Mathématiques discrètes appliquées à la cryptographie symétrique

Yann Rotella, thèse encadrée par Anne Canteaut,
effectuée à Inria équipe-projet SECRET
yann.rotella@inria.fr

2 septembre 2018

Résumé

Dans cette thèse, nous étudions la sécurité de systèmes cryptographiques symétriques qui sont des transformations reposant sur des objets mathématiques qui peuvent être représentés de multiples manières. Nous utilisons alors certaines structures inhérentes jusqu'alors non prises en compte, pour mettre en évidence de nouvelles vulnérabilités, en exploitant diverses représentations. Nous avons cryptanalysé des chiffrements authentifiés de la compétition CAESAR, des chiffrements à flot spécifiques et des constructions génériques. Nous avons donné des critères de conception en vue de la standardisation par le NIST sur la cryptographie légère et dans le cas des chiffrements à flot, nous avons défini de nouveaux critères cryptographiques plus pertinents que les critères classiques. Ces travaux ont donné lieu à des publications dans des conférences et journaux de référence du domaine (CRYPTO, FSE, IACR TOSC).

Introduction

La cryptographie. Un des principaux objectifs de la cryptographie est de permettre, grâce à un procédé de chiffrement, à deux entités de pouvoir communiquer de manière confidentielle sur un canal de communication non sécurisé. Il est bien connu depuis les travaux de Shannon [Sha49] que la sécurité parfaite nécessite le partage d'un secret de taille aussi longue que le message à échanger. Les systèmes de chiffrement parfaits sont donc inutilisables en pratique. La sécurité des algorithmes que nous employons est donc empirique dans le sens où elle est déterminée par le coût du meilleur algorithme permettant de "casser" le système. Un travail de cryptanalyse continuel et poussé est donc indispensable afin de déterminer le niveau de sécurité des algorithmes existants et de dégager des critères de conception permettant de garantir que les nouveaux chiffrements résistent par construction aux attaques connues.

Il existe deux types de chiffrements : symétrique et asymétrique. Dans un chiffrement symétrique, les deux interlocuteurs partagent un secret commun (la clef) et veulent communiquer sans que quiconque qui intercepte la communication ne puisse décrypter un message qui ne lui serait pas destiné. Dans un chiffrement asymétrique, chacun possède sa propre clef secrète (ainsi qu'une clef publique qui lui est associée), et tout le monde peut chiffrer un message avec la clef publique, mais seul le détenteur de la clef secrète peut déchiffrer ledit message. La sécurité des chiffrements asymétriques repose sur des problèmes algorithmiques supposés difficiles, à la différence des chiffrements symétriques où la sécurité repose essentiellement sur les cryptanalyses. En revanche, les algorithmes de chiffrements symétriques sont les seuls qui aient des performances acceptables en termes de débit, de taille de clef ou de complexité d'implémentation matérielle pour la plupart des applications.

Depuis une dizaine d'années, l'apparition de nouvelles applications et la multiplication des objets connectés ont imposé aux algorithmes de chiffrement de nouvelles contraintes portant par exemple sur la consommation d'énergie ou la taille du circuit implémentant l'algorithme. La conception de chiffrements à bas coût est donc actuellement une voie de recherche importante qui répond à

une demande industrielle pressante. Les travaux sur la cryptographie légère devraient notamment aboutir à un processus de standardisation qui sera probablement initié par le NIST (National Institute of Standards and Technology) en fin d'année 2018.

Problématique. Par définition, les chiffrements doivent être indistinguables d'une transformation tirée aléatoirement selon la distribution uniforme dans l'ensemble des fonctions ayant les mêmes paramètres. Il est beaucoup trop coûteux voire impossible d'implémenter en pratique des transformations opérant sur des données de taille réelle, par exemple sur des fonctions opérant sur des messages de taille 128 bits. Les chiffrements utilisés en pratique doivent donc nécessairement employer des transformations structurées, et non aléatoires, pour avoir un faible coût d'implémentation.

Toutefois, ces structures qui facilitent l'implémentation correspondent à des structures mathématiques très particulières, qui peuvent être la source de vulnérabilités. Déterminer si certaines structures mathématiques peuvent être exploitées dans une cryptanalyse est donc un problème essentiel, au coeur de la cryptographie symétrique. C'est dans cette problématique générale que s'inscrivent mes travaux de thèse.

Dans ma thèse, j'étudie en effet la sécurité d'un vaste choix de cryptosystèmes, à la fois des constructions générales tels que les réseaux de substitution-permutation et les registres filtrés, ou bien spécifiques et instanciés concrètement, tels que le chiffrement FLIP ou bien les chiffrements authentifiés Ketje et MORUS. Pour tous ces systèmes, j'ai conçu de nouvelles attaques exploitant les propriétés des objets mathématiques utilisés. De plus, je me suis attaché à identifier les structures qui sont à l'origine de ces attaques, ce qui m'a permis de définir de nouveaux critères de conception, plus pertinents que les critères existants, mais aussi de montrer que plusieurs représentations d'un même objet peuvent impliquer l'existence de vulnérabilités, ces vulnérabilités étant spécifiques à la représentation et non à l'objet lui-même.

