Université de Versailles Saint-Quentin Laboratoire de Recherche en Informatique

École doctorale
SOFT

T H È S E

présentée pour obtenir le grade de

Docteur de l'Université de Versailles

Laboratoire PR*i*SM
Spécialité : Informatique

soutenue publiquement par

Joana Treger

Étude de la Sécurité de Schémas de Chiffrement par Bloc et de Schémas Multivariés

Le 28 Juin, 2010

Jury :

Rapporteurs :	Henri Gilbert	-	Orange Labs
	David Naccache	-	ENS
Examinateurs :	Jean-Sébastien Coron	-	Université du Luxembourg
	Pierre-Alain Fouque	-	ENS
	Éliane Jaulmes	-	ANSSI
	Antoine Joux	-	DGA et UVSQ
Directeur de thèse :	Jacques Patarin	-	UVSQ

Université de Versailles Saint-Quentin Laboratoire de Recherche en Informatique

École doctorale
SOFT

T H È S E

présentée pour obtenir le grade de

Docteur de l'Université de Versailles

Laboratoire PR*i*SM
Spécialité : Informatique

soutenue publiquement par

Joana Treger

Étude de la Sécurité de Schémas de Chiffrement par Bloc et de Schémas Multivariés

Le 28 Juin, 2010

Jury :

Rapporteurs :	Henri Gilbert	-	Orange Labs
	David Naccache	-	ENS
Examinateurs :	Jean-Sébastien Coron	-	Université du Luxembourg
	Pierre-Alain Fouque	-	ENS
	Éliane Jaulmes	-	ANSSI
	Antoine Joux	-	DGA et UVSQ
Directeur de thèse :	Jacques Patarin	-	UVSQ

Remerciements

Mes premiers sentiments de reconnaissance vont à Jacques Patarin. Je tiens à le remercier d'avoir accepté d'être mon directeur de thèse et de m'avoir fait confiance dès le départ de cette course un peu folle. Merci de m'avoir très vite introduite au sein de la communauté scientifique. Merci à lui d'avoir partagé ses idées et de m'avoir guidée dans mes travaux. Une deuxième vague de reconnaissance va à Antoine Joux. Merci pour sa disponibilité, sa maîtrise et son enthousiasme contagieux pour (presque) tous les sujets en cryptologie. Je le remercie sincèrement de m'avoir encadrée, parallèlement à Jacques, et pour ses conseils durant ces années de thèse, notamment vers la fin.

Je souhaite ensuite remercier très chaleureusement chacune des personnes constituant mon jury. Tout d'abord, "chapeau" à mes deux rapporteurs Henri Gilbert et David Naccache, qui ont accepté cette tâche malgré leur emploi du temps plus que chargé. Merci à David, d'avoir accepté *in extremis* d'être mon rapporteur, puis d'avoir réussi à fournir son rapport dans la semaine suivante. Je lui en suis extrêmement reconnaissante. Merci à Henri d'avoir accepté d'être mon rapporteur alors qu'il était déjà très pris avec l'organisation d'Eurocrypt, je sais qu'il n'a lui aussi eu que très peu de temps pour faire le rapport et l'en remercie. Je le remercie également pour ses corrections qui m'ont quelques fois donné le sourire. Merci donc à eux de me faire l'honneur d'être dans mon jury, mais également à tous les autres membres. Je suis notamment très heureuse de pouvoir compter parmi eux Pierre-Alain Fouque, et garderai à l'esprit son attention et la manière dont il s'est occupé de l'organisation de ma soutenance à l'ENS. Merci à Éliane Jaulmes de me faire le plaisir de sa présence. Je la remercie aussi de m'avoir acceptée au sein de son équipe à l'ANSSI, avant même la finalisation de ma thèse. Je suis également très touchée que Jean-Sébastien Coron ait accepté de faire partie de mon jury de thèse et le remercie d'avoir fait le déplacement. Merci à nouveau infiniment à Antoine et Jacques, cette fois-ci pour venir compléter ce remarquable jury de thèse.

Je tiens à remercier tous ceux que je n'ai pas encore mentionné mais avec qui j'ai eu l'honneur et le plaisir de travailler. Dans l'ordre d'apparition : merci à Ludovic, qui m'a suivie depuis mon stage de Master, et pour son "In Gröbner bases we trust !" qui m'a marquée. Merci de rendre la collaboration si facile et si agréable, merci pour les cafés les repas dans sa super cantine. Merci à Olivier, pour son initiation à Magma et ses conseils, à Valérie et à Emmanuel, pour nos moments de panique avec la date d'envoi de Crunch ou autres serveurs de soumission. Je pense bien sûr également à Charles et encore une fois à Pierre-Alain, pour nos réunions motivées sur le thème "cassage de HFE", et avec qui j'ai énormément apprécié de travailler. Je remercie enfin encore Jean-Charles, Benjamin et Michaël, avec qui j'ai eu le privilège d'interagir également.

De tout coeur merci à tous ceux qui ont eu la gentillesse de me prêter main forte pour la relecture et la mise en forme du présent manuscrit. Merci notamment à Jean-Michel, qui a été le premier à se dévouer, Vanessa, pour nos discussions animées sur les bases de Gröbner, María, pour avoir relu toute une partie de la thèse *et* y

avoir pris du plaisir, Jean-René, pour ses remarques pertinentes, Thomas, pour sa relecture de dernière minute, et Fabien, pour ses scripts pour ma bibliographie. Je souhaite remercier très particulièrement Cédric, dont l'activité n'a rien à voir avec la cryptologie, mais qui a lu et relu minutieusement et avec beaucoup d'enthousiasme les points que je lui demandais et même au-delà. Enfin, un grand merci à Marcio pour avoir passé des soirées et des week-ends à faire à ma place le travail le plus ennuyeux : la mise en page, la correction des typos, des références, des citations,... Tout ce monde a largement contribué à rendre ce manuscrit de qualité meilleure qu'il n'aurait jamais pu l'être sans eux.

Ces années de thèse n'auraient pas été pareilles sans tous les membres du laboratoire PR*i*SM, passés ou présents. Je commence par ma "co-bureau" ou plutôt "co-bureaux" Sorina. Merci d'avoir rendu notre environnement scientifique (beaucoup) plus familier. Merci d'être la meilleure à la guerre des bureaux qui aura marqué beaucoup d'esprits (spéciale dédicace à Thierry), j'étais très fière d'être sa co-équipière. Merci ensuite à tout le reste de l'équipe crypto : Aurélie qui est passée la première et nous a tous accueillis et aidés comme une grande soeur et a continué de me faire bénéficier de son expérience lors des derniers préparatifs, Jean-Michel, pour aller plus souvent en Alsace que moi et me rapporter un peu de ma région à Versailles, Vanessa, pour l'énergie avec laquelle elle est arrivée (et sa carte de piscine), Anja, pour toutes ses invitations à danser la salsa, Bastien, Guilhem, Peter et Malika, les derniers arrivés, qui ont contribué à la bonne ambiance de l'équipe et du labo. Merci également aux permanents que je n'ai pas encore cités, Louis et Michaël, pour leur efficacité au quotidien, leur aide et leur disponibilité. Je ne peux oublier de mentionner tous les membres de l'équipe arch. Je commence par William, qui a accueilli notre équipe un peu comme la sienne. Merci pour son aide à plusieurs reprises, pour sa distribution de pruneaux ou de tomates. Merci aux anciens, Patrick, Jean. Je souhaite remercier en particulier à Seb, pour ses dépannages informatiques, son initiation au tennis, ses fausses dédicaces de Nadal, et je m'arrête là sinon je vais me mettre à écrire autant que lui. Merci à Andrès, pour nos échanges... de balles et nos visionnements de quelques moments forts de l'ATP tour. Merci à ceux de passage, et aux actuels : David, Emmanuel, Cédric, ou encore Bettina (mon autre "co-bureau"). Je remercie en particulier Stéphane, qui a pris le relais de Seb pour les dépannages informatiques et à qui j'ai donné beaucoup de travail. Je le remercie également pour sa disponibilité et ses explications ultra passionnées lorsqu'il s'agit d'informatique ou de code C. Enfin, merci à Souad, qui est tellement plus qu'une collègue, merci pour nos repas partagés, et pour tout le reste. Quitter Versailles a rimé pour moi avec mon arrivée à l'ANSSI. Je tiens vraiment à remercier chaleureusement toute l'équipe (et même au-delà, mais je ne peux malheureusement pas citer tout le monde) de m'avoir acceptée et de m'avoir autorisée à la finaliser ma thèse là-bas. Merci notamment à Florent, Loïc, Éliane, Jean-René, Thomas, Marion et Karim pour leur accueil chaleureux ou leurs conseils précieux de pré-soutenance.

Merci également à toutes les personnes, collègues de crypto ou non, qui ont agrémenté mes semaines durant la thèse (surtout les lundis), et permis de gagner des accessoires inoubliables... Merci à Los Pumas ! Pour citer quelques noms : Bea,

Chris, Yann, Andrea, Lore, Gaëtan, Céline, Anne, Stéphane, Christina, María, Fab, Sylvain, Isabelle. Merci tout particulièrement à María pour trop de choses, qu'elles soient en rapport avec la thèse ou pas ; j'ai eu beaucoup de chance de tomber sur elle en arrivant à Paris. Merci à la plupart de Los Pumas d'avoir transformé les soirées de conférences ou rencontres scientifiques en des moments inoubliables. J'ai en tête notamment les journées C2, avec les parties de loup-garou, de mime, et le poulet rôti de Bordeaux. Merci à Iwen, Léo, Ayoub, Fabien, Christophe, Céline, Manuel, Nicolas, Nadya, Yannick, Thomas et tous ceux que j'ai déjà cités ou que j'oublie, d'avoir contribué à certains de ces moments.

Une pensée particulière va à ma famille entière. Je les remercie d'avoir été là pour moi, de m'avoir poussée et d'avoir cru en moi. Merci à mes parents Liliane et Hubert d'avoir compris mes nombreuses absences aux repas de famille, mes absences lors des conversations téléphoniques parfois également. Merci à ma soeur Cynthia d'être là, toujours et quoi qu'il arrive. Merci à mes grand-parents Madeleine, Georges, Cécile et Albert de s'être intéressés et d'avoir fait l'effort tant de fois d'essayer de comprendre en quoi consistent mes travaux de thèse. Une pensée très spéciale va à mes grand-pères, qui m'auront vu commencer cette thèse, mais n'auront pas eu le plaisir de me voir la terminer.

Enfin, parce qu'il le mérite vraiment, merci encore à Marcio. Merci pour son aide qui m'a épargné bien des journées de travail, mais pour tellement plus encore : merci pour le scooter (!), merci d'avoir supporté mes humeurs (trop) variables pendant la thèse et surtout pendant la rédaction, merci pour ses leçons de positivisme... Valeu gatinhu !

J'ai sûrement oublié l'une ou l'autre personne dans ces remerciements, tant j'ai été bien entourée durant ces années. Je crois que si je le pouvais, je rajouterais sans doute encore plusieurs noms... Que ces dernières lignes puissent tenir lieu de sincères excuses auprès de tous ces oubliés et qu'ils trouvent ici le témoignage de ma reconnaissance.

Abstract :

The thesis focuses on the security of block ciphers and multivariate schemes.

In the first part, we study Feistel networks with internal permutations and Misty-like schemes, which are both involved in the design of many symmetric algorithms. The study is made in a generic context, which means that the internal permutations are supposed random. This allows to exhibit properties of the schemes' structure, without taking into account eventual weaknesses of the internal permutations. This part focuses on generic attacks on these schemes, and is related to the series of works done by Patarin *et al.* on similar structures. We consider attacks that allow to distinguish with high probability one scheme or the other from a random permutation. Different types of attacks are studied for the first rounds (*e.g.* two points, three points or four points attacks), then, we extend the two points attacks for any number of rounds, thanks to Patarin's H-coefficient technique.

The second part of the thesis deals with multivariate cryptosystems. Two schemes are studied in particular : the so-called HM scheme ("Hidden Matrix" scheme) and the HFE scheme ("Hidden Field Equations"), both designed by Patarin in 1998 and 1996 respectively. For HM, we exhibit a special property of the differential of the public key, which gives an efficient distinguisher between the system of equations forming the public key and a random system of equations. Moreover, the use of Gröbner bases (in particular, MAGMA's implementation of Faugère's F_4 algorithm) allows to efficiently invert the public key in polynomial time, for any practical paremeters. We also study the equations involved in such a Gröbner based attack. More precisely we show that many low-degree polynomials appear during the computation, which mostly explains the good behaviour of the Gröbner bases algorithms. Finally for HFE, we describe a key-recovery attack that affects a whole family of special instances, and whose complexity comes down to solving one instance of the IP problem. These weak instances are the polynomials with coefficients in the base field. They happen to offer a commutation property with the Frobenius map, allowing our attack to work.

Keywords : block cipher, Feistel cipher, MISTY, generic attacks, two-point attacks, H coefficients, multivariate cryptology, HM scheme, HFE, Gröbner bases, cryptanalysis.

Résumé :

La thèse se concentre sur l'étude de la sécurité de schémas de chiffrement par blocs, et de schémas multivariés.

Dans la première partie, nous nous intéressons à l'étude de schémas de chiffrement par blocs, notamment les schémas de Feistel avec permutations internes et les schémas du type Misty, impliqués dans la conception de plusieurs algorithmes symétriques. Le cadre de l'étude faite est générique, dans le sens où les permutations internes sont supposées aléatoires. Ceci nous permet d'obtenir des propriétés de la structure même des schémas, sans prendre en compte leur contexte d'utilisation. Cette partie se concentre sur des attaques génériques contre ces deux schémas et fait écho aux travaux de Patarin *et al.* sur des schémas apparentés. Les attaques considérées sont des attaques permettant de distinguer avec forte probabilité l'un ou l'autre des deux schémas d'une permutation purement aléatoire. Nous nous penchons sur différents types d'attaques pour les premiers tours (attaques deux points, trois points et quatre points), puis nous étendons les attaques deux points grâce à la technique des coefficients H de Patarin pour un nombre de tours quelconque.

La deuxième partie de la thèse concerne l'étude de cryptosystèmes multivariés. Nous étudions deux schémas : le schéma HM ("Hidden Matrix") et le schéma HFE ("Hidden Field Equation"), tous deux concus par Patarin en 1998 et 1996 respectivement. Concernant HM, nous mettons en évidence une propriété de la différentielle de la clé publique fournissant un distingueur efficace entre la clé publique du schéma et un système aléatoire d'équations. Par ailleurs, nous montons une attaque par bases de Gröbner, utilisant les implantations sous MAGMA de l'algorithme F_4 de Faugère, permettant d'inverser le système d'équations formant la clé publique efficacement en pratique. Nous accompagnons nos observations expérimentales d'éléments théoriques, notamment, nous montrons l'apparition de plusieurs polynômes de bas degré au cours du calcul d'une base de Gröbner. Pour ce qui est de HFE, nous exposons une attaque permettant le recouvrement de la clé privée pour une famille d'instances particulières, dont la complexité se ramène à la résolution d'une instance du problème IP. Ces instances faibles sont les polynômes HFE à coefficients dans le corps de base. Ces polynômes vérifient une propriété de commutativité avec le morphsisme de Frobenius, à la base de notre attaque.

Mots clés : chiffrement par bloc, schémas de Feistel, MISTY, attaques génériques, attaques deux points, coefficients H, cryptologie multivariable, schéma HM, HFE, bases de Gröbner, cryptanalyse.

Table des matières

Table des figures

Liste des tableaux

Notations et Définitions

$\mathcal{M}_n(K)$	Anneau de matrices carrées de taille n à coefficients dans K.
$\mathrm{GL}_n(k)$	Sous-groupe multiplicatif de $\mathcal{M}_n(K)$ des matrices invisibles.
$\mathbb{F}_q$	Corps fini à q éléments
$\mathbb{Z}$	Ensemble des entiers relatifs
$\mathbb{N}$	Ensemble des entiers naturels
I_n	Mots de n bits, $I_n = \{0,1\}^n$
F_n	Ensemble dans applications de I_n dans I_n
B_n	Ensemble de permutations de I_n
$\oplus$	Addition bit à bit, addition dans $\mathbb{F}_2$
$\circ$	Composition de fonctions
$[L,R]$	Concaténation du mot L et du mot R
φ	Indicatrice d'Euler qui à un entier strictement positif n associe le nombre d'entiers positifs inférieurs à n et premiers avec n.

Première partie

AUTOUR DES SCHÉMAS DE FEISTEL ET DE MISTY

Chapitre 1

Schémas de Feistel avec Permutations Internes et Schémas du type Misty, Attaques Génériques et Attaques Deux Points

Sommaire

1.1 Les schémas de Feistel avec permutations internes

1.1.1 Introduction générale

Les schémas de Feistel ont été introduits afin de construire des permutations de $\{0,\ldots,2^{2n}-1\}$ à partir de fonctions sur des ensembles plus petits, typiquement $\{0,\ldots,2^n-1\}$. Ces fonctions sur $\{0,\ldots,2^n-1\}$ sont usuellement appelées *fonctions internes*. Composer plusieurs schémas de Feistel utilisant des fonctions internes indépendantes, ce que l'on appelle considérer plusieurs tours de schémas de Feistel, permet de construire des permutations pseudo-aléatoires. Ceci explique l'utilisation intensive des schémas de Feistel en cryptologie symétrique, qui se trouvent être la base de nombreux schémas (par exemple, le DES). La figure 1.1 représente un tour de schéma de Feistel.

Luby et Rackoff ont initialisé les travaux de recherche sur ces schémas de Feistel [LR88], lorsque les fonctions internes sont aléatoires. Suivent nombreux résultats, tant sur ces schémas de Feistel, dits "classiques" que sur des schémas de Feistel "modifiés". Par exemple, des résultats de [Jut98], Schneier et Kelsey [SK96], et de Patarin

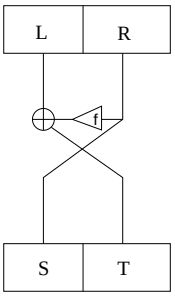

FIGURE 1.1: Schéma de Feistel avec fonction interne f. Message d'entrée $[L, R]$, message de sortie $[S, T]$.

et Nachef [PNB06b] traitent des schémas de Feistel dissymétriques avec fonctions internes expansives. Par ailleurs, Patarin *et al.* se sont intéressés aux schémas de Feistel dissymétriques avec fonctions contractantes [PNB06a]. Une autre construction consiste à considérer des schémas de Feistel dissymétriques, où certains tours sont expansifs et certains contractants, comme il fait usage dans Bear ou Lion [AB96].

Une autre construction se rapportant aux schémas de Feistel originels est celle des schémas de Feistel avec permutations internes. Ceux-ci sont utilisés dans de nombreux schémas, comme Twofish [Nyb96], Camellia [AIK+00] ou encore DEAL [Knu98]. Cependant, peu de résultats concernant ces schémas de Feistel particuliers se trouvent dans la littérature. Knudsen [Knu02] présente une attaque sur cinq tours de schémas de Feistel avec permutations internes, basée sur une différentielle impossible (pour deux entrées/sorties, certaines relations entre les blocs ne peuvent arriver). Plus récemment, Piret s'est intéressé dans [Pir06] aux preuves de sécurité de ces schémas de Feistel avec permutations internes pour trois et quatre tours. Pourtant, l'utilisation de *permutations internes* plutôt que de fonctions influence l'étude de ces schémas. Par exemple, Rijmen *et al.* exposent une attaque fonctionnant dans le cas de schémas de Feistel dont les fonctions internes présentent de mauvaises propriétés de surjectivité [RPW97]. Une autre illustration de ce fait se trouve dans [Bih97], où est exposée une attaque exploitant la bijectivité des fonctions internes.

Nous allons nous intéresser, entre autres, aux schémas de Feistel sur $\{0, \ldots, 2^{2n} - 1\}$, utilisant des permutations internes de $\{0, \ldots, 2^n - 1\}$, et plus précisément aux attaques génériques sur ces schémas. Ces attaques sont des attaques fonctionnant dans le cas générique où les permutations internes sont aléatoires [TP09]. Une description plus détaillée de ces attaques génériques est donnée à la section 1.3.

1.1.2 Définition des schémas de Feistel et propriétés élémentaires

Pour les notations utilisées, nous renvoyons vers la partie "Notations".

Définition 1 (Un tour de schéma de Feistel avec permutation interne)

Soit $f \in B_n$ et $L,\ R,\ S,\ T \in I_n$. La permutation ψ, définie par :

$$\psi(f)([L, R]) = [R, L \oplus f(R)],$$

est appelée un tour de schéma de Feistel avec permutation interne f.

Remarque : Lorsque la permutation interne impliquée est claire, ou lorsque nous parlons du schéma de manière générale, nous notons simplement ψ. Notons encore que nous ne considérons dans cette première partie que des schémas dont les permutations internes sont aléatoires. Par suite, lorsque nous faisons usage de la notation ψ, sauf mention contraire, nous supposons la permutations interne aléatoire.

La permutation ψ est représentée à la figure 1.1 de la sous-section précédente. Pour se convaincre que ψ est une permutation, il suffit de remarquer que $\psi([T, S]) = [R, L]$. Ainsi, en notant σ la permutation des deux blocs de taille n d'un message de taille $2n$, nous avons :

$$\psi^{-1} = \sigma \circ \psi \circ \sigma,$$

ce qui est résumé par la figure 1.2.

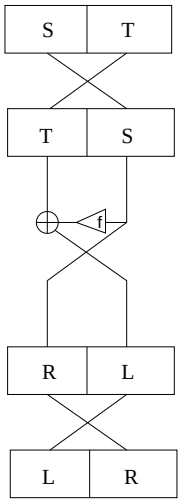

FIGURE 1.2: Inverse d'un schéma de Feistel, ψ^{-1}. Message d'entrée $[S, T]$, message de sortie $[L, R]$.

Nous introduisons également la définition suivante, correspondant aux représentations de la figure 1.3 :

Définition 2 (k tours de schéma de Feistel avec permutations internes) *Soit $(f_1, \ldots, f_k) \in B_n^k$ et $L,\ R \in I_n$. La permutation ψ^k pour $k \geq 1$, définie par :*

$$\psi^k(f_1, \ldots, f_k)([L, R]) = \psi(f_k) \circ \cdots \circ \psi(f_1)([R, L]),$$

est appelée k tours de schémas de Feistel avec permutations internes $(f_1, \ldots, f_k)$.

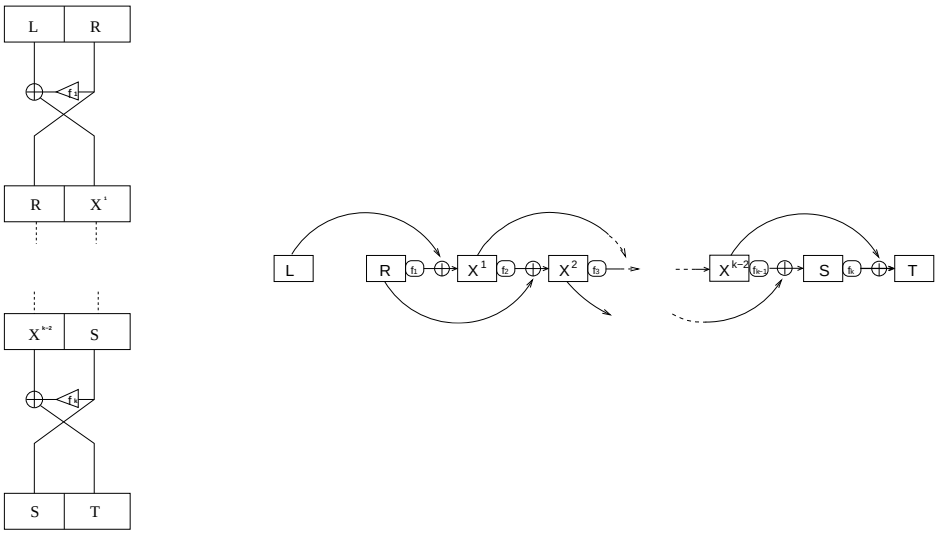

FIGURE 1.3: $\psi^k(f_1, \ldots, f_k)([L, R]) = [S, T]$.

Remarque : Ici encore, nous pouvons appeler cette permutation ψ^k sans spécifier les permutations internes. Sauf mention contraire, ψ^k désigne k tours de schémas de Feistel avec permutations internes aléatoires.
La représentation usuelle des schémas de Feistel est celle de gauche dans la figure 1.3. Cependant, avec cette représentation, les nouveaux blocs apparaissant lors du calcul d'un message sont représentés deux fois chacun. La représentation de droite de la figure 1.3 a l'avantage de mettre en évidence uniquement le nouveau bloc apparaissant à chaque tour. Notre analyse étudiant différentes configurations pour ces blocs (dits internes), nous donnons systématiquement la préférence à cette représentation moins classique.
La sortie de tels schémas sera appelée $[S, T]$.

1.2 Les schémas du type Misty

1.2.1 Introduction générale

La manière la plus répandue de construire des permutations pseudo-aléatoires à partir de fonctions aléatoires ou pseudo-aléatoires, opérant généralement sur un ensemble plus petit, est de considérer plusieurs tours de schémas de Feistel (voir section 1.1). Cependant, il existe d'autres constructions permettant d'obtenir des permutations pseudo-aléatoires, comme par exemple le schéma de Massey et Lai utilisé dans IDEA [LM91], toutes les variantes des schémas de Feistel, ou encore les schémas utilisés dans Misty [Mat97]. Ceux sont ces derniers qui font l'objet d'une étude particulière dans cette partie I, avec les schémas de Feistel avec permutations internes. Il y a deux schémas du type Misty (Misty L et Misty R), représentés à la figure 1.4.

FIGURE 1.4: Schémas Misty L (à gauche) et Misty R (à droite). Message d'entrée $[L, R]$, message de sortie $[S, T]$.

La structure de ces schémas est utilisée dans schéma de chiffrement par blocs de Matsui [Mat97], tout comme dans la variante de Kasumi [Ka], adoptée comme standard de chiffrement par blocs pour le chiffrement et la protection de l'intégrité dans les systèmes de téléphones portables troisième génération. Des attaques sur ces schémas ont déjà été étudiées, notamment [GM01, KW02, PQ05, SZ97, Suga, Sugb]. Dans cette partie I, tout comme pour les schémas de Feistel avec permutations internes, nous nous intéressons aux attaques génériques, lorsque les permutations internes sont aléatoires [NPT10]. Nous renvoyons vers la section 1.3 pour des détails sur ce type d'attaque.

1.2.2 Définition et propriétés élémentaires

Pour les notations utilisées, nous renvoyons vers la partie "Notations". Définissons les deux schémas du type Misty, déjà représentés à la figure 1.4 :

Définition 3 (Un tour de schéma Misty L) *Soit $f \in B_n$ et $L,\ R \in I_n$. La permutation M_L, définie par :*

$$M_L(f)([L, R]) = [R, R \oplus f(L)],$$

est appelée un tour de schéma de Misty L. avec permutation interne f.

Définition 4 (Un tour de schéma du type Misty R) *Soit $f \in B_n$ et $L,\ R \in I_n$. La permutation M_R, définie par :*

$$M_R(f)([L, R]) = [R \oplus f(L), f(L)],$$

est appelée un tour de schéma de Misty R. avec permutation interne f.

Remarque :

1. Pour ces deux schémas, nous ne précisons pas que la fonction interne est une permutation. En effet, lorsque f n'est pas bijective, le schéma défini n'est pas inversible. Ceci est détaillé dans la suite de cette sous-section.

2. Lorsque la permutation interne impliquée est claire, ou lorsque nous parlons du schéma de manière générale, nous notons simplement M_L ou M_R. Sauf mention contraire, M_L (respectivement M_R) désigne un schéma du type Misty L (respectivement Misty R), avec permutation interne aléatoire.

Voyons à quoi correspond l'inversion de ces schémas, ainsi que la relation entre eux. Soit $f \in B_n$. Introduisons les permutations de B_{2n}, $\Lambda(f)$ (ou simplement Λ) et μ, définies par :

$$\Lambda(f)([L,R]) = [f(L),R], \tag{1.1}$$
$$\mu([L,R]) = [R,L\oplus R]. \tag{1.2}$$

Ainsi, nous pouvons décomposer les permutations M_L et M_R :

$$M_L(f) = \mu\circ\Lambda(f), \tag{1.3}$$
$$M_R(f) = \mu^2\circ\Lambda(f). \tag{1.4}$$

L'inverse de Λ s'écrit :

$$\Lambda(f)^{-1} = \Lambda(f^{-1}), \tag{1.5}$$

et μ vérifie :

$$\mu^2([L,R]) = [L\oplus R,L],$$
$$\mu^3([L,R]) = [L,R] \Leftrightarrow \mu^2=\mu^{-1}. \tag{1.6}$$

De toutes les équations précédentes, l'inverse de $M_L(f)$ peut s'écrire :

$$M_L^{-1}(f) = \Lambda(f^{-1})\circ\mu^{-1} = \mu\circ M_R(f^{-1})\circ\mu^{-1}. \tag{1.7}$$

Ceci montre que l'inverse d'une permutation M_L est une permutation M_R à composition près par μ ou μ^{-1} sur les entrées et sorties de M_R. Par suite, la sécurité de M_L et M_R est la même, pour les attaques où l'attaquant peut autant choisir les entrées que les sorties. Dans notre situation, ceci exclut simplement les attaques CPA (attaques à clair choisi, voir la section 1.3 suivante).

Notre analyse se concentre uniquement sur les schémas L du type Misty, qui sont les plus classiques en cryptologie. Les schémas Misty L, M_L, ou plus généralement M_L^k sont représentés par la figure 1.5 et définis comme suit :

Définition 5 (k tour de schémas Misty L) *Soit $(f_1,\ldots,f_k) \in B_n^k$ et $L,\ R,\ S,\ T \in I_n$. La permutation M_L^k, définie par :*

$$M_L^k(f_1,\ldots,f_k)([L,R]) = M_L(f_k)\circ\cdots\circ M_L(f_1)[R,L],$$

est appelée k tours de schémas du type Misty.

Remarque : Ici encore, nous pouvons invoquer M_L^k sans spécifier les permutations internes. Sauf mention contraire, M_L^k désigne k tours de schémas du type Misty (Misty L) avec permutations internes aléatoires.
La sortie de tels schémas sera toujours notée $[S,T]$.

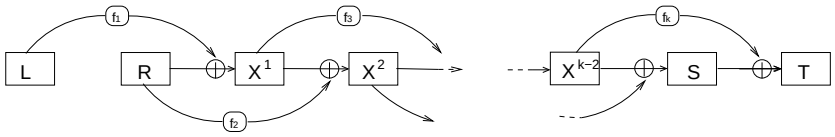

FIGURE 1.5: $M_L^k(f_1, \ldots, f_k)([L, R]) = [S, T]$.

1.3 Attaques Génériques et Attaques Deux Points

Définition 6 (Attaque Générique) *Une attaque sur un schéma de Feistel avec permutations internes ou sur un schéma du type Misty est dite* générique *lorsque les permutations internes sont supposées aléatoires.*

Dans les schémas de chiffrement par bloc utilisés, les permutations internes ne sont pas toujours pseudo-aléatoires. Par conséquent, de meilleures attaques que les génériques existent alors souvent sur ces schémas. Cependant, ceci fait également en quelque sorte l'intérêt de ces attaques génériques : ces attaques n'exploitent pas de faiblesse éventuelle des fonctions (ou permutations) internes utilisées, mais se basent uniquement sur la structure des schémas. Dans notre étude des permutations sur $2n$ bits, ψ^k ou M_L^k, nous considérons des attaques à but de distinguer l'une ou l'autre de ces permutations spécifiques d'une permutation aléatoire sur $2n$ bits. Ces travaux, correspondant à [TP09] pour les schémas de Feistel avec permutations internes et [NPT10] pour les schémas du type Misty, sont à rapprocher de travaux similaires précédents fait sur d'autres schémas basiques ([Pat01] pour les schémas de Feistel classiques, [PNB06b] pour les schémas de Feistel dissymétriques avec fonctions expansives ou [PNB06a] pour ces schémas avec des fonctions contractantes).

Nous nous intéressons principalement aux attaques *deux points*. Ces attaques deux points utilisent des corrélations entre des paires de messages (ce qui inclut les attaques différentielles). Ces attaques se sont montrées être jusqu'à présent généralement les meilleures possibles sur des schémas de Feistel avec *fonctions* internes aléatoires, et bien que le cas des schémas de Feistel avec *permutations* internes soit spécifique, ceci a motivé l'analyse faite dans [TP09], et développée ici. De plus, rappelons que Piret a fait dans [Pir06] des preuves de sécurité pour ces schémas, pour trois et quatre tours. Ces bornes de sécurité se trouvent être les mêmes que les complexités des meilleures attaques deux points que nous avons trouvées pour ce nombre de tours (sauf pour trois tours, CPA, où la meilleure attaque, comme pour les schémas de Feistel classiques, est une attaque trois points). Précisément, notons que les attaques deux points ne sont pas toujours les meilleures possibles. À titre de témoin, on peut citer les schémas "Benes" [PM06], les schémas du type Misty (Misty L et Misty R) [GM01], ou encore les schémas de Feistel dissymétriques avec fonctions expansives [Jut98, PNB06b], pour lesquels d'autres types d'attaques génériques fournissent de meilleures complexités.

Précisément, pour les schémas du type Misty (Misty L), nous faisons dans cette partie une analyse similaire à celle faite pour les schémas de Feistel avec permuta-

tions internes. Ainsi, nous donnons donc les meilleures attaques deux points pour n'importe quel nombre de tours de schémas Misty L. Cependant, comme ces attaques ne sont pas nécessairement les meilleures pour ce schéma, nous donnons autant que possible les attaques alternatives connues (non deux points) fournissant une meilleure complexité d'attaque.

L'objet de cette partie I est donc de regrouper les résultats obtenus concernant les attaques génériques pour les schémas de Feistel avec permutations internes ou schémas Misty L. Le chapitre 2 donne directement les meilleurs attaques génériques pour les premiers tours de ces deux schémas. Ensuite, nous expliquons une manière d'obtenir les meilleures attaques génériques deux points pour un nombre de tours plus grand. Les résultats finaux sont donnés au chapitre 4. Il est intéressant de comparer la sécurité de ces schémas avec celle des schémas de Feistel, plus largement utilisés.

Remarque : Les différentes attaques considérées sont : KPA (attaque à clair connu), CPA-1 (attaque à clair choisi non adaptative), CPA-2 (attaque à clair choisi adaptative), CPCA-1 (attaque à clair et chiffré choisis non adaptative) et CPCA-2 (attaque à clair et chiffré choisis adaptatives).

Lorsque l'on s'intéresse aux attaques sur des générateurs de permutations (plus d'une permutation sur $2n$ bits est utilisée), les KPA et CPA donnent la même complexité. L'intuition de ceci est que l'on utilise alors le nombre maximal de messages par permutation, mais ceci est justifié au chapitre 3.

Chapitre 2

Meilleures Attaques Génériques sur les Premiers Tours de Schémas de Feistel avec Permutations Aléatoires et Misty L

Dans ce chapitre, nous exposons directement les meilleures attaques génériques connues de complexité inférieure à $\mathcal{O}\left(2^{2n}\right)$, pour les cinq premiers tours des deux schémas qui nous intéressent. Ces attaque peuvent être trouvées dans [TP09, NPT10]. Nous nous intéressons principalement aux attaques deux points, mais d'autres que celles-ci peuvent être citées lorsqu'elles sont meilleures. Ces attaques deux points sont également l'objet d'une étude plus approfondie par la suite (chapitre 3 et 4).

Notons que les attaques ne sont pas uniques, dans le sens où deux attaques différentes (pour le cas des attaques deux points, deux attaques exploitant des relations différentes entre les blocs d'entrée et sortie de deux messages distincts) peuvent mener à la même complexité. Ceci sera mis en évidence dans le chapitre 4. Nous donnons ici une seule attaque par nombre de tours considéré, sauf lorsqu'une attaque autre que les attaques deux points fournit une meilleure complexité.

Les complexités de toutes ces attaques sont rappelées dans le tableau 4.9 de la sous-section 4.2.3 pour les schémas de Feistel et le tableau 4.3 de la sous-section 4.1.3 pour les schémas Misty L.

Sommaire

2.1 Meilleures attaques génériques sur les premiers tours de schémas de Feistel avec permutations internes

Les schémas de Feistel avec permutations internes n'ayant pas fait l'objet de beaucoup d'études, les attaques de cette section n'ont pas forcément été mentionnées lors de travaux précédents (sauf pour l'attaque sur cinq tours de la sous-section 2.1.5, donnée par Knudsen dans [Knu02]). Notons que les attaques sur les deux premiers tours de schémas de Feistel avec permutations internes (sous-section 2.1.1 et 2.1.2) restent inchangées comparées aux attaques sur un ou deux tours de schémas de Feistel classiques (avec fonctions internes) [Pat01]. Nous les rappelons tout de même dans ce chapitre. Nous pouvons noter que ce résultat n'est pas surprenant. En effet, distinguer une fonction aléatoire sur n bits d'une permutation aléatoire sur n bits nécessite de l'ordre de $2^{n/2}$ calculs. Ceci se déduit du paradoxe des anniversaires, car au bout de $2^{n/2}$ évaluations, une fonction aléatoire sur n bits fournit une collision sur deux sorties avec probabilité supérieure à $1/2$. Ainsi, lorsqu'une attaque sur des schémas de Feistel avec fonctions aléatoires internes nécessite un nombre de calculs très inférieur à $2^{n/2}$, cette attaque n'exploite pas la non-bijectivité des fonctions internes, et fonctionne encore lorsque les fonctions internes aléatoires sont en fait des permutations aléatoires.

Au-delà de deux tours, les attaques deux points sont différentes que dans le cas des schémas de Feistel avec fonctions aléatoires internes. Il existe une attaque trois points sur trois tours de schémas de Feistel avec fonctions internes aléatoires, à clair et chiffré choisis, nécessitant trois messages ([LR88] p.385). Pour la même raison que pour les attaques sur un ou deux tours invoquée plus haut, cette attaque trois points s'applique encore lorsque les fonctions internes aléatoires sont des permutations aléatoires (sous-section 2.1.3 ci-dessous). Jusqu'à cinq tours, les meilleures attaques deux points trouvées exploitent une différentielle impossible des schémas de Feistel avec permutations aléatoires internes. Cependant, ceci ne se généralise pas au-delà de cinq tours, comme nous le verrons dans l'exemple sur six tours du chapitre 3 (sous-section 3.2.2), ou dans le chapitre 4.

Pour ces cinq premiers tours, la complexité des attaques, excepté pour la KPA sur trois tours, est identique aux complexité des attaques deux points sur les schémas de Feistel classiques [Pat01]. Cependant, ceci ne pouvait être prédit avant l'analyse de [TP09]. Pour trois tours, la meilleure KPA deux points est de complexité $\mathcal{O}(2^n)$ calculs, alors que $\mathcal{O}\left(2^{n/2}\right)$ étaient nécessaires pour les schémas de Feistel classiques.

2.1.1 Un tour

Pour un tour de schéma de Feistel, nous avons les relations et la figure 2.1 suivantes :

$$\begin{cases} S = R \\ T = f_1(R) \oplus L \end{cases}$$

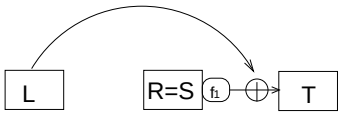

FIGURE 2.1: $\psi(f_1)$

2.1.1.1 KPA

Il existe une attaque à clair connu qui n'utilise qu'un seul message clair $[L, R]$. L'attaquant peut se contenter de tester si la sortie de la permutation testée, dénotée par $[S, T]$, vérifie $S = R$. Si la permutation est un seul tour de schéma de Feistel, cette égalité est toujours vérifiée. Si la permutation considérée est une permutation aléatoire de $2n$ bits sur $2n$ bits, l'égalité précédente entre le bloc R d'entrée et le bloc S de sortie apparaît avec probabilité $1/2^n$.

Pour un tour, nous avons donc une attaque à clair connu qui ne nécessite que de l'ordre de 1 calculs. Par conséquent, tout autre type d'attaque peut se monter avec $\mathcal{O}(1)$ calculs également.

2.1.2 Deux tours

Pour deux tours de schémas de Feistel, nous avons les relations et la figure 2.2 suivantes :

$$\begin{cases} S = f_1(R) \oplus L \\ T = f_2(f_1(R) \oplus L) \oplus R \end{cases}$$

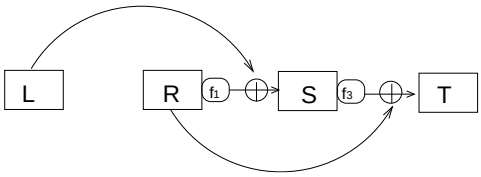

FIGURE 2.2: $\psi^2(f_1, f_2)$

2.1.2.1 CPA-1

Pour deux tours de schémas de Feistel, et dans le cas d'une attaque à clair choisi non adaptative, l'attaquant peut par exemple choisir deux messages d'entrée $[L_1, R_1]$ et $[L_2, R_2]$, tels que les blocs droits des deux messages soient égaux : $R_1 = R_2$ (et par suite $L_1 \neq L_2$). Soient $[S_1, T_1]$ et $[S_2, T_2]$ les sorties correspondantes, pour la permutation considérée. Alors, l'attaquant peut simplement tester si $S_1 \oplus S_2 = L_1 \oplus L_2$. En effet, cette égalité sur les les blocs S de sortie apparaît pour tous les messages d'entrée choisis de cette manière, quand la permutation est composée de 2 tours de schémas de Feistel. Cette même égalité apparaît avec probabilité $1/2^n$ dans le cas d'une permutation aléatoire.

Par conséquent, nous avons une attaque à clair choisi non adaptative (CPA-1) nécessitant de l'ordre de 2 calculs.

2.1.2.2 KPA

L'attaque précédente nécessite d'avoir des messages clairs vérifiant une certaine égalité sur leur blocs (en l'occurence, $R_1 = R_2$). Dans le cadre d'une attaque à clair connu, les messages d'entrée ne peuvent plus être choisis de la sorte. Par contre, par le paradoxe de anniversaire, deux tels messages clairs ont un probabilité supérieure à $1/2$ d'exister après la génération de $\mathcal{O}\left(2^{n/2}\right)$ messages. Une fois les deux messages $[L_i, R_i]$ et $[L_j, R_j]$ obtenus, avec $R_i = R_j$ et $L_i \neq L_j$, l'attaquant peut terminer l'attaque comme dans le cas de la CPA-1 précédente. Autrement dit, il teste si $S_i \oplus S_j = L_i \oplus L_j$.

Il en résulte une attaque deux points à clair connu en $\mathcal{O}\left(2^{n/2}\right)$ calculs.

2.1.3 Trois tours

Comme annoncé au début de ce chapitre, les attaques deux points décrites dans [Pat01] ne s'appliquent pas lorsque les fonctions utilisées sont des permutations, pour un nombre de tours supérieur ou égal à trois.

La figure 2.3 représente trois tours de schémas de Feistel et peut permettre de retrouver plus facilement les relations entre les blocs.

$$\begin{cases} S = f_2\left(f_1(R) \oplus L\right) \oplus R \\ T = f_3(S) \oplus f_1(R) \oplus L \end{cases}$$

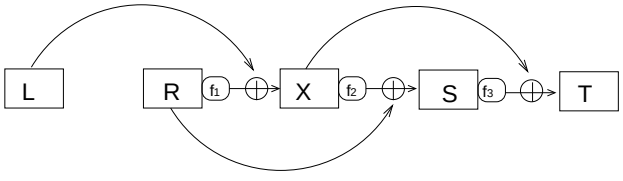

FIGURE 2.3: $\psi^3(f_1, f_2, f_3)$

2.1.3.1 CPA-1

Commençons par décrire une attaque à clair choisi, non adaptative. L'attaquant choisit des messages clairs d'entrée, $[L_i, R_i]$ (d'image $[S_i, T_i]$, par la permutation considérée), vérifiant : $L_i = L_j$ et $R_i \neq R_j$ quand $i \neq j$. Ensuite, pour différents couples (i, j), il teste si les messages de sortie ont la propriété suivante : $R_i \oplus R_j = S_i \oplus S_j$. La raison est que lorsque la permutation impliquée est 3 tours de schémas de Feistel avec *permutations internes*, une telle égalité n'apparaît jamais. Si au contraire, la permutation testée est une permutation aléatoire, alors une collision $R_i \oplus R_j = S_i \oplus S_j$, pour deux indices différents i, j, arrive après évaluation de l'ordre de $2^{n/2}$ messages.

Le deuxième résultat concernant les permutations aléatoires résulte du paradoxe des anniversaires. Focalisons-nous sur le résultat concernant 3 tours de schéma de Feistel. Considérons la figure 2.3.

Supposons que pour deux indices différents i, j, l'égalité $S_i \oplus S_j = R_i \oplus R_j$ a lieu. La fonction f_2 étant une permutation, les valeurs internes X_i et X_j (cf. figure 2.3) sont égales. En regardant au niveau de l'entrée de la permutation, le fait d'avoir choisi $L_i = L_j$, comme f_1 est une permutation et $X_i = X_j$, implique $R_i = R_j$. Or ceci est contradictoire avec le choix initial des messages. Ainsi, comme annoncé, avec le choix des messages d'entrée, l'égalité $S_i \oplus S_j = R_i \oplus R_j$ ne peut arriver pour $i \neq j$.

Il en résulte une attaque deux points à clair choisi non adaptative (CPA-1), nécessitant de l'ordre de $2^{n/2}$ calculs.

2.1.3.2 KPA

Pour trois tours, la meilleure attaque à clair connu (KPA) trouvée nécessite $\mathcal{O}(2^n)$ calculs, tandis que $\mathcal{O}\left(2^{n/2}\right)$ messages étaient suffisants pour l'attaque générique sur 3 tours de schémas de Feistel avec fonctions internes [Pat01]. Ce phénomène est expliqué au chapitre 3, paragraphe 4.2.2.2.

L'attaque est une adaptation de la CPA-1, comme dans le cas de la KPA sur 2 tours. L'attaquant attend de recevoir le nombre nécessaire de paires de messages clairs d'entrée vérifiant, pour deux indices i et j distincts : $L_i = L_j,\ R_i \neq R_j$. C'est à dire, pour la CPA-1 précédente, il nécessite de l'ordre de $2^{n/2}$ telles paires.

Par conséquent, l'attaque deux points à clair connu déduite de la CPA-1 a une complexité finale de l'ordre de 2^n calculs.

2.1.3.3 Meilleure attaque CPCA-2 trois points.

Le cas d'une attaque à clair et chiffré choisis adaptative (CPCA-2) est un peu particulier. Dans ce cas, il existe une attaque meilleure que les attaque deux points. Ceci peut également être le cas pour d'autres attaques sur d'autres tours présentées, mais les attaques deux points sont à notre connaissance celles donnant les meilleures attaques.

Dans le cas de cette CPCA-2, l'attaque sur trois tours de schémas de Feistel avec fonctions internes, présentée dans [LR88] p.385, utilisant trois messages, fonctionne encore lorsque l'on remplace les fonctions par des permutations. L'attaque n'est pas une attaque deux points, mais trois points. L'attaquant peut choisir ses entrées $[L_i, R_i]$ et sorties $[S_i, T_i]$ de la manière suivante : $[L_1, R_1]$ et la sortie $[S_1, T_1]$ correspondante aléatoires, puis $[L_2, R_2]$ avec $R_2 = R_1, L_2 \neq L_1$, et enfin $[S_3, T_3] = [S_1, T_1 \oplus L_1 \oplus L_2]$. Il peut alors simplement tester si $R_3 = S_2 \oplus S_3 \oplus R_2$. Dans le cas de trois tours d'un schéma de Feistel avec permutations internes, cette égalité arrive avec probabilité 1, alors que pour une permutation aléatoire, une telle égalité apparaît avec probabilité $1/2^n$.

On obtient bien une attaque deux points à clair et chiffré choisis adaptative avec seulement (de l'ordre de) trois calculs.

Remarque : Lorsque le nombre de messages m utilisés pour monter l'attaque est petit comparé à $\mathcal{O}\left(2^{n/2}\right)$, il n'est pas possible de distinguer une permutation aléatoire d'une fonction aléatoire. Pour un nombre de message en dessous de cette borne, les attaques mises en jeu dans le cadre des schémas de Feistel n'utilisent pas la bijectivité ou non-bijectivité des fonctions impliquées. Il est alors normal de retrouver les mêmes attaques. Cette remarque avait déjà été faite au début de ce chapitre.

2.1.4 Quatre tours

Dans le cas de quatre tours (figure 2.4), les équations souhaitées sur les blocs d'entrée et de sortie afin de monter les attaques, sont les mêmes que dans le cas de schémas de Feistel classiques ([Pat01] ou [AV96]). Cependant, les attaques sont différentes, car elles n'utilisent pas les mêmes propriétés du schéma. Sur quatre tours, et dans le cas des schémas de Feistel avec permutations internes aléatoires, les attaques sont par exemple toutes basées sur des différentielles impossibles, comme pour la CPA-1 sur trois tours (sous-section 2.1.3). Pour quatre tours, les blocs de sortie sont les suivants :

$$\begin{cases} S = f_3\left(f_2(f_1(R) \oplus L) \oplus R\right) \oplus f_1(R) \oplus L \\ T = f_4(S) \oplus f_2\left(f_1(R) \oplus L\right) \oplus R \end{cases}$$

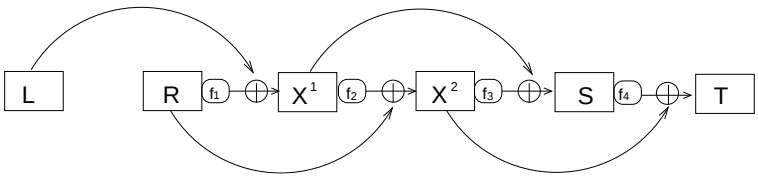

FIGURE 2.4: $\psi^4(f_1, f_2, f_3, f_4)$

2.1.4.1 CPA-1

Pour monter une attaque à chiffré choisi non adaptative, l'attaquant peut par exemple choisir différents messages d'entrée $[L_i, R_i]$, où les blocs de droite sont tous égaux à une valeur R_0. Ensuite, il teste l'égalité suivante sur les sorties, pour $i \neq j$: $L_i \oplus L_j = S_i \oplus S_j$. Pour une permutation aléatoire, par le paradoxe des anniversaires, au bout de $2^{n/2}$ évaluations, une telle égalité arrive avec une probabilité $\geq 1/2$. Pour quatre tours de schémas de Feistel, une telle configuration n'apparaît pas.

Pour s'assurer de l'existence cette différentielle impossible, considérons les quatre permutations internes (f_1, f_2, f_3, f_4). Soit encore X la valeur $f_2(L \oplus f_1(R))$ (le bloc noté X^2 dans la figure 2.4). L'égalité $X_i = X_j$, pour $i \neq j$, n'apparaît jamais car f_1, f_2 sont des permutations et $L_i \neq L_j$. Par suite, une autre égalité n'apparaissant pas est celle de $R_i \oplus X_i$ et de $R_j \oplus X_j$. Or nous avons $S_i \oplus S_j = f_3(X_i \oplus R_i) \oplus L_i \oplus f_3(X_j \oplus R_j) \oplus L_j$. Comme f_3 est une permutation, il est impossible pour $S_i \oplus S_j$ d'être égal à $L_i \oplus L_j$.

On en déduit une attaque deux points, $CPA-1$ en $\mathcal{O}\left(2^{n/2}\right)$ calculs.

2.1.4.2 KPA

La meilleure attaque à clair connu trouvée est une adaptation de la CPA-1 précédente. L'attaquant peut attendre d'obtenir $\mathcal{O}(2^{n/2})$ messages d'entrée vérifiant $L_i = L_j$, puis appliquer l'attaque précédente. Cette attaque nécessite de l'ordre de 2^n calculs.

2.1.5 Cinq tours

Pour cinq tours de schémas de Feistel avec permutations internes (figure 2.5 ci-dessous), nous n'avons pas de meilleure attaque deux points que celle donnée par Knudsen, sur ces mêmes schémas [Knu02]. L'attaque, comme pour celles présentées plus haut sur quatre tours, est basée sur une configuration impossible.

$$\begin{cases} S = f_4\left(f_3(f_2(f_1(R) \oplus L) \oplus R) \oplus f_1(R) \oplus L\right) \oplus f_2\left(f_1(R) \oplus L\right) \oplus R \\ T = f_5(S) \oplus f_3\left(f_2(f_1(R) \oplus L) \oplus R\right) \oplus f_1(R) \oplus L \end{cases}$$

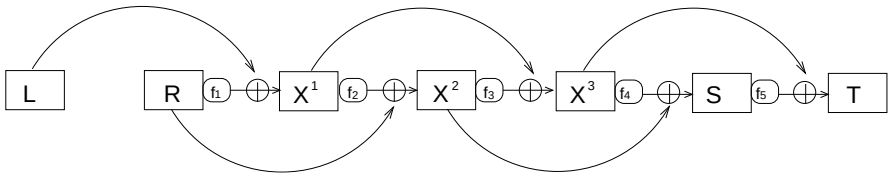

FIGURE 2.5: $\psi^5(f_1, f_2, f_3, f_4, f_5)$

Plus précisément, la différentielle impossible en question, pour cinq tours de schéma de Feistel avec permutations internes, est la suivante. Pour deux paires d'entrée/sorties $([L_1, R_1]/[S_1, T_1])$ et $([L_2, R_2]/[S_2, T_2])$, les égalités suivantes ne peuvent

être toutes vérifiées à la fois :

$$\begin{cases} L_1 \neq L_2, \\ R_1 = R_2, \\ S_1 = S_2, \\ T_1 \oplus T_2 = L_1 \oplus L_2. \end{cases}$$

En effet, regardons l'effet d'éventuelles telles égalités sur les blocs, dans le cas de cinq tours de schémas de Feistel. L'égalité $S_1 = S_2$ équivaut à $X_1^2 \oplus f_4(X_1^3) = X_2^2 \oplus f_4(X_2^3)$ et $T_1 \oplus T_2 = X_1^3 \oplus X_2^3$. Par ailleurs, l'égalité $R_1 = R_2$ équivaut à $L_1 \oplus L_2 = X_1^1 \oplus X_2^1$ et $X_1^2 \oplus X_2^2 = f_2(X_1^1) \oplus f_2(X_2^1)$. Utilisant ces nouvelles égalités, on a que $T_1 \oplus T_2 = L_1 \oplus L_2$ équivaut à $X_1^3 \oplus X_2^3 = X_1^1 \oplus X_2^1$. Or cette égalité implique $X_1^2 = X_2^2$. Or, comme $R_1 = R_2$, on a aussi $X_1^1 \oplus X_2^1 = 0$. On déduit que tous les blocs sont égaux, jusqu'aux blocs d'entrée et de sortie, ce qui est absurde.

Dans le cas d'une permutation aléatoire, ces égalités arrivent avec probabilité environ $1/2^{3n}$ entre deux messages. Par le paradoxe des anniversaires, on déduit une attaque CPA-1 en 2^n calculs (au bout de 2^n évaluations de messages $[L_i, R_0]$, R_0 constant, on attend d'avoir les égalités sur les blocs de sortie avec probabilité supérieur à $1/2$). On déduit également une attaque KPA en $2^{3n/2}$ calculs.

Autrement dit, il n'existe pas de quintuplet de permutations $(f_1, \ldots, f_5) \in B_n^5$, telles qu'utilisées comme fonctions internes, permettent d'obtenir toutes ces égalités sur les blocs. Cette propriété, comme dans le cas de quatre tours, va être exploitée pour déduire un distingueur entre cinq tours de schéma de Feistel et une permutation aléatoire.

2.1.5.1 CPA-1

Une manière d'exploiter cette différentielle impossible pour monter une attaque à clair choisi non adaptative est la suivante. L'attaquant peut choisir des entrées dont les blocs de droite et de gauche (les blocs L et R) vérifient les deux premières des conditions précédentes. Il attend ensuite de voir s'il obtient des sorties vérifiant les deux dernières des conditions. Après avoir calculé 2^n message, toutes les égalités ont une probabilité plus grande que $1/2$ d'être vraies pour un certain coule de message, dans le cas où la permutation est est une permutation aléatoire. Dans le cas de cinq tours de schéma de Feistel, cela n'arrive pas, comme annoncé plus haut.

