Calcul de traces de l'algorithme F4 et applications

Vanessa VITSE – Antoine Joux

Université de Versailles Saint-Quentin, Laboratoire PRISM

Séminaire CARAMEL, LORIA, Nancy

Part I

Introduction

Problématique

Objectif : donner une technique permettant de résoudre efficacement beaucoup de systèmes polynomiaux "similaires"

Famille paramétrée de systèmes

$V \subset \mathbb{K}^\ell$ variété algébrique

- Système paramétré générique : $F_1, \ldots, F_r \in \mathbb{K}(V)[\underline{X}]$
- Instance aléatoire :
  $\{f_1, \ldots, f_r\} = \{F_1(y), \ldots, F_r(y)\} \subset \mathbb{K}[\underline{X}]$ pour un $y \in V$ aléatoire

Techniques de résolution d'un système

Outil principal : calcul de base de Gröbner

Deux algorithmes standards dûs à Faugère

- F4 ('99) : simple et rapide mais beaucoup de calculs inutiles (réductions à zéro)
- F5 ('02) : critère sophistiqué évitant les réductions à zéro mais perte d'efficacité sur les autres réductions

- algorithmes généralistes
- pas de prise en compte de la similarité des systèmes

Variante F4

Notre contribution

Exploiter les calculs faits par F4 pour un premier système pour éviter les réductions à zéro dans les calculs suivants

Travaux antérieurs

- Idée provenant des calculs de GB sur $\mathbb{Q}$ par restes chinois
- Traverso ('88) : analyse de *traces de Gröbner* pour l'algorithme de Buchberger dans le cas rationnel

Variante F4

Notre contribution

Exploiter les calculs faits par F4 pour un premier système pour éviter les réductions à zéro dans les calculs suivants

Travaux antérieurs

- Idée provenant des calculs de GB sur $\mathbb{Q}$ par restes chinois
- Traverso ('88) : analyse de *traces de Gröbner* pour l'algorithme de Buchberger dans le cas rationnel

Notion utile lorsque :

- calcul de la GB du système instancié faisable
- beaucoup de systèmes d'une même famille à résoudre
- calcul d'une GB paramétrée ("comprehensive Gröbner basis") impossible

Exemples d'utilisation

Attaque par décomposition sur courbes elliptiques

Résolution du DL (et autres problèmes) sur $E(\mathbb{F}_{q^n})$ par calcul d'index

- Base de factorisation : $\mathcal{F} = \{(x, y) \in E(\mathbb{F}_{q^n}) : x \in \mathbb{F}_q\}$
- But : trouver de l'ordre de q décompositions de la forme
$$R = P_1 + \ldots + P_m, \text{ avec } P_i \in \mathcal{F}$$

Attaque algébrique

- traduire chaque essai de décomposition d'un point R dans $\mathcal{F}$ en une résolution d'un système polynomial $\mathcal{S}_R$ (Semaev + restriction de Weil)
- $\mathcal{S}_R = \{f_1, \ldots, f_n\} \subset \mathbb{F}_q[X_1, \ldots, X_m]$ est une instance d'un système polynomial paramétré

chaque test de décomposition $\leftrightarrow$ résoudre $\mathcal{S}_R$ sur $\mathbb{F}_q$

Exemples d'utilisation

Techniques de résolution de systèmes polynomiaux

- Approche hybride : compromis entre recherche exhaustive de solutions et calcul de GB
  - trouver une solution de $f_1, \ldots, f_r \in \mathbb{F}_q[X_1, \ldots, X_n]$ en testant toutes les valeurs possibles de quelques variables $X_1, \ldots, X_k$
  - calculs des GB des systèmes spécialisés $f_1(x_1, \ldots, x_k), \ldots, f_r(x_1, \ldots, x_k)$ beaucoup plus simples, mais q^k calculs à faire

- Changement de caractéristique
  - Restes chinois : déduire la GB de $f_1, \ldots, f_r \in \mathbb{Q}[\underline{X}]$ des calculs des GB de $\bar{f}_1, \ldots, \bar{f}_r \in \mathbb{Z}/p\mathbb{Z}[\underline{X}]$ pour de nombreux p premiers
  - Grande caractéristique : calcul de la GB de $f_1, \ldots, f_r \in \mathbb{Z}/p_1\mathbb{Z}[\underline{X}]$ accéléré par précalcul dans $\mathbb{Z}/p_2\mathbb{Z}$, $p_2 \ll p_1$.

Part II

F4 et sa variante

Rappels sur les bases de Gröbner

Définition

$\mathrm{I} = \langle f_1, \ldots, f_r \rangle \subset \mathbb{K}[X_1, \ldots, X_n]$ idéal
$G = \{g_1, \ldots, g_s\} \subset \mathrm{I}$ base de Gröbner de I si $\langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle = \mathrm{lt}(\mathrm{I})$

Opérations élémentaires :

- Division d'un polynôme multivarié par une liste de polynômes selon un ordre monomial
- S-polynôme (ou paire critique) : $f_1, f_2 \in \mathbb{K}[X_1, \ldots, X_n]$

$$S(f_1, f_2) = \frac{\mathrm{lm}(f_1) \vee \mathrm{lm}(f_2)}{\mathrm{lt}(f_1)} f_1 - \frac{\mathrm{lm}(f_1) \vee \mathrm{lm}(f_2)}{\mathrm{lt}(f_2)} f_2$$

Théorème de Buchberger

$G = \{g_1, \ldots, g_s\}$ base de Gröbner $\Leftrightarrow \overline{S(g_i, g_j)}^{G} = 0$ pour tout (i, j)