Mes publications

[AEL+18] Tomer Ashur, Maria Eichlseder, Martin M. Lauridsen, Gaëtan Leurent, Brice Minaud, Yann Rotella, Yu Sasaki et Benoit Viguier. "Cryptanalysis of Full MORUS". In : *ASIACRYPT 2018* (2018), p. 1–30.

[BCL+17] Christof Beierle, Anne Canteaut, Gregor Leander et Yann Rotella. "Proving Resistance Against Invariant Attacks : How to Choose the Round Constants". In : *CRYPTO 2017, Part II*. Sous la dir. de Jonathan Katz et Hovav Shacham. T. 10402. LNCS. Springer, Heidelberg, août 2017, p. 647–678.

[CDM+18] Geoffroy Couteau, Aurélien Dupin, Pierrick Méaux, Mélissa Rossi et Yann Rotella. "On the Concrete Security of Goldreich's Pseudorandom Generator". In : *ASIACRYPT 2018* (2018), p. 1–55.

[CMR17] Claude Carlet, Pierrick Méaux et Yann Rotella. "Boolean functions with restricted input and their robustness ; application to the FLIP cipher". In : *IACR Trans. Symm. Cryptol.* 2017.3 (2017), p. 192–227. issn : 2519-173X.

[CR16] Anne Canteaut et Yann Rotella. "Attacks Against Filter Generators Exploiting Monomial Mappings". In : *FSE 2016*. Sous la dir. de Thomas Peyrin. T. 9783. LNCS. Springer, Heidelberg, mar. 2016, p. 78–98.

[DLR16] Sébastien Duval, Virginie Lallemand et Yann Rotella. "Cryptanalysis of the FLIP Family of Stream Ciphers". In : *CRYPTO 2016, Part I*. Sous la dir. de Matthew Robshaw et Jonathan Katz. T. 9814. LNCS. Springer, Heidelberg, août 2016, p. 457–475.

[FNR18] Thomas Fuhr, María Naya-Plasencia et Yann Rotella. "State-Recovery Attacks on Modified Ketje Jr". In : *IACR Trans. Symmetric Cryptol.* 2018.1 (2018), p. 29–56.

1 Préliminaires

Les chiffrements symétriques se répartissent en deux grandes familles : les chiffrements par bloc et les chiffrements à flot. La plupart des chiffrements à flot consistent à additionner bit-à-bit (XOR) le texte clair avec une suite pseudo-aléatoire (la suite chiffrante) engendrée à partir de la clef secrète afin de reproduire le principe du chiffrement de Vernam (one-time pad). Les chiffrements par bloc consistent eux à chiffrer des blocs de message de taille fixée (typiquement 64 ou 128 bits), les opérations sur les différents blocs étant par ailleurs chaînées au moyen d'un mode opératoire.

Les attaques sur les chiffrements symétriques consistent à retrouver de l'information secrète en un temps plus rapide que la sécurité assurée par les concepteurs. Par exemple, cela peut être la clef utilisée dans un chiffrement par bloc ou l'état initial d'un générateur pseudo-aléatoire utilisé dans un chiffrement à flot. L'attaque de base consiste à tester toutes les clefs secrètes possibles, c'est la recherche exhaustive. Le but du cryptographe est donc souvent de concevoir un chiffrement sur lequel les meilleures attaques se font en un temps équivalent à la recherche exhaustive. De manière plus générale, la suite chiffrante ou la permutation définie par un chiffrement par bloc doivent être indistinguables de suites ou de permutations aléatoires.

2 Cryptanalyse de FLIP

FLIP est un chiffrement à flot proposé par Pierrick Méaux, Anthony Journault, François-Xavier Standaert et Claude Carlet à EUROCRYPT 2016 [MJS+16] qui a été conçu pour pouvoir être utilisé dans un chiffrement hybride, combiné avec un algorithme asymétrique complètement homomorphe. L'objectif des auteurs était donc de minimiser la profondeur multiplicative du circuit implémentant le générateur pseudo-aléatoire afin qu'il puisse être évalué "homomorphiquement" à un coût raisonnable. Comme nous allons le détailler maintenant, nous avons proposé une attaque sur FLIP avec Virginie Lallemand et Sébatien Duval [DLR16] qui "casse" complètement la version originale proposée par les auteurs. En effet, alors que les auteurs affirmaient que la meilleure attaque nécessitait au moins 2^{80} (respectivement 2^{128} pour la deuxième version) opérations, notre attaque a un coût de 2^{54} (respectivement 2^{68}) opérations.

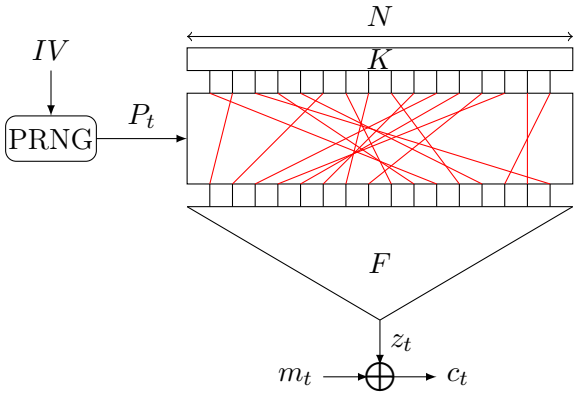

FIGURE 1 – Structure générale de la famille de chiffrements à flot FLIP.

