Application BASTRI

Fiches Equipes

CACAO (SR0058SR)

Courbes, Algèbre, Calculs, Arithmétique des Ordinateurs
SPACES (SR0300IR) CACAO CARAMEL (SR0435BR)

Statut: Terminée

Responsable : Guillaume Hanrot

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2023" : *Aucun mot-clé.*

Mots-clés de "B - Autres sciences et domaines d'application - 2023" : *Aucun mot-clé.*

Domaine : Algorithmique, programmation, logiciels et architectures
Thème : Algorithmique, calcul certifié et cryptographie

Période : 09/10/2006 -> 31/12/2009
Dates d'évaluation :

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 : 051067-0

Numéro RNSR : 200618304Z
N° de structure Inria: SR0058SR

Présentation

L'équipe-projet CACAO a deux objectifs convergents :

- L'étude de l'arithmétique des courbes de petit genre, avec en particulier à l'esprit les applications à la cryptologie,
- L'amélioration de l'efficacité et de la fiabilité des arithmétiques en un sens large.

Ces deux objectifs interagissent fortement. L'arithmétique est évidemment au cœur de l'optimisation des algorithmes sur les courbes, par exemple via l'arithmétique des courbes elles-mêmes. À contrario, les courbes peuvent constituer un outil pour des problèmes arithmétiques comme la factorisation des entiers. Pour atteindre ces objectifs, l'équipe-projet est structurée selon trois axes : courbes, arithmétique et algèbre linéaire. Le dernier constitue un outil important pour nos deux objectifs principaux, suffisamment central pour que nous ayons besoin de développer nos propres outils et logiciels, conformes à nos besoins.

Axes de recherche

- Courbes algébriques : l'objectif principal est l'étude de courbes de petit genre sur les corps finis (corps de base F_{p^n} pour divers types de valeurs (p, n)), c'est-à-dire principalement de savoir calculer efficacement dans la jacobienne de la courbe, de savoir vérifier que la variété convient pour la cryptographie (calcul du plus grand nombre premier divisant le cardinal), et d'étudier le calcul du logarithme discret dans ces structures. Les applications vont de la théorie algorithmique des nombres (factorisation) à la cryptographie (alternative à RSA).
- Arithmétique : nous étudions et concevons des algorithmes travaillant sur les entiers en multiprécision, les flottants (précision simple et multiple), les nombres p-adiques, les corps finis. Pour des structures aussi simples, nous ne nous attendons pas à trouver des algorithmes asymptotiquement meilleurs que ceux connus ; toutefois, comme ce sont nos objets "de base", toute accélération est pertinente, même un simple facteur 2 !
- La résolution de grands systèmes linéaires est un point-clé pour la factorisation et le logarithme discret, qu'il convient d'étudier dans le cadre des applications à la cryptologie. De même, la réduction des réseaux est un cadre central pour de nouvelles idées apparues récemment pour des questions d'arithmétique des ordinateurs ou de problèmes de logarithme discret. Nous étudions principalement les grands systèmes linéaires creux sur un corps fini, et diverses applications de la réduction des réseaux, bien que nous n'étudiions pas cette dernière en elle-même.

Contact

- **Responsable :** Guillaume Hanrot
- **Tél :** 03.83.59.20.62
- **Secrétariat Tél :** 03.83.59.30.09

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

- 5159 (24/10/2006) : création
- 6835 (16/07/2009) : cessation du responsable
- 6836 (16/07/2009) : nomination responsable
- 7015 (16/12/2009) : fermeture

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

L'équipe-projet a également une activité importante de développement logiciel, à la fois comme terrain d'expérience, comme résultat à part entière, ou encore comme validation de résultats obtenus par ailleurs. Une liste à jour des logiciels distribués par l'équipe-projet est accessible.

Relations industrielles et internationales

- Stockholm / GMP. Depuis 2000, l'équipe-projet a fait plusieurs contributions à la bibliothèque GMP, développée par Torbjörn Granlund (Swox Company, Stockholm, Suède).
- Canberra / Australian National University. Depuis 2000, nous entretenons une collaboration étroite avec R. Brent. En particulier, un livre décrivant l'état de l'art en arithmétique multi-précision (entiers, entiers modulo n, nombres flottants) est en cours de rédaction.
- Berlin (TU). Nous sommes partie prenante d'un PAI (programme d'action intégrée) avec l'équipe de Florian Hess à la TU Berlin, portant sur l'étude de diverses techniques pour attaquer le problème du logarithme discret sur les courbes elliptiques.