Diffusion totale dans le schéma de Feistel généralisé

S. Delaune[1], P. Derbez[1], A. Gontier[1], C. Prud'homme[2]

[1] Univ. Rennes, CNRS, IRISA, Rennes, France
[2] TASC, IMT-Atlantique Nantes, LS2N-CNRS, F-44307, Nantes, France
{stephanie.delaune,patrick.derbez,arthur.gontier}@irisa.fr,
charles.prudhomme@imt-atlantique.fr

Mots-clés : *CP, chiffrement, Feistel*

La cryptographie tient un rôle central dans nos sociétés actuelles. Elle consiste à protéger des messages en les chiffrant, la qualité d'un algorithme de chiffrement se juge sur son efficacité (rapidité à chiffrer/déchiffrer un message) et sa résistance aux attaques connues. Notre étude porte sur la cryptographie symétrique, où la même clé sert pour le chiffrement et le déchiffrement, et en particulier sur le schéma de Feistel généralisé. Il s'agit d'un schéma de chiffrement symétrique par bloc où une fonction dite *de tour* est appliquée sur le message et la clé, à plusieurs reprises ou *tours*. Un tour du schéma de Feistel est séparé en deux étapes : d'abord chaque paire de blocs mélange le contenu de ses deux blocs à l'aide d'un XOR bit à bit, puis une permutation est appliquée entre tous les blocs. La robustesse de ce schéma est directement liée à sa diffusion [3], c'est-à-dire, au fait que chaque bloc soit dépendant de tous les autres après τ applications de la fonction de tour. Le problème consiste à trouver la permutation P qui diffuse totalement tous les blocs en le moins de tours τ possible.

Les travaux précédents [1, 2] ont principalement exploré le cas spécifique appelé pair-impair, où la permutation envoie les blocs pairs sur les blocs impairs et inversement. Afin d'étudier l'existence de solutions optimales n'ayant pas cette structure, nous présentons ici des pistes de modélisation en programmation par contraintes pour résoudre ce problème.

1 Formalisation du problème

La diffusion pour une paire de bloc dans un tour de Feistel est la suivante. Le bloc d'indice pair est inchangé et le bloc d'indice impair propage la diffusion des deux blocs de la paire.

Le problème de la diffusion totale. Pour un nombre de tours $\tau > 0$ et un nombre de blocs $n = 2p$ donnés, le problème de la diffusion de Feistel consiste à trouver une permutation P qui diffuse totalement tous les blocs en exactement τ tours.

Une représentation à l'aide de graphe permet d'exprimer le problème de la manière suivante : Soit le graphe $G = (V, P \cup E)$ avec V l'ensemble des noeuds correspondant aux blocs et deux types d'arcs : P, les arcs de la permutation, et E, les epsilon-transitions correspondant au mélange dans une paire de bloc. La permutation P d'un ou plusieurs cycles doit permettre la diffusion totale de tous les nœuds. Ce qui signifie que pour toutes paires de nœuds (i, j) il existe au moins un chemin non-élémentaire de taille exactement τ qui va de i vers j.

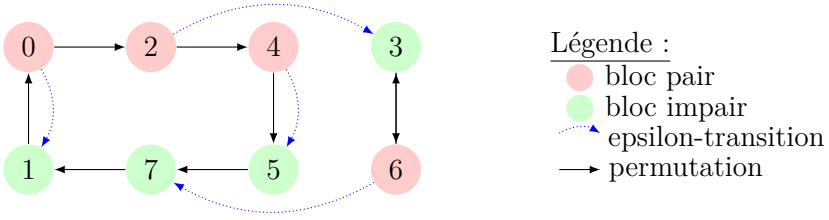

FIG. 1 – Solution pour une diffusion totale après $\tau = 6$ tours pour $n = 8$.

La figure 1 est une solution avec une diffusion totale minimale de $\tau = 6$. La diffusion totale est la partie difficile de ce problème et nous présentons plusieurs modélisation de ce problème.

Modèle avec produit matriciel. Un premier modèle repose sur la propriété suivante. Le nombre de chemins de taille τ pour aller de i vers j dans un graphe est donné par la matrice d'adjacence de ce graphe élevée à la puissance τ. Soit A la matrice d'adjacence de la permutation P. Une fois les epsilon-transitions intégrées à A, une diffusion totale implique que tous les coefficients de la matrice A^τ soient non nuls.

Modèle avec des variables de diffusion ensemblistes. Un second modèle exploite la représentation d'un graphe à l'aide d'ensemble d'arcs. Soit S_{i1}, l'ensemble des successeurs du nœud i et $S_{i,\tau}$, l'ensemble des nœuds atteignables au tour $\tau > 1$ depuis le nœud i. La diffusion au tour τ depuis le nœud i s'écrit comme l'union des diffusions atteintes par i au tour précèdent :

$$S_{i,\tau} = \bigcup_{j \in S_{i,\tau-1}} S_{j,\tau-1}$$

2 Conclusions et perspectives

Le problème de la diffusion totale de Feistel s'exprime aisément en programmation par contraintes. Dans le premier modèle, la puissance d'une matrice booléenne est représentée par une décomposition en formules logiques et nécessite la déclaration de variables booléennes uniquement ; le second modèle repose quant à lui sur des variables ensemblistes et des contraintes d'union plus proches des contraintes globales propres à la CP. Les heuristiques précédemment utilisées pour résoudre ce problème dans le cas général de la permutation [1] parvenaient à trouver des solutions en temps raisonnable jusqu'à 18 blocs. Nos meilleurs modèles retrouvent ces résultats en quelques secondes et peuvent aller jusqu'à trouver des solutions pour 24 blocs en moins d'une heure. Toutefois, nous aimerions pousser plus loin ces résultats pour se comparer aux cas spécifiques pairs-impairs de la permutations [2]. Pour ce faire, nous avons trois pistes. Tout d'abord nous remarquons que construire une solution en essayant de combiner des chemins de taille τ est assez efficace et nous pourrions utiliser cette idée comme stratégie de recherche. Nous remarquons aussi qu'il est possible de diviser le problème avec toutes les décomposition en cycles de la permutation. Chaque sous-problème devient alors un problème de graphe biparti sur les epsilon-transitions. Enfin, nous remarquons qu'il y a beaucoup de symétries dans le problème, inter-changer deux paires suffit pour trouver une solution équivalente. La suite de ce travail consistera donc à mettre en œuvre ces idées pour améliorer le filtrage et la stratégie de nos modèles.

Remerciements Ce travail est supporté par Agence Nationale de la Recherche Française dans le cadre du projet DeCrypt (ANR- 18-CE39-0007).

Références

[1] Victor Cauchois, Clément Gomez, and Gaël Thomas. General diffusion analysis : How to find optimal permutations for generalized type-ii Feistel schemes. *IACR Trans. Symmetric Cryptol.*, 2019(1) :264–301, 2019.

[2] Patrick Derbez, Pierre-Alain Fouque, Baptiste Lambin, and Victor Mollimard. Efficient search for optimal diffusion layers of Generalized Feistel Networks. *IACR Transactions on Symmetric Cryptology*, 2019(2) :218–240, Jun. 2019.

[3] Tomoyasu Suzaki and Kazuhiko Minematsu. Improving the generalized Feistel. In Seokhie Hong and Tetsu Iwata, editors, *Fast Software Encryption, 17th International Workshop, FSE 2010, Seoul, Korea, February 7-10, 2010, Revised Selected Papers*, volume 6147 of *Lecture Notes in Computer Science*, pages 19–39. Springer, 2010.