Ainsi, il y a une attaque deux points à clair choisi non adaptative en $\mathcal{O}(2^n)$ calculs.

2.1.5.2 KPA

Comme dans les cas précédents, cette attaque à clair choisi non adaptative peut être transformée en attaque à clair connu (KPA). L'attaquant peut attendre qu'assez de paires d'entrées soient générées. On obtient alors une attaque de complexité $\mathcal{O}(2^{3n/2})$ messages.

Remarque : Au-delà de cinq tours, les meilleures attaques génériques ne sont plus basées sur une différentielle impossible. On peut le voir déjà sur six tours à la

section 3.2. Ceci se déduit également de la valeur des coefficients H, introduits au chapitre 3.

2.2 Meilleures attaques génériques, de complexité inférieure à $\mathcal{O}\left(2^{2n}\right)$ sur les premiers tours de schémas du type Misty

Cette section est le pendant de la section 2.1, pour les schémas Misty L. Nous y exposons directement les meilleures attaques génériques pour les cinq premiers tours de schémas du type Misty. Ici encore, nous nous intéressons tout particulièrement aux attaques deux points. Ensuite, nous généralisons ces attaques deux points au chapitre 4 pour n'importe quel nombre de tours. Cependant, pour ces premiers tours, nous donnons les attaques alternatives (non deux points) fournissant une meilleure complexité d'attaque quand nous en trouvons. Toutes ces attaques (et même certaines non exposées ici) peuvent être trouvées dans [NPT10]. Les attaques sur les schémas du type Misty ont déjà été précédemment étudiées, par conséquent, certaines des attaques exposées ci-dessous ou dans [NPT10] étaient déjà connues, d'autres sont issues de [NPT10].

Pour un tour, un seul calcul permet a priori de distinguer un schéma du type Misty d'une permutation aléatoire. Pour deux tours, les attaques deux points sont les meilleures trouvées. Pour trois tours, il existe une attaque deux points à clair connu de complexité $\mathcal{O}\left(2^n\right)$ calculs, qui peut se transformer en attaque à clair choisi en $\mathcal{O}\left(2^{n/2}\right)$. Mais sur trois tours, on montre qu'il existe une attaque quatre points à clair choisi nécessitant de l'ordre de 1 calculs, et une attaque à clair et chiffrés choisi trois points de complexité $\mathcal{O}\left(1\right)$ également. Pour quatre tours, il n'y a que le cas de l'attaque à clair et chiffré choisis adaptative qui est de complexité meilleure en quatre points plutôt qu'en deux. Cette attaque est de complexité $\mathcal{O}\left(1\right)$ calculs, comparé à $\mathcal{O}\left(2^{n/2}\right)$ (qui est aussi la complexité de l'attaque à clair choisi).

Pour cinq tours, nous verrons à la sous-section 2.2.5 qu'il existe une attaque à clair choisi et clair connu de complexité $\ll 2^{2n}$. Ainsi, pour éviter les attaques génériques de complexité inférieure à 2^{2n} calculs, au moins six tours de schémas Misty L doivent être utilisés. Ceci était également le cas pour les schémas de Feistel (avec fonctions internes [Pat01] et permutations internes [TP09]). Cependant, Les attaques étaient alors des attaques deux points, tandis qu'ici, c'est une attaque quatre points qui fournit la meilleure complexité [1], les complexités fournies par les attaques deux points étant alors toutes de complexité supérieure à 2^{2n} (voir la sous-section 2.2.5 ou le chapitre 4).

2.2.1 Un tour

La figure 2.6 ci-dessous rappelle la structure d'un schéma du type Misty.

1. On a cette complexité également avec une attaque par saturation, cf. sous-section 2.2.5.

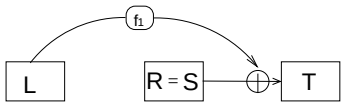

FIGURE 2.6: $M_L^1(f_1)$

2.2.1.1 KPA

Après seulement un tour de schéma du type Misty, nous avons que $S = R$. Cette égalité arrive donc avec probabilité 1 dans ce cas ; dans le cas d'une permutation aléatoire, un telle égalité entre deux blocs arrive avec probabilité $1/2^n$.

On déduit une attaque à clair connu (KPA) en $\mathcal{O}(1)$ calculs.

2.2.2 Deux tours

Comme l'indique la figure 2.7, pour deux tours de schémas Misty L, nous avons les relations suivantes entre les blocs :

$$\begin{cases} S = R \oplus f_1(L) \\ T = f_2(R) \oplus S \end{cases}$$

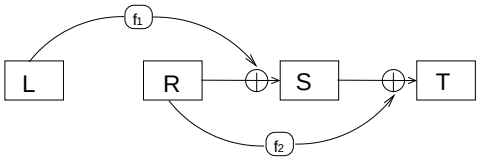

FIGURE 2.7: $M_L^2(f_1, f_2)$

2.2.2.1 CPA-1

Dans le cadre d'une attaque à clair choisi sur deux tours de schémas du type Misty, l'attaquant peut par exemple choisir deux messages d'entrée $[L_1, R_1]$ et $[L_2, R_2]$ tels que $L_1 = L_2$ (et $R_1 \neq R_2$). L'attaquant peut alors tester l'égalité $R_1 \oplus R_2 = S_1 \oplus S_2$ sur ses messages de sortie. Cette égalité arrive avec probabilité $1/2^n$ dans le cas d'une permutation aléatoire, et avec probabilité 1 dans le cas de M_L^2. En effet, d'après les relations rappelées plus haut, on a pour M_L^2 : $S_1 \oplus S_2 = R_1 \oplus f_1(L_1) \oplus R_2 \oplus f_1(L_2) = R_1 \oplus R_2$ (par le choix de L_1 et L_2, et la bijectivité de f_1).

Ainsi, on déduit une attaque deux points à clair choisi en $\mathcal{O}(1)$ calculs.

2.2.2.2 KPA

L'attaque précédente peut être transformée en attaque à clair connu comme il a été fait plusieurs fois dans le cas de schémas de Feistel à la section 2.1. L'attaquant ne peut pas choisir deux entrées comme dans l'attaque à clair choisi, mais il peut attendre de les obtenir. Par le paradoxe des anniversaires, au bout de $\mathcal{O}\left(2^{n/2}\right)$ messages, il obtiendra deux messages $[L_i, R_i]$ et $[L_j, R_j]$ avec une collision sur leur bloc L. Il peut alors terminer l'attaque comme dans le cas de la CPA-1, en testant si $S_i \oplus S_j = R_i \oplus R_j$.

Ceci décrit une attaque deux points à clair connu en $\mathcal{O}\left(2^{n/2}\right)$ calculs.

2.2.3 Trois tours

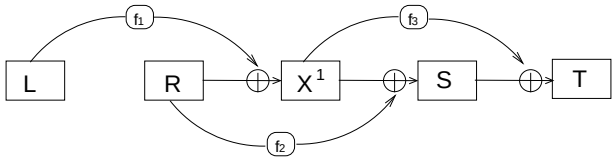

FIGURE 2.8: $M_L^3(f_1, f_2, f_3)$

Ici, comme rappelé dans la figure 2.8 :

$$\begin{cases} S = f_1(L) \oplus f_2(R) \oplus R \\ T = f_3\left(R \oplus f_1(L)\right) \oplus S \end{cases}$$

2.2.3.1 CPA-1

Pour réaliser une attaque à clair choisi sur trois tours, l'attaquant peut considérer deux messages d'entrée $[L_1, R_1]$ et $[L_2, R_2]$ tels que $L_1 = L_2$ (et $R_1 \neq R_2$). Il s'intéresse alors à l'équation suivante entre les blocs d'entrée et sortie : $S_1 \oplus T_1 = S_2 \oplus T_2$. Cette égalité apparaît avec probabilité $1/2^n$ dans le cas d'une permutation aléatoire et n'apparaît jamais dans le cas de trois tours de schémas Misty L.

En effet, sommer les blocs S et T revient à considérer $f_3(f_1(L) \oplus R)$. Dans le cas de trois tours de schémas Misty L, l'égalité précédente considérée sur les blocs de sortie, ne peut apparaître que si les entrées de la permutation f_3 sont les mêmes. Autrement dit, $S_1 \oplus T_1 = S_2 \oplus T_2 \Leftrightarrow f_1(L_1) \oplus R_1 = f_1(L_2) \oplus R_2$. Comme L_1 et L_2 sont choisis égaux par l'attaquant, cette égalité est encore équivalente à l'égalité $R_1 = R_2$. Or cette égalité est impossible, car les messages sont initialement choisis distinct.

Par suite, on déduit une attaque deux points à clair choisi de complexité $\mathcal{O}\left(2^{n/2}\right)$ calculs. Ceci correspond par exemple au nombre de messages $[L_0, R_i]$, avec L_0 un bloc constant, nécessaire pour avoir une collision sur deux valeurs $S \oplus T$ avec probabilité $> 1/2$ (paradoxe des anniversaires) dans le cas d'une permutation aléatoire.

2.2.3.2 KPA

L'attaque précédente peut se transformer en une attaque à clair connu, par le même procédé que celui utilisé dans les autres attaques. L'attaquant cherche à savoir si, pour la permutation à laquelle il a affaire, peuvent correspondre deux entrées/sorties $[L_i, R_i]/[S_i, T_i]$ et $[L_j, R_j, S_j, T_j]$ telles que $L_i = L_j$ et $S_i \oplus T_i = S_j \oplus T_j$. Si la permutation en question est une permutation aléatoire, l'évaluation de 2^n messages devrait lui fournir deux telles entrées/sorties avec probabilité supérieure à $1/2$. Ceci est encore dû au paradoxe des anniversaire : l'attaquant cherche à avoir une collision sur une valeur de taille $2n$ bits (deux blocs de n bits).

Par suite, on a une attaque deux points à clair connu nécessitant l'évaluation de $\mathcal{O}(2^n)$ messages.

2.2.3.3 Meilleure CPA-1, attaque quatre points

Nous intéressons principalement aux attaques deux points. Mais notons tout de même que pour trois tours, il existe une CPA-1 meilleure en quatre points. Cette attaque a été publiée dans [SZ97] et nécessite seulement $\mathcal{O}(1)$ calculs en CPA-1. Elle ne permet par contre pas d'avoir une KPA meilleure que celle présentée plus haut.

L'attaquant peut choisir quatre messages d'entrée de la manière suivante : $[L_1, R_1]$, $[L_2, R_2]$, $[L_3, R_3] = [L_1, R_2]$ et $[L_4, R_4] = [L_2, R_1]$. Avec quatre tels messages, nous avons que l'égalité suivante :

$$S_1 \oplus S_2 \oplus S_3 \oplus S_4 = 0,$$

est vérifiée avec probabilité 1 dans le cas d'un schéma du type Misty, et avec probabilité $1/2^n$ dans le cas d'une permutation aléatoire.

Voyons la raison d'une telle égalité dans le cas des schémas Misty L. Rappelons que $S = R \oplus f_1(L) \oplus f_2(R)$ (voir aussi la figure 2.8 ci-dessus). Par le choix des messages d'entrée, sommer S_1 et S_4 donne $f_1(L_1) \oplus f_1(L_2)$ (les blocs R étant les mêmes pour les deux messages d'entrée). De la même manière, comme $R_2 = R_3$, la somme $S_2 \oplus S_4$ vaut également $f_1(L_1) \oplus f_1(L_2)$. Ainsi, la somme des quatre blocs S est bien le bloc 0 pour tout choix de tels quatre messages.

Ceci montre qu'une CPA-1 quatre point en $\mathcal{O}(1)$ calculs existe. On peut dériver de cette attaque une KPA en 2^n messages. Ceci vient du fait qu'il faut de l'ordre de 2^{2n} couples $([L_1, R_1], [L_2, R_2])$ pour espérer avoir une collision entre deux couple selon les quatre égalités souhaitées voir vérifiées. Or 2^{2n} tels couples peuvent être obtenus avec $\mathcal{O}(2^n)$ messages $[L, R]$.

2.2.3.4 Meilleure CPCA-2, attaque trois points

Nous indiquons une attaque à clair et chiffré choisis adaptative, fonctionnant avec seulement trois messages. Cette attaque s'inspire des attaques de [Pat01] et [SZ97].

L'attaquant commence par évaluer la permutation inconnue sur un message d'entrée aléatoire $[L_1, R_1]$, et obtient $[S_1, T_1]$. Puis, il demande le déchiffrement

du message $[S_2, T_2]$, vérifiant : $T_1 \oplus S_1 = T_2 \oplus S_2$. Il obtient alors $[L_2, R_2]$, tel que $f_1(L_1) \oplus R_1 = f_1(L_2) \oplus R_2$, si la permutation correspond à trois tours de schémas du type Misty. En effet, l'égalité sur le bloc $T \oplus S$ équivaut à $f_3(f_1(L_1) \oplus R_1) = f_3(f_1(L_2) \oplus R_2)$. Par bijectivité de f_3, on obtient bien l'égalité sur les blocs d'entrée annoncée. Cette relation n'est pas encore suffisante pour lui permettre de réaliser son attaque, car elle implique f_1. L'attaquant évalue alors ensuite le message $[L_3, R_3] = [L_1, R_2]$, et obtient $[S_3, T_3]$. Cette fois, dans le cadre de trois tours de schémas du type Misty, il a la relation suivante :

$$S_2 \oplus S_3 = f_2(R_2) \oplus f_2(R_3) \oplus f_1(L_2) \oplus f_1(L_3) \oplus R_2 \oplus R_3 = R_1 \oplus R_2.$$

En effet, le choix de $R_3 = R_2$ élimine quatre éléments dans la somme ci-dessus. La relation $f_1(L_1) \oplus R_1 = f_1(L_2) \oplus R_2$ permet de conclure.

Ainsi, pour un tel choix de messages, la relation $S_2 \oplus S_3 = R_1 \oplus R_2$ apparaît avec probabilité 1 dans le cas de trois tours de schémas Misty L. Dans le cas d'une permutation aléatoire, cette même égalité apparaît avec probabilité $1/2^n$ environ.

Ceci fournit une attaque à clair et chiffré choisis avec trois messages et une complexité en calculs de l'ordre de 1.

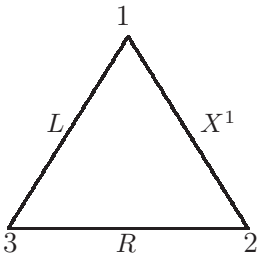

FIGURE 2.9: Les égalités utilisées dans la CPCA-2 sur M_L^3, avec trois messages

2.2.4 Quatre tours

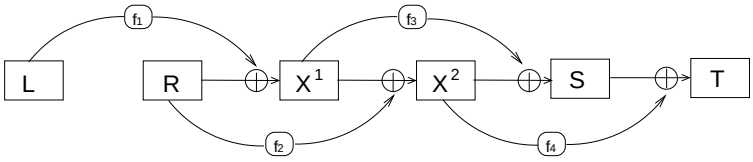

FIGURE 2.10: $M_L^4(f_1, f_2, f_3, f_4)$

Dans le cas de quatre tours de schémas Misty L (figure 2.10) :

$$\begin{cases} S = R \oplus f_1(L) \oplus f_2(R) \oplus f_3(R \oplus f_1(L)) \\ T = f_4(X^2) = f_4(R \oplus f_1(L) \oplus f_2(R)) \oplus S \end{cases}$$

2.2.4.1 CPA-1

Pour attaquer quatre tours de schémas Misty L, un attaquant, dans le cadre d'une attaque à clair choisi choisi non-adaptative, peut raisonner comme suit. Considérons deux messages $[L_1, R_1]$ et $[L_2, R_2]$, avec $R_1 = R_2$ ($L_1 \neq L_2$). Alors, dans le cas de quatre tours de schémas Misty L, l'égalité $S_1 \oplus T_1 = S_2 \oplus T_2$ ne se produit jamais, alors que dans le cas d'une permutation aléatoire, cette égalité se produit avec probabilité $1/2^n$.

En effet, pour quatre tours de schémas Misty L, $S \oplus T = f_4(R \oplus f_1(L) \oplus f_2(R))$ (on peut se référer par exemple à la figure 2.10). Revenons aux deux entrées/sorties : $S_1 \oplus T_1 = S_2 \oplus T_2 \leftrightarrow R_1 \oplus f_1(L_1) \oplus f_2(R_1) = R_2 \oplus f_1(L_2) \oplus f_2(R_2)$, car f_4 est une permutation. Finalement, avec le choix des entrées comme précédemment, on a bien le résultat annoncé, car $S_1 \oplus T_1 = S_2 \oplus T_2 \leftrightarrow L_1 = L_2$, qui est impossible.

L'attaquant peut alors exploiter cette différence en générant de l'ordre de $2^{n/2}$ messages $[L_i, R_0]$, où R_0 est constant. Si la permutation testée est une permutation aléatoire, alors par le paradoxe des anniversaire avec probabilité supérieure à $1/2$, il existe $i \neq j$, tels que $S_i \oplus T_i = S_j \oplus T_j$. Si la permutation testée est quatre tours de schémas du type Misty, cela ne se produit pas.

On en déduit une attaque à clair choisi non-adaptative en $\mathcal{O}\left(2^{n/2}\right)$ calculs.

2.2.4.2 KPA

La CPA-1 précédente peut être transformée en attaque à clair connu. L'attaquant calcule de l'ordre de 2^n entrées/sorties $[L_i, R_i]/[L_j, R_j]$. En effet, si la permutation est aléatoire, avec probabilité supérieure à $1/2$, il existera deux indices $i \neq j$ pour lesquels les messages correspondant vérifient à la fois la relation $R_i = R_j$ et la relation $S_i \oplus T_i = S_j \oplus T_j$. Si la permutation correspond à quatre tours de schémas Misty L, il n'y aura pas deux tels indices.

La complexité de cette KPA est $\mathcal{O}\left(2^n\right)$ calculs.

2.2.4.3 Meilleure CPCA-2, attaque quatre points

L'attaque qui suit est une attaque quatre points, utilisant quatre messages. Elle est extraite de [SZ97].

Le premier message que l'attaquant choisit est aléatoire : soit $[L_1, R_1]$ cette entrée et $[S_1, T_1]$ la sortie obtenue. Puis, l'attaquant peut demander l'entrée $[L_2, R_2]$ correspondant à la sortie $[S_2, T_2]$, telle que $S_1 \oplus T_1 = S_2 \oplus T_2$. Il choisit les deux messages d'entrée suivants comme suit : $[L_3, R_3] = [L_1, R_2]$ et $[L_4, R_4] = [L_2, R_1]$. Alors, $S_3 \oplus T_3 = S_4 \oplus T_4$ apparaît avec probabilité 1 dans le cas de quatre tours de schémas du type Misty, et avec probabilité $1/2^n$ dans le cas d'une permutation aléatoire.

Montrons l'affirmation concernant quatre tours de schémas du type Misty. Le choix de $[L_1, R_1]/[S_1, T_1]$ et $[L_2, R_2]/[S_2, T_2]$ implique déjà que les blocs X^2 (cf figure 2.10, $T = S \oplus f_4(X^2)$) correspondant à ces deux entrées/sorties sont égaux, car f_4 est une permutation. Ensuite, rappelons que dans l'attaque quatre points sur

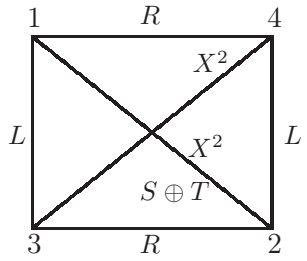

FIGURE 2.11: Les égalités utilisées dans la CPCA-2 sur M_L^4, avec quatre messages

trois tours de la sous-section 2.2.3, les seules relations $[L_1, R_1]$, $[L_2, R_2]$ aléatoires et $[L_3, R_3] = [L_1, R_2]$, $[L_4, R_4] = [L_2, R_1]$, suffisaient à conclure $S_1 \oplus S_2 \oplus S_3 \oplus S_4 = 0$. Ici, dans le cas de quatre tours, cette somme nulle correspond à $X_1^2 \oplus X_2^2 \oplus X_3^2 \oplus X_4^2 = 0$ (le bloc X^2 pour quatre tours est le bloc S pour trois tours). Nous avons donc :

$$\begin{aligned} X_1^2 &= X_2^2 \\ X_1^2 \oplus X_2^2 \oplus X_3^2 \oplus X_4^2 &= 0 \end{aligned}$$

On peut déduire $X_3^2 = X_4^2$. Par définition de ce bloc, on a alors $T_3 \oplus S_3 = T_4 \oplus T_4$.

Cette attaque fournit une CPCA-2 nécessitant quatre messages et $\mathcal{O}(1)$ calculs. Elle peut être transformée en CPA-1 et KPA de la même manière que d'habitude (voir les attaques CPA-1 précédentes, et plus particulièrement l'attaque quatre points sur trois tours sous-section 2.2.3). Cependant, les complexités respectives alors obtenues ne sont pas meilleures que pour l'attaque deux points présentée ci-dessus. En CPA-1, l'adaptation de cette attaque nécessite de l'ordre de $2^{n/2}$ messages, car l'attaquant attend d'avoir une collision sur les blocs $S \oplus T$ de deux messages, puis il choisit les deux derniers messages pour monter son attaque. En KPA, cette attaque se transforme en une attaque de complexité $\mathcal{O}\left(2^{5n/4}\right)$: l'attaquant nécessite de l'ordre de $2^{5n/2}$ paires $([L_i, R_i]/[S_i, T_i], [R_j, L_j]/[S_j, T_j])$ (soit $2^{5n/4}$ entrées/sorties aléatoires) pour avoir de bonnes chances d'obtenir deux paires (quatre messages) avec une égalité sur cinq blocs de taille n. Ces estimations comme d'habitude se déduisent du paradoxe des anniversaires. –

2.2.5 Cinq tours

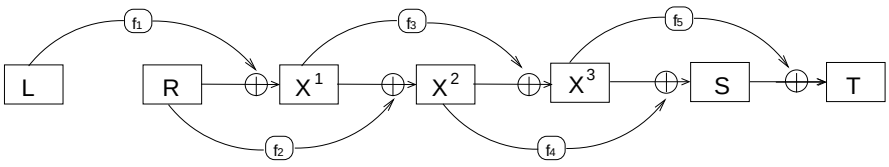

FIGURE 2.12: $\psi^5(f_1, f_2, f_3, f_4, f_5)$

Ici

$$\begin{cases} S = f_4\left(f_1(L) \oplus R \oplus f_2(R)\right) \oplus f_3\left(f_1(L) \oplus R\right) \oplus f_2(R) \oplus f_1(L) \oplus R \\ T = S \oplus f_5\left(f_3\left(f_1(L) \oplus R\right) \oplus f_2(R) \oplus f_1(L) \oplus R\right) \end{cases}$$

Pour cinq tours, les attaques génériques deux points, CPA-1 ou KPA, sont de complexité au moins $\mathcal{O}\left(2^{2n}\right)$. Nous revenons sur ces attaques au chapitre 4, et plus précisément au paragraphe 4.1.2.2. Présentons plutôt une attaque quatre points, qui fournit une complexité d'attaque inférieure à $\mathcal{O}\left(2^{2n}\right)$.

2.2.5.1 CPA-1, quatre points

L'attaque exposée consiste à s'intéresser à des quadruplets de messages du type de ceux déjà rencontrés dans des attaques précédentes sur les Misty, à savoir : $[L_1, R_1], [L_2, R_2], [L_2, R_1], [L_1, R_2]$ ($[L_3, R_3] = [L_2, R_1]$ et $[L_4, R_4] = [L_1, R_2]$).

Comme pour les autres attaques, voyons que la probabilité d'avoir certaines relations sur les blocs de sortie est différente selon que la permutation utilisée est une permutation aléatoire ou cinq tours de schémas Misty L. Les relations considérées sont les suivantes :

$$\begin{cases} S_1 \oplus T_1 = S_4 \oplus T_4 \\ S_2 \oplus T_2 = S_3 \oplus T_3 \end{cases}$$

Dans le cas d'une permutation aléatoire, ces égalités sur les blocs de sortie se produisent avec probabilité $\frac{1}{2^{2n}}$.

Dans le cas de cinq tours de schémas Misty L, remarquons que :

$$\begin{cases} S_1 \oplus T_1 = S_4 \oplus T_4 \\ S_2 \oplus T_2 = S_3 \oplus T_3 \end{cases} \Leftrightarrow \begin{cases} X_1^3 = X_4^3 \\ X_2^3 = X_3^3, \end{cases}$$

car $S \oplus T = f_5(X^3)$, et f_5 est une permutation.

On a encore les équivalences suivantes :

$$\begin{array}{rl} & \begin{cases} X_1^3 = X_4^3 \\ X_2^3 = X_3^3 \end{cases} \Leftrightarrow \begin{cases} f_3(X_1^1) \oplus X_1^2 = f_3(X_4^1) \oplus X_4^2 \\ f_3(X_2^1) \oplus X_2^2 = f_3(X_3^1) \oplus X_3^2 \end{cases} \\ \Leftrightarrow & \begin{cases} f_3\left(f_1(L_1) \oplus R_1\right) \oplus f_2(R_1) \oplus R_1 = f_3\left(f_1(L_1) \oplus R_2\right) \oplus f_2(R_2) \oplus R_2 \\ f_3\left(f_1(L_2) \oplus R_2\right) \oplus f_2(R_2) \oplus R_2 = f_3\left(f_1(L_2) \oplus R_1\right) \oplus f_2(R_1) \oplus R_1 \end{cases} \end{array}$$

Nous avons que $f_3\left(f_1(L_1) \oplus R_1\right) \oplus f_3\left(f_1(L_1) \oplus R_2\right)$ est forcément non nul ($R_1 \neq R_2$) et chaque valeur non nulle est équiprobable. Ainsi, la probabilité d'avoir la première égalité est $\frac{1}{2^n - 1}$.

Maintenant, pour évaluer la probabilité d'avoir les deux égalités vérifiées, évaluons la probabilité d'avoir la deuxième égalité vérifiée sachant que la première l'est déjà :

1. Si $f_1(L_1) \oplus R_1 = f_1(L_2) \oplus R_2$, alors on a aussi $f_1(L_1) \oplus R_2 = f_1(L_2) \oplus R_1$, et la deuxième égalité est automatiquement vérifiée si la première l'est. La probabilité d'avoir cette égalité est $\frac{1}{2^n - 1}$.

2. Si $f_1(L_1) \oplus R_1 \neq f_1(L_2) \oplus R_2$, alors on a aussi $f_1(L_1) \oplus R_2 \neq f_1(L_2) \oplus R_1$, et la probabilité d'avoir la deuxième égalité sachant la première vérifiée est $\frac{(2^n-2)\cdot 1}{(2^n-2)\cdot(2^n-3)} = \frac{1}{2^n-3}$. (Remarquons que l'on ne peut avoir $f_1(L_1) \oplus R_1 = f_1(L_2) \oplus R_1$.)

Ainsi, la probabilité conditionnelle cherchée est $\frac{1}{2^n-1} + \frac{2^n-2}{2^n-1} \cdot \frac{1}{2^n-3}$.

Finalement, la probabilité d'avoir les deux égalités de vérifiées dans le cas de cinq tours de schémas Misty L est :

$$\begin{array}{rl} & \frac{1}{2^n-1} \cdot \left(\frac{1}{2^n-1} + \frac{2^n-2}{2^n-1} \cdot \frac{1}{2^n-3} \right) \\ = & \frac{1}{(2^n-1)^2} + \frac{2^n-2}{(2^n-1)^2(2^n-3)} \\ = & \frac{2}{2^{2n}} + \mathcal{O}\left(\frac{1}{2^{3n}}\right) \end{array}$$

Nous avons donc que cette probabilité est double pour cinq tours de schémas du type Misty que pour une permutation aléatoire. Voyons comment l'attaquant peut se servir de cette différence pour monter une attaque.

Dans le cadre d'une CPA-1, il peut par exemple fixer deux valeurs L_1 et L_2, puis il évalue des messages $[L_{(1,i)}, R_{(1,i)}] = [L_1, R_i]$ et $[L_{(2,i)}, R_{(2,i)}] = [L_2, R_i]$. Il peut alors compter le nombre de quadruplets $((1,i),(2,j),(2,i),(1,j))$ $(i<j)$, pour lesquels il obtient :

$$\begin{cases} S_{(1,i)} \oplus T_{(1,i)} = S_{(1,j)} \oplus T_{(1,j)} \\ S_{(2,i)} \oplus T_{(2,i)} = S_{(2,j)} \oplus T_{(2,j)} \end{cases}$$

Ce nombre, tant dans le cas d'une permutation aléatoire que pour cinq tours de schémas Misty L, devrait être non nul au bout de $\mathcal{O}\left(2^n\right)$ messages évalués. En effet, ceci provient du fait que 2^n tels messages fournissent $\mathcal{O}\left(2^{2n}\right)$ quadruplets à considérer, et du calcul de probabilité fait plus haut. De plus, dès que ce nombre est non nul, il est deux fois plus élevé dans le cas de cinq tours de schémas Misty L que dans le cas d'une permutation aléatoire, ce qui permet à l'attaquant de conclure.

On a donc une attaque CPA-1 en $\mathcal{O}\left(2^n\right)$ calculs.

Cette attaque CPA-1 est illustrée par les tests ci-dessous (table 2.1), où :

- Nous avons considéré des messages de 32 bits (blocs de longueur $n = 16$ bits).
- La permutation aléatoire a été simulée par des schémas de Feistel, avec un nombre de tours entre 20 et 50.

La table donne le nombre de quadruplets de messages obtenus (correspondant à des messages d'indice (i,j,k,l)) présentant les relations $L_i = L_l$, $L_j = L_k$, $R_i = R_k$, $R_j = R_l$, $S_i \oplus T_i = S_j \oplus T_j$ et $S_k \oplus T_k = S_l \oplus T_l$. Notons que nous n'avons considéré qu'un seul quadruplet parmi (i,j,k,l), (j,i,l,k), (l,k,j,i) et (k,l,i,j).

Remarque :

1. Dans [GM01], Gilbert et Minier prouvent une sécurité en CPCA-2 pour M_L^5, lorsque $m \leq \sqrt{2^n}$.

2. Il existe une attaque CPA-1 par saturation en 2^n calculs, reliée aux attaques de [KW02]. Cette attaque consiste à évaluer tous les messages $[R_0, L]$, pour un R_0 fixé, par exemple, $R_0 = 0$. La somme de tous les blocs S obtenus

	cas de M_L^5	cas d'une permutation aléatoire
$3{\cdot}2^n$ messages évalués $\{[L,R], L=a,b,c,\ R\in I_n\}$	1	0.23
$4{\cdot}2^n$ messages évalués $\{[L,R], L=a,b,c,d,\ R\in I_n\}$	1.6	0.84
$5{\cdot}2^n$ messages évalués $\{[L,R], L=a,b,c,d,e,\ R\in I_n\}$	3.15	1.3

TABLE 2.1: Nombre moyen de quadruplets de messages (indices $\{i,j,k,l\}$) présentant les collisions $S_i \oplus T_i = S_j \oplus T_j$ et $S_k \oplus T_k = S_l \oplus T_l$, dans le cadre d'une attaque CPA-1. Ce nombre est donné pour une permutation correspondant à cinq tours de schémas Misty L, et pour une permutation (supposée) aléatoire.

donne 0 avec probabilité $1/2^n$ dans le cas d'une permutation aléatoire, et avec probabilité 1 dans le cas de cinq tours de schémas du type Misty.

En effet, pour cinq tours de schémas Misty L :

$$S = R \oplus f_1(L) \oplus f_2(R) \oplus f_3(R \oplus f_1(L)) \oplus f_4(R \oplus f_1(L) \oplus f_2(R)).$$

Sommer 2^n fois $f_2(R)$ ou R donne 0, car R est fixe. Par ailleurs, R étant fixe, et toutes les fonctions intervenant étant des permutations, les 2^n valeurs de sortie possibles vont apparaître une fois pour chacune d'entre elle. Or $\bigoplus_{B\in I_n} B = 0$ dès que $n > 1$. On déduit donc (avec nos notations) que $\bigoplus_{L\in I_n} S = 0$.

Notons par contre que dès que un bloc S se trouve modifié, cette attaque ne fonctionne plus. L'attaque deux points décrite précédemment est moins sensible à d'éventuelles modifications des blocs de sortie.

2.2.5.2 KPA, quatre points

L'attaque précédente se transforme en attaque à clair connu. L'attaquant attend d'obtenir les six relations sur n bits chacune de l'attaque $CPA-1$, entre deux paires de messages $([L_i,R_i]/[S_i,T_i],[L_j,R_j]/[S_j,T_j])$ et $([L_k,R_k]/[S_k,T_k],[L_l,R_l]/[S_l,T_l])$. En générant de l'ordre de 2^{3n} paires de messages, soit $\mathcal{O}\left(2^{3n/2}\right)$ messages, l'attaquant obtient avec forte probabilité au moins un quadruplet de messages avec les six relations voulues (par le paradoxe des anniversaires), dans le cas d'une permutation aléatoire. Dès que le nombre de quadruplets vérifiant les six relations voulues est non nul, l'attaquant peut distinguer entre une permutation aléatoire et six tours de schémas Misty L, car la probabilité d'avoir un tel quadruplet reste double dans le cas de M_L^6.

Cette attaque quatre points à clair connu nécessite de l'ordre de $2^{3n/2}$ messages.

Chapitre 3

Limitations de la Méthode Utilisée sur Les Premiers Tours, Principe de l'Analyse Systématique

Dans le chapitre 2, nous avons donné les meilleures attaques génériques connues, pour les cinq premiers tours de schémas de Feistel avec permutations internes, ou pour les cinq premiers tours des schémas Misty L. Rappelons que nous cherchons à distinguer un schéma (k tours de schémas de Feistel avec permutations internes ou k tours de schémas Misty L) d'une permutation aléatoire. Pour ces premiers tours, les attaques sont plus ou moins évidentes. Cependant, nous n'avons pas simplement donné une attaque deux points (ou trois ou quatre points) par nombre de tours : concernant les attaques deux points du moins, nous prétendons avoir exposé pour chaque tour celle fournissant la meilleure complexité possible. En fait, l'exposé des attaques génériques des sections 2.1 et 2.2 requiert, pour chaque nombre de tours, de réaliser toutes les attaques puis de sélectionner celle fournissant la meilleure complexité. Pour les attaques deux points, ceci consiste à considérer chaque ensemble de relations possible entre deux messages distincts d'entrée/sortie et réaliser l'attaque correspondante (nous pouvons voir en annexe, sous-sections A.1.4 et A.2.4 qu'il y a treize cas à considérer par tour, tant pour les schémas de Feistel avec permutations internes que pour les schémas du type Misty). Ainsi, non seulement il y a un certain nombre d'attaques à considérer par nombre de tours, mais en plus, dès que le nombre de tours augmente, les relations entre les blocs d'entrée et de sortie ne sont plus si évidentes. Par exemple, les attaques génériques sur cinq tours précédentes (sous-sections 2.2.5 ou 2.1.5) restent abordables, mais nous verrons dans la sous-section 3.2 ci-dessous, que réaliser une attaque générique sur six tours de l'un ou l'autre des schémas devient fastidieux.

Si nous souhaitons continuer l'analyse des attaques deux points pour un nombre de tours supérieurs, ou simplement pour valider l'affirmation que les attaques des sections 2.1 et 2.2 sont celles donnant les meilleures complexités, il serait bon de trouver une méthode générale pour obtenir rapidement toutes les attaques génériques deux points possibles. Dans ce chapitre, nous présentons une telle méthode pour l'analyse systématique des attaques génériques deux points pour les deux schémas auxquels nous nous intéressons, à savoir les schémas de Feistel avec permutations internes et les schémas Misty L. L'analyse systématique des attaques génériques deux points consiste à balayer tous les ensembles de relations possibles entre les blocs de deux entrées/sorties distinctes, et pour chacun d'entre eux, évaluer la complexité de

l'attaque correspondante. Par conséquent, comme toutes les relations possibles sont prises en compte pour un nombre de tours donné, on peut détacher avec certitude de toutes ces attaques la meilleure attaque deux points.

L'idée globale concernant une manière de généraliser les attaques du chapitre 2 est donnée à la section 3.1. Les sous-sections 3.2.1 et 3.2.2 illustrent cette section 3.1, en donnant des attaques génériques sur six tours pour les deux schémas. Ces deux exemples permettent aussi de mieux comprendre les détails plus techniques de l'exposé de l'analyse systématique, fait aux sections 3.3 et 3.4. Dans ce chapitre est introduite la notion de "coefficient H" (section 3.3, definition 8), qui est une notion clé pour l'évaluation de la complexité des attaques, comme expliqué aux sections 3.3 et 3.4. En résumé, le coefficient H pour deux entrées/sorties distinctes, correspond au nombre de k-uplets de fonctions (dans notre cas, permutations) internes d'un schéma à k tours, pouvant faire correspondre les deux entrées/sorties pour ledit schéma. La section 3.5 présente une manière de calculer ces coefficients H pour les schémas de Feistel avec permutations internes ou les schémas Misty L, résumée au théorème 1 de la sous-section 3.5.2. L'application de cette approche aux deux schémas est faite en annexe A.

Gardons en tête que nous nous intéressons aux attaques génériques deux points pour les schémas de Feistel avec permutations internes aléatoires (notés ψ^k, pour k tours), ainsi qu'aux schémas Misty L (notés M_L^k, pour k tours). Dans la présentation qui suit, les propositions seront modelées pour ces deux schémas (notamment, les fonctions internes sont dans les deux cas des permutations). Pour le cas d'autres schémas, cette analyse devrait sans doute être modifiée.

Notons enfin que lorsque le nombre de calculs nécessaires pour réaliser l'attaque est plus grand que le nombre total d'entrées, nous attaquons un générateur de permutations. Ces attaques consistent alors à distinguer un générateur de permutations ψ^k, ou M_L^k, d'un générateur de permutations aléatoires *paires*. La raison pour cela est que les permutations ψ^k et M_L^k sont paires, et l'on peut les distinguer en $\mathcal{O}\left(2^{2n}\right)$ calculs d'une permutation aléatoire quelconque.

Sommaire

3.1 Idée de la méthode générale

La méthode pour trouver les meilleures attaques génériques deux points est inspirée des travaux présentés dans [PNB06a]. On peut aussi la retrouver dans [TP09].

Essayons d'analyser les attaques faites dans les sections 2.1 et 2.2 du chapitre 2. Dans ces attaques, l'attaquant est confronté à une permutation "boîte noire", qui est soit une permutation aléatoire de I_{2n}, soit une permutation ayant une structure particulière, notamment un schéma de Feistel avec permutations internes ou un schéma Misty L, selon la situation. Le but de l'attaquant est de déterminer avec forte probabilité laquelle de la permutation aléatoire ou de la permutation structurée il a affaire. L'attaquant, pour réaliser ceci et dans le cadre d'une attaque deux points, choisit deux entrées $[L_1, R_1] \neq [L_2, R_2]$, et utilise la boîte noire pour calculer les sorties qui leur correspondent, $[S_1, T_1]$ et $[S_2, T_2]$. Il espère voir apparaître certaines relations entre les blocs de ces entrées et sorties, tout comme dans les attaques du chapitre 2. Ces relations se produisent avec une certaine probabilité, qui diffère selon que la permutation testée est une permutation aléatoire ou non. Au bout d'un certain nombre de messages évalués, la différence de probabilité d'obtenir certaines relations résulte en une différence du nombre de paires vérifiant ces relations. Par suite, pour un nombre signifiant de couples de messages calculés, l'attaquant déduit la permutation en jeu, ce qui termine l'attaque.

Ainsi, nous nous intéressons à la probabilité qu'a l'attaquant d'avoir des relations particulières sur des paires d'entrées/sorties $[L_1, R_1]/[S_1, T_1] \neq [L_2, R_2]/[S_2, T_2]$. Cette probabilité est notée P_{r} dans le cas d'une permutation aléatoire, P_{ψ^k} dans le cas d'un schéma de Feistel avec permutations internes aléatoires, et $P_{M_L^k}$ dans le cas de k tours de schémas Misty L avec permutations internes aléatoires. Avant de rentrer dans les détails, intéressons-nous au cas $k = 6$, qui n'a pas été traité dans les attaques des sections 2.1 et 2.2.

3.2 Illustrations : attaques génériques sur six tours de schémas Misty L et six tours de schémas de Feistel avec permutations internes

Pour six tours, l'analyse des attaques est déjà plus délicate que pour un nombre de tours inférieurs (voir chapitre 2). Ceci est dû au fait que plus le nombre de tours de schémas est grand, plus il est difficile de voir les relations entre les blocs

d'entrée et de sortie. Les deux exemples ci-dessous sont importants car ils motivent la formalisation de la sous-section 3.3 qui suit.

3.2.1 Illustration 1 : attaque générique sur six tours de schémas Misty L

La figure 3.1 représente six tours de schémas Misty L.

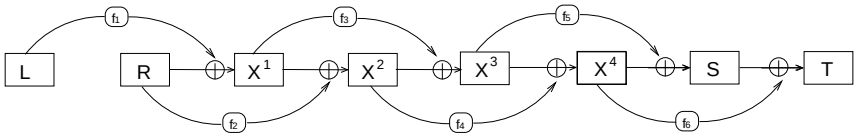

FIGURE 3.1: $M_L^6(f_1, f_2, f_3, f_4, f_5, f_6)$

3.2.1.1 Une propriété pour M_L^6

Proposition 1 *Soient* $[L_1, R_1]$ *et* $[L_2, R_2]$ *deux messages tels que* $R_1 = R_2$ *et* $L_1 \neq L_2$. *Notons* $[S_1, T_1]$ *et* $[S_2, T_2]$ *les sorties respectives de ces deux messages par une permutation. Soit* P_{r} *la probabilité d'avoir* $S_1 \oplus T_1 = S_2 \oplus T_2$ *si la permutation correspond à une permutation aléatoire. Soit encore* $P_{M_L^6}$ *la probabilité d'avoir* $S_1 \oplus T_1 = S_2 \oplus T_2$ *si la permutation correspond à six tours de schémas Misty L avec permutations internes* $(f_1, f_2, f_3, f_4, f_5, f_6)$. *On a :*

$$\begin{aligned} P_{\mathrm{r}} &= \frac{1}{2^n} - \frac{1}{2^{2n}} + \mathcal{O}\left(\frac{1}{2^{3n}}\right), \\ P_{M_L^6} &= \frac{1}{2^n} - \frac{1}{2^{3n}} + \mathcal{O}\left(\frac{1}{2^{4n}}\right). \end{aligned}$$

Démonstration : :
Dans le cas d'une permutation aléatoire, remarquons qu'il y a $2^{2n}(2^{2n}-1)$ possibilités pour la paire $([S_1, T_1], [S_2, T_2])$, les deux sorties $[S_1, T_1]$ et $[S_2, T_2]$ étant distinctes car les entrées sont distinctes. Parmi ces possibilités, $2^{2n}(2^n - 1)$ vérifient l'égalité $S_1 \oplus T_1 = S_2 \oplus T_2$. En effet, pour n'importe quelle valeur prise par $[S_1, T_1]$ parmi les 2^{2n} possibles, il y a encore $2^n - 1$ valeurs possibles pour S_2 (qui doit être différent de S_1, pour ne pas que les messages de sorties soient égaux) et la valeur de T_2 est alors fixée par la relation. Ainsi :

$$\begin{aligned} P_{\mathrm{r}} &= \frac{2^{2n}(2^n-1)}{2^{2n}(2^{2n}-1)} \\ &= \frac{2^n-1}{2^{2n}-1} \\ &= \frac{1}{2^n+1} \\ &= \frac{1}{2^n} - \frac{1}{2^{2n}} + \mathcal{O}\left(\frac{1}{2^{3n}}\right). \end{aligned}$$

Dans le cas de six tours de schémas Misty L, notons tout d'abord que :

$$R_1 = R_2 \;\Leftrightarrow\; \left\{ \begin{array}{rcl} f_1(L_1) \oplus f_1(L_2) & = & X_1^1 \oplus X_2^1 \\ X_1^2 \oplus X_2^2 & = & X_1^1 \oplus X_2^1. \end{array} \right.$$

Maintenant :

$$\begin{aligned}
& S_1 \oplus T_1 = S_2 \oplus T_2 \\
\Leftrightarrow \quad & f_6(X_1^4) = f_6(X_2^4) \\
\Leftrightarrow \quad & X_1^4 = X_2^4 \\
\Leftrightarrow \quad & f_4(X_1^2) \oplus X_1^3 = f_4(X_2^2) \oplus X_2^3 \\
\Leftrightarrow \quad & f_4\left(f_2(R_1) \oplus X_1^1\right) \oplus f_3(X_1^1) \oplus X_1^2 = f_4\left(f_2(R_2) \oplus X_2^1\right) \oplus f_3(X_2^1) \oplus X_2^2 \\
\Leftrightarrow \quad & f_4\left(f_2(R_1) \oplus f_1(L_1) \oplus R_1\right) \oplus f_3(f_1(L_1) \oplus R_1) \oplus f_1(L_1) \\
= \quad & f_4\left(f_2(R_2) \oplus f_1(L_2) \oplus R_2\right) \oplus f_3(f_1(L_2) \oplus R_2) \oplus f_1(L_2).
\end{aligned}$$

Considérons dans un premier temps la probabilité P_{part} que $f_1(L_1) \oplus f_3(f_1(L_1) \oplus R_1) = f_1(L_2) \oplus f_3(f_1(L_2) \oplus R_2)$. $L_1 \neq L_2$ et f_1 est une permutation aléatoire donc $f_1(L_1) \oplus f_1(L_2)$ peut prendre $2^n - 1$ valeurs, chacune avec la même probabilité. Nous avons aussi $2^n - 1$ valeurs possibles équiprobables pour $f_3(f_1(L_1) \oplus R_1 \oplus f_3(f_1(L_2) \oplus R_2$. En effet, $R_1 = R_2$, $L_1 \neq L_2$ et f_1 est une permutation aléatoire, donc $f_1(L_1) \oplus R_1 \neq f_1(L_2) \oplus R_2$. Comme f_3 est une permutation aléatoire, on a bien $2^n - 1$ valeurs possibles équiprobables pour $f_3(f_1(L_1) \oplus R_1 \oplus f_3(f_1(L_2) \oplus R_2)$. Finalement, la probabilité P_{part} vaut $P_{\text{part}} = \frac{1}{2^n-1}$.
Si $f_1(L_1) \oplus f_3(f_1(L_1) \oplus R_1) = f_1(L_2) \oplus f_3(f_1(L_2) \oplus R_2) : S_1 \oplus T_1 = S_2 \oplus T_2 \Leftrightarrow f_1(L_1) = f_1(L_2)$, par bijectivité de f_4, ce qui qui est impossible.
Si $f_1(L_1) \oplus f_3(f_1(L_1) \oplus R_1) \oplus f_1(L_2) \oplus f_3(f_1(L_2) \oplus R_2) = c \neq 0 : S_1 \oplus T_1 = S_2 \oplus T_2 \Leftrightarrow f_4\left(f_2(R_1) \oplus f_1(L_1) \oplus R_1\right) \oplus f_4\left(f_2(R_2) \oplus f_1(L_2) \oplus R_2\right) = c$. Pour chaque valeur de c, cette égalité arrive avec probabilité $\frac{1}{2^n-1}$, car $f_2(R_1) \oplus f_1(L_1) \oplus R_1 \neq f_2(R_2) \oplus f_1(L_2) \oplus R_2$ par bijectivité de f_1, et f_4 est une permutation aléatoire.
On peut alors conclure que :

$$\begin{aligned}
P_{M_L^6} &= (1 - P_{\text{part}}) \cdot \tfrac{1}{2^n-1} \\
&= \left(1 - \tfrac{1}{2^n-1}\right) \cdot \tfrac{1}{2^n-1} \\
&= \left(1 - \tfrac{1}{2^n}\tfrac{1}{1-1/2^n}\right) \cdot \tfrac{1}{2^n}\tfrac{1}{1-1/2^n} \\
&= \left(1 - \tfrac{1}{2^n}(1 + \tfrac{1}{2^n} + \tfrac{1}{2^{2n}} + \mathcal{O}\left(\tfrac{1}{2^{3n}}\right)\right) \cdot \tfrac{1}{2^n}\left(1 + \tfrac{1}{2^n} + \tfrac{1}{2^{2n}} + \mathcal{O}\left(\tfrac{1}{2^{3n}}\right)\right) \\
&= \left(1 - \left(\tfrac{1}{2^n} + \tfrac{1}{2^{2n}} + \tfrac{1}{2^{3n}} + \mathcal{O}\left(\tfrac{1}{2^{4n}}\right)\right) \cdot \left(\tfrac{1}{2^n} + \tfrac{1}{2^{2n}} + \tfrac{1}{2^{3n}} + \mathcal{O}\left(\tfrac{1}{2^{4n}}\right)\right) \\
&= \left(\tfrac{1}{2^n} + \tfrac{1}{2^{2n}} + \tfrac{1}{2^{3n}} + \mathcal{O}\left(\tfrac{1}{2^{4n}}\right)\right) - \left(\tfrac{1}{2^{2n}} + \tfrac{1}{2^{3n}} + \mathcal{O}\left(\tfrac{1}{2^{4n}}\right)\right) \\
&\quad - \left(\tfrac{1}{2^{3n}} + \mathcal{O}\left(\tfrac{1}{2^{4n}}\right)\right) + \mathcal{O}\left(\tfrac{1}{2^{4n}}\right) \\
&= \tfrac{1}{2^n} - \tfrac{1}{2^{3n}} + \mathcal{O}\left(\tfrac{1}{2^{4n}}\right).
\end{aligned}$$

□

3.2.1.2 KPA

La proposition 1 précédente nous permet de déduire une attaque. De plus amples explications sur la manière de déduire une attaque de l'évaluation des probabilités comme dans la proposition 1, sont données à la section 3.4. Nous exposons ici directement l'attaque. On pourra aussi se référer à cet exemple lors de la lecture de cette section 3.4.

Supposons l'attaquant en connaissance de l'ordre de m messages, ou $\frac{m(m-1)}{2}$ paires de messages $([L_i, R_i]/[S_i, T_i], [L_j, R_j]/[S_j, T_j]$ (m sera déterminé à la fin de l'analyse). Il peut compter, parmi ces paires de messages, combien d'entre elles vérifient toutes les relations de la proposition 1 :

$$\begin{cases} R_i = R_j \\ L_i \neq L_j \end{cases} \quad \begin{cases} T_i \neq T_j \\ S_i \oplus S_j = T_i \oplus T_j. \end{cases}$$

Notons X_{r} le nombre de paires vérifiant ces relations dans le cas d'une permutation aléatoire. D'après la proposition 1, on a :

$$\begin{aligned} E(X_{\mathrm{r}}) &= \tfrac{m(m-1)}{2} \cdot \tfrac{2^{2n}\cdot(2^n-1)}{2^{2n}\cdot(2^{2n}-1)} \cdot P_{\mathrm{r}} \\ &= \tfrac{m(m-1)}{2} \cdot \tfrac{1}{2^n+1} \cdot (\tfrac{1}{2^n} - \tfrac{1}{2^{2n}} + \mathcal{O}\left(\tfrac{1}{2^{3n}}\right)) \\ &= \tfrac{m(m-1)}{2} \cdot (\tfrac{1}{2^n} - \tfrac{1}{2^{2n}} + \mathcal{O}\left(\tfrac{1}{2^{3n}}\right)) \cdot (\tfrac{1}{2^n} - \tfrac{1}{2^{2n}} + \mathcal{O}\left(\tfrac{1}{2^{3n}}\right)) \\ &= \tfrac{m(m-1)}{2} \cdot (\tfrac{1}{2^{2n}} - \tfrac{2}{2^{3n}} + \tfrac{1}{2^{4n}} + \mathcal{O}\left(\tfrac{1}{2^{5n}}\right)). \end{aligned}$$

Passons à l'écart type. La justification de l'approximation suivante est donnée à la section 3.4, nous l'admettons pour le moment :

$$\begin{aligned} \sigma(X_{\mathrm{r}}) &= \mathcal{O}\left(\sqrt{E(X_{\mathrm{r}})}\right) \\ &= \mathcal{O}\left(\sqrt{\tfrac{m(m-1)}{2} \cdot \tfrac{1}{2^{2n}}}\right) \\ &= \mathcal{O}\left(\sqrt{\tfrac{m(m-1)}{2}} \tfrac{1}{2^n}\right). \end{aligned}$$

Notons $X_{M_L^6}$ le nombre de paires vérifiant les relations de la proposition 1 dans le cas de six tours de schémas Misty L avec permutations internes aléatoires. Toujours d'après la proposition 1, on a :

$$\begin{aligned} E(X_{M_L^6}) &= \tfrac{m(m-1)}{2} \cdot \tfrac{2^{2n}\cdot(2^n-1)}{2^{2n}\cdot(2^{2n}-1)} \cdot P_{M_L^6} \\ &= \tfrac{m(m-1)}{2} \cdot \tfrac{1}{2^n+1} \cdot (\tfrac{1}{2^n}\mathcal{O}\left(\tfrac{1}{2^{3n}}\right)) \\ &= \tfrac{m(m-1)}{2} \cdot (\tfrac{1}{2^n} - \tfrac{1}{2^{2n}} + \mathcal{O}\left(\tfrac{1}{2^{3n}}\right)) \cdot (\tfrac{1}{2^n}\mathcal{O}\left(\tfrac{1}{2^{3n}}\right)) \\ &= \tfrac{m(m-1)}{2} \cdot (\tfrac{1}{2^{2n}} - \tfrac{1}{2^{3n}} + \mathcal{O}\left(\tfrac{1}{2^{4n}}\right)), \end{aligned}$$

et l'on approxime :

$$\begin{aligned} \sigma(X_{M_L^6}) &= \mathcal{O}\left(\sqrt{E(X_{M_L^6})}\right) \\ &= \mathcal{O}\left(\sqrt{\tfrac{m(m-1)}{2} \cdot \tfrac{1}{2^n}}\right). \end{aligned}$$

L'attaquant peut distinguer M_L^6 d'une permutation aléatoire lorsque [1] :

$$\begin{aligned} & |E(X_{\mathrm{r}}) - E(X_{M_L^6})| > \sigma(X_{\mathrm{r}}) + \sigma(X_{M_L^6}) \\ \Leftrightarrow\ & \tfrac{m(m-1)}{2} \cdot \tfrac{1}{2^{3n}} > \sqrt{\tfrac{m(m-1)}{2}} \tfrac{1}{2^n} \\ \Leftrightarrow\ & \tfrac{m(m-1)}{2} > 2^{4n}. \end{aligned}$$

1. Toutes les justifications sont données section 3.4

Lorsque l'on attaque une seule permutation M_L^6, le nombre de messages qu'il est possible d'évaluer est 2^{2n} (les messages sont sur n bits). La complexité de cette attaque est de $\mathcal{O}\left(2^{2n}\right)$, ainsi lorsqu'une seule permutation est utilisée, cette attaque a une probabilité non négligeable de succès, mais si l'on veut avoir une probabilité de succès plus grande, nous supposons attaquer un générateur de permutations M_L^6. Pour plus de détails, voir la sous-section 3.4.2.

3.2.1.3 CPA-1

La même attaque en CPA-1, ne fournit pas une meilleure complexité. L'intuition de cela est que lorsque l'on attaque un générateur de permutations, on utilise toutes les entrées possibles de chaque permutation. Ceci est détaillé plus loin, à la section 3.4. Ainsi, une attaque CPA-1 ou KPA donne la même complexité.
Remarque :

1. Il existe une attaque quatre points sur M_L^6 qui fournit des attaques avec la même complexité que l'attaque deux points ci-dessus. Pour quatre messages distincts $[L_1, R_1]/[S_1, T_1]$, $[L_2, R_2]/[S_2, T_2]$, $[L_3, R_3]/[S_3, T_3]$, $[L_4, R_4]/[S_4, T_4]$, cette attaque exploite les relations :

$$\begin{cases} L_1 = L_3 \\ L_2 = L_4 \\ R_1 = R_4 \\ R_2 = R_3 \\ S_1 \oplus T_1 = S_4 \oplus T_4 \\ S_2 \oplus T_2 = S_3 \oplus T_3, \end{cases}$$

   comme les autres attaques quatre points présentées sur les schémas Misty L (cf. section 2.2, sous-sections 2.2.3, 2.2.4 et 2.2.5). Cette attaque peut se trouver dans [NPT09].

