PROJET DUBLIN

PHILIPPE LANGEVIN

Résumé. Je vous propose deux sujets indépendants concernant la classification des fonctione vectorielles en petite dimension. Prévoir un rdv de suivi hebdomadaire d'une heure.

1. projet Dublin



La permutation de Dublin est le seul exemple connu de permutation APN en dimension paire. Elle a été annoncée à la conférence FQ9 (Dublin) par Browning, Dillon, McQuistan et Wolfe. Depuis, aucune autre permutation APN en dimension 6 n'a été trouvée. On connaît 14 classes CCZ de fonctions APN (6,6), c'est-à-dire de 6 bits vers 6 bits, qui se décomposent en 716 classes EA. L'article de Gillot et Langevin présente de nouveaux invariants, un critère d'extensibilité APN et une approche par backtracking, qui appuient numériquement la conjecture selon laquelle ces 14 classes CCZ épuisent les APN sur 6 bits.

phase 1 : classer les (6,3) sous-fonctions des 716 APNs de la littérature.

phase 2 : calculer les 3-switchs des APNs de la littérature.

Le sujet proposé concerne la phase 1 uniquement, réalisable en 5 semaines. En effet, l'extension APN des (6,3) fonctions vectorielles, second volet de l'article, phase 2 de ce projet, n'est pas demandée mais pourra faire l'objet d'un sujet de stage de recherche de 5 mois. Notions clés à maîtriser : le groupe affine général, matrice échelonnée et sous-espace, fonction APN, espace des composantes, sous-fonction, critère d'APNéité, invariant affine, coefficient de Walsh, invariant EA et CCZ, backtracking.

(1) Engendrer les (6,3) sous-fonctions des APNs à 6 bits.

(2) Utiliser les invariants de la littérature pour EA-classer les sous-fonctions (6,3) des APNs.

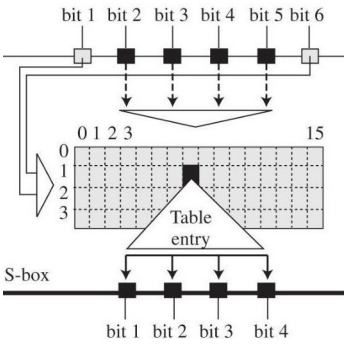
(3) Terminer la classification en gérant les collisions avec des tests d'équivalence.

(4) Reprendre ces questions pour la CCZ-classification.

(5) Estimer le temps de calcul pour déterminer les extensions APN.

Date: Automne 2026.

2. Classification des 4-sbox



On considère l'espace $V_3(4,4)$ des fonctions de 4 variables sans terme linéaire.

(1) Faire un état de l'art sur la classification EA de $V_2(4,4)$.

(2) Compter le nombre de classes EA avec la formule de Burnside.

(3) Utiliser les invariants de la littérature pour EA-classer les APNs.

(4) Terminer la classification en gérant les collisions avec des tests d'équivalence.

Références

[1] Valérie Gillot Philippe Langevin *On Known APNs* (2026), https://arxiv.org/abs/2601.11247