Algorithme de Buchberger et implémentation

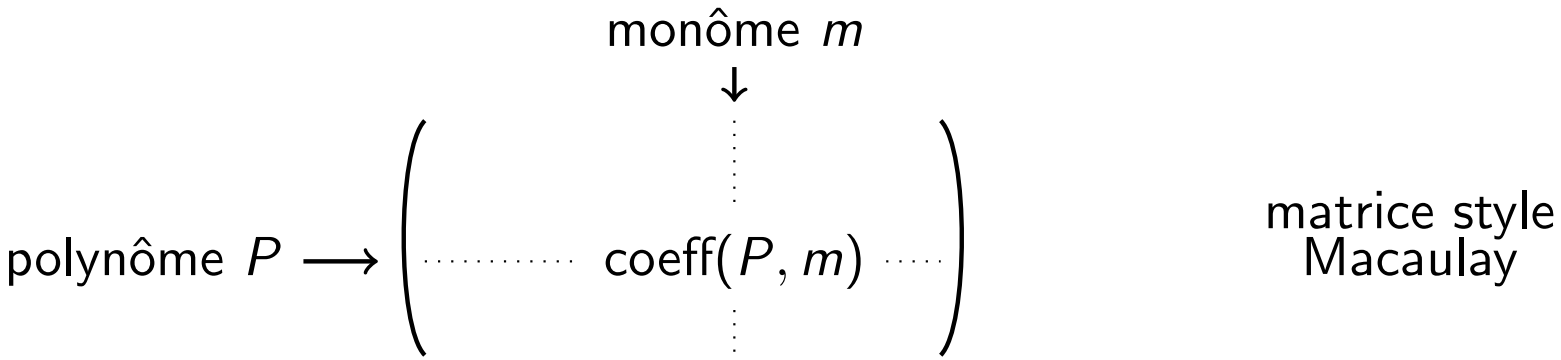
Algo

$G \leftarrow \{f_1, \ldots, f_k\}$
$CP \leftarrow \{S(f_i, f_j), 1 \leq i < j \leq k\}$
while $CP \neq \emptyset$ **do**
  choisir $s \in CP$
  $r \leftarrow \overline{s}^G$
  if $r \neq 0$ **then**
    $CP \leftarrow CP \cup \{S(g, r) : g \in G\}$
    $G \leftarrow G \cup \{r\}$
return G

- stratégie optimale de choix des paires ?
  $\longrightarrow$ par degré du lcm croissant
- temps de calcul concentré sur réduction des paires
  $\longrightarrow$ critères de Buchberger

Algorithme F4: deux idées clés

1. Algèbre linéaire pour réduire simultanément les paires sélectionnées $(lcm, u_1, f_1, u_2, f_2)$ où $lcm = \mathrm{lm}(f_1) \vee \mathrm{lm}(f_2)$, $u_i = \frac{lcm}{\mathrm{lm}(f_i)}$
   $\longrightarrow$ construction d'une matrice type Macaulay contenant
   - les produits $u_i f_i$ provenant des paires sélectionnées
   - les multiples des polynômes de G permettant de réduire les queues



Algorithme F4: deux idées clés

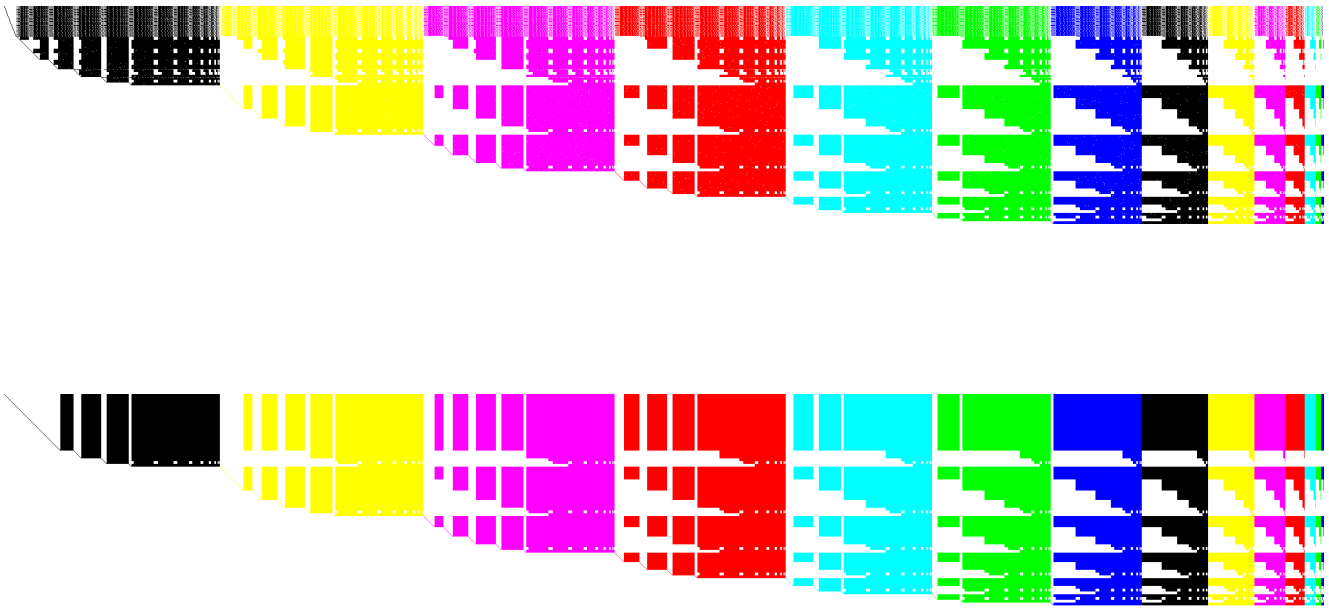
1. Algèbre linéaire pour réduire simultanément les paires sélectionnées $(lcm, u_1, f_1, u_2, f_2)$ où $lcm = \mathrm{lm}(f_1) \vee \mathrm{lm}(f_2)$, $u_i = \frac{lcm}{\mathrm{lm}(f_i)}$
   $\longrightarrow$ construction d'une matrice type Macaulay contenant
   - les produits $u_i f_i$ provenant des paires sélectionnées
   - les multiples des polynômes de G permettant de réduire les queues