2. Il existe une attaque par saturation similaire à celle indiquée pour cinq tours (sous-section 2.2.5 de la section 2.2). Cette attaque consiste à compter le nombre de paires de messages $([L_1, R_1], [L_2, R_2])$, telles que :

$$\begin{cases} R_1 = R_2 \\ S_1 \oplus T_1 = S_2 \oplus T_2. \end{cases}$$

   Dans le cas de six tours de schémas Misty L, soit $([L_1, R_1], [L_2, R_2])$ une paire de messages d'entrée vérifiant ces relations. Alors la paire $([L'_1, R'_1], [L'_2, R'_2])$, où :

$$\begin{cases} f_1(L'_1) \oplus R'_1 = X_2^1, \ f_2(R'_1) \oplus X_2^1 = X_1^2, \\ f_1(L'_2) \oplus R'_2 = X_1^1, \ f_2(R'_2) \oplus X_1^1 = X_2^2, \end{cases}$$

   va également vérifier ces relations. Ceci figure dans [NPT09]. Ainsi, en sommant sur toutes les entrées possibles, dans le cas de six tours de schémas Misty L, le nombre de paires vérifiant ces relations est toujours pair. Dans le cas d'une permutation aléatoire, ce nombre est pair avec probabilité 1/2.

Cette attaque fonctionne avec probabilité $\mathcal{O}\left(2^{2n}\right)$, tout comme l'attaque deux points précédente. Cependant, et à la différence de celle-ci, cette attaque est sensible à une modification de quelques valeurs. ceci est le même phénomène observé pour l'attaque par saturation sur cinq tours de la sous-section 2.2.5.

Pour les schémas Misty L, six tours est le nombre de tours maximal pour lequel on connaisse des attaques en $\mathcal{O}\left(2^{2n}\right)$ calculs permettant de distinguer M_L^k ou des générateurs de permutations M_L^k, lorsque plus d'une permutation est utilisée de permutations aléatoires avec signature paire.

3.2.2 Illustration 2 : attaque générique sur six tours de schémas de Feistel avec permutations internes

Six tours de schémas de Feistel correspondent à la figure 3.2. On a les relations suivantes :

$$\begin{cases} S = & f_5\left(f_4(f_3(f_2(f_1(L)\oplus R)\oplus R)\oplus f_1(R)\oplus L)\oplus f_2(f_1(R)\oplus L)\right) \\ & \oplus f_3(f_2(f_1(R)\oplus L)\oplus R)\oplus f_1(R)\oplus L \\ T = & f_6(S)\oplus f_4\left(f_3(f_2(f_1(R)\oplus L)\oplus R)\oplus f_1(R)\oplus L\right)\oplus f_2(f_1(R)\oplus L) \end{cases}$$

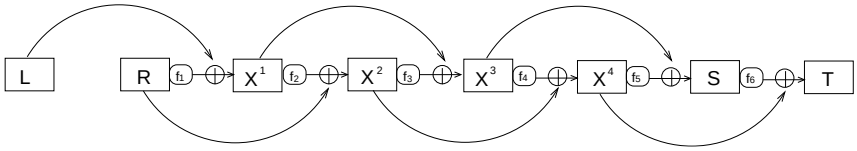

FIGURE 3.2: $\psi^6(f_1, f_2, f_3, f_4, f_5, f_6)$

3.2.2.1 Une propriété pour ψ^6

Proposition 2 *Soient $[L_1, R_1]$ et $[L_2, R_2]$ deux messages tels que $R_1 = R_2$ et $L_1 \neq L_2$, et $[S_1, T_1]$ et $[S_2, T_2]$ les images respectives de ces messages par une permutation. Notons P_{r} la probabilité que $S_1 \oplus S_2 = L_1 \oplus L_2$ et $T_1 = T_2$ lorsque la permutation est une permutation aléatoire. Soit aussi P_{ψ^6} la probabilité d'avoir ces deux mêmes relations sur les blocs de sortie lorsque la permutation correspond à six tours de schémas de Feistel avec permutations internes $(f_1, f_2, f_3, f_4, f_5, f_6)$. Nous avons :*

$$P_{\mathrm{r}} = \frac{1}{2^{2n}} + \mathcal{O}\left(\frac{1}{2^{4n}}\right),$$
$$P_{\psi^6} = \frac{1}{2^{2n}} + \frac{1}{2^{3n}} + \mathcal{O}\left(\frac{1}{2^{4n}}\right).$$

Démonstration :
Pour une permutation aléatoire, le nombre de possibilités totales pour $([S_1, T_1], [S_2, T_2])$ est $2^{2n} \cdot (2^{2n} - 1)$, car les messages d'entrée sont distincts. Le

nombre de telles deux sorties vérifiant $T_1 = T_2$ et $S_1 \oplus S_2 = L_1 \oplus L_2$ est $2^n \cdot 2^n = 2^{2n}$. Ainsi :

$$\begin{aligned} P_{\mathrm{r}} &= \frac{2^{2n}}{2^{2n} \cdot (2^{2n}-1)} \\ &= \frac{1}{2^{2n}-1} \\ &= \frac{1}{2^{2n}} \cdot \frac{1}{1-1/2^{2n}} \\ &= \frac{1}{2^{2n}} \cdot \left(1 + \frac{1}{2^{2n}} + \frac{1}{2^{4n}} + \frac{1}{2^{6n}} + \ldots\right) \\ &= \frac{1}{2^{2n}} + \mathcal{O}\left(\frac{1}{2^{4n}}\right). \end{aligned}$$

Pour six tours de schémas de Feistel, notons tout d'abord que :

$$R_1 = R_2 \;\Leftrightarrow\; \left\{ \begin{array}{rcl} L_1 \oplus L_2 & = & X_1^1 \oplus X_2^1 \\ X_1^2 \oplus X_2^2 & = & f_2(X_1^1) \oplus f_2(X_2^2). \end{array} \right.$$

Maintenant, avec ces relations, considérons les égalité $S_1 \oplus L_1 \oplus S_2 \oplus L_2 = 0$ et $T_1 = T_2$.

1. Notons P_{part} la probabilité d'avoir $S_1 \oplus L_1 \oplus S_2 \oplus L_2 = 0$. Nous avons la suite d'équivalences suivante pour $S_1 \oplus L_1 \oplus S_2 \oplus L_2 = 0$:

$$\begin{array}{rl} & S_1 \oplus L_1 \oplus S_2 \oplus L_2 = 0 \\ \Leftrightarrow & f_5(X_1^4) \oplus X_1^3 \oplus L_1 \oplus f_5(X_2^4) \oplus X_2^3 \oplus L_2 = 0 \\ \Leftrightarrow & f_5\left(f_4(X_1^3) \oplus X_1^2\right) \oplus f_3(X_1^2) \oplus X_1^1 \oplus L_1 \\ = & \oplus f_5\left(f_4(X_2^3) \oplus X_2^2\right) \oplus f_3(X_2^2) \oplus X_2^1 \oplus L_2 \\ \Leftrightarrow & f_5\left(f_4(f_3(X_1^2) \oplus X_1^1) \oplus f_2(X_1^1) \oplus R_1\right) \oplus f_3\left(f_2(X_1^1) \oplus R_1\right) \\ = & f_5\left(f_4(f_3(X_2^2) \oplus X_2^1) \oplus f_2(X_2^1) \oplus R_2\right) \oplus f_3\left(f_2(X_2^1) \oplus R_2\right) = 0 \\ \Leftrightarrow & f_5\left(f_4(f_3(f_2(X_1^1) \oplus R_1) \oplus f_1(R_1) \oplus L_1 \oplus f_2(f_1(R_1) \oplus L_1) \oplus R_1\right) \\ & \oplus f_3\left(f_2(f_1(R_1) \oplus L_1) \oplus R_1\right) \\ = & f_5\left(f_4(f_3(f_2(X_2^1) \oplus R_2) \oplus f_1(R_2) \oplus L_2 \oplus f_2(f_1(R_2) \oplus L_2) \oplus R_2\right) \\ & \oplus f_3\left(f_2(f_1(R_2) \oplus L_2) \oplus R_2\right) \\ \Leftrightarrow & f_5(f_4(f_3(f_2(f_1(R_1) \oplus L_1) \oplus R_1) \oplus f_1(R_1) \oplus L_1 \oplus f_2(f_1(R_1) \oplus L_1) \\ & \oplus R_1) \oplus f_3\left(f_2(f_1(R_1) \oplus L_1) \oplus R_1\right) \\ = & f_5(f_4(f_3(f_2(f_1(R_2) \oplus L_2) \oplus R_2) \oplus f_1(R_2) \oplus L_2 \oplus f_2(f_1(R_2) \oplus L_2) \\ & \oplus R_2) \oplus f_3\left(f_2(f_1(R_2) \oplus L_2) \oplus R_2\right). \end{array}$$

Remarquons que $f_3\left(f_2(f_1(R_1) \oplus L_1) \oplus R_1\right)$ est forcément différent de $f_3\left(f_2(f_1(R_2) \oplus L_2) \oplus R_2\right)$. De plus, $f_3\left(f_2(f_1(R_1) \oplus L_1) \oplus R_1\right) \oplus f_3\left(f_2(f_1(R_2) \oplus L_2) \oplus R_2\right)$ prend chaque valeur non nulle avec même probabilité $\frac{1}{2^n-1}$. En effet, $f_2(f_1(R_1) \oplus L_1) \neq f_2(f_1(R_2) \oplus L_2)$ car $f_1(R_1) = f_1(R_2)$, $L_1 \neq L_2$ et f_2 est bijective. Par suite

$f_2(f_1(R_1) \oplus L_1) \oplus R_1 \neq f_2(f_1(R_2) \oplus L_2) \oplus R_2$ et l'on a le résultat car f_3 est une permutation aléatoire.

Par suite, $S_1 \oplus S_2 = L_1 \oplus L_2$ ne peut arriver si
$f_5\left(f_4(f_3(f_2(f_1(R_1) \oplus L_1) \oplus R_1) \oplus f_1(R_1) \oplus L_1 \oplus f_2(f_1(R_1) \oplus L_1) \oplus R_1\right)$
$= f_5\left(f_4(f_3(f_2(f_1(R_2) \oplus L_2) \oplus R_2) \oplus f_1(R_2) \oplus L_2 \oplus f_2(f_1(R_2) \oplus L_2) \oplus R_2\right).$
Or, on a le lemme suivant :

Lemme 1 *la probabilité d'avoir :*

$$f_5\left(f_4(f_3(f_2(f_1(R_1) \oplus L_1) \oplus R_1) \oplus f_1(R_1) \oplus L_1 \oplus f_2(f_1(R_1) \oplus L_1) \oplus R_1\right)$$
$$= f_5\left(f_4(f_3(f_2(f_1(R_2) \oplus L_2) \oplus R_2) \oplus f_1(R_2) \oplus L_2 \oplus f_2(f_1(R_2) \oplus L_2) \oplus R_2\right),$$

est $\left(1 - \frac{1}{2^n-1}\right) \cdot \frac{1}{2^n-1}$.

Démonstration : Pour s'en convaincre, voyons les équivalences suivantes :

$$\begin{array}{rcl}
 & f_5(f_4(f_3(f_2(f_1(R_1) \oplus L_1) \oplus R_1) \oplus f_1(R_1) \oplus L_1 \\
 & \oplus f_2(f_1(R_1) \oplus L_1) \oplus R_1) \\
= & f_5(f_4(f_3(f_2(f_1(R_2) \oplus L_2) \oplus R_2) \oplus f_1(R_2) \oplus L_2 \\
 & \oplus f_2(f_1(R_2) \oplus L_2) \oplus R_2) \\
\Leftrightarrow & f_4(f_3(f_2(f_1(R_1) \oplus L_1) \oplus R_1) \oplus f_1(R_1) \oplus L_1) \\
 & \oplus f_2(f_1(R_1) \oplus L_1) \oplus R_1 \\
= & f_4(f_3(f_2(f_1(R_2) \oplus L_2) \oplus R_2) \oplus f_1(R_2) \oplus L_2) \\
 & \oplus f_2(f_1(R_2) \oplus L_2) \oplus R_2 \\
\Leftrightarrow & f_4(f_3(f_2(f_1(R_1) \oplus L_1) \oplus R_1) \oplus f_1(R_1) \oplus L_1) \oplus f_2(f_1(R_1) \oplus L_1) \\
= & f_4(f_3(f_2(f_1(R_2) \oplus L_2) \oplus R_2) \oplus f_1(R_2) \oplus L_2) \oplus f_2(f_1(R_2) \oplus L_2).
\end{array}$$

Maintenant, notons que $f_2(f_1(R_1) \oplus L_1) \neq f_2(f_1(R_2) \oplus L_2)$, car $f_1(R_1) \oplus L_1 \neq f_2(R_2) \oplus L_2$, et f_2 est une permutation aléatoire. Pour les mêmes raisons, les valeurs possibles pour $f_2(f_1(R_1) \oplus L_1) \oplus f_2(f_1(R_2) \oplus L_2)$ sont toutes les valeurs non nulles et leur probabilité est $\frac{1}{2^n-1}$.

La probabilité d'avoir $f_4(f_3(f_2(f_1(R_1) \oplus L_1) \oplus R_1) \oplus f_1(R_1) \oplus L_1) = f_4(f_3(f_2(f_1(R_2) \oplus L_2) \oplus R_2) \oplus f_1(R_2) \oplus L_2)$ est la probabilité que $f_3(f_2(f_1(R_1) \oplus L_1) \oplus R_1) \oplus f_3(f_2(f_1(R_2) \oplus L_2) \oplus R_2) = L_1 \oplus L_2$. Or cette probabilité est $\frac{1}{2^n-1}$ (on a déjà vu que ces images de f_3 sont distinctes et équiprobables).

Lorsque cette égalité sur les images de f_4 a lieu, alors l'égalité du lemme impliquant f_5 est impossible, car $f_2(f_1(R_1) \oplus L_1) \neq f_2(f_1(R_2) \oplus L_2)$. Lorsque l'égalité précédente sur les images de f_4 n'a pas lieu, alors l'égalité du lemme arrive avec probabilité $\frac{1}{2^n-1}$, car la probabilité pour $f_2(f_1(R_1) \oplus L_1) \oplus f_2(f_1(R_2) \oplus L_2)$ de prendre n'importe quelle valeur non nulle est $\frac{1}{2^n-1}$.

Ainsi, la probabilité recherchée est bien $\left(1 - \frac{1}{2^n-1}\right) \cdot \frac{1}{2^n-1}$. □

Revenons à la probabilité P_{part} d'avoir $S_1 \oplus S_2 = L_1 \oplus L_2$. Celle-ci vaut alors :

$$P_{\text{part}} = \left(1 - \left(1 - \frac{1}{2^n - 1}\right) \cdot \frac{1}{2^n - 1}\right) \cdot \frac{1}{2^n - 1}.$$

Entre parenthèses, on a la probabilité de ne pas avoir l'égalité du lemme 1 sur les images de f_5. L'autre valeur, $\frac{1}{2^n-1}$, est la probabilité pour $f_3\left(f_2(f_1(R_1)\oplus L_1)\oplus R_1\right)\oplus f_3\left(f_2(f_1(R_2)\oplus L_2)\oplus R_2\right)$ de prendre une valeur non nulle fixée.

Cette probabilité peut encore s'écrire :

$$\begin{aligned} P_{\text{part}} = & \left(1-\left(1-\tfrac{1}{2^n-1}\right)\right)\cdot\tfrac{1}{2^n-1} \\ = & \tfrac{1}{(2^n-1)}-\tfrac{1}{(2^n-1)^2}+\tfrac{1}{(2^n-1)^3}. \end{aligned}$$

2. Passons à l'autre égalité :

$$\begin{aligned} & T_1\oplus T_2=0 \\ \Leftrightarrow\quad & f_6(S_1)\oplus X_1^4\oplus f_6(S_2)\oplus X_2^4=0 \\ \Leftrightarrow\quad & f_6(S_1)\oplus f_4(X_1^3)\oplus X_1^2\oplus f_6(S_1)\oplus f_4(X_2^3)\oplus X_2^2=0 \\ \Leftrightarrow\quad & f_6(S_1)\oplus f_4\left(f_3(X_1^2)\oplus X_1^1\right)\oplus f_2(X_1^1)\oplus R_1 \\ = \quad & f_6(S_2)\oplus f_4\left(f_3(X_2^2)\oplus X_2^1\right)\oplus f_2(X_2^1)\oplus R_2 \\ \Leftrightarrow\quad & f_6(S_1)\oplus f_4\left(f_3(f_2(X_1^1)\oplus R_1)\oplus f_1(R_1)\oplus L_1\right) \\ & \oplus f_2(f_1(R_1)\oplus L_1)\oplus R_1 \\ = \quad & f_6(S_2)\oplus f_4\left(f_3(f_2(X_2^1)\oplus R_2)\oplus f_1(R_2)\oplus L_2\right) \\ & \oplus f_2(f_1(R_2)\oplus L_2)\oplus R_2 \\ \Leftrightarrow\quad & f_6(S_1)\oplus f_4(f_3(f_2(f_1(R_1)\oplus L_1)\oplus R_1) \\ & \oplus f_1(R_1)\oplus L_1)\oplus f_2(f_1(R_1)\oplus L_1) \\ = \quad & f_6(S_2)\oplus f_4(f_3(f_2(f_1(R_2)\oplus L_2)\oplus R_2) \\ & \oplus f_1(R_2)\oplus L_2)\oplus f_2(f_1(R_2)\oplus L_2). \end{aligned}$$

Remarquons que les valeurs possibles pour $f_6(S_1)\oplus f_6(S_2)$ sont toutes les valeurs non nulles, avec probabilité $\frac{1}{2^n-1}$ chacune. En effet, nous avons $S_1\neq S_2$ (car $T_1=T_2$ et les messages sont distincts) et f_6 est une permutation aléatoire.

Les valeurs possibles pour :

$$\begin{aligned} & f_2(f_1(R_1)\oplus L_1)\oplus f_2(f_1(R_2)\oplus L_2) \quad et \\ & f_4\left(f_3(f_2(f_1(R_1)\oplus L_1)\oplus R_1)\oplus f_1(R_1)\oplus L_1\right) \\ & \oplus f_4\left(f_3(f_2(f_1(R_2)\oplus L_2)\oplus R_2)\oplus f_1(R_2)\oplus L_2\right) \end{aligned} \quad ,$$

sont déjà prises en compte dans l'évaluation de la probabilité que $S_1\oplus S_2=L_1\oplus L_2$, où elles avaient été choisies différentes (ceci est important pour avoir un choix de $f_6(S_1)\oplus f_6(S_2)$ cohérent). Ainsi, pour avoir la probabilité P_{ψ^6} cherchée, il reste à multiplier la probabilité d'avoir $S_1\oplus S_2=L_1\oplus L_2$ par la probabilité d'avoir une valeur fixée non nulle pour $f_6(S_1)\oplus f_6(S_2)$.

Au final :

$$\begin{aligned} P_{\psi^6} & = P_{\text{part}}\cdot\tfrac{1}{2^n-1} \\ & = \left(\tfrac{1}{(2^n-1)}-\tfrac{1}{(2^n-1)^2}+\tfrac{1}{(2^n-1)^3}\right)\cdot\tfrac{1}{2^n-1} \\ & = \tfrac{1}{(2^n-1)^2}-\tfrac{1}{(2^n-1)^3}+\tfrac{1}{(2^n-1)^4} \\ & = \tfrac{1}{2^{2n}}(1+\tfrac{2}{2^n}+\mathcal{O}\left(\tfrac{1}{2^{2n}}\right))-\tfrac{1}{2^{3n}}(1+\tfrac{3}{2^n}+\mathcal{O}\left(\tfrac{1}{2^{2n}}\right))+\mathcal{O}\left(\tfrac{1}{2^{4n}}\right) \\ & = (\tfrac{1}{2^{2n}}+\tfrac{2}{2^{3n}}+\mathcal{O}\left(\tfrac{1}{2^{4n}}\right))-(\tfrac{1}{2^{3n}}+\mathcal{O}\left(\tfrac{1}{2^{5n}}\right))+\mathcal{O}\left(\tfrac{1}{2^{4n}}\right) \\ & = \tfrac{1}{2^{2n}}+\tfrac{1}{2^{3n}}+\mathcal{O}\left(\tfrac{1}{2^{4n}}\right). \end{aligned}$$

□

3.2.2.2 KPA

La proposition 2 précédente nous permet de déduire une attaque. Ici encore, l'attaque est exposé directement. Des explications sur la manière de dériver une attaque du calcul des probabilités de la proposition 2, sont données à la section 3.4.

Supposons l'attaquant en connaissance de m messages, c'est à dire $\frac{m(m-1)}{2}$ paires de messages $([L_i, R_i]/[S_i, T_i], [L_j, R_j]/[S_j, T_j]$ (m sera déterminé à la fin de l'analyse). Il peut alors compter, parmi ces $\frac{m(m-1)}{2}$ paires, combien d'entre elles vérifient toutes les relations de la proposition 2 :

$$\begin{cases} R_i = R_j, & L_i \neq L_j \\ T_i = T_j, & S_i \oplus S_j = L_i \oplus L_j. \end{cases}$$

Notons X_{r} le nombre de paires vérifiant ces relations dans le cas d'une permutation aléatoire. D'après la proposition 2, on a :

$$\begin{aligned} E(X_{\mathrm{r}}) &= \tfrac{m(m-1)}{2} \cdot \tfrac{2^{2n}\cdot(2^n-1)}{2^{2n}\cdot(2^{2n}-1)} \cdot P_{\mathrm{r}} \\ &= \tfrac{m(m-1)}{2} \cdot \tfrac{1}{2^n+1} \cdot (\tfrac{1}{2^{2n}} + \mathcal{O}\left(\tfrac{1}{2^{4n}}\right)) \\ &= \tfrac{m(m-1)}{2} \cdot (\tfrac{1}{2^n} - \tfrac{1}{2^{2n}} + \mathcal{O}\left(\tfrac{1}{2^{3n}}\right)) \cdot (\tfrac{1}{2^{2n}} + \mathcal{O}\left(\tfrac{1}{2^{4n}}\right)) \\ &= \tfrac{m(m-1)}{2} \cdot \tfrac{1}{2^{3n}} - \tfrac{1}{2^{4n}} + \mathcal{O}\left(\tfrac{1}{2^{5n}}\right). \end{aligned}$$

On verra section 3.4 que l'on peut approximer l'écart type de X_{r} par la racine de l'espérance de X_{r} :

$$\begin{aligned} \sigma(X_{\mathrm{r}}) &= \mathcal{O}\left(\sqrt{E(X_{\mathrm{r}})}\right) \\ &= \mathcal{O}\left(\sqrt{\tfrac{m(m-1)}{2}} \cdot \tfrac{1}{2^{3n/2}}\right) \\ &= \mathcal{O}\left(\sqrt{\tfrac{m(m-1)}{2}} \tfrac{1}{2^{3n/2}}\right). \end{aligned}$$

Notons X_{ψ^6} ce nombre de paires dans le cas de six tours de schémas de Feistel avec permutations internes aléatoires. On a de même :

$$\begin{aligned} E(X_{\psi^6}) &= \tfrac{m(m-1)}{2} \cdot \tfrac{2^{2n}\cdot(2^n-1)}{2^{2n}\cdot(2^{2n}-1)} \cdot P_{\psi^6} \\ &= \tfrac{m(m-1)}{2} \cdot \tfrac{1}{2^n+1} \cdot (\tfrac{1}{2^{2n}} + \tfrac{1}{2^{3n}} + \mathcal{O}\left(\tfrac{1}{2^{4n}}\right)) \\ &= \tfrac{m(m-1)}{2} \cdot (\tfrac{1}{2^n} - \tfrac{1}{2^{2n}} + \mathcal{O}\left(\tfrac{1}{2^{3n}}\right)) \cdot (\tfrac{1}{2^{2n}} + \tfrac{1}{2^{3n}} + \mathcal{O}\left(\tfrac{1}{2^{4n}}\right)) \\ &= \tfrac{m(m-1)}{2} \cdot \tfrac{1}{2^{3n}} + \mathcal{O}\left(\tfrac{1}{2^{5n}}\right), \\ \sigma(X_{\psi^6}) &= \mathcal{O}\left(\sqrt{E(X_{\psi^6})}\right) \\ &= \mathcal{O}\left(\sqrt{\tfrac{m(m-1)}{2}} \cdot \tfrac{1}{2^{3n/2}}\right). \end{aligned}$$

L'attaquant peut distinguer ψ^6 d'une permutation aléatoire lorsque [2] :

$$\begin{array}{rl} & |E(X_{\mathrm{r}}) - E(X_{\psi^6})| > \sigma(X_{\mathrm{r}}) + \sigma(X_{\psi^6}) \\ \Leftrightarrow & \frac{m(m-1)}{2} \cdot \frac{1}{2^{4n}} > \sqrt{\frac{m(m-1)}{2}} \frac{1}{2^{3n/2}} \\ \Leftrightarrow & \frac{m(m-1)}{2} > 2^{5n}. \end{array}$$

Le nombre de paires que l'attaquant doit distinguer est supérieur au nombre de paires possibles d'évaluer avec une seule permutation. Plaçons dans le cas où l'attaquant souhaite attaquer un générateur de permutations aléatoires, c'est à dire, il a accès à $\lambda \geq 1$ permutations. Alors :

$$\begin{array}{rcl} E(X_{\mathrm{r}}) & = & \lambda \frac{m(m-1)}{2} \cdot \frac{1}{2^{3n}} - \frac{1}{2^{4n}} + \mathcal{O}\left(\frac{1}{2^{5n}}\right), \\ E(X_{\psi^6}) & = & \lambda \frac{m(m-1)}{2} \cdot \frac{1}{2^{3n}} + \mathcal{O}\left(\frac{1}{2^{5n}}\right), \\ \sigma(X_{\mathrm{r}}) & = & \mathcal{O}\left(\sqrt{\lambda \frac{m(m-1)}{2}} \frac{1}{2^{3n/2}}\right), \\ \sigma(X_{\psi^6}) & = & \mathcal{O}\left(\sqrt{\frac{m(m-1)}{2}} \cdot \frac{1}{2^{3n/2}}\right). \end{array}$$

De sorte que l'attaquant peut distinguer un générateur de permutations aléatoires d'un générateur de permutations ψ^6 lorsque :

$$\begin{array}{rl} & |E(X_{\mathrm{r}}) - E(X_{\psi^6})| > \sigma(X_{\mathrm{r}}) + \sigma(X_{\psi^6}) \\ \Leftrightarrow & \lambda \frac{m(m-1)}{2} \cdot \frac{1}{2^{4n}} > \sqrt{\lambda \frac{m(m-1)}{2}} \frac{1}{2^{3n/2}} \\ \Leftrightarrow & \sqrt{\lambda} > \frac{2^{4n}}{\sqrt{\frac{m(m-1)}{2}} \cdot 2^{3n/2}}. \end{array}$$

Le nombre de paires messages considérées par permutations est supposé maximal, *i.e.* $m \simeq 2^{2n}$. On trouve alors :

$$\begin{array}{rl} & \lambda > \frac{2^{8n}}{2^{4n} \cdot 2^{3n}} \\ \Leftrightarrow & \lambda > 2^n. \end{array}$$

Ainsi, pour distinguer un générateur de permutations aléatoires d'un générateur de permutations ψ^6 en utilisant les relations de la proposition 2, l'attaquant doit évaluer toutes les entrées possibles de $\mathcal{O}\left(2^n\right)$ permutations, soit faire $\mathcal{O}\left(2^{3n}\right)$ calculs.

3.2.2.3 CPA-1

De même que pour M_L^6, et pour les mêmes raisons détaillées section 3.4, la même attaque en CPA-1, ne fournit pas une meilleure complexité.

3.3 Probabilités P_{r}, P_{ψ^k} et $P_{M_L^k}$, Coefficients H

Pour trouver les attaques pour un nombre de tours plus grand, nous allons devoir évaluer les probabilités P_{r}, $P_{M_L^k}$, P_{ψ^k}, pour différentes relations entre les blocs d'entrée et sortie de deux messages.

2. Des explications sont données à la section 3.4.

Une remarque importante est que les probabilités auxquelles nous nous intéressons diffèrent selon le type d'attaque montée (KPA, CPA, etc). Pour s'en convaincre, on peut voir que dans les attaques sur les cinq premiers tours présentées plus haut, les complexités n'étaient pas les mêmes selon le type d'attaque. Dans les exemples sur six tours donnés précédemment, les propositions établies se plaçaient en fait dans le cas d'une attaque à clair choisi (CPA-1), car l'énoncé supposait données deux entrées distinctes avec la relation $R_1 = R_2$. Ensuite, pour adapter le résultat à une KPA, il a fallu encore évaluer la probabilité d'obtenir deux telles entrées.

Nous souhaitons établir une formule nous donnant P_{r}, P_{ψ^k} et $P_{M_L^k}$ selon le type d'attaque (KPA ou CPA), *i.e.* nous souhaitons pouvoir appliquer directement le résultat pour évaluer la complexité de l'attaque considérée.

Pour pouvoir établir de telles formules, nous introduisons une notion. Plaçons dans le cadre d'une attaque deux points. L'attaquant est en possession d'un certain nombre de couples de messages d'entrée/sortie et considère certaines contraintes sur les blocs d'entrée et sortie. Par exemple, pour un couple de messages $[L_1, R_1]/[S_1, T_1] \neq [L_2, R_2]/[S_2, T_2]$, il considère des équations du type $L_1 = L_2$, $L_1 \oplus L_2 = T_1 \oplus T_2$, etc, comme dans les attaques deux points présentées précédemment (attaques sur les cinq premiers tours, sections 2.1 et 2.2 ; attaques sur six tours, sous-section 3.2.1). Dans ces conditions, nous définissons la valeur suivante :

Définition 7 (n_e) *Étant données des contraintes sur des blocs de couples entrées/sorties, on définit la valeur n_e comme suit, selon le pouvoir supposé de l'attaquant de choisir ou non ses entrées et sorties :*

1. *Dans le cadre d'une attaque à clair connu (KPA), n_e est le nombre total d'égalités demandées par les contraintes.*
2. *Dans le cadre d'une attaque à clair choisi (CPA), n_e dénote le nombre total d'égalités demandées par les contraintes, auquel on soustrait le nombre d'égalités impliquant les entrées uniquement.*
3. *Dans le cadre d'une attaque à clair et chiffré choisis (CPCA), l'attaquant peut choisir ses messages de manière à ce que certaines des égalités demandées par les contraintes soient déjà vérifiées. Le paramètre n_e dénote alors le nombre d'égalités restant à être vérifiées pour satisfaire toutes les égalités des contraintes.*

*En résumé, n_e est le nombre d'égalités sur les blocs demandées par les contraintes, apparaissant (éventuellement) après évaluation de paires messages, que l'attaquant ne peut choisir d'avoir au départ. Cette valeur est encore appelée nombre d'*égalités non-imposées *(dans le sens non-imposées au départ par l'attaquant).*

Explication : Parmi les égalités entre les blocs d'entrée et sortie que l'attaquant cherche à tester sur une paire de messages, c'est à dire, les équations des contraintes, certaines peuvent être vérifiées pour tous les couples, dû à la classe d'attaque considérée. Par exemple, dans le cadre d'une attaque à clair choisi (CPA), l'égalité $R_1 = R_2$ se produit avec probabilité 1, car l'attaquant peut l'imposer sur ses messages. Par

contre, dans le cadre de cette même attaque, l'égalité $R_1 \oplus R_2 = S_1 \oplus S_2$ ne peut être imposée par l'attaquant et arrive a priori avec probabilité plus faible.
Ceci explique la terminologie "égalités non-imposées" concernant les égalités entre les blocs ne pouvant être imposées avec probabilité 1 par l'attaquant au moment du choix des messages.

Considérons toujours une série de relations sur les blocs d'entrée et de sortie de deux messages. Établissons maintenant les formules pour les probabilités P_{r}, P_{ψ^k} et $P_{M_L^6}$ recherchées. Pour chacune des permutations considérées, on s'intéresse à deux valeurs, qu'il suffira de multiplier entre elle ensuite pour avoir la probabilité correspondante voulue :

1. Tout d'abord, la probabilité d'avoir deux entrée avec les relations souhaitées sur leurs blocs (cette probabilité peut valoir 1, comme par exemple dans le cas d'une attaque à clair choisi).
2. Deuxièmement, la probabilité pour que les images respectives par la permutation de ces entrées soient deux messages de sortie tels que toutes les relations soient vérifiées. Cette deuxième probabilité peut être obtenue en calculant la probabilité pour que les images de la permutation de deux telles entrées soit un couple de messages de sortie en particulier, multipliée par le nombre de couples "admissibles", dans le sens nombre de couples permettant de satisfaire les équations voulues (étant données les entrées).

Proposition 3 *Pour une permutation aléatoire, la probabilité P_{r} pour un attaquant d'avoir deux couples d'entrée/sortie $[L_1, R_1]/[S_1, T_1] \neq [L_2, R_2]/[S_2, T_2]$ vérifiant les relations sur leur blocs correspondant à un certain ensemble de contraintes peut être approximée par :*

$$P_{\mathrm{r}} = \frac{2^{(4-n_e)\cdot n}}{2^{2n}(2^{2n}-1)}.$$

Remarque : Le nombre *exact* de paires de messages de sortie admissibles est difficile à exprimer. Nous en donnons donc une approximation, très proche de la vraie valeur et surtout largement assez bonne pour le besoin.

Démonstration : La probabilité pour qu'un couple donné de messages d'entrée vérifie les relations voulues sur les blocs d'entrée, multipliée par le nombre total de couples de sortie admissibles peut être approximé par $\frac{1}{2^{n_e \cdot n}} \cdot 2^{4n}$. La probabilité qu'une permutation aléatoire fournisse un couple fixé de messages de sortie est $\frac{1}{2^{2n}(2^{2n}-1)}$. D'après ce qui a été énoncé avant l'énoncé de la proposition 3, le résultat est obtenu en multipliant ces deux valeurs. □

Afin de pouvoir énoncer la probabilité équivalente pour les permutations auxquelles on s'intéresse, à savoir k tours de schémas de Feistel avec permutations internes ou k tours d'un schéma du type Misty, introduisons la notion de coefficient H.

Cette notion de coefficient H a été initialement introduite par Jacques Patarin dans son étude sur les schémas de Feistel classiques, *i.e.* balancés [Pat91]. Ces coefficients H ont ensuite été la clef de voûte de beaucoup d'études sur des variantes de schémas de Feistel : les schémas de Feistel dissymétriques avec fonctions internes expansives, ou fonctions internes compressives. Cette notion a ensuite été reprise notamment par Gilles Piret, cette fois pour réaliser des preuves de sécurité de schémas de Feistel avec permutations internes. Dans le cas présent, nous nous intéressons encore aux attaques génériques, sur les schémas mentionnés. Ces attaques, tout comme celles de Patarin, sont basées sur le calcul des coefficients H.

La définition suivante de coefficient H reste valable pour les deux schémas, comme tous deux utilisent des permutations sur n bits comme fonctions internes :

Définition 8 (coefficient H) *Considérons la permutation S^k (k tours de l'un ou l'autre des deux schémas considérés : $S^k = \psi^k$ ou M_L^k). Soient $[L_1, R_1] \neq [L_2, R_2]$ et $[S_1, T_1] \neq [S_2, T_2]$ quatre éléments de I_{2n}.*

Le coefficient H pour S^k (noté $H([L_1, R_1], [L_2, R_2], [S_1, T_1], [S_2, T_2])$ ou plus simplement H) est le nombre de k-uplets de permutations $(f_1, \ldots, f_k) \in B_n^k$, tels que $\begin{cases} S^k(f_1, \ldots, f_k)([L_1, R_1]) = [S_1, T_1], \text{ et} \\ S^k(f_1, \ldots, f_k)([L_2, R_2]) = [S_2, T_2]. \end{cases}$

En d'autre mots, le coefficient H compte le nombre de k-uplets de permutations, permettant de faire correspondre (lorsqu'utilisées comme fonctions internes du schéma considéré) les deux entrées sur les deux sorties données. La valeur du coefficient H, pour k fixé, dépend évidemment du schéma considéré. La définition 8 s'écrit en fait, pour chacun de ces deux schémas :

1. Dans le cas de k tours de schémas de Feistel avec permutations internes, H est le nombre de k-uplets de permutations $(f_1, \ldots, f_k) \in B_n^k$ telles que :
   $\begin{cases} \psi^k(f_1, \ldots, f_k)([L_1, R_1]) = [S_1, T_1] \\ \psi^k(f_1, \ldots, f_k)([L_2, R_2]) = [S_2, T_2]. \end{cases}$
   Ceci peut être représenté par le schéma 3.3 ci-dessous.

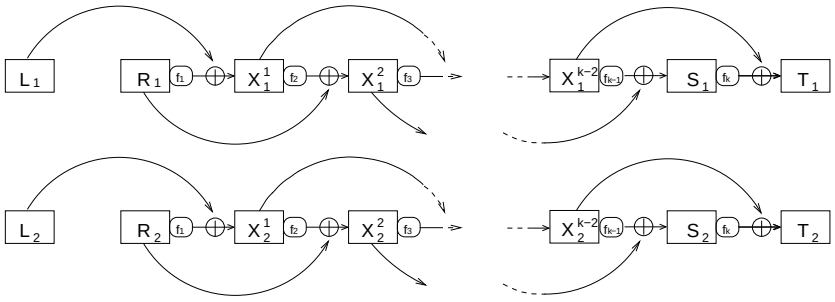

FIGURE 3.3: $\psi^k(f_1, \ldots, f_k)([L_1, R_1]) = [S_1, T_1]$, $\psi^k(f_1, \ldots, f_k)([L_2, R_2]) = [S_2, T_2]$

2. Dans le cas de k tours de schémas Misty L, H est le nombre de k-uplets de permutations $(f_1, \ldots, f_k) \in B_n^k$ telles que :

$$\begin{cases} M_L^k(f_1,\ldots,f_k)([L_1,R_1]) = [S_1,T_1] \\ M_L^k(f_1,\ldots,f_k)([L_2,R_2]) = [S_2,T_2]. \end{cases}$$

Ceci peut être représenté par le schéma 3.4 ci-dessous.

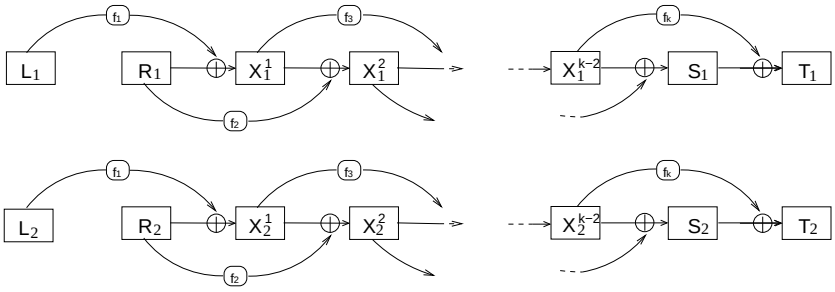

FIGURE 3.4: $M_L^k(f_1,\ldots,f_k)([L_1,R_1]) = [S_1,T_1]$,$M_L^k(f_1,\ldots,f_k)([L_2,R_2]) = [S_2,T_2]$

Remarque : Nous verrons que H, pour un schéma donné et un nombre de tours considéré, ne dépend que des relations entre les blocs d'entrée et de sorties. Ceci apparaît lors du calcul des coefficients H (voir par exemple l'annexe A). Les différente relations que nous sommes amenés à considérer pour les schémas Misty L sont également rapelées au début de la section 4.1, et au début de la section 4.2 pour les schémas de Feistel avec permutations internes.

Proposition 4 *Pour k tours de schémas de Feistel avec permutations internes aléatoires (ψ^k), ou pour k tours de schémas Misty L, la probabilité pour un attaquant d'avoir deux couples d'entrée/sortie $[L_1,R_1]/[S_1,T_1] \neq [L_2,R_2]/[S_2,T_2]$ vérifiant les relations sur leur blocs correspondant à un certain ensemble de contraintes peut être approximée par :*

$$\frac{2^{(4-n_e)\cdot n}\cdot H}{|B_n|^k},$$

où n_e a été défini à la définition 7 et H à la définition 8.

Remarque : Même remarque qu'à la proposition 3.

Démonstration : Comme tout à l'heure, la probabilité pour un couple donné de messages d'entrée vérifie les bonnes relations sur ses blocs, multipliée par le nombre de messages de sortie admissibles peut être approximé par $2^{(4-n_e)\cdot n}$. La probabilité que la permutation particulière S^k ($S^k = \psi^k$ ou $S^k = M_L^k$ selon le cas étudié) fournisse en sortie un couple spécifique de messages de sortie s'exprime en fonction du coefficient H (définition 8) : $\frac{H}{|B_n|^k}$. D'après ce qui a été dit au début de cette sous-section 3.3, le résultat se déduit en multipliant ces deux valeurs. □

3.4 Implication des probabilités P_{r} et P_{ψ^k} ou $P_{M_L^k}$ dans les attaques deux points

Considérons m entrées/sorties distinctes aléatoires $[L_i, R_i]/[S_i, T_i]$. Considérons également certaines relations (que l'attaquant attend de voir réalisées, ou non) entre les blocs d'entrée et de sortie de deux messages $[L_i, R_i]/[S_i, T_i]$, $[L_j, R_j]/[S_j, T_j]$. Tout comme dans les exemple sur six tours (section 3.2), l'attaquant compte le nombre de paires de messages vérifiant ces relations. Comme d'habitude, si les relations observées sont bien choisies, il attend d'avoir une différence dans le nombre de paires vérifiant ces relations, selon que la permutation ayant fourni ces entrées/sorties soit aléatoire ou soit la permutation S^k (selon le cas, $S^k = \psi^k$ ou $S^k = M_L^k$).

Définissons X_{S^k} comme étant le nombre de paires de messages vérifiant les relations considérées par l'attaquant, dans le cas où la permutation en jeu correspond à S^k. Définissons encore X_{r} comme étant le nombre de paires de messages vérifiant les relations considérées par l'attaquant, dans le cas où la permutation en jeu correspond à une permutation aléatoire.

Rappelons la formule de Chebyshev :

Proposition 5 (Formule de Chebyshev) *Soit X une variable aléatoire.*

$$P\{|X - E(X)| \geq \alpha \cdot \sigma(X)\} \leq \frac{1}{\alpha^2},\ \alpha \in \mathbb{R}_+^*,$$

où P est la fonction de probabilité, E l'espérance et σ l'écart type.

La formule de la proposition 5 signifie que la probabilité d'avoir des réalisations d'une variable aléatoire qui soient à une distance de l'espérance plus grande que de l'ordre de l'écart type, est faible. Par conséquent, revenant à nos variables aléatoires X_{S^k} et X_{r}, lorsque les espérances de ces deux variables aléatoires sont éloignées de plus que de l'ordre de $\sigma(X_{S^k}) + \sigma(X_{\mathrm{r}})$, les nuages de points correspondant aux deux variables sont différentiables. Autrement dit, lorsque l'on a assez de paires de messages pour que l'inégalité suivante soit réalisée :

$$|E(X_{S^k}) - E(X_{\mathrm{r}})| \quad \geq \quad \mathcal{O}\left(\sigma(X_{S^k}) + \sigma(X_{\mathrm{r}})\right), \tag{3.1}$$

alors l'attaquant sait distinguer la permutation S^k d'une permutation aléatoire.

On voit maintenant l'intérêt des propositions 3 et 4 : les formules donnant les probabilités d'avoir certaines relations entre des blocs d'entrée et de sortie de deux messages permettent de calculer les espérances et écarts types précédents en fonction de m (le nombre de messages générés). Ainsi, pour savoir la complexité d'une attaque basée sur un certain ensemble de relations, il suffit de résoudre en m l'inégalité (3.1) précédente.

Les sous-sections suivantes rentrent dans les détails de ces constatations. La partie 3.4.2 traite du cas où le nombre de messages nécessaires à la réalisation de l'attaque dépasse le nombre maximal de messages possibles d'évaluer (2^{2n}).

3.4.1 Attaque d'une permutation

Les notations suivantes sont celles utilisées précédemment (H et n_e sont définis à la section 3.3). Les résultats des propositions 3 et 4 de cette même section donnent pour l'espérance :

$$\begin{aligned} E(X_{\mathrm{r}}) &= \frac{m(m-1)}{2} \cdot P_{\mathrm{r}} \\ &\simeq \frac{m(m-1)}{2} \cdot \frac{2^{(4-n_e)\cdot n}}{2^{2n}(2^{2n}-1)} \\ E(X_{S^k}) &= \frac{m(m-1)}{2} \cdot P_{S^k} \\ &\simeq \frac{m(m-1)}{2} \cdot \frac{2^{(4-n_e)\cdot n} \cdot H}{\mid B_n^k \mid}. \end{aligned}$$

Passons aux expressions des écarts type. Pour cela, voyons que X_{r} (respectivement X_{S^k}) peut s'écrire comme la somme de $\frac{m(m-1)}{2}$ variables aléatoires suivant une loi de Bernoulli $\mathcal{B}(1, P_{\mathrm{r}})$ (respectivement $\mathcal{B}(1, P_{S^k})$). Par exemple :

$$X_{\mathrm{r}} = \sum_{1 \leq i < j \leq m} X_{\mathrm{r}}^{(i,j)},$$

où $X_{\mathrm{r}}^{(i,j)}$ vaut 1 si les relations attendues par l'attaquant sont vérifiées entre $[L_i, R_i]/[S_i, T_i]$ et $[L_j, R_j]/[S_j, T_j]$, dans le cas d'une permutation aléatoire, et 0 sinon. De même :

$$X_{S^k} = \sum_{1 \leq i < j \leq m} X_{S^k}^{(i,j)},$$

où $X_{S^k}^{(i,j)}$ vaut 1 si les relations attendues sont vérifiées entre $[L_i, R_i]/[S_i, T_i]$ et $[L_j, R_j]/[S_j, T_j]$, dans le cas de S^k, et 0 sinon.

Or, pour n variables aléatoires Y_i telles que $E(Y_i^2)$ existe, nous avons la formule suivante, appelée parfois ([PNB06b, PNB06a, TP09, NPT10]) formule "de covariance" (Var désigne la variance et Cov la covariance) :

$$\begin{aligned} \mathrm{Var}(\sum_{i=1}^{n} Y_i) &= E((\sum_{i=1}^{n} Y_i)^2) - E(\sum_{i=1}^{n} Y_i)^2 \\ &= \sum_{i=1}^{n} E(Y_i^2) + 2 \sum_{1 \leq i < j \leq n} E(Y_i \cdot X_j) - \sum_{i=1}^{n} E(Y_i)^2 - 2 \sum_{1 \leq i < j \leq n} E(Y_i) \cdot E(Y_j) \\ &= \sum_{i=1}^{n} E(Y_i^2) - E(Y_i)^2 + 2 \sum_{1 \leq i < j \leq n} E(Y_i \cdot Y_j) - E(Y_i) \cdot E(Y_j) \\ &= \sum_{i=1}^{n} \mathrm{Var}(Y_i) + 2 \sum_{1 \leq i < j \leq n} \mathrm{Cov}(Y_i, Y_j). \end{aligned}$$

Dans notre cas ($\sum_{1\leq i<j\leq m} X_{\mathrm{r}}^{(i,j)}$ ou $\sum_{1\leq i<j\leq m} X_{S^k}^{(i,j)}$) les termes issus de la covariance sont négligeables. On a :

$$\begin{aligned}
\mathrm{Var}(\sum_{1\leq i<j\leq m} X_{\mathrm{r}}^{(i,j)}) &\simeq \sum_{1\leq i<j\leq m} \mathrm{Var}(X_{\mathrm{r}}^{(i,j)}) \\
&= \sum_{1\leq i<j\leq m} P_{\mathrm{r}}(1-P_{\mathrm{r}}) \\
&\simeq \frac{m(m-1)}{2} P_{\mathrm{r}}, \\
\mathrm{Var}(\sum_{1\leq i<j\leq m} X_{S^k}^{(i,j)}) &\simeq \sum_{1\leq i<j\leq m} \mathrm{Var}(X_{S^k}^{(i,j)}) \\
&= \sum_{1\leq i<j\leq m} P_{S^k}(1-P_{S^k}) \\
&\simeq \frac{m(m-1)}{2} P_{S^k}.
\end{aligned}$$

Finalement, l'inégalité (3.1) se réécrit :

$$\begin{aligned}
&\frac{m(m-1)}{2} \cdot \left| \frac{H \cdot 2^{(4-n_e)\cdot n}}{|B_n|^k} - \frac{2^{(4-n_e)\cdot n}}{2^{2n}(2^{2n}-1)} \right| \geq \sqrt{\frac{m(m-1)}{2 \cdot 2^{n_e \cdot n}}} \\
\Leftrightarrow \quad &\frac{m(m-1)}{2} \geq 2^{n_e \cdot n} \cdot \left(\frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{2^{2n}}{2^{2n}-1} \right)^{-2}, \qquad (3.2)
\end{aligned}$$

et la complexité de l'attaque considérée est $\mathcal{O}(m)$, où m est tel que cette inégalité puisse être vérifiée.

Remarque : Nous introduisons la valeur ε, définie par :

$$\varepsilon = \left(\frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{2^{2n}}{2^{2n}-1} \right)^{-2}.$$

En fait, la probabilité d'avoir une paire de messages de sortie donnée est $\frac{1}{2^{2n}(2^{2n}-1)}$ dans le cas d'une permutation aléatoire. La valeur $\frac{H}{|B_n|^k}$ est cette probabilité dans le cas de S^k ($S^k = \psi^k$ ou $S^k = M_L^k$). Cette variable ε est importante lors de l'estimation de la meilleure des attaques parmi toutes les attaques deux points. En effet, par l'inégalité précédente, on voit que les attaques ayant une meilleure complexité sont celles pour lesquelles ε est maximal, pour un nombre d'égalités sur les blocs d'entrées et de sorties demandées par l'attaque (n_e, cf. définition 7) minimal. En fait, lorsque ε est grand, cela signifie que la probabilité d'obtenir toutes les équations entre les blocs d'entrée et de sortie varie beaucoup selon que la permutation est aléatoire ou M_L^k. Cependant, l'attaquant doit obtenir des paires vérifiant ces relations. Par conséquent, plus il y a d'égalités demandées entre les blocs d'entrée et de sortie, moins il obtient de paires de messages vérifiant ces relations.

Différentes valeurs exactes pour ε sont données en annexe A. Une table avec de plus nombreuses valeurs donnée à la section 4.1 pour les schémas Misty L, et à la section 4.2 pour les schémas de Feistel avec permutations internes (sous-sections 4.1.2.1

et 4.2.2.1). Ces tables donnent uniquement l'ordre de grandeur de ε, qui suffit à déduire la complexité des attaques. Dans ce chapitre 4 sont également donnés des exemples d'application aux attaques (sous-sections 4.1.2.2 et 4.2.2.2).

3.4.2 Attaque d'un générateur de permutations

Lorsque le nombre de messages m nécessaires pour que l'inégalité (3.1) soit vérifiée est supérieur à 2^{2n}, l'attaque ne peut être réalisée, car la permutation prend en entrée des messages de taille $2n$ bits. Lorsque c'est le cas, nous supposons alors attaquer un générateur de permutations, *i.e.* nous supposons avoir accès $\lambda > 1$ permutations.

Nous avons alors :

$$\begin{aligned} E(X_{\mathrm{r}}) &= \frac{\lambda \cdot m(m-1)}{2} \cdot P_{\mathrm{r}} \\ &\simeq \frac{\lambda \cdot m(m-1)}{2} \cdot \frac{2^{(4-n_e)\cdot n}}{2^{2n}(2^{2n}-1)}, \\ E(X_{S^k}) &= \frac{\lambda \cdot m(m-1)}{2} \cdot P_{S^k} \\ &\simeq \frac{\lambda \cdot m(m-1)}{2} \cdot \frac{2^{(4-n_e)\cdot n} \cdot H}{\mid B_n^k \mid}. \end{aligned}$$

Notons que le nombre maximal de paires de messages est toujours utilisé par permutation (soit $m(m-1)/2 \simeq 2^{4n}$ dans le cas d'une attaque à clair connu). L'inégalité 3.1 est à résoudre alors en λ et s'écrit :

$$\begin{aligned} & \frac{\lambda \cdot m(m-1)}{2} \cdot \left| \frac{H \cdot 2^{(4-n_e)\cdot n}}{|B_n|^k} - \frac{2^{(4-n_e)\cdot n}}{2^{2n}(2^{2n}-1)} \right| \geq \sqrt{\frac{\lambda \cdot m(m-1)}{2 \cdot 2^{n_e \cdot n}}} \\ \Leftrightarrow \quad & \frac{\lambda \cdot m(m-1)}{2} \geq 2^{n_e \cdot n} \cdot \left(\frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{2^{2n}}{2^{2n}-1} \right)^{-2}. \end{aligned} \tag{3.3}$$

La complexité finale de l'attaque est λ multiplié par le nombre de messages évalués par permutation. Cependant, comme le nombre maximal de paires de messages est utilisé par permutation, on a aussi $m = 2^{2n}$. La complexité de l'attaque est alors $\mathcal{O}\left(\lambda \cdot 2^{2n}\right)$.

Remarque :

- Ici encore, les meilleures attaques sont celles pour lesquelles ε (voir la remarque de la sous-section 3.4.1) est maximal, pour n_e minimal. Quelques valeurs pour ε sont données en annexe A. Une table de valeurs peut être retrouvée à la section 4.1 pour les schémas Misty L, et 4.2 pour les schémas de Feistel avec permutations internes (sous-sections 4.1.2.1 et 4.2.2.1). On pourra aussi y trouver des exemples d'application aux attaques.
- Dans le cas d'une attaque d'un générateur de permutations, la complexité des attaques deux points KPA ou CPA est la même. En effet, lorsque l'on considère

un générateur de permutations, on évalue tous les messages possibles par permutation. Plus rigoureusement, ceci est dû au fait que passer d'une KPA à une CPA fait éventuellement augmenter le nombre d'égalités imposables (n_e diminue). Mais alors, le nombre de paires de messages à considérer par permutation diminue. On peut voir que ces deux variations se compensent dans l'inégalité (3.3). On en déduit qu'une attaque mène à une même complexité en KPA ou CPA. Ceci peut se vérifier dans les tableaux finaux du chapitre 4 : dès que la complexité des attaques est supérieure à 2^{2n}, les attaques deux points ont la même complexité quel que soit le type d'attaque.

3.4.3 Choix de l'ensemble de relations menant à la meilleure attaque

Notons simplement que les formules (3.2) et (3.3) permettent directement de déduire quels cas mènent aux meilleures attaques.

Proposition 6 (Attaque d'une permutation) *Soient c_1 et c_2 deux ensembles de relations sur les blocs d'entrée et sortie de deux messages distincts. L'ensemble c_1 mène à une attaque meilleure ou une attaque équivalente que l'ensemble c_2 si :*

$$\varepsilon_{\mathrm{c_1}}^2 \geq \varepsilon_{\mathrm{c_2}}^2 \cdot 2^{n_e(\mathrm{c_1})-n_e(\mathrm{c_2})}.$$

Par conséquent, pour décider quel ensemble de relations mène à la meilleure attaque, on peut commencer par repérer les cas où pour un nombre de relations n_e donné, les valeurs de ε sont les plus grandes. Ensuite, on peut se servir de cette proposition pour conclure quel(s) cas mènent à la meilleure complexité. Des exemples sont donnés à la sous-section 4.1.2.2 du chapitre 4 pour les schémas Misty L, et à la section 4.2.2.2 pour les schémas de Feistel avec permutations internes.

Proposition 7 (Attaque d'un générateur de permutations) *Soient c_1 et c_2 deux ensembles de relations sur les blocs d'entrée et sortie de deux messages distincts. Notons $M_{\mathrm{c_1}}$ et $M_{\mathrm{c_2}}$ le nombre de paires de messages évaluées par permutation dans chacun des cas. Alors, l'ensemble c_1 mène à une attaque meilleure ou une attaque équivalente si :*

$$\varepsilon_{\mathrm{c_1}}^2 \geq \varepsilon_{\mathrm{c_2}}^2 \cdot 2^{n_e(\mathrm{c_1})-n_e(\mathrm{c_2})} \cdot \frac{M_{\mathrm{c_2}}}{M_{\mathrm{c_1}}}.$$

Remarque : Notons que pour les mêmes raisons qu'à la remarque de la sous-section 3.4.2, l'expression $2^{n_e(\mathrm{c_1})-n_e(\mathrm{c_2})} \cdot \frac{M_{\mathrm{c_2}}}{M_{\mathrm{c_1}}}$ garde la même valeur quelle que soit le type d'attaque considéré.

