AriC : Arithmetic and Computing

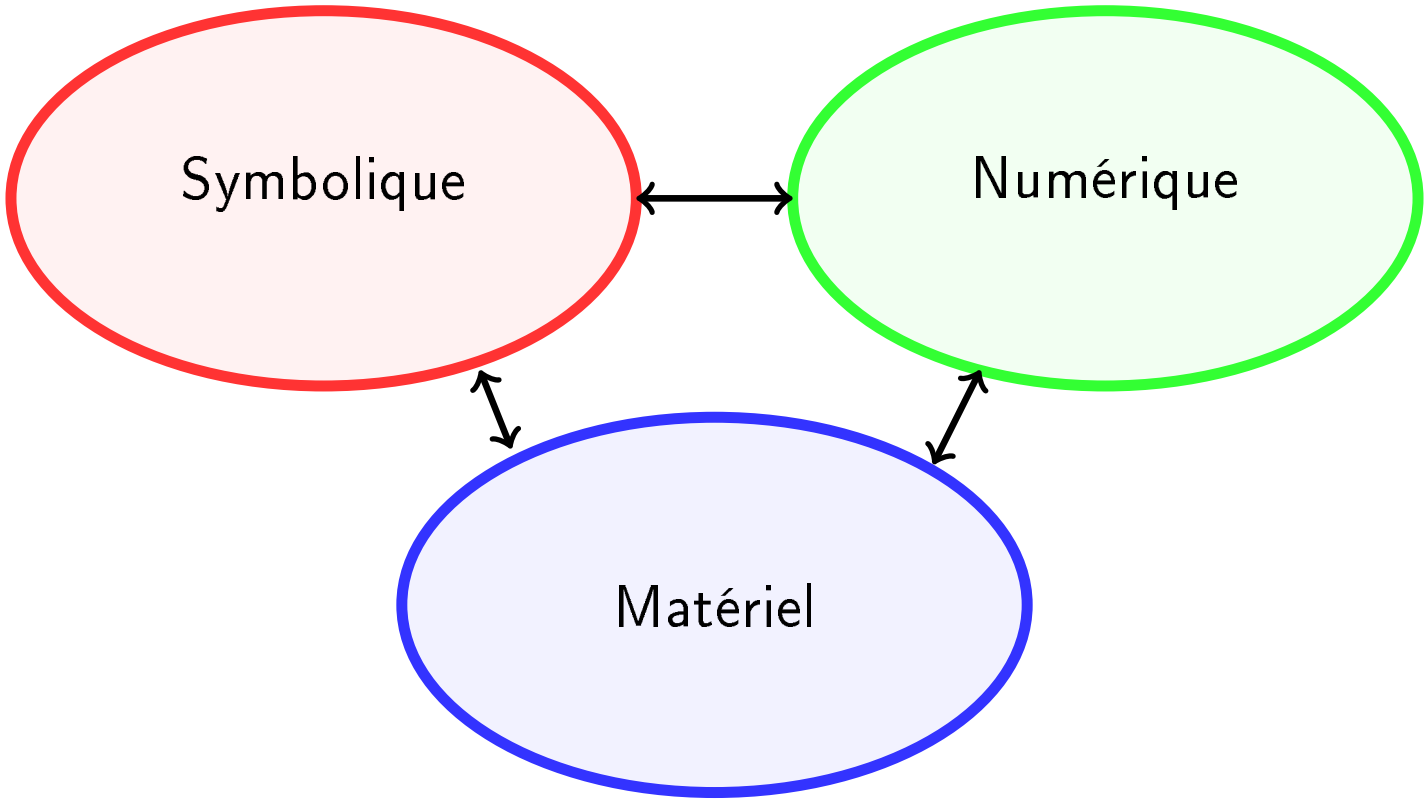
Améliorer le calcul, en termes de performance, d'efficacité et de fiabilité.

http://www.ens-lyon.fr/LIP/AriC/

Novembre 2014 – Évaluation du LIP

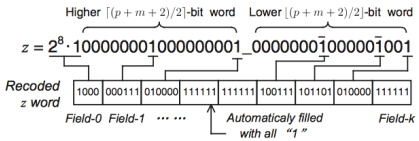
AriC : Arithmetic and Computing

Améliorer le calcul, en termes de performance, d'efficacité et de fiabilité.