2. Mémoriser les réductions
   - remplacer le produit $u_i f_i$ par $\left(\frac{\mathrm{lm}(u_i f_i)}{\mathrm{lm}(f')}\right) f'$
     où f' obtenu dans matrices réduites précédentes tel que $\mathrm{lm}(f') | \mathrm{lm}(u_i f_i)$
   - avantage : queue du nouveau produit déjà partiellement réduite
     $\longrightarrow$ moins de lignes dans la matrice, moins de réductions nécessaires

Réduction des matrices

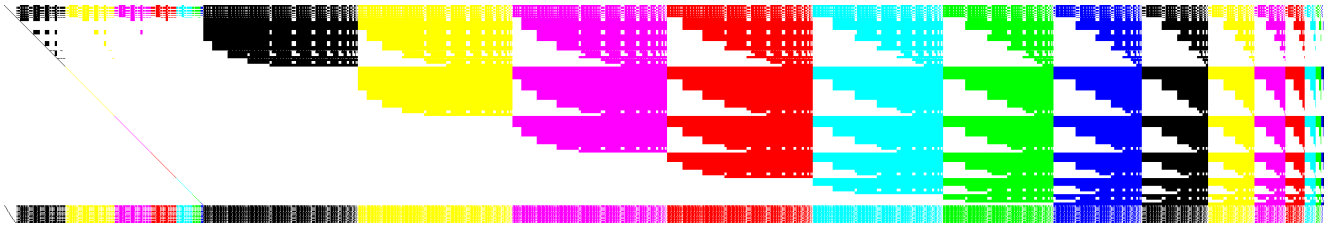
Particularités :

- tailles très variables
- presque triangulaires supérieures
- beaucoup de zéros, mais pas creuses non plus



Choix d'implémentation

- localisation a priori des pivots et de certains zéros



- instructions SIMD pour opération élémentaire $L_{\text{todo}} \leftarrow L_{\text{todo}} + c.L_{\text{pivot}}$
  $\longrightarrow$ on traite plusieurs coefficients simultanément
- réduction modulaire compatible SIMD, à base de $\gg$ et de $\wedge$
- découpage en tranches de la matrice et déroulage de boucles
- pas de techniques de réduction avancée (Strassen/Winograd)
  - perte de la localisation des zéros
  - compatibilité SIMD ?
  - tests réalisés non concluants

Notre variante de F4

Structure du programme

1. `F4Precomp`: sur le premier système
   - à chaque étape, enregistrer la liste des multiples de la base utilisés
   - réduction à zéro $\longrightarrow$ retirer un multiple bien choisi de la liste
2. `F4Remake`: sur les systèmes suivants
   - pas de liste d'attente des paires critiques à traiter
   - à chaque étape, considérer seulement les multiples nécessaires listés durant le précalcul

Choix des polynômes à éliminer :

- calcul de A tq $AM = M'$, $M' =$ matrice échelon réduite de M
  RAZ dans $M' \leftrightarrow$ dépendance linéaire entre lignes de M, coeffs dans A
- utilisation de A pour éliminer de façon cohérente un multiple par RAZ

Analyse de F4Remake

Systèmes "similaires"

- Système paramétré générique : $F_1, \ldots, F_r \in \mathbb{K}(V)[\underline{X}]$
- Instance aléatoire : $\{f_1, \ldots, f_r\} \subset \mathbb{K}[\underline{X}]$

Comportement générique

1. "calculer" avec F4 la GB de $\langle F_1, \ldots, F_r \rangle$ dans $\mathbb{K}(V)[\underline{X}]$
2. $f_1, \ldots, f_r$ a un comportement générique si durant le calcul de la GB avec F4
   - même nombre d'étapes
   - à chaque étape, mêmes termes de tête (donc mêmes paires)

Analyse de F4Remake

Systèmes "similaires"

- Système paramétré générique : $F_1, \ldots, F_r \in \mathbb{K}(V)[\underline{X}]$
- Instance aléatoire : $\{f_1, \ldots, f_r\} \subset \mathbb{K}[\underline{X}]$

Comportement générique

1. "calculer" avec F4 la GB de $\langle F_1, \ldots, F_r \rangle$ dans $\mathbb{K}(V)[\underline{X}]$
2. $f_1, \ldots, f_r$ a un comportement générique si durant le calcul de la GB avec F4
   - même nombre d'étapes
   - à chaque étape, mêmes termes de tête (donc mêmes paires)

F4Remake calcule la GB de $f_1, \ldots, f_r$
si le système a un comportement générique

Analyse de F4Remake

Systèmes modulaires

- $F_1, \ldots, F_r \in \mathbb{Z}[\underline{X}]$ système de polynômes primitifs
- $f_1, \ldots, f_r \in \mathbb{F}_p[\underline{X}]$ sa réduction modulo p premier

F4-lucky primes

1. "calculer" avec F4 la GB de $\langle F_1, \ldots, F_r \rangle$ dans $\mathbb{Q}[\underline{X}]$
2. p est F4-lucky si durant le calcul avec F4 de la GB $f_1, \ldots, f_r$
   - même nombre de étapes
   - à chaque étape, mêmes termes de têtes (donc mêmes paires)

Analyse de F4Remake

Systèmes modulaires

- $F_1, \ldots, F_r \in \mathbb{Z}[\underline{X}]$ système de polynômes primitifs
- $f_1, \ldots, f_r \in \mathbb{F}_p[\underline{X}]$ sa réduction modulo p premier

F4-lucky primes

1. "calculer" avec F4 la GB de $\langle F_1, \ldots, F_r \rangle$ dans $\mathbb{Q}[\underline{X}]$
2. p est F4-lucky si durant le calcul avec F4 de la GB $f_1, \ldots, f_r$
   - même nombre de étapes
   - à chaque étape, mêmes termes de têtes (donc mêmes paires)

