Diffusion dans les schémas de Feistel généralisés*

Gaël Thomas†

Avec les réseaux substitution-permuation, les schémas de Feistel constituent l'une des deux grandes familles de chiffrement par bloc. Popularisé par le Data Encryption Standard, le schéma de Feistel a depuis subi de nombreuses généralisations visant à augmenter le nombre de blocs en lesquels est subdivisé le message. Ceci amène alors à se poser la question du nombre minimum d'itérations à effectuer pour « bien mélanger » ces blocs. Plus précisément, on s'intéresse ici à la notion de (délai de) diffusion qui est le nombre minimum de tours au bout desquels chaque bloc en sortie dépend de tous les blocs en entrée.

Dans cet exposé, on se propose d'abord de faire un tour d'horizon des différentes familles de schémas de Feistel généralisés en se focalisant sur la notion de diffusion, notamment via les travaux de [SM10], puis d'expliciter une vision matricielle du problème de la diffusion qui nous permettra finalement de donner une définition plus générale du schéma de Feistel, englobant la majorité des cas préexistants.

Références

[SM10] Tomoyasu Suzaki et Kazuhiko Minematsu : Improving the Generalized Feistel. *In* Seokhie Hong et Tetsu Iwata, éditeurs : *FSE*, volume 6147 de *LNCS*, pages 19–39. Springer, 2010.

*Ce travail a été partiellement financé par l'Agence nationale de la recherche : ANR-11-INS-011.

†XLIM - UMR CNRS n° 7252 - 123, avenue Albert Thomas - 87060 Limoges cedex - ✉ gael.thomas@xlim.fr