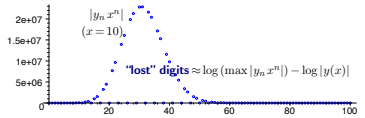


AriC : Arithmetic and Computing

- algorithmes arithmétiques & leur implantation (matérielle, logicielle) :
  - arithmétique entière et virgule flottante ;
  - arithmétique complexe, multi-précision ;

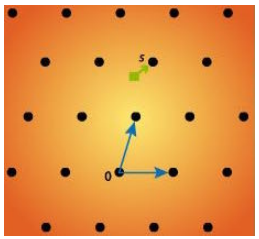


- méthodes d'approximation :
  - approximation sous contraintes particulières ;
  - approximation certifiée ;



$$\mathrm{Ai}(x) = A - Bx + \frac{A}{6}x^3 - \frac{B}{12}x^4 + \frac{A}{180}x^6 - \frac{B}{504}x^7 + \frac{A}{12960}x^9 - \cdots$$

- réseaux euclidiens et cryptographie :
  - algorithmique des réseaux ;
  - cryptographie reposant sur les réseaux ;



- calcul certifié et calcul formel :
  - algèbre linéaire, systèmes polynomiaux, équations différentielles ;
  - arithmétique d'intervalles.

AriC : Arithmetic and Computing

Équipe commune    

- fait suite à l'équipe Arénaire ;
- Effectifs actuels :
  - 13 permanents : 4 enseignants-chercheurs (3PR+1MCF), 7 chercheurs (3DR+4CR), 1 IR, 1 administratif ;
  - 8 non-permanents : 6 doctorants, 1 délégation, 1 postdoc ;
- direction :
  - $\longrightarrow$ 30 juin 2013 : Florent de Dinechin (maintenant PR INSA Lyon) ;
  - juillet 2013 $\longrightarrow$ mars 2015 : Jean-Michel Muller ;
  - mars 2015 $\longrightarrow$: Bruno Salvy et Gilles Villard.

Membres permanents présents actuellement

4 Enseignants-chercheurs

- Guillaume Hanrot, PR ENS Lyon ;
- Fabien Laguillaumie, PR UCBL ;
- Nicolas Louvet, MCF UCBL ;
- Damien Stehlé, PR ENS Lyon ;

2 Ingénieurs et administratifs

- Damien Séon, assistant, ENS Lyon ;
- Serge Torres, IR ENS Lyon ;

7 Chercheurs

- Nicolas Brisebarre, CR CNRS ;
- Claude-Pierre Jeannerod, CR Inria ;
- Vincent Lefèvre, CR Inria ;
- Jean-Michel Muller, DR CNRS ;
- Nathalie Revol, CR Inria ;
- Bruno Salvy, DR Inria ;
- Gilles Villard, DR CNRS.

Arrivées : Hanrot, Laguillaumie, Salvy.

Départ : de Dinechin.

Membres non permanents présents actuellement

7 Doctorants

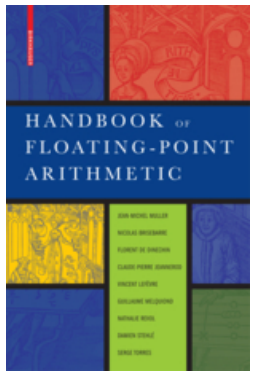
- Silviu Filip (allocation ordinaire) ;
- Sébastien Maulat (ENS Lyon) ;
- Vincent Neiger (ENS Lyon) ;
- Marie Paindavoine (CIFRE Orange Labs) ;
- Antoine Plet (ENS Lyon) ;
- Valentina Popescu (allocation Région Rhône-Alpes) ;
- Serge Torres (ENS Lyon) ;

2 Autres

- Clément Pernet, MCF Grenoble 1, délégation CNRS puis Inria ;
- Benoît Libert, Chercheur CDD PALSE ;

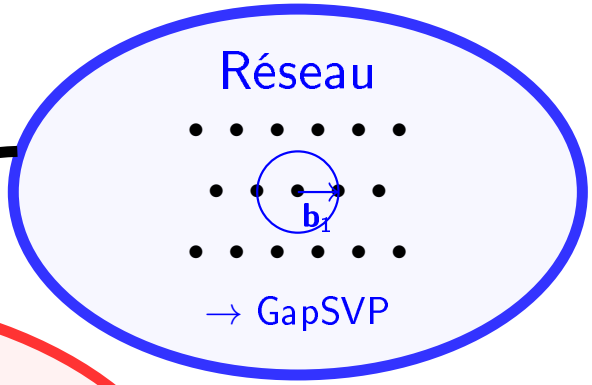
Quelques faits marquants

- Médaille de bronze du CNRS attribuée à Damien Stehlé en 2012 ;
- Médaille d'argent du CNRS attribuée à Jean-Michel Muller en 2013 ;
- ERC Starting Grant attribuée en 2013 à Damien Stehlé pour son projet *Lattices : Algorithms and Cryptography (LattAC)* ;
- Prix La Recherche 2013 pour les Sciences de l'Information attribué à Vincent Lefèvre, Nicolas Louvet, Jean-Michel Muller et notre collègue danois Peter Kornerup ;
- IEEE Working Group P1788 for standardization of interval arithmetic, présidé par Nathalie Revol ;
- Handbook of Floating-Point Arithmetic (Birkhäuser 2010 ; 572 pages) ;

