Application BASTRI

Fiches Equipes

CARAMEL (SR0449PR)

Cryptologie, Arithmétique : Matériel et Logiciel
CARAMEL (SR0435BR) CARAMEL CARAMBA (SR0730NR)

Statut: Terminée

Responsable : Pierrick Gaudry

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2024" : *Aucun mot-clé.*

Mots-clés de "B - Autres sciences et domaines d'application - 2024" : *Aucun mot-clé.*

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

Période : 01/01/2011 -> 31/12/2015
Dates d'évaluation : 24/03/2011 , 17/03/2015

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

CRI : Centre Inria de l'Université de Lorraine
Localisation : Bâtiment Ada Lovelace - Centre Inria de l'Université de Lorraine
Code structure Inria : 051090-1

Numéro RNSR : 201020971F
N° de structure Inria: SR0449PR

Présentation

Un mot-clef général qui pourrait résumer la plupart de nos objectifs de recherche est *arithmétique*. En effet, dans la proposition CARAMEL, le but est de repousser les possibilités pour le calcul efficace avec des objets ayant une nature arithmétique. Ceci inclut les nombres entiers, les nombres réels et complexes, les polynômes, les corps finis, et *last but not least* les courbes algébriques.
Nos domaines d'application principaux sont la cryptographie à clef publique et les systèmes de calcul formel. En ce qui concerne la cryptographie, nous nous concentrons sur l'étude des primitives s'appuyant sur le problème de la factorisation ou du logarithme discret dans les corps finis ou les (jacobiennes de) courbes algébriques. À la fois les aspects constructifs et destructifs sont étudiés. Pour les applications au calcul formel, nous nous intéressons principalement aux briques de bases de l'arithmétique que sont les entiers, les nombres flottants, les polynômes et les corps finis. De plus, des fonctionnalités plus évoluées telles que la factorisation ou le calcul de log discret sont en général souhaitées dans les systèmes de calcul formel.
Comme nous développons notre expertise à tous les niveaux, depuis l'implantation matérielle ou logicielle de briques de base au plus bas niveau jusqu'à des algorithmes haut-niveau compliqués tels que la factorisation ou le comptage de points, nous avons remarqué qu'il est souvent trop naïf de vouloir les séparer: nous pensons que les interactions entre les algorithmes de bas niveau et de haut niveau sont de la plus grande importance pour les applications arithmétiques, et peuvent des améliorations substantielles qui n'auraient pas pu voir le jour avec une vision compartimentée.

Axes de recherche

Nous avons trois directions principales de recherche:

- Factorisation et calcul de logarithme discret dans les corps finis
  Nous sommes particulièrement intéressés par l'algorithme du crible algébrique (ou *number field sieve*, NFS), qui est le meilleur algorithme connu pour factoriser des grands entiers comme les clefs RSA et pour résoudre le problème du logarithme discret dans les corps finis premiers. Un algorithme cousin, le crible de corps de fonctions (FFS) est le meilleur algorithme connu pour calculer des logarithmes discrets dans les corps finis de petite caractéristique. Dans tous ces cas, nous comptons améliorer les algorithmes existants, avec un point de vue pratique, afin de pouvoir établir de nouveaux records.
- Courbes algébriques et cryptographie
  sur ce sujet, nous nous intéressons principalement à deux domaines: la cryptographie utilisant les courbes de genre 2 et l'arithmétique des

Contact

- **Responsable :** Pierrick Gaudry
- **Tél :** 03.83.59.20.62
- **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 :

Documents sur la structure

- Intranet
- Privés

Décisions

- 7156 (13/04/2011) : création
- 8337 (19/01/2012) : prolongation
- 11408 (11/01/2016) : fermeture

Localisation

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

couplages, dans les deux cas d'un point de vue constructif. Pour les courbes de genre 2, a outil algorithmique que nous souhaitons développer est la calcul d'isogénies explicites; cela fournira un outil algorithmique pour divers calculs liés à la cryptographie tels que le comptage de points en grande caractéristique, la construction par multiplication complexe ou le calcul d'anneaux d'endomorphismes. En ce qui concerne les couplages, notre objectif est d'optimiser les calculs, en particulier en matériel ou en environnement contraint. Nous développerons des outils automatiques pour aider à choisir la courbe (hyper-)elliptique la plus adaptée et générer du matériel efficace pour un niveau de sécurité et un ensemble de contraintes donnés.

- Arithmétique
  L'arithmétique des entiers, des corps finis et des polynômes est omniprésente dans nos recherches. Nous la considérons pas seulement comme un outil pour d'autres algorithmes, mais bien comme un thème de recherches en soi. Nous nous intéressons aux avancées algorithmiques, en particulier pour les très grandes tailles pour lesquelles les algorithmes asymptotiquement rapides deviennent pertinents en pratique. Nous gardons aussi une importante activité d'implantation, à la fois en logiciel et en matériel.

Relations industrielles et internationales

- Collaboration à long terme avec Richard Brent (Canberra, Australia) sur l'arithmétique efficace.
- Collaboration à long terme avec Eric Schost (London, Ontario, Canada) sur le comptage de points en genre 2.
- Collaboration avec Arjen Lenstra et Thorsten Kleinjung (Lausanne, Switzerland) sur la factorisation d'entiers
- Co-encadrement d'un doctorant avec Tanja Lange (Eindhoven, Netherlands)
- Collaboration avec Francisco Rodríguez-Henríquez (Mexico) sur les calculs de couplages