Application BASTRI

Fiches Equipes

CARAMBA (SR0755YR)

Cryptology, arithmetic : algebraic methods for better algorithms
CARAMBA (SR0730NR) CARAMBA

Statut: Décision signée

Responsable : Emmanuel Thome

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2023" : A1.1.2. Accélérateurs matériels (GPGPU, FPGA, DSP, etc.) , A4.3.1. Cryptographie à clé publique , A4.3.2. Cryptographie à clé secrète , A4.8. Technologies pour la protection de la vie privée , A6.2.7. HPC , A7.1. Algorithmique , A7.1.4. Algorithmique quantique , A8.4. Calcul formel, calcul algébrique , A8.5. Théorie des nombres , A8.10. Arithmétique des ordinateurs

Mots-clés de "B - Autres sciences et domaines d'application - 2023" : B8.5. Société intelligente , B9.5.1. Informatique , B9.5.2. Mathématiques , B9.10. Confidentialité, vie privée

Domaine : Algorithmique, programmation, logiciels et architectures
Thème : Algorithmique, calcul formel et cryptologie

Période : 01/09/2016 -> 31/12/2024
Dates d'évaluation : 19/03/2019 ,

Etablissement(s) de rattachement : U. DE LORRAINE, CNRS
Laboratoire(s) partenaire(s) : LORIA (UMR7503)

CRI : Centre Inria de l'Université de Lorraine
Localisation : Centre Inria de l'Université de Lorraine
Code structure Inria : 051104-1

Numéro RNSR : 201622054G
N° de structure Inria: SR0755YR

Présentation

Nos travaux visent le domaine général d'application de la cryptographie et de la cryptanalyse, d'un point de vue algorithmique. Nous étudions tous les aspects algorithmiques, du bagage mathématique fondamental jusqu'à l'implémentation optimisée dans un contexte de calcul à haute performances. Plusieurs types d'objets sont fréquemment utilisés dans nos travaux. Certains sont réellement omniprésents: entiers, corps finis, polynômes, nombres réels et complexes. Nous manipulons également des objets plus structurés comme des corps de nombres, des courbes algébriques, ou des systèmes polynomiaux. Dans tous les cas, notre travail est orienté vers le fait de rendre les calcul avec ces objets efficace.

Les objets mathématiques que nous manipulons sont de première importance pour les applications à la cryptologie, puisqu'ils constituent l'assise des primitives cryptographiques les plus répandues, tels le cryptosystème RSA ou l'échange de clés de Diffie--Hellman. Les deux aspects de la cryptologie (cryptographie et cryptanalyse) jouent un rôle central dans notre recherche. Les défis principaux sont d'une part l'évaluation de la sécurité offerte par les primitives cryptographiques, via l'étude des problèmes essentiels que sont la factorisation d'entiers et le problème du logarithme discret, et d'autre part le travail d'optimisation (mathématique, algorithmique, et aussi de plus bas niveau) rendant possible des implémentations à la fois efficaces et sûres.

Axes de recherche

Parmi les axes de recherche mis en avant par Caramba, deux sont guidés par les objets mathématiques les plus importants utilisés dans la cryptographie actuelle, deux autres sont plutôt guidés par le bagage technologique qui nous est nécessaire pour aborder les problèmes qui y ont trait.

- La famille étendue du crible algébrique. Un cadre algorithmique commun, le crible algébrique (NFS), s'applique à la fois à la factorisation d'entiers ainsi qu'au problème du logarithme discret sur les corps finis. Nous avons de nombreuses contributions algorithmiques dans ce contexte, et nous développons des logiciels qui les illustrent.

  Nous souhaitons améliorer l'état de l'art dans ce domaine par le

Contact

- **Responsable :** Emmanuel Thome
- **Tél :** +3.33.54.95.86.59
- **Secrétariat Tél :** 03.83.59.20.89

En savoir plus

- Site de l'équipe
- Site sur inria.fr
- Site du responsable
- Derniers Rapports d'Activité : 2016 , 2017 , 2018 , 2019 , 2020 , 2021 , 2022 , 2023

Documents sur la structure

- Intranet
- Privés

Décisions

- 11767 (01/09/2016) : création
- 14024 (16/12/2019) : prolongation
- 14983 (16/08/2021) : nomination responsable
- 15656 (26/09/2022) : nomination responsable
- 16661 (11/12/2023) : prolongation
- 17000 (26/04/2024) : prolongation

Localisation

- **Adresse postale :** Centre Inria de l'Université de Lorraine, 615 rue du Jardin Botanique, 54600 Villers-lès-Nancy France
- **Coordonnées GPS :** 48.666, 6.157

développement de nouveaux algorithmes, par l'amélioration de la performance des logiciels. Notre travail est naturellement assorti de démonstrations pratique de la portée des avancées obtenues, sous la forme de calculs record.

- Les courbes algébriques et leurs jacobiennes. Nous développons des algorithmes et des logiciels pour calculer les propriétés essentielles des courbes algébriques pour la cryptologie, rendant possible *in fine* leur déploiement le plus large possible.

  Un des défis que nous abordons est celui du comptage de points. Dans une perspective plus vaste, nous étudions également le lien entre les variétés abéliennes sur des corps finis, et les variétés abéliennes principalement polarisées sur des corps de caractéristique nulle, et leur anneau d'endomorphismes. En particulier, nous travaillons à rendre ce lien explicite d'un point de vue pratique. Nous étudions également plusieurs approches pour attaquer au problème du logarithme discret sur les jacobiennes de courbes algébriques.

- L'arithmétique. Notre travail repose de façon essentielle sur l'efficacité des opérations arithmétiques sous-jacentes, qu'il s'agisse d'opérations sur des objets de petite ou de grande tailles. Nous travaillons à l'amélioration des algorithmes et des implémentations pour les calculs qui sont en lien avec nos domaines d'application.

- Les systèmes polynomiaux. De façon naturelle dans le contexte des courbes algébriques, mais également dans les problèmes liés au crible algébriques, de nombreux problèmes importants peuvent être exprimés dans le cadre des systèmes polynomiaux. Les systèmes ainsi obtenus ont des spécificités structurelles fortes, en lien avec le problème d'origine. Nous développons des algorithme et des outils qui, lorsque c'est possible, tirent parti de ces spécificités structurelles.

Relations industrielles et internationales

University of California San Diego, Aarhus University, University of Calgary. Nos travaux sont repris par les organismes gouvernementaux émettant des recommandations cryptographiques (ANSSI, BSI, NIST).