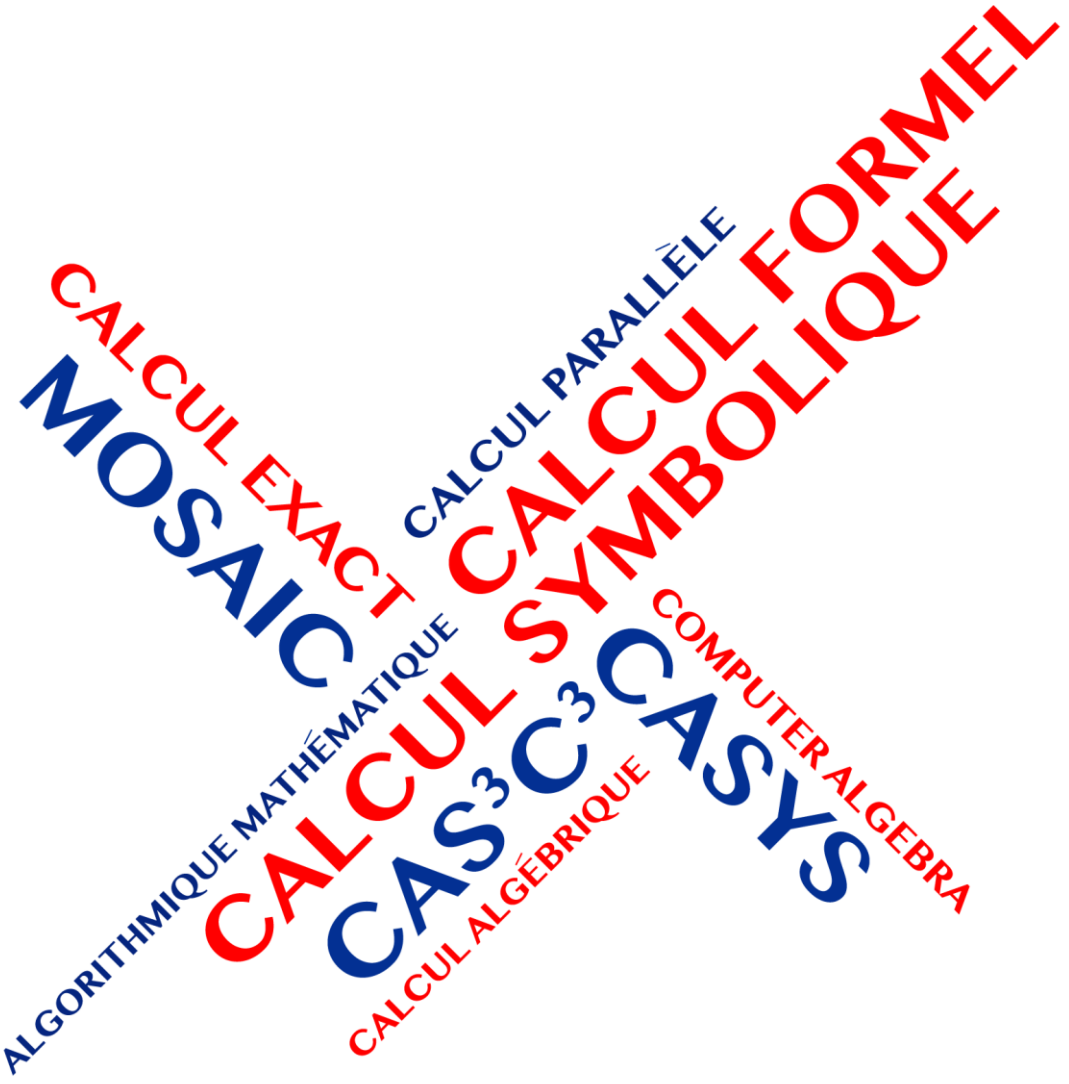
Calcul Formel et Symbolique

Équations algébriques et différentielles, Algèbre linéaire exacte, Cryptanalyse

Jean-Guillaume Dumas, Françoise Jung, Clément Pernet

Université Grenoble Alpes, Laboratoire Jean Kuntzmann, UMR CNRS

Grenoble, 28 novembre 2019


CALCUL FORMEL
CALCUL SYMBOLIQUE
CALCUL PARALLÈLE
CALCUL EXACT
MOSAIC
ALGORITHMIQUE MATHÉMATIQUE
CALCUL
CAS
C3
C3
CASYS
COMPUTER ALGEBRA
CALCUL ALGÉBRIQUE

Une des premières rencontres à Strasbourg

DESIR

Differential Equations Solutions

at Irregular and Regular singular points

DESIR-I de 1982 à 1988

DESIR-II de 1988 à 1992

Un logiciel qui permet l'étude

des équations différentielles scalaires linéaires et homogènes en temps complexe

d'un ordre quelconque

au voisinage de points singuliers réguliers et irréguliers.

$$L = a_d(x)\partial^d + \cdots + a_1(x)\partial + a_0(x), \qquad \partial = \frac{d}{dx}, \quad a_i \in \mathbb{Q}[x]$$

Singularités

$$a_d(x_0) \neq 0$$

oui → Point ordinaire

$$y(x) = \sum_{i=0}^{\infty} g_i (x - x_0)^i$$

non → Point singulier

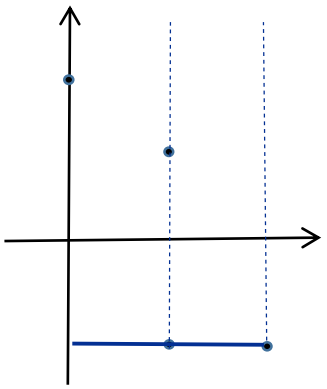
$$(x - x_0)^{d-i} \frac{a_i(x)}{a_d(x)}$$ analytique au voisinage de $x_0, \forall i$

oui → Point singulier régulier

non → Point singulier irrégulier

Polygone de Newton

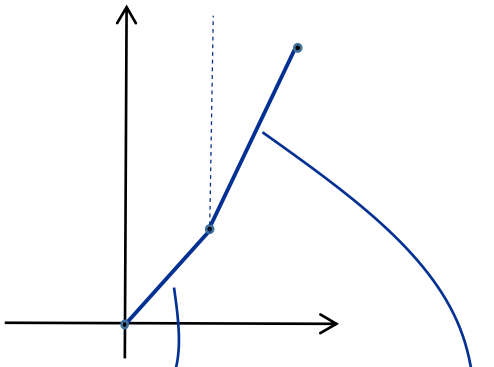
$$L = 4x\partial^2 + 2(4 - x^2)\partial + x^2$$



$$L = \sum a_{i,j}\, x^j \partial^i$$

$$a_{i,j} \neq 0 \longrightarrow (i, j - i)$$

$$L = 4x^5\partial^2 + 2x^2\partial + 1$$



2 arêtes, de pentes 1 et 2

0 est point singulier régulier ssi une unique arête horizontale.

