Proposition de recherche doctorale

Théorie des corps finis et cryptographie symétrique

Mots clés :

- **Directeur de thèse** : anne CANTEAUT
- **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)

Les algorithmes à clef secrète (également appelés symétriques) sont essentiels en cryptographie car ils sont les seuls à pouvoir assurer la confidentialité des données avec les performances requises par la plupart des applications (en termes de vitesse, de taille de circuit mettant en oeuvre l'algorithme...). Ces contraintes d'implémentation sont donc au coeur même de leur conception. Pour cette raison, cette dernière ne repose pas sur des problèmes mathématiques bien connus, contrairement aux algorithmes à clef publique, comme le RSA ou les chiffrements à base de courbe elliptique. La conception des algorithmes symétriques n'est pourtant pas moins mathématisée. Au lieu de reposer sur la théorie des nombres comme beaucoup de systèmes à clef publique, elle tire parti essentiellement de résultats relevant de la théorie des corps finis. En effet, afin de résister aux grandes familles d'attaques connues, les fonctions impliquées dans ces chiffrements doivent satisfaire certains critères. Les systèmes cryptographiques opérant naturellement sur des données binaires, ces fonctions sont des fonctions de F_2^n dans F_2^m , et les critères de sécurité sont par exemple liés au degré de leurs coordonnées (représentés par des polynômes multivariés), à leurs différentielles... La nécessité de minimiser les coûts de mise en oeuvre imposant le choix de fonctions qui garantissent une résistance optimale aux attaques, la construction de ces fonctions (et leur optimalité) met généralement en jeu une structure algébrique forte, reposant typiquement sur l'identification de F_2^n avec le corps F_{2^n}. Ainsi, la seule fonction non-linéaire utilisée dans le standard de chiffrement symétrique par bloc AES est une fonction de F_2^8 dans F_2^8 qui, à une transformation affine près, correspond à « l'inversion » dans le corps fini à 2^8 éléments. Il s'agit en effet de la seule permutation connue (à équivalence près) qui résiste de manière optimale aux cryptanalyses différentielle et linéaire. Toutefois, le lien entre théorie des corps finis et cryptographie symétrique n'a été exploité jusqu'à présent que pour construire des objets optimaux. L'objet de cette thèse est d'explorer plus en détail ces liens et de tenter de les exploiter plus systématiquement, notamment dans deux directions : –* l'utilisation de la structure de corps fini pour la cryptanalyse, c'est-à-dire pour l'attaque de systèmes cryptographiques symétriques ; –* l'utilisation de travaux récents dans le domaine de la cryptographie pour aborder des problèmes relevant classiquement de la théorie des corps finis, par exemple pour le calcul de certaines sommes de Weil.

Résumé du projet de recherche (Langue 2)