F4Remake calcule la GB de $f_1, \ldots, f_r$
si p est F4-lucky

Condition algébrique

1. Supposons que $f_1, \ldots, f_r$ ait un comportement générique jusqu'à l'étape $(i-1)$
2. À l'étape i, F4 construit
   - M_g =matrice des multiples des polynômes à l'étape i pour le système paramétrique
   - M =matrice des multiples des polynômes à l'étape i pour $f_1, \ldots, f_r$

Condition algébrique

1. Supposons que $f_1, \ldots, f_r$ ait un comportement générique jusqu'à l'étape $(i-1)$
2. À l'étape i, F4 construit
   - M_g =matrice des multiples des polynômes à l'étape i pour le système paramétrique
   - M =matrice des multiples des polynômes à l'étape i pour $f_1, \ldots, f_r$
3. Forme échelon réduite de M_g et M

$$s\left\{\overbrace{\left(\begin{array}{c|c} \begin{array}{cc} A_{g,0} & \\ 0 & \end{array} & A_{g,1} \\ \hline A_{g,3} & A_{g,2} \end{array}\right.}^{LT(M)}\right. \qquad \left(\begin{array}{c|c} \begin{array}{cc} A_0 & \\ 0 & \end{array} & A_1 \\ \hline A_3 & A_2 \end{array}\right)$$

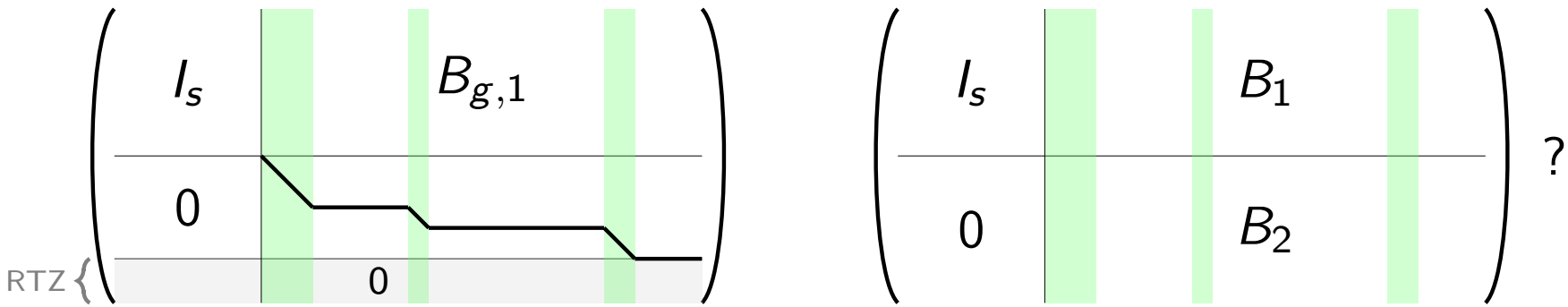
Condition algébrique

1. Supposons que $f_1, \ldots, f_r$ ait un comportement générique jusqu'à l'étape $(i-1)$
2. À l'étape i, F4 construit
   - M_g =matrice des multiples des polynômes à l'étape i pour le système paramétrique
   - M =matrice des multiples des polynômes à l'étape i pour $f_1, \ldots, f_r$
3. Forme échelon réduite de M_g et M

$$\left(\begin{array}{c|c} I_s & B_{g,1} \\ \hline 0 & B_{g,2} \end{array}\right) \qquad \left(\begin{array}{c|c} I_s & B_1 \\ \hline 0 & B_2 \end{array}\right)$$

Condition algébrique

1. Supposons que $f_1, \ldots, f_r$ ait un comportement générique jusqu'à l'étape $(i-1)$
2. À l'étape i, F4 construit
   - M_g =matrice des multiples des polynômes à l'étape i pour le système paramétrique
   - M =matrice des multiples des polynômes à l'étape i pour $f_1, \ldots, f_r$
3. Forme échelon réduite de M_g et M



Condition algébrique

1. Supposons que $f_1, \ldots, f_r$ ait un comportement générique jusqu'à l'étape $(i-1)$
2. À l'étape i, F4 construit
   - M_g =matrice des multiples des polynômes à l'étape i pour le système paramétrique
   - M =matrice des multiples des polynômes à l'étape i pour $f_1, \ldots, f_r$
3. Forme échelon réduite de M_g et M

$$\left(\begin{array}{c|c|c} I_s & 0 & C_{g,1} \\ \hline 0 & I_\ell & C_{g,2} \\ \hline 0 & 0 & 0 \end{array}\right) \qquad \left(\begin{array}{c|c|c} I_s & & B'_1 \\ \hline 0 & B & B'_2 \end{array}\right) \; ?$$

Condition algébrique

1. Supposons que $f_1, \ldots, f_r$ ait un comportement générique jusqu'à l'étape $(i-1)$
2. À l'étape i, F4 construit
   - M_g =matrice des multiples des polynômes à l'étape i pour le système paramétrique
   - M =matrice des multiples des polynômes à l'étape i pour $f_1, \ldots, f_r$
3. Forme échelon réduite de M_g et M

$$\left(\begin{array}{c|c|c} I_s & 0 & C_{g,1} \\ \hline 0 & I_\ell & C_{g,2} \\ \hline 0 & 0 & 0 \end{array}\right) \qquad \left(\begin{array}{c|c|c} I_s & & B'_1 \\ \hline 0 & B & B'_2 \end{array}\right)$$

$f_1, \ldots, f_r$ a un comportement générique à l'étape $i \Leftrightarrow B$ est de rang plein

Probabilité de succès de F4Remake

Hypothèse heuristique

- Les matrices B sont uniformément distribuées dans $\mathcal{M}_{n,\ell}(\mathbb{F}_q)$
- Les probabilités qu'elles soient de rang plein sont indépendantes