$$y(x) = x^{\lambda} \sum_{i=0}^{\infty} g_i x^i$$

λ est racine de l'équation indicielle

$$y(x) = e^{\frac{a}{x}}\varphi(x) \qquad y(x) = e^{\frac{b}{x^2}}\varphi(x)$$

a et b sont racines des équations caractéristiques

Les séries formelles solutions

Une base de solutions de la forme :

$$x = t^r, r \in \mathbb{N}^*$$

$$y(t) = e^{P(\frac{1}{t})} t^{\lambda} \sum_{i=0}^{s} \hat{\varphi}_i(t) \log^i(t), \quad \hat{\varphi}_i \in \mathbb{C}[[t]]$$

Un prototype écrit en REDUCE, incluant plusieurs modules

- Module arithmétique D5 : calcul avec des nombres algébriques
- Module FROBENIUS : étude des singularités régulières
- Module NEWTON : étude des singularités irrégulières
- Module RESOMMATION : module numérique développé à Strasbourg en FORTRAN
- Module AGILE : module graphique développé à Strasbourg

Thèses soutenues

A. DUVAL Equations aux différences dans le champ complexe – thèse d'Etat 1984 – U.L.P.

D. DUVAL Diverses questions relatives au calcul formel avec des nombres algébriques – thèse d'Etat 1987 – U.J.F.

E. TOURNIER Solutions formelles d'équations différentielles. Le logiciel de calcul formel DESIR – thèse d'Etat 1987 – U.J.F.

A. HILALI Solutions formelles de systèmes différentiels linéaires au voisinage d'un point singulier – thèse d'Etat 1987 – U.J.F.

F. RICHARD-JUNG Représentations graphiques de solutions d'équations différentielles dans le champ complexe – thèse 1988 – U.L.P.

A. HILALI Contribution à l'étude des points singuliers des systèmes différentiels linéaires – thèse de 3ème cycle 1982 – U.J.F.

EL-TAHIRI Algorithme du polygone de Newton appliqué à la résolution d'équations algébriques – thèse de 3ème cycle 1984 – U.J.F.

C. CHAFFY-CAMUS Interpolation polynomiale et rationnelle d'une fonction de plusieurs variables complexes – thèse de 3ème cycle 1984 – U.J.F.

H. NAJID-ZEJLI Extensions algébriques : cas général et cas des radicaux – thèse de 3ème cycle 1985 – U.J.F.

CATHODE

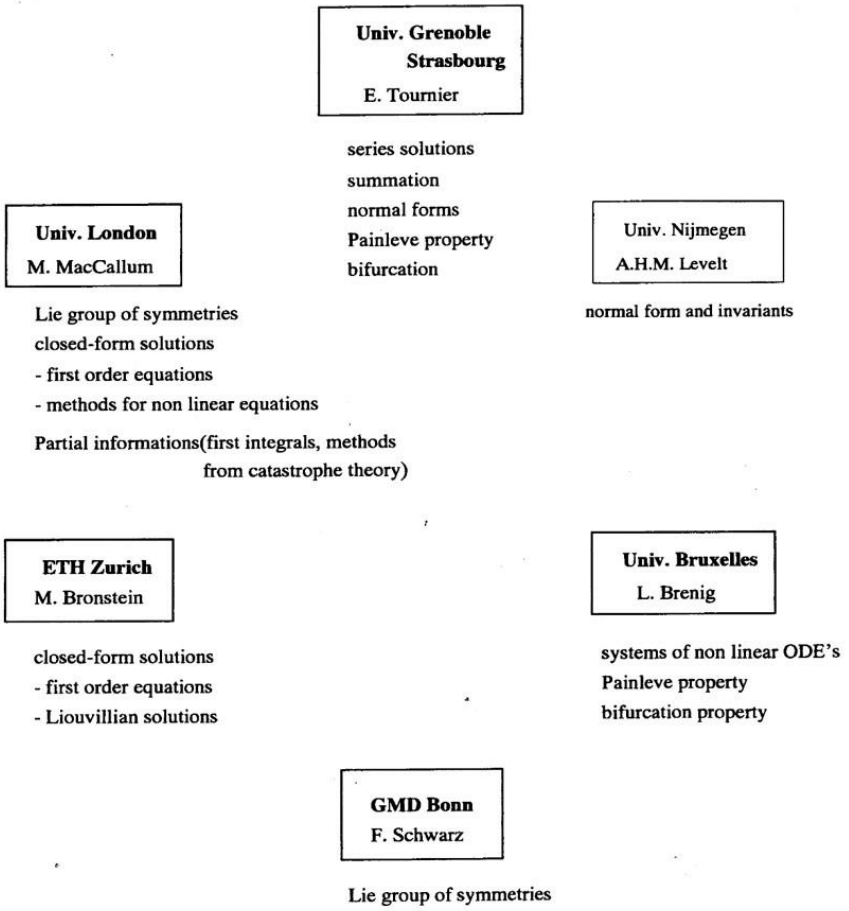
Computer Algebra Tools for Handling Ordinary Differential Equations

CATHODE-1 de 1992 à 1995

CATHODE-2 de 1997 à 2000

3 Composition of the working group and main domains activities

The composition of the Working group is given in the following figure



Les objectifs de CATHODE

Objectifs à long terme

Produire un logiciel de calcul formel qui accepte en entrée une équation ou un système d'EDO et qui retourne toutes les informations *analytiques et qualitatives* sur les solutions.

