Propriétés différentielles et linéaires des FCSR*

Gaël Thomas†

Les Registres à décalage à rétroaction avec retenue ou FCSR (*Feedback with Carry Shift Register*) ont été proposés par Andrew Klapper et Mark Goresky dans [KG93] et sont analogues aux LFSR à la différence près que les additions ne se font plus modulo 2 mais avec propagation des retenues. Les FCSR disposent d'une structure algébrique qui permet de déduire des propriétés similaires à celles des LFSR mais en ayant une fonction de transition quadratique.

Une utilisation classique des FCSR consiste à appliquer un filtre linéaire sur son état interne pour en casser sa structure, comme fait dans [ABL+09] ou [BDM+12]. En s'inspirant notamment des travaux de Tian Tian et Wen-Feng Qi ([TQ09]), on se propose de comparer quelques biais différentiels et linéaires de cette nouvelle primitive cryptographique avec ce que l'on obtiendrait pour une fonction aléatoire.

Références

[ABL+09] François Arnault, Thierry P. Berger, Cédric Lauradoux, Marine Minier et Benjamin Pousse : A New Approach for FCSRs. *In Selected Areas in Cryptography*, volume 5867 de *LNCS*, pages 433–448. Springer, 2009.

[BDM+12] Thierry P. Berger, Joffrey D'Hayer, Kevin Marquet, Marine Minier et Gaël Thomas : The GLUON Family : A Lightweight Hash Function Family Based on FCSRs. *In AFRICACRYPT*, volume 7374 de *LNCS*, pages 306–323. Springer, 2012.

[KG93] Andrew Klapper et Mark Goresky : 2-Adic Shift Registers. *In Fast Software Encryption*, volume 809 de *LNCS*, pages 174–178. Springer, 1993.

[TQ09] Tian Tian et Wen-Feng Qi : Linearity properties of binary FCSR sequences. *Des. Codes Cryptography*, 52(3):249–262, 2009.

*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