Attaques exploitant les représentations équivalentes des LFSRs filtrés

Anne Canteaut et Yann Rotella

Inria équipe-projet SECRET
anne.canteaut@inria.fr, yann.rotella@inria.fr

Dans beaucoup de systèmes de chiffrement à flot, les registres à décalage filtrés sont encore utilisés [1]. Récemment, Rønjom et Cid [2] ont proposé des représentations équivalentes des LFSRs filtrés à partir du résultat suivant, dans lequel les $n$uplets sont identifiés à des éléments du corps $\mathbb{F}_{2^n}$.

Proposition 1. *[2] Soit σ une suite produite par un LFSR de taille n, de polynôme de rétroaction primitif P définissant une racine primitive α sur le corps $\mathbb{F}_{2^n}$ et filtré par une fonction booléenne f. Soit k un entier premier avec 2^n-1 et s est tel que $sk \equiv 1 \mod 2^n-1$. Alors σ est également produite par le LFSR ayant pour polynôme de rétroaction le polynôme minimal de α^k, filtré par la fonction booléenne $f'(x) = f(x^s)$.*

Nous étudions donc l'impact de cette équivalence sur la cryptanalyse de systèmes de chiffrement à flot à base de LFSR. En particulier, certaines attaques classiques (attaques par corrélation, attaques algébriques...) peuvent s'appliquer à cette représentation équivalente car il est possible que, contrairement à la fonction f d'origine, la nouvelle fonction de filtrage f' n'ait plus de bonnes propriétés cryptographiques.

Nous nous sommes intéressés à l'influence de ces transformations sur le degré algébrique de la fonction, en particulier quand la fonction booléenne est une fonction monomiale ou une somme de deux monômes. Ceci est lié aux valeurs minimales des ensembles du type

$$\{\mathsf{w}_H(us \mod (2^n-1)); \mathrm{pgcd}(s, 2^n-1) = 1\}$$

Par ailleurs, pour se prémunir contre les attaques par corrélation, nous savons déjà qu'il est important d'utiliser des fonctions ayant une non-linéarité élevée. En revanche, d'après ce qui précède, il est clair que pour tout s tel que $\mathrm{pgcd}(s, 2^n-1) = 1$, $f(x^s)$ doit aussi avoir une grande non-linéarité afin d'éviter une attaque sur un système équivalent exploitant la corrélation entre la suite chiffrante et la suite produite par le même LFSR filtré par x^s. La résistance à cette attaque est alors mesurée par la notion de non-linéarité généralisée, liée aux fonctions courbes, introduites dans [3].

De plus, nous nous sommes aussi intéressés aux cas où k n'est pas premier avec 2^n-1. Alors nous pouvons aussi retrouver une partie de l'état initial du registre filtré en réalisant des attaques par corrélation sur des registres de taille parfois plus petite, dont le polynôme de rétroaction n'est plus nécessairement primitif. Il est aussi possible de recouper les résultats de ces attaques afin de récupérer l'état initial plus rapidement que la recherche exhaustive.

Références

[1] An Braeken, Joseph Lano, Nele Mentens, Bart Preneel, and Ingrid Verbauwhede. Sfinks : A synchronous stream cipher for restricted hardware environments. *eSTREAM*, 2008.

[2] Sondre Rønjom and Carlos Cid. Nonlinear equivalence of stream ciphers. In *Fast Software Encryption, 17th International Workshop, FSE 2010, Seoul, Korea, February 7-10, 2010, Revised Selected Papers*, pages 40–54, 2010.

[3] Amr M. Youssef and Guang Gong. Hyper-bent functions. In *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*, pages 406–419, 2001.