Comme dans tous les générateurs pseudo-aléatoires, l'état interne de FLIP est stocké dans un registre, auquel on applique une fonction non-linéaire F, dite de filtrage, qui extrait à chaque instant un bit d'information du registre. La particularité de FLIP est que le contenu de son registre est fixé (et égal à la clef K), et n'évolue pas au cours du chiffrement (*cf.* figure 1). À chaque itération, les bits de ce registre sont permutés par une permutation pseudo-aléatoire publique. Une fonction booléenne F est ensuite appliquée à la clef permutée, produisant ainsi un bit de suite chiffrante. Le bit de la suite chiffrante correspondant vaut donc $F(P_t(K))$ où P_t est une permutation connue.

La fonction de filtrage F a été soigneusement choisie par les concepteurs de manière à satisfaire tous les critères cryptographiques classiques : degré algébrique élevé, haute non-linéarité, immunité

aux corrélations,... Elle est définie par une somme de monômes faisant intervenir des variables indépendantes. Sa spécificité que nous allons exploiter dans notre attaque est que, alors qu'elle possède de nombreux monômes de degré 1 et 2, elle ne comporte qu'un seul monôme de degré i, pour tout $3 \leq i \leq \deg F$.

Notre attaque est une technique de type "supposer et déterminer" dont l'idée est de deviner quelques positions où les bits de la clef valent 0 afin d'annuler les monômes de haut degré de F et de déterminer des relations quadratiques entre les bits de la suite chiffrante et les bits de la clef. On fait donc l'hypothèse dans un premier temps que ℓ bits de la clef sont à 0 ; la probabilité que cette hypothèse soit vérifiée est notée $\mathbb{P}_{rg}$. L'attaquant conserve donc l'équation $z_t = F(P_t(K))$ à tous les instants t pour lesquels cette équation est de degré au plus 2, *i.e.* si les positions supposées à zéro initialement sont envoyées par P_t dans les monômes de degré supérieur ou égal à 3, afin que ceux-ci s'annulent. La probabilité qu'une permutation aléatoire P_t fournisse une équation de degré 2 est notée $\mathbb{P}_\ell$. Il suffit alors de résoudre un système de degré 2 par linéarisation, ce qui nécessite $v_\ell \simeq N^2$ équations quadratiques, donc $v_\ell \mathbb{P}_\ell^{-1}$ bits de suite chiffrante.

La complexité totale de notre attaque est donc $v_\ell^3 \mathbb{P}_{rg}^{-1}$ en temps et $v_\ell \mathbb{P}_\ell^{-1}$ en données, ce qui donne une attaque en 2^{54} (respectivement 2^{68}) opérations élémentaires pour les paramètres proposés par les auteurs. Un compromis entre la complexité en temps et le nombre de bits de suite chiffrante requis est possible, en augmentant la valeur de ℓ. Notre attaque amena les concepteurs de FLIP à modifier leur chiffrement dans la version finale de leur article, en augmentant la taille de la clef. L'instance de FLIP résultant de cette modification pour une sécurité supposée de 80 bits (resp. 128) demande une clef de taille 530 bits (resp. 1394).

3 Cryptanalyse du PRG de Goldreich

Le générateur pseudo-aléatoire (PRG) de Goldreich [Gol00] est une construction théorique très célèbre, permettant d'étendre une source d'*alea* (graine) en une suite de taille plus grande. La sécurité repose sur l'absence d'attaque fonctionnant en temps polynomial et pose la question de l'existence de PRG, dont les bits de sortie ne dépendraient que d'un faible nombre de bits en entrée. Cette construction a une structure similaire à celle de FLIP. On peut donc lui appliquer une attaque similaire à celle que nous avons proposé sur FLIP. Cependant, la difficulté de la résolution des équations ne provient pas de leur degré, mais du trop petit nombre d'équations disponibles. Nous pouvons toutefois utiliser la technique qui permet un compromis entre la complexité en données et la complexité en temps dans l'attaque sur FLIP. Ceci conduit alors à une attaque sur ce PRG, avec la complexité de $\mathcal{O}(2^{\sqrt{n}})$, où n est la taille de la graine [CDM+18].

De plus, nous utilisons une autre technique qui utilise des dépendances particulières dans les équations, permettant de dériver un bien plus grand nombre d'équations linéairement indépendantes afin de pouvoir résoudre un système quadratique selon certaines conditions.

En combinant ces deux techniques, nous montrons qu'un niveau de sécurité minimal (par exemple 80 bits) dans le générateur de Goldreich impose une taille de graine très importante (au moins 10000 bits), ce qui rend l'utilisation de ce PRG très peu pratique, voire impossible.