Ceci en utilisant toutes les techniques modernes de calcul pour implémenter les algorithmes mathématiques : solutions analytiques, resommation, formes normales, méthode d'approximation locale et asymptotique, aide graphique pour l'étude locale. …

Objectifs à court terme

- Spécifications du concept de solution d'une EDO
- Spécifications des primitives mathématiques communes à divers aspects de la résolution d'EDO
- Implémenter ces primitives

Les workshops de CATHODE-1

- 1993 (28 mars-2 avril) à Han sur Lesse
- 1994 (5 – 10 septembre) à Dagsthul
- 1994 (21 – 25 mars) à Londres
- 1995 (9 – 12 janvier) à Nijmegen

Londres, 1994

Les workshops de CATHODE-2

- 1997 (1-5 septembre) à Han sur Lesse
- 1998 (11-15 mai) à Valladolid, Castillo de la Mota
- 1999 (3-7 mai) au CIRM, Luminy
- 2000 (4-8 avril) au CIRM, Luminy

Han sur Lesse - 1997

Les principales applications étudiées

« Five main types of applications whose diversity reflects the versatility of our methods, have been considered during the three years of CATHODE-2 :

1- Electric discharges in gases

2- Electric power networks at national scale

3- Properties of neural networks

4- Methods for generating thermodynamical equations of state for mixture of unperfect gases

5- Cosmology »

Thèses soutenues

M. BARKATOU Contribution à l'étude des équations différentielles et aux différences dans le champ complexe - 1989

G. CHEN Solutions formelles de systèmes d'équations différentielles linéaires ordinaires homogènes - 1990

L. STOLOVITCH Classification analytique de champs de vecteurs - 1994

F. NAEGELE Autour de quelques équations fonctionnelles analytiques - 1995

E. HUBERT Etude Algébrique et Algorithmique des Singularités des Equations Différentielles Implicites - 1997

L. TESTARD Calcul et visualisation en nombres complexes - 1997

G. THOMAS Contributions théoriques et algorithmiques à l'étude des équations différentielles algébriques. Approche par le calcul formel - 1997

E. PFLUGEL Résolution symbolique des systèmes différentiels linéaires - 1998

L. REBILLARD Etude théorique et algorithmique des séries de Chebyshev solutions d'équations différentielles holonomes - 1998

R AID Contribution à l'estimation de l'erreur globale des méthodes d'intégration numérique à un pas. Application à la simulation de réseaux électriques - 1998

A. WAZNER Formes canoniques invariantes d'un système linéaire différentiel homogène, polygone de Newton, calcul de la partie exponentielle des solutions formelles - 1998

J. VISCONTI Résolution numérique des Equations Algébro-Différentielles, Estimation de l'erreur globale et Réduction formelle de l'indice - 1999

G. EICHENMULLER Réduction et Intégration symbolique des systèmes d'équations différentielles non-linéaires - 2000

M. MIRICA-RUSE Contribution à l'étude des systèmes hybrides - 2002

F. BERINGER Contributions à la résolution d'équations différentielles non linéaires scalaires par la méthode du polygone de Newton - 2002

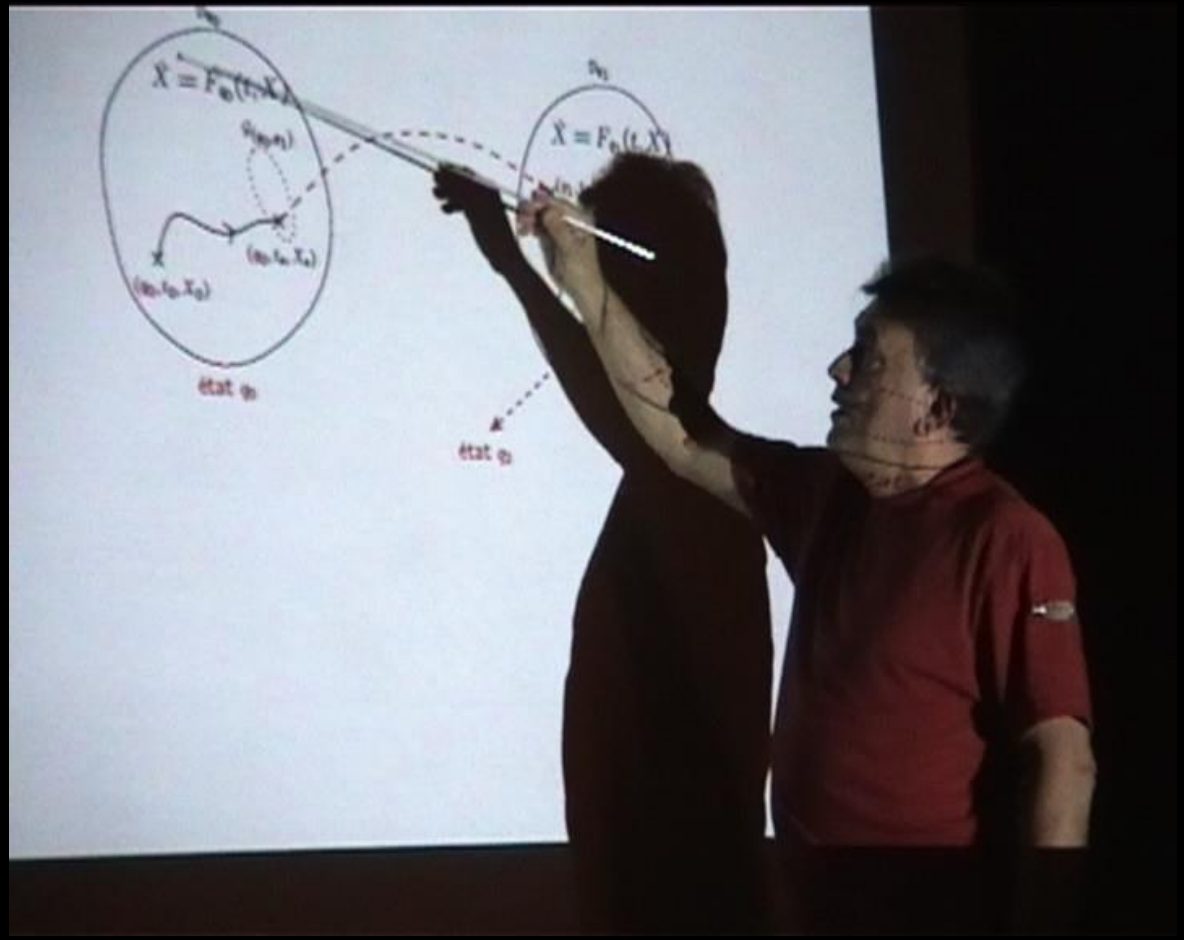
A. GIRARD Analyse Algorithmique des Systèmes Hybrides - 2004