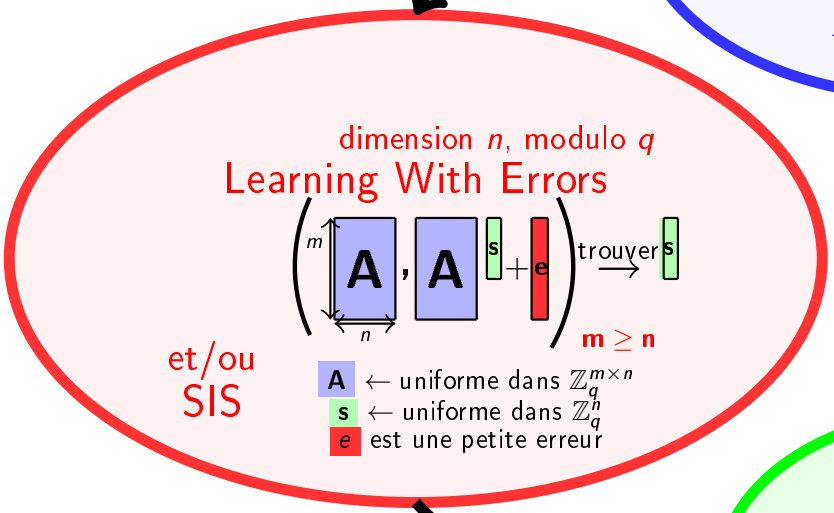


Quelques résultats — Réseaux et Cryptographie

1. Fondements



Première analyse en complexité
de l'algorithme BKZ (CRYPTO 2011)



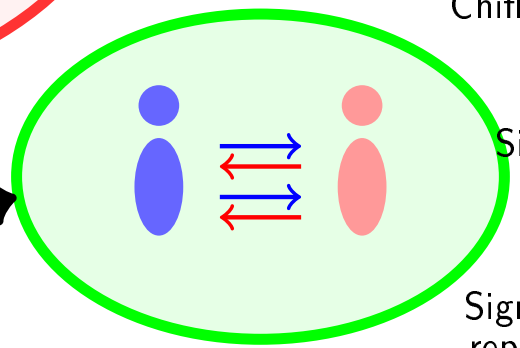
Preuve de la difficulté classique de LWE
pour tout module (STOC 2013)

Chiffrement basé
sur LWE

Signature reposant
sur SIS

Signature de groupe
reposant sur SIS et LWE

2. Constructions



Signatures de groupe plus efficaces
à base de réseaux euclidiens (Asiacrypt 2013)

Quelques résultats — Arithmétique virgule flottante

Algorithme de Kahan pour $x = ad - bc$ avec un FMA.

$\hat{w} \leftarrow \mathrm{RN}(bc)$
$e \leftarrow \mathrm{RN}(\hat{w} - bc)$
$\hat{f} \leftarrow \mathrm{RN}(ad - \hat{w})$
$\hat{x} \leftarrow \mathrm{RN}(\hat{f} + e)$
Return $\hat{x}$

($\mathrm{RN}(t) = t$ arrondi au nombre VF le + proche)

$$u = 2^{-p}$$

p : précision du système VF utilisé.

- approche classique (Higham, 2002) :

$$|\hat{x} - x| \leq H \cdot |x|$$

avec $H = 2u + u^2 + (u + u^2)u\frac{|bc|}{|x|}$
$\rightarrow$ précis tant que $u|bc| \not\gg |x|$

- en utilisant des propriétés de RN [a]

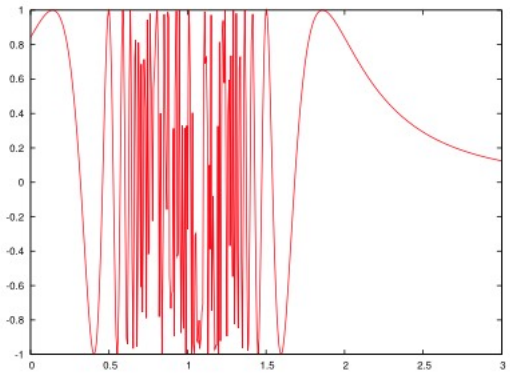
$$|\hat{x} - x| \leq 2u|x|$$

asymptotiquement optimal

$\rightarrow$ $\times, \div$ complexes.