3.5 Résultats généraux pour le calcul direct des coefficients H

Soient $[L_1, R_1] \neq [L_2, R_2]$ et $[S_1, T_1] \neq [S_2, T_2]$ quatre éléments de I_{2n}. Rappelons que la définition des coefficients est donné à la définition 8 de ce chapitre. Dans cette

section, nous donnons la ligne directrice pour le calcul direct des coefficients H, dans le cas des schémas de Feistel avec permutations internes et Misty L. Le détail du calcul effectif des coefficients H pour ces deux schémas est donné en annexe A.

La méthode présentée ici est appelée "directe", car elle permet de déterminer la valeur d'un coefficient H, directement à partir du nombre de tours d'un schéma[3] et des relations initiales entre les blocs de deux entrées/sorties. Pour comprendre comment l'on peut obtenir une formule directe pour H, dans chacun de ces deux cas, nous allons "décortiquer" ces schémas. La sous-section 3.5.1 introduit certains objets reliés aux schémas. La sous-section 3.5.2 donne un théorème général pour le calcul des coefficients H, sur lequel nous nous basons pour le calcul effectif présenté en annexe A.

Remarque : Notons que les coefficients H peuvent aussi être obtenus par récurrence. Le principe est de décomposer $k+1$ tours de schémas (de Feistel avec permutations internes ou misty L) en 1 tour et k tours, et ainsi obtenir les expressions des coefficients H pour $k+1$ tours en fonctions des expressions pour un nombre de tours inférieur. Nous donnons en annexe A, sections A.3 et A.4, les formules de récurrence obtenues pour les deux schémas.

3.5.1 Familiarisation avec des objets en relation avec les schémas considérés, blocs internes et séquences $\mathcal{R}$

3.5.1.1 Les blocs internes

La donnée d'un message d'entrée (ou de sortie) ainsi que d'un k-uplet de permutations internes, détermine uniquement les blocs internes du schéma correspondant jusqu'aux blocs de sortie (ou d'entrée). Ces blocs internes sont les blocs indexés par X_1^i, $i = 1, \ldots, k-2$ pour les messages d'entrée/sortie $[L_1, R_1]/[S_1, T_1]$, et par X_2^i, $i = 1, \ldots, k-2$ pour les messages d'entrée/sortie $[L_2, R_2]/[S_2, T_2]$ dans les figures 3.3 et 3.4 que l'on peut trouver au début de ce chapitre. À l'inverse, lorsque les blocs d'entrée et de sortie sont connus et que l'on cherche à déterminer les permutations internes pouvant correspondre à ces deux couples d'entrée/sortie (ce qui correspond à notre situation, lorsque l'on cherche à déterminer le coefficient H), on peut s'intéresser aux blocs internes.

Dans le cas des deux schémas considérés et étant fixées deux entrées et sorties, chaque possibilité de blocs internes détermine plusieurs k-uplets de permutations internes possibles. Dans le cadre d'une attaque deux points, le coefficient H est le nombre total de permutations internes. Une manière de déterminer le coefficient H correspondant à un couple d'entrée/sorties est de considérer toutes les possibilités de blocs internes. H est alors obtenu en sommant le nombre de k-uplets de permutations que la donnée de chacune de ces possibilités de blocs internes détermine.

De manière sommaire, on peut écrire l'égalité suivante (nous utilisons à nouveau la notation S^k désignant soit k tours de schémas de Feistel avec permutations internes soit k tours de schémas de Misty) :

3. Nous focalisons sur les schémas de Feistel avec permutations internes ou Misty L.

$$H\left([L_1,R_1],[L_2,R_2],[S_1,T_1],[S_2,T_2]\right) = \sum_{\substack{(X_1^1,\dots X_1^{k-2});\\(X_2^1,\dots X_2^{k-2})\\ \text{possibles}}} \#\left\{(f_1,\dots,f_k) \text{ déterminés par } (X_1^1,\dots X_1^{k-2}) \text{ et } (X_2^1,\dots X_2^{k-2})\right\}. \tag{3.4}$$

3.5.1.2 Suite de relations $\mathcal{R}$

Plaçons-nous toujours dans le cadre d'une attaque deux points. Nous avons la proposition suivante :

Proposition 8 *Soient deux entrées/sorties* $[L_1,R_1]/[S_1,T_1]$ *et* $[L_2,R_2]/[S_2,T_2]$ *du schéma* S^k, $S^k = \psi^k$ *ou* $S^k = M_L^k$. *On s'intéresse au nombre de permutations internes* $(f_1,\dots,f_k)$ *déterminées par ces entrées/sorties ainsi que par des blocs internes* compatibles *donnés :* $(X_1^1,\dots X_1^{k-2})$ *et* $(X_2^1,\dots X_2^{k-2})$. *Ce nombre ne dépend que de la relation entre les deux blocs que chacune des permutations prend en entrée.*

Remarque :

1. On mentionne dans la proposition des "blocs internes compatibles". Ceci signifie simplement que cette suite de blocs internes est possible, prenant en considération le type de schéma, les deux entrées et sorties de la proposition et sachant que les fonctions utilisées dans les schémas sont des permutations. Par exemple, si $L_1 = L_2$ et $R_1 \neq R_2$, on ne pourra jamais avoir de blocs internes X_1^1 et X_2^1 égaux, tant pour un schéma de Feistel avec permutations internes que pour un schéma du type Misty. Ceci est dû à la manière dont se définit X^1 et au fait que f_1 est une permutation.
2. Les blocs d'entrée L, R et de sortie S, T vont jouer dans la suite de l'analyse un rôle similaire aux blocs internes X^i. Ainsi, pour unifier les notation et conserver l'ordre des indices des blocs, les blocs L et R seront aussi respectivement désignés par X^{-1} et X^0. Similairement, les blocs S et T pourront aussi être désignés par X^{k-1} et X^k. En clair, on pose :

$$\begin{cases} L_1 = X_1^{-1} & L_2 = X_2^{-1}, \\ R_1 = X_1^0 & R_2 = X_2^0, \\ S_1 = X_1^{k-1} & S_2 = X_2^{k-1}, \\ T_1 = X_1^k & T_2 = X_2^k. \end{cases}$$

Démonstration : Commençons par remarquer que le nombre total de permutations sur n bits est $\#B_n = 2^n!$. Si l'on s'intéresse au nombre de permutations qui associent une sortie donnée parmi les 2^n possibles à une entrée donnée, on obtient $(2^n-1)!$. Si l'on demande deux contraintes d'entrée/sortie, le nombre de permutations vérifiant

les deux contraintes est $(2^n-2)!$. On pourrait continuer ainsi pour un plus grand nombre d'entrées/sorties fixées, mais dans le cadre des attaques deux points, le cas de deux contraintes suffit.
Intéressons-nous à la permutation f_i, $i \in \{1 \dots k\}$. Nous avons, dans le cas d'un schéma de Feistel avec permutations internes :

$$f_i\left(X^{i-1}\right) = X^{i-2} \oplus X^i,$$

et dans le cas d'un schéma du type Misty :

$$f_i\left(X^{i-2}\right) = X^{i-1} \oplus X^i.$$

Pour les deux schémas, dans le cadre d'une attaque deux points, f_i doit vérifier deux telles égalités, correspondant aux deux entrées/sorties et blocs internes associés. Dans le cas d'un schéma de Feistel avec permutations internes :

$$\begin{cases} f_i\left(X_1^{i-2}\right) = X_1^{i-1} \oplus X_1^i \text{ et} \\ f_i\left(X_2^{i-2}\right) = X_2^{i-1} \oplus X_2^i, \end{cases}$$

et dans le cas d'un schéma du type Misty :

$$\begin{cases} f_i\left(X_1^{i-2}\right) = X_1^{i-1} \oplus X_1^i \text{ et} \\ f_i\left(X_2^{i-2}\right) = X_2^{i-1} \oplus X_1^i. \end{cases}$$

Notons que tous les blocs sont fixés, ainsi, les variables intervenant dans ces équations sont toutes déterminées. Alors, le nombre de possibilités pour f_i, dans le cas d'un schéma de Feistel avec permutations internes est : $(2^n-1)!$ si $X_1^{i-1} = X_2^{i-1}$ et $(2^n-2)!$ si $X_1^{i-1} \neq X_2^{i-1}$. Dans le cas d'un schéma du type Misty, ce nombre est $(2^n-1)!$ si $X_1^{i-2} = X_2^{i-2}$ et $(2^n-2)!$ si $X_1^{i-2} \neq X_2^{i-2}$. □

Pour obtenir la valeur du coefficient H selon (3.5), il convient alors de s'intéresser uniquement aux différentes configurations possibles d'égalité ou d'inégalité entre les blocs internes, et de calculer le nombre de k-uplets de fonctions internes possibles dans chacune de ces configurations :

$$\begin{aligned} & H\left(L_1, R_1, S_1, T_1, L_2, R_2, S_2, T_2\right) \\ = & \sum_{\mathcal{R} \in \{=,\neq\}^{k+2}} \#\left\{(f_1, \dots, f_k) \text{ correspondant à la suite } \mathcal{R}\right\} \times \\ & \qquad \#\left\{(X_1^1, \dots, X_1^{k-2}); (X_2^1, \dots, X_2^{k-2}) \text{ pouvant vérifier } \mathcal{R}\right\}. \end{aligned}$$

Le nombre de $(X_1^1, \dots, X_1^{k-2})$; $(X_2^1, \dots, X_2^{k-2})$ pouvant vérifier $\mathcal{R}$ correspond au nombre de telles deux suite de blocs internes compatibles avec les entrées $[L_1, R_1]/[S_1, T_1]$ et $[L_2, R_2]/[S_2, T_2]$ et le schéma considéré, et telles que, pour tout $i \in \{1, \dots, k-2\}$:

$$\begin{cases} X_1^i = X_2^i, \text{ si } \mathcal{R}_i \text{ est le symbole } = \\ X_1^i \neq X_2^i, \text{ si } \mathcal{R}_i \text{ est le symbole } \neq \end{cases}$$

Notons que les deux premières valeurs de la séquence $\mathcal{R}$, ainsi que les deux dernières, sont imposées par les messages d'entrée/sortie.

Selon que $S^k = \psi^k$ ou $S^k = M_L^k$, les possibilités de telles suites sont différentes. Elles dépendent également des blocs $L_1, R_1, S_1, T_1, L_2, R_2, S_2$ et T_2. Ces points plus techniques sont analysés à l'annexe A. Pour le moment, énonçons une formule générale pour H, à partir des éléments déjà donnés.

3.5.2 Théorème général sur l'expression du coefficient H

Le calcul d'une formule pour les coefficients H est fait rigoureusement dans la section A.1 de l'annexe A pour les schémas Misty L, et dans la section A.2 pour les schémas de Feistel avec permutations internes. Le théorème 1 suivant permet d'avoir une vue d'ensemble des idées mises en jeu pour calculer ces coefficients H.

Soient $[L_1, R_1]$, $[L_2, R_2]$ and $[S_1, T_1]$ et $[S_2, T_2]$, quatre éléments de I_{2n}. On considère les représentations suivantes des deux schémas (figure 3.5 pour les schémas de Feistel et 3.6 pour les Misty L), déjà données à la section 3.3. Nous énonçons dans cette partie une formule pour déterminer le nombre H de permutations $(f_1, \ldots, f_k) \in B_n^k$, telles que :

$$\begin{cases} \psi^k(f_1, \ldots, f_k)([L_1, R_1]) = [S_1, T_1] \\ \psi^k(f_1, \ldots, f_k)([L_2, R_2]) = [S_2, T_2], \end{cases}$$

dans le cas des schémas de Feistel avec permutations internes, ou

$$\begin{cases} M_L^k(f_1, \ldots, f_k)([L_1, R_1]) = [S_1, T_1] \\ M_L^k(f_1, \ldots, f_k)([L_2, R_2]) = [S_2, T_2], \end{cases}$$

dans le cadre des schémas Misty L.

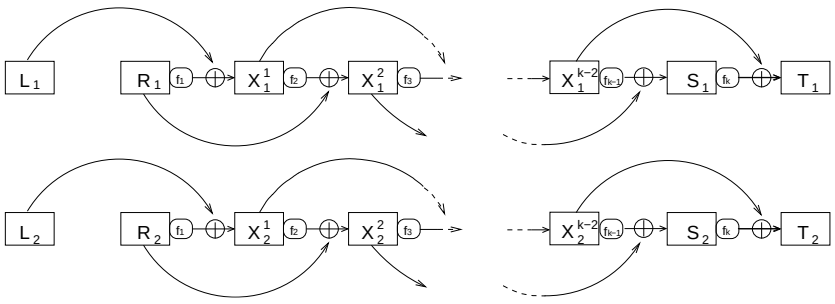

FIGURE 3.5: $\psi^k(f_1, \ldots, f_k)([L_1, R_1]) = [S_1, T_1]$, $\psi^k(f_1, \ldots, f_k)([L_2, R_2]) = [S_2, T_2]$

Le théorème suivant est assez général pour permettre de donner une formule valable à la fois dans le cas des schémas de Feistel avec permutations internes et dans le cas des schémas Misty L. Dans le théorème, k tour de l'un ou l'autre de ces deux schémas est dénoté par S^k ($S^k = \psi^k$ ou M_L^k).

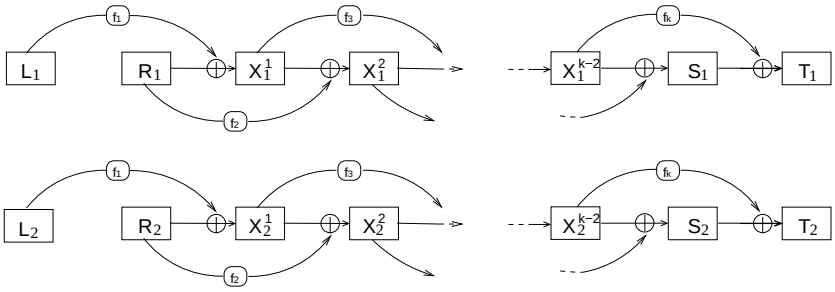

FIGURE 3.6: $M_L^k(f_1,\ldots,f_k)([L_1,R_1]) = [S_1,T_1]$, $M_L^k(f_1,\ldots,f_k)([L_2,R_2]) = [S_2,T_2]$

Théorème 1 *Une formule directe pour H est donnée par*

$$H = \sum_{\substack{\text{suites } \mathcal{R} \text{ possibles} \\ \mathcal{R}\in\{=,\neq\}^{k+2}}} (2^n-1)!^{e(s)}(2^n-2)!^{d(s)} \cdot (2^n)^{k-2} \cdot N(d_1)\cdots N(d_{k-2}),$$

où :

- *$\mathcal{R}$ dénote une suite de relations vérifiées par les blocs, à savoir $X_1^i = X_2^i$ or $X_1^i \neq X_2^i$, pour $i = -1,\ldots,k$,*
- *$e(s)$ est le nombre d'égalités de la suite $\mathcal{R}$,*
- *$d(s)$ est le nombre d'inégalités de la suite $\mathcal{R}$,*
- *$N(d_i)$, pour $i = 1,\ldots,k-2$, est le nombre de valeurs possibles pour la différence $X_1^i \oplus X_2^i$, pour une suite $\mathcal{R}$ fixée.*

Démonstration : Dans une première étape, fixons une séquence $\mathcal{R}$, comme dans le théorème 1. Évaluons, pour $\mathcal{R}$ fixée, le nombre de possibilités pour $(f_1,\ldots,f_k)$, noté $H(\mathcal{R})$. La deuxième étape consistera ensuite à sommer sur toutes les séquences $\mathcal{R}$ possibles.

Détaillons la première étape, tout d'abord dans le cas de schémas de Feistel avec permutations internes, $S^k = \psi^k$:

Dans la suite, $f_1,\ldots,f_k$ dénotera les permutations qui nous intéressent. Une séquence $\mathcal{R}$ est fixée.

- Pour $i = 1\ldots k-2$, d'après la définition de $N(d_i)$ donnée dans le théorème, $N(d_i)\cdot 2^n$ correspond au nombre de possibilités pour le couple (X_1^i, X_2^i).
- Dans le cas d'un schéma de Feistel, on a : $f_i(X^{i-1}) = X^{i-2} \oplus X^i$ pour $i = 1,\ldots,k$. Ainsi, $N(d_1)\cdot 2^n$ est le nombre de possibilités pour le couple $\big(f_1(X_1^0), f_1(X_2^0)\big)$. Par suite, pour $i = 2,\ldots,k-2$, $N(d_i)\cdot 2^n$, est le nombre de possibilités pour le couple $\big(f_i(X_1^{i-1}), f_i(X_2^{i-1})\big)$, lorsque $f_1,\ldots,f_{i-1}$ sont fixées (car alors X^{i-1} et X^{i-2} sont fixés et le nombre de possibilités pour $\big(f_i(X_1^{i-1}), f_i(X_2^{i-1})\big)$ est le nombre de possibilités pour (X_1^i, X_2^i)).
- Dénotons $F_1(\mathcal{R})$ le nombre de possibilités pour f_1, et pour $i = 2,\ldots,k$, $F_i(s)$ le nombre de possibilités pour f_i, lorsque $f_1,\ldots,f_{i-1}$ sont fixées. Alors dans le cas d'un schéma de Feistel :

$$\text{si } X_1^{i-1} \neq X_2^{i-1} \ : \ \begin{cases} F_i(s) := N(d_i)2^n(2^n-2)!, \text{for } i = 1, \dots k-2, \\ F_{k-1}(s) = F_k(s) = (2^n-2)! \end{cases}$$
$$\text{si } X_1^{i-1} = X_2^{i-1} \ : \ \begin{cases} F_i(s) := N(d_i)2^n(2^n-1)!, \text{for } i = 1, \dots k-2, \\ F_{k-1}(s) = F_k(s) = (2^n-1)! \end{cases}$$

Ce résultat provient du point précédent et de la remarque que $(2^n-2)!$ (respectivement $(2^n-1)!$) est le nombre de permutations, pour lesquelles on a déjà imposé l'image de deux éléments (respectivement un élément) (voir aussi la démonstration de la proposition 8 de la sous-section 3.5.1.2). Pour $i = k-1, k$, toutes les variables de l'équation $f_i(X^{i-1}) = X^{i-2} \oplus X^i$ (schémas de Feistel) sont fixées, le nombre de possibilités pour le couple $\left(f_i(X_1^{i-1}), f_i(X_2^{i-1})\right)$ est alors 1.

– Finalement, pour une séquence fixée $\mathcal{R}$, le nombre de possibilités pour $(f_1, \dots, f_k)$ est

$$H(s) = \prod_{i=1}^{k} F_i(s) = (2^n-1)!^{e(s)}(2^n-2)!^{d(s)} \cdot (2^n)^{k-2} \cdot N(d_1) \cdots N(d_{k-2}).$$

Revenons au cas des schémas Misty L, $S^k = M_L^k$:
Les étapes sont les mêmes que dans le cas des schémas de Feistel, mais certaines d'entre elles se montrent différemment :

– Pour $i = 1 \dots k-2$, $N(d_i) \cdot 2^n$ correspond toujours au nombre de possibilités pour le couple (X_1^i, X_2^i).
– Pour $i = 1 \dots k-2$, d'après la définition de $N(d_i)$ donnée dans le théorème, $N(d_i) \cdot 2^n$ correspond au nombre de possibilités pour le couple (X_1^i, X_2^i). Dans le cas d'un schéma du type Misty, nous avons $f_i(X^{i-2}) = X^{i-1} \oplus X^i$ pour $i = 1, \dots, k$. Ainsi, $N(d_1) \cdot 2^n$ est le nombre de possibilités pour le couple $\left(f_1(X_1^{-1}), f_1(X_2^{-1})\right)$. Par suite, pour $i = 2, \dots, k-2$, $N(d_i) \cdot 2^n$, est le nombre de possibilités pour le couple $\left(f_i(X_1^{i-2}), f_i(X_2^{i-2})\right)$, lorsque $f_1, \dots, f_{i-1}$ sont fixées (car alors X^{i-1} et X^{i-2} sont fixés et le nombre de possibilités pour $\left(f_i(X_1^{i-1}), f_i(X_2^{i-1})\right)$ est le nombre de possibilités pour (X_1^i, X_2^i)).
– Dénotons $F_1(\mathcal{R})$ le nombre de possibilités pour f_1, et pour $i = 2, \dots, k$, $F_i(s)$ le nombre de possibilités pour f_i, lorsque $f_1, \dots, f_{i-1}$ sont fixées. Alors, dans le cas d'un schéma du type Misty et avec une justification similaire que dans le cas des schémas de Feistel plus haut :

$$\text{si } X_1^{i-2} \neq X_2^{i-2} \ : \ \begin{cases} F_i(s) := N(d_i)2^n(2^n-2)!, \text{pour } i = 1, \dots k-2, \\ F_{k-1}(s) = F_k(s) = (2^n-2)! \end{cases}$$
$$\text{si } X_1^{i-1} = X_2^{i-1} \ : \ \begin{cases} F_i(s) := N(d_i)2^n(2^n-1)!, \text{pour } i = 1, \dots k-2, \\ F_{k-1}(s) = F_k(s) = (2^n-1)! \end{cases}$$

Pour $i = k-1, k$, toutes les variables de l'équation $f_i(X^{i-2}) = X^{i-1} \oplus X^i$ (schémas Misty L) sont fixées, le nombre de possibilités pour le couple $\left(f_i(X_1^{i-1}), f_i(X_2^{i-1})\right)$ est alors 1.

– On a donc également, pour une séquence fixée $\mathcal{R}$, que le nombre de possibilités pour $(f_1, \ldots, f_k)$ est

$$H(s) = \prod_{i=1}^{k} F_i(s) = (2^n - 1)!^{e(s)}(2^n - 2)!^{d(s)} \cdot (2^n)^{k-2} \cdot N(d_1) \cdots N(d_{k-2}).$$

La formule finale pour les coefficients H est donc, *dans les deux cas* $S^k = \psi^k$ et $S^k = M_L^k$:

$$H = \sum_{\substack{\text{suites } \mathcal{R} \text{ possibles} \\ \mathcal{R} \in \{=, \neq\}^{k+2}}} (2^n - 1)!^{e(s)}(2^n - 2)!^{d(s)} \cdot (2^n)^{k-2} \cdot N(d_1) \cdots N(d_{k-2}),$$

comme annoncé.

□

Comme déjà annoncé au paragraphe 3.5.1.2 précédent, les éléments intervenant dans cette formule, notamment, les relations possibles entre les blocs, $\mathcal{R}$, diffèrent selon que $S^k = \psi^k$ ou $S^k = M_L^k$. Ceci est détaillé dans les sections A.1 et A.2 de l'annexe A, correspondant à chacun des deux schémas.

Chapitre 4

Attaques Deux Points Systématiques sur les Schémas de Feistel avec Permutations Internes et Misty L. Résultats

Ce chapitre est l'application aux schémas de Feistel avec permutations internes ψ^k et schémas Misty L M_L^k, des résultats du chapitre 3. Il se concentre principalement sur les attaques génériques deux points, mais résume aussi les attaques génériques trois points et quatre points présentées au chapitre 2.

Pour chacun de ces deux schémas, nous commençons par rappeler les principaux résultats obtenus dans les chapitres précédents. Ensuite, nous donnons une table fournissant les valeurs de $\varepsilon = \frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1-1/2^{2n}}$ pour les 12 premiers tours, table de laquelle on peut déduire facilement les meilleures attaques deux points. Un exemple d'utilisation de cette table est donné pour chacun des deux schémas. Enfin, nous donnons un tableau résumant les complexités des meilleures attaques obtenues. Ce tableau peut être comparée au tableau 4.1 similaire, issu de [Pat01], présentant les meilleures attaques génériques sur les schémas de Feistel classiques.

Sommaire

nombre k de tours	KPA	CPA-1	CPA-2	CPCA-1	CPCA-2
1	1	1	1	1	1
2	$2^{n/2}$	2	2	2	2
3	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	3
4	2^{n}	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
5	$2^{3n/2}$	2^{n}	2^{n}	2^{n}	2^{n}
6	2^{2n}	2^{2n}	2^{2n}	2^{2n}	2^{2n}
7	2^{3n}	2^{3n}	2^{3n}	2^{3n}	2^{3n}
8	2^{4n}	2^{4n}	2^{4n}	2^{4n}	2^{4n}
9	2^{5n}	2^{5n}	2^{5n}	2^{5n}	2^{5n}
10	2^{6n}	2^{6n}	2^{6n}	2^{6n}	2^{6n}
11	2^{7n}	2^{7n}	2^{7n}	2^{7n}	2^{7n}
12	2^{8n}	2^{8n}	2^{8n}	2^{8n}	2^{8n}
$k \geq 6$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$

TABLE 4.1: Nombre maximum de calculs nécessaires pour distinguer k tours de schémas de Feistel avec fonctions internes, d'une permutation aléatoire avec signature paire.

4.1 Approche systématique et résultats pour les schémas Misty L

La figure 4.1 rappelle la structure générale d'un schéma du type Misty.

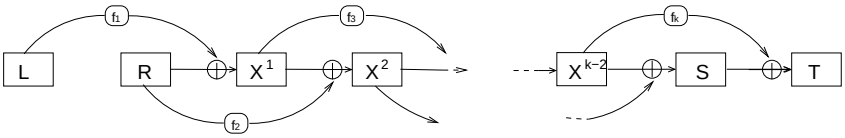

FIGURE 4.1: k tours de schémas Misty L

4.1.1 Résumé des résultats pour les schémas Misty L

Dans cette sous-section, nous rappelons rapidement les résultats déjà obtenus sur ces schémas Misty L, ou renvoyons vers les parties du manuscrit où se trouvent ces résultats. L'intérêt de faire ces rappels est que ces résultats servent de brique de base pour l'analyse systématique des attaque génériques exposée dans cette section 4.1.

4.1.1.1 Les différents cas à considérer pour H ou ε

Nous rappelons ci-dessous les treize cas à distinguer lors du calcul des coefficients H ou $\varepsilon = \frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{2^{2n}}{2^{2n}-1}$. La définition des coefficients H est donnée à la section 3.3, définition 8. L'implication de H dans l'analyse systématique des attaques génériques est expliquée à la section 3.4 de ce même chapitre 3.

$$
\begin{aligned}
1: &\quad L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 \neq S_1 \oplus S_2, S_1 \oplus S_2 \neq T_1 \oplus T_2 \\
2: &\quad L_1 \neq L_2, R_1 = R_2, S_1 \neq S_2, S_1 \oplus S_2 \neq T_1 \oplus T_2 \\
3: &\quad L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 \neq S_1 \oplus S_2, S_1 \oplus S_2 \neq T_1 \oplus T_2 \\
4: &\quad L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 = S_1 \oplus S_2, S_1 \oplus S_2 \neq T_1 \oplus T_2 \\
5: &\quad L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 = S_1 \oplus S_2, S_1 \oplus S_2 \neq T_1 \oplus T_2 \\
6: &\quad L_1 \neq L_2, R_1 \neq R_2, S_1 = S_2, S_1 \oplus S_2 \neq T_1 \oplus T_2 \\
7: &\quad L_1 \neq L_2, R_1 = R_2, S_1 = S_2, S_1 \oplus S_2 \neq T_1 \oplus T_2 \\
8: &\quad L_1 = L_2, R_1 \neq R_2, S_1 = S_2, S_1 \oplus S_2 \neq T_1 \oplus T_2 \\
9: &\quad L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 \neq S_1 \oplus S_2, S_1 \oplus S_2 = T_1 \oplus T_2 \\
10: &\quad L_1 \neq L_2, R_1 = R_2, S_1 \neq S_2, R_1 \oplus R_2 \neq S_1 \oplus S_2, S_1 \oplus S_2 = T_1 \oplus T_2 \\
11: &\quad L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 \neq S_1 \oplus S_2, S_1 \oplus S_2 = T_1 \oplus T_2 \\
12: &\quad L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 = S_1 \oplus S_2, S_1 \oplus S_2 = T_1 \oplus T_2 \\
13: &\quad L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, R_1 \oplus R_2 = S_1 \oplus S_2, S_1 \oplus S_2 = T_1 \oplus T_2
\end{aligned}
$$

4.1.1.2 Formules pour les coefficients H des schémas Misty L

Les formules pour les coefficients H dans le cas de M_L^k sont données dans l'annexe A, basées sur le théorème de la section 3.5.2. La formule directe est donnée au théorème 7 de la section 3.5. Les formules pour obtenir ces coefficients H par récurrence (ainsi que des valeurs pour les deux premiers tours) sont données en annexe, à la section A.3. Les valeurs exactes pour H, pour un nombre de tours $1 \leq k \leq 6$ se trouvent dans les tables de la sous-section 4.1.4 à la fin de ce chapitre.

Dans la section A.3 de l'annexe A, nous donnons les formules de récurrence pour les ε, ainsi que des valeurs pour les quatre premiers tours. Rappelons que pour analyser les complexités des différentes attaques, nous nous basons sur l'ordre de grandeur des ε. Cet ordre de grandeur pour un nombre de tours $1 \leq k \leq 12$ fait l'objet de la table 4.2 de la sous-section 4.1.2 suivante.

4.1.2 Valeurs numériques et exemples d'application aux attaques deux points

4.1.2.1 Table de valeurs pour $\varepsilon = \frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1-1/2^{2n}}$

Au chapitre 3, section 3.4, nous avons vu que de la valeur $\varepsilon = \frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1-1/2^{2n}}$, nous pouvions facilement déduire les meilleures attaques deux points. Nous renvoyons vers cette section pour les explications, ou vers la sous-section 4.1.2.2 pour des exemples d'utilisation de cette table pour estimer la complexité des meilleures attaques deux points pour $k = 5$ ou 6. La table 4.2 suivante donne l'ordre de gran-

deur des ε, pour chacun des cas exposés en annexe (sous-section A.1.4) et rappelés à la sous-section 4.1.1 précédente.

cas :	1	2	3	4	5	6	7	8	9	10	11	12	13
1 tour	1	1	1	2^{2n}	1	1	2^{2n}	1	1	1	1	1	2^{3n}
2 tours	$\frac{1}{2^n}$	1	1	1	2^n	$\frac{1}{2^n}$	1	1	1	2^n	1	1	1
3 tours	$\frac{1}{2^{2n}}$	$\frac{1}{2^n}$	$\frac{1}{2^n}$	$\frac{1}{2^n}$	1	$\frac{1}{2^n}$	1	$\frac{1}{2^n}$	$\frac{1}{2^n}$	1	1	$\frac{1}{2^n}$	1
4 tours	$\frac{1}{2^{2n}}$	$\frac{1}{2^n}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^n}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^n}$	$\frac{1}{2^n}$	$\frac{1}{2^n}$	1	$\frac{1}{2^n}$	$\frac{1}{2^n}$	$\frac{1}{2^n}$
5 tours	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^n}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^n}$	$\frac{1}{2^n}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^n}$
6 tours	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^n}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$
7 tours	$\frac{1}{2^{4n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$
8 tours	$\frac{1}{2^{4n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$
9 tours	$\frac{1}{2^{5n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{3n}}$
10 tours	$\frac{1}{2^{5n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{4n}}$
11 tours	$\frac{1}{2^{6n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{6n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{4n}}$
12 tours	$\frac{1}{2^{6n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{6n}}$	$\frac{1}{2^{6n}}$	$\frac{1}{2^{6n}}$	$\frac{1}{2^{6n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{5n}}$

TABLE 4.2: Ordre de grandeur des $\varepsilon = \frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1-1/2^{2n}}$, dans les différents cas considérés. De ces valeurs se déduisent facilement les meilleures attaques deux points.

4.1.2.2 Exemple d'application aux attaques

Au cours du chapitre 3, nous avons vu que de la valeur de ε et du nombre d'égalités n_e demandées par l'attaque deux points, il est possible de déduire la complexité de l'attaque. Ceci se résume par la formule (3.2) de la section 3.4 pour le cas d'une permutation, ou (3.3) de cette même section pour le cas d'un générateur de permutations. Accessoirement, ces formules permettent de déduire directement quel cas mènent aux meilleures attaques (propositions 6 et 7 de la sous-section 3.4.3). De la table 4.2 précédente, nous pouvons maintenant directement choisir le ou les cas menant à la meilleure complexité d'attaque deux points, comme le montrent les exemples ci-dessous. Les complexités des attaques deux points obtenues pour un nombre de tours quelconque sont données au tableau 4.3 de la section 4.1.3.

Attaque générique sur cinq tours, CPA Pour cinq tours, nous avons annoncé au chapitre 2 qu'aucune attaque deux points de fournit de complexité meilleure que $\mathcal{O}\left(2^{2n}\right)$. Examinons donc les treize cas de la sous-section A.1.4 de l'annexe A (voir aussi la section 4.1.1). Dans le cadre d'une attaque CPA-1, les cas 1 à 3 ne demandent aucune égalité impliquant les sorties, les cas 4 à 11 demandent une égalité sur les blocs de sortie, et les cas 12 et 13 en demandent deux. De la table 4.2, donnant l'ordre de grandeur de la valeur des $\varepsilon = \frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{2^{2n}}{2^{2n}-1}$, on a que les cas intéressants sont les cas 2, 3, 7, 10 et 11, car ils offrent le meilleur compromis entre l'ordre de grandeur de ε et le nombre d'égalités requises. D'après la proposition 6 de la sous-section 3.4.3, tous ces cas mènent à des attaques de même complexité. Plaçons-nous

dans un de ces cas. La formule (3.2) montre que l'on peut distinguer un schéma de Feistel d'une permutation aléatoire en calculant de l'ordre de m messages, où m vérifie :

$$\frac{m(m-1)}{2} \geq 2^{n_e n} \cdot \frac{1}{\varepsilon^2} \Leftrightarrow \frac{m(m-1)}{2} \geq 2^{4n} \tag{4.1}$$

Autrement dit, tous ces cas mènent à une attaque de complexité $\mathcal{O}\left(2^{2n}\right)$. Comme annoncé à la sous-section 2.2.5 du chapitre 2, la meilleure attaque deux points sur cinq tours nécessite de l'ordre de 2^{2n} messages. Pour que cette attaque fournisse une probabilité de succès plus proche de un, il vaut mieux supposer que nous attaquons un générateur de permutations. Cette attaque deux points fournit une complexité de l'ordre de 2^{2n} calculs, et ce quel que soit le type d'attaque considéré.

Attaque générique sur six tours, CPA Pour six tours, examinons les treize cas de la sous-section A.1.4 de l'annexe A (voir aussi la section 4.1.1). Dans le cadre d'une attaque CPA-1, tout comme pour l'attaque exposé ci-dessus, les cas 1 à 3 ne demandent aucune égalité impliquant les sorties, les cas 4 à 11 demandent une égalité sur les blocs de sortie, et les cas 12 et 13 en demandent deux. De la table 4.2, on a que les cas intéressants sont les cas 2 et 10. D'après la proposition 6, ces deux cas fournissent des attaques de complexité équivalentes (sous-section 3.4.3 du chapitre 3). Prenons le cas 10 par exemple, on a alors, dans le cas où l'on attaque une seule permutation, que le nombre m de messages à calculer pour pouvoir distinguer ψ d'une permutation aléatoire vérifie :

$$\frac{m(m-1)}{2} \geq 2^{n_e n} \cdot \frac{1}{\varepsilon^2} \Leftrightarrow \frac{m(m-1)}{2} \geq 2^{n} \cdot 2^{2n} \tag{4.2}$$

Il nous faut $\mathcal{O}\left(2^{3n}\right)$ paires de messages vérifiant les conditions sur les blocs d'entrée du cas 10, soit $R_1 = R_2$ pour deux messages. Le nombre maximal de telles paires que l'on peut obtenir pour une permutation est 2^{3n}, en calculant alors toutes les entrées possibles. Cette attaque a une probabilité de succès non-négligeable sur une seule permutation, mais pour avoir une probabilité de succès plus proche de 1, supposons que nous attaquons un générateur de permutations. Cette attaque fournit une complexité de l"ordre de $\mathcal{O}\left(2^{2n}\right)$ calculs, quel que soit le type d'attaque considéré.

Ce résultat confirme le résultat annoncé à la section 3.2 du chapitre 3. La complexité de la meilleure attaque deux points générique est $\mathcal{O}\left(2^{2n}\right)$ dans le cas des schémas Misty L (l'attaque présentée à cette section pour les schémas Misty L correspond au cas 10).

4.1.3 Résultats

Cette sous-section donne les complexités des meilleures attaques génériques sur les schémas Misty L. La première table (table 4.3), se restreint aux complexités des attaques deux points, comme nous avons privilégié ces attaques pour un nombre

de tours grands. La seconde table, table 4.4, donne les complexités des meilleures attaques trouvées, *i.e.* on ne restreint plus aux attaques deux points.

Comme annoncé au début du chapitre 3, lorsque les complexités de attaques dépassent 2^{2n}, les attaques présentées sont en fait les meilleures connues permettant de distinguer un générateur de permutations M_L^k d'un générateur de permutations aléatoires paires.

Ces deux tables peuvent être comparées à titre indicatif avec la table des meilleures complexités des schémas de Feistel classiques rappelée en début de chapitre (table 4.1), ces schémas ayant été plus étudiés.

	KPA	CPA-1	CPA-2	CPCA-1	CPCA-2
M_L^1	1	1	1	1	1
M_L^2	$2^{n/2}$	2	2	2	2
M_L^3	2^n	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	3
M_L^4	2^n	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
M_L^5	2^{2n}	2^{2n}	2^{2n}	2^{2n}	2^{2n}
M_L^6	2^{2n}	2^{2n}	2^{2n}	2^{2n}	2^{2n}
M_L^7	2^{4n}	2^{4n}	2^{4n}	2^{4n}	2^{4n}
M_L^8	2^{4n}	2^{4n}	2^{4n}	2^{4n}	2^{4n}
M_L^9	2^{6n}	2^{6n}	2^{6n}	2^{6n}	2^{6n}
M_L^{10}	2^{6n}	2^{6n}	2^{6n}	2^{6n}	2^{6n}
M_L^{11}	2^{8n}	2^{8n}	2^{8n}	2^{8n}	2^{8n}
M_L^{12}	2^{8n}	2^{8n}	2^{8n}	2^{8n}	2^{8n}
M_L^k $k\geq 6$, k pair	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$
M_L^k $k\geq 5$, k impair	$2^{(k-3)n}$	$2^{(k-3)n}$	$2^{(k-3)n}$	$2^{(k-3)n}$	$2^{(k-3)n}$

TABLE 4.3: Meilleures complexités des attaques deux points permettant de distinguer k tours de schémas Misty L d'une permutation aléatoire paire.

On voit de ces tables, qu'au moins 5 tours de schémas Misty L sont nécessaires pour éviter les attaques génériques connues. Ceci est semblable aux schémas de Feistel classiques.

Ces deux tables 4.3 et 4.4 retranscrivent bien le fait qu'il existe des attaques génériques sensiblement meilleures que les attaques deux points pour M_L^k. L'étude des attaques trois points ou quatre points n'a pas été poussée au-delà des premiers tours. La raison pour cela est que l'analyse systématique devient alors plus complexe.

Remarque : Notons que les valeurs de ces complexités ont été vérifiées jusqu'à $k = 12$ tours. Au-delà, les complexités annoncées sont des estimations. L'étude asymptotique des ε, faite en annexe, prouve une évolution *globale* des ε tous les deux tours. Plus précisément, cette étude montre une évolution de $\frac{1}{2^{2n}}$ de la plus grande valeur de ε pour un nombre de tours k, par rapport à la plus grande valeur de ε pour $k-2$ tours. Ceci ne permet pas de prouver l'évolution des complexités indiquées par les tables, mais seulement que les complexités augmentent asymptotiquement.

	KPA	CPA-1	CPA-2	CPCA-1	CPCA-2
M_L^1	1	1	1	1	1
M_L^2	$2^{n/2}$	2	2	2	2
M_L^3	2^n	4	4	4	3
M_L^4	2^n	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	4
M_L^5	$2^{3n/2}$	2^n	2^n	2^n	2^n
M_L^6	2^{2n}	2^{2n}	2^{2n}	2^{2n}	2^{2n}
M_L^7	2^{4n}	2^{4n}	2^{4n}	2^{4n}	2^{4n}
M_L^8	2^{4n}	2^{4n}	2^{4n}	2^{4n}	2^{4n}
M_L^9	2^{6n}	2^{6n}	2^{6n}	2^{6n}	2^{6n}
M_L^{10}	2^{6n}	2^{6n}	2^{6n}	2^{6n}	2^{6n}
M_L^{11}	2^{8n}	2^{8n}	2^{8n}	2^{8n}	2^{8n}
M_L^{12}	2^{8n}	2^{8n}	2^{8n}	2^{8n}	2^{8n}
M_L^k $k\geq 6$, k pair	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$
M_L^k $k\geq 7$, k impair	$2^{(k-3)n}$	$2^{(k-3)n}$	$2^{(k-3)n}$	$2^{(k-3)n}$	$2^{(k-3)n}$

TABLE 4.4: Nombre minimum de calculs nécessaires pour distinguer k tours de schémas Misty L, d'une permutation aléatoire paire.

4.1.4 Complément : valeur exacte des coefficients H pour les six premiers tours

Les tables de cette sous-section donnent les valeurs exactes des coefficients H pour les premiers six tours.

cas	1 tour	2 tours	3 tours	4 tours
1	0	$((2^n-2)!)^2$	$(2^n-3)((2^n-2)!)^3 2^n$	$(2^n-3)^2((2^n-2)!)^4 2^{n\,2}+(2^n-2)((2^n-2)!)^4 2^{n\,2}$ $+2^{2n}(2^n-1)!\,((2^n-2)!)^3$
2	0	0	$2^n(2^n-1)!\,((2^n-2)!)^2$	$2^{2n}(2^n-1)!\,((2^n-2)!)^3(2^n-2)$
3	0	0	$2^n(2^n-1)!\,((2^n-2)!)^2$	$(2^n-3)(2^n-1)!\,((2^n-2)!)^3 2^{2n}$
4	$(2^n-2)!$	$((2^n-2)!)^2$	$(2^n-2)((2^n-2)!)^3 2^n$	$(2^n-2)(2^n-3)((2^n-2)!)^4 2^{2n}$ $+2^{2n}(2^n-1)!\,((2^n-2)!)^3$
5	0	0	0	$2^{2n}(2^n-1)!\,((2^n-2)!)^3(2^n-2)$
6	0	0	$(2^n-2)((2^n-2)!)^3 2^n$	$2^{2n}((2^n-2)!)^4(2^n-2)^2$
7	0		0	$2^{2n}(2^n-1)!\,((2^n-2)!)^3(2^n-1)$
8	0	0	$2^n(2^n-1)!\,((2^n-2)!)^2$	$2^{n\,2}(2^n-1)!((2^n-2)!)^3(2^n-2)$
9	0	0	$2^n(2^n-1)!\,((2^n-2)!)^2$	$2^{2n}(2^n-1)!\,((2^n-2)!)^3(2^n-2)$
10	0		0	0
11	0	0	0	$2^{2n}((2^n-1)!)^2((2^n-2)!)^2$
12	0	$(2^n-1)!\,(2^n-2)!$	$2^n(2^n-1)!\,((2^n-2)!)^2$	$2^{2n}(2^n-1)!\,((2^n-2)!)^3(2^n-2)$
13	0		0	$2^{2n}((2^n-1)!)^2((2^n-2)!)^2$

TABLE 4.5: Valeurs des coefficients H dans les différents cas considérés, pour 1, 2, 3, et 4 tours.

cas	5 tours
1	$(2^n-3)^3((2^n-2)!)^5 2^{3n}+2\,(2^n-2)(2^n-3)((2^n-2)!)^5 2^{3n}+2\,2^{3n}(2^n-1)!\,((2^n-2)!)^4(2^n-2)$
2	$2^{3n}(2^n-1)!\,((2^n-2)!)^4(2^n-2)^2$
3	$(2^n-3)^2(2^n-1)!\,((2^n-2)!)^4 2^{3n}+2^{3n}(2^n-1)!\,((2^n-2)!)^4(2^n-2)+2^{3n}((2^n-1)!)^2((2^n-2)!)^3$
4	$(2^n-2)(2^n-3)^2((2^n-2)!)^5 2^{3n}+(2^n-2)^2((2^n-2)!)^5 2^{3n}+2\,2^{3n}(2^n-1)!\,((2^n-2)!)^4(2^n-2)$
5	$(2^n-2)(2^n-3)(2^n-1)!\,((2^n-2)!)^4 2^{3n}+2^{3n}((2^n-1)!)^2((2^n-2)!)^3$
6	$2^{3n}((2^n-2)!)^5(2^n-2)^3+2^{3n}(2^n-1)!\,((2^n-2)!)^4(2^n-1)$
7	$2^{3n}(2^n-1)!\,((2^n-2)!)^4(2^n-1)(2^n-2)$
8	$2^{3n}(2^n-1)!\,((2^n-2)!)^4(2^n-2)^2$
9	$2^{3n}(2^n-1)!\,((2^n-2)!)^4(2^n-2)^2$
10	$2^{3n}((2^n-1)!)^2((2^n-2)!)^3(2^n-1)$
11	$2^{3n}((2^n-1)!)^2((2^n-2)!)^3(2^n-2)$
12	$2^{3n}(2^n-1)!\,((2^n-2)!)^4(2^n-2)^2$
13	$2^{3n}((2^n-1)!)^2((2^n-2)!)^3(2^n-2)$

TABLE 4.6: Valeurs des coefficients H dans les différents cas considérés, pour 5 tours.

cas	6 tours
1	$(2^n-3)^4((2^n-2)!)^6 2^{4n}+3\,(2^n-2)(2^n-3)^2((2^n-2)!)^6 2^{4n}+(2^n-2)^2((2^n-2)!)^6 2^{4n}$
	$+3\,2^{4n}(2^n-1)!\,((2^n-2)!)^5(2^n-2)^2$
2	$2^{4n}(2^n-1)!\,((2^n-2)!)^5(2^n-2)^3+2^{4n}((2^n-1)!)^2((2^n-2)!)^4(2^n-1)$
3	$(2^n-3)^3(2^n-1)!\,((2^n-2)!)^5 2^{4n}+2\,(2^n-2)(2^n-3)(2^n-1)!\,((2^n-2)!)^5 2^{4n}$
	$+2\,2^{4n}((2^n-1)!)^2((2^n-2)!)^4(2^n-2)$
4	$(2^n-2)(2^n-3)^3((2^n-2)!)^6 2^{4n}+2\,(2^n-2)^2(2^n-3)((2^n-2)!)^6 2^{4n}+3\,2^{4n}(2^n-1)!\,((2^n-2)!)^5(2^n-2)^2$
5	$(2^n-2)(2^n-3)^2(2^n-1)!\,((2^n-2)!)^5 2^{4n}+2^{4n}(2^n-1)!\,((2^n-2)!)^5(2^n-2)^2$
	$+2\,2^{4n}((2^n-1)!)^2((2^n-2)!)^4(2^n-2)$
6	$2^{4n}((2^n-2)!)^6(2^n-2)^4+2\,2^{4n}(2^n-1)!\,((2^n-2)!)^5(2^n-1)(2^n-2)$
7	$2^{4n}(2^n-1)!\,((2^n-2)!)^5(2^n-1)(2^n-2)^2$
8	$2^{4n}(2^n-1)!\,((2^n-2)!)^5(2^n-2)^3+2^{4n}((2^n-1)!)^2((2^n-2)!)^4(2^n-1)$
9	$2^{4n}(2^n-1)!\,((2^n-2)!)^5(2^n-2)^3+2^{4n}((2^n-1)!)^2((2^n-2)!)^4(2^n-1)$
10	$2^{4n}((2^n-1)!)^2((2^n-2)!)^4(2^n-1)(2^n-2)$
11	$2^{4n}((2^n-1)!)^2((2^n-2)!)^4(2^n-2)^2$
12	$2^{4n}(2^n-1)!\,((2^n-2)!)^5(2^n-2)^3+2^{4n}((2^n-1)!)^2((2^n-2)!)^4(2^n-1)$
13	$2^{4n}((2^n-1)!)^2((2^n-2)!)^4(2^n-2)^2$

TABLE 4.7: Valeurs des coefficients H dans les différents cas considérés, pour 6 tours.

4.2 Approche systématique et résultats pour les schémas de Feistel avec permutations internes

La figure 4.2 rappelle la structure générale d'un schéma de Feistel.

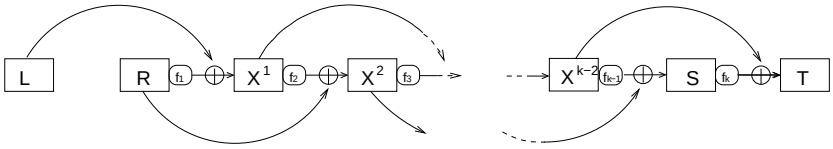

FIGURE 4.2: k tours de schémas de Feistel

4.2.1 Résumé des résultats pour les schémas de Feistel avec permutations internes

Comme dans la section précédente sur les schémas Misty L, nous rappelons dans cette sous-section les résultats obtenus sur les schémas de Feistel avec permutations internes aléatoires. Les analyses et résultats exposés dans la suite de cette section 4.2 se déduisent de ces résultats préliminaires.

4.2.1.1 Les différents cas à considérer pour H ou ε

Nous rappelons ci-dessous les cas à distinguer lors du calcul des coefficients H (définition 8 de la section 3.3) pour les schémas de Feistel avec permutations internes. Ces mêmes cas sont à distinguer lors de l'évaluation de $\varepsilon = \frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{2^{2n}}{2^{2n}-1}$, qui intervient dans lors de la déduction des meilleures attaques génériques (voir section 3.4 et 3.4.3). Pour ψ^k, il faut distinguer entre k pair et k impair (voir annexe A).

Pour un nombre k de tours impair :

$$
\begin{aligned}
1 &: \ L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq T_1 \oplus T_2, R_1 \oplus R_2 \neq S_1 \oplus S_2 \\
2 &: \ L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 = T_1 \oplus T_2, R_1 \oplus R_2 \neq S_1 \oplus S_2 \\
3 &: \ L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq T_1 \oplus T_2, R_1 \oplus R_2 = S_1 \oplus S_2 \\
4 &: \ L_1 \neq L_2, R_1 \neq R_2, S_1 = S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq T_1 \oplus T_2, R_1 \oplus R_2 \neq S_1 \oplus S_2 \\
5 &: \ L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq T_1 \oplus T_2, R_1 \oplus R_2 \neq S_1 \oplus S_2 \\
6 &: \ L_1 = L_2, R_1 \neq R_2, S_1 = S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq T_1 \oplus T_2, R_1 \oplus R_2 \neq S_1 \oplus S_2 \\
7 &: \ L_1 \neq L_2, R_1 \neq R_2, S_1 = S_2, T_1 \neq T_2, L_1 \oplus L_2 = T_1 \oplus T_2, R_1 \oplus R_2 \neq S_1 \oplus S_2 \\
8 &: \ L_1 \neq L_2, R_1 = R_2, S_1 = S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq T_1 \oplus T_2, R_1 \oplus R_2 = S_1 \oplus S_2 \\
9 &: \ L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq T_1 \oplus T_2, R_1 \oplus R_2 = S_1 \oplus S_2 \\
10 &: \ L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 = T_2, L_1 \oplus L_2 = T_1 \oplus T_2, R_1 \oplus R_2 \neq S_1 \oplus S_2 \\
11 &: \ L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 = T_1 \oplus T_2, R_1 \oplus R_2 = S_1 \oplus S_2 \\
12 &: \ L_1 \neq L_2, R_1 = R_2, S_1 = S_2, T_1 \neq T_2, L_1 \oplus L_2 = T_1 \oplus T_2, R_1 \oplus R_2 = S_1 \oplus S_2 \\
13 &: \ L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 = T_2, L_1 \oplus L_2 = T_1 \oplus T_2, R_1 \oplus R_2 = S_1 \oplus S_2
\end{aligned}
$$

Pour un nombre k de tours pair :

$$
\begin{aligned}
1 &: \; L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq S_1 \oplus S_2, R_1 \oplus R_2 \neq T_1 \oplus T_2 \\
2 &: \; L_1 \neq L_2, R_1 = R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq S_1 \oplus S_2, R_1 \oplus R_2 \neq T_1 \oplus T_2 \\
3 &: \; L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq S_1 \oplus S_2, R_1 \oplus R_2 \neq T_1 \oplus T_2 \\
4 &: \; L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 = S_1 \oplus S_2, R_1 \oplus R_2 \neq T_1 \oplus T_2 \\
5 &: \; L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 = T_2, L_1 \oplus L_2 \neq S_1 \oplus S_2, R_1 \oplus R_2 \neq T_1 \oplus T_2 \\
6 &: \; L_1 \neq L_2, R_1 = R_2, S_1 = S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq S_1 \oplus S_2, R_1 \oplus R_2 \neq T_1 \oplus T_2 \\
7 &: \; L_1 \neq L_2, R_1 = R_2, S_1 \neq S_2, T_1 = T_2, L_1 \oplus L_2 \neq S_1 \oplus S_2, R_1 \oplus R_2 = T_1 \oplus T_2 \\
8 &: \; L_1 \neq L_2, R_1 = R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 = S_1 \oplus S_2, R_1 \oplus R_2 \neq T_1 \oplus T_2 \\
9 &: \; L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 = T_2, L_1 \oplus L_2 = S_1 \oplus S_2, R_1 \oplus R_2 \neq T_1 \oplus T_2 \\
10 &: \; L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 = S_1 \oplus S_2, R_1 \oplus R_2 = T_1 \oplus T_2 \\
11 &: \; L_1 \neq L_2, R_1 = R_2, S_1 \neq S_2, T_1 = T_2, L_1 \oplus L_2 = S_1 \oplus S_2, R_1 \oplus R_2 = T_1 \oplus T_2
\end{aligned}
$$

4.2.1.2 Formules pour les coefficients H pour schémas de Feistel avec permutations internes

Les formules pour les coefficients H dans le cas de ψ^k sont données en annexe A. Les formules directes sont basées sur le théorème 7 de la section 3.5. Les formules directes obtenues sont données à la sous-section A.2.3. Les formules pour obtenir ces coefficients H par récurrence (ainsi que des valeurs pour les deux premiers tours) sont données à la section A.4 en annexe. À titre indicatif, les valeurs exactes des coefficients H pour ψ^k, $1 \leq k \leq 6$, sont données à la section 4.2.4 de ce chapitre, tables 4.3 à 4.5.

À la section A.4 de l'annexe A, nous donnons les formules de récurrence pour les ε, ainsi que des valeurs exactes pour les deux premiers tours. Cependant, pour déduire les meilleures attaques génériques deux points, seul l'ordre de grandeur importe. La table 4.8 de la section 4.2.2 suivante donne l'ordre de grandeur des ε dans les différents cas de la partie 4.2.1.1 précédentes, pour un nombre de tours entre 1 et 12.