E. FARCOT Etude d'une classe d'équations différentielles affines par morceaux modélisant des réseaux de régulation biologique - 2005

L. TOURNIER Etude et modélisation mathématique de réseaux de régulation génétique et métabolique - 2005

A. RONDEPIERRE Algorithmes hybrides pour le contrôle optimal des systèmes non linéaires - 2006

S. KOLB Théorie des bifurcations appliquée à l'analyse de la dynamique du vol des hélicoptères - 2007



Transgressive Computing 2006 – Grenade – 24-26 avril 2006

Plan

Équations algébriques et différentielles

Algèbre linéaire exacte
- Multiplication de matrices
- Élimination de Gauss

Cryptanalyse : affiner les paramètres de cryptosystèmes
- Échange de clef secrète dans un groupe (Diffie-Hellman)
- Logarithme discret modulaire par calcul d'index dans une courbe elliptique
- Bases de Gröbner, algorithme de Buchberger et algèbre linéaire
- Challenge de calcul HPAC

Algèbre linéaire exacte

Domaine de calcul : $\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}, \mathbb{F}_{p^k}, \mathbb{F}_{p^k}[X]$, etc

Similarité avec l'algèbre linéaire numérique :

- brique de base centrale,
- forte intensité calcul/mémoire,
- algorithmique (relativement) simple et régulière.

Spécificités :

- Déficience de rang,
- Absence de problème de stabilité,
- diversité des arithmétiques (corps finis, multiprécision, etc).

Illustration ici sur

- deux problèmes clés : le produit de matrices et l'élimination de Gauss
- illustrés par les contributions Grenobloises

Algorithmes rapides de produits matriciels

Algorithme de Strassen

$$\begin{aligned}
\rho_1 &\leftarrow (a_{11}+a_{22})(b_{11}+b_{22}), & \rho_4 &\leftarrow (a_{11}+a_{12})b_{22},\\
\rho_2 &\leftarrow (a_{12}-a_{22})(b_{21}+b_{22}), & \rho_5 &\leftarrow a_{11}(b_{12}-b_{22}),\\
\rho_3 &\leftarrow (a_{21}-a_{11})(b_{11}+b_{12}), & \rho_6 &\leftarrow a_{22}(b_{21}-b_{11}),\\
& & \rho_7 &\leftarrow (a_{21}+a_{22})b_{11},
\end{aligned}$$

$$\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = \begin{pmatrix} \rho_1+\rho_2-\rho_4+\rho_6 & \rho_6+\rho_7, \\ \rho_4+\rho_5 & \rho_1+\rho_3+\rho_5-\rho_7 \end{pmatrix}.$$

V. Strassen 1969 : 2×2 en $\mathbf{18}+$ et $\mathbf{7}\times$ ⇨$n\times n$ en $\mathbf{7n^{2.8074}+o(n^{2.8076})}$

S. Winograd circa 1970 : 2×2 en $\mathbf{15}+$ et $\mathbf{7}\times$ ⇨$n\times n$ en $\mathbf{6n^{2.8074}+o(n^{2.8074})}$

N. Gastinel 1971 : Interpréte Strassen comme produits de Hadamard.
⇨introduit une paramétrisation

P. Chatelin 1985 : Transformations invariantes d'algorithmes
⇨Dérive Winograd de Strassen

Algorithmes rapides de produits matriciels

Dumas Gautier Pernet 2002 : Mise en oeuvre pour les corps finis : BLAS + Strassen

Boyer Dumas Pernet Zhu 2009 : Empreinte mémoire de Strassen-Winograd

Dumas Pernet Sedoglavitch (en cours) : $A \times A^T$ en 7.5 + et 5 $\times$

⇨généralise les paramétrisations de Chatelin

Autres algorithmes sous-cubiques praticables :

Kaporin'04 : Mise en pratique de [Pan'72]

Boyer Dumas 16 : Adaptation exacte de [Bini & al.' 79] aux corps finis

BLIS'16, Balard'14 : Strassen pour les BLAS numériques

Schwartz & al. 17,19 : Transformations invariantes en pratique

Mise en oeuvre

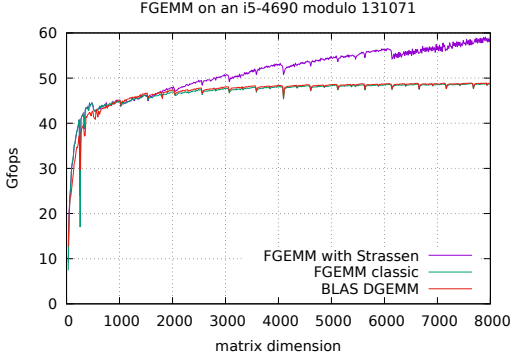
Bibliothèques d'algèbre linéaire exacte : `LinBox`, `fflas-ffpack`

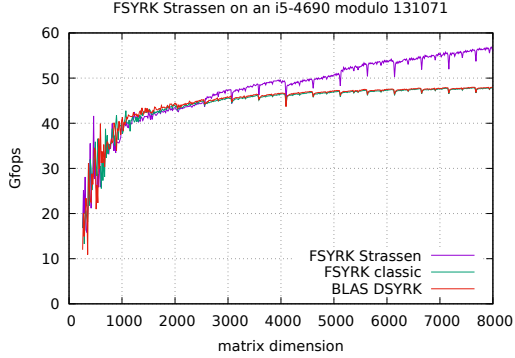
- Open source, paquets : `Debian, arch, fedora`
- Noyaux dans `SageMath, Macaulay2`
- Approche adoptée par `Maple, Mathematica, magma`

