quotient $\mathcal{D}_0/\mathcal{P}$**

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

JLS CONSEIL

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

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

- **Γ sur K = Z/pZ avec p premier à 160 bits ou 256 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 Γ**
- **Cas particulier des courbes elliptiques**

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

JLS CONSEIL

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

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

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

JLS CONSEIL

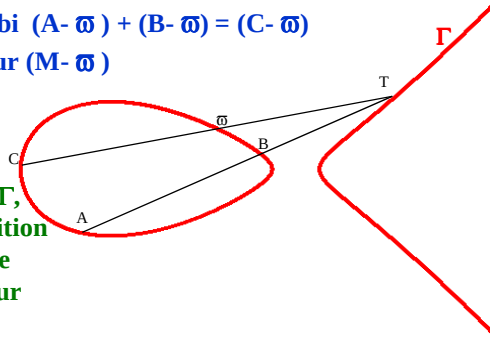
Un peu de géométrie algébrique : Groupe de Jacobi d'une courbe elliptique

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 𝕂 quelconque

JLS CONSEIL

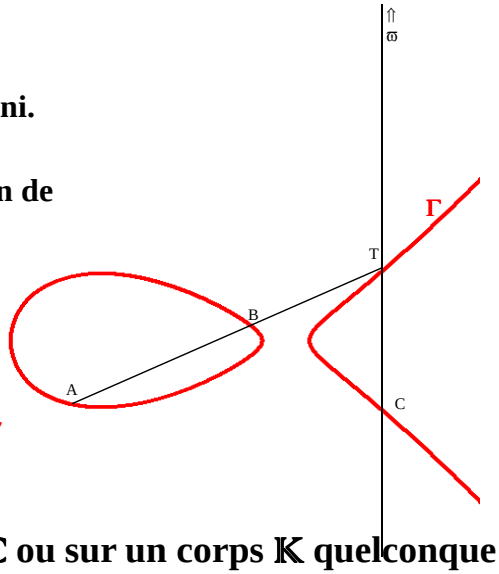
Cryptographie en courbe elliptique

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.

Une multiplication sur une courbe elliptique dans ℤ/pℤ nécessite environ 12 multiplications dans ℤ/pℤ

La technique des échelles de Montgomery ramène ce facteur à 6

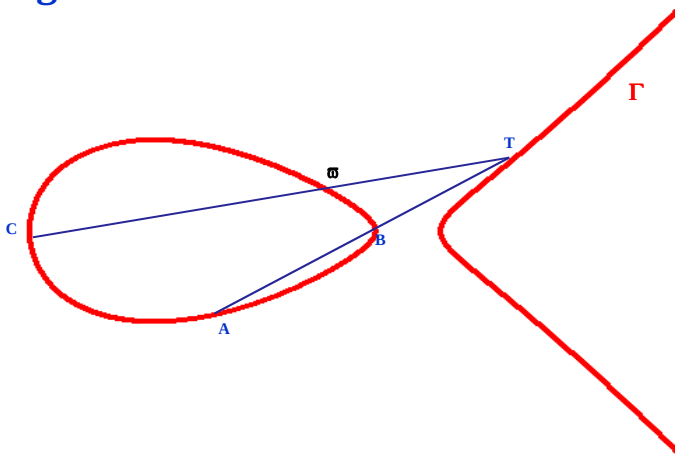


On travaille sur ℝ, sur ℂ ou sur un corps 𝕂 quelconque

Cryptographie en courbe elliptique
Changement d'élément neutre

JLS CONSEIL

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



Cryptographie en courbe elliptique
Changement d'élément neutre

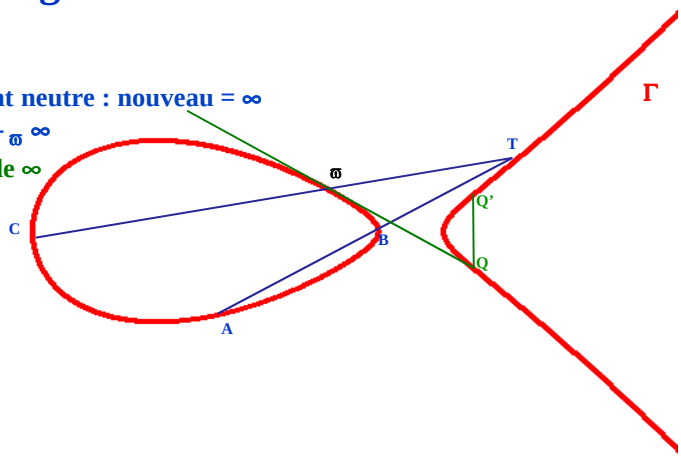
JLS CONSEIL

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

Changer d'élément neutre : nouveau = ∞

Il faut calculer $C -_{\varpi} \infty$

Q' est l'opposé$_{\varpi}$ de ∞



JLS CONSEIL

Cryptographie en courbe elliptique
Changement d'élément neutre

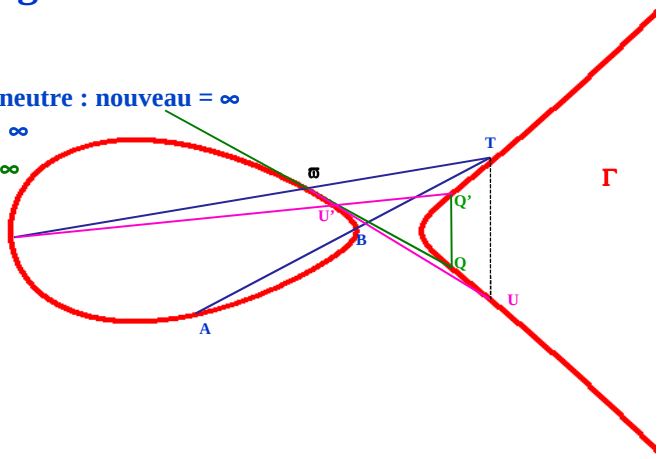
C = A +$_{\varpi}$ B

Changer d'élément neutre : nouveau = ∞

Il faut calculer C -$_{\varpi}$ ∞

Q' est l'opposé$_{\varpi}$ de ∞

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



JLS CONSEIL

Questions?