Cryptanalysis using CP solvers the case of division property

Laboratory, institution and university The internship will be located at IRISA (Rennes).

Team or project of the Lab Team EMSEC at IRISA

Advisors Patrick Derbez (Patrick.Derbez@irisa.fr), and Stéphanie Delaune (Stephanie.Delaune@irisa.fr)

Indemnisation The internship is supported by the ANR grant **DeCrypt**.

Keywords cryptanalysis, constraint programming solvers

Description du stage

Dans ce stage l'étudiant devra étudier l'effet d'un changement de représentation d'un système de chiffrement par bloc sur la propagation de *division property*.

La *division property* est une méthode de cryptanalyse inspirée des attaques intégrales et se révèle très efficace contre certaines primitives cryptographique. L'idée générale est l'étude de l'expression polynomiale des bits du message chiffré en fonction du message clair. Plus précisément, l'objectif est de déterminer la présence ou non de certains monômes dans ces expressions polynomiales.

Ces dernières années, ce type d'attaques cryptographique est devenu un sujet majeur de recherche en cryptographie symétrique. La recherche automatique de distingueurs type *division property* repose sur des règles de propagation relativement simples mais est fortement liée à la description du système de chiffrement. De plus, de récents résultats ont exhibé des fonctions de chiffrement E pour lesquels on peut prouver qu'il n'existe pas de *division property* mais telles qu'il en existe sur $L_1 \circ E \circ L_2$ où L_1 et L_2 sont des applications linéaires.

Dans un premier temps, l'étudiant aura pour objectif de concevoir et d'implémenter un algorithme permettant de trouver (si elles existent) de telles couches linéaires. Dans un second temps, on s'intéressera à modifier la

représentation interne de la fonction de chiffrement avec l'espoir d'améliorer encore ce type d'attaques cryptographiques.

Références

— Sun, Wang and Wang. *Automatic Search of Bit-Based Division Property for ARX Ciphers and Word-Based Division Property.*
— Zhang and Rijmen. *Division Cryptanalysis of Block Ciphers with a Binary Diffusion Layer.*