Proposition de recherche doctorale

Cryptanalyse Algébrique: Outils et 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)

Ce sujet de thèse se situe dans le domaine de la protection de l'information; les deux thèmes de recherche concernés sont la cryptographie et le calcul scientifique certifié. Dans le but d'évaluer la sécurité de nouveaux schémas, il convient de développer des méthodes de cryptanalyse puissantes et efficaces. L'objet de la thèse est d'évaluer la sécurité de primitives cryptographiques par des méthodes algébriques (le principal outil est le calcul des bases de Gröbner). L'idée est de modéliser une primitive cryptographique à l'aide d'un système d'équations algébriques. Le système est construit de telle sorte à avoir une correspondance entre les solutions du système et une information secrète sur la primitive en question (clef secrète, message en clair, ...). Une fois cette mise en équation réalisée, il s'agit de résoudre le système algébrique et d'évaluer la complexité théorique et pratique des calculs. La méthode la plus adaptée pour ce type de problème est l'utilisation d'algorithmes rapides pour le calcul de bases de Gröbner. Cette méthode, dite de cryptanalyse algébrique, est apparue il y a quelques années seulement, et constitue donc une nouvelle méthode d'investigation des primitives cryptographiques. Le candidat devra appliquer et développer cette technique d'analyse algébrique dans le contexte des schémas issus de la cryptographie à clef secrète (schémas par blocs comme AES, schémas à flot comme E0). Il pourra aussi s'intéresser à d'autres primitives (comme Sha1). Le sujet est motivé par le fait que l'analyse algébrique, dans ces contextes, n'est pas bien maîtrisée aujourd'hui, tant sur le plan pratique que théorique.

Résumé du projet de recherche (Langue 2)

La cryptanalyse algébrique est sujet important dans le monde de la Cryptologie sur le plan international. L'enjeu est de repousser les limites et d'appliquer ces techniques a de nouveaux cryptosystèmes.