Attaques par corrélation sur chiffrements à flot

Université de Versailles Saint-Quentin en Yvelines

2022

Résumé Une manière de concevoir un chiffrement symétrique est d'utiliser un générateur pseudo-aléatoire, initialisé par une clef et l'IV et d'utiliser la suite chiffrante comme un one-time-pad. Ainsi, il est nécessaire d'avoir de bonnes propriétés de la suite chiffrante qui rendent celle-ci difficile à distinguer d'une suite aléatoire. Une manière de réussir cela est d'utiliser des registres à décalages et à rétroaction linéaires, qui sont une construction implémentant la multiplication par un élément du corps.

Or ces LFSRs sont, par définition linéaires et donc ne suffisent pas à eux seuls pour faire un chiffrement, l'algorithme de Berlekamp Massey [1] permettant de retrouver très facilement l'état initial et le polynôme de rétroaction utilisé.

Pour cette raison, ces LFSRs peuvent être combinés ou filtrés, à chaque fois à l'aide d'une ou plusieurs fonctions booléennes. Au delà du fait que la fonction booléenne doit avoir un haut degré algébrique ou immunité algébrique, celle-ci doît aussi être loin en distance de Hamming de toutes les fonctions affines, dans le cas d'un registre filtré ou qu'elle ne puisse pas être approchée par une fonction en moins de variables dans le cas d'un registre combiné (E0 ou A5/1 par exemple), sinon le chiffrement est vulnérable aux attaques par corrélation rapides dans le premier cas et aux attaques par corrélation dans le deuxième cas.

Objectifs Le but de ce projet est de programmer des LFSRs filtrés et combinés, puis de programmer les attaques par corrélations et les attaques par corrélations rapides sur des exemples de tailles les plus grandes possibles. Enfin, s'il y a du temps, on pourra s'intéresser à un récent papier revisitant ces attaques.

Prérequis Aucun

Références

1. page 260 de l'article original : `https://link.springer.com/content/pdf/10.1007/3-540-39799-X.pdf`, mais l'idée peut être trouvée dans la plupart de polycopiés de cryptographie, en francais.
2. `https://link.springer.com/content/pdf/10.1007/BF02252874.pdf`
3. `https://eprint.iacr.org/2018/522.pdf`

1. `https://en.wikipedia.org/wiki/Berlekamp\%E2\%80\%93Massey_algorithm`