Estimation des probas sur $\mathbb{F}_q$

Sous l'hypothèse heuristique:

$$\text{Proba}(\{f_1, \ldots, f_r\} \text{ se comporte génériquement}) \geq c(q)^{n_{step}}$$

- n_{step} = nb d'étapes durant F4 pour le calcul de la GB du système paramétrique
- $c(q) = \prod_{i=1}^{\infty}(1 - q^{-i}) = 1 - 1/q + \underset{q\to\infty}{O}(1/q^2)$

Quid de la non généricité

1. Si le précalcul est correct:
   - possibilité de détecter facilement si `F4Remake` est correct : comportement pas générique du système si à une étape monôme de tête plus petit (ou RAZ)
   - si échec de `F4Remake`, poursuite du calcul avec F4 classique

2. Le précalcul est incorrect si :
   - `F4Remake` trouve un monôme de tête plus grand que celui trouvé par `F4Precomp` à la même étape
   - le résultat sur un des systèmes suivants n'est pas une GB
   - autre possibilité de détection : lancer `F4Precomp` sur plusieurs systèmes et comparer les résultats

Limites de l'heuristique

Cas particuliers

Systèmes paramétrés de partie homogène de plus haut degré dans $\mathbb{K}[\underline{X}]$

- Hypothèse heuristique non valide
- Mais comportement générique jusqu'à la première chute de degré

Schéma de signature UOV

Forger une signature $\leftrightarrow$ résoudre un système quadratique sous-déterminé
Paramètres recommandés : 16 équations, 32 (ou 48) variables sur $\mathbb{K} = \mathbb{F}_{2^4}$

$$P_k = \sum_{i,j=1}^{48} a_{ij}^k x_i x_j + \sum_{i=1}^{48} b_i^k x_i + c^k, \quad k = 1 \ldots 16$$

Limites de l'heuristique

Cas particuliers

Systèmes paramétrés de partie homogène de plus haut degré dans $\mathbb{K}[\underline{X}]$

- Hypothèse heuristique non valide
- Mais comportement générique jusqu'à la première chute de degré

Schéma de signature UOV

Paramètres recommandés : $m = 16$ éq, $n = 32$ (ou 48) var sur $\mathbb{K} = \mathbb{F}_{2^4}$

Faugère et al.:

- fixer $m - n$ variables et trouver une solution valide
- faire une recherche exhaustive sur 3 variables supplémentaires

$$P_k = \sum_{i,j=1}^{13} a_{ij}^k x_i x_j + \sum_{i=1}^{13} \left(b_i^k + \sum_{j=14}^{16} a_{ij}^k x_j \right) x_i + \left(\sum_{i,j=14}^{16} a_{ij}^k x_i x_j + \sum_{i=14}^{16} b_i^k x_i + c^k \right)$$

Exemple UOV par approche hybride

But : calculer les GB des systèmes $S_{x_{14},x_{15},x_{16}} = \{P_1, \ldots, P_{16}\}$ pour tout $(x_{14}, x_{15}, x_{16}) \in \mathbb{F}_{2^4}^3$ où

$$P_k = \sum_{i,j=1}^{13} a_{ij}^k x_i x_j + \sum_{i=1}^{13} \left(b_i^k + \sum_{j=14}^{16} a_{ij}^k x_j \right) x_i + \left(\sum_{i,j=14}^{16} a_{ij}^k x_i x_j + \sum_{i=14}^{16} b_i^k x_i + c^k \right)$$

Résolution avec F4Remake

- 6 étapes, première chute de degré constatée à l'étape 5

$$\text{Proba}(S_{x_{14},x_{15},x_{16}} \text{ se comporte génériquement}) \geq c(16)^2 \simeq 0.87$$

- exploration exhaustive : la probabilité constatée sur différents exemples est d'environ 90%

Exemple UOV par approche hybride

	F4Remake[1]	F4[1]	F4 Magma[2]	F4/F4Remake
Timing (sec)	5.04	16.77	120.6	3.3
Largest matrix	5913×7005	10022×8329	10245×8552	2.0

- précalcul fait en 32.3 sec rapidement amorti
- à comparer aux 9.41 sec de F5[3] mentionnés par Faugère et al.
- génériquement, la GB est $\langle 1 \rangle$
  $\longrightarrow$ solutions à rechercher parmi les systèmes non génériques

[1] 2.6 GHz Intel Core 2 duo
[2] V2.16-12
[3] 2.4 GHz Bi-pro Xeon

Part III

Applications aux attaques par décomposition sur courbes elliptiques

Attaques de problèmes standards et moins standards

Calcul d'index sur courbes elliptiques

ECDLP : soient $P \in E(\mathbb{F}_{q^n})$ et $Q \in \langle P \rangle$, trouver x tel que $Q = [x]P$

- Base de factorisation : $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : P = (x_p, y_p), x_p \in \mathbb{F}_q\}$
- Recherche de relations (au moins q indépendantes) : décomposer $[a_i]P + [b_i]Q$ (a_i, b_i aléatoires) comme somme de points de $\mathcal{F}$
- Phase d'algèbre linéaire : déduire des relations obtenues le DLP de Q

Attaques de problèmes standards et moins standards

Calcul d'index sur courbes elliptiques

ECDLP : soient $P \in E(\mathbb{F}_{q^n})$ et $Q \in \langle P \rangle$, trouver x tel que $Q = [x]P$

- Base de factorisation : $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : P = (x_p, y_p), x_p \in \mathbb{F}_q\}$
- Recherche de relations (au moins q indépendantes) : décomposer $[a_i]P + [b_i]Q$ (a_i, b_i aléatoires) comme somme de points de $\mathcal{F}$
- Phase d'algèbre linéaire : déduire des relations obtenues le DLP de Q

Problème Static Diffie-Hellman assisté d'un oracle

G groupe fini, d entier secret

- Phase d'apprentissage : l'attaquant a accès à un oracle qui calcul $[d]Y$ pour tout $Y \in G$
- L'attaquant doit ensuite calculer $[d]X$ pour un challenge X non vu précédemment

$\longrightarrow$ attaque de SDHP sur $E(\mathbb{F}_{q^n})$ si on sait décomposer dans $\mathcal{F}$

Approches existantes : Gaudry-Diem, variante Joux-V.