Finalement, cette étude remet sévèrement en cause la sécurité du PRG de Goldreich qui reposait sur l'absence d'attaque en temps polynomial, puisque nous avons proposé un algorithme en temps sous-exponentiel qui s'avère extrêmement puissant pour des tailles "raisonnables". De plus, nous concluons à l'impossibilité de construire un générateur pseudo-aléatoire ayant une petite localité, c'est-à-dire dont la sortie ne dépend que de peu de bits de l'entrée, ce qui affine les connaissances sur cette construction théorique.

4 Analyse des LFSR filtrés par équivalence monomiale

De nombreux générateurs pseudo-aléatoires utilisent, pour leurs bonnes propriétés statistiques des registres à décalage à rétroaction linéaires (LFSR), qui sont les circuits qui engendrent des suites binaires régies par une relation de récurrence linéaire. Ces LFSR ne sont jamais utilisés seuls : on

applique à chaque instant à leur état interne une fonction booléenne non-linéaire comme décrit à la figure 2. Ces LFSR filtrés sont alors utilisés soit directement, comme dans Sfinks [BLM+05], soit

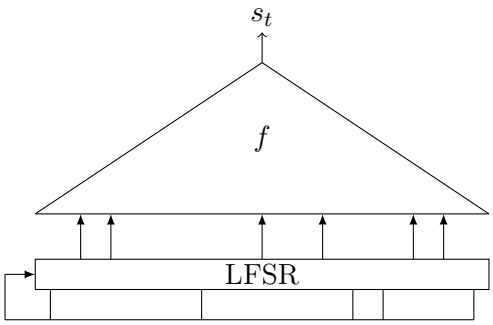

FIGURE 2 – Registre filtré.

le plus souvent comme partie d'un générateur pseudo-aléatoire plus sophistiqué. L'analyse de leur sécurité est donc essentielle. Les attaques les plus efficaces sont les attaques algébriques et leurs variantes [CM03 ; RH07 ; GRH+11] et les attaques par corrélation rapide [MS88]. Or, les registres à décalage à rétroaction linéaire possèdent une structure mathématique forte : si l'on identifie le contenu d'un registre de n bits à un élément du corps fini à 2^n éléments $\mathbb{F}_{2^n}$, la fonction de transition d'un LFSR correspond à la multiplication par un élément primitif donné α du corps fini.

Une équivalence non-linéaire. Dans ce qui suit, nous définissons l'équivalence non-linéaire décrite dans [RC10] car nous l'utiliserons pour monter une attaque sur les registres filtrés. Soit X_0 l'état initial du registre vu comme un élément du corps fini à 2^n éléments. Dans ces conditions, la suite binaire pseudo-aléatoire produite par le LFSR filtré par la fonction f est définie par

$$\forall t \geq 0, s_t = f(\alpha^t X_0) \ .$$

Considérons un entier k tel que $\text{pgcd}(k, 2^n - 1) = 1$. Le registre défini par le polynôme de rétroaction dont la racine est α^k, filtré par la fonction booléenne $g(X) = f(X^{k^{-1}})$ où k^{-1} est l'inverse de k mod $(2^n - 1)$ et initialisé avec $Y_0 = X_0^k$, est équivalent au registre initial filtré par f, dans le sens où les deux générateurs produisent exactement la même suite chiffrante, lorsque leurs états initiaux sont liés par la bijection $Y_0 = X_0^k$. Ainsi, on peut créer une relation d'équivalence entre des registres filtrés, que nous avons appelée équivalence monomiale, et l'attaquant peut choisir d'attaquer non pas le registre filtré initial, mais le plus faible (au regard des attaques classiques) dans la classe d'équivalence.

Nous avons donc étudié la complexité des deux grandes familles classiques, les attaques algébriques et les attaques par corrélation, afin de déterminer comment elle variait à l'intérieur d'une même classe d'équivalence monomiale [CR16].

La meilleure attaque algébrique connue consiste à résoudre un système linéaire de taille $\Lambda \times \Lambda$ où Λ est la complexité linéaire de la suite, *i.e.* la taille du plus petit LFSR qui l'engendre [GRH+11]. Nous prouvons que la notion d'équivalence monomiale entre les registres filtrés préserve la complexité linéaire. Autrement dit, la complexité des meilleures attaques algébriques ne peut être améliorée par l'équivalence monomiale.

Les attaques par corrélation rapides exploitent, elles, la faible distance de la fonction de filtrage à une fonction de degré 1 [MS88]. Les concepteurs de cryptosystèmes utilisent donc des fonctions de filtrage ayant une bonne non-linéarité, *i.e.* éloignée de toutes les fonctions affines. Toutefois, l'équivalence monomiale implique que le critère pertinent pour analyser la sécurité des LFSR filtrés n'est pas la non-linéarité de la fonction de filtrage mais bien la non-linéarité généralisée, définie comme la distance de f à l'ensemble de toutes les fonctions de la forme $\mathsf{Tr}(\lambda X^k)$ où k est premier avec $2^n - 1$ et Tr est l'application trace définie classiquement. De manière surprenante, le critère de non-linéarité généralisée avait été introduit en 2001 par Gong et Youssef [YG01] mais sans

la moindre motivation cryptographique, alors qu'ici, nous prouvons que cette quantité mesure directement la résistance à une attaque concrète.