Mise en oeuvre

Bibliothèques d'algèbre linéaire exacte : `LinBox`, `fflas-ffpack`

- Open source, paquets : `Debian, arch, fedora`
- Noyaux dans `SageMath, Macaulay2`
- Approche adoptée par `Maple, Mathematica, magma`



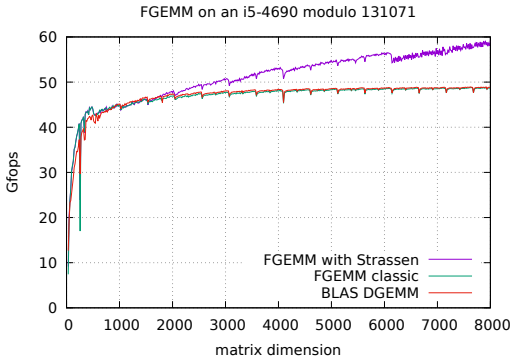


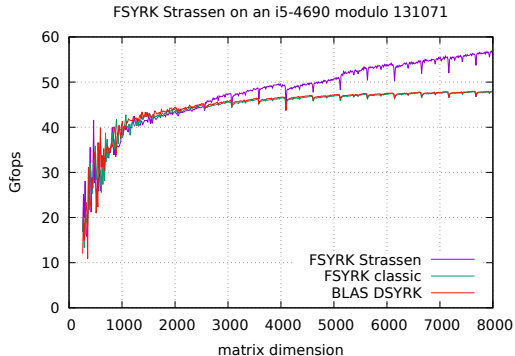
Mise en oeuvre

Bibliothèques d'algèbre linéaire exacte : `LinBox`, `fflas-ffpack`

- Open source, paquets : `Debian, arch, fedora`
- Noyaux dans `SageMath, Macaulay2`
- Approche adoptée par `Maple, Mathematica, magma`

	$A \times B$	$A \times A^T$
$n = 2000$	0.37s	0.19s
$n = 8000$	s 17.3	9.15s





Élimination de Gauss

Algorithmique et implantations haute performance

Villard 88 : Parallélisation sur un hypercube 16 proc.

Dumas Giorgi Pernet 08 : Mise en pratique des réductions au produit de matrice

Dumas Pernet Sultan 16 : Parallélisation multi-coeur

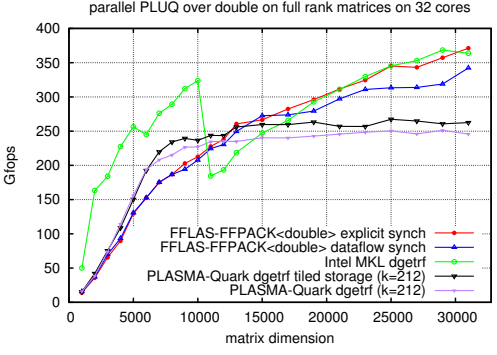
Élimination de Gauss

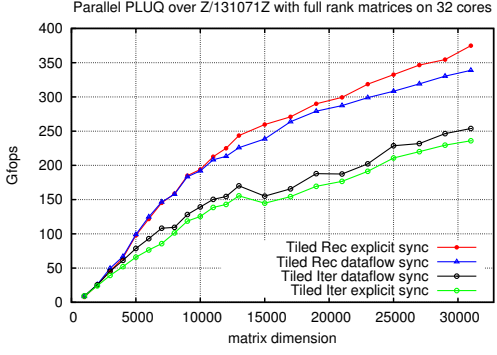
Algorithmique et implantations haute performance

Villard 88 : Parallélisation sur un hypercube 16 proc.

Dumas Giorgi Pernet 08 : Mise en pratique des réductions au produit de matrice

Dumas Pernet Sultan 16 : Parallélisation multi-coeur





Pivotage et profils de rang

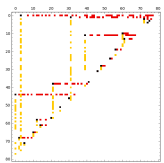
Spécificité du calcul exact :

- Déficience de rang
- Le rang ou le profil de rang sont l'objet du calcul

Dumas Pernet Sultan 15 : *Computing the rank profile matrix*

- Nouvel invariant, résumant toute l'information des profils de rang
- caractérisation des conditions sur le pivotage pour la calculer
- $O(n^\omega)$ par un nouvel algorithme récursif par tuiles.
- Connexion avec la forme généralisée de Bruhat [Della-Dora 73]

Pernet 16 : application à l'algorithmique des matrices quasi-séparables



Plan

Équations algébriques et différentielles

Algèbre linéaire exacte
- Multiplication de matrices
- Élimination de Gauss

Cryptanalyse : affiner les paramètres de cryptosystèmes
- Échange de clef secrète dans un groupe (Diffie-Hellman)
- Logarithme discret modulaire par calcul d'index dans une courbe elliptique
- Bases de Gröbner, algorithme de Buchberger et algèbre linéaire
- Challenge de calcul HPAC

Diffie-Hellman (1976)

● est public

secret ●

● secret

Diffie-Hellman (1976)

● est public

● & ●

secret ●

● secret

Diffie-Hellman (1976)

● est public

● & ●

● & ●

secret ●

● secret

Diffie-Hellman (1976)

● est public

● & ●

● & ●

secret ●

● & ● & ●

● secret

Diffie-Hellman (1976)

● est public

● & ●

● & ●

secret ●

● & ● & ●

● secret

- $g =$ ●
- $a =$ ●
- $b =$ ●

Groupe mult. : $(g^a)^b = g^{ab} = (g^b)^a$

Diffie-Hellman (1976)

● est public

g^a

● & ●

secret ●

● & ● & ●

● secret

- $g =$ ●
- $a =$ ●
- $b =$ ●

Groupe mult. : $(g^a)^b = g^{ab} = (g^b)^a$

Diffie-Hellman (1976)

● est public

g^a

g^b

secret ● ● & ● & ● ● secret

- $g =$ ●
- $a =$ ●
- $b =$ ●

Groupe mult. : $(g^a)^b = g^{ab} = (g^b)^a$

Diffie-Hellman (1976)

● est public

g^a

g^b

secret ● clef : g^{ab} ● secret

- $g =$ ●
- $a =$ ●
- $b =$ ●

Groupe mult. : $(g^a)^b = g^{ab} = (g^b)^a$

Diffie-Hellman (1976)