4.2.2 Valeurs numériques et exemples d'application aux attaques deux points

4.2.2.1 Table de valeurs pour $\varepsilon = \frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1-1/2^{2n}}$

Au chapitre 3, section 3.4, nous avons vu que de la valeur $\varepsilon = \frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1-1/2^{2n}}$, nous pouvions facilement déduire les meilleures attaques deux points. La table 4.8 suivante donnent l'ordre de grandeur des ε, pour chacun des cas exposés à la sous-section A.2.4 et rappelés à la section 4.2.1 précédente. Notons que les cas considérés lorsque le nombre de tours de schémas de Feistel est pair, ne sont pas les mêmes que lorsque le nombre de tours de schémas de Feistel est impair. Le paragraphe 4.2.2.2 illustre comment l'on peut déduire la complexité des meilleures attaques génériques deux points, pour un nombre de tours donnés, à partir de cette table. Notamment, nous revenons sur les attaques sur ψ^3 et ψ^6.

cas :	1	2	3	4	5	6	7	8	9	10	11	12	13
1 tour	1	1	$2^{n\,2}$	1	1	1	1	1	1	1	1	$2^{n\,3}$	1
2 tours	$\frac{1}{2^n}$	1	$\frac{1}{2^n}$	1	$\frac{1}{2^n}$	1	1	2^n	1	1	1		
3 tours	$\frac{1}{2^{2n}}$	$\frac{1}{2^n}$	$\frac{1}{2^n}$	$\frac{1}{2^n}$	$\frac{1}{2^n}$	$\frac{1}{2^n}$	1	1	1	$\frac{1}{2^n}$	$\frac{1}{2^n}$	1	1
4 tours	$\frac{1}{2^{3n}}$	$\frac{1}{2^n}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^n}$	$\frac{1}{2^n}$	1	$\frac{1}{2^n}$	$\frac{1}{2^{2n}}$	1		
5 tours	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^n}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^n}$	$\frac{1}{2^n}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^n}$	1	$\frac{1}{2^n}$
6 tours	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^n}$		
7 tours	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^n}$	$\frac{1}{2^{3n}}$
8 tours	$\frac{1}{2^{4n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{2n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$		
9 tours	$\frac{1}{2^{5n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{3n}}$
10 tours	$\frac{1}{2^{6n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{6n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{3n}}$		
11 tours	$\frac{1}{2^{5n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{6n}}$	$\frac{1}{2^{6n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{6n}}$	$\frac{1}{2^{4n}}$	$\frac{1}{2^{3n}}$	$\frac{1}{2^{4n}}$
12 tours	$\frac{1}{2^{6n}}$	$\frac{1}{2^{6n}}$	$\frac{1}{2^{6n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{6n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{6n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{6n}}$	$\frac{1}{2^{5n}}$	$\frac{1}{2^{4n}}$		

TABLE 4.8: Ordre de grandeur des $\varepsilon = \frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1-1/2^{2n}}$, dans les différents cas considérés. De ces valeurs se déduisent facilement les meilleures attaques deux points.

4.2.2.2 Exemples d'application aux attaques

Au cours du chapitre 3, nous avons vu que de la valeur de ε et du nombre d'égalités n_e demandées par l'attaque deux points, il est possible de déduire la complexité de l'attaque. Ceci se résume par la formule (3.2) de la section 3.4 pour le cas d'une permutation, ou (3.3) de cette même section pour le cas d'un générateur de permutations. Ces formules permettent également de déduire directement quel cas mènent aux meilleures attaques (propositions 6 et 7 de la sous-section 3.4.3). De la table 4.8 précédente, nous pouvons alors directement choisir, pour chaque nombre de tours, le ou les cas menant à la meilleure complexité d'attaque deux points. Ceci est illustré par les exemples ci-dessous, et les résultat pour un nombre de tours quelconque sont donnés dans le tableau 4.9 de la section 4.2.3.

Rappelons que pour trois tours, nous avions observé au chapitre 2 une moins bonne complexité des attaques deux points (en KPA) que pour des schémas de Feistel classiques, avec fonctions internes. Six tours est le deuxième moment où apparaissent des différences avec les schémas de Feistel classiques, et le moment à partir duquel ces différences deviennent régulières (on peut par exemple comparer la table 4.1 du début de ce chapitre et la table 4.9 de la section 4.2.3. Nous revenons ici sur ces deux cas, et voyons qu'effectivement, les attaques exposées au chapitre 2 étaient les attaques deux points fournissant la meilleure complexité.

Attaque générique sur trois tours, KPA Étudions les KPA sur trois tours de schémas de Feistel avec permutations internes, pour lesquelles nous avons vu que, à la différence des schémas de Feistel classiques, il n'existe pas d'attaque de complexité $\mathcal{O}\left(2^{n/2}\right)$. Pour trois tours, il y a treize cas à considérer (cf. sous-section A.2.4 de l'annexe A ou la section 4.2.1 ci-dessus). Pour ce qui est du nombre d'égalités sur

les entrées/sorties demandées par chaque cas dans le cadre d'une KPA : le cas 1 ne demande aucune égalité, les cas 2 à 5 demandent une égalité, les cas 6 à 11 en demandent deux, et les cas 12 et 13 demandent trois égalités. La table 4.8 donne l'ordre de grandeur de la valeur des $\varepsilon = \frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{2^{2n}}{2^{2n}-1}$ dans les différents cas. On obtient de cette table que les cas les plus intéressants sont le cas 1, les cas 2 à 5, et les cas 7, 8 et 9, car ceux sont ceux présentant le meilleur compromis entre l'ordre de grandeur de ε et le nombre d'égalités requises (voir section 3.4 du chapitre 3). De la proposition 6 de la sous-section 3.4.3 du chapitre 3, on déduit que les cas menant à la meilleure complexité d'attaque sont les cas 7, 8 et 9 (et ils mènent tous trois à la même complexité).

Plaçons-nous dans un de ces cas. La formule (3.2) montre que l'on peut distinguer un schéma de Feistel d'une permutation aléatoire en calculant de l'ordre de m messages, où m vérifie :

$$\frac{m(m-1)}{2} \geq 2^{n_e n} \cdot \frac{1}{\varepsilon^2} \Leftrightarrow \frac{m(m-1)}{2} \geq 2^{2n} \tag{4.3}$$

Autrement dit, ces cas 7, 8, et 9 mènent à une attaque de complexité $\mathcal{O}(2^n)$, comme annoncé à la sous-section 2.1.3 de la section 2.1. On peut remarquer que dans cette sous-section 2.1.3, c'est le cas 9 qui avait été exposé. Ceci confirme qu'il n'existe pas d'attaque deux points de complexité meilleure que $\mathcal{O}(2^n)$, car nous avons balayé toutes les possibilités d'égalités entre les blocs d'entrée et de sortie de deux messages, soit toutes les attaques deux points.

Remarque : Nous aurions pu déduire des valeurs de la table 4.8, sans rentrer dans le détail des calculs de complexité des attaques, qu'aucun cas ne mène à une attaque en $\mathcal{O}\left(2^{n/2}\right)$.

En effet, pour trois tours de schémas de Feistel classiques, dans le cas $R_1 \oplus S_1 = R_2 \oplus S_2$, la valeur de ε est grande (elle vaut 1) alors que seule une condition sur les blocs d'entrée et de sortie est demandée ($n_e = 1$). Pour des schémas de Feistel avec permutations internes, il n'y a pas de situation similaire. Ceci se voit directement dans la table 4.8. La sécurité en KPA semble ainsi meilleure pour les schémas de Feistel avec permutations internes, et ceci confirme que l'étude de ces deux schémas doit se faire séparément.

Énonçons rapidement la KPA sur trois tours de schémas de Feistel classiques pour ce cas $R_1 \oplus S_1 = R_2 \oplus S_2$ [Pat01], et voyons la différence avec cette même attaque sur trois tours de schémas Misty L. Pour des schémas de Feistel classiques, la probabilité d'avoir cette égalité entre deux messages est $\mathcal{O}\left(\frac{2}{2^n}\right)$. En effet, elle se produit soit lorsque $R_1 \neq R_2$ et $L_1 \oplus f_1(R_1) = L_2 \oplus f_1(R_2)$ (avec probabilité $\frac{1}{2^n}$), soit lorsque $L_1 \oplus f_1(R_1) \neq L_2 \oplus f_1(R_2)$ et $f_2(L_1 \oplus f_1(R_1)) = f_2(L_2 \oplus f_1(R_2))$ (avec probabilité $\frac{1}{2^n}$, car f_2 est une fonction aléatoire). Dans le cas de schémas de Feistel avec permutations internes, l'égalité à laquelle on s'intéresse ne se produit alors plus que[1] lorsque $R_1 \neq R_2$ et $L_1 \oplus f_1(R_1) = L_2 \oplus f_1(R_2)$ et avec probabilité $\frac{1}{2^n}$, tout comme pour une permutation aléatoire.

1. En particulier, f_2 est une permutation et ne permet plus la deuxième des conditions précédente.

Attaque générique sur six tours, CPA Pour six tours, nous examinons les onze cas de la sous-section A.2.4 de l'annexe A (voir aussi la section 4.2.1). Dans le cadre d'une attaque CPA-1, les cas 1 à 3 ne demandent aucune égalité impliquant les sorties, les cas 4 à 8 demandent une égalité sur les blocs de sortie, et les cas 9 à 11 en demandent deux. De la table 4.8, on a que les cas intéressants sont tous les cas sauf les cas 5, 9 et 10. De la proposition 6 (sous-section 3.4.3 du chapitre 3), on déduit que le cas menant à l'attaque de meilleur complexité est le cas 11. On a alors, dans le cas où l'on attaque une seule permutation, le nombre m de messages à calculer pour pouvoir distinguer ψ d'une permutation aléatoire vérifie :

$$\frac{m(m-1)}{2} \geq 2^{n_e n} \cdot \frac{1}{\varepsilon^2} \Leftrightarrow \frac{m(m-1)}{2} \geq 2^{2n} \cdot 2^{2n} \tag{4.4}$$

Il nous faut 2^{4n} paires de messages vérifiant les conditions sur les blocs d'entrée du cas 11, soit $R_1 = R_2$ pour deux messages. Or le nombre maximal de telles paires que l'on peut obtenir pour une permutation est 2^{3n}, en calculant alors toutes les entrées possibles. Cette attaque ne permet pas de distinguer une seule permutation ψ^6 d'une permutation aléatoire. Plaçons-nous dans le cas d'une attaque sur un générateur de permutations. La table 4.8 et la proposition 7 de la sous-section 3.4.3 montrent qu'à la fois le cas 4 et le cas 11 mènent à l'attaque de meilleure complexité. Le nombre de permutations nécessaires pour que l'attaque aboutisse (voir la formule (3.3) de la section 3.4) est λ vérifiant (ici $\frac{m(m-1)}{2} = 2^{3n}$) :

$$\frac{\lambda \cdot m(m-1)}{2} \geq 2^{n_e n} \cdot \frac{1}{\varepsilon^2} \Leftrightarrow \lambda \cdot \frac{m(m-1)}{2} \geq 2^{2n} \cdot 2^{2n} \tag{4.5}$$

On trouve $\lambda = \mathcal{O}(2^n)$, pour une complexité de l'ordre de $\lambda \cdot 2^{2n}$, où 2^{2n} est le nombre de messages évalués par permutation, soit $\mathcal{O}\left(2^{3n}\right)$. Ceci permet de confirmer que l'attaque sur six tours présentée à la section 3.2 du chapitre 3 est l'attaque deux points de meilleure complexité.

4.2.3 Résultats

Cette sous-section donne les complexités des meilleures attaques génériques sur les schémas de Feistel avec permutations internes. La première table (table 4.9), se restreint aux complexités des attaques deux points, comme nous avons privilégié ces attaques. La seconde table, table 4.10, donne les complexités des meilleures attaques génériques trouvées. Notons que pour le cas des schémas de Feistel, nous n'avons pas forcément cherché d'autres attaques que les attaques deux points. Par suite, la seule différence entre ces deux tables est l'attaque CPCA-2 sur trois tours, fonctionnant aussi pour des schémas de Feistel avec fonctions internes (voir section 2.1.3 du chapitre 2).

Rappelons que les complexités supérieures à 2^{2n} indiquées dans les tables correspondent au nombre de calculs nécessaires pour distinguer un générateur de permutations ψ^k d'un générateur de permutations aléatoires paires (voir aussi l'introduction au chapitre 3).

Enfin, comme suggéré plus haut ou dans le cas des schémas Misty L, ces deux tables peuvent être comparées à titre indicatif avec la table des meilleures complexités des schémas de Feistel classiques rappelée en début de chapitre (table 4.1).

	KPA	CPA-1	CPA-2	CPCA-1	CPCA-2
ψ^1	1	1	1	1	1
ψ^2	$2^{n/2}$	2	2	2	2
ψ^3	2^n	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
ψ^4	2^n	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
ψ^5	$2^{3n/2}$	2^n	2^n	2^n	2^n
ψ^6	2^{3n}	2^{3n}	2^{3n}	2^{3n}	2^{3n}
ψ^7	2^{3n}	2^{3n}	2^{3n}	2^{3n}	2^{3n}
ψ^8	2^{4n}	2^{4n}	2^{4n}	2^{4n}	2^{4n}
ψ^9	2^{6n}	2^{6n}	2^{6n}	2^{6n}	2^{6n}
ψ^{10}	2^{6n}	2^{6n}	2^{6n}	2^{6n}	2^{6n}
ψ^{11}	2^{7n}	2^{7n}	2^{7n}	2^{7n}	2^{7n}
ψ^{12}	2^{9n}	2^{9n}	2^{9n}	2^{9n}	2^{9n}
$\psi^k, k\geq 6,\ k=0\ mod\, 3$	$2^{(k-3)n}(+)$	$2^{(k-3)n}$	$2^{(k-3)n}$	$2^{(k-3)n}(+)$	$2^{(k-3)n}$
$\psi^k, k\geq 6,\ k=1 \text{ or } 2\ mod\, 3$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$

TABLE 4.9: Meilleure complexité des attaques deux points permettant de distinguer k tours de schémas de Feistel d'une permutation aléatoire paire.

Ici, à part pour trois tours et dans le cas d'une CPCA-2, nous n'avons pas repéré d'autres attaques que les attaques deux points, les deux tableaux sont quasi-identiques. On voit encore qu'au moins cinq tours de schémas de Feistel avec permutations internes doivent être utilisés pour éviter les attaques génériques connues.

En comparaison aux schémas de Feistel classiques, on observe une première différence pour trois tours, en KPA. Ceci a déjà été développé à la partie 4.2.2.2. Ensuite, une différence apparaît tous les trois tours, où la complexité des attaques est alors moins bonne que pour les schémas de Feistel classiques. Autrement dit, utilisés avec des permutations internes, la sécurité des schémas de Feistel balancés semble meilleure, mais plus d'études devraient être menées sur ce schéma.

4.2.4 Complément : valeur exacte des coefficients H, pour les six premiers tours

Les tables de cette sous-section donnent les valeurs exactes des coefficients H pour les premiers six tours.

nombre k de tours	KPA	CPA-1	CPA-2	CPCA-1	CPCA-2
ψ^1	1	1	1	1	1
ψ^2	$2^{n/2}$	2	2	2	2
ψ^3	2^n	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	3
ψ^4	2^n	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
ψ^5	$2^{3n/2}$	2^n	2^n	2^n	2^n
ψ^6	2^{3n}	2^{3n}	2^{3n}	2^{3n}	2^{3n}
ψ^7	2^{3n}	2^{3n}	2^{3n}	2^{3n}	2^{3n}
ψ^8	2^{4n}	2^{4n}	2^{4n}	2^{4n}	2^{4n}
ψ^9	2^{6n}	2^{6n}	2^{6n}	2^{6n}	2^{6n}
ψ^{10}	2^{6n}	2^{6n}	2^{6n}	2^{6n}	2^{6n}
ψ^{11}	2^{7n}	2^{7n}	2^{7n}	2^{7n}	2^{7n}
ψ^{12}	2^{9n}	2^{9n}	2^{9n}	2^{9n}	2^{9n}
ψ^k $k\geq 6$, $k=0$ $mod\,3$	$2^{(k-3)n}$	$2^{(k-3)n}(+)$	$2^{(k-3)n}$	$2^{(k-3)n}$	$2^{(k-3)n}$
$\psi^k, k\geq 6$, $k=1$ or 2 $mod\,3$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$

TABLE 4.10: Nombre maximum de calculs nécessaires pour distinguer k tours de schémas de Feistel avec permutations internes, d'une permutation aléatoire paire.

cas	1 tour	2 tours	3 tours	4 tours
1	0	$((2^n-2)!)^2$	$((2^n-2)!)^3 2^n (2^n-3)$	$((2^n-2)!)^4 2^{2n} (2^n-3)^2$ $+2\,(2^n-1)!\,((2^n-2)!)^3 2^{2n}$
2	0	0	$((2^n-2)!)^3 2^n (2^n-2)$	$(2^n-1)!\,((2^n-2)!)^3 2^{n\,2} (2^n-2)$
3	$(2^n-2)!$	$((2^n-2)!)^2$	$(2^n-1)!\,((2^n-2)!)^2 2^n$	$((2^n-2)!)^4 2^{2n} (2^n-2)(2^n-3)$ $+(2^n-1)!\,((2^n-2)!)^3 2^{2n}$
4	0	0	$(2^n-1)!\,((2^n-2)!)^2 2^n$	$((2^n-2)!)^4 2^{2n} (2^n-2)(2^n-3)$ $+(2^n-1)!\,((2^n-2)!)^3 2^{2n}$
5	0	$((2^n-2)!)^2$	$((2^n-2)!)^3 2^n (2^n-2)$	$((2^n-2)!)^4 2^{2n} (2^n-2)^2$
6	0	0	$(2^n-1)!\,((2^n-2)!)^2 2^n$	$((2^n-1)!)^2 ((2^n-2)!)^2 2^{2n}$
7	0	0	0	$(2^n-1)!\,((2^n-2)!)^3 2^{n\,2} (2^n-1)$
8	0	$(2^n-1)!\,(2^n-2)!$	0	0
9	0	0	0	$((2^n-2)!)^4 2^{2n} (2^n-2)^2$ $+(2^n-1)!\,((2^n-2)!)^3 2^{n\,2}$
10	0	0	$((2^n-2)!)^3 2^n (2^n-1)$	$((2^n-2)!)^4 2^{2n} (2^n-2)^2$ $+(2^n-1)!\,((2^n-2)!)^3 2^{n\,2}$
11	0	0	$(2^n-1)!\,((2^n-2)!)^2 2^n$	0
12	$(2^n-1)!$		0	
13	0		0	

FIGURE 4.3: valeurs des coefficients H dans les différents cas considérés, pour 1,2,3 et 4 tours.

cas	5 tours
1	$((2^n-2)!)^5 2^{3n}\left((2^n-3)^2+2^n-2\right)(2^n-3)+(2^n-1)!\,((2^n-2)!)^4 2^{3n}(3\,2^n-7)$
2	$((2^n-2)!)^5 2^{3n}(2^n-2)(2^n-3)^2+(2^n-1)!\,((2^n-2)!)^4 2^{3n}(3\,2^n-6)$
3	$((2^n-2)!)^5 2^{3n}\left((2^n-3)^2+2^n-2\right)(2^n-2)+(2^n-1)!\,((2^n-2)!)^4 2^{3n}(2^n-3)$
4	$(2^n-1)!\,((2^n-2)!)^4 2^{3n}(2^n-2)(2^n-3)+((2^n-1)!)^2((2^n-2)!)^3 2^{n\,3}$
5	$((2^n-2)!)^5 2^{3n}(2^n-2)^2(2^n-3)+(2^n-1)!\,((2^n-2)!)^4 2^{3n}(2\,2^n-3)$
6	$(2^n-1)!\,((2^n-2)!)^4 2^{3n}(2^n-2)^2$
7	$(2^n-1)!\,((2^n-2)!)^4 2^{n\,3}(2^n-2)^2+((2^n-1)!)^2((2^n-2)!)^3 2^{3n}$
8	$((2^n-1)!)^2((2^n-2)!)^3 2^{3n}(2^n-1)$
9	$((2^n-2)!)^5 2^{3n}(2^n-2)^3+(2^n-1)!\,((2^n-2)!)^4 2^{n\,3}(2^n-2)$
10	$((2^n-2)!)^5 2^{3n}(2^n-3)(2^n-1)(2^n-2)+(2^n-1)!\,((2^n-2)!)^4 2^{3n}(2^n-1)$
11	$((2^n-2)!)^5 2^{3n}(2^n-2)^2(2^n-3)+(2^n-1)!\,((2^n-2)!)^4 2^{3n}(2^n-2)$
12	0
13	$((2^n-2)!)^5 2^{3n}(2^n-2)^2(2^n-1)+(2^n-1)!\,((2^n-2)!)^4 2^{3n}(2^n-1)$

FIGURE 4.4: Valeurs des coefficients H dans les différents cas considérés, pour 5 tours.

cas	6 tours
1	$((2^n-2)!)^6 2^{4n}\left((2^n-3)^2+2^n-2\right)^2+4\,(2^n-1)!\,((2^n-2)!)^5 2^{4n}(2^n-2)(2^n-3)+((2^n-1)!)^2((2^n-2)!)^4 2^{4n}$
2	$(2^n-1)!\,((2^n-2)!)^5 2^{n\,4}(2^n-3)(2^n-2)^2+((2^n-1)!)^2((2^n-2)!)^4 2^{n\,4}(2\,2^n-3)$
3	$((2^n-2)!)^6 2^{4n}\left((2^n-3)^2+2^n-2\right)(2^n-2)^2+(2^n-1)!\,((2^n-2)!)^5 2^{4n}\left((2^n-3)(2^n-1)+2\,(2^n-2)^2\right)$
4	$((2^n-2)!)^6 2^{4n}(2^n-2)(2^n-3)\left((2^n-3)^2+2^n-2\right)+(2^n-1)!\,((2^n-2)!)^5 2^{n\,4}\left(2\,(2^n-2)^2+2\,(2^n-2)(2^n-3)\right)$ $+\ ((2^n-1)!)^2((2^n-2)!)^4 2^{4n}$
5	$((2^n-2)!)^6 2^{4n}(2^n-2)^4+2\,(2^n-1)!\,((2^n-2)!)^5 2^{4n}(2^n-1)(2^n-2)$
6	$((2^n-1)!)^2((2^n-2)!)^4 2^{4n}(2^n-2)^2$
7	$(2^n-1)!\,((2^n-2)!)^5 2^{4n}(2^n-3)(2^n-1)(2^n-2)+((2^n-1)!)^2((2^n-2)!)^4 2^{4n}(2^n-1)$
8	$(2^n-1)!\,((2^n-2)!)^5 2^{n\,4}(2^n-2)^3+((2^n-1)!)^2((2^n-2)!)^4 2^{4n}(2^n-2)$
9	$((2^n-2)!)^6 2^{4n}(2^n-2)^3(2^n-3)+(2^n-1)!\,((2^n-2)!)^5 2^{4n}\left((2^n-2)(2^n-1)+2\,(2^n-2)^2\right)$
10	$((2^n-2)!)^6 2^{4n}(2^n-2)^2(2^n-3)^2+4\,(2^n-1)!\,((2^n-2)!)^5 2^{4n}(2^n-2)^2+((2^n-1)!)^2((2^n-2)!)^4 2^{4n}$
11	$(2^n-1)!\,((2^n-2)!)^5 2^{4n}(2^n-1)(2^n-2)^2+((2^n-1)!)^2((2^n-2)!)^4 2^{n\,4}(2^n-1)$

FIGURE 4.5: Valeurs des coefficients H dans les différents cas considérés, pour 6 tours.

Deuxième partie

CRYPTANALYSE EN CRYPTOLOGIE MULTIVARIÉE

Chapitre 5

Introduction à la Cryptologie Multivariée, Outils

La cryptologie multivariée est une branche de la cryptologie à clé publique, ayant émergé dans les années 1980. Les algorithmes en cryptologie multivariée sont basés sur des systèmes de polynômes multivariés. On parle encore de "schémas multivariés". Ces schémas se sont longtemps montrés très attractifs car ils permettent notamment de fournir des signatures asymétriques très courtes nécessitant très peu de mémoire vive. De plus, ils sont basés sur un problème difficile différent de ceux utilisés classiquement en cryptologie asymétrique, à savoir le problème "MQ", qui consiste à résoudre un système de polynômes en plusieurs variables. Plus précisément, le chiffrement par exemple consiste à évaluer un tel système de polynômes publics en le message clair. Sans information supplémentaire, l'attaquant se trouve face au problème MQ. L'intérêt de baser des schémas à clé publique sur ce problème est qu'il résisterait à l'émergence éventuelle des ordinateurs quantiques, à la différence du problème de la factorisation ou du logarithme discret par exemple.

Malheureusement, des cryptanalyses de beaucoup de schémas multivariés ont été proposées ces dernières années, faisant perdre la foi de la communauté en ces schémas. Les cryptanalyses proposées sont souvent dues au fait que la génération du système d'équations quadratiques formant la clé publique est très particulière (le principe général de construction est décrit avec plus de précision à la section 5.1). Le système quadratique de la clé publique se trouve être souvent plus simple à résoudre qu'une instance générique de même taille. Parfois encore, la manière dont est conçu l'algorithme permet d'obtenir plus d'information que celle donnée par la clé publique. De telles astuces nous ont en particulier permis de cryptanalyser le schéma HM [PCG98a, FJPT10], ou encore de retrouver la clé secrète pour certaines instances de HFE [Pat96, BFJT09]. Ces cryptanalyses font l'objet des chapitres 6 et 7.

Dans ce chapitre, nous donnons à la section 5.1, comme annoncé, une description générale des schémas multivariés. Nous y donnons également la description de quelques schémas particuliers. Dans la section 5.2, nous donnons les préliminaires nécessaires à la compréhension de la partie II. Plus précisément, nous y exposons quelques rappels mathématiques ainsi que des complexités existantes concernant la résolution de problèmes associés à la cryptologie multivariée.

Sommaire

5.1 Description générale des schémas multivariés et problèmes difficiles sous-jacents

La plupart des fonctions à sens unique utilisées en cryptologie multivariée sont basées sur l'évaluation d'un ensemble de polynômes quadratiques $\mathbf{p}$:

$$\begin{cases} \mathbf{p}_1(x_1, \ldots, x_u) \\ \quad \vdots \\ \mathbf{p}_m(x_1, \ldots, x_u). \end{cases}$$

Le problème difficile justifiant l'appellation "à sens unique" pour ces applications, est le problème "MQ", consistant à résoudre un système de polynômes quadratiques en plusieurs variables :

MQ-décisionnel

Donnée : Un corps fini K et un ensemble $\mathbf{p}$ de m polynômes quadratiques de $K[x_1, \ldots, x_u]$:

$$\begin{cases} \mathbf{p}_1(x_1, \ldots, x_u) \\ \quad \vdots \\ \mathbf{p}_m(x_1, \ldots, x_u). \end{cases}$$

Problème : Existe-t-il $(z_1, \ldots, z_u) \in K^u$ tel que :

$$\begin{cases} \mathbf{p}_1(z_1, \ldots, z_u) = 0 \\ \quad \vdots \\ \mathbf{p}_m(z_1, \ldots, z_u) = 0. \end{cases}$$

MQ

Donnée : Un corps fini K et un ensemble $\mathbf{p}$ de m polynômes quadratiques de $K[x_1, \ldots, x_u]$:

$$\begin{cases} \mathbf{p}_1(x_1, \ldots, x_u) \\ \quad \vdots \\ \mathbf{p}_m(x_1, \ldots, x_u). \end{cases}$$

PROBLÈME : Trouver $(z_1, \ldots, z_u) \in K^u$ tel que :

$$\begin{cases} \mathbf{p}_1(z_1, \ldots, z_u) = 0 \\ \quad \vdots \\ \mathbf{p}_m(z_1, \ldots, z_u) = 0. \end{cases}$$

Le problème MQ décisionnel est un problème NP-complet [FY30, GP97], le problème MQ est un problème NP-dur. En cryptologie, les algorithmes généralement les plus performants pour la résolution de systèmes multivariés sont les algorithmes de calcul de bases de Gröbner. Ce point est détaillé à la sous-section 5.2.2. Un aspect attirant de la cryptologie multivariée est que dans l'éventualité de l'apparition d'ordinateurs quantiques, il n'existe pas d'algorithme polynomial pour la résolution de MQ, contrairement à d'autres problèmes difficiles fréquemment utilisés en cryptologie à clé publique. Par exemple, le problème du logarithme discret ou encore celui de la factorisation, notamment à la base du RSA, seraient à proscrire. D'ailleurs, et bien que le problème sous-jacent ne soit pas le même, les schémas multivariés peuvent être vus comme une généralisation du RSA, où l'évaluation sur $\mathbb{Z}/n\mathbb{Z}$ du polynôme $x \mapsto x^e$ est remplacée par l'évaluation d'un système de polynômes en plusieurs inconnues sur K.

Afin que l'utilisateur légitime puisse facilement inverser un tel système d'équations $\mathbf{p}$, les schémas en cryptologie multivariée nécessitent l'introduction d'une trappe (tout comme l'élévation à la puissance secrète $d = e^{-1} \mod \phi(n)$ dans le RSA). Pour établir $\mathbf{p}$, nous partons alors d'un système algébrique bien choisi $\mathbf{f}$:

$$\begin{cases} \mathbf{f}_1(a_1, \ldots, a_u) \\ \quad \vdots \\ \mathbf{f}_m(a_1, \ldots, a_u), \end{cases}$$

qui soit *facile à inverser*. Autrement dit, pour tout élément $(b_1, \ldots, b_m) \in K^m$, il existe une méthode efficace pour calculer l'ensemble des zéros du système [1] :

$$\begin{cases} \mathbf{f}_1(a_1, \ldots, a_u) - b_1 \\ \quad \vdots \\ \mathbf{f}_m(a_1, \ldots, a_u) - b_m. \end{cases}$$

Ensuite, afin de cacher la structure spécifique de $\mathbf{f}$, on compose ce système polynomial par deux applications affines inversibles S et T :

$$S : K^u \to K^u \ ; \ T : K^m \to K^m.$$

De cette manière, le système $\mathbf{p}$ est construit comme $T \circ \mathbf{f} \circ S$. Ceci est représenté par la figure 5.1.

1. Plusieurs solutions peuvent exister, ce qui peut être problématique, notamment en chiffrement. On peut alors par exemple introduire de la redondance pour repérer, parmi toutes ces solutions, la bonne.

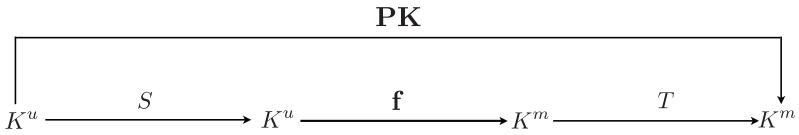

FIGURE 5.1: $\mathbf{p} = T \circ \mathbf{f} \circ S$.

La clé publique de tels systèmes, notée **PK** au cours de la partie II, consiste en le système $\mathbf{p}$. La clé secrète est constituée des deux applications S et T, et inclut parfois également $\mathbf{f}$. Beaucoup de schémas sont basés sur ce principe et diffèrent fondamentalement uniquement dans le choix de $\mathbf{f}$ [Pat97, PCG01a, PCG01b, Kob98, WP05b]. Nous en exposons quelques-uns à la section 5.3. Voyons leur fonctionnement en chiffrement ou signature.

Le chiffrement d'un message $\mathbf{x} = (x_1, \ldots, x_u) \in K^u$ se fait en évaluant **PK** en $\mathbf{x}$:

$$\begin{cases} y_1 = \mathbf{p}_1(x_1, \ldots, x_u) \\ \quad \vdots \\ y_m = \mathbf{p}_m(x_1, \ldots, x_u). \end{cases}$$

Pour retrouver le message clair $\mathbf{x}$ à partir du chiffré $\mathbf{y} = (y_1, \ldots, y_m) \in K^m$, l'utilisateur détenteur de la clé secrète peut successivement :

1. Appliquer l'inverse de T à $\mathbf{y}$. Il évalue $\mathbf{b} = T^{-1}(\mathbf{y}) \in K^m$.

2. Calculer $\mathbf{a} \in K^u$ tel que $\mathbf{f}(\mathbf{a}) = \mathbf{b}$. Ceci peut se faire efficacement grâce au choix du système $\mathbf{f}$.

3. Retrouver $\mathbf{x} \in K^u$ en évaluant l'inverse de S en $\mathbf{a}$.

Les schémas multivariés s'utilisent aussi pour le calcul de signatures. Il existe d'ailleurs des déclinaisons de certains schémas multivariés s'utilisant uniquement en signature. Nous y revenons à la sous-section 5.3. Pour générer la signature d'un message $\mathbf{y} \in K^m$, on peut appliquer la procédure de déchiffrement décrite précédemment. On obtient la signature $\mathbf{x} \in K^u$. Pour vérifier cette signature, n'importe qui peut évaluer **PK** en $\mathbf{x}$ et vérifier si le résultat est bien $\mathbf{y}$.

Remarquons enfin que lorsque $\mathbf{f}$ est supposée publique, ou peut se retrouver plus facilement que prévu, on peut être tenté de retrouver S et T à partir de $\mathbf{f}$ et **PK**. Ce problème, décrit dans son énoncé général à la sous-section 5.2.3, est appelé "IP" (pour Isomorphisms of Polynomials). Le problème IP est intimement lié à la cryptologie multivariée, et peut apparaître dans d'autres contextes, différents de celui mentionné, comme nous verrons au chapitre 7.

5.2 Outils mathématiques

5.2.1 Corps finis et extensions de corps fini, morphisme de Frobenius

Dans cette sous-section nous introduisons les outils mathématiques de base dont nous nous servons. Nous donnons quelques définitions et résultats concernant les corps finis. Nous définissons également le morphisme de Frobenius (définition 10). Les principales propriétés concernant ce morphisme sont rappelées. Nous donnons aussi des résultats secondaires, mais dont nous ferons usage dans la partie I.

Les résultats les plus classiques sont rappelés sans démonstration. Nous renvoyons vers la littérature pour plus de détails (par exemple [Goz97, LN96]). Les démonstrations des autres résultats sont fournies.

Définition 9 *Soit $\mathbb{K}$ un corps fini. Un corps $\mathbb{L}$ est une* extension de corps *de $\mathbb{K}$ s'il existe un morphisme de corps de $\mathbb{K}$ dans $\mathbb{L}$. Le* degré *de cette extension est la dimension de $\mathbb{L}$ comme $\mathbb{K}$-espace vectoriel.*

Remarque : Nous ne nous intéressons qu'aux extensions finies de corps, *i.e.* lorsque le degré de l'extension est fini.

Proposition 9 *Soit $\mathbb{K}$ un corps fini à q éléments, de caractéristique $p > 0$:*

i) Il existe $m \in \mathbb{N}^*$ tel que $q = p^m$.

ii) $\mathbb{K}$ est le corps de décomposition de $X^q - X$.

iii) Deux corps à q éléments sont $\mathbb{F}_p$-isomorphes.

Remarque : Par suite, tous les corps finis de même cardinal q sont isomorphes. On note $\mathbb{F}_q$ le corps à q éléments. L'équation $X^q = X$ est appelée *équation de corps* de $\mathbb{F}_q$.

Proposition 10 *Soit $\mathbb{K}$ un corps fini et $\mathbb{L}$ une extension finie de degré n de $\mathbb{K}$. Il existe un polynôme irréductible P de degré n de $\mathbb{K}[X]$, tel que :*

$$\mathbb{L} = \mathbb{K}[X]/\langle P \rangle ,$$

où $\langle P \rangle$ désigne l'idéal principal de $\mathbb{K}[X]$ engendré par P.

Soit θ une racine de P dans $\mathbb{L}$. θ engendre $\mathbb{L}$ sur $\mathbb{K}$ et $(1, \theta, \ldots, \theta^{n-1})$ est une base de $\mathbb{L}$ comme $\mathbb{K}$-espace vectoriel.

Remarque : Il existe un isomorphisme entre $\mathbb{L}$ et l'espace vectoriel $\mathbb{K}^n$. Ainsi, dans la suite nous considérons indifféremment le corps $\mathbb{L}$ ou l'espace vectoriel $\mathbb{K}^n$.

Définition 10 (Morphisme de Frobenius) *Soit $q = p^m$, avec p premier et $m \in \mathbb{N}^*$. L'automorphisme :*

$$\begin{array}{rccc} \mathcal{F} : & \mathbb{F}_q & \to & \mathbb{F}_q \\ & x & \mapsto & x^p \end{array} ,$$

est appelé morphisme de Frobenius *de $\mathbb{F}_q$.*

Proposition 11 *Gardons les notations de la définition 10. Pour* $1 \leq i \leq m$*, l'automorphisme* $\mathcal{F}^i$ *restreint à* $\mathbb{F}_{p^i}$ *est l'identité de* $\mathbb{F}_{p^i}$*.*

Démonstration : Cette assertion provient simplement des équations de corps pour $\mathbb{F}_{p^i}$. Tout élément x de $\mathbb{F}_{p^i}$ vérifie $x^{p^i} = x$. □

Théorème 2 *Soit* $\mathbb{K} = \mathbb{F}_q$ *un corps de caractéristique* p *(*$q = p^m$*,* $m \geq 1$*), et* $\mathbb{L}$ *une extension de* $\mathbb{K}$ *de degré* $n \geq 1$*. Le groupe des automorphismes* $\mathbb{K}$*-linéaires de* $\mathbb{L}$ *est d'ordre* n*, engendré par* $\mathcal{F}^m : x \mapsto x^q$*, encore noté Fr .*

Enfin, énonçons un dernier théorème, bien utile lors de l'étude des corps finis. Comme annoncé au début de cette section, les démonstrations de ce résultat ainsi que des précédents peuvent être trouvées dans des livres d'algèbre classiques, par exemple ceux déjà cités [LN96, Goz97].

Théorème 3 (Existence d'une base normale) *Soit* $\mathbb{L}$ *est une extension de degré* n *du corps fini* $\mathbb{K} = \mathbb{F}_q$*. Il existe* $\theta \in \mathbb{L}$ *tel que* $(\theta, \theta^q, \theta^{q^2}, \ldots, \theta^{q^{n-1}})$ *soit une base du* $\mathbb{K}$*-espace vectoriel* $\mathbb{L}$*. Une telle base est appelée* base normale*.*

Passons maintenant aux résultats plus spécifiques dont nous allons également avoir besoin.

Proposition 12 *Soit* $\mathbb{K} = \mathbb{F}_q$*,* $\mathbb{L} = \mathbb{F}_{q^n}$ *et* $M \in \mathcal{M}_n(\mathbb{K})$*. Supposons fixée une base de* $\mathbb{L}$*. Par la correspondance entre* $\mathbb{L}$ *et* $\mathbb{K}^n$*,* M *est un endomorphisme* $\mathbb{K}$*-linéaire de* $\mathbb{L}$*. Il existe* $P \in \mathbb{L}[X]$ *de la forme :*

$$P(X) = \lambda_1 X + \lambda_2 X^q + \ldots + \lambda_n X^{q^{n-1}},$$

tel que P *corresponde à* M *sur* $\mathbb{L}$*. On dit que* P *est la* représentation polynomiale *de* M *sur* $\mathbb{L}$*.*

Explication : Ceci est un corollaire du théorème 2. Donnons tout de même quelques explications.
Supposons fixée une base normale $(\theta, \theta^q, \ldots, \theta^{q^{n-1}})$ de $\mathbb{L}$ (ce choix n'est pas nécessaire mais simplifie l'exposé qui suit). Soit $X \in \mathbb{L}[X]$, que l'on écrit $X = x_1\theta + x_2\theta^{q^2} + \ldots + x_n\theta^{q^{n-1}}$, où $x_1, \ldots, x_n$ sont les indéterminées de l'anneau $\mathbb{K}[x_1, \ldots, x_n]$. On suppose que ces x_i vérifient les équations de corps de $\mathbb{K}$: $x_i^q = x_i$. Pour $1 \leq i \leq n-1$, chaque monôme X^{q^i} fait intervenir les indéterminées x_i de manière linéaire :

$$\begin{cases} X & = & x_1\theta + \ldots + x_n\theta^{q^{n-1}}, \\ X^q & = & x_n\theta + \ldots + x_{n-1}\theta^{q^{n-1}}, \\ & \vdots & \\ X^{q^{n-1}} & = & x_2\theta + \ldots + x_1\theta^{q^{n-1}}. \end{cases}$$

Autrement dit, on peut définir une matrice inversible $M_{\mathbb{L}} \in \mathcal{M}_n(\mathbb{L})$, telle que :

$$M_{\mathbb{L}} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} X \\ \vdots \\ X^{q^{n-1}} \end{pmatrix}.$$

Soit M une matrice de $\mathcal{M}_n(\mathbb{K})$. On a alors :

$$M \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = M \cdot M_{\mathbb{L}}^{-1} \cdot \begin{pmatrix} X \\ \vdots \\ X^{q^{n-1}} \end{pmatrix},$$

ce qui permet de déterminer le polynôme P représentant la matrice M sur $\mathbb{L}$.

Proposition 13 *Soit $\mathbb{K} = \mathbb{F}_q$ et $Fr : X \mapsto X^q$. L'ensemble des matrices de $\mathcal{M}_n(\mathbb{K})$ commutant avec Fr est le $\mathbb{K}$- espace vectoriel de dimension n engendré par $\left(Fr^{\,0}, Fr, \ldots, Fr^{\,n-1}\right)$.*

Démonstration : Soit M une matrice telle que $M \circ Fr = Fr \circ M$. Soit P la représentation polynomiale de M sur $\mathbb{L} = \mathbb{F}_{q^n}$, $P(X) = \sum_{i=0}^{n-1} \lambda_i X^{q^i}$. L'égalité $M \circ Fr = Fr \circ M$ équivaut à $P^q(X) = P(X^q)$. Nécessairement, on a alors $\forall i$, $\lambda_i \in \mathbb{K}$. Ceci s'écrit encore $P = \sum_{i=0}^{n-1} \lambda_i Fr^{\,i}$, comme annoncé. □

Corollaire 1 *Soit $M \in \mathrm{GL}_n(\mathbb{K})$ une matrice inversible. Si sa représentation polynomiale sur $\mathbb{L}$ est à coefficients dans $\mathbb{K}$, alors son inverse M^{-1} a une représentation polynomiale à coefficients dans $\mathbb{K}$ également.*

Démonstration : Par la proposition 13, une matrice de $\mathcal{M}_n(\mathbb{K})$ a une représentation polynomiale à coefficients dans $\mathbb{K}$ si et seulement si elle commute avec $Fr : x \mapsto x^q$. Or M commute avec Fr si et seulement si son inverse M^{-1} commute avec Fr. □

5.2.2 Les bases de Gröbner

En cryptologie, nous sommes fréquemment confrontés au problème de résoudre un système d'équations polynomiales en plusieurs variables. En particulier, dans le cadre de la cryptologie multivariée ce problème apparaît naturellement, tant du côté cryptographie (conception de schémas) que du côté cryptanalyse (attaque de schémas), comme l'illustre le problème MQ exposé à la sous-section 5.1. Un outil très performant pour la résolution de systèmes d'équations multivariées est l'utilisation de bases de Gröbner. Son implication dans les attaques a déjà permis la cryptanalyse de beaucoup de schémas, auparavant sortis indemnes d'autres tentatives d'attaque. Un exemple mémorable est la cryptanalyse algébrique de HFE [FJ03a], qui permit

de casser le premier challenge HFE de [Pat96] sept années après sa publication. Détaillons le principe du calcul des bases de Gröbner.

La théorie des bases de Gröbner se rapporte initialement à la branche de l'algèbre commutative et concerne les anneaux de polynômes en plusieurs indéterminées sur un corps commutatif. Ces bases de Gröbner ont été introduites par Buchberger en 1965 [Buc65]. Étant donné K un corps commutatif et $K[x_1, \ldots, x_n]$ l'anneaux des polynômes de K en n indéterminées. Calculer une base de Gröbner d'un idéal I de $K[x_1, \ldots, x_n]$ consiste à transformer le système de générateurs de I en un système de générateurs particulier, présentant de "bonnes propriétés", dans un sens que nous allons détailler. Ces base de Gröbner sont parfois encore appelées "bases standards", qui sont l'analogue des bases de Gröbner pour les anneaux locaux [Hir64]. Comme pour la sous-section 5.2.1, nous énonçons les principaux résultats et définitions dont nous avons besoin, sans démonstration. Nous renvoyons pour toute cette sous-section à [CLO07] ou [Jou09].

5.2.2.1 Idéal monomial, Idéal polynomial

Afin de comprendre le principe du calcul de bases de Gröbner d'un idéal I de $K[x_1, \ldots, x_n]$, plaçons-nous d'abord dans le cas monomial. Soit I_{m} un idéal monomial de $K[x_1, \ldots, x_n]$:

$$I_{\mathrm{m}} = \langle m_1, \ldots, m_r \rangle$$

Dans le cas monomial, il est facile de décider si un polynôme $\mathrm{f} \in K[x_1, \ldots, x_n]$ appartient à I_{m} : $\mathrm{f} \in I$ si et seulement si tous les monômes intervenant dans f sont divisibles par un des générateurs m_i, $1 \leq i \leq r$, de I_{m}. Dans le cas général d'un idéal polynomial, un critère similaire n'existe pas.

Par ailleurs, lorsque l'on s'intéresse à la résolution d'un système d'équations polynomiales en n variables :

$$\begin{cases} \mathrm{f}_1(x_1, \ldots, x_n) &= 0 \\ \qquad \vdots & \\ \mathrm{f}_m(x_1, \ldots, x_n) &= 0, \end{cases}$$

on veut trouver $(z_1, \ldots, z_n)$, tel que tous les polynômes du système s'annulent en $(z_1, \ldots, z_n)$. Soit $I = \langle \mathrm{f}_1, \ldots, \mathrm{f}_m \rangle$ l'idéal de $K[x_1, \ldots, x_n]$ engendré par ces polynômes. Dans ce contexte, on est naturellement amenés à s'intéresser à l'intersection de I avec les anneaux $K[x_{i_1}, \ldots, x_n]$, pour $1 \leq i_1 \leq n$. Autrement dit, on s'intéresse aux polynômes de I ne dépendant pas des premières variables [2]. Dans le cas monomial toujours, $I_{\mathrm{m}} \cap K[x_{i_1}, \ldots, x_n]$ est engendré par les monômes m_i, $1 \leq i \leq r$, appartenant à $K[x_{i_1}, \ldots, x_n]$. Dans le cas polynomial, ceci n'est pas vrai pour un système de générateurs quelconque.

2. Par exemple, dans le cas d'un système d'équations polynomiales "échelonné", on peut se ramener à résoudre, successivement (et en intégrant le résultat obtenu), un système de polynômes en la variable x_n, puis un système de polynômes en la variable x_{n-1}, etc.

Les bases de Gröbner apportent une solution dans le cas général d'idéaux polynomiaux aux limitations illustrées par les deux exemples précédents. Pour détailler ce concept, introduisons la notion d'ordre monomial.

5.2.2.2 Ordre Monomial

Définition 11 (Ordre monomial) *Un* ordre monomial $>$ *sur* $K[x_1, \ldots, x_n]$ *est un ordre total sur l'ensemble des monômes de* $K[x_1, \ldots, x_n]$*, tel que :*

$$\forall m \neq 1, m_1, m_2 \, : \, m_1 > m_2 \Rightarrow m \cdot m_1 > m \cdot m_2 > m_2. \tag{5.1}$$

*On parle encore d'*ordre admissible.

Remarque : De l'équation (5.1) de la définition 11, remarquons que l'on a en particulier :

$$\forall m_1, m \neq 1, \; m \cdot m_1 > m_1, \tag{5.2}$$

qui implique que 1 est le plus petit monôme (cas $m_1 = 1$ dans l'équation (5.2)).

Donnons deux exemples d'ordres monomiaux. Ces exemples sont les ordres monomiaux les plus classiques et sont aussi ceux qui nous intéresseront dans la suite.
Exemple : Soit $\alpha = (\alpha_1, \ldots \alpha_n)$. Pour alléger les notations, nous notons X^α pour le monôme $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

1. Un premier exemple d'ordre est l'ordre lexicographique $\overset{\mathsf{lex}}{>}$, encore appelé lex. Soient $m_1 = X^\alpha$ et $m_2 = X^\beta$.

$$\begin{aligned} & m_1 \overset{\mathsf{lex}}{>} m_2 \\ \iff \quad & \exists 1 \leq i_0 \leq n \, : \, \forall i = 1, \ldots, i_0 - 1, \; \alpha_i = \beta_i, \text{ et } \alpha_{i_0} > \; \beta_{i_0}. \end{aligned}$$

2. Un deuxième exemple d'ordre monomial est l'ordre lexicographique inverse du degré $\overset{\mathsf{DRL}}{>}$, appelé degrevlex dans la littérature française (grevlex dans la littérature anglophone pour "graded reverse lexicographic (ordering)"). Soient $m_1 = X^\alpha$ et $m_2 = X^\beta$.

$$\begin{aligned} & m_1 \overset{\mathsf{DRL}}{>} m_2 \\ \iff \quad & \begin{cases} \deg(m_1) > \deg(m_2), \text{ ou} \\ \deg(m_1) = \deg(m_2) \text{ et } \exists n \geq i_0 \geq 1 \, : \, \forall i = n, \ldots, i_0 + 1, \\ \qquad\qquad \alpha_i = \beta_i, \text{ et } \alpha_{i_0} < \beta_{i_0}. \end{cases} \end{aligned}$$

Remarque :

1. Un ordre comme degrevlex, où deux monômes sont d'abord comparés selon leur degré, est appelé "ordre du degré".
2. Sans rentrer dans les détails, l'introduction d'un ordre monomial sur $K[x_1, \ldots, x_n]$ permet de définir un algorithme de "division euclidienne" sur $K[x_1, \ldots, x_n]$, d'un polynôme f par une suite de polynômes $(\mathrm{f}_1, \ldots, \mathrm{f}_m)$,

par exemple l'algorithme de Hironaka, qui peut se trouver entre autres dans [CLO07]. Nous admettons ici l'existence d'un tel algorithme et notons :

$$\mathrm{f}\,\mathcal{R}\,(\mathrm{f}_1,\ldots,\mathrm{f}_m),$$

le reste de la division de f par $(\mathrm{f}_1,\ldots,\mathrm{f}_m)$. Notons que l'on a :

$$\mathrm{f}\,\mathcal{R}\,(\mathrm{f}_1,\ldots,\mathrm{f}_m)=0 \Rightarrow \mathrm{f}\in\langle \mathrm{f}_1,\ldots,\mathrm{f}_m\rangle.$$

Cependant, la réciproque est fausse. Néanmoins, ceci apporte un premier élément de réponse au problème exposé au paragraphe 5.2.2.1, de savoir si un polynôme appartient ou non à un idéal.

Enfin, pour introduire les bases de Gröbner, donnons la définition de terme initial et d'idéal initial :

Définition 12 (Terme initial et idéal initial) *Supposons fixé un ordre monomial $>$ de $K[x_1,\ldots,x_n]$.*

1. *Soit $f\in K[x_1,\ldots,x_n]$. Le* terme initial *de f, noté $in_>(f)$ est le terme de f correspondant au plus grand monôme de f pour l'ordre $>$.*
2. *Soit I un idéal non nul de $K[x_1,\ldots,x_n]$. L'*idéal initial *de I, noté $in(I)$, est l'idéal monomial engendré par les termes initiaux de tous les polynômes de I.*

5.2.2.3 Bases de Gröbner

Avec tous ces préliminaires, nous pouvons donner la définition de base de Gröbner d'un idéal, ainsi que ses propriétés.

Définition 13 (Base de Gröbner d'un idéal) *Soit I un idéal non nul de $K[x_1,\ldots,x_n]$ et $(f_1,\ldots,f_m)$ des polynômes de I. On dit que $(f_1,\ldots,f_m)$ est une base de Gröbner de I si :*

1. *$I=\langle f_1,\ldots,f_m\rangle$,*
2. *$in(I)=\langle in(f_1),\ldots,in(f_m)\rangle$.*

Remarque : Dans la définition 13, on a en fait que 2. implique 1., de sorte que 2. suffit à définir une base de Gröbner.

Notons qu'il existe toujours une base de Gröbner d'un idéal. Voyons que ces bases de Gröbner permettent de répondre aux limitations des idéaux de polynômes par rapport aux idéaux monomiaux exposées dans la sous-section 5.2.2.1.

Théorème 4 *Nous avons les deux résultats suivants :*

1. *Soit $(f_1,\ldots,f_m)$ une base de Gröbner d'un idéal I non nul de $K[x_1,\ldots,x_n]$.*

$$f\in I \Leftrightarrow f\,\mathcal{R}\,(f_1,\ldots,f_m)=0.$$

2. *Soit* $(f_1, \ldots, f_m)$ *une base de Gröbner* pour l'ordre lex *d'un idéal* I *non nul de* $K[x_1, \ldots, x_n]$. *Soit* $1 \leq i_1 \leq n$. *Alors :*
   - *Si* $\forall i = 1, \ldots, m$, $f_i \notin K[x_{i_1}, \ldots, x_n]$, *alors* $I \cap K[x_{i_1}, \ldots, x_n] = \emptyset$.
   - *Sinon, une base de Gröbner de l'idéal* $I \cap K[x_{i_1}, \ldots, x_n] \subset K[x_{i_1}, \ldots, x_n]$, *pour l'ordre* lex *est composée des* $f_i\, 1 \leq i \leq m$, *appartenant à* $K[x_{i_1}, \ldots, x_n]$.

Autrement dit, les base de Gröbner permettent d'obtenir des situations similaires au cas des idéaux monomiaux.

5.2.2.4 Applications du calcul de bases de Gröbner à la résolution d'un système de polynômes multivariés

Nous nous focalisons sur les systèmes d'équations algébriques de dimension 0, *i.e.* ceux ayant un nombre fini de solutions dans la clôture algébrique du corps considérée[3] :

$$\begin{cases} \mathrm{f}_1(x_1, \ldots, x_n) &= 0 \\ \qquad \vdots & \\ \mathrm{f}_m(x_1, \ldots, x_n) &= 0. \end{cases}$$

Dans ce cas, une base de Gröbner B de l'idéal $I = \langle \mathrm{f}_1, \ldots, \mathrm{f}_m \rangle$ pour l'ordre lex vérifie :

$$\forall 1 \leq i_1 \leq n,\ \{\mathrm{f} \in B \cap K[x_{i_1}, \ldots, x_n]\} \neq \emptyset,$$

autrement dit, pour tout $1 \leq i_1 \leq n$, il existe au moins un polynôme de la base de Gröbner pour lex de I ne dépendant que des variables $x_{i_1}, \ldots, x_n$.

Lorsqu'une telle base B est établie, trouver une solution $(z_1, \ldots, z_n)$ au système d'équations précédent devient facile. On commence par considérer les polynômes de la base de Gröbner appartenant à $K[x_n]$ et l'on résout ce système d'équations. Puis pour chaque solution z_n trouvée, on remplace x_n par z_n dans les autres polynômes de la base et l'on continue le processus. À chaque étape, on considère un système d'équations univariées.

Revenant à la cryptologie multivariable, une stratégie d'attaque (ou une précaution lors de la conception) consiste à résoudre directement le système d'équations donné par la clé publique pour tenter d'inverser le système. Dans ce contexte, le calcul d'une base de Gröbner pour lex se révèle être souvent une bonne option.

Notons enfin que le nombre de solutions d'un tel système d'équations peut être de l'ordre de $\exp n \log(d)$, ou d est le plus haut degré des polynômes univariés intervenant dans le processus décrit précédemment. Ceci explique que les algorithmes de calcul de bases de Gröbner, qui sont abordés dans le paragraphe 5.2.2.5 qui suit, restent assez coûteux. En effet, leur complexité repose sur le degré des polynômes intervenant dans le calcul. Ceci est détaillé ci-dessous.

3. Notons que lorsque le système n'a pas de solution, la base de Gröbner se réduit à 1.

5.2.2.5 Algorithmes de calcul et complexités existantes

Algorithmes de calcul Le premier algorithme de calcul de bases de Gröbner est dû à Buchberger [Buc65] et date de 1965. Notons que Macaulay dans [Mac16] a développé l'idée de représenter matriciellement les idéaux de polynômes homogènes. On peut en particulier représenter matriciellement une base de Gröbner d'un idéal I. En effet, dans une matrice de Macauley, les différentes colonnes de la matrice en question correspondent à différents monômes, et chaque ligne correspond à un polynôme : le coefficient (i, j) de la matrice correspond au coefficient du j-ème monôme dans le i-ème polynôme. Réciproquement, les travaux de Lazard [Laz83] dans les années 1980 et ensuite, montrent que réaliser de l'algèbre linéaire sur des matrices de Macaulay d'un idéal I permet d'obtenir une base de Gröbner de I.

Plus récemment, des algorithmes plus performants ont été proposés. Parmi eux notamment les algorithmes F_4 et F_5 de Faugère [Fau99, Fau02]. L'algorithme F_4 se trouve être une rencontre entre l'idée de représentation matricielle de Macaulay et l'algorithme de Buchberger, où certaines décision arbitraires sont remplacées dans F_4 par des choix stratégiques. L'algorithme F_5 est l'algorithme le plus puissant connu à ce jour. En fait l'algorithme de Buchberger et l'algorithme F_4 passent beaucoup de temps à faire des divisions de polynômes [4] dont le reste est nul. Dans F_5, Faugère a intégré un nouveau critère permettant d'éviter beaucoup [5] de réductions à zéro. Notons également l'existence de l'algorithme XL présenté dans [CKPS00], où les auteurs redécouvrirent sans le savoir les bases de Gröbner.

