Construction de fonctions quaternaires courbes, Projection et Généralisation binaire

Soukayna QARBOUA[1]

Télécom Bretagne/ITI, Lab-STICC, soukayna.qarboua@@telecom-bretagne.eu
ESCC/CREC, UR MACCLIA, soukayna.qarboua@st-cyr.terre-net.defense.gouv.fr
Université Mohamed V Agdal, Faculté des Sciences Rabat, LMIA, MAROC

Mots clés : Anneaux de Galois, fonctions quaternaires, fonctions booléennes, non-linéarité, immunité algébrique.

Notre recherche porte sur l'étude et la conception de fonctions booléennes qui jouent un rôle important en cryptographie. Elles sont activement utilisées dans les protocoles de chiffrement itératifs par blocs et par flux et dans la combinaison ou le filtrage de registres à décalage à rétroaction linéaire pour la génération de suites chiffrantes. Les critères cryptographiques que doivent satisfaire les fonctions booléennes sont nombreux et sujets à compromis selon leurs compatibilités. Parmi ces critères, on retiendra l'équilibre, l'immunité aux corrélations, le critère de propagation, la non-linéarité (d'ordre r), le degré algébrique et l'immunité algébrique. Ils varient avec le système dans lequel elles sont employées et assurent sa résistance aux différents types d'attaques connues comme l'attaque linéaire, l'attaque différentielle, l'attaque par corrélation ou encore l'attaque algébrique et l'attaque algébrique rapide. Habituellement, les fonctions booléennes à n variables, comme leur nom l'indique, sont des fonctions binaires, de $\mathbb{F}_2^n = \{0,1\}^n$, muni de la métrique de *Hamming*, à valeurs dans $\mathbb{F}_2 = \{0,1\}$ L'espace vectoriel $\mathbb{F}_2^n$ étant isomorphe au corps fini à 2^n éléments $\mathbb{F}_{2^n}$, ces fonctions sont généralement construites sur des corps finis binaires résultant d'extensions Galoisiennes du sous corps premier $\mathbb{F}_2$. L'idée génitrice porte sur l'investigation d'une nouvelle approche de l'étude et de la conception de ces fonctions à partir de fonctions quaternaires définies de $\mathbb{Z}_4^m$, muni de la métrique de *Lee*, à valeurs dans l'anneau des entiers modulo 4 noté $\mathbb{Z}_4 = \{0,1,2,3\}$. Ces fonctions quaternaires sont alors construites sur des extensions de $\mathbb{Z}_4$ que sont les anneaux de Galois notés $GR(4,m) \simeq \mathbb{Z}_4^m$. La fonction de Gray ϕ nous offre une projection isométrique de $\mathbb{Z}_4$ dans $\mathbb{F}_2 \times \mathbb{F}_2$ avec $\forall a, b \in \mathbb{Z}_4^m,\ d_{Lee}(a,b) = d_{Hamming}(\phi(a), \phi(b))$. Cette passerelle nous permet de transiter entre fonctions quaternaires et fonctions booléennes.

Nous présentons ici, une nouvelle construction de fonctions quaternaires courbes à m variables dont la projection binaire donne des fonctions booléennes à $2m$ variables courbes et à $2m+1$ variables de nonlinéarité maximale, ainsi qu'une généralisation de ces projections qui donne dans le cas pair une nouvelle définition vectorielle de la classe de fonctions $\mathcal{PS}$ (*Partial Spread*, Dillon) de degré algébrique maximal et dans le cas impair une nouvelle classe de fonctions *Plateau*. En 2010, Tu et Deng établissent une conjecture permettant de montrer selon certains paramètres, qu'il existe des fonctions booléennes d'immunité algébrique optimale dans la classe des fonctions $\mathcal{PS}$. Dans notre cas, les expérimentations numériques menées pour des valeurs de $m < 7$, témoignent que l'immunité algébrique des fonctions booléennes projetées est optimale ($\mathcal{AI} = m$) dans le cas pair ($n = 2m$) et bornée ($m - 1 \leq \mathcal{AI} \leq m$) dans le cas impair($n = 2m + 1$). L'aspect formel de la démonstration de ces propriétés est actuellement en cours.