● est public

g^a

g^b

secret ● clef : g^{ab} ● secret

- $g =$ ●
- $a =$ ●
- $b =$ ●

Groupe mult. : $(g^a)^b = g^{ab} = (g^b)^a$

Groupe add. : $[b][a]G = [ab]G = [a][b]G$

Groupe des points d'une courbe elliptique

$$\mathbb{E}(\mathbb{F}_q) = (\{(x, y) \in \mathbb{F}_q \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}, \oplus)$$

$$[a]P = \underbrace{P \oplus \ldots \oplus P}_{a \text{ fois}}$$

Groupe des points d'une courbe elliptique

$$\mathbb{E}(\mathbb{F}_q) = (\{(x, y) \in \mathbb{F}_q \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}, \oplus)$$

$$[a]P = \underbrace{P \oplus \ldots \oplus P}_{a \text{ fois}}$$

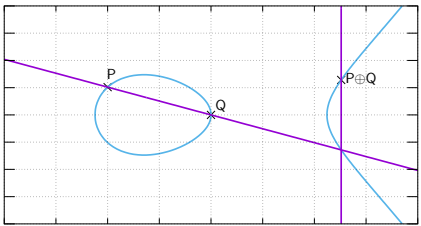
⚠ Le logarithme discret ($a = \log_P(Q)$ pour $Q = [a]P$, connaissant P et Q) doit être difficile pour protéger les clefs

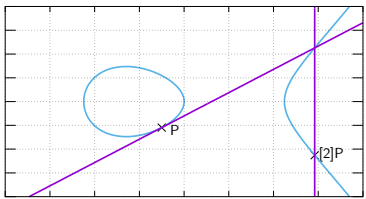
Groupe des points d'une courbe elliptique

$$\mathbb{E}(\mathbb{F}_q) = (\{(x, y) \in \mathbb{F}_q \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}, \oplus)$$

$$[a]P = \underbrace{P \oplus \ldots \oplus P}_{a \text{ fois}}$$

Loi de groupe :





⚠ Le logarithme discret ($a = \log_P(Q)$ pour $Q = [a]P$, connaissant P et Q) doit être difficile pour protéger les clefs

Calcul d'index sur courbes elliptiques

- *[Gaudry 2005]*
- *[Faugère, Gaudry, Huot, Renault 2013]*
- *[Faugère, Huot, Joux, Renault, Vitse 2014]*

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

Calcul d'index sur courbes elliptiques

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

1: Famille : $\mathcal{F} = \{(x, y) \in \mathbb{E}(\mathbb{F}_{2^{n\ell}}) | x \in \mathbb{F}_{2^{\ell}}\}$

Calcul d'index sur courbes elliptiques

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

1: Famille : $\mathcal{F} = \{(x, y) \in \mathbb{E}(\mathbb{F}_{2^{n\ell}}) | x \in \mathbb{F}_{2^\ell}\}$

2: Crible : $[a_j]P \oplus [b_j]Q = R_1 \oplus \ldots \oplus R_k$, avec $R_i \in \mathcal{F}$

Calcul d'index sur courbes elliptiques

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

1: Famille : $\mathcal{F} = \{(x, y) \in \mathbb{E}(\mathbb{F}_{2^{n\ell}}) | x \in \mathbb{F}_{2^{\ell}}\}$

2: Crible : $[a_j]P \oplus [b_j]Q = R_1 \oplus \ldots \oplus R_k$, avec $R_i \in \mathcal{F}$

3: LinAlg. : $\sum_j [\lambda_j \cdot aj]P \oplus [\lambda_j \cdot b_j]Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$

Calcul d'index sur courbes elliptiques

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

1: Famille : $\mathcal{F} = \{(x, y) \in \mathbb{E}(\mathbb{F}_{2^{n\ell}}) | x \in \mathbb{F}_{2^{\ell}}\}$

2: Crible : $[a_j]P \oplus [b_j]Q = R_1 \oplus \ldots \oplus R_k$, avec $R_i \in \mathcal{F}$

3: LinAlg. : $\sum_j [\lambda_j \cdot aj]P \oplus [\lambda_j \cdot b_j]Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$

4: Remontée : $\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} P \oplus \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$; $u\beta_1 + v\beta_2 = 1$; $a \leftarrow -(u\alpha_1 + v\alpha_2)$

Calcul d'index sur courbes elliptiques

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

1: Famille : sous-ensemble structuré $\#\mathcal{F} \approx 2^{\ell}/4$

2: Crible : $[a_j]P \oplus [b_j]Q = R_1 \oplus \ldots \oplus R_k$, avec $R_i \in \mathcal{F}$

3: LinAlg. : $\sum_j [\lambda_j \cdot aj]P \oplus [\lambda_j \cdot b_j]Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$

4: Remontée : $\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} P \oplus \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$; $u\beta_1 + v\beta_2 = 1$; $a \leftarrow -(u\alpha_1 + v\alpha_2)$

Calcul d'index sur courbes elliptiques

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

1: Famille : sous-ensemble structuré $\#\mathcal{F} \approx 2^{\ell}/4$

2: Crible : bases de Gröbner Proba. $1/(2^{n-1}n!)$

3: LinAlg. : $\sum_j [\lambda_j \cdot aj]P \oplus [\lambda_j \cdot b_j]Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$

4: Remontée : $\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} P \oplus \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$; $u\beta_1 + v\beta_2 = 1$; $a \leftarrow -(u\alpha_1 + v\alpha_2)$

Calcul d'index sur courbes elliptiques

Entrées: $P, Q \in \mathbb{E}(\mathbb{F}_{2^{n\ell}})$.

Sortie: $a \in \mathbb{Z}$ tel que $Q = [a]P$.