Enfin, l'attaque par corrélation classique de Siegenthaler [Sie85] est une attaque de type "diviser pour mieux régner" sur des systèmes utilisant plusieurs LFSR. Elle ne se généralise donc pas au LFSR filtré qui comporte un unique registre car il n'est pas possible de retrouver une partie de l'état interne indépendamment du reste. Le principal résultat de mon travail sur les registres filtrés est de montrer comment on peut, contre toute attente, exploiter l'équivalence monomiale pour réaliser une attaque de type "diviser pour mieux régner" en présence d'un unique registre.

Au lieu d'exploiter une corrélation entre le générateur ciblé et un deuxième générateur défini par une racine primitive α^k avec $\text{pgcd}(k, 2^n - 1) = 1$, on utilise le fait que la sortie de notre générateur est corrélée avec la sortie d'un générateur (*cf.* figure 3) de polynôme de rétroaction P_{α^k} où k n'est plus premier avec $(2^n - 1)$. Ainsi, le nombre d'états internes possibles de ce deuxième générateur n'est plus $2^n - 1$ mais l'ordre multiplicatif τ_k de α^k.

Dans cette situation, on peut tester tous les τ_k états internes possibles du "petit" générateur, puisque cela coûte moins cher que la recherche exhaustive. On retrouve alors X_0^k, ce qui fournit $\log(\tau_k)$ bits d'information sur l'état initial. On peut d'ailleurs réaliser cette attaque avec plusieurs k premiers entre eux, et, à l'aide du théorème des restes chinois, retrouver l'état initial complet du générateur étudié. Nous parvenons donc à décomposer en plusieurs parties le contenu d'un unique registre en fonction des sous-groupes multiplicatifs de $\mathbb{F}_{2^n}$, afin de réaliser une attaque de type "diviser pour mieux régner".

FIGURE 3 – Attaque par corrélation généralisée quand $\text{pgcd}(k, 2^n - 1) > 1$.

5 De nouveaux critères de sécurité pour les fonctions de filtrage

Dans les systèmes de chiffrement à flot existants, le choix des fonctions booléennes de filtrage est régi par divers critères de sécurité qui portent sur la totalité de leur table de vérité. Par exemple, une fonction de filtrage doit être équilibrée, *i.e.* elle doit produire les valeurs 0 et 1 avec la même probabilité quand l'entrée décrit l'ensemble des mots de n bits. Ce critère garantit que la sortie d'un LFSR filtré est uniformément distribuée. Toutefois, ceci repose sur le fait que l'ensemble des états internes d'un LFSR est uniformément distribué. En revanche, dans FLIP, la fonction ne prend en entrée que des versions permutées d'un même mot de n bits (la clef). En particulier, toutes ses entrées possèdent le même poids de Hamming, *i.e.* le même nombre de 1. Ainsi, le fait que la fonction booléenne est équilibrée ne garantit aucunement que la sortie du générateur est uniformément distribuée. Par exemple, la fonction booléenne à 5 variables définie par $f(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2 + x_3 + x_4 + x_5$ est équilibrée sur $\mathbb{F}_2^5$, mais est constante dès que le poids de Hamming est fixé en entrée puisque $f(x) = \mathsf{w}_H(x) \mod 2$ où $\mathsf{w}_H(x)$ est le poids de Hamming de x.

Il en va de même pour les autres critères cryptographiques qui doivent être modifiés pour prendre en compte le fait que l'entrée de la fonction de filtrage est de poids de Hamming constant. Ainsi, avec Pierrick Méaux et Claude Carlet, nous avons analysé comment les propriétés cryptographiques classiques des fonctions booléennes [CMR17] (équilibre, non-linéarité et immunité algébrique) pouvaient se dégrader lorsque l'entrée des fonctions est restreinte à un sous-ensemble, et plus particulièrement

aux sous-ensembles composés des mots de n bits et de poids k : $S_{n,k} = \{x \in \mathbb{F}_2^n, \mathsf{w}_H(x) = k\}$.

Nous avons notamment construit des familles de fonctions équilibrées sur chaque sous-ensemble $S_{n,k}$. Ces fonctions n'existent que si tous les $S_{n,k}$ ont un cardinal pair, *i.e.* si n est une puissance de 2. Pour un nombre de variables quelconque, nous avons construit des fonctions presque parfaitement équilibrées au sens où le nombre de valeurs 0 et le nombre de valeurs 1 prises par la fonction sur chaque $E_{n,k}$ diffèrent au plus de 1.

Comme pour l'équilibre, la non-linéarité d'une fonction de filtrage (*i.e.* sa distance de Hamming aux fonctions affine) peut s'effondrer quand on se focalise sur les mots de poids constant. Nous avons par exemple mis en évidence des fonctions courbes (qui ont la meilleure non-linéarité classique possible) qui sont linéaires sur les mots de poids k. Nous avons trouvé des bornes sur la non-linéarité restreinte à des sous-ensembles pris arbitrairement ainsi que sur la non-linéarité restreinte aux $S_{n,k}$.