La complexité de calcul d'une base de Gröbner d'un idéal dépend de plusieurs paramètres, comme la taille du système considéré ou encore la structure du corps. Cependant, afin de comprendre les paramètres importants pour la complexité des calculs, détaillons sommairement le principe de fonctionnement d'un algorithme de calcul de bases de Gröbner. Nous renvoyons vers les articles originaux pour un détail plus rigoureux de ces algorithmes, ou vers [Jou09] pour plus d'explication. Prenons l'exemple de l'algorithme F_5 matriciel décrit dans [Bar04], qui se rapproche dans sa description d'un algorithme F_4 intégrant le critère F_5. Plaçons nous dans le cadre de polynômes homogènes. Nous supposons fixé un ordre du degré, par exemple l'ordre degrevlex sur $K[x_1, \ldots, x_n]$, qui est l'ordre donnant généralement les meilleures complexités d'exécution.

En résumé, l'idée est de générer de nouveaux polynômes à partir des polynômes de départ $(f_1, \ldots, f_m)$, générateurs de l'idéal I considéré. De plus, on génère des polynômes de degré croissant avec la progression de l'algorithme. Plus précisément, supposons que l'on ait $f_1 \leq f_2 \leq \ldots \leq f_m$, pour l'ordre degrevlex considéré. On commence par considérer parmi ces polynômes, ceux de même degré petit $d_0 : (f_1, \ldots, f_k)$. Ces polynômes sont réduits selon le principe de la division [6] : f_i est divisé par la suite de polynômes $(f_1, \ldots, f_{i-1})$. Notons que des critères permettent d'éviter de considé-

4. Voir le paragraphe 5.2.2.2.
5. Toutes, sous certaines hypothèses de régularité du système (voir [Bar04]).
6. Paragraphe 5.2.2.2.

rer certains polynômes ou certaines réductions inutiles[7]. Les polynômes obtenus après réductions forment la base courante B :

$$B = (\mathrm{g}_1, \ldots, \mathrm{g}_{i_{d_0}}).$$

L'algorithme fonctionne par récurrence sur le degré d des polynômes considérés et est incrémental en m. Ainsi, nous numérotons les étapes en fonction du degré des polynômes intervenant à cette étape. Dans notre cas, cette première étape décrite est l'étape d_0.
Supposons à présent terminée une certaine étape $d \geq d_0$ de l'algorithme. La base courante à ce stade est :

$$B = (\mathrm{g}_1, \ldots, \mathrm{g}_{i_d}).$$

À l'étape $d+1$, les polynômes de B sont multipliés par certains monômes bien choisis, selon les critères invoqués plus haut, et de telle sorte que les polynômes résultants soient de degré $d+1$. Par ailleurs, nous prenons en plus en compte les polynômes f_i de degré $d+1$ du système de départ (non encore pris en compte). Tous ces polynômes de degré $d+1$ sont ordonnés et l'on procède à des réductions, comme à l'étape d_0. Plus précisément, pour chaque tel polynôme, on réalise une division par les polynômes le précédant dans l'ordonnancement. Ici encore, selon les critères de Faugère, certaines réductions ne sont pas à considérer. Les polynômes réduits ainsi obtenus sont ajoutés à la base courante :

$$B = (\mathrm{g}_1, \ldots, \mathrm{g}_{i_{d+1}}),$$

et l'on passe à l'étape d'après $d+2$. Finalement, l'algorithme termine lorsque tous les polynômes générés à une certaine étape peuvent se réduire à zéro, autrement dit, lorsqu'aucun nouveau polynôme ne peut être ajouté à la base courante. La base de Gröbner de I consiste alors en les polynômes de la base B à la fin de l'algorithme.

Complexités existantes Restons dans le cadre des polynômes homogènes, qui est le contexte habituel des théories d'étude des bases de Gröbner. Heuristiquement, on se rend compte que dès qu'une des réductions faite au cours de l'algorithme F5 entraîne une réduction à zéro, l'algorithme termine ensuite souvent très rapidement. Essayons de comprendre ce phénomène. Dans le cadre de l'algorithme F5, les polynômes ajoutés à la base courante au cours de l'algorithme sont choisis afin d'éviter des réductions à zéro non significatives. Ainsi, supposons que l'on obtienne une réduction à zéro à l'étape d de l'algorithme (c'est à dire, nous considérons à cette étape des polynômes de degré d). Intuitivement, ceci indique que les termes initiaux (ceux intervenant dans la division) des polynômes de la base courante à cette étape d, couvrent une grande partie des monômes de degré d. Il n'est pas totalement

7. Sans rentrer dans les détails, nous considérons en fait des "S-polynômes" ou "syzygies" : ceux sont des multiples particuliers des polynômes de départ, choisis afin d'éliminer les termes "de tête" (les plus grands pour l'ordre) de polynômes, deux à deux (cf. [CLO07] pour une définition rigoureuse). Les critères auxquels nous faisons référence sont les critères de Buchberger [Buc65], ainsi que plus récemment le critère de Faugère [Fau02].

surprenant qu'ensuite rapidement, les polynômes générés se réduisent tous à zéro, signifiant la fin de l'algorithme. Pour certains systèmes (dits réguliers, voir [Bar04]), il est montré que grâce aux critères de F5, aucune réduction à zéro ne se produit au cours de l'algorithme. L'étape à laquelle l'algorithme se termine correspond alors au degré d où devraient se produire les premières réductions à zéro.

Dans tous les cas, ceci explique l'hypothèse répandue que la complexité d'un calcul de base de Gröbner d'un idéal de polynômes multivariés dépend du degré d atteint lors de l'algorithme où se produit la première réduction à zéro. Dans le cas de polynômes non-homogènes, ceci correspond à la première chute de degré. En effet, on a coutume de ramener la complexité du calcul de base de Gröbner d'un système non-homogène à celui du système formé par les composantes homogènes de plus haut degré de ces polynômes. Dans le cas de systèmes réguliers (ou semi-réguliers pour des polynômes non-homogènes), nous avons déjà mentionné que cette hypothèse se justifie et ce degré d coïncide avec la notion de "degré de régularité" d'un ensemble de polynômes, définie ci-dessous :

Définition 14 (degré de régularité) *Soit $(f_1, \ldots, f_m)$ un ensemble de polynômes homogènes de $K[x_1, \ldots, x_n]$ et $I = \langle f_1, \ldots, f_m \rangle$. Le* degré de régularité *de $(f_1, \ldots, f_m)$, $\mathrm{D_{reg}}$, est le plus petit entier $d \geq 0$, tel que les polynômes de degré d de I engendrent comme K-espace vectoriel, l'ensemble des monômes de degré d en n variables (au nombre de $\binom{n+d-1}{d}$) sans prendre en compte les équations de corps) :*

$$\mathrm{D_{reg}} = \min \left\{ d \geq 0 \,:\, \dim_K \left(\{ f \in I \,:\, \deg(f) = d \} \right) = \binom{n+d-1}{d} \right\}.$$

Pour un ensemble $(f_1, \ldots, f_m)$ non-homogène de polynômes, le degré de régularité *est défini comme le degré de régularité des composantes homogènes de plus haut degré de $(f_1, \ldots, f_m)$.*

Remarque : Dans cette thèse et les travaux [BFJT09, FJPT10], nous nous sommes parfois placés sous l'hypothèse courante que le degré de régularité correspond en pratique au degré auquel survient la première chute de degré dans les algorithmes de Faugère. Comme déjà mentionné, hormis pour le cas de systèmes réguliers ou semi-réguliers et le cas de l'algorithme F5, ceci n'est pas justifié théoriquement. Cependant, afin d'expliquer ce choix, remarquons que ces systèmes réguliers ou semi réguliers correspondent en quelque sorte au cas aléatoire, où les polynômes sont le moins "liés entre eux". (Encore une fois, nous renvoyons à [Bar04] pour une définition rigoureuse.) Par ailleurs, il est démontré que la proportion de systèmes semi-réguliers tend vers 1 lorsque n tend vers l'infini.

Proposition 14 (Complexité de calculs de base de Gröbner) *Avec cette définition la complexité d'un calcul de base de Gröbner est :*

$$\mathcal{O}\left(n^{\omega \mathrm{D_{reg}}}\right),$$

où $2 < \omega \leq 3$ est la "constante de l'algèbre linéaire" ([Bar04, BFSY05]), et n le nombre de variables du système.

Explication : Cette complexité correspond simplement à la réduction d'un matrice de taille $n^{\mathrm{D_{reg}}}$. En effet, l'algorithme décrit plus haut peut se voir comme une suite de réductions particulières de matrices de Macaulay de taille de plus en plus grosse. Selon ce qui précède, la taille de la matrice la plus grosse à considérer correspond au nombre de monômes de degré $\mathrm{D_{reg}}$ en n variables, soit :

$$\binom{\mathrm{D_{reg}}+n-1}{\mathrm{D_{reg}}} \simeq n^{\mathrm{D_{reg}}}.$$

Revenons au degré de régularité. Nous avons la propriété suivante :

Proposition 15 (Invariance du degré de régularité) *Le degré de régularité d'un système de polynômes reste inchangé par changement linéaire ou affine inversible des coordonnées ou des générateurs.*

Pour des systèmes réguliers ou semi-réguliers, notons le théorème suivant dû à Bardet concernant l'évolution asymptotique du degré de régularité [Bar04, BFSY05] :

Théorème 5 (Évolution asymptotique du degré de régularité) *Soit $\alpha > 1$, α entier fixé.*

1. *Lorsque n tend vers l'infini, le degré de régularité d'un système de αn équations quadratiques en n inconnues est majoré par :*

$$n\left(\alpha - \frac{1}{2} - \sqrt{\alpha(\alpha-1)}\right) - \frac{a_1}{2(\alpha(\alpha-1))^{\frac{1}{6}}} n^{\frac{1}{3}} - \left(2 - \frac{2\alpha-1}{4\sqrt{\alpha(\alpha-1)}}\right) + \mathcal{O}\left(1/n^{1/3}\right), \tag{5.3}$$

   où $a_1 \simeq -2,33811$.

2. *Le degré de régularité d'un système de αn équations quadratiques sur $\mathbb{F}_2$ en n inconnues (les équations de corps sont implicitement prises en compte mais sont pas comptées dans α) est équivalent en $+\infty$, à :*

$$\left(-\alpha + \frac{1}{2} + \frac{1}{2}\sqrt{2\alpha^2 - 10\alpha - 1 + 2(\alpha+2)\sqrt{\alpha(\alpha+2)}}\right) n. \tag{5.4}$$

Remarque : Nous n'avons donné ici que les complexités de calcul de bases de Gröbner. Nous avons par ailleurs mentionné que les meilleures complexités de calcul sont généralement observées avec l'ordre degrevlex. Cependant, dans les applications des chapitres 6 et 7 qui suivent, nous utilisons le calcul de bases de Gröbner pour résoudre des systèmes d'équations. Nous avons vu que dans ce contexte d'application, c'est une base de Gröbner pour l'ordre lex qu'il vaut mieux calculer (voir paragraphe 5.2.2.4).
La meilleure stratégie pour obtenir une base de Gröbner pour lex reste en général de calculer une base de Gröbner pour degrevlex, puis d'utiliser un algorithme de "changement d'ordre", par exemple FGLM [FGLm93], pour se ramener à une base

de Gröbner pour lex. Dans nos applications, c'est cette stratégie qui est appliquée. L'algorithme FGLM est très efficace. Pour cette raison, lors de l'évaluation de la complexité de résolution de systèmes d'équations, nous considérons en général uniquement la complexité du calcul d'une base de Gröbner pour degrevlex.

5.2.3 Le problème "IP" (Isomorphisms of Polynomials)

Le problème IP est un problème introduit dans [Pat96]. Il s'énonce comme suit.

Le problème IP :
DONNÉE : Deux systèmes $\mathbf{A}$ et $\mathbf{B}$ de m polynômes sur un corps fini K en u inconnues.
PROBLÈME : Trouver $U_L \in \mathrm{GL}_u(K)$, $V_L \in \mathrm{GL}_m(K)$, ainsi que deux vecteurs $U_c \in K^u$ et $V_c \in K^m$, tels que :

$$\mathbf{B}(x) = V_L(\mathbf{A}(U_L \cdot x + U_c)) + V_c \tag{5.5}$$

Ce problème consiste à trouver deux application affines inversibles transformant un de ces ensembles d'équations en l'autre. Certains schémas multivariés reposent en plus sur la difficulté de ce problème, comme par exemple C*, décrit à la section 5.3. Par contre, la sécurité de HFE ne repose a priori pas sur IP, car à la différence de C*, $\mathbf{f}$ ne peut être supposé public. Ainsi, nous n'avons pas les deux systèmes d'équations de l'énoncé du problème IP et ne pouvons pas essayer de retrouver S et T de la sorte. Ce problème IP est cependant très lié à la cryptologie multivariée et peut apparaître dans des situations plus subtiles. Par exemple, dans l'attaque sur HFE [BFJT09], la complexité de recouvrement de la clé secrète pour l'instance considérée repose sur la résolution d'une instance d'IP, bien que la sécurité de HFE ne repose généralement pas sur ce problème.

Revenant à IP, nous présentons rapidement les techniques existantes de résolution de ce problème, comme il apparaîtra naturellement dans le chapitre 7. Remarquons déjà que pour le cas particulier d'instances issues de C*, il exite un algorithme polynomial, présenté dans [FMRS08].

Le premier algorithme pour IP, connu sous le nom de "To and Fro" est du à Courtois. C'est en fait une première version de cet algorithme qui porte ce nom dans [PGC98]. Cette version suppose possible l'inversion des systèmes $\mathbf{a}$ et $\mathbf{b}$ et présente une complexité exponentielle. La deuxième version, appelée "Combined power attack" dans [PGC98], mais connue sous le même nom "To and Fro", est une amélioration de la première version. Dans cette seconde version, l'idée est d'éviter une recherche exhaustive pour l'inversion de $\mathbf{a}$ et $\mathbf{b}$, et de se servir du paradoxe des anniversaire dans certaines parties de la version initiale. L'algorithme est annoncé comme fonctionnant en $\mathcal{O}\left(q^{n/2}\right)$ en calculs et en mémoire pour des instances linéaires de IP. Cependant, aucune implantation de l'algorithme n'a jamais pu confirmer cette complexité.

Plus récemment, d'autres approches ont permis de comprendre un peu mieux la complexité de ce problème et de différencier plusieurs classes de difficulté.

Dans [FP06], Faugère et Perret proposent une résolution par bases de Gröbner de ce problème. Dans leur papier, ils considèrent le cas $U_c = V_c = 0$. Notons d le degré des polynômes de l'instance. Leur idée est de voir que l'équation 5.5 :

$$\begin{aligned} & \mathbf{b}(x) = V_L(\mathbf{a}(U_L \cdot x)) \\ \Leftrightarrow \quad & V_L^{-1}(\mathbf{b}(x)) - \mathbf{a}(U_L \cdot x) = 0, \end{aligned}$$

définit m polynômes multivariés égaux au polynôme nul. On peut alors identifier tous les coefficients de ces m polynômes avec 0. Ceci fournit un certain nombre d'équations polynomiales en U et V, de degré compris entre 1 et d. Le système est largement surdéterminé et l'on peut calculer une base de Gröbner de l'idéal engendré par les polynômes de degré petit (1 et 2 est observé en pratique dans [FP06]). Il ressort de leur analyse que les instances où les applications U et V cherchées sont linéaires et les systèmes $\mathbf{a}$ et $\mathbf{b}$ aléatoires se résolvent en temps polynomial. Par contre, l'instance où $\mathbf{a}$ et $\mathbf{b}$ sont homogènes est beaucoup plus difficile. Le cas des instances affines n'est pas traité.

Un papier récent de Bouillaguet *et al.* [BFFP10] indique en fait deux classes d'instance :

A. *Les instances où U et V sont linéaires et $\mathbf{a}$ et $\mathbf{b}$ non-homogènes.* Ces instances correspondent aux instances repérées comme résolubles en temps polynomial dans [FP06]. Un nouvel algorithme est présenté dans [BFFP10], faisant baisser la complexité de résolution du problème IP pour ces instances de $\mathcal{O}(n^9)$ à $\mathcal{O}(n^6)$.

B. *Les instances où U et V sont affines* ou *les instances où U et V sont linéaires avec $\mathbf{a}$ et $\mathbf{b}$ homogènes.* Les auteurs de [BFFP10] montrent que ces deux types d'instances sont "équivalentes", dans le sens où la partie linéaire d'une solution d'une instance affine est solution de l'instance correspondant aux systèmes formés des parties homogènes de plus haut degré de $\mathbf{a}$ et $\mathbf{b}$. Réciproquement, supposons obtenue une solution à l'instance formée par les composantes homogènes de plus haut degré des deux système d'équations. Alors, notamment dans le cas de polynômes quadratiques, les deux constantes manquant pour former une solution complète de l'instance de départ se trouvent très facilement. Pour cette situation, [BFFP10] donne des algorithmes de complexité équivalente à celle de To and Fro.

5.3 Quelques exemples de schémas multivariés

La cryptologie multivariée compte plusieurs schémas qui ont marqué leur époque. Nous en énumérons quelques-uns, soit pour leur intérêt historique, soit parce que nous nous y intéresserons de plus près dans la suite.

5.3.1 C* (ou MI)

L'émergence de la cryptologie multivariée vient avec la publication en 1988 de l'algorithme C* de Matsumoto et Imai [MI88]. Pour décrire ce schéma, partons de la description du "squelette" des schémas multivariés, faite à la sous-section 5.1.

Dans C*, le corps K est le corps fini de cardinal q, noté $\mathbb{K}$. Considérons une extension [8] $\mathbb{L}$ de degré $n \geq 1$ de $\mathbb{K}$. L'application interne $\mathbf{f}$ est un monôme sur $\mathbb{L}$ de la forme : $\mathbf{f} : x \mapsto x^{1+q^\theta}$. Notons que la correspondance de $\mathbb{L}$ avec $\mathbb{K}^n$, expliquée à la sous-section 5.2.1, permet de voir $\mathbf{f}$ comme un ensemble de n équations *quadratiques* sur $\mathbb{K}$ (car l'application $x \mapsto x^q$ est $\mathbb{K}$-linéaire). Lorsque la caractéristique de $\mathbb{K}$ et $\mathbb{L}$ est 2, et que $1 + q^\theta$ est premier avec $q^n - 1$ (le cardinal du groupe des inversibles de $\mathbb{L}$), alors l'application $\mathbf{f}$ est inversible. Comme annoncé à la sous-section 5.1, la clé publique $\mathbf{PK}$ est obtenue par composition de $\mathbf{f}$ avec deux applications affines inversibles S et T. La clé secrète est composée de S, $\mathbf{f}$ et T.

Pour inverser le schéma à partir de la clé publique, un attaquant se retrouve face au problème MQ. Notons enfin que comme le nombre de possibilités pour $\mathbf{f}$ est petit, $\mathbf{f}$ peut être supposé public, de sorte que la sécurité de C* repose également sur le problème IP (voir la sous-section 5.1 pour ce point et 5.2.3 pour une description de IP et des algorithmes existants).

La clé publique de C* est inversible, de sorte que ce schéma peut facilement être utilisé à la fois en chiffrement et en signature. De plus, les calculs requis pour le déchiffrement sont moindres que dans le cas de RSA. Cependant, une attaque très efficace sur C* a été publiée en 1995 par Patarin [Pat95]. Cette attaque ne résout pas le problème MQ associé au schéma, ni le problème IP entre $\mathbf{f}$ et $\mathbf{PK}$. L'attaque se base sur la structure du monôme interne utilisé, pour générer à partir d'un certain nombre de couples clairs/chiffrés (de l'ordre de n^2), un ensemble d'équations bilinéaires en les entrées et sorties de $\mathbf{PK}$, vérifiées par *tous* les clairs/chiffrés. Par suite, lorsqu'un attaquant souhaite déchiffrer un message donné, il peut simplement utiliser le système d'équations linéaires pour retrouver le message clair correspondant.

Cette cryptanalyse signe donc la fin du schéma C* tel que conçu dans [MI88]. Cependant, des variantes de ce schéma ont été proposées par la suite, permettant d'éviter cette attaque, par exemple SFLASH ou HFE. Nous revenons sur ces schémas dans la suite.

5.3.2 HFE

HFE est une variante de C*, proposée par Patarin [Pat96] un an après sa cryptanalyse de C^*. Dans HFE, le monôme secret constituant $\mathbf{f}$ est remplacé par un polynôme plus général, toujours $\mathbb{K}$-quadratique. La propriété d'inversibilité de $\mathbf{f}$ n'est pas conservée, mais une restriction sur le degré de $\mathbf{f}$ permet de rendre sa factorisation efficace. Par ailleurs, la restriction à des corps de caractéristique 2 n'a plus lieu d'être, bien que ceci reste le contexte le plus classique. Le schéma HFE fait l'objet d'une étude plus détaillée au chapitre 7, nous renvoyons vers ce chapitre pour une description précise du schéma, ainsi que pour les attaques existantes.

Notons que des variantes du système HFE ont été décrites (voir [Pat96]). Ces variations consistent à retirer quelques équations de la clé publique (HFE$^-$), ou au

8. Cette notion est rappelée à la sous-section 5.2.1.

contraire à en ajouter (HFE^+) ; à ajouter des variables (HFEv) ou au contraire à en retirer en fixant leur valeur (HFEf).

La meilleure attaque connue sur HFE est de complexité sous-exponentielle [FJ03a, GJS06], mais certaines des variations semblent encore sûres. Cette attaque consiste à calculer une base de Gröbner de l'idéal engendré par les équations de la clé publique (voir section 5.2 pour les base de Gröbner).

5.3.3 SFLASH

SFLASH est une variante de C^* [PCG98a] s'utilisant en signature, proposée par Patarin, Goubin et Courtois et sélectionné par le projet européen NESSIE ("New European Schemes for Signature, Integrity and Encryption") en 2003 comme schéma de signature à clé publique recommandé [SFL]. L'idée simple est qu'en retirant quelques équations à l'ensemble des équations quadratiques de la clé publique d'un C^*, l'attaque de [Pat95] peut être évitée. Le principe de retirer quelques équations à la clé publique est une variante répandue en cryptologie multivariée (déjà décrite pour HFE), appelée "moins". Dans notre cas, on note C^{*-} [PCG98a].

SFLASH a été proposé en 2001 à la sélection NESSIE, pour le choix d'un algorithme de signature à clé publique recommandé. La première version de SFLASH propose, afin de réduire la taille de la clé publique de choisir les coefficients des applications secrètes S et T à coefficients dans $\mathbb{F}_2$ au lieu de $\mathbb{K}$, de sorte que toute la clé publique se trouve à coefficients dans $\mathbb{F}_2$. Cette version a cependant été attaquée par Gilbert et Minier [GM02], car la restriction suggérée invite à changer les estimations de sécurité, donc le choix des paramètres, ce que les auteurs n'avaient pas fait. La deuxième version de SFLASH, SFLASHv2 proposée, et considérée dans la suite du processus d'évaluation, ne suppose plus les coefficients des applications à valeur dans un sous-corps. Cette version a finalement été sélectionnée en 2003 par le projet NESSIE.

SFLASHv2 a été cryptanalysé en 2007 [DFSS07, DFS07, Dub07] par Dubois Fouque, Shamir et Stern. Leur attaque consiste à recouvrer astucieusement les équations manquantes de la clé publique, de manière à obtenir la clé publique d'un C^* complet. Par suite, l'attaque initiale de Patarin sur C^* s'applique. Nous revenons sur cette attaque dans le chapitre 7. Comme il est d'usage en cryptographie multivariée, on pourrait penser pouvoir réparer encore ce schéma, en supprimant plus d'équations de la clé publique que suggéré dans SFLASH. Plus précisément, l'attaque de [DFSS07] fonctionne lorsqu'un nombre limité d'équations sont retirées de la clé publique. Une manière "naturelle" de parer à cette attaque est d'en retirer plus que ce nombre limité. Cette issue semble cependant compromise par les récentes attaques de Macariot-Rat, notamment [FMR10].

5.3.4 OV et UOV

Un dernier exemple d'algorithme que nous donnons est l'algorithme OV (pour "oil and vinegar"[9]) et sa variante UOV (pour "unbalanced oil and vinegar"). UOV est l'un des seuls schémas multivariés qui n'ait pas encore été attaqué par les cryptanalyses récentes.

L'algorithme OV a été inventé par Patarin en 1997 et fonctionne en signature. La signature d'un message $\mathbf{y}$ est donnée par $n+v$ valeurs satisfaisant n équations quadratiques publiques (dans OV, nous avons $n=v$). Ces équations sont obtenues comme composition d'équations de la forme :

$$\mathbf{f}_i = \sum_{\substack{1\leq i\leq n\\ 1\leq j\leq n}} \alpha_{i,j} h_i v_j + \sum_{\substack{1\leq i\leq n\\ 1\leq j\leq n}} \beta_{i,j} v_i v_j + \sum_{1\leq i\leq n} \gamma_i h_i + \sum_{1\leq i\leq n} \delta_i v_i, \qquad (5.6)$$

avec une application affine inversible $S : K^{2n} \to K^{2n}$. Ceci correspond à la trappe du système.

Pour signer un message $\mathbf{y} \in K^{2n}$, le détenteur de la clé secrète doit calculer n valeurs h_i et n valeurs v_i vérifiant les n équations $\mathbf{f}_i = \mathbf{y}_i$ ($\mathbf{f}_i$ de la forme (5.6)). L'image par S^{-1} de ce vecteur solution de longueur $2n$ forme la signature de $\mathbf{y}$. Or, ni le système d'équations formant la clé publique, ni celui décrit ci-dessus faisant partie de la clé secrète, n'est résoluble tel quel. Cependant, on remarque que les variables h_i dans le système secret n'interviennent que linéairement. Pour résoudre le système secret, le détenteur de la clé secrète peut choisir aléatoirement n valeurs v_i. Ensuite, grâce à la particularité du système soulignée, il lui suffit de résoudre un système linéaire pour trouver les valeurs h_i telles que $S^{-1}((h_1,\ldots,h_n,v_1,\ldots,v_n))$ corresponde à une signature pour $\mathbf{y}$. Si aucune solution n'est trouvée, il peut choisir d'autres valeurs aléatoires h_i et recommencer.

Pour vérifier la signature $\mathbf{x}$ d'un message $\mathbf{y}$, il suffit d'évaluer les équations publiques en les valeurs $\mathbf{x}_i,\ 1\leq i\leq 2n$, et voir que l'on obtient bien $(y_1,\ldots,y_n)$.

Dans [KS98] est présentée une cryptanalyse de OV permettant à un attaquant de signer aussi efficacement que le détenteur de la clé secrète. Cette attaque utilise la construction même du schéma. Shamir *et al.* remarquent que le sous-espace vectoriel inconnu $\mathcal{O}_S = S^{-1}(K^n \times \{0\}^n)$ est stable par certaines applications. Cette propriété permet de retrouver $\mathcal{O}_S$. Il est alors possible pour l'attaquant de signer avec la même astuce que l'utilisateur légitime. En effet, soit $\mathcal{V}_S$ un supplémentaire de $\mathcal{O}_S$ dans K^{2n} et v un vecteur de $\mathcal{V}_S$ fixé aléatoirement par l'attaquant. Par construction de $\mathcal{O}_S$, la spécification, dans les équations de la clé publique, des variables correspondant à l'espace $\mathcal{V}_S$, réduit le système quadratique à un système linéaire en les variables restantes. Il ne reste donc plus à l'attaquant qu'à résoudre ce système de n équations linéaires en $2n-n=n$ inconnues afin de retrouver la composante de $\mathcal{O}_S$ manquante du vecteur formant la signature.

Ce schéma a été réparé en choisissant $v>n$, donnant naissance à UOV [KPG99]. À ce jour, aucune attaque particulière n'est connue sur UOV.

9. huile et vinaigre

Chapitre 6

Faiblesses du Schéma HM (Hidden Matrix)

Ce chapitre présente des propriétés remarquables du schéma HM, permettant de distinguer efficacement la clé publique de HM d'un système aléatoire d'équations, notamment sur un corps de caractéristique 2. Il est également possible de monter pour une attaque consistant à inverser le système d'équations (qui peut aussi être vue comme une autre manière de distinguer les équations d'un système aléatoire). Cette seconde attaque fonctionne pour K un corps fini quelconque. Ces résultats correspondent à [FJPT10].

La section 6.1 introduit le schéma HM, en spécifiant sa construction, ainsi que les travaux s'y rapportant. La section 6.2 présente un distingueur entre le système d'équations publiques du schéma HM et un système d'équations aléatoire de même taille. Cette attaque repose simplement sur la composition de la différentielle de la clé publique. Ensuite, dans la section 6.3, nous nous concentrons sur l'inversion du schéma. La résolution par calcul de base de Gröbner du système donné par la clé publique se trouve être faisable pour tout choix pratique de paramètres. Ceci est illustré par une série d'expériences (sous-section 6.3.2), où l'on voit que la résolution dudit système nécessite quelques centaines de secondes, pour des paramètres précédemment conseillés. Par ailleurs, nous observons que le degré de régularité est borné par trois lorsque le corps de base est $\mathbb{F}_2$ et quatre sinon. Ceci justifie que l'on puisse inverser le système en temps polynomial (voir chapitre 5, paragraphe 5.2.2.5) . Notons que la borne indiquée sur le degré de régularité n'est pas prouvée. Nous apportons cependant des éléments permettant de comprendre ce comportement atypique. Ceci est intéressant, car exception faite du système HFE [Pat96, FJ03b, GJS06] (voir aussi le chapitre 7), les attaques sur les schémas multivariés utilisant les techniques de bases de Gröbner ne s'accompagnent généralement pas d'une telle explication.

Sommaire

6.1 Le schéma HM

6.1.1 Description du schéma HM

Le schéma HM a été proposé par Patarin *et al.* en 1998 dans [PCG98a]. Il y est présenté comme remplaçant des schémas $[C]$ et $[C_n]$ de Matsumoto et Imai [IM85], dont la cryptanalyse est également exposée dans [PCG98a].

Tous ces schémas suivent la "règle" habituelle de construction des schémas cryptographiques multivariés. On part d'un système d'équations algébriques bien spécifique et facile à résoudre, constituant la "trappe" du schéma. Ensuite, pour cacher cette structure particulière, on compose ce système par des transformations inversibles. Le système résultant paraît aléatoire et constitue la clé publique, alors que la transformation constituant la trappe et les deux applications inversibles constituent la clé secrète du schéma. Ceci est détaillé au chapitre 5.

Plus précisément, dans le cas des schémas cités, les messages sont représentés par des vecteurs de taille n^2 sur un corps fini $\mathbb{K}$, généralement $\mathbb{K} = \mathbb{F}_2$. L'idée est de se ramener, grâce aux transformations secrètes inversibles à l'espace des matrices de taille n sur $\mathbb{K}$, $\mathcal{M}_n(\mathbb{K})$.

L'application interne constituant la trappe dans le cas des schémas $[C_n]$ est :

$$\begin{array}{rccc} \mathbf{f}: & \mathcal{M}_n(\mathbb{K}) & \to & \mathcal{M}_n(\mathbb{K}) \\ & X & \mapsto & X^2. \end{array}$$

Cette application est remplacée, pour le schéma HM, par l'application :

$$\begin{array}{rccc} \mathbf{f}: & \mathcal{M}_n(\mathbb{K}) & \to & \mathcal{M}_n(\mathbb{K}) \\ & X & \mapsto & X^2 + M \cdot X, \end{array}$$

où $M \in \mathcal{M}_n(\mathbb{K})$ est une matrice secrète fixée.

Enfin, la clé publique **PK** est définie par :

$$\mathbf{PK} = T \circ \mathbf{f} \circ S,$$

où $S : \mathbb{K}^{n^2} \to \mathcal{M}_n(\mathbb{K})$ et $T : \mathcal{M}_n(\mathbb{K}) \to \mathbb{K}^{n^2}$ sont deux applications affines inversibles.

Il existe un algorithme polynomial permettant au détenteur de la clé privée d'inverser le schéma efficacement. Celui-ci est basé sur des réductions de matrices de Jordan et peut se trouver dans [Gan59]. Comme d'habitude, dans la suite, $\mathbf{f}$ peut désigner à la fois l'application de $\mathcal{M}_n(\mathbb{K})$ ou le système d'équations défini par cette application sur $\mathbb{K}$.

6.1.2 Travaux précédents en rapport avec le schéma HM, quelques considérations

6.1.2.1 Attaque sur $[C_n]$ (HM avec $M = 0$)

Dans [PCG98a], Patarin *et al.* présentent une attaque sur le schéma $[C_n]$. Rappelons que $[C_n]$ correspond à un schéma HM "dégénéré", où la matrice M est nulle (voir sous-section 6.1.1 précédente). Dans ce cas, nous avons la relation suivante, valable pour tout $X \in \mathcal{M}_n(\mathbb{K})$:

$$X \cdot \mathbf{f}(X) \quad = \quad \mathbf{f}(X) \cdot X. \tag{6.1}$$

Ceci vient du fait que $\mathbf{f}(X) = X^2$ commute avec X. Soit alors $\mathbf{x} \in \mathbb{K}^{n^2}$, et $\mathbf{y} = \mathbf{PK}(\mathbf{x})$. L'égalité (6.1) précédente peut s'écrire également :

$$S(\mathbf{x}) \cdot T^{-1}(\mathbf{y}) \quad = \quad T^{-1}(\mathbf{y}) \cdot S(\mathbf{x}). \tag{6.2}$$

Les applications S et T étant méconnues de l'attaquant, l'équation (6.2) correspond pour l'attaquant à un ensemble de n^2 équations sur $\mathbb{K}$, quadratiques en $\mathbf{x}$ et $\mathbf{y}$ (connus), dont les coefficients sont inconnus :

$$\begin{cases} \sum_{i,j} a_{i,j}^{(1)} \cdot \mathbf{x}_i \mathbf{y}_j + \sum_i b_i^{(1)} \cdot \mathbf{x}_i + \sum_i c_i^{(1)} \mathbf{y}_i + d^{(1)} = 0 \\ \vdots \\ \sum_{i,j} a_{i,j}^{(n^2)} \cdot \mathbf{x}_i \mathbf{y}_j + \sum_i b_i^{(n^2)} \cdot \mathbf{x}_i + \sum_i c_i^{(n^2)} \mathbf{y}_i + d^{(n^2)} = 0. \end{cases}$$

Notons que les coefficients de ces équations sont les mêmes pour tout couple clair/chiffré. Par suite, chaque couple clair/chiffré fournit n^2 telles équations en les inconnues $a_{i,j}^{\alpha}$, b_i^{α}, c_i^{α} et d^{α}. Si l'attaquant génère assez de couples de messages clair/chiffré (de l'ordre de $(n^2)^2 + 2n^2 + 1$), il peut résoudre le système d'équations linéaires alors formé, c'est à dire trouver les coefficients $a_{i,j}^{\alpha}$, b_i^{α}, c_i^{α} et d^{α}. Pour finir, l'attaquant peut déchiffrer n'importe quel message chiffré $\mathbf{y}$, en utilisant cet ensemble d'équations, cette fois linéaires en l'inconnue $\mathbf{x}$. Cette attaque est à rapprocher de l'attaque sur le schéma C* de Patarin [Pat95].

6.1.2.2 Considérations sur HM

Afin de parer à l'attaque sur $[C_n]$, les auteurs de [PCG98a] proposent le schéma HM décrit plus haut (sous-section 6.1.1). L'ajout de la partie linéaire $M \cdot X$ à l'application $\mathbf{f}$ évite d'avoir l'égalité (6.1), car $M \cdot X$ ne commute pas avec X en général. Plus précisément, on a dans ce cas :

$$X \cdot \mathbf{f}(X) - \mathbf{f}(X) \cdot X = X \cdot M \cdot X - M \cdot X^2. \tag{6.3}$$

En raisonnant comme pour le cas $[C_n]$ précédent, cette égalité indique que tout couple clair/chiffré $(\mathbf{x}, \mathbf{y})$ vérifie un ensemble de n^2 équations quadratiques aux

coefficients inconnus :

$$\begin{cases} \sum_{i,j} a_{i,j}^{(1)} \cdot \mathbf{x}_i \mathbf{x}_j + \sum_{i,j} b_{i,j}^{(1)} \cdot \mathbf{x}_i \mathbf{y}_j + \sum_i c_i^{(1)} \cdot \mathbf{x}_i + \sum_i d_i^{(1)} \mathbf{y}_i + e^{(1)} = 0 \\ \vdots \\ \sum_{i,j} a_{i,j}^{(n^2)} \cdot \mathbf{x}_i \mathbf{x}_j + \sum_{i,j} b_{i,j}^{(n^2)} \cdot \mathbf{x}_i \mathbf{y}_j + \sum_i c_i^{(n^2)} \cdot \mathbf{x}_i + \sum_i d_i^{(n^2)} \mathbf{y}_i + e^{(n^2)} = 0. \end{cases}$$

Dans le même papier [PCG98a], Patarin *et al.* ne recommandent pas l'utilisation du schéma HM. Ils n'étaient alors pas capables d'exploiter cette propriété (même si l'attaquant retrouve les coefficients de ces équations comme pour $[C_n]$, il doit tout de même résoudre des équations quadratiques pour retrouver un clair à partir d'un chiffré), mais craignaient qu'elle puisse tout de même induire une faille dans la sécurité du schéma.

Dans [FJPT10], nous ne partons pas de cette entame d'attaque. Nous exhibons tout d'abord une propriété très spéciale de la différentielle de la clé publique. Ceci nous fournit un distingueur puissant entre un système d'équations quadratiques aléatoires et celui issu du schéma HM. Ensuite, nous montons une attaque permettant de retrouver le message clair à partir d'un chiffré, utilisant les techniques de bases de Gröbner. Le point commun de ces deux attaques est qu'elles tirent toutes deux partie de la non-commutativité des matrices. Concernant cette inversion du schéma, nous donnons quelques éléments permettant de comprendre pourquoi la résolution du système dans le cas de HM se fait plus facilement que dans le cas d'équations aléatoires. Notons que même si notre attaque ne repose pas sur la propriété de pouvoir obtenir n^2 équations quadratiques supplémentaires en générant assez de clairs/chiffrés (voir le début de ce paragraphe), l'équation (6.3) donnée précédemment est cependant à la base de nos explications. Tout ceci est détaillé dans les sous-sections qui suivent.

6.2 Mise en évidence d'un distingueur : propriété de la différentielle de HM

Rappelons que la différentielle en a d'une application f se décrit de la manière suivante :

$$\mathrm{D}\, f_a(x) = f(x+a) - f(x) - f(a) + f(0). \tag{6.4}$$

La différentielle d'un application quadratique est une application bilinéaire symétrique en a et x. Nous notons encore $\mathrm{D}\, f(x,y)$ l'application qui à y associe la différentielle de f en y, appliquée à x :

$$\begin{array}{rccl} \mathrm{D}: & \mathbb{K}^2 & \to & \mathbb{K} \\ & (x,y) & \mapsto & \mathrm{D}\, f_y(x) = \mathrm{D}\, f_x(y). \end{array}$$

6.2.1 Propriété de la différentielle de l'application interne secrète f de HM

Rappelons que l'on note $\mathbf{f}$ la fonction interne du schéma HM :

$$\mathbf{f} \ : \ X \mapsto X^2 + M \cdot X.$$

Nous nous intéressons ici à la différentielle de $\mathbf{f}$. Dans le cas de la fonction interne d'un HM, nous obtenons :

$$\mathrm{D}\,\mathbf{f}(X,Y) = X \cdot Y + Y \cdot X,$$

qui est la même différentielle que celle de la fonction $X \mapsto X^2$. En fixant X à une valeur arbitraire A_0 par exemple, on a que la différentielle de $\mathbf{f}$ en A_0 est :

$$\mathrm{D}_{A_0}\,\mathbf{f}(B) = A_0 \cdot B + B \cdot A_0.$$

Intéressons-nous maintenant à l'équation matricielle en B :

$$\mathrm{D}_{A_0}\,\mathbf{f}(B) \;=\; 0. \tag{6.5}$$

Cette équation fournit n^2 équations linéaires en les coefficients de la matrice inconnue B. Lorsque les n^2 équations sont indépendantes, un tel système admet une unique solution. Pour un système aléatoire, la dimension attendue de l'espace solution est très petite. Dans notre situation, le système (6.5) est très particulier. En effet, l'équation (6.5) peut se réécrire :

$$\begin{array}{rll} & \mathrm{D}_{A_0}\,\mathbf{f}(B) & = \; 0 \\ \Leftrightarrow & A_0 \cdot B + B \cdot A_0 & = \; 0. \end{array}$$

Le corps de base étant $\mathbb{K} = \mathbb{F}_2$, les solutions de l'équation (6.5) sont les matrices commutant avec A_0. Ceci inclut les polynômes en A_0. Pour un A_0 bien choisi (*i.e.* dont le polynôme minimal est de degré maximal n), la dimension de l'espace vectoriel des polynômes en A_0 est n. Le nombre exact de matrices linéairement indépendantes commutant avec une matrice donnée est $n_1 + 3n_2 + \ldots + (2t-1)n_t$, où $n_1, \ldots, n_t$ sont les degrés des polynômes invariants non constants. Ce nombre se situe entre n et n^2 et est proche de n dans la plupart des cas [PCG98b].

Dans tous les cas, il est possible de distinguer l'ensemble des équations déduites de (6.5) d'un ensemble aléatoire de n équations linéaires.

6.2.2 Propriété de la différentielle de la clé publique PK de HM

L'analyse précédente (sous-section 6.2.1) vaut pour la fonction interne *secrète* $\mathbf{f}$ d'un schéma HM. Cependant, nous allons voir comment cette particularité se transmet au niveau de la clé publique **PK** de HM.

Rappelons que la clé publique de HM est définie comme

$$\mathbf{PK} = T \circ \mathbf{f} \circ S.$$

La différentielle de la clé publique s'écrit alors, avec T_L désignant la composante linéaire de T :

$$\begin{array}{rcl} \mathrm{D}\,\mathbf{PK}\,(\mathbf{x},\mathbf{y}) & = & T_L\left(S\left(\mathbf{x}\right) \cdot S\left(\mathbf{y}\right) + S\left(\mathbf{y}\right) \cdot S\left(\mathbf{x}\right) + \mathbf{f}(S(0))\right) \\ & = & T_L\left(S\left(\mathbf{x}\right) \cdot S\left(\mathbf{y}\right) + S\left(\mathbf{y}\right) \cdot S\left(\mathbf{x}\right)\right) + T_L\left(\mathbf{f}\left(S(0)\right)\right), \end{array} \tag{6.6}$$

où la première égalité se produit pour $\mathbb{K}$ un corps de caractéristique 2.

Si l'on fixe un vecteur $\mathbf{x_0} \in \mathbb{K}^{n^2}$ et que l'on considère comme précédemment la différentielle de la clé publique en $\mathbf{x_0}$, on obtient :

$$\mathrm{D}_{\mathbf{x_0}} \mathbf{PK}(\mathbf{y}) \quad = \quad T_L \left(S\left(\mathbf{x_0}\right) \cdot S\left(\mathbf{y}\right) + S\left(\mathbf{y}\right) \cdot S\left(\mathbf{x_0}\right) \right) + T_L\left(S(0)\right).$$

L'étude de la différentielle pour le cas de la clé secrète nous a conduit à considérer l'équation $A_0 \cdot B + B \cdot A_0 = 0$, pour A_0 fixé. Nous souhaitons observer une propriété similaire à celle obtenue pour la clé secrète dans la partie 6.2.1 précédente. Ainsi, nous ne considérons pas l'équation $\mathrm{D}_{\mathbf{x_0}} \mathbf{PK}(\mathbf{y}) = 0$, mais cette fois :

$$\mathrm{D}_{\mathbf{x_0}} \mathbf{PK}(\mathbf{y}) = T_L\left(S(0)\right), \tag{6.7}$$

où $T_L\left(S(0)\right)$ peut être obtenu comme $\mathrm{D}\,\mathbf{PK}(0,0)$ sur $\mathbb{F}_2$ ou sur un corps de caractéristique 2 (voir l'équation (6.6), sur $\mathbb{F}_2$, nous avons $2 \cdot S(0)^2 = 0$). L'équation (6.7) se ré-écrit :

$$\begin{array}{ll} & \mathrm{D}_{\mathbf{x_0}} \mathbf{PK}(\mathbf{y}) = T_L\left(S(0)\right) \\ \Leftrightarrow & T_L\left(S\left(\mathbf{x_0}\right) \cdot S\left(\mathbf{y}\right) + S\left(\mathbf{y}\right) \cdot S\left(\mathbf{x_0}\right) \right) = 0 \\ \Leftrightarrow & S\left(\mathbf{x_0}\right) \cdot S\left(\mathbf{y}\right) + S\left(\mathbf{y}\right) \cdot S\left(\mathbf{x_0}\right) = 0. \end{array}$$

Comme S est inversible, on peut appliquer ici le même raisonnement que pour la fonction $\mathbf{f}$. L'équation matricielle (6.7) a le même nombre de solutions que l'équation (6.5).

On en déduit un distingueur efficace entre n^2 équations quadratiques aléatoires en autant d'inconnues et les équations quadratiques composant la clé publique $\mathbf{PK}$ du schéma HM.

6.3 Inversion du Schéma

La section 6.2 précédente présente une attaque permettant de distinguer la clé publique du schéma HM d'un système aléatoire d'équations, lorsque $\mathbb{K}$ est de caractéristique 2. Cependant, nous avons également monté une attaque consistant à retrouver un message clair à partir d'un message chiffré, sans restriction sur la caractéristique de $\mathbb{K}$. Le principe de l'attaque est de résoudre directement les équations quadratiques données par le chiffré $\mathbf{y}$ d'un message $\mathbf{x}$, à savoir :

$$\mathbf{PK}(X) - \mathbf{y} = 0.$$

Cette attaque utilise les algorithmes F_4, F_5 de calcul de bases de Gröbner. Comme annoncé au début de ce chapitre, l'attaque fonctionne pour des paramètres précédemment conseillés de HM. Les équations données par un tel système sont en fait plus faciles à résoudre que des systèmes de même taille, mais aléatoires. En l'occurrence, nous observons que le degré maximal des polynômes intervenant lors du calcul d'une base de Gröbner se trouve borné par 3 ou 4.

Premièrement, nous nous penchons sur le cas $M = 0$, donnant une introduction à la suite de l'analyse (paragraphe 6.3.1). Puis, la partie 6.3.2 présente nos observations

à travers les expériences que nous avons faites, pour différents paramètres. Ensuite, dans la partie 6.3.3, nous donnons quelques éléments théoriques pour expliquer ces observations. Nous nous concentrons toujours sur le cas où $\mathbb{K} = \mathbb{F}_2$, comme cela est spécifié dans [PCG98a], mais explicitons également les résultats pour $\mathbb{K}$ quelconque.

6.3.1 Illustration : Cas $M = 0$

Le cas $M = 0$, qui n'est pas un cas souhaité pour HM (ce cas correspond en fait au cas du schéma [C_n] cassé dans [PCG98a]), permet cependant d'avoir une bonne vision quant au comportement du système d'équations donné par $\mathbf{PK}(X) - \mathbf{PK}(\mathbf{x}) = 0$, pour $\mathbf{x} \in \mathbb{K}^{n^2}$.

Raisonnons tout d'abord sur l'application $\mathbf{f}$ plutôt que sur $\mathbf{PK}$. Dans le cas où $M = 0$, $\mathbf{f}(X) = X^2$. Soit B une matrice de $\mathcal{M}_n(\mathbb{K})$. Nous cherchons à résoudre le système d'équations donné par $\mathbf{f}(X) - B = 0$. Posons $\Delta = X^2 - B$, et multiplions Δ à droite et à gauche par X. Nous obtenons :

$$X \cdot \Delta = X^3 - X \cdot B = 0 \tag{6.8}$$

$$\Delta \cdot X = X^3 - B \cdot X = 0. \tag{6.9}$$

En les soustrayant, nous obtenons une nouvelle équation, à savoir $X \cdot \Delta - \Delta \cdot X = X \cdot B - B \cdot X = 0$. Cette équation fournit n^2 équations *linéaires* en les n^2 coefficients inconnus $X_{i,j}$ de la matrice X, et permet de résoudre a priori complètement le système $\Delta = 0$.

Cependant, cette astuce ne fonctionne plus pour $M \neq 0$. De plus, nous avons travaillé sur la résolution du système d'équations $\Delta = 0$, issu de la clé secrète, et non sur celui issu de la clé publique $\mathbf{PK}$ définissant l'inversion du schéma.

Dans la suite de cette section, pour générer de nouvelles équations à partir des équations de départ dans le cas général, nous utilisons des algorithmes de calcul de bases de Gröbner. En effet, ces algorithmes génèrent de nouvelles équations dans l'esprit de ce qui est fait ici pour $M = 0$, mais à un niveau supérieur. On peut se référer à la partie 5.2.2. Par exemple, imaginons que l'on applique un algorithme de calcul de bases de Gröbner sur l'idéal engendré par les polynômes de l'équation $\Delta = 0$. Les équations constituant les matrices données par les équations (6.8) et (6.9), apparaissent au cours du calcul. Comme nous avons vu, l'algorithme réduit les différents polynômes générés pendant le calcul. Par suite les polynômes de degré 1 obtenus plus haut dans l'équation $X \cdot \Delta - \Delta \cdot X = 0$, apparaissent également lors de l'exécution de l'algorithme. De plus, nous savons par la proposition 15 que le paramètre permettant de déduire la complexité d'un calcul de base de Gröbner, à savoir le degré de régularité, reste inchangé par transformations affines inversibles des coordonnées ou des équations engendrant l'idéal considéré. On déduit d'une part, que cet outil permet de résoudre aussi facilement que précédemment le système issu de la clé publique dans ce cas $M = 0$. D'autre part, il semble alors assez naturel d'utiliser les algorithmes de bases de Gröbner lorsque l'on s'intéresse au cas plus général $M \neq 0$.

La sous-section 6.3.2 suivante rapporte les résultats obtenus lors de l'exécution d'un algorithme de calcul bases de Gröbner, pour différents jeux de paramètres. Nous y verrons que le degré de régularité reste petit, même pour des paramètres élevés. La sous-section 6.3.3 fournit des éléments permettant de comprendre ce comportement atypique du degré de régularité pour les systèmes d'équations issus de la clé publique d'un schéma HM.

6.3.2 Résultats expérimentaux et observations

Nous nous intéressons à l'attaque qui consiste à recouvrer un message clair, à partir d'un chiffré donné. Soit $\mathbf{x}$ un message clair et $\mathbf{y}$ le message chiffré par HM correspondant. Tenter de retrouver $\mathbf{x}$ à partir de $\mathbf{y}$ et de la clé publique $\mathbf{PK}$ d'un schéma HM, revient à résoudre le système de n^2 équations quadratiques en n^2 variables sur $\mathbb{F}_2$ induit par la clé publique :

$$\mathbf{PK}(X) - \mathbf{y} \quad = \quad \mathbf{PK}(X) - \mathbf{PK}(\mathbf{x}) = 0. \tag{6.10}$$

La table 6.1 ci-dessous regroupe plusieurs résultats expérimentaux obtenus pour la résolution de ce système, utilisant l'algorithme F_4 disponible sous Magma (v2.15-7) [BCP97]. Ces résultats sont obtenus avec un ordinateur Xeon 4.2 Ghz disposant de 128 Go de RAM. L'attaque a été implantée avec la version 15 de Magma. Les éléments suivants sont indiqués dans cette table 6.1 :

- q : La taille du corps $\mathbb{K}$
- n^2 : Nombre de variables du système
- t : Temps total pour inverser le schéma en secondes (s.) ou heures (h.)
- Mem : Mémoire utilisée en Mega octets (Mo.) ou Giga octets (Go.)
- D_{reg} : Le degré de régularité.

q	n^2	t	Mem	D_{reg}
2	64	138 s.	1.4 Go.	3
2	81	685 s.	5.8 Go.	3
2	100	6249 s.	19 Go.	3
2	121	6 h.	56 Go.	3
2	144	26 h.	171 Go.	3
65521	25	13 s.	60 Mo.	4
65521	36	790 s.	500 Mo.	4
65521	49	2.7h.	3 Go.	4

TABLE 6.1: Résultats expérimentaux pour l'attaque consistant à recouvrer un clair à partir d'un chiffré, utilisant l'algorithme F_4 de calcul de bases de Gröbner disponible sous Magma.

De ces expériences, il ressort qu'avec les paramètres conseillés dans les papiers originaux [IM85, PCG98a, PCG98b], à savoir $n^2 \geq 64$ (on peut aujourd'hui supposer que ceci correspondrait à $n^2 \geq 80$), le système est cassé et l'attaque est même

facilement réalisable en pratique. Ceci reste vrai pour tout choix de paramètres pratiques.

D'un point de vue plus technique, nous constatons que dans tous les calculs de base de Gröbner, le degré de régularité D_{reg} ne dépasse pas 3 sur $\mathbb{F}_2$. Quand le corps de base $\mathbb{K}$ n'est pas $\mathbb{F}_2$, ce degré de régularité est borné par 3 ou 4. Ceci permet d'obtenir une attaque en temps polynomial sur le schéma HM. En effet, en se basant sur la formule de la proposition 14 de la partie 5.2.2.5, on voit que la complexité du calcul d'une base de Gröbner de l'idéal formé des polynômes de la clé publique est polynomiale en D_{reg}. Nous nous penchons dans la partie suivante sur ce comportement atypique du degré de régularité.

6.3.3 À propos du comportement du degré de régularité

Comme annoncé, nous tentons d'expliquer les observations faites sur le degré de régularité à la sous-section 6.3.2, en fournissant quelques éléments permettant d'avoir une meilleure compréhension du système d'équations donné par l'équation (6.10) de cette même sous-section. Plus précisément, nous essayons de voir pour quelle raison les degrés des polynômes apparaissant dans le calcul d'une base de Gröbner ne dépassent pas 3 dans le cas où le corps de base $\mathbb{K}$ est $\mathbb{F}_2$, et 4 sinon, menant à une inversion en temps polynomial, alors que les paramètres sont choisis de sorte qu'un système aléatoire de même taille ne soit pas résoluble.

Dans le cas précédent $M = 0$ (sous-section 6.3.1), nous avons prouvé l'apparition de nombreuses [1] équations linéaires par réduction de polynômes de degré trois. Dans le cas général $M \neq 0$, nous n'avons pas nécessairement quelque chose de similaire. Cependant, nous montrons que beaucoup d'équations quadratiques et parfois linéaires apparaissent lors de la génération de polynômes de degré 3 dans le calcul d'une base de Gröbner. Par rapport à la définition 14 du degré de régularité, on voit que plus on a d'équations quadratiques, plus on se rapproche de la forme combinatoire de cette définition.

6.3.3.1 Préliminaires

Soit $\mathbf{x}$ un vecteur de longueur n^2 sur $\mathbb{K}$. Nous étudions le système d'équations (6.10) de la sous-section 6.3.2, donné par la clé publique :

$$\mathbf{PK}(X) - \mathbf{PK}(\mathbf{x}) = 0.$$

Pour simplifier, notons qu'il est équivalent d'observer le système d'équations fournies par la transformation interne $\mathbf{f}$. En effet, le degré de régularité d'un idéal reste invariant par des changements linéaires ou affines des coordonnées ou des générateurs (proposition 15). Dans le cas de l'équation que nous considérons, nous pouvons ainsi omettre les actions de S et T et nous restreindre à considérer l'équation, pour $A \in \mathcal{M}_n(\mathbb{K})$:

$$\mathbf{f}(X) - \mathbf{f}(A) = 0. \tag{6.11}$$

1. Suffisamment pour permettre a priori de résoudre le système.

Pour parler en terme d'idéal (comme nous allons considérer des calculs de base de Gröbner), considérons l'idéal I sur $\mathbb{K}$ engendré par les équations $\mathbf{f}(X) - \mathbf{f}(A)$. Soit tout d'abord $B = \mathbf{f}(A)$, *i.e.* $B = A^2 + M \cdot A$. Introduisons aussi $\Delta \in \mathcal{M}_n(\mathbb{K})$, défini par $\Delta = X^2 + M \cdot X - B$. Alors, l'idéal I sur $\mathbb{K}$, engendré par les polynômes de l'équation $\mathbf{f}(X) - \mathbf{f}(A) = 0$, est défini par :

$$I \quad = \quad \langle \Delta_{i,j},\ 1 \leq i, j \leq n \rangle . \tag{6.12}$$

Nous allons étudier dans la suite le degré de régularité de cet idéal I, ou encore, comme dans le cas $M = 0$ de la sous-section 6.3.1, les polynômes apparaissant lors du calcul d'une base de Gröbner de cet idéal.