a. Math. Comp., Oct. 2013

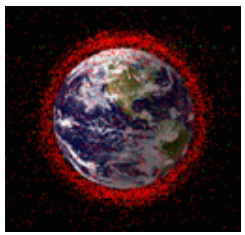
Quelques résultats — Approximations rigoureuses



$$J = \int_0^3 \sin\left(\frac{1}{(10^{-3} + (1-x)^2)^{3/2}}\right) dx$$

- Maple15 : 0.7499743685 ;
- PARI/GP : 0.7927730971479080755 ;
- Mathematica, Chebfun : pas de réponse. . .
- Chen, '06 : 0.7578918118
- $J = 0.749974368527$ [1,3]

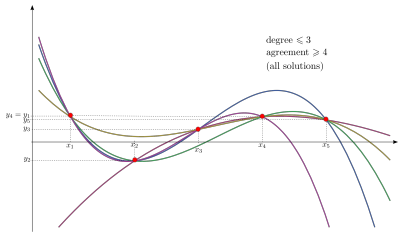
- thèse M. Joldes, 2011 ;
- Chebyshev interpolation polynomial-based tools for rigorous computing, ISSAC'10.

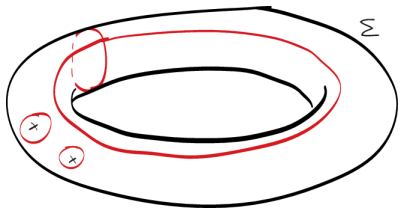


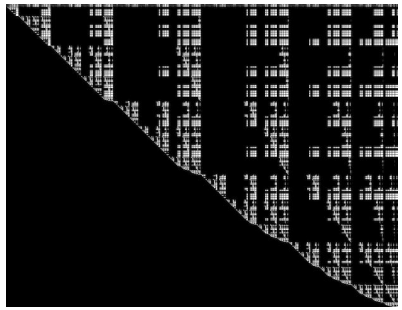
Collision de satellites (LAAS)

Quelques résultats – Complexité en calcul formel

- Interpolation de polynômes multivariés :
  - Nouveaux algorithmes, à base d'algèbre linéaire structurée
  - Application : meilleurs coûts connus pour le décodage en liste des codes de Reed-Solomon
- Équations différentielles linéaires : algorithmes exacts plus rapides pour l'intégration ;
- Résolution de systèmes polynomiaux : analyse de complexité des meilleurs algorithmes.[1]