Objectif

Savoir décomposer rapidement un point $R \in E(\mathbb{F}_{q^n})$ aléatoire en somme de m points de la base $\mathcal{F} = \{(x, y) \in E(\mathbb{F}_{q^n}) : x \in \mathbb{F}_q\}$

Outils :

- Semaev : $(m+1)$-ème poly de sommation $(\deg_{x_i}(f_{m+1}) = 2^{m-1})$

$$f_{m+1}(x_R, x_{P_1}, \ldots, x_{P_m}) = 0$$
$$\Leftrightarrow \exists \epsilon_1, \ldots, \epsilon_m \in \{1, -1\}, R = \epsilon_1 P_1 + \cdots + \epsilon_m P_m$$

- Restriction de Weil : décomposer dans base $\mathbb{F}_q$ linéaire de $\mathbb{F}_{q^n}$

$$f_{m+1}(x_R, x_{P_1}, \ldots, x_{P_m}) = 0 \Leftrightarrow \begin{cases} \varphi_1(x_{P_1}, \ldots, x_{P_m}) = 0 \\ \vdots \qquad\qquad (\mathcal{S}_R) \\ \varphi_n(x_{P_1}, \ldots, x_{P_m}) = 0 \end{cases}$$

chaque essai de décomposition d'un point $R \leftrightarrow$ résoudre $\mathcal{S}_R$ sur $\mathbb{F}_q$

Choix des paramètres

$E(\mathbb{F}_{q^n})$, $\mathcal{F} = \{(x,y) \in E(\mathbb{F}_{q^n}) : x \in \mathbb{F}_q\}$, $R = \epsilon_1 P_1 + \cdots + \epsilon_m P_m$

	Gaudry-Diem	Joux-V.
nb de points	$m = n$	$m = n-1$
nb essais par relation	$n!$	$(n-1)!q$
caractéristiques de $\mathcal{S}_R$	deg 2^{n-1} n eq/var	deg 2^{n-2} n eq, $n-1$ var
$deg(\mathrm{I}(\mathcal{S}_R))$	$2^{n(n-1)}$	0 (1 except.)
complexité de l'attaque	$n!2^{3n(n-1)}q^{2-2/n}$	$n!2^{\omega(n-1)(n-2)}e^{\omega n}q^2$

Cas limite en pratique : on sait décomposer au mieux en $m = 4$ points

Résultats sur $E(\mathbb{F}_{p^5})$, p impair (variante Joux-V.)

- $\mathcal{S}_R$ est composé de 5 éq sur $\mathbb{F}_p$ en 4 variables, degré total 8
- Heuristique valide : coeffs de $\mathcal{S}_R$ poly. en x_R aléatoire
- Précalcul en 8.963 sec, 29 étapes dans le calcul, degré max 19

taille de p	est. proba. échec	F4Remake[1]	F4[1]	F4/F4Remake	F4 Magma[2]
8 bits	0.11	2.844	5.903	2.1	9.660
16 bits	4.4×10^{-4}	3.990	9.758	2.4	9.870
25 bits	2.4×10^{-6}	4.942	16.77	3.4	118.8
32 bits	5.8×10^{-9}	8.444	24.56	2.9	1046

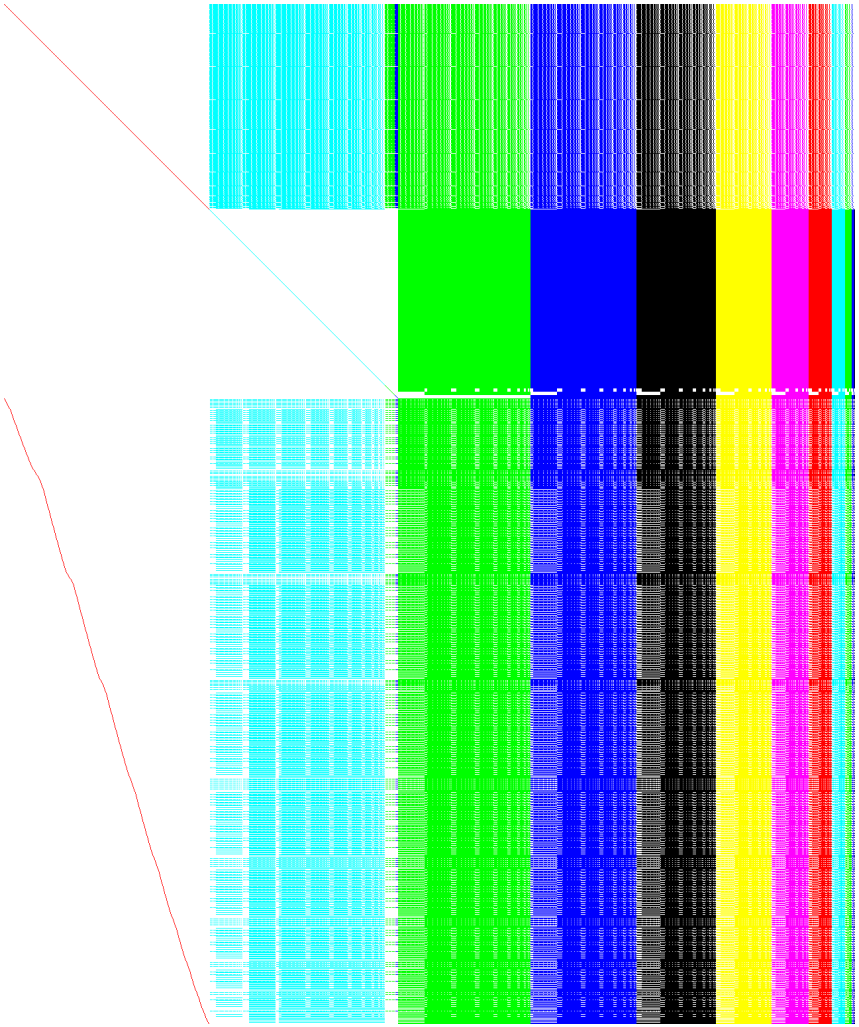
Étape	degré	taille matrices F4Remake	taille matrices F4	ratio
14	17	1062×3072	1597×3207	1.6
15	16	1048×2798	1853×2999	1.9
16	15	992×2462	2001×2711	2.2
17	14	903×2093	2019×2369	2.5
18	13	794×1720	1930×2000	2.8

