Proposition de recherche doctorale

Solving Polynomial Systems over Finite Fields: Algorithms, Implementations and Applications

Mots clés :

- **Directeur de thèse** : Jean-Charles Faugère
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire d'informatique de Paris 6
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Polynomial systems, as generalization of linear systems, have been widely used in various scientific and engineering fields, and polynomial system solving is one of the major interests of the study of Symbolic Computations, an interdisciplinary area of Computer Science and Mathematics. Furthermore, solving polynomial systems over finite fields may lead to many potential applications to problems from Coding Theory and Cryptography, which are mainly embedded in the setting of finite fields, and therefore is of particular importance. This thesis aims at a relatively comprehensive study on the subject of solving polynomial systems over finite fields, including algorithms designing, program implementation, and its applications to practical problems. The two main methods for polynomial system solving, namely Gröbner bases and triangular sets, are both considered. Several algorithms are designed and implemented to perform the change of ordering of Gröbner bases and the squarefree decomposition of triangular sets over finite fields. The applications of these solving methods to Biology and Coding Theory are also investigated.