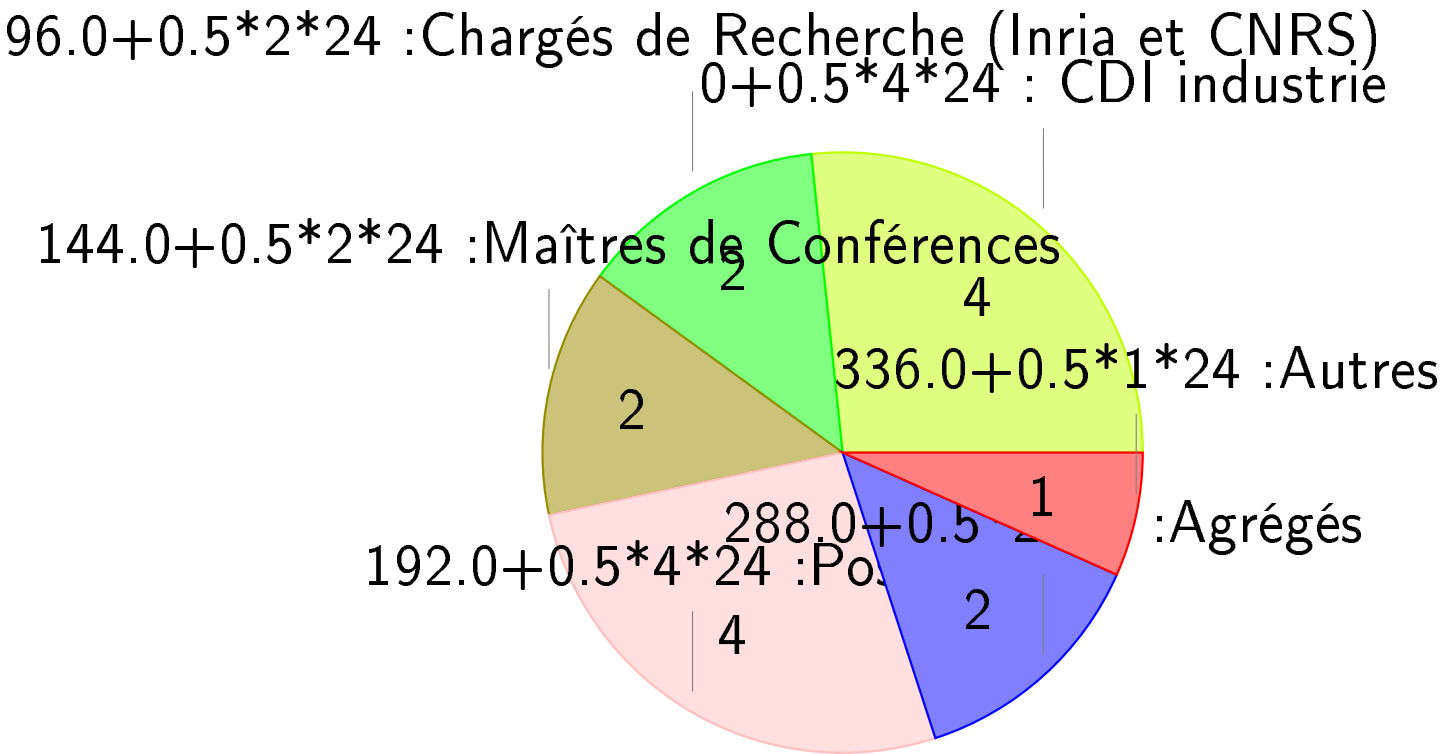






[1] J. of Symbolic Computation, 2014.

Devenir des doctorants de la période



Production scientifique (hors logiciels)

- livre «Handbook of Floating-Point Arithmetic» ;
- 41 articles dans des journaux internationaux ;
- 7 conférences invitées ;
- 84 communications à des conférences internationales ;
- 2 brevets.

Production logicielle

Amélioration du calcul : de la preuve de faisabilité (CRLibm) aux applications industrielles (FLIP).

- CRLibm : bibliothèque de fonctions élémentaires avec arrondi correct ;
- FloPoCo : générateur d'opérateurs arithmétiques pour FPGAs ;
- FLIP : bibliothèque virgule flottante pour processeurs entiers ;
- FPLLL : bibliothèque de réduction de réseaux euclidiens ;
- GFUN : bibliothèque de calcul formel pour la D-finitude ;
- contribution à LinBox : algèbre linéaire exacte ;
- contribution à la bibliothèque GNU MPFR (basée au Loria).

(peuvent être obtenus à `http://www.ens-lyon.fr/LIP/AriC/`).

Implication dans des projets

- Pilotage de trois projets ANR : EVA-Flo (2006–2010, N. Revol) ; TaMaDi (2010–2013, J.-M. Muller) et FastRelax (2014–2018, B. Salvy) ;
- participation aux projets TCHATER (2008–2011), LAREDA (2008–2011), HPAC (2011–2014), et MetaLibm (2013–2017) ;
- D. Stehlé est porteur de l'ERC Starting Grant LattAC (2013–2018) ;
- B. Libert est porteur du projet PALSE (Programme d'Avenir Lyon-St Etienne, 2014–2016) Towards practical enhanced asymmetric encryption schemes (500 k€ pour 2 ans).

Animation scientifique

- direction d'unités :
  - direction du LIP
  - co-direction du GDR IM (+ responsabilité pôle et GT)
- editorial boards : Journal of Symbolic Computation, Journal of Algebra, IEEE Transactions on Computers ;
- comités de programme et comités de pilotage : ACM-CCS, Analco, ANTS, AofA, IEEE ARITH, IEEE ASAP, Asiacrypt, CRYPTO, Eurocrypt, FPL, FPT, Indocrypt, ISSAC, PASCO, PKC, SCAN ;
- organisation d'événements : SCAN 2010 ; École de Printemps d'Informatique Théorique 2013 ; Journées Nationales du GDR IM 2013 ; ARITH'2015 ;
- présidence du comité de standardisation IEEE P1788 ;
- conseils scientifiques : INS2I, Cerfacs, ENS Lyon, ENSIIE Évry, Grenoble INP ;
- doctorants : conseil de labos et journée des doctorants.