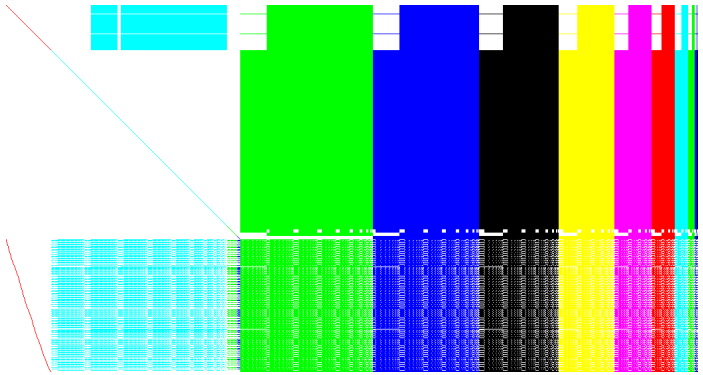
[1] 2.93 GHz Intel Xeon processor

[2] V2.15-15

Un exemple de matrice sans et avec précalcul

Étape 20





Comparaison avec F5

Points communs :

- élimination des réductions à zéro
- même borne supérieure pour complexité théorique

$$\tilde{O}\left(\binom{d_{reg}+n}{n}^{\omega}\right)$$

Comparaison avec F5

Points communs :

- élimination des réductions à zéro
- même borne supérieure pour complexité théorique

$$\tilde{O}\left(\binom{d_{reg}+n}{n}^{\omega}\right)$$

En pratique sur le système précédent :

- performances nettement inférieures pour notre implémentation de F5
- F5 crée de nombreux polynômes redondants (critère F5) : 17249 polynômes dans la base avant minimalisation
- F4 crée seulement 2789 polynômes
  $\longrightarrow$ meilleur comportement quelle que soit l'implémentation

Résultats en caractéristique paire

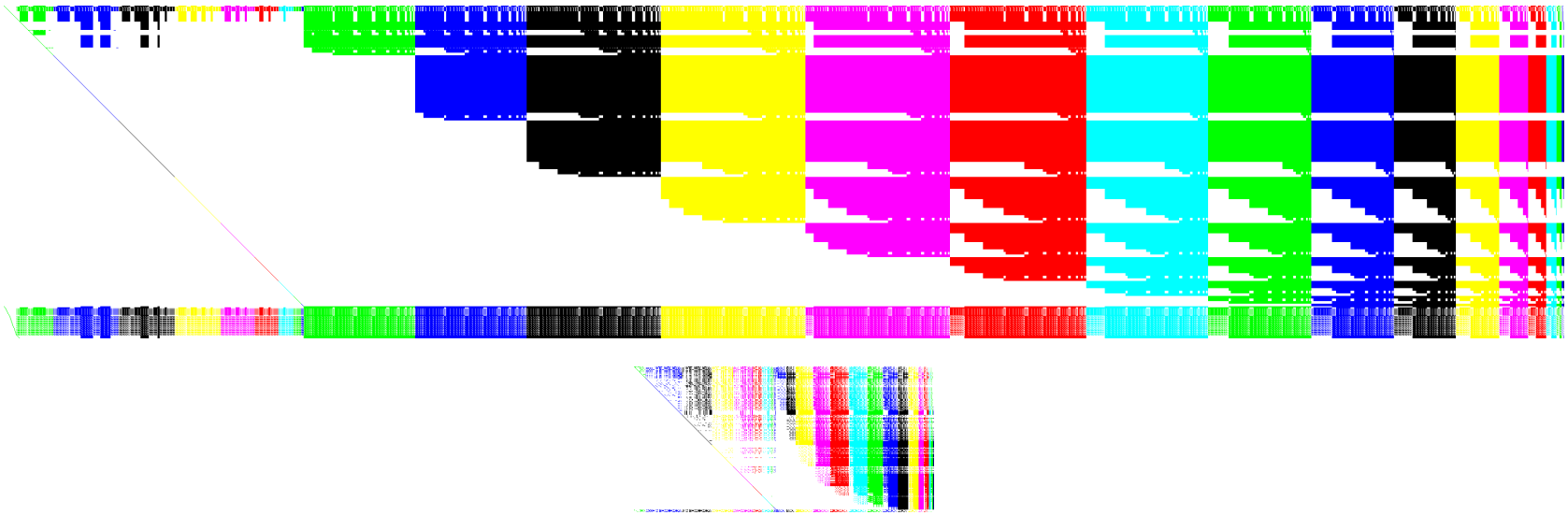
Courbe Oakley : 'Well Known Group' 3 curve d'IPSEC

$\mathbb{F}_{2^{155}} = \mathbb{F}_2[u]/_{(u^{155}+u^{62}+1)}$
$E : y^2+xy = x^3+(u^{18}+u^{17}+u^{16}+u^{13}+u^{12}+u^9+u^8+u^7+u^3+u^2+u+1)$
$\#E(\mathbb{F}_{2^{155}}) = 12 * 38059938472158930161554638261953866397436443$

- F4 classique : 148 étapes, degré max 17, 85 ms (Magma: 620 ms)
- Précalcul en 135 ms
- F4Remake : 30 ms/test de décomposition, $4!2^{31} \simeq 5.10^{10}$ tests à faire $\Rightarrow \leq 2$ semaines pour attaquer SDHP assisté d'un oracle (2^{30} appels) avec 1300 processeurs
- 300 fois plus rapide qu'en caractéristique impaire !