1: Famille : sous-ensemble structuré $\#\mathcal{F} \approx 2^{\ell}/4$

2: Crible : bases de Gröbner Proba. $1/(2^{n-1}n!)$

3: LinAlg. : creuse $2^{\ell-2} \times 2^{\ell-2}$, sur $\mathbb{F}_{2^{n\ell}}$

4: Remontée : $\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} P \oplus \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} Q = 0_{\mathbb{E}(\mathbb{F}_{2^{n\ell}})}$; $u\beta_1 + v\beta_2 = 1$; $a \leftarrow -(u\alpha_1 + v\alpha_2)$

Crible algébrique

- Trouver des $M = [a_j]P \oplus [b_j]Q$ (recherche aléatoire) en relation avec la sous-famille $\mathcal{F}$:

$$R_1, \ldots, R_k, \text{ avec } R_i \in \mathcal{F} \text{ tels que } M = R_1 \oplus \ldots \oplus R_k \ ?$$

Crible algébrique

- Trouver des $M = [a_j]P \oplus [b_j]Q$ (recherche aléatoire) en relation avec la sous-famille $\mathcal{F}$:

$$R_1, \ldots, R_k, \text{ avec } R_i \in \mathcal{F} \text{ tels que } M = R_1 \oplus \ldots \oplus R_k \ ?$$

$$\text{PoSSo} : \begin{cases} x_i \in \mathbb{F}_{2^\ell} \\ (x_i, y_i) \in \mathbb{E}(\mathbb{F}_{2^{n\ell}}) : y_i^2 = x_i^3 + ax_i + b \\ (M_x, M_y) - (x_1, y_1) \oplus (x_2, y_2) \oplus \ldots \oplus (x_k, y_k) = 0 \end{cases}$$

Crible algébrique

- Trouver des $M = [a_j]P \oplus [b_j]Q$ (recherche aléatoire) en relation avec la sous-famille $\mathcal{F}$:

$$R_1, \ldots, R_k, \text{ avec } R_i \in \mathcal{F} \text{ tels que } M = R_1 \oplus \ldots \oplus R_k \ ?$$

$$\text{PoSSo} : \begin{cases} x_i \in \mathbb{F}_{2^\ell} \\ (x_i, y_i) \in \mathbb{E}(\mathbb{F}_{2^{n\ell}}) : y_i^2 = x_i^3 + ax_i + b \\ (M_x, M_y) - (x_1, y_1) \oplus (x_2, y_2) \oplus \ldots \oplus (x_k, y_k) = 0 \end{cases}$$

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_1 + x_2 y_2}{x_1 x_2 + y_1 y_2}, \frac{x_1 y_1 - x_2 y_2}{x_1 y_2 - y_1 x_2} \right) \in \mathbb{F}_{2^{n\ell}}^2$$

Crible algébrique

- Trouver des $M = [a_j]P \oplus [b_j]Q$ (recherche aléatoire) en relation avec la sous-famille $\mathcal{F}$:

$$R_1, \ldots, R_k, \text{ avec } R_i \in \mathcal{F} \text{ tels que } M = R_1 \oplus \ldots \oplus R_k \ ?$$

$$\text{PoSSo} : \begin{cases} x_i \in \mathbb{F}_{2^\ell} \\ (x_i, y_i) \in \mathbb{E}(\mathbb{F}_{2^{n\ell}}) : y_i^2 = x_i^3 + ax_i + b \\ (M_x, M_y) - (x_1, y_1) \oplus (x_2, y_2) \oplus \ldots \oplus (x_k, y_k) = 0 \end{cases}$$

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_1 + x_2 y_2}{x_1 x_2 + y_1 y_2}, \frac{x_1 y_1 - x_2 y_2}{x_1 y_2 - y_1 x_2} \right) \in \mathbb{F}_{2^{n\ell}}^2$$

$$x_i, y_i \in \mathbb{F}_{2^{n\ell}} \cong \left(\mathbb{F}[z] \mod z^{n\ell} + \ldots + p_2 z^2 + p_1 z + 1 \mod 2 \right)$$

Bases de Gröbner et systèmes polynomiaux

- base de Gröbner d'un idéal polynomial $\mathcal{I}$  *[Buchberger 1976]*
  - $\prec$ ordre monomial
  - Base de Gröbner G :

$$\forall p \in \mathcal{I}, \exists g \in G, \mathrm{LeadMonom}(g, \prec) \mid \mathrm{LeadMonom}(p, \prec)$$

Bases de Gröbner et systèmes polynomiaux

- base de Gröbner d'un idéal polynomial $\mathcal{I}$  *[Buchberger 1976]*
  - $\prec$ ordre monomial
  - Base de Gröbner G :

$$\forall p \in \mathcal{I}, \exists g \in G, \mathrm{LeadMonom}(g, \prec) \mid \mathrm{LeadMonom}(p, \prec)$$

- Résolution de Systèmes Polynomiaux sur un corps fini
  - PoSSo_q :

$$\begin{cases} p_1(z_1, \ldots, z_m) = 0 \\ \vdots \\ p_n(z_1, \ldots, z_m) = 0 \end{cases}$$

  - NP-dur

Exemple de résolution avec base de Gröbner

$$\begin{cases} 0 = & 2TX - 2YZ + 3Z^2 \\ 0 = & -2TY + 2XZ \\ 0 = & 2TZ - 2XY - 2X \\ 0 = & T^2 + X^2 + Z^2 - 1 \end{cases}$$

Exemple de résolution avec base de Gröbner

$$\begin{cases} 0 = & 2TX - 2YZ + 3Z^2 \\ 0 = & -2TY + 2XZ \\ 0 = & 2TZ - 2XY - 2X \\ 0 = & T^2 + X^2 + Z^2 - 1 \end{cases} \iff \begin{cases} 0 = & 1152X^7 - 1763X^5 + 655X^3 - 44X \\ 0 = & -1152X^6 + 118TX^3 + 1605X^4 - 118TX - 453X^2 \\ 0 = & -1152X^5 + 3835TX^2 - 1404X^3 + 3835XZ + 2556X \\ 0 = & -335232X^6 + 477321X^4 - 11505TX - 134419X^2 + 7670Y - 1150 \\ 0 = & -6912X^5 + 3835T^2X + 10751X^3 - 3839X \\ 0 = & -19584X^5 + 25987X^3 + 3835TZ - 6403X \\ 0 = & -9216X^5 + 3835T^3 + 3835TX^2 + 11778X^3 - 3835T - 2562X \\ 0 = & T^2 + X^2 + Z^2 - 1 \end{cases}$$

