1

Distribution de la non-linéarité des fonctions booléennes

François Rodier

Institut de Mathématiques de Luminy
Marseille

Contexte

Le projet concerne l'étude des fonctions booléennes dans le contexte de la cryptographie à clef secrète. Rappelons que l'étude des fonctions booléennes est primordiale dans ce cadre; elles sont en effet utilisées pour combiner la sortie de registres à décalage dans les mécanismes de chiffrement à flot, elles sont aussi utilisées dans la construction de systèmes performants de chiffrement à clé secrète par bloc. Bien entendu, il est intéressant de les étudier des deux points de vue : la construction de bonnes fonctions et les attaques des systèmes qui les utilisent.

Pour être résistantes aux attaques modernes, les fonctions booléennes, qui sont une composante essentielle des algorithmes de cryptographie, doivent répondre à plusieurs critères, notamment avoir une non-linéarité élevée.

Dans le cas où le nombre de variable est pair, on a identifié, sous le nom de fonctions "courbes" celles dont la non-linéarité était la plus grande possible. Celle-ci est alors bien connue, on sait construire plusieurs séries de fonctions courbes, mais on ne connaît encore ni leur nombre, ni leur classification malgré les travaux de nombreux chercheurs sur le sujet.

Dans le cas où le nombre de variable est impair, la situation est bien différente : on ne connaît alors la valeur de la non-linéarité maximale que pour quelques valeurs de m, et on n'a qu'une conjecture pour les autres valeurs. Il y a un grand fossé entre la non-linéarité maximum théorique et la non-linéarité des fonctions que nous savons réellement construire. Par conséquent, il est essentiel de se préoccuper des fonctions qui sont dans cet intervalle.

Une autre raison pour s'intéresser aux fonctions qui ne sont pas courbes est que, pour raisons de sécurité en cryptographie, et également parce que les fonctions booléennes doivent avoir d'autres propriétés telles que l'équilibre ou le degré algébrique élevé qui sont incompatibles avec la non-linéarité, il est important d'avoir la possibilité de choix parmi beaucoup de fonctions booléennes, non seulement fonctions courbes, mais également des fonctions proches des fonctions courbes dans le sens que leur non-linéarité est près de la non-linéarité des fonctions courbes. Il est essentiel, dès lors, de s'intéresser aux fonctions qui ont une non linéarité presque maximale, afin d'étudier le plus grand nombre de fonctions disponibles, dans le but de mieux lutter contre les attaques possibles.

Présentation

Le projet est donc d'avoir une connaissance plus précise de la distribution de la non-linéarité des fonctions booléennes en particulier lorsque cette non-linéarité est élevée.

On se fondera sur le principe, énoncé par J.-P. Kahane qu'il est quelquefois difficile de trouver des objets mathématiques ayant des propriétés données, alors qu'il peut être assez facile d'exhiber un objet aléatoire ayant ces propriétés.

Pour connaître plus précisément la distribution de la non-linéarité au voisinage de la non-linéarité maximale, une des voies pour attaquer ce problème serait d'étudier un problème plus simple : celui de la "somme des carrés" qui est très reliée à la non-linéarité. Une possibilité est alors l'adaptation des théorèmes de grandes déviations.

Le problème se pose plus généralement pour les réactions aux attaques par corrélation multiples. Pour y répondre, on a défini la notion de r-non-linéarité pour laquelle se pose naturellement le problème de la distribution. Il se pose aussi dans le cas des fonctions booléennes vectorielles impliquées dans la cryptographie par blocs.

Enfin, il y a lieu d'examiner comment varie la difficulté lors d'une attaque sur une fonction de linéarité plus ou moins proche de la non-linéarité maximale.

Connaissances requises

On demandera au candidat d'avoir de bonnes notions de cryptographie, ainsi que de probabilités.