Dans l'algorithme décrit au paragraphe 5.2.2.5, on voit que pour le calcul d'une base de Gröbner, on construit successivement, pour d croissant, les espaces vectoriels I_d, constitués des polynômes de I de degré d et du polynôme nul. Dans le cas affine qui nous intéresse ici, à cause d'éventuelles chutes de degré qui peuvent apparaître lors du calcul, nous sommes amenés à considérer plutôt les ensembles suivants :

Définition 15 *$I_{\leq d}$ désigne l'ensemble des polynômes de l'idéal I de degré inférieur ou égal à d.*

Dans le cas de HM, plusieurs polynômes de bas degré apparaissent rapidement lors du calcul d'une base de Gröbner de l'idéal I. De plus, ils apparaissent avant la génération de polynômes de degré élevé, plus précisément lors de la génération de polynômes de degré au plus 3. Ceci explique que l'algorithme termine rapidement, comme illustré par les expériences de la sous-section 6.3.2. Ceci est développé dans ce qui suit.

6.3.3.2 Étude de l'idéal I dans le cas où la caractéristique de $\mathbb{K}$ est quelconque

Nous montrons à travers la proposition 16 suivante que beaucoup de nouveaux polynômes quadratiques sont générés lors du calcul d'une base de Gröbner de I. Ce résultat est valide quel que soit le corps fini $\mathbb{K}$ considéré. Des propriétés supplémentaires dans le cas particulier où $\mathbb{K} = \mathbb{F}_2$ sont données dans la partie 6.3.3.3.

Plus précisément, la proposition 16 montre que n^2 équations quadratiques sont obtenues à chaque nouvelle étape du calcul d'une base de Gröbner de I. De plus, ces polynômes de degré deux sont obtenus par réduction de polynômes (correspondant à des équations matricielles) de degré deux, obtenus à une étape antérieure du calcul, par la matrice X. Tous ces éléments se trouvent dans la preuve de la proposition 16.

Proposition 16 *Pour tout $k \geq 1$, il existe des matrices A_k, B_k, C_k et D_k telles que :*

$$P_k = X(M^k + A_k)X + B_k \cdot X + X \cdot C_k + D_k \in I_{\leq 3}.$$

Ce résultat est obtenu en utilisant une astuce similaire au cas $M = 0$. Nous le montrons par récurrence sur k. Le lemme qui suit prouve la proposition 16 pour $k = 1$, la preuve complète de la proposition suit le lemme.

Lemme 2 *Les n^2 équations quadratiques suivantes appartiennent à $I_{\leq 3}$:*

$$P_1 = X \cdot M \cdot X + (B + M^2)X - X \cdot B - M \cdot B \in I_{\leq 3}.$$

Démonstration : [lemme 2] Dénotons toujours par Δ l'expression $X^2 + M \cdot X - B$ (voir le paragraphe 6.3.3.1). Ré-écrivons $\Delta = 0$ comme :

$$X^2 = B - M \cdot X. \tag{6.13}$$

On voit alors deux façons d'obtenir X^3, multiplier l'équation (6.13) précédente par X à droite, ou à gauche :

$$\begin{aligned} X^3 &= X \cdot B - X \cdot M \cdot X, \\ X^3 &= B \cdot X - M \cdot X^2 \\ &= B \cdot X - M \cdot X^2 + M\Delta \\ &= B \cdot X - M\,(B - M \cdot X) \\ &= B \cdot X - M \cdot B + M^2 \cdot X \end{aligned}$$

Soustrayons maintenant ces deux équations. On obtient l'égalité :

$$\Delta \cdot X - X \cdot \Delta - M \cdot \Delta = X \cdot M \cdot X + \left(B + M^2\right) X - X \cdot B - M \cdot B \in I_{\leq 3}.$$

□

Démonstration : [proposition 16] Comme annoncé, montrons le résultat de la proposition 16 par récurrence sur k. D'après le lemme 2, les équations fournies par P_1 sont dans $I_{\leq 3}$. Nous posons donc :

$$\begin{aligned} A_1 &= 0 \\ B_1 &= B + M^2 \\ C_1 &= -B \\ D_1 &= -M \cdot B. \end{aligned}$$

Supposons la propriété vraie pour $P_k, k \geq 1$. Il vient alors :

$$\begin{aligned} -P_k \cdot X &= X(M^{k+1} + A_k \cdot M - C_k)X - X(M^k \cdot B + A_k \cdot B) \\ &\quad +(B_k \cdot M - D_k)X - B_k \cdot B \\ &= X(M^{k+1} + A_{k+1})X + B_{k+1} \cdot X + X \cdot C_{k+1} + D_{k+1} \\ &= P_{k+1}, \end{aligned}$$

avec ces notations :

$$\begin{aligned} D_{k+1} &= -B_k \cdot B \\ A_{k+1} &= A_k \cdot M - C_k \\ C_{k+1} &= -M^k \cdot B - A_k \cdot B \\ B_{k+1} &= B_k \cdot M - D_k. \end{aligned}$$

Les équations formant P_{k+1} sont dans $I_{\leq 3}$, ce qui achève de prouver la proposition. □

Dans le cas général, les observations expérimentales indiquent que l'algorithme de base de Gröbner ne génère pas de polynôme de degré plus grand que 4 pour terminer ; le degré de régularité est borné par 4. Voyons à présent que dans le cas où la caractéristique de $\mathbb{K}$ est deux, la situation est meilleure encore (du point de vue de la cryptanalyse), car des propriétés supplémentaires apparaissent.

6.3.3.3 Étude de l'idéal I dans le cas où $\mathbb{K} = \mathbb{F}_2$

Intéressons-nous donc au cas $\mathbb{K} = \mathbb{F}_2$, qui est le contexte classique. Dans ce cas, les équations quadratiques données par la proposition 16 apparaissent toujours, mais en plus, un certain nombre d'équations linéaires surgissent, dues à la caractéristique du corps $\mathbb{K}$. Ces équations sont décrites dans les propositions ci-dessous, et apparaissent lors de la génération de polynômes de degré au plus 3 dans le calcul de base de Gröbner.

Soit $D \in \mathcal{M}_n(\mathbb{K})$, une matrice de $\mathbb{K}$ de taille $n \times n$. Dans ce qui suit, $tr(D)$ représente la trace de $D \in \mathcal{M}_n(\mathbb{K})$ et C_D le polynôme caractéristique de D.

Proposition 17 *Soit $Q_0 = tr((M + I)X) - tr(B)$. Les équations composant Q_0 appartiennent à $I_{\leq 3}$.*

Démonstration : L'application tr étant une forme linéaire, et comme $X^2 + M \cdot X = B$, on déduit :

$$tr(X^2) + tr(M \cdot X) = tr(B).$$

Le résultat s'en déduit si :

$$tr(X^2) = tr(X),$$

résultat faisant l'objet du lemme 3 ci-dessous. □

Lemme 3 *$C_D(z) = C_{D^2}(z)$ et $tr(D^2) = tr(D)$.*

Démonstration : Soit $C_D(z) = (z - \lambda_1) \cdots (z - \lambda_n)$. Notons que si $\lambda \in \overline{\mathbb{K}}$ est valeur propre de D alors λ^2 est valeur propre de D^2. Ainsi, et puisque l'on est en caractéristique 2, on a :

$$\begin{aligned} C_D(z)^2 &= (z^2 + \lambda_1^2) \cdots (z^2 + \lambda_n^2) \\ &= C_{D^2}(z^2). \end{aligned} \tag{6.14}$$

Maintenant, comme $C_D(z) \in \mathbb{F}_2[z]$, on a $C_D(z)^2 = C_D(z^2)$. Cette égalité, combinée avec (6.14) implique $C_D(z^2) = C_{D^2}(z^2)$ ou encore $C_D(z) = C_{D^2}(z)$. Ceci permet déjà de prouver le premier point de la proposition.
Pour la seconde assertion du lemme, remarquons que la trace d'une application linéaire correspond au coefficient de z^{n-1} dans le polynôme caractéristique de cette

application. Comme nous venons de voir que $C_D(z) = C_{D^2}(z)$, le deuxième point du lemme s'en déduit. □

Proposition 18 *Pour tout $k \geq 1$ et avec les notations de la proposition 16, définissons*

$$Q_k = (X + B_k \cdot X + X \cdot C_k + D_k)(M^k + A_k).$$

Alors, pour tout $k \geq 1$, l'équation linéaire donnée par la trace de Q_k, $tr(Q_k)$, appartient à $I_{\leq 3}$:

$$tr((X + B_k X + X \cdot C_k + D_k)(M^k + A_k)) \in I_{\leq 3}.$$

Les Q_k se déduisent des P_k de la proposition 16, comme on peut le remarquer dans la preuve qui suit :
Démonstration : De la proposition 16, on déduit que pour tout $k \geq 1$:

$$P_k = X(M^k + A_k)X + B_k \cdot X + X \cdot C_k + D_k \in I_{\leq 3}.$$

En multipliant à droite par $M^k + A_k$, nous obtenons :

$$(X(M^k + A_k))^2 + (B_k \cdot X + X \cdot C_k + D_k)(M^k + A_k) \in I_{\leq 3}.$$

À présent, $tr((X(M^k + A_k))^2) = tr(X(M^k + A_k))$ par le lemme 3. Finalement, on obtient :

$$tr((X + B_k \cdot X + X \cdot C_k + D_k)(M^k + A_k)) \in I_{\leq 3}.$$

□

On observe experimentalement que le degré de régularité est seulement 3 dans le cas $\mathbb{K} = \mathbb{F}_2$. Ceci signifie que dans les expériences faites, ces équations linéaires décrites dans les propositions précédentes, permettent de terminer les calculs de base de Gröbner après la génération de polynômes de degré 3.

6.3.4 Résumé des observations

Nous nous sommes intéressés à la résolution à l'aide des bases de Gröbner du système d'équations donné par la clé publique d'un shcéma HM : $\mathbf{PK}(X) - \mathbf{PK}(\mathbf{x}) = 0$, pour $\mathbf{x}$ un vecteur fixé de longueur n^2 sur $\mathbb{K}$. Les observations de la sous-section 6.3.2 montrent que le degré de régularité observé, atteint lors du calcul effectif d'une base de Gröbner de l'idéal I engendré par ces équations est borné par 3 lorsque $\mathbb{K} = \mathbb{F}_2$ et 4 sinon. Dans la sous-section 6.3.1 et plus généralement dans 6.3.3, nous avons prouvé l'apparition de plusieurs équations de bas degré. Ceci est rappelé dans la table 6.2, pour les différentes situations étudiées, où l'on indique également le degré de ces équations. Les résultats de cette table ont été vérifiés expérimentalement jusqu'à $n = 14$ dans le cas $\mathbb{K} = \mathbb{F}_2$ et $n = 6$ sinon.

Cas	$M = 0$	$\mathbb{K} = \mathbb{F}_2$	$\mathbb{K} \neq \mathbb{F}_2$
Nombre d'équations quadratiques	0	$k_{\max} n^2$	$k_{\max} n^2$
Nombre d'équations linéaires	n^2	$k_{\max}$	0
Nombre total d'équations quadratiques	0	n^3	n^3
Nombre total d'équations linéaires	n^2	n	0
Degré de régularité observé D_{reg}	3	3	4

TABLE 6.2: Résumé des équations obtenues au cours d'un calcul de base de Gröbner de l'idéal engendré par les équations de la clé publique de HM

L'indice $k_{\max}$ désigne le nombre d'étapes de l'algorithme F_4 utilisant le critère F_5 [Fau02] nécessaires au calcul de $I_{\leq d}$. La valeur de $k_{\max}$ dicte parfois le nombre de polynômes de bas degré apparaissant au cours du calcul. Par exemple, les polynômes indexés par k dans les propositions 16 ou 18 précédentes sont obtenues à une étape k de l'établissement de $I_{\leq 3}$.
Remarque : On suppose que $k_{\max}$ vaut n. Ceci provient du fait que les équations obtenues à l'étape k impliquent M^k (voir propositions 16 et 18). Ainsi, au bout de n étapes, comme M^n peut s'écrire en fonction de puissances précédentes par le théorème de Cayley-Hamilton, les équations apparaissant alors peuvent éventuellement se réduire à des équations précédemment obtenues.

Dans tous les cas, le degré de régularité étant borné, on a une résolution polynomiale du système d'équation correspondant à l'inversion du schéma HM.

6.4 Conclusion

Les deux nouveaux distingueurs présentés sont très efficaces et permettent de casser le système HM. Le premier se base sur la résolution d'un système d'équations issu de la différentielle de la clé publique d'un schéma HM. Le deuxième permet d'inverser, en pratique, le système d'équations formé par la clé publique en temps polynomial. De plus, certaines explications concernant cette résolution en temps polynomial ont été apportées.

Chapitre 7

Une Famille de Clés Faibles pour le Système HFE (Hidden Field Equations)

Le système HFE, déjà cité à la sous-section 5.3.2, a été conçu par Jacques Patarin et présenté à Eurocrypt'96 [Pat96]. Il généralise le schéma C* de 1988 de Matsumoto et Imai [MI88], cryptanalysé par Patarin en 1995 [Pat95]. À la différence de ce dernier, l'application interne est un polynôme plutôt qu'un monôme. Ceci permet d'éviter l'attaque sur C* et, lorsque le degré du polynôme interne n'est pas trop grand, d'inverser tout de même efficacement le système.

HFE a longtemps été considéré comme l'un des systèmes multivariés les plus robustes. La première attaque effective n'apparaît qu'en 2003 dans [FJ03a], et est de complexité sous-exponentielle. Plusieurs autres cryptanalyses ont été publiées ensuite, détaillées dans la sous-section 7.1.3. Cependant, malgré ces attaques, HFE ne peut être considéré comme cassé. Par exemple, les estimations de [BFSY05] sur la complexité des calculs de bases de Gröbner par l'algorithme F5 [Fau02] montrent que la complexité des attaques basées sur cette technique reste élevée pour des instances générales. En particulier, HFE utilisé avec les paramètres définis par le second challenge de HFE ([Pat96]) est loin d'être menacé. Par ailleurs, les versions de HFE consistant à retirer certaines équations de la clé publique, ou ajouter des variables à ces équations (voir la sous-section 5.3.2), restent imperméables aux attaques. Un autre travail [DSW08] suggère que la complexité sous-exponentielle du calcul de bases de Gröbner pour HFE est due au choix du corps de base ($\mathbb{F}_2$), et que pour un choix de corps de base plus gros, la complexité reste exponentielle.

Dans [BFJT09], nous avons trouvé une attaque permettant de retrouver la clé privée. Cette attaque ne fonctionne que pour une famille de clés privées spéciales, qui est donc une famille de clés faibles pour HFE. Elle permet néanmoins un recouvrement efficace des secrets pour des paramètres conseillés de HFE, ce qu'aucune attaque ne permettait précédemment. Bien que retrouver la clé privée d'un système HFE ne dépende en général pas de la difficulté de résolution du problème IP [1], la sécurité de HFE se réduit entièrement à la résolution d'une instance de ce problème dans le cadre de notre attaque. Cette attaque est décrite dans ce chapitre. Notons que dans [Pat96], Patarin propose une version "sous-corps" de HFE, permettant de réduire la taille de la clé publique. Ces instances de HFE font entièrement partie

1. Nous renvoyons pour ceci vers la sous-section 5.2.3.

de notre famille de clés faibles et sont désormais à prohiber (à l'instar des versions "sous-corps" de SFLASH v1 [GM02] ou de UOV [KPG99, BWP05]).

Sommaire

7.1 Description du schéma HFE et attaques existantes

7.1.1 Description du système HFE

Considérons le corps fini $\mathbb{K}$ à q éléments. Soit $\mathbb{L}$ une extension de $\mathbb{K}$ de degré n. Nous avons vu à la section 5.2 du chapitre 5 que $\mathbb{L}$ et l'espace vectoriel $\mathbb{K}^n$ sont isomorphes [2]. Dans le cas du système HFE, la trappe consiste en l'extension $\mathbb{L}$ ainsi qu'une application polynomiale particulière $\mathbf{f}$ de $\mathbb{L}$ dans $\mathbb{L}$. L'extension $\mathbb{L}$, l'application $\mathbf{f}$, ainsi que deux applications affines inversibles S et T constituent la clé secrète du système HFE. La clé publique de HFE est constituée des n équations sur $\mathbb{K}$: $\mathbf{PK} = T \circ \mathbf{f} \circ S$.

Afin de ne pas avoir une taille de clé publique trop grande, $\mathbf{f}$ est construite de manière à ce que les équations de la clé publique soient quadratiques. Pour cela, on

2. Notons que, un isomorphisme entre $\mathbb{L}$ et $\mathbb{K}^n$ étant fixé, nous considérons indifféremment des éléments ou applications de $\mathbb{L}$ ou $\mathbb{K}^n$.

définit $\mathbf{f}$ selon le modèle suivant :

$$\mathbf{f}(X) = \sum_{\substack{0 \le i,j \le n \\ q^i + q^j \le d}} a_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \le i \le n \\ q^i \le d}} b_k X^{q^k} + c,\ a_{i,j},\ b_k,\ c \in \mathbb{K}. \qquad (7.1)$$

L'application de Frobenius $x \mapsto x^q$ étant $\mathbb{K}$-linéaire, les n équations sur $\mathbb{K}$ définies par $\mathbf{f}$ sont bien quadratiques, tout comme **PK**.

Par ailleurs, le déchiffrement demande à l'utilisateur légitime l'inversion de $\mathbf{f}$, qui peut se réaliser par le recouvrement de ses racines. Les algorithmes de factorisation sur des corps finis étant au moins quadratiques en le degré du polynôme à factoriser, le degré d de $\mathbf{f}$ doit être choisi relativement petit pour permettre une inversion efficace, par exemple de l'ordre de 2^{16}.

Pour la suite, nous introduisons la notation $d = 2 \cdot q^D$. Ainsi, plutôt que de borner $q^i + q^j$ par d dans l'équation (7.1), nous pouvons borner i et j par D.

Comme annoncé à la sous-section 5.3, notons qu'il existe des variations pour le système HFE (voir [Pat96]). Cependant, dans le présent chapitre, nous nous intéressons uniquement à la version basique de HFE.

7.1.2 Clés secrètes équivalentes et extension publique

Pour le système HFE, il existe beaucoup de clés secrètes équivalentes à une clé secrète donnée (voir [WP05a]). Rappelons que deux clés secrètes équivalentes engendrent la même clé publique.

Cette diversité de clés équivalentes permet même de supposer les bijections a priori affines S et T comme linéaires. Cette supposition revient à considérer un polynôme $\mathbf{f}$ modifié par rapport au polynôme original, mais cette modification n'atteint pas le degré du polynôme $\mathbf{f}$, ce qui permet de considérer la nouvelle clé alors formée comme une clé secrète HFE valable.

Une autre constatation est que la représentation secrète φ de l'extension $\mathbb{L}$ peut en fait être supposée publique. Ceci est déjà mentionné dans le papier original [Pat96] et de fait, dans les spécifications de l'algorithme Quartz [PCG01b], un schéma de signature de la famille HFE (utilisant les variations "moins" et v), l'extension est supposée publique. Plus précisément, supposons donnée une clé secrète HFE. Alors, pour n'importe quelle représentation de $\mathbb{L}$ sur $\mathbb{K}$, il est possible de dériver la *même* clé publique de la *même* clé secrète. Ceci revient à modifier légèrement S et T, comme le résume la proposition suivante :

Proposition 19 *Soit* $\mathbf{SK} = (T, \mathbf{f}, S, \varphi)$ *une clé secrète HFE. Pour tout choix d'isomorphisme* φ' *entre* $\mathbb{L}$ *et* $\mathbb{K}^n$*, il existe deux bijections affines* S' *et* T' *telles que* $\mathbf{SK}' = (T', \mathbf{f}, S', \varphi')$ *est équivalente à* $\mathbf{SK}$ *(i.e. génère la même clé publique).*

Démonstration : Si φ' dénote un autre isomorphisme entre $\mathbb{L}$ et $\mathbb{K}^n$, alors $\phi = \varphi' \circ \varphi^{-1}$ est une application inversible $\mathbb{K}$-linéaire telle que $\varphi' = \phi \circ \varphi$. En utilisant la correspondance φ', la composition $T' \circ \mathbf{f} \circ S'$ correspond également à

PK, avec $T' = \phi \circ T$ et $S' = S \circ \phi^{-1}$. □

Ainsi, choisir de garder la représentation de $\mathbb{L}$ sur $\mathbb{K}$ secrète, ou la rendre publique, n'a pas d'influence sur la sécurité du système HFE. Dans le cas où l'extension $\mathbb{L}$ est secrète, un attaquant peut simplement fixer une représentation arbitraire et supposer que les applications secrètes sont le polynôme original $\mathbf{f}$, accompagné de deux applications affines modifiées S' et T'.

7.1.3 Attaques existantes sur le système HFE

Plusieurs voies d'investigation ont été empruntées afin d'attaquer le système HFE. Les plus heureuses ont été celles s'intéressant à la résolution du système d'équations de la clé publique par des techniques de bases de Gröbner [FJ03a, GJS06]. D'autres sont basées sur les techniques dites de relinéarisation [KS99] ou encore sur le rang de la différentielle de la clé publique [FGS05].

Les attaques se ramènent toutes à la résolution d'un système d'équations quadratiques, et leur complexité dépend du degré d du polynôme interne. Lorsque ce degré est fixé, la complexité de ces attaques est polynomiale en le paramètre de sécurité, n. Cette situation n'est cependant pas réaliste, et l'on supposera d relié au paramètre de sécurité. Or par ailleurs, le degré d de $\mathbf{f}$ doit être choisi de sorte que les algorithmes de factorisation s'appliquent facilement. Ces algorithmes étant au moins quadratiques en le degré du polynôme, d peut être au plus polynomial en le paramètre de sécurité. Nous supposons donc d polynomial en n, et dans ce cas les attaques mentionnées ne sont plus polynomiales. Ces principales attaques sont succinctement rappelées ci-dessous.

Une attaque ayant pour but le recouvrement de la clé secrète est présentée dans [KS99]. Cette attaque transforme le problème de la cryptanalyse de HFE en un problème de résolution d'un système quadratique largement surdéterminé sur l'extension $\mathbb{L}$. La technique proposée pour la résolution de ce système est la technique de relinéarisation. La cryptanalyse correspondant à cette approche, reprise dans [Cou01], est annoncée avoir une complexité polynomiale, mais se trouve impraticable pour des paramètres raisonnables. En effet dans leur analyse, les auteurs de [KS99] ou [Cou01] supposent le degré d du polynôme $\mathbf{f}$ fixe, indépendant du paramètre de sécurité. Nous avons déjà vu que ceci n'est pas un modèle réaliste, et que d doit être supposé polynomial en n. L'attaque est alors sous-exponentielle, avec une complexité l'ordre de $\exp\left(\log^3 n\right)$, ce qui est trop élevé pour être une menace pour HFE utilisé avec les paramètres conseillés.

En 2003, Faugère et Joux ont montré expérimentalement que les équations de **PK** ne peuvent être considérées comme un système aléatoire d'équations quadratiques [FJ03a]. Le calcul d'une base de Gröbner du système d'équations issu de **PK** est en fait plus facile à réaliser que dans le cas d'équations aléatoires. Ces résultats ont été obtenus en utilisant l'algorithme F5 [Fau02] de Faugère et ont permis de casser le système HFE pour des paramètres constituant le premier challenge HFE [Pat96] (80 équations en 80 inconnues sur $\mathbb{K} = \mathbb{F}_2$).

Suite à l'article [FJ03a], Granboulan *et al.* [GJS06] exhibèrent des propriétés spécifiques pour HFE, permettant de prouver la complexité de l'inversion du système HFE sous-exponentielle, de complexité $\mathcal{O}\left(\exp\left(\log^2 n\right)\right)$. Plus exactement, on peut montrer que du système d'équations fourni par la clé publique **PK**, on peut se ramener par des transformations inversibles impliquant les coordonnées à un système beaucoup plus petit. Ceci est dû à la borne sur le degré d du polynôme interne $\mathbf{f}$. Or, le degré de régularité d'un système d'équations reste inchangé par changement inversible, linéaire ou affine de coordonnées ou de générateurs. Comme le degré de régularité régit la complexité de calcul d'une base de Gröbner, ceci permet d'expliquer les résultats de [FJ03a].

Enfin, une dernière approche consiste à s'intéresser au rang de la différentielle de la clé publique. Dans [FGS05], Fouque *et al.* étudient ce rang pour extraire de l'information sur la structure interne du schéma, ce qui leur permet par exemple de cryptanalyser le schéma PMI (perturbated Matsumoto-Imai). Dans [DGF06], Dubois *et al.* reprennent cette approche différentielle et obtiennent un distingueur quasipolynomial pour HFE. La complexité de cette attaque par distingueur est cependant la même que la complexité du distingueur décrite dans [GJS06], qui de plus est basée sur le déchiffrement du système.

Notons que les attaques ayant fonctionné en pratique sont celles consistant à inverser le système, ou encore les attaques par distingueur. Aucune attaque pratique n'a jamais permis de retrouver la clé privée d'un schéma HFE.

7.2 Nouvelle famille de clés faibles pour HFE

Afin de mettre en évidence notre famille de clés faibles pour HFE, intéressons-nous d'abord au "cas C^*". Dans C*, nous avons vu à la sous-section 5.3.1 que $\mathbb{K}$ et $\mathbb{L}$ sont de caractéristique 2 et $\mathbf{f}(x) = x^{1+q^\theta}$ est inversible. Ici, considérons $\mathbb{K}$ et $\mathbb{L}$ sans restriction sur leur caractéristique et $\mathbf{f}$ de la forme générale $\mathbf{f} = a \cdot X^{q^i+q^j},\ a \in \mathbb{L}$. Plus précisément, nous allons revenir sur l'attaque réalisée par Dubois *et al.* sur SFLASH [PCG01a], décrit à la section 5.3, qui est un algorithme de signature basé sur cette configuration. Nous introduisons ensuite notre famille de clés faibles pour HFE.

7.2.1 Rappel : Attaque sur SFLASH

Commençons par remarquer que dans le cas où $\mathbf{f} = a \cdot X^{q^i+q^j}$, on peut supposer $a = 1$. En effet, une clé équivalente à $\mathbf{PK} = T \circ \mathbf{f} \circ S$ est $T' \circ X^{q^i+q^j} \circ S$, où la multiplication par a est absorbée par la transformation affine T'.

Dans cette configuration, des propriétés très spéciales apparaissent, mises en évidence dans [DFSS07, DFS07, Dub07]. Le monôme secret $\mathbf{f}$ a des propriétés de commutativité avec plusieurs applications. Par exemple, multiplier $\mathbf{f}$ à droite par un élément ξ équivaut à multiplier à gauche par $\xi^{q^i+q^j}$. Une autre propriété est que $\mathbf{f}$ commute avec le morphisme de Frobenius $x \mapsto x^q$ noté Fr . C'est la première

propriété cependant qui a permis à Dubois *et al.* d'attaquer le schéma SFLASH. Exposons rapidement leur idée.

L'égalité $\mathbf{f} \circ M_\xi = M_{\mathbf{f}(\xi)} \circ \mathbf{f}$, où M_ξ représente la multiplication par un élément ξ, se répercute sur la clé publique d'un C* de la manière suivante :

$$\mathbf{PK} \circ (S^{-1} \circ M_\xi \circ S) \quad = \quad (T \circ M_{\mathbf{f}(\xi)} \circ T^{-1}) \circ \mathbf{PK}. \tag{7.2}$$

Dans le cas de SFLASH, la clé publique consiste en la clé publique d'un C*, privée d'un certain nombre r de ses équations (C*−) : $\overline{\mathbf{PK}} = \bar{T} \circ \mathbf{f} \circ S$, où la matrice $\overline{T}$ n'est constituée que de $n - r$ lignes de T. Cependant, de (7.2) on obtient :

$$\overline{\mathbf{PK}} \circ (S^{-1} \circ M_\xi \circ S) = \overline{T} \circ M_{\mathbf{f}(\xi)} \circ \mathbf{f} \circ S. \tag{7.3}$$

Rapidement, la suite de l'attaque consiste à remarquer que dès que $\xi \in \mathbb{L} \backslash \mathbb{K}$, l'équation (7.3) fournit de nouvelles coordonnées de $\mathbf{f} \circ S$, coordonnées qui sont cachées dans la version "moins". Ainsi, en retrouvant suffisamment de multiplications M_ξ, on peut reconstituer une clef publique d'un C* puis terminer en appliquant l'attaque de Patarin [Pat95].

7.2.2 Propriété de commutativité avec le polynôme interne pour le morphisme de Frobenius

Nous ne prétendons pas adapter l'attaque précédente sur SFLASH au système HFE.s Nous nous sommes plus intéressés à la particularité du système utilisée pour monter l'attaque, à savoir la commutativité du polynôme interne correspondant à un C* avec des applications linéaires, en l'occurrence multiplications et applications Frobenius. L'idée première étant que la commutativité d'un système d'équations quadratiques avec une application linéaire révèle a priori une singularité dans ledit système.

Nous nous intéressons au problème plus large de savoir si pour un polynôme général $\mathbf{f}$ du type HFE, décrit par l'équation (7.1) de la sous-section 7.1.1, il existe deux applications linéaires $\mathcal{L}, \mathcal{L}'$ telles que $\mathbf{f} \circ \mathcal{L} = \mathcal{L}' \circ \mathbf{f}$.

Tout d'abord, notons que la propriété $\mathbf{f} \circ \mathcal{L} = \mathcal{L}' \circ \mathbf{f}$ pour $\mathcal{L}, \mathcal{L}'$ des multiplications, n'est en général pas vérifiée. Dès que $\mathbf{f}$ est composé de plus d'un terme, une telle égalité ne se produit (éventuellement) que dans le cas où $\mathbf{f}$ est homogène lorsque $\mathbb{K} \neq \mathbb{F}_2$, ou dans le cas où $\mathbf{f}$ est sans terme constant lorsque $\mathbb{K} = \mathbb{F}_2$:

$$\begin{aligned} f \circ M_\lambda(X) &= \sum_{i,j} a_{i,j} \cdot (\lambda \cdot X)^{q^i+q^j} + \sum_i b_i \cdot (\lambda \cdot X)^{q^i} + c \\ &= \sum_{i,j} a_{i,j} \cdot \lambda^{q^i+q^j} \cdot X^{q^i+q^j} + \sum_i b_i \cdot \lambda^{q^i} \cdot X^{q^i} + c; \\ M_\delta \circ \mathbf{f}(X) &= \sum_{i,j} a_{i,j} \cdot \delta \cdot X^{q^i+q^j} + \sum_i b_i \cdot \delta \cdot X^{q^i} + \delta \cdot c. \end{aligned}$$

Notons que lorsque $\mathbf{f}$ est composée de deux termes, cette propriété de commutativité avec les multiplications, lorsqu'elle existe, se restreint souvent aux multiplications

par des éléments contenus dans un sous-corps strict de $\mathbb{L}$. Dès que le nombre de terme dépasse 2, la chance d'avoir une telle propriété pour des multiplications par des éléments n'appartenant pas à $\mathbb{K}$ devient faible.

Pour ce qui est des applications de Frobenius (plus précisément, $Fr : x \mapsto x^q$ ou Fr^{α}), remarquons que la propriété de commutativité remarquée pour les monômes dans le cas de C*, n'est en général plus vérifiée. Cependant, si l'on se restreint à considérer les polynômes du type HFE (équation (7.1)) *à coefficients dans* $\mathbb{K}$, alors la propriété de commutativité avec l'application Frobenius ou une de ses itérées subsiste. En effet, dans ce cas particulier, les coefficients de $\mathbf{f}$ restent inchangés sous l'action de l'application du morphisme de Frobenius Fr :

$$\begin{aligned} Fr \circ \mathbf{f}(X) &= \left(\sum_{i,j} a_{i,j} \cdot X^{q^i+q^j} + \sum_i b_i \cdot X^{q^i} + c\right)^{q^\alpha} \\ &= \sum_{i,j} {a_{i,j}}^{q^\alpha} \cdot X^{q^{i+\alpha}+q^{j+\alpha}} + \sum_i {b_i}^{q^\alpha} \cdot X^{q^{i+\alpha}} + c^{q^\alpha} \\ &= \sum_{i,j} a_{i,j} \cdot X^{q^{i+\alpha}+q^{j+\alpha}} + \sum_i b_i \cdot X^{q^{i+\alpha}} + c \\ &= \mathbf{f} \circ Fr\,(X). \end{aligned}$$

Nous sommes invités à étudier cet ensemble de polynômes à coefficients dans $\mathbb{K}$, dont on sait qu'ils commutent déjà avec le morphisme du Frobenius. Soient $\mathbf{f}$ un polynôme de cet ensemble et $\mathcal{L}, \mathcal{L}'$ deux applications linéaires. Notons :

$$\begin{aligned} \mathcal{L}(X) &= \sum_l \lambda_l X^{q^l}, \\ \mathcal{L}'(X) &= \sum_l \delta_l X^{q^l}, \\ \mathbf{f} &= \sum_{i,j} a_{i,j} \cdot X^{q^i+q^j} + \sum_i b_i \cdot X^{q^i} + c. \end{aligned}$$

Nous avons :

$$\begin{aligned} \mathbf{f} \circ \mathcal{L}(X) &= \sum_{i,j} a_{i,j} \left(\sum_l \lambda_l \cdot X^{q^l}\right)^{q^i+q^j} + \sum_i b_i \left(\sum_l \lambda_l \cdot X^{q^l}\right)^{q^i} + c \\ &= \sum_{i,j} a_{i,j} \left(\sum_{l_1,l_2} \lambda_{l_1}^{q^i} \cdot \lambda_{l_2}^{q^j} \cdot X^{q^{i+l_1}+q^{j+l_2}}\right) + \sum_i b_i \left(\sum_l \lambda_l^{q^i} \cdot X^{q^{l+i}}\right) + c \\ &= \sum_{i,j} \sum_{l_1,l_2} \lambda_{l_1}^{q^i} \cdot \lambda_{l_2}^{q^j} \cdot a_{i,j} \cdot X^{q^{i+l_1}+q^{j+l_2}} + \sum_i \sum_l \lambda_l^{q^i} \cdot b_i \cdot X^{q^{i+l}} + c, \quad (7.4) \end{aligned}$$

et :

$$\begin{aligned}\mathcal{L}' \circ \mathbf{f}(X) &= \sum_l \delta_l \left(\sum_{i,j} a_{i,j} \cdot X^{q^i+q^j} + \sum_i b_i \cdot X^{q^i} + c \right)^{q^l} \\ &= \sum_l \delta_l \left(\sum_{i,j} {a_{i,j}}^{q^l} \cdot X^{q^{i+l}+q^{j+l}} + \sum_i {b_i}^{q^l} \cdot X^{q^{i+l}} + c^{q^l} \right) \\ &= \sum_{i,j} \sum_l \delta_l \cdot a_{i,j} \cdot X^{q^{i+l}+q^{j+l}} + \sum_i \sum_l \delta_l \cdot b_i \cdot X^{q^{i+l}} + \sum_l \delta_l \cdot c. \qquad (7.5)\end{aligned}$$

Lorsque la représentation polynomiale de $\mathcal{L}$ comporte plus d'un terme, remarquons que dans les deux expressions (7.5) et (7.4), on peut avoir le même nombre de termes linéaires, mais en général pas simultanément le même nombre de termes quadratiques. Ceci provient des doubles produits intervenant dans l'équation (7.4). Ainsi dans ce cas, et sauf quelques éventuelles situations ésotériques [3], $\mathbf{f} \circ \mathcal{L} = \mathcal{L}' \circ \mathbf{f}$ ne semble possible que lorsque les applications linéaires sont composées d'un seul terme. Lorsque c'est le cas, ces applications linéaires correpondent soit à une multiplication par un élément de $\mathbb{L}$, soit à une itérée de Fr , soit à la composée de ces deux applications. Leur cas a déjà été considéré plus haut.

Nous nous penchons plus précisément sur ces polynômes et cette propriété de commutativité dans la sous-section suivante, afin de définir une famille de clés secrètes pour HFE ayant la même propriété particulière, qui fait l'objet de l'attaque décrite dans la section 7.3.

7.2.3 Identification d'une famille $\mathcal{P}_{\mathbb{K}}$ de clés faibles pur HFE

7.2.3.1 Une propriété pour la clé publique

Dans le paragraphe 7.2.2 précédent, nous avons mis en évidence un ensemble de polynômes sur $\mathbb{L}$ ayant une propriété de commutativité avec l'application de Frobenius $Fr : x \mapsto x^q$. L'intérêt de ces polynômes ne s'arrête pas là. En effet, d'un point de vue cryptanalyste, si le polynôme secret $\mathbf{f}$ de HFE appartient à cet ensemble, alors la propriété de commutativité se détecte sur la clé publique $\mathbf{PK} = T \circ \mathbf{f} \circ S$. Ceci est justifié par les équations suivantes :

$$\begin{aligned} \mathbf{PK} \circ \left(S^{-1} \circ Fr \circ S\right) &= T \circ \mathbf{f} \circ S \circ \left(S^{-1} \circ Fr \circ S\right) \\ &= T \circ \mathbf{f} \circ S \circ S^{-1} \circ Fr \circ S \\ &= T \circ Fr \circ \mathbf{f} \circ S \\ &= \left(T \circ Fr \circ T^{-1}\right) \circ \mathbf{PK} \\ \Leftrightarrow \quad \mathbf{PK} &= \left(T \circ Fr \circ T^{-1}\right)^{-1} \circ \mathbf{PK} \circ \left(S^{-1} \circ Fr \circ S\right). \end{aligned}$$

Autrement dit, on voit que le système d'équations quadratiques formé par la clé publique a la propriété particulière qu'une composition à droite par une application

3. Les situations où les monômes $X^{q^{i+l_1}+q^{i+l_2}}$, avec $l_1 \neq l_2$, correspondent à un monôme $X^{q^{u+l}+q^{v+l}}$ apparaissant également dans $\mathbf{f}$ (*i.e.* $a_{u,v} \neq 0$), ce qui peut éventuellement encore arriver par réduction modulo $X^{q^n} - X$.

affine revient à effectuer une composition à gauche par *une autre application affine*. Dans la section 7.3, nous voyons comment exploiter cette propriété particulière du système HFE pour réaliser une attaque permettant de retrouver la clé secrète. Mais avant, détaillons plus précisément la famille de polynômes secrets HFE impliquant cette propriété.

7.2.3.2 La famille $\mathcal{P}_{\mathbb{K}}$

Pour plus de clarté, nous allons dénoter par $\mathcal{P}_{\mathbb{K}}$ la famille de polynômes HFE vérifiant l'équivalence précédente, du début de la sous-section 7.2.3. Cette famille contient déjà tous les polynômes à coefficients dans $\mathbb{K}$, d'après l'analyse faite plus haut.

À présent, notons que si un polynôme secret HFE $\mathbf{f}$ n'est pas à coefficients dans $\mathbb{K}$, mais que chaque coefficient peut s'écrire comme le produit d'un *même* élément $a \in \mathbb{L}$ par un élément de $\mathbb{K}$, alors on peut supposer que ce polynôme appartient à $\mathcal{P}_{\mathbb{K}}$ également. En effet, de la même manière que pour les monômes C* (cf. sous-section 7.2.1), on peut supposer que l'application T de la clé publique est remplacée par la composition de T avec la multiplication par a. De manière symétrique, si en remplaçant S par la composition de S avec la multiplication par un élément a de $\mathbb{L}$, le polynôme secret résultant est à coefficients dans $\mathbb{K}$, alors le polynôme de départ peut aussi être supposé dans $\mathcal{P}_{\mathbb{K}}$. En fait, ceci revient uniquement à considérer des clés équivalentes (voir sous-section 7.1.2).

Finalement, les polynômes de la famille mise en évidence sont de la forme (7.6) ci-dessous, encore résumée par la définition 16 qui suit :

$$\mathbf{f}(X) = \sum_{\substack{0 \le i,j \le n \\ q^i + q^j \le d}} \delta \cdot a_{i,j} \cdot \lambda^{q^i+q^j} \cdot X^{q^i+q^j} + \sum_{\substack{0 \le i \le n \\ q^i \le d}} \delta \cdot b_i \cdot \lambda^{q^i} \cdot X^{q^i} + \delta \cdot c, \qquad (7.6)$$

où $a_{i,j}, b_i, c \in \mathbb{K}$, $\delta \in \mathbb{L}$, et $\lambda \in \mathbb{L}$.

Définition 16 (Famille $\mathcal{P}_{\mathbb{K}}$) *Un polynôme $\mathbf{f}$ d'une clé secrète HFE, k, appartient à la famille $\mathcal{P}_{\mathbb{K}}$ de polynômes HFE, si $\mathbf{f}$ est à coefficients dans $\mathbb{K}$, ou s'il existe une clé secrète équivalente à k dont le polynôme secret est à coefficients dans $\mathbb{K}$.*

La proposition 20 suivante donne un encadrement du nombre de polynômes HFE appartenant à cette famille $\mathcal{P}_{\mathbb{K}}$, faisant l'objet de l'attaque de la section 7.3 :

Proposition 20 (Cardinal de $\mathcal{P}_{\mathbb{K}}$) *Le nombre de polynômes secrets HFE appartenant à la famille $\mathcal{P}_{\mathbb{K}}$ est supérieur ou égal à :*

i) $(q^{\frac{(D+1)(D+2)}{2}} - 1) \cdot q^{D+2} \cdot (q^n - q)$, lorsque $\mathbb{K} \neq \mathbb{F}_2$,

ii) $(q^{\frac{D(D+1)}{2}} - 1) \cdot q^{D+3} \cdot (q^n - q)$, lorsque $\mathbb{K} = \mathbb{F}_2$,

ce qui correspond à $\mathcal{O}\left(q^{D^2+n}\right)$. *Ce nombre est par ailleurs majoré par :*

i) $\left((q^{\frac{(D+1)(D+2)}{2}}-1)\cdot q^{D+2}-\frac{(D+1)(D+2)}{2}\cdot(q-1)\right)\cdot(q^n-q)^2+\frac{(D+1)(D+2)}{2}\cdot(q-1)\cdot(q^n-q)$, when $\mathbb{K}\neq\mathbb{F}_2$,

ii) $\left((q^{\frac{D(D+1)}{2}}-1)\cdot q^{D+2}-\frac{(D+1)(D+2)}{2}\cdot(q-1)\right)\cdot(q^n-q)^2+\frac{(D+1)(D+2)}{2}\cdot(q-1)\cdot(q^n-q)$, when $\mathbb{K}=\mathbb{F}_2$,

correspondant à $\mathcal{O}\left(q^{D^2+2n}\right)$.

Démonstration : Un polynôme HFE est composé de $\frac{(D+1)(D+2)}{2}+(D+1)+1=\frac{D(D+5)}{2}+3$ termes quand $\mathbb{K}\neq\mathbb{F}_2$, $\frac{(D+1)(D+2)}{2}-(D+1)+(D+2)+1=\frac{(D+1)(D+2)}{2}+2$ quand $\mathbb{K}=\mathbb{F}_2$. Nous avons :

1. Le corps $\mathbb{K}$ possède q éléments. Le nombre de polynômes HFE à coefficients dans $\mathbb{K}\neq\mathbb{F}_2$ est $q^{\frac{D(D+5)}{2}+3}$ ($q^{\frac{(D+1)(D+2)}{2}+2}$ when $\mathbb{K}=\mathbb{F}_2$). Nous nous intéressons cependant aux polynômes *non-linéaires* uniquement. Ceux-ci sont au nombre de $(q^{\frac{(D+1)(D+2)}{2}}-1)\cdot q^{D+2}$ quand $\mathbb{K}\neq\mathbb{F}_2$ et $\mathbb{K}\neq\mathbb{F}_2$, $(q^{\frac{(D+1)(D+2)}{2}-(D+1)}-1)\cdot q^{D+3}=(q^{\frac{D(D+1)}{2}}-1)\cdot q^{D+3}$ sinon.
2. Le nombre d'élément appartenant à $\mathbb{L}\setminus\mathbb{K}$ est q^n-q. Ainsi, le nombre de polynômes HFE pouvant s'écrire comme un polynôme à coefficients dans $\mathbb{K}$ (un polynôme de ceux décrits au point 1.), composé à gauche par la multiplication M_λ par un élément $\lambda\in\mathbb{L}\setminus\mathbb{K}$ est :

$$\begin{aligned}&(q^{\frac{(D+1)(D+2)}{2}}-1)\cdot q^{D+2}\cdot(q^n-q), && \text{lorsque } \mathbb{K}\neq\mathbb{F}_2,\\ &(q^{\frac{D(D+1)}{2}}-1)\cdot q^{D+3}\cdot(q^n-q), && \text{lorsque } \mathbb{K}=\mathbb{F}_2.\end{aligned}$$

   Ceci fournit la borne inférieure de la proposition.

À présent, notons que pour évaluer le nombre exact de polynômes appartenant à $\mathcal{P}_{\mathbb{K}}$, il faut encore évaluer le nombre de polynômes HFE s'écrivant comme un polynôme décrit au point 2., composé à droite par une multiplication par un élément de $\mathbb{L}\setminus\mathbb{K}$. Or, nous avons vu que certains polynômes ont la propriété que la composition à droite par une multiplication revient à faire une composition à gauche par une autre multiplication. Ces polynômes ont été repérés dans la sous-section 7.2.2 précédente. Parmi eux, seuls les monômes ont avec certitude une telle propriété pour les multiplications par n'importe quels éléments de $\mathbb{L}\setminus\mathbb{K}$. Or, les monômes $\mathbb{K}$-quadratiques à sur $\mathbb{L}$, à coefficient dans $\mathbb{K}$ sont au nombre de $\frac{(D+1)(D+2)}{2}\cdot(q-1)$ ou $\frac{(D(D+1)}{2})\cdot(q-1)$, selon que $\mathbb{K}=\mathbb{F}_2$ ou non. On peut alors établir la borne supérieure annoncée dans l'énoncé :

$$\begin{aligned}&\left((q^{\frac{(D+1)(D+2)}{2}}-1)\cdot q^{D+2}-\frac{(D+1)(D+2)}{2}\cdot(q-1)\right)\cdot(q^n-q)^2\\ &+\frac{(D+1)(D+2)}{2}\cdot(q-1)\cdot(q^n-q), && \text{lorsque } \mathbb{K}\neq\mathbb{F}_2,\\ &\left((q^{\frac{D(D+1)}{2}}-1)\cdot q^{D+2}-\frac{(D+1)(D+2)}{2}\cdot(q-1)\right)\cdot(q^n-q)^2\\ &+\frac{(D+1)(D+2)}{2}\cdot(q-1)\cdot(q^n-q), && \text{lorsque } \mathbb{K}=\mathbb{F}_2.\end{aligned}$$

□

Remarque : La propriété de commutativité de certains polynômes avec les multiplications rend le calcul d'une valeur exact du nombre de polynômes de $\mathcal{P}_{\mathbb{K}}$ difficile et explique pourquoi nous ne donnons qu'un encadrement de cette valeur. Faisant l'hypothèse que cette propriété de commutativité avec les multiplications par des éléments de $\mathbb{L} \setminus \mathbb{K}$ s'étend à tous les polynômes formés de deux monômes [4], on obtient cependant un ordre de grandeur raisonnable sur le nombre de polynômes de la famille $\mathcal{P}_{\mathbb{K}}$. Les polynômes de degré 2 à coefficient dans $\mathbb{K}$ formés de un ou deux monômes sont au nombre de $\binom{(D+1)(D+2)/2}{2} \cdot q(q-1)$. On obtient une approximation pour le nombre de polynômes HFE appartenant à la famille $\mathcal{P}_{\mathbb{K}}$:

$$\left(q^{(D+1)(D+2)/2+1} - 1) \cdot q^{D+3} - \binom{\frac{(D+1)(D+2)}{2}}{2} \cdot q(q-1)\right) \cdot (q^n - q)^2$$
$$+\binom{\frac{(D+1)(D+2)}{2}}{2} \cdot q(q - 1 \cdot (q^n - q).$$

Dans la suite, nous allons nous focaliser sur cette famille de polynômes secrets. Par abus de langage, on pourra se référer à un poynôme de la famille $\mathcal{P}_{\mathbb{K}}$ par l'appellation "polynôme secret HFE à coefficients dans $\mathbb{K}$", bien que cette appellation ne soit pas complètement rigoureuse, comme on a pu le voir à la définition 16. La figure 7.1 représente la décomposition d'une clé publique HFE, où le polynôme interne est à coefficients dans $\mathbb{K}$.

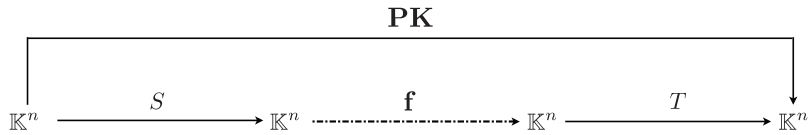

FIGURE 7.1: $\mathbf{PK} = T \circ \mathbf{f} \circ S$, La flèche discontinue indique que $\mathbf{f}$ est à coefficients dans $\mathbb{K}$.

7.3 Description de l'attaque des systèmes HFE utilisant des polynômes secrets de la famille $\mathcal{P}_{\mathbb{K}}$

Notre attaque sur les instances de HFE utilisant un polynôme de $\mathcal{P}_{\mathbb{K}}$ comme polynôme secret, est décrite dans cette section. Comme annoncé dans la sous-section 7.2, nous exploitons la propriété de commutativité de la clé publique de ces instances.

Plus précisément, nous récupérons les applications F_S et F_T, qui "commutent" (*i.e.* qui ont la propriété de commutativité) avec la clé publique. Rappelons que ces applications sont reliées à S et T. Mieux encore, nous allons voir que l'interpolation

4. Ceci est vrai lorsque $\mathbb{K} = \mathbb{F}_2$, et qu'un des monômes est $\mathbb{K}$-linéaire, mais pas nécessairement autrement (cf. sous-section 7.2.2).

de la combinaison de F_S et F_T avec la clé publique $\mathbf{PK}$, génère un autre polynôme à coefficients dans $\mathbb{K}$. Pour terminer, utilisant la limitation sur le degré des polynômes secrets HFE, nous déduisons de ce polynôme le polynôme original $\mathbf{f}$, ou un polynôme équivalent de bas degré. Dans tous les cas, on retrouve une clé secrète offrant l'efficacité de déchiffrement du détenteur légitime de la clé secrète.

7.3.1 Recouvrement des applications de Frobenius F_S et F_T

La première étape consiste à recouvrer les applications $S^{-1} \circ Fr \circ S$ et $T \circ Fr \circ T^{-1}$. Dénotons par F_S la composition $S^{-1} \circ Fr \circ S$ et par F_T l'application $T \circ Fr \circ T^{-1}$. D'après la partie 7.2.3, ces applications sont solutions du problème IP entre la clé publique et elle-même :

$$\mathbf{PK} \circ F_S \quad = \quad F_T \circ \mathbf{PK} \ .$$

De manière rigoureuse, nous avons :

Proposition 21 *Il existe un isomorphisme polynomial entre la clé publique et elle-même. Des isomorphismes sont en particulier donnés par* $({F_T}^{-1}, F_S), \ldots,$ $({F_T}^{-n}, {F_S}^{n})$. □

Il est dit dans cette proposition 21 que (F_T^{-1}, F_S) et leurs itérées sont des solutions au problème IP entre la clé publique et elle-même. Ceci indique qu'il peut y avoir des solutions parasites. Cependant, le cas où $\mathbf{f}$ est monomial correspond à C*, qui est à proscrire à cause de la cryptanalyse de [Pat95] par exemple. D'après la discussion du paragraphe 7.2.2, il est alors peu probable d'avoir d'autres solutions que celles indiquées [5] par la proposition 21. Nos expériences pratiques, pour des $\mathbf{f}$ génériques, n'ont d'ailleurs jamais fait apparaître d'autres solutions. Nous faisons donc la supposition raisonnable que que ces applications (F_T^{-1}, F_S) et leurs itérées sont seules solutions du problème IP entre la clé publique et elle-même.

À présent, en nous basant sur les algorithmes existants pour la résolution du problème IP (voir section 5.2 du chapitre 5), nous considérons différentes configurations correspondant à différentes complexités de résolution du problème IP dans le cas qui nous intéresse, à savoir, quand le polynôme secret est à coefficients dans $\mathbb{K}$ au lieu de $\mathbb{L}$.

Meilleures conditions de résolution du problème IP. La réunion de conditions permettant une résolution en temps polynomial du problème IP dans notre situation est :

1. S et T sont linéaires (plutôt qu'affines).
2. Il existe une partie linéaire dans $\mathbf{f}$.
3. La constante dans $\mathbf{f}$ est non nulle.

5. Nous avons d'autre solutions (les multiplications par exemple) pour certaines configurations de polynômes $\mathbf{f}$ formés de très peu de termes (typiquement deux). Notons que dans ce cas, on peut alors également simplement deviner le polynôme $\mathbf{f}$ puis trouver S et T. Cette attaque est également mentionnée dans la section 7.4.2.

Commençons par apporter une précision par rapport au paragraphe 7.1.2. Dans ce paragraphe, nous annonçons que les applications S et T peuvent en général être supposées linéaires. Concernant l'ensemble de clés considérées, *i.e.* celles dont le polynôme secret appartient à $\mathcal{P}_{\mathbb{K}}$, cette supposition n'est plus possible. En effet, restreindre S et T à leur partie linéaire est compensé par des transformations sur le polynôme $\mathbf{f}$, afin de pouvoir continuer à dériver la même clé publique. Le polynôme $\mathbf{f}$ ne pourrait alors plus être supposé comme ayant ses coefficients dans $\mathbb{K}$, propriété sur laquelle est basée notre attaque [6].

Revenant à la condition 1., S et T linéaires peut se réaliser dans deux cas de figure. Premièrement, cela peut arriver par hasard, mais la probabilité d'obtenir S et T linéaires, alors qu'elles sont choisies parmi l'ensemble des applications affines, est très faible, de l'ordre de $(1/q^n)^2$. L'autre possibilité est que le choix de S et T linéaires soit délibéré. Par exemple, il se peut que les applications soient systématiquement choisies linéaires à cause du discours sur les clés équivalentes (cf. paragraphe 7.1.2). Les choisir linéaires est également une manière de réduire la taille des clés.

Concernant la condition 2., celle-ci est réalisée avec forte probabilité. En effet, si les coefficients de X^{q^k} de $\mathbf{f}$ (voir l'équation (7.1) de la sous-section 7.1.1) sont choisis aléatoirement dans $\mathbb{K}$, la probabilité qu'ils soient tous nuls est de l'ordre de $\frac{1}{q^D}$.

Enfin, la dernière condition est réalisée avec probabilité $\frac{q-1}{q}$, toujours dans le cas où les coefficients sont choisis aléatoirement dans $\mathbb{K}$. Par ailleurs, notons que si la constante dans $\mathbf{f}$ est nulle, alors la clé publique $\mathbf{PK}$ envoie zéro sur zéro, ce qui n'est pas souhaité.

Par conséquent, il n'est pas complètement insensé d'avoir ces trois conditions réunies.

Autres situations. Dans le cas où S et T sont affines, nous avons déjà vu au chapitre 5 que la situation est plus délicate. La complexité de résolution de l'instance IP devient en fait q'^n, où les coefficients du polynôme définissant S appartiennent à $\mathbb{F}_{q'}$. Dans notre situation, nous avons $q' = q$ en général. Notons tout de même que dans la version "sous-corps", qui rentre dans notre situation, on suppose S et T à coefficients dans $\mathbb{K}$. Dans ce cas, si $q' = 2$ et n n'est pas trop grand, résoudre l'instance IP reste faisable (voir la sous-section 7.4.2).

7.3.2 Appropriation d'information en rapport avec S et T

Supposons à présent résolu le problème IP entre la clé publique $\mathbf{PK}$ et elle-même, et être en possession d'un automorphisme solution (U, V). Rappelons que l'on peut supposer (U, V) de la forme $(S^{-1} \circ Fr^{\,i_0} \circ S, T \circ Fr^{\,i_0} \circ T^{-1})$, $1 \leq i_0 \leq n-1$ (voir la sous-section 7.3.1 précédente).