Le troisième critère important à prendre en compte lorsque l'on conçoit un nouveau système de chiffrement à flot est l'immunité algébrique de la fonction de filtrage f. Il s'agit du degré minimal d'une fonction booléenne h annulatrice de f, *i.e.* telle que $h(x)f(x) = 0$ pour tout $x \in \mathbb{F}_2^n$. Nous avons trouvé des bornes sur l'immunité algébrique quand la fonction est restreinte aux entrées d'un sous-espace S fixé, en utilisant les codes de Reed et Muller poinçonnés. Nous en déduisons par exemple que l'immunité algébrique de la restriction de f à $S_{n,k}$ est au plus égale plus petit entier e qui vérifie $2\binom{n}{e} > \binom{n}{k}$.

Plus généralement, cette étude a montré que les critères de sécurité classiques ne sont absolument pas pertinents dans le contexte de FLIP et qu'ils doivent être remplacés par d'autres propriétés. Nous avons notamment construit plusieurs familles de fonctions de filtrage appropriées qui assurent un excellent niveau de sécurité dans ce type de situations.

6 Comprendre les attaques par sous-ensembles invariant

Les travaux mentionnés précédemment exploitent des structures mathématiques dans les composantes de certains chiffrements à flot. Une autre partie de ma thèse porte sur la deuxième grande famille de chiffrements symétriques : les chiffrements par blocs.

De nombreux chiffrements par bloc légers ont déjà été proposés au cours des dernières années et la plupart d'entre eux suivent une construction itérative : ils itèrent une permutation relativement simple, en insérant après chaque itération une quantité secrète, appelée sous-clef, dérivée de la clef-maître de l'algorithme comme décrit à la figure 4.

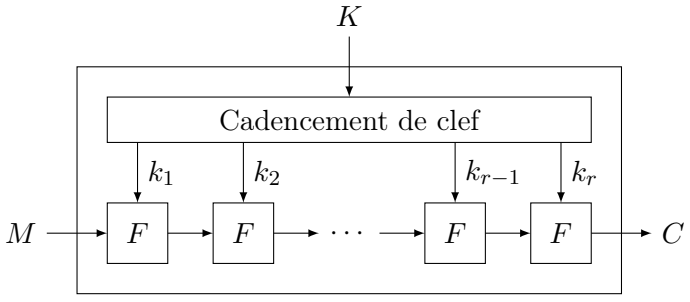

FIGURE 4 – Schéma d'un chiffrement par bloc E_K construit de manière itérative.

Une des spécificités des algorithmes légers est de dériver chaque clef de tour en additionnant la clef-maître à une constante. Cette simplicité dans le calcul des sous-clefs a cependant ouvert la voie à de nouvelles attaques, notamment les attaques par invariant [LAA+11] et leur généralisation [TLS16].

Le principe de ces attaques est de trouver un sous-ensemble des entrées du chiffrement, $\mathcal{S} \subset \mathbb{F}_2^n$, tel que la partition des entrées en $(\mathcal{S}, \mathbb{F}_2^n \backslash \mathcal{S})$ soit préservée, *i.e.*

$$E_K(\mathcal{S}) = \mathcal{S} \text{ ou } E_K(\mathcal{S}) = \mathbb{F}_2^n \backslash \mathcal{S} \ .$$

Les clefs K vérifiant cette propriété sont alors des clefs faibles. Le cas particulier où $\mathcal{S}$ est un sous-espace vectoriel correspond à l'attaque par sous-espace invariant [LAA+11]. Si le sous-ensemble est un sous-ensemble invariant par la partie non-linéaire et par la partie linéaire de la fonction itérée, et qu'il est invariant par l'addition de chaque clef de tour, alors il sera invariant pour tout le chiffrement.

Les travaux que j'ai menés avec Anne Canteaut et Christof Beierle et Gregor Leander de l'université de Bochum (Allemagne) [BCL+17] sur le sujet m'ont permis de caractériser les propriétés mathématiques de la partie linéaire de la fonction itérée et des constantes de tour qui permettent d'éviter cette attaque. Nous avons montré que l'existence d'une attaque par invariant est étroitement liée à la dimension de l'espace $W_L(c_1, \ldots, c_t)$ défini comme le plus petit espace vectoriel invariant par L qui contient toutes les différences $c_1, \ldots, c_t$ entre les constantes de tour. En particulier, si cet espace couvre $\mathbb{F}_2^n$, alors on peut conclure à l'absence de sous-ensembles invariants, conclusion à laquelle nous avons pu aboutir pour un grand nombre de chiffrements.