Exemple de résolution avec base de Gröbner

$$\begin{cases} 0 = & 2TX - 2YZ + 3Z^2 \\ 0 = & -2TY + 2XZ \\ 0 = & 2TZ - 2XY - 2X \\ 0 = & T^2 + X^2 + Z^2 - 1 \end{cases} \iff \begin{cases} 0 = & 1152X^7 - 1763X^5 + 655X^3 - 44X \\ 0 = & -1152X^6 + 118TX^3 + 1605X^4 - 118TX - 453X^2 \\ 0 = & -1152X^5 + 3835TX^2 - 1404X^3 + 3835XZ + 2556X \\ 0 = & -335232X^6 + 477321X^4 - 11505TX - 134419X^2 + 7670Y - 1150 \\ 0 = & -6912X^5 + 3835T^2X + 10751X^3 - 3839X \\ 0 = & -19584X^5 + 25987X^3 + 3835TZ - 6403X \\ 0 = & -9216X^5 + 3835T^3 + 3835TX^2 + 11778X^3 - 3835T - 2562X \\ 0 = & T^2 + X^2 + Z^2 - 1 \end{cases}$$

- Buchberger 1976 : $\mathcal{O}\left(d^{2^{n+o(1)}}\right)$
- Aujourd'hui : algorithmes F4, F5, systèmes creux, invariants, FGLM, ...

⇨ plusieurs centaines de polynômes, chacun avec plusieurs centaines de termes et coefficients de plusieurs centaines de chiffres.

Algorithme de Buchberger

Entrées: un système de polynômes $F = (f_1, ..., f_n)$, un ordre monomial $\prec$
Sortie: une base de Gröbner de $\langle f_1, ..., f_n \rangle$

1: $G \leftarrow F$
2: **Répéter**
3: $G' \leftarrow G$
4: **Pour** chaque paire $\{P, Q\}$ de G' **Faire**
5: $m \leftarrow ppcm(\text{LeadMonom}(P), \text{LeadMonom}(Q))$
6: $S \leftarrow \text{LeadCoeff}(P) \frac{m}{\text{LeadMonom}(P)} P - \text{LeadCoeff}(Q) \frac{m}{\text{LeadMonom}(Q)} Q$
7: $R \leftarrow S \mod G'$
8: **Si** $R \neq 0$ **Alors** $G \leftarrow G \cup \{R\}$
9: **Fin Pour**
10: **Jusqu'à ce que** $G = G'$
11: **Retourner** G

- Borne de complexité générique : $\mathcal{O}\left(d^{2^{m+o(1)}}\right)$

40 ans de bases de Gröbner

- Algorithmes F4, F5 : n equations, m variables, D_{reg} degré de régularité [1] :

$$\mathcal{O}\left(m \cdot \binom{n + D_{reg}}{D_{reg}}^{\omega}\right)$$

- Systèmes creux ou structurés ;
- Invariants ;
- Puis FGLM : Idéal de dimensions 0, Z nombre de solutions, changement d'ordre monomial en $\mathcal{O}(mZ^{\omega})$;
- ...

⇨Aujourd'hui : plusieurs centaines de polynômes, chacun avec plusieurs centaines de termes et coefficients de plusieurs centaines de chiffres.

1. $D_{reg}(p_1, \ldots, p_n) = min\left\{D_0 \geq 0 | dim_{F_q}(\{p \in \mathcal{I} | deg(p) = D_0\}) = \#\text{Monomials}_q(m, D_0)\right\}$

Projet HPAC

ANR HPAC [2012-2016] : Grenoble, Lyon, Montpellier, Paris, North Carolina

- Logarithme discret dans une courbe ayant $\approx 2^{114}$ points dans $\mathbb{F}_{2^{116}}^2 = \mathbb{F}_{2^{4\times 29}}^2$

Projet HPAC

ANR HPAC [2012-2016] : Grenoble, Lyon, Montpellier, Paris, North Carolina

- Logarithme discret dans une courbe ayant $\approx 2^{114}$ points dans $\mathbb{F}_{2^{116}}^2 = \mathbb{F}_{2^{4\times 29}}^2$

1. Crible :
   - $2^{29} = 536\,870\,912$ relations creuses
   - Une semaine sur plus de 1000 ordinateurs personnels de Paris 6

Projet HPAC

ANR HPAC [2012-2016] : Grenoble, Lyon, Montpellier, Paris, North Carolina

- Logarithme discret dans une courbe ayant $\approx 2^{114}$ points dans $\mathbb{F}_{2^{116}}^2 = \mathbb{F}_{2^{4\times 29}}^2$

1. Crible :
   - $2^{29} = 536\,870\,912$ relations creuses
   - Une semaine sur plus de 1000 ordinateurs personnels de Paris 6
2. Algèbre linéaire :
   - Filtrage : 7 196 707 équations et inconnues, 11Go de coefficients
   - Solution : Un serveur 32 cœurs à Grenoble
     - 2.1 Séquence (itérations) : 57 jours
     - 2.2 Polynôme minimal : 54 heures avec 561 Go de RAM/Swap
     - 2.3 Évaluation : 19 jours

Projet HPAC

ANR HPAC [2012-2016] : Grenoble, Lyon, Montpellier, Paris, North Carolina

- Logarithme discret dans une courbe ayant $\approx 2^{114}$ points dans $\mathbb{F}_{2^{116}}^2 = \mathbb{F}_{2^{4\times 29}}^2$

1. Crible :
   - $2^{29} = 536\,870\,912$ relations creuses
   - Une semaine sur plus de 1000 ordinateurs personnels de Paris 6
2. Algèbre linéaire :
   - Filtrage : 7 196 707 équations et inconnues, 11Go de coefficients
   - Solution : Un serveur 32 cœurs à Grenoble
     - 2.1 Séquence (itérations) : 57 jours
     - 2.2 Polynôme minimal : 54 heures avec 561 Go de RAM/Swap
     - 2.3 Évaluation : 19 jours

⇨Courbe IPSEc, $\approx 2^{151}$ points dans $\mathbb{F}_{2^{155}}^2 = \mathbb{F}_{2^{5\times 31}}^2$: Crible $\times$ 3000, LinAlg $\times$ 22 ...