Proposition de recherche doctorale

La cryptanalyse différentielle et ses généralisations

Mots clés :

- **Directeur de thèse** : pascale CHARPIN
- **Co-encadrant(s)** :
- **Unité de recherche** : INRIA-Paris
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Le travail de recherche présenté dans cette thèse se place en cryptographie symétrique. En particulier, nous nous intéressons à l'analyse et au design des systèmes de chiffrement par blocs. Le début des années 1990 a vu l'avènement d'un certain nombre d'attaques statistiques pour les système de chiffrements par bloc. Durant cette thèse, je me suis intéressée aux généralisations de la cryptanalyse différentielle. La première partie de ma thèse est dédiée à la présentation d'un certain nombre d'attaques statistiques sur les systèmes de chiffrement par bloc. Nous proposons une étude générale qui permet de calculer la complexité en donnée et la probabilité de succès d'un certain nombre d'attaques statistiques des systèmes de chiffrements par bloc. Le fil conducteur de cette partie reste l'analyse de la cryptanalyse différentielle et de ses généralisations. Des travaux plus récents, nous ont permis en utilisant plusieurs différentielles de généraliser la cryptanalyse différentielle et la cryptanalyse différentielle tronquée. Dans ces travaux nous étudions la complexité d'une attaque différentielle multiple. La seconde partie de cette thèse est dédiée à l'étude des critères sur les boîtes-S des systèmes de chiffrement par bloc qui permettent de prémunir les systèmes de chiffrement parbloc contre des attaques différentielles. A la suite d'une étude approfondie sur les boîtes-S de ces systèmes de chiffrement par bloc, nous avons introduit un nouveau critère, plus précis que l'uniformité différentielle, nous permettant de mesurer la vulnérabilité des boîtes-S aux attaques différentielles. Ainsi, avec Anne Canteaut et Pascale Charpin, nous avons introduit la notion de spectre différentiel et étudié le spectre différentiel de différentes classes de monômes.