Si nous nous plaçons du point de vue du concepteur, nous cherchons à construire un chiffrement sans invariant et donc à trouver une fonction L et des éléments $c_1, \ldots, c_t$ (correspondant aux différences entre les constantes de tour) qui maximisent la dimension de $W_L(c_1, \ldots, c_t)$. Nous avons montré que cette dimension est conditionnée par la forme canonique rationnelle de la matrice représentant L où L est la couche linéaire de la fonction itérée. En effet, pour toute fonction linéaire L de $\mathbb{F}_2^n$, il existe une base de $\mathbb{F}_2^n$ dans laquelle L a la forme suivante :

$$\begin{pmatrix} C(Q_r) & & & \\ & C(Q_{r-1}) & & \\ & & \ddots & \\ & & & C(Q_1) \end{pmatrix}$$

où les $C(Q_i)$ sont des matrices compagnons de polynôme Q_i, avec $Q_r \mid Q_{r-1} \mid \cdots \mid Q_1$ et le polynôme Q_1 est égal au polynôme minimal de L. Les polynômes Q_i sont appelés facteurs invariants de L. Nous avons en effet prouvé que la plus grande dimension atteignable pour $W_L(c_1, \ldots, c_t)$, avec $(t+1)$ constantes de tour, est égale à la somme des degrés des t premiers facteurs invariants de L :

$$\max_{c_1,\ldots,c_t \in \mathbb{F}_2^n} \dim W_L(c_1, \ldots, c_t) = \sum_{i=1}^{t} \deg Q_i$$

Il s'ensuit que le degré du polynôme minimal de la fonction linéaire L et le nombre de facteurs invariants sont des paramètres essentiels pour la sécurité quand les sous-clefs sont obtenues par addition de la clef-maître avec une constante de tour. C'est la première fois que cette propriété mathématique de la fonction linéaire apparaît dans une analyse de sécurité : nos travaux sont donc à l'origine d'un nouveau critère désormais utilisé pour tous les nouveaux chiffrements par bloc légers.

7 Cryptanalyse de chiffrements authentifiés soumis la standardisation

L'intérêt du chiffrement authentifié (qui assure l'authenticité des messages) a grandi dans la communauté cryptographique ces dernières années, avec pour conséquence la tenue de la compétition CAESAR, ayant pour but de sélectioner les meilleurs algorithmes de chiffrement authentifiés, proposés par l'ensemble de la communauté cryptographique internationale et qui est censée se terminer par l'annonce des vainqueurs à la fin de l'année.

KETJE [BDP+14] est un chiffrement authentifié proposé par les auteurs du standard de hachage SHA-3 [BDP+13] et inspiré de ce dernier. Sans rentrer dans les détails, KETJE suit une construction itérative appelée éponge qui absorbe une partie du message clair et produit une partie du chiffré à chaque tour. Pour un état interne secret de 200 bits, nous avons accès à une partie

de l'information sur cet état après chaque application de la fonction de tour. L'attaque consiste à récupérer l'information issue de l'état interne à des instants différents et à combiner cette information intelligemment de manière à en déduire la valeur complète de l'état à un instant donné. Dans le cas de KETJE, nous parvenons dans un premier temps à exploiter de l'information sur deux tours consécutifs et dans un second temps, nous utilisons des techniques non-triviales d'algorithmes de fusion de listes, en criblant avec des équations non-linéaires pour exploiter de l'information sur 3 tours consécutifs.

Notre cryptanalyse [FNR18] s'applique à une version affaiblie de KETJE dans laquelle le *ratio* (paramètre critique de la construction en éponge) est augmenté (32 ou 40 bits au lieu de 16). Si elle ne contredit pas la sécurité revendiquée par les concepteurs, notre attaque apporte un éclairage nouveau sur KETJE car elle met en évidence une faiblesse jusqu'ici non exploitée, issue de la possibilité d'obtenir des équations creuses.

MORUS [WH14] est aussi un chiffrement authentifié et fait partie des finalistes de la compétition CAESAR. Nous avons décrit un distingueur sur les chiffrés seuls produits par cet algorithme de chiffrement [AEL+18]. Plus précisément, nous avons trouvé une combinaison linéaire des chiffrés qui admet un biais de 2^{-76}, indépendamment de la clef, ce qui constitue une attaque dans un modèle de multi-utilisateurs.

8 Conclusion et perspectives

L'ensemble de mes travaux montre qu'une vision structurelle des objets mathématiques mis en jeu dans les systèmes cryptographiques peut avoir un apport important en cryptanalyse. Cette vision permet de découvrir de nouvelles attaques et de mettre en évidence des nouveaux critères de conception. Il est donc nécessaire de faire des allers-retours entre la conception de chiffrements, la cryptanalyse et les notions mathématiques fondamentales exploitées dans les attaques afin de déterminer précisément le niveau de sécurité pratique des algorithmes de chiffrement.

