Proposition de recherche doctorale

Analyse du décodage générique en métrique de Hamming et étude des cryptosystèmes basés sur la métrique rang

Mots clés :

- **Directeur de thèse** : nicolas SENDRIER
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire inconnu!
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Contexte et enjeux. La cryptographie à clé publique est l'un des outils clé pour assurer la confidentialité et l'intégrité des données. La sécurité de la plupart des systèmes déployés aujourd'hui pour l'échange de clé et la signature numérique repose sur hypothèses de théorie des nombres, à savoir la difficulté de la factorisation d'entiers et celle du logarithme discret. Ce manque de diversité dans les hypothèses de sécurité est un risque qui est mis en évidence par la menace du calcul quantique (Shor a montré en 1994 que la factorisation d'entiers et le logarithme discret sont facile sur un ordinateur quantique). La recherche sur des cryptosystèmes basés sur d'autres hypothèses s'intensifie, et la communauté de « cryptographie post-quantique » s'efforce de proposer des schémas cryptographique reposant sur des problèmes qui demeurent difficiles contre un ordinateur quantique. Le but n'est pas de remplacer la théorie des nombres par technologie unique, avec le même risque que précédemment, mais de proposer, étudier, et finalement normaliser un ensemble de systèmes reposant sur des problèmes algorithmiques durs et variés. Les techniques les plus prometteuses aujourd'hui sont la cryptographie basée sur les codes, sur les réseaux, sur le hachage, et la cryptographie multivariée. Projet de thèse. Le projet de thèse s'intéresse à la cryptographie basée sur le codes. Nous proposons d'explorer deux voies de recherche : 1- Analyse des algorithmes de décodage générique. La meilleure attaque contre la plupart des cryptosystèmes basés sur les codes et en particulier contre le système de chiffrement de McEliece, consiste à décoder dans un code lineaire binaire (d'apparence) aléatoire. Ces techniques de décodage ont un coût exponentiel. Ces dernières années de nombreuses améliorations ont été proposées pour diminuer la valeur de l'exposant (la dernière amélioration date du printemps 2015). Des travaux préliminaires indiquent, que dans le cas où l'erreur est de poids sous-linéaire, cette amélioration devient asymptotiquement négligeable. Ce premier axe consistera à poursuivre l'analyse asymptotique de ces algorithmes pour mieux comprendre leur comportement. Cette analyse est rendue complexe par un grand nombre de paramètres à optimiser qui ne permet pas l'obtention de formules closes. Pour chaque taille de système il faut résoudre un problème d'optimisation pour obtenir le meilleur réglage de l'algorithme et sa complexité. En particulier, nous envisageons de concevoir et de mettre à la disposition de la communauté un outil logiciel permettant d'évaluer précisément les coûts algorithmiques des divers algorithmes. Un tel outil n'existe pas et serait d'une grande utilité pour les concepteurs de schémas cryptographiques basés sur les codes. 2- Étude des codes en métrique rang. Les cryptosystèmes basés sur les codes utilisent le plus souvent la métrique de Hamming : le décodage consiste à trouver le mot de code le plus proche d'un mot donné pour la métrique de Hamming. Si l'on remplace les mots par des matrices, le code devient un espace vectoriel de matrices, et on parle de code matriciel. L'espace correspondant peut être muni de la métrique rang : la distance entre deux matrices est le rang de leur différence, une erreur de petit poids est une matrice de petit rang (mais pas de petit poids de Hamming). Des cryptosystèmes peuvent être définis comme pour la métrique de Hamming. Des travaux récents ont introduit les codes LRPC (Low Rank Parity Check) et ont montré que cette approche était digne d'intérêt, en particulier pour contruire des schémas de signature numérique. Ce volet de l'étude est plus prospectif, et de nombreuses voies sont possibles. Nous étudierons en particulier la possibilité d'adapter les algorithmes de décodage générique en métrique de Hamming à la métrique rang.

Résumé du projet de recherche (Langue 2)

Sécuriser les données et les communications après l'apparition de l'ordinateur quantique