Participation à l'évaluation de la recherche

- vice-présidence de la Commission d'Évaluation Inria ;
- présidence des comités d'évaluation Aeres du LIMOS (2011), du LIAFA (2012), de PPS (2012) ;
- participation aux comités du GREYC (2010) ; du LIRMM (2013) ;
- vice-présidence du CES (Comité d'Evaluation Scientifique) «Mathématiques et Informatique Théorique» de l'ANR en 2014 ;
- jury de recrutement CR2 Inria GRA (2009, 2013 et 2014) ;
- 8 comités de sélection MCF ;
- 6 comités de sélection PR ;
- participation jury PES Inria (2013), présidence jury PES CNRS/INS2I (2014).

Enseignement et études doctorales

- direction du département d'informatique de l'ENS Lyon ;
- responsabilité du Master d'Informatique à l'ENS Lyon ;
- responsabilité de la 2ème année «Ingénierie des Risques» du Master SAFIR (Lyon 1) ;
- forte implication dans des cours de Master à l'ENS Lyon et à l'ISFA (Univ. Lyon 1) ;
- participation au conseil de l'ED Infomaths.

Relations industrielles

- Compilation Expertise Center de STMicroelectronics :
  - Mediacom (Nano2012) ;
  - CIFRE (Jourdan-Lu),
  - projet Région Rhône-Alpes,
  - Nano2017 ;
- Kalray : financement thèse Brunie ;
- Orange Labs : CIFRE (Paindavoine) ;
- Bosch : conseil ;
- donations Intel, Altera (carte d'accélération FPGA).

Diffusion, vulgarisation

- N. Revol : une vingtaine d'interventions en lycées (encourager aux carrières scientifiques) + journées «maths en jeans» + Forum des jeunes mathématicien-ne-s + . . . ;
- N. Brisebarre : organisateur scientifique du cycle «Éclats de sciences», à la maison du livre, de l'image et du son de Villeurbanne.
  3 conférences/an ;
- 2 articles dans «La Recherche» : sept. 2013 (2 p.) et oct. 2014 (7 p.).


actualités
Mathématiques Cryptographie

Les systèmes d'équations bruités sont difficiles à résoudre

Une équipe franco-américaine vient d'apporter la première preuve de la difficulté d'un problème d'algèbre linéaire baptisé « LWE », très utilisé en cryptographie.

Damien Stehlé, professeur à l'école normale supérieure de Lyon, est spécialiste de cryptographie. Au laboratoire de l'informatique du parallélisme, il combine des méthodes issues de plusieurs branches des mathématiques pour étudier et concevoir des systèmes cryptographiques, dont la sécurité repose sur des problèmes difficiles portant sur les réseaux euclidiens.

Vous avez démontré qu'un problème baptisé « LWE » est difficile. Qu'est-ce que cela signifie ?

D.S. La difficulté intrinsèque, ou complexité, d'un problème, est la possibilité de trouver ou non un algorithme efficace – par exemple de temps d'exécution polynomial – qui résolve ce problème. Un problème est difficile s'il n'existe pas d'algorithme efficace, même très compliqué à décrire, le résolvant. Nous avons démontré que le problème LWE, abréviation de Learning with Errors (« apprendre avec des erreurs »), est difficile.

Quelle est la nature du problème LWE ?

D.S. Nous travaillons sur les réseaux euclidiens. Un réseau est une grille infinie et régulière de points en dimension quelconque, avec une origine. Nous savons que, pour de grandes dimensions, trouver par le calcul des vecteurs (non nuls) courts d'un réseau donné et même estimer la longueur des vecteurs les plus courts sont des problèmes difficiles. En 2005, Oded Regev, de l'Institut Courant de New York, a introduit le problème LWE qui est lié aux réseaux. Il consiste à résoudre un système d'équations modulaires auquel on ajoute du bruit (lire « Un problème pour la cryptographie », ci-dessus).

Comment avez-vous montré que c'est un problème difficile ?

D.S. Les travaux d'Oded Regev ont engendré un nombre considérable de développements utilisant LWE pour faire de la cryptographie. Ceux-ci ont élaboré des outils assez raffinés. En recyclant un certain nombre de ces outils et en les adaptant, nous avons montré, avec des collaborateurs américains et ma doctorante Adeline Langlois, que si LWE n'était pas difficile, alors le problème des vecteurs les plus courts de réseaux arbitraires ne le serait pas non plus (3). Comme nous savons que ce dernier est difficile, cela prouve que LWE l'est aussi. Nous avons fini par apporter une meilleure garantie de sécurité à toutes ces constructions cryptographiques fondées sur LWE, à l'aide des outils conçus pour construire ces protocoles.