En particulier, les différentes études menées pendant ma thèse mettent bien en évidence la fragilité des systèmes utilisant des objets mathématiques possédant une représentation très structurée. Par exemple, nous avons attaqué des générateurs pseudo-aléatoires comme FLIP ou le PRG de Goldreich en tirant partie d'équations multivariées creuses, alors que nos attaques sur les LFSR filtrés exploitent le caractère creux de la représentation univariée du polynôme employé. La représentation multivariée regarde l'espace d'entrée comme un espace vectoriel, alors que la représentation univariée l'identifie à un corps fini de caractéristique 2. Ces représentations sont naturellement liées, mais les équations peuvent être creuses dans un cas, et denses dans l'autre, ce qui montre que les deux approches ne captent pas le même phénomène. Cette multiplicité des représentations possibles ouvre un vaste potentiel de recherche. On peut par exemple s'interroger sur la pertinence d'éventuelles représentations intermédiaires fondées sur des sous-corps de $\mathbb{F}_2^n$, par exemple l'utilisation de polynômes bivariés à coefficients dans $\mathbb{F}_2^{n/2}$ quand n est pair, plutôt que de polynômes univariés à coefficients dans $\mathbb{F}_2^n$.

Par ailleurs, le lien entre les différentes représentations des fonctions booléennes n'est pas bien compris et est un sujet difficile d'autant plus que la cardinalité des ensembles (le nombre de fonctions booléennes à n variables est 2^{2^n}) interdit toute recherche exhaustive au-delà de 6 variables.

Références

[BDP+13] Guido Bertoni, Joan Daemen, Michael Peeters et Gilles Van Assche. "Keccak". In : *EUROCRYPT 2013*. Sous la dir. de Thomas Johansson et Phong Q. Nguyen. T. 7881. LNCS. Springer, Heidelberg, mai 2013, p. 313–314.

[BDP+14] Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche et Ronny Van Keer. "Ketje v1". In : *Soumission à la compétition CAESAR* (2014).

[BLM+05] A. Braeken, J. Lano, N. Mentens, B. Preneel et I. Verbauwhede. *SFINKS : a synchronous stream cipher for restricted hardware environments*. Soumission au projet eSTREAM. `http://www.ecrypt.eu.org/stream/`. 2005.

[CM03] Nicolas Courtois et Willi Meier. "Algebraic Attacks on Stream Ciphers with Linear Feedback". In : *EUROCRYPT 2003*. Sous la dir. d'Eli Biham. T. 2656. LNCS. Springer, Heidelberg, mai 2003, p. 345–359.

[Gol00] Oded Goldreich. *Candidate One-Way Functions Based on Expander Graphs*. Cryptology ePrint Archive, Report 2000/063. `http://eprint.iacr.org/2000/063`. 2000.

[GRH+11] Guang Gong, Sondre Rønjom, Tor Helleseth et Honggang Hu. "Fast Discrete Fourier Spectra Attacks on Stream Ciphers". In : *IEEE Trans. Information Theory* 57.8 (2011), p. 5555–5565.

[LAA+11] Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi et Erik Zenner. "A Cryptanalysis of PRINTcipher : The Invariant Subspace Attack". In : *CRYPTO 2011*. Sous la dir. de Phillip Rogaway. T. 6841. LNCS. Springer, Heidelberg, août 2011, p. 206–221.

[MJS+16] Pierrick Méaux, Anthony Journault, François-Xavier Standaert et Claude Carlet. "Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts". In : *EUROCRYPT 2016, Part I*. Sous la dir. de Marc Fischlin et Jean-Sébastien Coron. T. 9665. LNCS. Springer, Heidelberg, mai 2016, p. 311–343.

[MS88] Willi Meier et Othmar Staffelbach. "Fast Correlation Attacks on Stream Ciphers (Extended Abstract)". In : *EUROCRYPT'88*. Sous la dir. de C. G. Günther. T. 330. LNCS. Springer, Heidelberg, mai 1988, p. 301–314.

[RC10] Sondre Rønjom et Carlos Cid. "Nonlinear Equivalence of Stream Ciphers". In : *FSE 2010*. Sous la dir. de Seokhie Hong et Tetsu Iwata. T. 6147. LNCS. Springer, Heidelberg, fév. 2010, p. 40–54.

[RH07] Sondre Rønjom et Tor Helleseth. "A New Attack on the Filter Generator". In : *IEEE Trans. Information Theory* 53.5 (2007), p. 1752–1758.

[Sha49] C. Shannon. "Communication Theory of Secrecy Systems". In : *Bell System Technical Journal, Vol 28, pp. 656715* (1949).

[Sie85] Thomas Siegenthaler. "Decrypting a class of stream ciphers using ciphertext only". In : *IEEE Trans. Computers* C-34.1 (1985), p. 81–84.

[TLS16] Yosuke Todo, Gregor Leander et Yu Sasaki. "Nonlinear Invariant Attack - Practical Attack on Full SCREAM, iSCREAM, and Midori64". In : *ASIACRYPT 2016, Part II*. Sous la dir. de Jung Hee Cheon et Tsuyoshi Takagi. T. 10032. LNCS. Springer, Heidelberg, déc. 2016, p. 3–33.

[WH14] Hongjun Wu et Tao Huang. "MORUS". In : *Soumission à la compétition CAESAR* (2014).

[YG01] Amr M. Youssef et Guang Gong. "Hyper-bent Functions". In : *EUROCRYPT 2001*. Sous la dir. de Birgit Pfitzmann. T. 2045. LNCS. Springer, Heidelberg, mai 2001, p. 406–419.