Application BASTRI
Fiches Equipes

TANC (SR0144PR)

Théorie algorithmique des nombres pour la cryptologie
TANC GRACE (SR0511VR)

Statut: Terminée

Responsable : Daniel Augot (Par intérim)

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 certifié et cryptographie

Période : 10/03/2003 -> 31/12/2011
Dates d'évaluation : 24/03/2011

Etablissement(s) de rattachement : EC. POLYTECHNIQUE, CNRS
Laboratoire(s) partenaire(s) : LIX (UMR7161)

CRI : Centre Inria de Saclay
Localisation : Laboratoire d'Informatique de l'Ecole polytechnique
Code structure Inria : 111032-0

Numéro RNSR : 200318378T
N° de structure Inria: SR0144PR

Présentation

L'équipe-projet TANC a pour but de promouvoir l'étude, la programmation et l'utilisation de cryptosystèmes asymétriques robustes et vérifiables basés sur la théorie algorithmique des nombres.

Des idées tirées de l'arithmétique des nombres ont donné naissance à des primitives cryptographiques robustes, qui sont maintenant prêtes à être utilisées dans de nombreux contextes où la sécurité des transactions ou des données est nécessaire. Au-delà des besoins de confidentialité présents dans les réseaux de toute nature, le marché est prêt à s'ouvrir à la signature électronique.

Certains problèmes réputés difficiles ont été convertis en des primitives de chiffrement. Celles-ci sont utilisées comme briques de base dans des algorithmes plus complexes résistant à différents scénarios d'attaque. A leur tour, ces algorithmes sont intégrés à des protocoles qui sont alors implantés. Notre activité se situe au début de la chaîne : nous nous intéressons aux problèmes sur lesquels reposent les cryptosystèmes modernes, à leur nature bien souvent mathématique, à la construction efficace et robuste des objets utilisés.

TANC est une équipe-projet géographiquement située au Laboratoire d'Informatique de l'Ecole polytechnique.

Axes de recherche

- Théorie algorithmique arithmétique Nous nous intéressons aux preuves de primalité à base de courbes elliptiques (F. Morain est le leader du sujet), à la factorisation des nombres entiers, et au problème du logarithme discret dans les corps finis. Ces problèmes sont à la base de la théorie algorithmique arithmétique et des cryptosystèmes qui s'appuient dessus.
- Multiplication complexe La théorie de la multiplication complexe est un point de convergence de l'algèbre, de l'analyse complexe et de la géométrie algébrique. Ses applications vont de la preuve de primalité à la construction efficace de cryptosystèmes elliptiques.
- Courbes algébriques sur les corps finis Les problèmes algorithmiques auxquels nous nous attaquons sont le calcul efficace de la loi de groupe dans les jacobiennes de courbes, le calcul de la cardinalité et plus généralement de l'anneau d'endomorphismes de ces groupes, et finalement le problème du logarithme discret. Ces divers points sont cruciaux pour la construction de cryptosystèmes robustes à base de courbes.

Contact

- **Responsable :** Daniel Augot
- **Tél :** 01.69.33.40.51
- **Secrétariat Tél :** 01.69.33.40.73

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

- 3788 (05/03/2003) : création
- 5787 (11/09/2007) : prolongation
- 6078 (19/02/2008) : changement de rattachement
- 6357 (18/09/2008) : nomination responsable
- 7426 (06/09/2010) : nomination responsable
- 7616 (03/01/2011) : prolongation
- 7777 (07/03/2011) : nomination responsable
- 8404 (03/01/2012) : fermeture
- 8337 (19/01/2012) : prolongation

Localisation

- **Adresse postale :** LIX 1 rue Honoré d'Estienne d'Orves Bâtiment Alan Turing Campus de l'École Polytechnique 91120 Palaiseau France
- **Coordonnées GPS :** 48.713208, 2.209024

- Construction de cryptosystèmes robustes Nous comptons mettre en oeuvre les points précédents de manière à construire efficacement des cryptosystèmes robustes, aussi bien pour le système RSA que pour les courbes elliptiques. Autant que faire se peut, on s'attache à donner des preuves ou des certificats des propriétés arithmétiques importantes.

Relations industrielles et internationales