Pourquoi ce problème est-il utilisé en cryptographie ?

D.S. LWE est particulièrement bien adapté à l'élaboration de protocoles de chiffrement, parce qu'il permet de construire des fonctions à la fois injectives et difficiles à inverser. L'injectivité est le fait qu'à tout élément dans l'ensemble de départ correspond au plus un élément dans celui d'arrivée. Elle assure que deux messages clairs distincts sont envoyés sur des messages chiffrés distincts (sinon, on ne pourrait pas déchiffrer !). La difficulté d'inversion assure la sécurité du chiffrement. De plus, ces fonctions que l'on construit à l'aide de LWE sont simples et rapides à calculer : il s'agit de faire des produits entre des matrices et des vecteurs. Comme cela prend très peu de temps à un ordinateur de faire ce type de calcul, cela permet la conception de protocoles de chiffrement efficaces.

LWE présente-t-il d'autres avantages ?

D.S. Oui. On s'est aussi progressivement aperçu que c'était le bon outil pour faire du chiffrement homomorphe. Ce type de chiffrement, encore théorique, excite beaucoup les cryptographes : il permet de réaliser des calculs directement sur des données chiffrées. On pourrait donc manipuler des données sans savoir ce qu'elles contiennent !

Propos recueillis par Philippe Pajot

sur le web

Cours de Chris Peikert, informaticien à Georgia Tech, sur le problème LWE, with Errors (en anglais).

Chronologie

XXIe siècle : l'Allemand Gauss met au point un algorithme qui permet de trouver des points proches de l'origine sur un réseau.

en dimension 2 (problème du plus court vecteur).

1982 : les Néerlandais Hendrik Lenstra Jr., Arjen Lenstra et le Hongrois László Lovász généralisent l'algorithme de Gauss à la dimension quelconque ; le Néerlandais Peter van Emde Boas montre que le calcul de la longueur des vecteurs courts d'un réseau est un problème difficile.

1996-1998 : Miklos Ajtai, d'IBM, montre la difficulté de trouver des vecteurs courts dans un réseau donné.

2005 : Oded Regev propose un problème lié aux réseaux, LWE, qui est bien adapté au chiffrement. Il prouve que si l'on s'astreint à des calculs quantiques, résoudre LWE permettrait de trouver des vecteurs courts dans un réseau.

2009 : Chris Peikert donne une preuve de difficulté classique de LWE si des grandes valeurs des modulos dans les équations linéaires sont utilisées.

2013 : Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev et Damien Stehlé prouvent la difficulté de LWE dans un cadre général.


Informatique

Des ordinateurs capables de calculer plus juste

Additionner 3 nombres quelconques sans erreur peut devenir mission impossible pour un ordinateur. Afin de pallier ce manque de fiabilité, les informaticiens inventent une nouvelle arithmétique. Indispensable pour construire un pont ou une aile d'avion.

par Sylvie Boldo, chargée de recherche Inria à Orsay, et Jean-Michel Muller, directeur de recherche CNRS au laboratoire de l'informatique du parallélisme à Lyon, l'un des lauréats du prix La Recherche 2013.

L'essentiel

› LES ORDINATEURS, ayant une précision finie, ne peuvent pas calculer de manière exacte.

› POUR AUGMENTER la précision des calculs et ne pas obtenir de résultats aberrants, il faut faire les calculs selon des règles d'arrondi spécifiques.

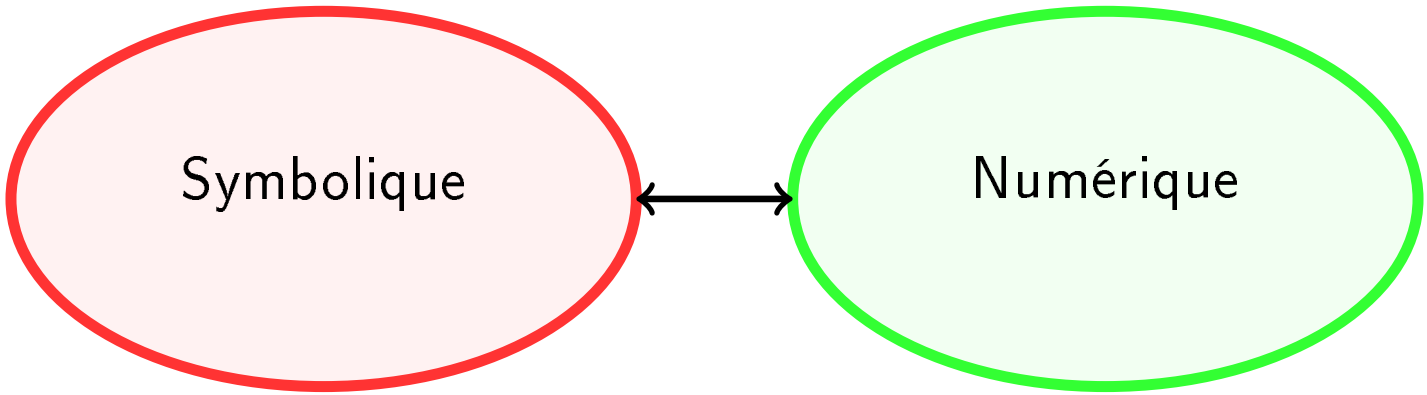
› CES RÈGLES permettent de construire des algorithmes qui compensent partiellement les erreurs commises.