Différence caractéristique paire/impaire

- polynôme de Semaev 13 fois plus creux en caractéristique paire
  $\longrightarrow$ matrices beaucoup plus petites
  Exemple au degré 16 :



- à partir du step 18 :
  2 paires max à chaque étape, toujours de la même forme
  $\longrightarrow$ optimisation en conservant la matrice d'une étape à l'autre
  (2 fois plus rapide)

Attaque par décomposition sur $E(\mathbb{F}_{q^n})$, $n > 6$

Quel compromis ?

- complexité des tests de décomposition $\longrightarrow$ approches précédentes irréalisables
- m petit $\longrightarrow$ modifier le choix de la base de factorisation
- complexité algèbre linéaire vs complexité décomposition

Attaque par décomposition sur $E(\mathbb{F}_{q^n})$, $n > 6$

Quel compromis ?

- complexité des tests de décomposition $\longrightarrow$ approches précédentes irréalisables
- m petit $\longrightarrow$ modifier le choix de la base de factorisation
- complexité algèbre linéaire vs complexité décomposition

Idée 1 : décomposer en m points et agrandir la base

$$\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x_P = x_{1,P} + \cdots + x_{d,P} t^{d-1}, \quad x_{1,P}, \ldots, x_{d,P} \in \mathbb{F}_q\}$$

- proba de décomposition : $\simeq q^{md-n}/m!$
- coût algèbre linéaire : $\tilde{O}(mq^{2d})$
- coût décomposition : polynômes obtenus par restriction de Weil seulement invariants par $\mathfrak{S}_m$ et non plus $\mathfrak{S}_{md}$
  $\longrightarrow$ travailler dans $\mathbb{F}_q\left[(X_{ij})_{1\leq i\leq m, 1\leq j\leq d}\right]^{\mathfrak{S}_m}$ infructueux
  $\longrightarrow$ bases de Gröbner SAGBI ?

Attaque par décomposition sur $E(\mathbb{F}_{q^n})$, $n > 6$

Idée 2 : variation "one/double large prime"

Algèbre linéaire en $\tilde{O}(q^2)$, décomposition dans différentes bases

$\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x_P \in \mathbb{F}_q\}$

$\mathcal{F}_0 = \{P \in E(\mathbb{F}_{q^n}) : x_P = x_{0,P} + x_{1,P}t,\ x_{0,P}, x_{1,P} \in \mathbb{F}_q\}$

1. Version "One large prime" :
   $R = P_1 + \ldots + P_{m-2} + Q, \quad P_i \in \mathcal{F}, Q \in \mathcal{F}_0$
   $\rightarrow$ nb tests nécessaires $\simeq (m-2)!q^{n-m+3/2}$

Attaque par décomposition sur $E(\mathbb{F}_{q^n})$, $n > 6$

Idée 2 : variation "one/double large prime"

Algèbre linéaire en $\tilde{O}(q^2)$, décomposition dans différentes bases

$\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x_P \in \mathbb{F}_q\}$

$\mathcal{F}_0 = \{P \in E(\mathbb{F}_{q^n}) : x_P = x_{0,P} + x_{1,P}t,\ x_{0,P}, x_{1,P} \in \mathbb{F}_q\}$

1. Version "One large prime" :
   $R = P_1 + \ldots + P_{m-2} + Q, \quad P_i \in \mathcal{F}, Q \in \mathcal{F}_0$
   $\rightarrow$ nb tests nécessaires $\simeq (m-2)!q^{n-m+3/2}$
2. Version "Double large prime" :
   $R = P_1 + \ldots + P_{m-4} + Q_1 + Q_2, \quad P_i \in \mathcal{F}, Q_i \in \mathcal{F}_0$
   $\rightarrow$ nb tests nécessaires $\simeq 2(m-4)!q^{n-m+2}$

Attaque par décomposition sur $E(\mathbb{F}_{q^n})$, $n > 6$

Idée 2 : variation "one/double large prime"

Algèbre linéaire en $\tilde{O}(q^2)$, décomposition dans différentes bases

$\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x_P \in \mathbb{F}_q\}$

$\mathcal{F}_0 = \{P \in E(\mathbb{F}_{q^n}) : x_P = x_{0,P} + x_{1,P}t,\ x_{0,P}, x_{1,P} \in \mathbb{F}_q\}$

1. Version "One large prime" :
   $R = P_1 + \ldots + P_{m-2} + Q, \quad P_i \in \mathcal{F}, Q \in \mathcal{F}_0$
   $\longrightarrow$ nb tests nécessaires $\simeq (m-2)!q^{n-m+3/2}$
2. Version "Double large prime" :
   $R = P_1 + \ldots + P_{m-4} + Q_1 + Q_2, \quad P_i \in \mathcal{F}, Q_i \in \mathcal{F}_0$
   $\longrightarrow$ nb tests nécessaires $\simeq 2(m-4)!q^{n-m+2}$

- intérêt : polynôme de Semaev de plus petit degré
- mais pas suffisant pour compenser la perte de symétrie
  $\rightsquigarrow$ GB incalculable

Calcul de traces de l'algorithme F4 et applications

Vanessa VITSE – Antoine Joux

Université de Versailles Saint-Quentin, Laboratoire PRISM

Séminaire CARAMEL, LORIA, Nancy