Nouveaux résultats sur la conjecture de Tu-Deng et addition modulo $2^k - 1$

Les fonctions booléennes constituent des blocs de construction couramment utilisés dans la conception de systèmes cryptographiques symétriques, en particulier dans le chiffrement à flot. De toute évidence, les propriétés de ces fonctions sont essentielles pour les exigences de sécurité du système final qui les utilise. Par conséquent, plusieurs propriétés cryptographiques sur les fonctions booléennes ont été définies pour assurer l'immunité du système face aux différents types d'attaques. On retiendra ici *l'immunité algébrique*. Suite à l'évolution permanente du domaine de la cryptanalyse et l'apparition de nouvelles attaques, la conception de fonctions booléennes reste en constante évolution. Naturellement, ceci implique de nouvelles restrictions sur les classes de fonctions booléennes adoptées et rend parfois obsolètes les familles de fonctions connues. Par ailleurs, ces critères présentent des incompatibilités, et des compromis doivent être considérés. Les incompatibilités entres les différents critères cryptographiques pourraient laisser croire que la construction de fonctions booléennes satisfaisant tous les critères cryptographiques est hors de portée. Heureusement, ce n'est pas le cas. Nous nous intéresserons ici à des classes infinies de fonctions booléennes qui répondent à la plupart des critères requis pour le chiffrement à flot et dont l'optimalité de l'immunité algébrique dépend de la validité d'une conjecture combinatoire appelée conjecture de Tu-Deng.

Conjecture 1 (Tu-Deng)**.** *Soit $k \geq 2$ un entier, $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ et posons :*

$$S_{t,k} = \{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2, \text{ tel que } \underbrace{a+b=t}_{\text{équation}(1)} \text{ et } \underbrace{w_H(a)+w_H(b) \leq k-1}_{\text{inéquation}(2)}\},$$

alors $|S_{t,k}| \leq 2^{k-1}$.

Nous présentons ici, une nouvelle approche de la problématique, en considérant une relation d'équivalence particulière sur les couples (a, b). Cette approche nous conduit dans un premier temps à une formule du cardinal de l'ensemble des solutions $(a, b) \in (\mathbb{Z}/(2^k - 1)\mathbb{Z})^2$ de même poids (dépendant d'un paramètre i). Notons cette ensemble $S_t(i)$, nous avons démonté que :

$$|S_t(i)| = \sum_{(x_0,\ldots,x_{w-1}) \in E_t \text{ et } \sum_{i=0}^{w-1} x_i = i} 2^i \prod_{x_i=-1} 4 - 2\delta_{k-w}(i).$$

Ensuite, en introduisant un polynôme P_t qui présente un lien particulier avec l'ensemble des solutions $(a, b) \in (\mathbb{Z}/(2^k - 1)\mathbb{Z})^2$ de même poids et $m(t)$ l'image "miroir" de l'entier t (si $t = \sum_{i=0}^{k-1} t_i 2^i$, alors $m(t) = \sum_{i=0}^{k-1} t_{k-1-i} 2^i$) nous avons démontré que : P_t est égal à $P_{m(t)}$.

Ce dernier résultat nous permet de trouver une famille de t vérifiant la conjecture : La famille d'entiers construits par une concaténation de deux entiers vérifiant $m(t) = -t$.

Ce travail est en collaboration avec Caroline Fontaine, CNRS, Lab-STICC, Télécom Bretagne et Julien Shreck , CNRS, Lab-STICC, Télécom Bretagne.

[SQF16] Soukayna Qarboua, Julien Schrek, Caroline Fontaine
New results about Tu-Deng's conjecture, conference,
IEEE International Symposium on Information
Theory, ISIT, 2016.