Les ordinateurs ne savent pas calculer. Ou du moins, ils ne peuvent pas calculer exactement, sans erreurs. Dès lors, les résultats des calculs numériques effectués avec une machine ne peuvent être que des approximations. Et si ces approximations sont mal faites, ou s'il y a des erreurs de programmation, on aboutit parfois à des résultats étranges.

Ainsi, dans les années 1960, sur certains ordinateurs IBM 360, lorsqu'on attribuait dans un programme Fortran la valeur 14,0 divisé par 7,0 à la variable I, celle-ci devenait par la suite égale à 1. À la fin des années 1970, sur certains ordinateurs de la société Cray, on pouvait déclencher un dépassement de capacité en multipliant un nombre par un. Ou encore, l'algorithme de division de la première version du processeur Pentium de la société Intel lancé en 1994 était incorrect : la division de 8 391 667 par 12 582 905 donnait 0,666 869... au lieu de 0,666 910. On pourrait multiplier les exemples.

Le comportement étrange de ces systèmes anciens est certes anecdotique, mais il illustre la nécessité de concevoir pour les ordinateurs une arithmétique qui calcule bien... ou le moins mal possible. Sans comportement prévisible, pas de calculs numériques fiables, ce qui est problématique pour la recherche scientifique, mais aussi si l'on veut construire un pont solide ou une aile qui permette à un avion de voler.

Projet de recherche



Trois volets :

- Réseaux euclidiens : algorithmes et cryptologie ;
- Méthodes d'approximation efficaces ;
- Noyaux de calcul fiables et haute performance.

Projet de recherche – 1. Réseaux euclidiens : algorithmes et cryptologie

- algorithmes sur les réseaux : algorithmes rapides de réduction ; compromis entre temps de calcul et taille de la base calculée ; algorithmes de recherche du vecteur le plus court ;
- cryptographie à base de réseaux : renforcer les fondations ; améliorer les performances des primitives ; montrer que les réseaux permettent des primitives élaborées ;
- applications : équations diophantiennes, cryptanalyse de variantes de RSA.

Projet de recherche – 2. Méthodes d'approximation efficaces

- calcul formel pour construction d'approximations certifiées : approximations de solutions d'équations différentielles linéaires ; automatisation $\rightarrow$ fonctions «rares», adaptation rapide à un nouveau contexte (exigences, processeur, etc.) ;
- filtres certifiés, méthodes optimales d'arrondi de coefficients ;
- dilemme du fabricant de tables : optimisation/réécriture des algorithmes existants ; techniques diophantiennes pour attaquer la quadruple précision.

Projet de recherche – 3. Noyaux de calcul fiables et haute performance

- construction et analyse d'algorithmes symboliques ou numériques :
  - côté symbolique : jusqu'ici, algorithmes rapides pour matrices polynomiales et structurées, indépendamment. Exploiter les liens ;
  - côté numérique : nettoyer/revisiter des résultats classiques (bornes), estimation de conditionnements, comparaison de représentations en arithmétique d'intervalles (p.ex. mid-rad vs. bornes) ;
- virgule flottante symbolique : manipulation de nombres VF comme expressions en fonction de la base et de la précision ;
- multi-précision haute performance : précision d'au plus quelques centaines de bits.

Conclusion

- grande équipe (4 EC + 7 C + 2 ITA + 7 doc + 2 postdoc) ;
- spectre large, avec comme motto l'amélioration du calcul, en termes de performance, d'efficacité et de fiabilité ;
- de la théorie aux applications industrielles ;
- vrai souci de diffusion ;
- forte implication des permanents dans l'animation scientifique locale, nationale et internationale.