{{{Exploiter la structure de corps fini pour la cryptanalyse}}} La question générale sous-jacente est ici de se demander si l'existence d'une structure algébrique forte sur le corps F_{2^n} peut introduire des faiblesses dans le système cryptographique et être exploitée par un attaquant. Une première piste à explorer est l'analyse de sécurité de certains chiffrements à flot à base de LFSR. Un LFSR est simplement un dispositif communément utilisé dans les générateurs pseudo-aléatoires cryptographiques pour produire une suite binaire régie par une récurrence linéaire. Lorsque le polynôme caractéristique de la suite est primitif, ce qui est le cas dans les applications, l'état interne de ce générateur est un mot de F_2^n qui évolue en fonction du temps t suivant x_t = x_0 a^t si les mots de n bits sont identifiés à des éléments du corps F_{2^n}, a étant un élément primitif du corps. La suite pseudo-aléatoire est alors obtenue en appliquant à chaque instant à certains bits de cet état interne une fonction non-linéaire f de F_2^m dans F2, m <= n. Les travaux récents de Rønjom et Helleseth ont montré sur certains exemples que l'expression de la fonction f comme une fonction de F_{2^n} dans F_2 pouvait revéler certaines faiblesses. Par exemple, si f peut être représentée comme Trace d'un monôme, alors il est possible d'effectuer un changement de racine primitive dans le corps, et de construire un générateur équivalent entièrement linéaire. L'idée est donc de généraliser ces travaux dans deux voies : la première consiste à utiliser cette idée pour des fonctions f dont la représentation sous forme de trace d'un polynôme univarié comporte plusieurs monômes. Dans ce cas, on peut composer f avec une fonction puissance, obtenir un générateur équivalent et tenter d'appliquer d'autres types d'attaques sur ce dernier. Ainsi, les attaques par corrélation rapides exploiteront l'existence d'un exposant s pour lequel la fonction f(P) a une faible non-linéarité, notion proche de celle de fonction hyperbent introduite par Gong et Youssef (sans que celle-ci ait été motivée par une application cryptographique). Les exposants s qui ne sont pas premiers avec (2^n-1) jouent probablement un rôle particulier dans ce contexte. L'exploitation de cette même idée mais pour d'autres attaques, comme les attaques algébriques, les attaques algébriques rapides et certaines attaques par distingueur, pourra être envisagée. Un second problème à aborder dans ce contexte, issu directement de la problématique cryptographique, est lié au fait que dans les applications, le nombre de bits m utilisés en entrée de la fonction f est très significativement inférieur au nombre de bits de l'état interne. Typiquement, n est de l'ordre de quelques centaines, alors que m sera entre 10 et 20. La fonction f peut donc être exprimée comme une fonction sur F_2^n , pour laquelle la plupart des valeurs d'entrées n'influence pas la valeur de f. Toutefois, déterminer l'expression de f sur F_{2^n} dans ce cas semble être un problème ardu dans la mesure où le degré d'extension n, égal à plusieurs centaines, rend tout calcul exhaustif hors de portée. {{{Exploiter des résultats de cryptanalyse dans le calcul de sommes de Weil}}} De nombreux travaux dans la communauté « corps finis » ont porté depuis 40 ans sur le calcul de certaines sommes de Weil, notamment celles dont l'argument est un binôme. Ces sommes de caractères apparaissent notamment en télécommunications car elles correspondent aux valeurs de la corrélation mutuelle entre une suite périodique d'éléments de F_p et sa décimée par s. Elles ont également été utilisées en cryptographie symétrique pour calculer la non-linéarité des fonctions monômes, par exemple la non-linéarité et les propriétés différentielles de la fonction inversion utilisée dans le standard AES proviennent directement de l'évaluation de sommes de Kloosterman. Une question ouverte depuis plus de 40 ans est de déterminer les valeurs de q et s pour lesquelles la somme de Weil correspondant prend exactement trois valeurs quand la fonction lin'eaire varie. Un progrès significatif a été accompli récemment par Katz qui a démontré la conjecture de Helleseth de 1976 selon laquelle la somme de Weil ne peut jamais prendre exactement trois valeurs quand q est de la forme p^{2^k} pour les caractéristiques 2 et 3 (la conjecture restant à prouver en caractéristique supérieure). De nombreux problèmes sur ce sujet restent ouverts, en particulier la caractérisation des exposants s pour lesquels la somme de Weil prend trois valeurs, ou la conjecture selon laquelle cette somme s'annule toujours en un point quand s est congru à 1 mod (p-1), q > 2. Les techniques utilisées par Katz pour démontrer la conjecture de Helleseth s'appuient notamment sur les moments d'ordre supérieur de la fonction. Or, ces quantités apparaissent indirectement dans une série de travaux récents en cryptographie qui visent à établir une analogie entre les cryptanalyses linéaire et différentielle. Un des résultats est la relation (à travers leurs moments d'ordre supérieur) entre la transformée de Fourier discrète d'une fonction et son spectre différentiel. Il est alors naturel de se demander si une telle relation ne pourrait pas être exploitée pour aborder certains de ces problèmes sur les sommes de Weil.