Si i_0 est premier avec n, c'est à dire, si U et V sont semblables au morphisme de Frobenius Fr , on a le résultat suivant :

6. Par contre, supposer $\mathbb{L}$ publique n'a pas de répercussions sur $\mathbf{f}$ et nous continuons donc de faire cette supposition.

Proposition 22 *Soit* $(U, V) = \left(S^{-1} \circ Fr^{\,i_0} \circ S, T \circ Fr^{\,i_0} \circ T^{-1}\right)$, *avec* $\mathrm{pgcd}(i_0, n) = 1$. *Soit* k *l'inverse de* i_0 *modulo* n.

i) Il existe $\widetilde{S}, \widetilde{T} \in \mathrm{GL}_n(\mathbb{K})$ *tels que* $Fr = \widetilde{S} \circ V^k \circ \widetilde{S}^{-1}$ *et* $Fr = \widetilde{T}^{-1} \circ U^k \circ \widetilde{T}$.

ii) $\widetilde{S} = F_1 \circ S$ *et* $\widetilde{T} = T \circ F_2$, *où* F_1 *et* F_2 *sont combinaisons linéaires sur* $\mathbb{K}$ *de puissances de* Fr .

Démonstration :

i) U et V sont semblables à F^{i_0}, donc U^k et V^k sont semblables à $Fr^{\,i_0 \cdot k} = Fr^{\,1 \mod n} = Fr$.

ii) Prenons $\widetilde{S}$. Nous avons :

$$\begin{aligned} Fr &= \widetilde{S} \circ V^k \circ \widetilde{S}^{-1} \\ &= \widetilde{S} \circ S^{-1} \circ Fr^{\,i_0 \cdot k} \circ S \circ \widetilde{S}^{-1} \\ &= \widetilde{S} \circ S^{-1} \circ Fr \circ S \circ \widetilde{S}^{-1}. \end{aligned}$$

Donc $Fr \circ \widetilde{S} \circ S^{-1} = \widetilde{S} \circ S^{-1} \circ Fr$. Autrement dit, $\widetilde{S} \circ S^{-1}$ commute avec Fr , donc est combinaison linéaire à coefficients dans $\mathbb{K}$ de puissances du Frobenius (proposition 13). Ceci conclut le point *ii)* pour $\widetilde{S}$. Un raisonnement similaire nous mène aux mêmes conclusions pour $\widetilde{T}$.

□

Pour pouvoir continuer notre attaque, nous souhaitons avoir des applications $\widetilde{S}$, $\widetilde{T}$ comme dans l'énoncé de la proposition 22. Autrement dit, nous aimerions avoir des solutions U et V au problème IP, semblables au morphisme de Frobenius. Ceci revient à avoir la puissance i_0 premier avec n dans l'expression de U et V ci-dessus. De plus, la valeur de i_0 est souhaitée connue, afin de pouvoir trouver facilement $\widetilde{S}$ et $\widetilde{T}$.

Il est facile de tester si U et V sont semblables à Fr . En effet, ceci équivaut à ce que i_0 soit premier avec n, et le nombre d'entiers inférieurs à n et premiers avec n est $\phi(n)$. On trouve un automorphisme candidat au bout d'environ $n/\phi(n) = \mathcal{O}(\log \log n)$ tests des automorphismes fournis par la solution du problème IP. Quant à la valeur exacte de i_0, nous allons en faire pour le moment une simple supposition. La suite de l'attaque fournit un moyen d'invalider cette supposition si nécessaire.

7.3.3 Création d'une clé secrète équivalente g

Nous sommes maintenant dans les conditions de la proposition 22 et en possession de tous les objets impliqués dans cette proposition. À cette étape de l'attaque, nous allons voir comment nous pouvons essayer de neutraliser l'effet des applications S et T sur $\mathbf{f}$. Pour cela, regardons la structure des applications $\widetilde{S}$ et $\widetilde{T}$, définies au paragraphe précédent 7.3.2, proposition 22 :

$$\begin{aligned} \widetilde{S} &= F_1 \circ S \\ \widetilde{T} &= T \circ F_2. \end{aligned}$$

Au niveau des inverses, cela donne :

$$\begin{aligned} \widetilde{S}^{-1} &= S^{-1} \circ F_1^{-1} \\ \widetilde{T}^{-1} &= F_2^{-1} \circ T^{-1}. \end{aligned}$$

Si bien que finalement, en composant $\widetilde{S}^{-1}$ et $\widetilde{T}^{-1}$ de part et d'autre de la clé publique **PK**, cela donne :

$$\begin{aligned} \widetilde{T}^{-1} \circ \mathbf{PK} \circ \widetilde{S}^{-1} &= F_2^{-1} \circ T^{-1} \circ T \circ \mathbf{f} \circ S \circ S^{-1} \circ F_1^{-1} \\ &= F_2^{-1} \circ \mathbf{f} \circ F_1^{-1}. \end{aligned} \tag{7.7}$$

Ceci nous invite à définir le polynôme révélé par l'équation (7.7) ci-dessus :

$$\mathbf{g} = \widetilde{T}^{-1} \circ \mathbf{PK} \circ \widetilde{S}^{-1} \pmod{X^{q^n} - X}$$

On remarque que le triplet $\left(\widetilde{T}, \mathbf{g}, \widetilde{S}\right)$ constitue une clé secrète équivalente à la clé initiale $(T, \mathbf{f}, S)$. On a le résultat intéressant suivant pour $\mathbf{g}$, illustré par la figure 7.2.

Proposition 23 $\mathbf{g}$ *est un polynôme HFE, à coefficients dans* $\mathbb{K}$.

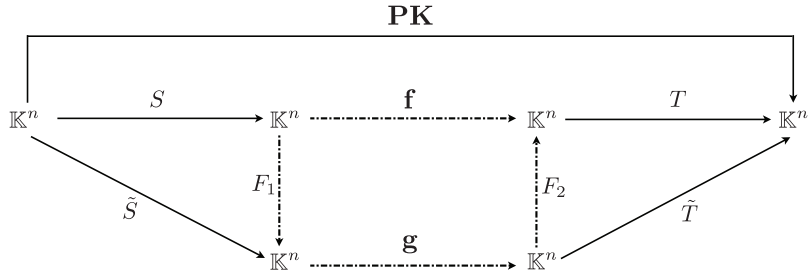

FIGURE 7.2: $\mathbf{PK} = T \circ \mathbf{f} \circ S = \widetilde{T} \circ \mathbf{g} \circ \widetilde{S}$. Les flèches discontinues indiquent les applications à coefficients dans $\mathbb{K}$.

Démonstration : Les polynômes du type HFE étant stables par composition avec des polynômes additifs [7] et réduction modulo $X^{q^n} - X$, $\mathbf{g}$ est un polynôme HFE au même titre que $\mathbf{f}$. Les coefficients de $\mathbf{f}$ sont dans $\mathbb{K}$ par hypothèse. Ceux des représentations polynomiales de F_1 et F_2 le sont également, par la proposition 22, donc aussi ceux de ${F_1}^{-1}$ et ${F_2}^{-1}$ par le corollaire 1 (sous-section 5.2.1 du chapitre 7.1).□

Remarque :

1. Notons tout de même que ce polynôme $\mathbf{g}$ se retrouve facilement par interpolation. Nous considérons $\mathbf{g}$ modulo $X^{q^n} - X$, il est alors composé de l'ordre de $\mathcal{O}\left(n^2\right)$ coefficients, qui peuvent être déterminés uniquement.

7. Ces polynômes désignent les applications $\mathbb{K}$-linéaires, comme F_1 ou F_2. Nous ne prenons en compte que la structure des monômes composant les polynômes HFE, pas leur restriction sur le degré.

2. Une autre remarque est que le résultat de cette proposition permet de tester notre supposition concernant l'exposant i_0 (paragraphe 7.3.2 précédent). Si $\mathbf{g}$ n'est pas à coefficients dans $\mathbb{K}$, notre supposition était mauvaise. Il nous reste alors à modifier l'hypothèse sur la valeur de i_0 et construire un nouveau polynôme $\mathbf{g}$. Heureusement, cette étape de l'attaque n'est pas coûteuse et nous pouvons la faire $\phi(n)$ fois. Notons encore que $\mathbf{g}$ peut être à valeurs dans $\mathbb{K}$ sans que nécessairement la valeur supposée de i_0 soit la bonne. Cependant, pour la suite de l'attaque, ceci n'a pas d'importance car nous avons juste besoin d'un polynôme à coefficients dans $\mathbb{K}$ pour continuer.

Cependant, à la différence du polynôme $\mathbf{f}$, le degré de $\mathbf{g}$ n'est a priori plus borné par d.

En effet, F_1 et F_2 sont de la forme : $\sum_i \lambda_i X^{q^{\theta_i}}$, où les $\lambda_i \in \mathbb{K}$ sont presque tous nuls. Dans cette expression, les θ_i peuvent être arbitrairement grands. La composition de $\mathbf{f}$ avec ces applications, à droite ou à gauche, rend ainsi les monômes du polynôme résultant de degré également arbitrairement grand [8].

L'attaque ne se termine donc pas à cette étape. Le polynôme $\mathbf{g}$ n'est pas utilisable en tant que tel comme polynôme secret HFE : essayer de résoudre le système polynomial donné par la clé publique $\mathbf{PK}$ en utilisant la clé secrète équivalente $\left(\widetilde{T}, \mathbf{g}, \widetilde{S}\right)$, revient à chercher les racines d'un polynôme de très haut degré (de l'ordre de q^n).

L'intérêt de ce polynôme $\mathbf{g}$ est, comme nous allons le voir, que les propriétés annoncées à la proposition 23 vont nous permettre de déduire de $\mathbf{g}$ un polynôme HFE, à coefficients dans $\mathbb{K}$ *et* de bas degré. Ce polynôme pourra être utilisé, conjointement à deux applications linéaires que nous allons définir, pour le déchiffrement.

7.3.4 Recouvrement d'une clé secrète de bas-degré équivalente à la clé secrète de départ

Nous arrivons à la dernière étape de l'attaque. Cette étape consiste à effectuer une décomposition fonctionnelle de $\mathbf{f}$ à l'aide de $\mathbf{g}$. Afin de souligner l'intérêt des étapes précédentes, commençons par considérer le cas où la décomposition est faite à l'aide de $\mathbf{PK}$.

7.3.4.1 Décomposition de f à l'aide de PK

La sécurité de HFE, comme les autres schémas multivariés, repose sur la difficulté de résoudre le système d'équations donné par la clé publique. Ainsi, la solution triviale consistant à effectuer une décomposition directe de la clé publique $\mathbf{PK}$, similaire à (7.7), pour retrouver la clé secrète, n'est pas réalisable en général. Détaillons ce point pour le cas de notre polynôme $\mathbf{f}$.

En considérant $\mathbf{PK} = T \circ \mathbf{f} \circ S$, les inconnues intervienne de manière cubique.

8. On peut se référer aux expressions données au paragraphe 7.2.2, (7.4) et (7.5) pour les degrés des monômes de $\mathbf{f}$ composé à droite ou à gauche par de telles applications.

Considérons donc plutôt l'équation :

$$T^{-1} \circ \mathbf{PK} = \mathbf{f} \circ S \pmod{X^{q^n} - X}, \text{ ou} \tag{7.8}$$
$$\mathbf{PK} \circ S^{-1} = T \circ \mathbf{f} \pmod{X^{q^n} - X}. \tag{7.9}$$

Se basant sur la représentation polynomiale de ces élément, le nombre d'inconnues est dans les deux situations (7.8) ou (7.9) : $2 \cdot (n+1)$ pour les deux applications inversibles S et T, ainsi que $\frac{(D+1)(D+2)}{2} + (D+2) + 1$ pour les coefficients de $\mathbf{f}$, soit $\mathcal{O}\left(D^2 + n\right)$ inconnues. L'identification coefficient par coefficient des polynômes de part et d'autre de l'égalité, fournit $n(n+1)2+n+1$ équations, soit $\mathcal{O}\left(n^2\right)$ équations.

Cependant, ces équations n'ont pas de raison d'être de degré petit. Dans le cas de l'équation (7.8), les coefficients inconnus de l'application S, ne sont a priori pas à coefficients dans $\mathbb{K}$ et intervienne avec un degré élevé par composition avec $\mathbf{f}$. De même, les coefficients de $\mathbf{PK}$ appartiennent à $\mathbb{L}$ et interviennent dans (7.8) avec un degré élevé par composition avec T. Pour ce qui est de l'équation (7.8), le membre de droite fournit une expression $\mathbb{K}$-quadratique en les inconnues, car $\mathbf{f}$ est à coefficients dans $\mathbb{K}$ et T est $\mathbb{K}$-linéaire. Par contre, dans le membre de gauche, les inconnues interviennent toujours avec un degré élevé. Pour s'en convaincre (avec des notations évidentes), considérons les expressions suivantes sur $\mathbb{L}[X]$:

$$\begin{aligned}
T^{-1} \circ \mathbf{PK} &= \sum_{k=0}^{n-1} t_k \left(\sum_{i,j} e_{ij} X^{q^i+q^j} + \sum_i f_i X^{q^i} + g \right)^{q^k} \\
&= \sum_{i,j,k} t_k \cdot e_{ij}^{q^k} \cdot X^{q^{i+k}+q^{j+k}} + \sum_{i,k} t_k \cdot f_i^{q^k} \cdot X^{q^{i+k}} + g^{q^k} \cdot \sum_k t_k, \\
\mathbf{PK} \circ S^{-1} &= \sum e_{ij} \left(\sum_{k=0}^{n-1} s_k X^{q^k} \right)^{q^i+q^j} + \sum f_i \left(\sum_{k=0}^{n-1} s_k X^{q^k} \right)^{q^i} + g \\
&= \sum_{i,j,k,l} e_{ij} \cdot s_k^{q^i} \cdot s_l^{q^j} \cdot X^{q^{i+k}+q^{l+j}} + \sum_{i,k} f_i \cdot s_k^{q^i} \cdot X^{q^{i+k}} + g.
\end{aligned}$$

7.3.4.2 Décomposition de f à l'aide de g

Voyons maintenant comment l'utilisation de $\mathbf{g}$ retrouvé au paragraphe 7.3.3, dans la décomposition de $\mathbf{f}$, plutôt que $\mathbf{PK}$, permet d'obtenir une situation plus favorable au cryptanalyste. Rappelons que sa relation avec le polynôme $\mathbf{f}$ est la suivante :

$$\mathbf{g} = F_2^{-1} \circ \mathbf{f} \circ F_1^{-1} \pmod{X^{q^n} - X},$$

qui peut se réécrire en composant à droite par F_1 de part et d'autre de l'égalité :

$$\mathbf{g} \circ F_1 = F_2^{-1} \circ \mathbf{f} \pmod{X^{q^n} - X}. \tag{7.10}$$

L'équation (7.10) peut se représenter par la figure 7.3.

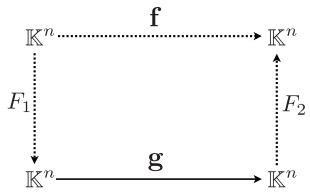

FIGURE 7.3: $\mathbf{g} = F_2^{-1} \circ \mathbf{f} \circ F_1^{-1}$. Les flèches en pointillés indiquent les applications inconnues.

Proposition 24 *L'équation* (7.10) *fournit* $\mathcal{O}\left(n^2\right)$ *équations* quadratiques *en* $\mathcal{O}\left(D^2+n\right)$ *inconnues.*

Démonstration : Introduisons les notations suivantes :

$$\begin{aligned} F_1(X) &= \sum_{k=0}^{n-1} x_k X^{q^k}, \\ F_2^{-1}(X) &= \sum_{k=0}^{n-1} y_k X^{q^k}, \\ \mathbf{g}(X) &= \sum_{q^i+q^j<q^n} e_{ij} X^{q^i+q^j} + \sum_{i=0}^{n-1} f_i X^{q^i} + g. \end{aligned}$$

Nous avons également :

$$\mathbf{f}(X) = \sum_{q^i+q^j \leq d} a_{ij} X^{q^i+q^j} + \sum_{q^i \leq d} b_i X^{q^i} + c.$$

Notons que plusieurs triplets $(F_1, \mathbf{f}, F_2)$ peuvent être solutions de l'équation (7.10). Par exemple, puisque toutes ces applications commutent avec le morphisme de Frobenius, nous pouvons prendre une solution particulière, multiplier F_2^{-1} et F_1 par Fr , et obtenir une nouvelle solution. En particulier, le polynôme $\mathbf{f}$ retrouvé ainsi peut être différent du polynôme secret $\mathbf{f}$ utilisé initialement. Cependant, comme dans tous les cas nous imposons au degré de ce polynôme d'être borné par $d = 2 \cdot q^D$, obtenir $\mathbf{f}$ ou un autre polynôme de bas degré, n'a pas d'importance. Nous conservons donc pour les coefficients inconnus de ce polynôme, les notations utilisées initialement pour le polynôme de la clé secrète.
Développons les deux termes de l'équation (7.10), $\mathbf{g} \circ F_1$ et $F_2^{-1} \circ \mathbf{f}$.
Pour $\mathbf{g} \circ F_1$, on a :

$$\begin{aligned} \mathbf{g} \circ F_1 &= \sum_{i,j} e_{ij} \left(\sum_{k=0}^{n-1} x_k X^{q^k} \right)^{q^i+q^j} + \sum_i f_i \left(\sum_{k=0}^{n-1} x_k X^{q^k} \right)^{q^i} + g \\ &= \sum_{i,j,k,l} e_{ij} \cdot x_k \cdot x_l \cdot X^{q^{i+k}+q^{l+j}} + \sum_{i,k} f_i \cdot x_k \cdot X^{q^{i+k}} + g. \end{aligned}$$

Nous obtenons un polynôme dont les coefficients sont quadratiques en les coefficients inconnus de F_1, car ceux-ci sont dans $\mathbb{K}$ donc invariants par le morphisme de Frobenius Fr .
Quant à $F_2^{-1} \circ \mathbf{f}$:

$$\begin{aligned} F_2^{-1} \circ \mathbf{f} &= \sum_{k=0}^{n-1} y_k \left(\sum_{q^i+q^j \leq d} a_{ij} X^{q^i+q^j} + \sum_{q^i \leq d} b_i X^{q^i} + c \right)^{q^k} \\ &= \sum_{i,j,k} y_k \cdot a_{ij} \cdot X^{q^{i+k}+q^{j+k}} + \sum_{i,k} y_k \cdot b_i \cdot X^{q^{i+k}} + c \cdot \sum_k y_k. \end{aligned}$$

Ici encore, cette expression se réduit à un polynôme dont les coefficients sont quadratiques en les coefficients inconnus de F_2^{-1} et de $\mathbf{f}$.
Réduisant ces deux expressions modulo $X^{q^n} - X$, et les identifiant coefficient par coefficient, il résulte bien $\frac{n(n+1)}{2} + n + 1$ équations quadratiques en les $\frac{(D+1)(D+2)}{2} + (D+2) + 1$ coefficients inconnus de $\mathbf{f}$ et les $2n$ coefficients inconnus de F_1 et F_2^{-1}. □

Le nombre d'inconnues intervenant dans cette équation est $D(D+1)/2 + D + 1$ pour $\mathbf{f}$ plus $2n$ pour les applications F_1 et F_2. Tous ces coefficients sont dans $\mathbb{K}$ donc il peut éventuellement être intéressant de rajouter les équations de corps (une par variable). L'égalité (7.10) fournit donc $\mathcal{O}\left(n^2\right)$ équations en $\mathcal{O}\left(D^2 + n\right)$ inconnues de $\mathbb{K}$, mais ces équations sont cette fois toutes *quadratiques*. Détaillons à présent ce point et voyons que la résolution de ce système est bien plus facile que dans le cas précédent.

Penchons-nous à présent un peu plus sur ce système et voyons que sa résolution est réalisable en pratique.

7.3.4.3 Résolution du système correspondant à la décomposition de f à l'aide de g

L'équation donnée par (7.10) fournit $\mathcal{O}\left(n^2\right)$ équations quadratiques en $\mathcal{O}\left(n + D^2\right)$ inconnues (proposition 24). Parmi les solutions de ce système, il y a les solutions triviales du type $F_1 = \mathbf{f} = 0$. Ceci provient du fait que F_1 et F_2^{-1} ne sont pas perçues à ce moment comme des applications inversibles. On peut par exemple aussi avoir $F_1 = F_2^{-1} = 0$. Une solution naturelle est d'encoder l'inversibilité de F_1 et F_2. Ceci revient à rajouter les $2n$ équations correspondant à $F_1 \circ F_1^{-1}(X) = X \pmod{X^{q^n} - X}$ et $F_2 \circ F_2^{-1}(X) = X \pmod{X^{q^n} - X}$, quadratiques en les coefficients de F_1, F_2^{-1} et les $2n$ nouveaux coefficients inconnus de F_1^{-1} et F_2. Toutes les inconnues étant dans $\mathbb{K}$, il peut être intéressant d'également rajouter les équations de corps, une par variable.

Plaçons-nous dans le cadre de la stratégie usuelle pour résoudre un tel système surdéterminé d'équations, à savoir de calculer une base de Gröbner pour l'ordre grevlex, puis de convertir le résultat en une base de Gröbner pour l'ordre lex par l'algorithme FGLM (voir le paragraphe 5.2.2).

Estimation empirique de la complexité Procédant de la sorte, nous nous retrouvons avec $\frac{n(n-1)}{2} + n + 1 + 2n$ équations quadratiques en $\frac{(D+1)(D+2)}{2} + (D + 2) + 1 + 4n = \frac{D(D+5)}{2} + 4n + 4$ inconnues. D étant de l'ordre de $log(n)$, ce système est surdéterminé. De plus, il peut être intéressant selon la taille de q, de rajouter les équations de corps correspondant à chacune des variables, celles-ci étant toutes dans $\mathbb{K}$. En tout cas, grâce à l'équation (7.7) établie au paragraphe 7.3.3, nous sommes assurés de l'existence d'une solution.

Observation 1 *La complexité empirique de résolution de ce système d'équations est* $\mathcal{O}\left(n^9\right)$.

Explication : C'est l'utilisation de l'algorithme F_4 disponible sous Magma (v2.15-7) [BCP97], pour résoudre ce système pour différents paramètres, qui nous a permis de faire cette observation (les résultats des expériences se trouvent au paragraphe 7.4.2). Lors de l'exécution de l'algorithme, on observe que le degré des polynômes manipulés ne dépasse pas 3. D'après les résultats et suppositions exposés à partie 5.2.2, ceci indique une complexité empirique de $\mathcal{O}\left(n^9\right)$.

Exposons ce que l'on peut dire avec la théorie se rapportant au sujet, exposée au paragraphe 5.2.2.5 du chapitre 5.

Éléments théoriques Donnons quelques éléments théoriques, appuyant l'observation que notre système d'équations peut se résoudre en temps polynomial, bien que le nombre de variables soit plus élevé que ce que supportent les algorithmes actuels de calcul de bases de Gröbner. Ceci s'explique en partie par le fait que le système d'équations est largement surdéterminé.

Conjecture 1 *La complexité de résolution d'un système quadratique aléatoire de même taille que notre système est polynomiale. Le degré de régularité est asymptotiquement* 7.

Explication :
Dans le cas de systèmes réguliers ou semi-réguliers, nous avons vu au chapitre 7.1 que Bardet *et al.* [BFSY05, Bar04] fournissent des développements asymptotiques de l'expression du degré de régularité dans le cas de $\alpha \cdot n$ équations en n variables. Dans notre cas, le système d'équations considéré n'est ni régulier ou semi-régulier, ni formé de $\alpha \cdot n$ équations en n variables.
La pratique montre cependant que le cas de ces systèmes réguliers ou semi-réguliers correspond en quelque sorte à la pire situation, au regard de la complexité de résolution par bases de Gröbner. Par suite, et bien que ceci ne soit pas vraiment justifié, nous utilisons les estimations asymptotiques du degré de régularité rappelées dans le théorème 5 de la sous-section 5.2.2 dans le cas des systèmes réguliers ou semi-réguliers, comme valeur de référence pour le degré de régularité notre système. Avant de pouvoir appliquer le résultat de [BFSY05] à notre système d'équation, il faut encore faire une autre supposition. Nous supposons que les résultats obtenus

pour $\alpha \cdot n$ équations en n variables peuvent s'appliquer dans le cas de βn^2 équations en n variables (en posant $\alpha = \beta n$ et exprimant $\mathrm{D}_{\mathrm{reg}}$ en fonction de β). Le résultat du premier point du théorème 5 s'écrivent alors :

$$\mathrm{D}_{\mathrm{reg}} = \frac{1}{8\beta} - \frac{a_1}{2\beta^{1/3}} - \frac{3}{2} + \mathcal{O}\left(1/n\right), \text{ où } a_1 \simeq 2,33811. \tag{7.11}$$

À présent, appliquons ceci au cas d'un système de $\mathcal{O}\left(\frac{n^2}{2}\right)$ équations en $\mathcal{O}\left(\frac{D^2}{2} + 4n\right)$ inconnues, qui est la taille de notre système. Pour d fixé ou d polynomial [9] en n, on trouve $\beta = 1/32$. L'équation (7.11) indique dans ce cas $\mathrm{D}_{\mathrm{reg}} \simeq 7$.
Ce résultat est un résultat asymptotique et lorsque n est borné, cette estimation n'a plus lieu d'être. Cependant, ceci appuie l'affirmation que la complexité du calcul d'une base de Gröbner devrait être polynomiale. Encore une fois, ceci ne s'applique à notre système que si l'on peut supposer que notre système se comporte comme un système semi-régulier de $\alpha \cdot n$ équations en n inconnues, avec $\alpha = \beta n$.

7.4 Implantation de l'attaque des systèmes HFE utilisant des polynômes secrets de la famille $\mathcal{P}_{\mathbb{K}}$

7.4.1 Pseudo-code de l'attaque

Pour résumer l'attaque et mettre en évidence les différentes étapes, un pseudo-code de l'attaque est donné dans la figure 7.4.

7.4.2 Expériences

Afin d'illustrer l'attaque décrite dans les parties précédentes, nous avons programmé, à l'aide du logiciel de calculs Magma [BCP97], toutes les étapes de l'attaque, de la génération de la clé publique au recouvrement d'une clé secrète efficace.

Les expériences ont été faites sur un ordinateur unicoeur Intel 2.3Ghz Xeon "Nehalem", de 74 Goctets de RAM. Les différents paramètres pour lesquels l'attaque a été réalisée sont décrits dans ce qui suit.

7.4.2.1 Clés faibles générales (ensembles A, B et C de paramètres)

Nous avons commencé par tester l'attaque sur des instances génériques de HFE, dans le sens où les clés ainsi que leur taille sont recommandées (mais l'on s'intéresse aux instances faibles de ces clés). Dans cette configuration et avec les notations utilisées dans tout le chapitre, nous considérons trois ensembles de paramètres, résumés dans la table 7.1 :

– Ensemble **A** de paramètres. Le corps de base est $\mathbb{K} = \mathbb{F}_{256}$. L'extension $\mathbb{L}$ de $\mathbb{K}$ sur laquelle sont définis $\mathbf{f}$, S et T est de degré 32, soit $\mathbb{L} = \mathbb{F}_{2^{256}}$. Le degré de $\mathbf{f}$ est choisi élevé, $\deg(f) = 2^{17} = 131072$.

9. d polynomial en n équivaut à D polynomial en $\log_2(n)$.

FIGURE 7.4 Pseudo-code de l'attaque

Entrée : Une clé publique HFE **PK**, obtenue à partir de la clé secrète $(T, \mathbf{f}, S)$, où $\mathbf{f} \in \mathcal{P}_{\mathbb{K}}$.

Sortie : Une clé secrète équivalente $(T', \mathbf{f}', S')$, avec $\deg \mathbf{f}' \leq \deg \mathbf{f}$.

1: // paragraphe 7.3.1
2: **répéter**
3: Soit (U, V) une solution aléatoire du problème IP : $U \circ \mathbf{PK} = \mathbf{PK} \circ V$.
4: **jusqu'à ce que** U et Fr soient similaires
5: // paragraphe 7.3.2
6: **pour tout** $i_0 \in [1; n-1]$, i_0 premier avec n **faire**
7: Soit $k = {i_0}^{-1} \mod n$.
8: Calculer $\widetilde{S}, \widetilde{T}$ tels que : $Fr = \widetilde{S} \circ V^k \circ \widetilde{S}^{-1} = \widetilde{T}^{-1} \circ U^k \circ \widetilde{T}$.
9: // paragraphe 7.3.3
10: Interpoler $\mathbf{g} = \widetilde{T}^{-1} \circ \mathbf{PK} \circ \widetilde{S}^{-1}$.
11: **si** $\mathbf{g}$ est à coefficients dans $\mathbb{K}$ **alors**
12: // paragraphe 7.3.4
13: Calculer F_1, F_2 et $\mathbf{f}$, tel que $\mathbf{g} \circ F_1 = F_2^{-1} \circ \mathbf{f}$.
14: **retourner** $\left(\widetilde{T} \cdot F_2^{-1}, \mathbf{f}, F_1^{-1} \cdot \widetilde{S}\right)$
15: **fin si**
16: **fin pour**

- Ensemble **B** de paramètres. Le corps de base est le corps à 4 éléments $\mathbb{K} = \mathbb{F}_4$. L'extension $\mathbb{L}$ de $\mathbb{K}$ est une extension de degré 67, $\mathbb{L} = \mathbb{F}_{2^{134}}$. Le degré de $\mathbf{f}$ est toujours 2^{17}.
- Ensemble **C** de paramètres. Cette fois, $\mathbb{K} = \mathbb{F}_2$ et $\mathbb{L} = \mathbb{K}^{97} = \mathbb{F}_{2^{97}}$. Le degré de $\mathbf{f}$ est 2^7.

Remarquons que pour ces trois ensembles de paramètres, les applications S et T sont choisies linéaires plutôt qu'affines. Ce choix sert cependant juste à résoudre plus facilement l'instance IP du début de l'attaque. Nous avons pu voir dans la description complète de l'attaque, que ce choix n'influence pas sur la difficulté du reste de l'attaque. Les mesures de temps obtenues pour chacun de ces trois ensembles de paramètres sont données dans le tableau 7.1 qui suit.

Remarque : Le degré du polynôme interne est toujours choisi beaucoup plus élevé que les paramètres conseillés, et notamment proposés par les challenges HFE. Aucune des attaques existantes sur HFE ne fonctionne en pratique, de près ou de loin, pour des choix de paramètres correspondant aux ensembles **A** ou **B**.

7.4.2.2 La variante "sous-corps" de Patarin (ensembles D et E de paramètres)

Penchons-nous à présent sur la variante dite "sous-corps" de HFE [Pat96]. Rappelons que dans le cas de cette variante, les coefficients des polynômes formant la clé publique **PK** sont dans un sous-corps $\Bbbk$ de $\mathbb{K}$, plutôt que dans $\mathbb{K}$, afin de ré-

Ensemble de paramètres	**A**	**B**	**C**
Taille des blocs (en bits)	256	134	97
q	256	4	2
n	32	67	97
$\deg \mathbf{f}$	131072	131072	128
Coefficients de $\mathbf{f}$ à valeur dans	$\mathbb{F}_{256}$	$\mathbb{F}_4$	$\mathbb{F}_2$
S et T	linéaires	linéaires	linéaires
Coefficients de S et T à valeur dans (représentations matricielles)	$\mathbb{F}_{256}$	$\mathbb{F}_4$	$\mathbb{F}_2$
Nombre de termes de $\mathbf{f}$	10	54	29
Taille de la clé publique (en bits)	143'616	314'364	461'138
IP	polynomial		
Interpolation de $\mathbf{g}$	79s	30 min	140 min
Résolution par bases de Gröbner	7h	1 jour	1 semaine
Variables / Équations	136 / 593	322/4947	423/10028
Mémoire utilisée	2.1Go	45Go	180Go
Changement d'ordre (FGLM)	15s	30 min	4h

TABLE 7.1: Mesures de temps pour les différentes étapes de l'attaque, pour les ensembles de paramètres **A**, **B** et **C**.

duire la taille de la clé publique. Pour générer une telle clé publique, S, T, ainsi que le polynôme de définition de l'extension $\mathbb{L}$ de $\mathbb{K}$ doivent être choisis à coefficients dans $\Bbbk$ plutôt que $\mathbb{K}$, et $\mathbf{f}$ à coefficients dans $\Bbbk$ au lieu de $\mathbb{L}$ (voir [Pat96]). Un tel polynôme $\mathbf{f}$ appartient donc bien à la famille $\mathcal{P}_{\mathbb{K}}$ faisant l'objet de notre attaque, puisque $\Bbbk \subset \mathbb{K}$.

Pour cette variante, nous allons considérer deux nouveaux ensembles de paramètres, résumés dans la table 7.2 :

- Ensemble **D** de paramètres. Le corps $\mathbb{K}$ est $\mathbb{F}_{256}$, l'extension $\mathbb{L}$ où sont définis $\mathbf{f}$, S et T est $\mathbb{K}^{29} = \mathbb{F}_{2^{232}}$. Toutes les applications sont à coefficients dans $k = \mathbb{F}_2 \subset \mathbb{K}$. Le degré de $\mathbf{f}$ est de 2^{17}, S et T ne font pas l'objet de restrictions particulières.
- Ensemble **E** de paramètres. $\mathbb{K} = \mathbb{F}_{16}$, $\mathbb{L} = \mathbb{K}^{59} = \mathbb{F}_{2^{236}}$. Le polynôme $\mathbf{f}$ est de degré 2^{17} et à coefficients dans $k = \mathbb{F}_2$, tout comme les applications affines S et T.

Les paramètres proposés par Patarin pour cette version sous-corps sont ceux donnés dans l'ensemble D. Choisir $\mathbb{K} = \mathbb{F}_{256}$ et $\Bbbk = \mathbb{F}_2$, permet de réduire la taille de la clé publique d'un facteur 8. Notons que les paramètres suggérés dans l'ensemble E sont deux fois plus grands que ceux suggérés en pratique, illustrant l'efficacité de l'attaque mise en oeuvre. Remarquons encore que S et T sont affines dans cette variante, de sorte que la résolution du problème IP ne se fait pas en temps polynomial (voir sous-section 5.2.3). Toutes les mesures de temps figurent dans le tableau 7.2

ci-dessous.

Remarque : Afin d'avoir une réduction effective de la clé publique, $\mathbb{K}$ doit être relativement gros en comparaison à $\Bbbk$. Ceci implique des restrictions sur la taille de D, afin que le déchiffrement reste praticable par le détenteur de la clé secrète. Cependant, choisir D petit réduit l'entropie du polynôme interne $\mathbf{f}$. Une attaque naturelle pour ce type d'instances consiste à deviner $\mathbf{f}$, puis résoudre le problème IP pour retrouver S et T. Comparons cette attaque simple avec la nouvelle attaque présentée plus haut (et issue de [BFJT09]). Notons aussi que cette attaque, bien que naturelle, n'a pas été notée avant [BFJT09].

– Ensemble **D** de paramètres. Pour assurer un déchiffrement efficace au détenteur légitime de la clé secrète, le paramètre D tel que $d = 2 \cdot q^D$ doit être choisi égal à 2 (pour un déchiffrement pouvant prendre jusqu'à quatre minutes sur nos machines). Le polynôme interne a au plus dix termes, dont les coefficients sont dans $\mathbb{F}_2$. L'attaque intuitive mentionnée nécessite alors la résolution de 2^{10} instances affines du problème IP, avec des paramètres $q = 2$ et $n = 29$. La complexité de cette attaque est alors de l'ordre de 2^{68}, ce qui signifie que cette instance de HFE est cassée avec les techniques déjà existantes. Cependant, notre attaque nécessite dans ce cas moins d'une minute pour aboutir.
– Ensemble **E** de paramètres. Le polynôme interne a cette fois 21 termes (on a toujours que le degré de $\mathbf{f}$ est 131072, mais q cette fois vaut 16, donc $D = 4$). Pour chacun des 2^{21} possibilités pour $\mathbf{f}$, dans le cas de l'attaque mentionnée, l'attaquant doit résoudre un problème IP avec $q = 2$ et $n = 59$. Selon les résultats annoncés pour IP au paragraphe 5.2.3, résoudre une telle instance IP a une complexité de l'ordre de 2^{59} (et nécessite environ cinq semaines de temps), pour une complexité finale d'attaque de l'ordre de 2^{80}. L'attaque consistant à deviner $\mathbf{f}$ et résoudre l'instance IP mentionnée plus haut, ne permet donc pas de casser HFE pour cet ensemble **E** de paramètres. Dans le cas de notre attaque, nous avons besoin de cinq semaines pour la résolution initiale de l'instance d'IP (étape du paragraphe 7.3.1), plus quatre heures pour terminer l'attaque une fois en possession d'une solution de ce problème IP.

7.5 Conclusion

Pour la famille d'instances spéciales traitées dans ce chapitre, nous avons montré qu'il existe un isomorphisme non trivial entre la clé publique et elle-même. De plus, retrouver cet isomorphisme permet de monter une attaque menant au recouvrement en pratique des éléments secrets de la clé utilisée ou d'une clé privée permettant de déchiffrer aussi efficacement que l'utilisateur légitime.

Ensemble de paramètres	**D**	**E**
Taille des blocs (en bits)	232	236
q	256	16
n	29	59
$\deg \mathbf{f}$	131072	131072
Coefficients de $\mathbf{f}$ à valeur dans	$\mathbb{F}_2$	$\mathbb{F}_2$
S et T	affine	affine
Coefficients de S et T à valeur dans (représentations matricielles)	$\mathbb{F}_2$	$\mathbb{F}_2$
Nombre de termes de $\mathbf{f}$	10	21
Taille de la clé publique (en bits)	13'485	107'970
IP	$\approx$ 1s	$\approx$ 5 semaines
Interpolation de $\mathbf{g}$	51s	23min
Résolution par bases de Gröbner	45s	3h
Variables / Équations	124 / 494	253 / 1889
Mémoire utilisée	350Mo	13.9Go
Changement d'ordre (FGLM)	0s	30s

TABLE 7.2: Mesures de temps pour les différentes étapes de l'attaque, pour les ensembles de paramètres **D** et **E**.

Chapitre 8

Conclusions et Perspectives

8.1 Contributions et conclusions

Deux branches de la cryptologie ont été abordées durant cette thèse. D'une part, nous nous sommes inétressés à l'étude générique de la sécurité des schémas de Feistel avec permutations internes et des schémas du type Misty. D'autre part, nous avons réalisé des cryptanalyses de cryptosystèmes multivariés.

Les schémas de Feistel ou encore les constructions du type Misty sont des briques de base pour les concepteurs en cryptologie symétrique.
Les schémas de Feistel classiques, *i.e.* balancés et avec fonctions internes, ont fait l'objet de nombreuses études. Cependant, l'utilisation de permutations internes plutôt que de fonctions intervient dans de nombreux algorithmes. Il existe en effet des exemples d'attaques fonctionnant pour le cas de fonctions internes présentant de mauvaises propriétés de surjectivité [RPW97]. Pourtant, cette structure a fait l'objet de moins d'études que sa version classique. Nous avons tout d'abord montré que des différences existent du fait de l'utilisation de permutations au lieu de fonctions et que de fait, on ne peut se contenter d'adapter les résultats sur les schémas de Feistel classiques. Nos résultats concernant ce schéma se trouvent dans [TP09] et ont fait l'objet d'une acceptation à la session poster d'Eurocrypt 2009 ainsi que d'une publication à la conférence internationale Africacrypt 2009. Dans cet article, nous exposons les meilleures attaques génériques contre les schémas de Feistel avec permutations internes. Par génériques nous entendons que les permutations internes utilisées sont supposées aléatoires, ce qui permet de concentrer l'étude sur le schéma en lui-même et non sur son contexte d'utilisation. Nous nous sommes principalement concentrés pour ce schéma aux attaques deux points, *i.e.* des attaques exploitant des corrélations entre des paires de messages distincts, que nous pouvons réaliser pour n'importe quel nombre de tours. Nous prouvons par l'utilisation des coefficients H [Pat91] que les complexités obtenues sont les meilleurs possibles pour ce type d'attaques. Nous avons ainsi pu comparer les meilleures attaques génériques contre les schémas de Feistel avec permutations internes avec celles contre les schémas de Feistel classiques. Nous avons mis en évidence que certaines différences apparaissent tous les trois tours au niveau des complexités des attaques, mais que ces complexités sont proches. Ce résultat n'était pas prévisible et l'étude indépendante de cette structure était nécessaire pour l'établissement de ce résultat. Nous ne nous sommes pas concentrés sur des preuves de sécurité, ainsi, de meilleures attaques peuvent encore être découvertes, mais ces résultats génériques sont les seuls connus sur ces schémas et devront dorénavant être pris en compte dans la conception d'algorithmes

utilisant cette structure. En particulier, au moins six tours de schémas de Feistel avec permutations internes doivent être utilisés pour éviter les attaques génériques. Les schémas utilisés dans Misty, ont eux fait l'objet de plusieurs études, vu qu'ils sont notamment à la base du schéma de chiffrement par blocs KASUMI, utilisé dans les téléphones portables troisième génération. Dans [NPT10], nous nous sommes intéressés aux attaques génériques sur les schémas appelés Misty L. Cet article a fait l'objet d'une publication dans la conférence internationale Latincrypt 2010. Nous fournissons tout d'abord les meilleures attaques génériques précédemment connues ou nouvelles pour les premiers tours de ces schémas. Notamment, nous exposons des attaques deux points, trois points ou quatre points sur les schémas Misty L. Lorsque le nombre de tours dépasse six, nous nous sommes restreints à l'étude des attaques deux points uniquement, tout comme dans [TP09]. L'utilisation des coefficients H nous a permis d'exposer les meilleures complexités d'attaques deux points. Un tableau récapitulatif permet de servir de référence quant au nombre de tours à utiliser pour éviter les meilleures attaques génériques connues. Pour cette structure, comme pour les schémas de Feistel avec permutations internes, nous nous sommes contentés d'étudier les attaques génériques, non pas les preuves de sécurité. Par conséquent, de meilleures attaques génériques peuvent encore être découvertes. Cependant, pour le moment, au moins six tours de Misty L doivent être utilisés pour éviter les meilleures attaques génériques connues.

Quant à la cryptologie assymétrique, nos résultats concernent des cryptanalyses des schémas HM et HFE.
Le schéma HM a été proposé en 1998 par Patarin *et al.* à Asiacrypt [PCG98a]. HM est proposé comme remplaçant du schéma [C] conçu par Matsumoto et Imai [IM85]. L'application à la base de ce schéma est une fonction de l'espace des matrices de taille n dans lui-même. Dans le papier original, Patarin *et al.* mettent en évidence une propriété qui leur semble être mauvaise pour le schéma proposé, sans pouvoir toutefois l'exploiter. Ce schéma n'a pas pourtant pas fait l'objet de cryptanalyse depuis, et des versions perturbées ont été proposées par Ding [WDGY05]. Nous montons deux types d'attaque, une attaque fournissant un distingueur entre la clé publique de HM et un système aléatoire d'équations, et une autre attaque permettant l'inversion du système formant la clé publique (qui peut elle aussi être vue comme un distingueur). Cette cryptanalyse fait l'objet d'une publication [FJPT10] dans la conférence internationale Latincrypt 2010. Le premier distingueur mis en évidence se base sur une propriété de la différentielle de la clé publique : nous montrons dans [FJPT10] que la résolution du système linéaire correspondant à la différentielle de la clé publique prise en un point a un ensemble de solutions beaucoup plus grand que l'ensemble de solutions attendu pour des équations aléatoires. Le deuxième distingueur correspond à une inversion de la clé publique par l'utilisation de bases de Gröbner. Nous montrons l'apparition de nombreuses équations de bas degré lors du calcul d'une base de Gröbner de l'idéal engendré par le système d'équations de la clé publique. Ces nouvelles équations permettent de justifier en partie les observations expérimentales indiquant que le degré de régularité, qui est un élément clé dans l'évaluation de la complexité correspondant à un calcul de base de Gröbner, est anormalement bas.

Ces deux attaques montrent que l'utilisation de HM est à proscrire, de même qu'une des versions perturbées de ce schéma.
Le schéma HFE est un des descendants direct du premier schéma multivarié C*, proposé par Matsumoto et Imai à Eurocrypt en 1988 [MI88]. Une cryptanalyse de C* réalisée par Patarin presque dix ans suivant sa publication [Pat95] l'a invité à proposer le schéma HFE [Pat96], qui est une adaptation de C* permettant d'éviter son attaque. De nombreuses cryptanalyses ont été proposées, offrant pour les meilleures une complexité quasi-polynômiale [GJS06, DGF06]. Les attaques en question sont d'une part une attaque utilisant les bases de Gröbner pour inverser le système formant la clé publique de HFE, accompagnée d'explications théoriques concernant la complexité de cette attaque, d'autre part une attaque se basant sur le rang de la différentielle de la clé publique et fournissant un distingueur entre le système formée par la clé publique et un système aléatoire d'équations. Dans [BFJT09], nous proposons une attaque permettant le recouvrement de la clé privée. Le résultat [BFJT09] a été publié au workshop SCC 2010 et fait l'objet d'une soumission comme article de journal, à savoir le Journal of Mathematical Cryptology. Notre attaque ne s'applique que sur une famille particulière d'instances de HFE, à savoir les polynômes HFE à coefficient dans $\mathbb{K}$ et lorsque S et T permettent une résolution du problème IP associé, et ne remet pas en question la sécurité globale de HFE. Cependant, cette attaque montre qu'il faut être un peu précautionneux lors du choix des paramètres. Notre attaque se sert de propriétés de commutativité vérifiés par le polynôme interne, comme l'attaque sur SFLASH [DFSS07], et permet un recouvrement en temps polynômial des secrets sous les hypothèses évoquées plus haut. En l'occurence nous atteignons, dans notre configuration, des recouvrements de clés pour des tailles de paramètres qu'aucune des attaques existantes ne permettait précédemment. Cette attaque montre également que la tentation de choisir des applications à coefficients dans un sous-corps afin de réduire la taille de la clé publique n'est pas une bonne initiative, comme l'ont déjà montré des attaques sur d'autres "versions sous-corps" de schémas multivariés [GM02, BWP05].

8.2 Perspectives

Concernant les sujets abordés au cours de cette thèse, plusieurs voies restent à investiguer, et des questions restent ouvertes.

Pour ce qui est des attaques génériques, un résultat qu'il serait intéressant d'obtenir, pour les attaques trois points ou quatre points par exemple, est le même genre de généralisation que l'on a développé pour les attaques deux points. Ceci permettrait d'avoir un idée plus claire concernant le type d'attaques auxquelles il faut s'intéresser encore et celles pour lesquelles la généralisation permet de conclure que les meilleures possibles ont été obtenues.
Une autre voie d'investigation serait, plutôt que de passer en revue toutes les attaques possibles, de trouver un moyen de décider le(s) type(s) d'attaques fournissant les meilleures complexités, pour un schéma donné. Il semblerait que pour les schémas

de Feistel, les attaques deux points fournissent les meilleures complexités (après un certain nombre de tours) d'attaques génériques, mais ceci n'est pas prouvé. Cela reste une question complètement ouverte pour d'autres schémas également, notamment les schémas du type Misty, pour lesquelles on a vu que l'on n'a pas une dominance aussi forte des attaques deux points comme meilleures attaques génériques, du moins pour les tours pour lesquels l'on a pu étudier différents types d'attaque.

Pour ce qui est des cryptanalyses proposées du schéma HM et du schéma HFE, il reste une marge de perfection. Par exemple, on peut essayer de réaliser une attaque par recouvrement de clé sur HM, souvent plus intéressante que la simple inversion. Cependant, ce schéma n'était déjà initialement pas vraiment recommandé par ses concepteurs, et, notre attaque permettant de monter une inversion en temps polynômial du système formé par la clé publique, il ne semble pas vraiment utile (si ce n'est pour l'introduction d'éventuelles nouvelles techniques) de continuer à chercher des attaques sur ce schéma. Le cas de HFE est plus complexe. Notre attaque ne s'étend en aucun cas à une classe de clés faibles plus grande, car la propriété de commutativité sur laquelle elle est basée ne fonctionne pas pour d'autres instances. Par contre, on peut se demander s'il ne serait pas possible de terminer cette attaque en se défaisant du calcul de base de Gröbner final, ce qui permettrait à cette attaque de ne vraiment utiliser que des propriétés mathématiques des objets impliqués. On peut aussi se demander s'il n'existe pas d'autres propriétés mathématiques non encore remarquées, sur HFE ou d'autres schémas multivariés (et qui pourraient éventuellement s'appliquer aux versions plus résistantes, par exemple les versions "moins"). De telles attaques pourraient mener à des cryptanalyses plus théoriques et sans doute permettre de mieux comprendre ce qui fait défaut au niveau de la conception.

Quant à la discipline de la cryptologie asymétrique multivariée en elle-même, le gros engouement qu'elle a créé lors de son apparition dans les années 1980, s'est beaucoup tempéré avec la multiplication des attaques sur les schémas proposés. Il semblerait pourtant qu'après chacune des attaques proposées, il soit possible de trouver une manière de modifier légèrement le schéma pour parer à ces attaques, ce qui peut paraître une force aux yeux de certains, mais induit une perte de confiance en ces schémas pour d'autres. Le problème MQ est pourtant un problème intéressant sur lequel il est légitime de baser les schémas cryptographiques. Un exemple d'utilisation adroite de ce problème se trouve dans le domaine de la cryptologie symétrique, avec l'algorithme QUAD [BGP06]. Par ailleurs, du côté de la cryptologie asymétrique, il reste encore le schéma UOV [KPG99] qui a été épargné par la vague de cryptanalyses récentes. Ceci montre qu'en se servant autrement de ce problème ou en s'éloignant un peu de la construction classique de schémas multivariés, on peut espérer continuer à travailler en cryptologie multivariée.

Annexe A

Calcul des Coefficients H

Dans la formule pour les coefficients H du théorème 1 de la section 3.5 interviennent les suites possibles de relations entre les blocs successifs apparaissant au cours de l'évaluations de ψ^k, correspondant aux deux entrées/sorties. Ce sont les séquences $\mathcal{R}$, cf. paragraphe 3.5.1.2. De $\mathcal{R}$ dépendent les autres éléments impliqués dans la formule.

Pour trouver la formule exacte, nous pouvons commencer par chercher toutes les séquences $\mathcal{R}$ possibles pour deux entrées/sorties données. Ensuite, pour chacune de ces séquences, nous pouvons évaluer le produit $N(d_1)\cdots N(d_{k-2})$, où d_i est la valeur de $X_1^i \oplus X_2^i$ et $N(d_i)$ le nombre de valeurs possibles pour d_i.

Dans les sections A.1 et A.2, nous commençons par voir quelles sont les implications sur les blocs voisins des relations que l'on peut avoir entre deux blocs (sous-section A.1.1). Ceci permet de mieux cibler les possibilités de séquences $\mathcal{R}$, et d'évaluer les produit $N(d_1)\cdots N(d_{k-2})$ pour $\mathcal{R}$ donné (sous-section A.1.2). Une fois balayés tous les cas de paires d'entrées/sorties, nous déduisons une formule finale pour les coefficients H (sous-section A.1.3, théorème 7).

Aux sections A.3 et A.4, nous nous focalisons sur l'obtention des coefficients H par récurrence.

Sommaire

A.1 Calcul des Coefficients H pour les schémas du type Misty, Méthode directe

A.1.1 Restrictions sur les relations $\mathcal{R}$ entre les blocs

Soient $[L_1, R_1]/[S_1, T_1]$ et $[L_2, R_2]/[S_2, T_2]$ deux entrées/sorties distinctes de k tours de schémas du type Misty, On s'intéresse aux différentes séquences de relations $\mathcal{R}$ entre les blocs internes correspondant à ces deux entrées/sorties (voir le paragraphe 3.5.1.2 du chapitre 3). Afin de voir quelles restrictions sont imposées par le schéma, regardons à nouveau la figure A.1.

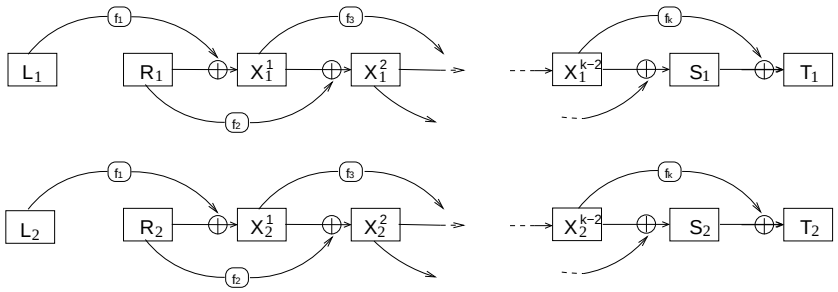

FIGURE A.1: $M_L^k(f_1, \ldots, f_k)([L_1, R_1]) = [S_1, T_1]$, $M_L^k(f_1, \ldots, f_k)([L_2, R_2]) = [S_2, T_2]$

On voit qu'il y a certaines contraintes pour les séquences $\mathcal{R}$ de relations entre les blocs valides :

1. Si $\mathcal{R}_i$ est le symbole $=$ (autrement dit, si $X_1^i = X_2^i$), alors $\mathcal{R}_{i+1}, \mathcal{R}_{i+2}$ correspondent au symbole $\neq$ (de même que $\mathcal{R}_{i-1}$ et $\mathcal{R}_{i-2}$).
   Raisonnons sur les blocs suivant X^i. On a $X^{i+2} = f_{i+2}(X^i) \oplus X^{i+1}$. $X_1^i = X_2^i$ implique alors que $X_1^{i+2} \oplus X_2^{i+2} = X_1^{i+1} \oplus X_2^{i+1}$. Ainsi, l'égalité $X_1^{i+1} = X_2^{i+1}$ équivaut à $X_1^{i+2} = X_2^{i+2}$. Il en résulte que tous les blocs, des blocs d'entrée aux blocs de sortie, sont égaux, ce qui est impossible par le choix des entrées/sorties distinctes dans le cadre des attaques deux points. Pour les blocs précédents, on a $X^i = f_i(X^{i-2}) \oplus X^{i-1}$ et ici encore, cette fois par bijectivité de f_i, $X_1^i = X_2^i$ implique $X_1^{i-1} = X_2^{i-1} \Leftrightarrow X_1^{i-2} = X_2^{i-2}$. De telles égalités consécutives entre les blocs impliquent des égalité entre chacun des blocs, ce qui est impossible par choix des messages d'entrées/sorties distincts.
2. Il y a aussi des contraintes sur les d_i : $d_i = 0 \Leftrightarrow d_{i+1} = d_{i+2}$ (et d_{i+1} peut prendre toutes les valeurs non nulles).

L'égalité entre d_i et d_{i+1} provient de la définition même des blocs : $X^{i+2} = f_{i+2}(X^i) \oplus X^{i+1}$ ($d_i = 0$ signifie $X_1^i = X_2^i$). Alors, d_{i+1} est simplement défini comme $f_{i+1}(X_1^{i-2}) \oplus f_{i+1}(X_2^{i-2})$. Or, nous avons $X_1^{i-2} \neq X_2^{i-2}$, pour les raisons énoncées plus haut. Ainsi, d_{i+1} peut prendre n'importe quelle valeur non nulle.

Ces contraintes impliquent différentes séquences $\mathcal{R}$ possibles, selon les conditions initiales $\mathcal{R}_{-1}, \mathcal{R}_0, \mathcal{R}_{k-1}, \mathcal{R}_k$, et $d_{-1}, d_0, d_{k-1}, d_{k-2}$. Et en fait, les séquences $\mathcal{R}$ possibles ne dépendent que de ces conditions initiales. Par suite, on a le résultat déjà annoncé au chapitre 3 :

Théorème 6 *Les coefficients H de deux entrées/sorties distinctes $[L_1, R_1]/[S_1, T_1]$ et $[L_2, R_2]/[S_2, T_2]$ ne dépendent que des relations entre les blocs d'entrée et de sorties de ces deux messages.*

A.1.2 Séquences $\mathcal{R}$ possibles et produit des $N(d_i)$, $i = 1 \ldots k-2$

Dans cette partie, notons $A_{X^{i_1}, X^{i_2}}$ le nombre de relations d'égalités dans une séquence $\mathcal{R}$, correspondant à la relation entre deux blocs X_1^i et X_2^i, $i_1 < i < i_2$. Lorsque $i_1 = 0$ et $i_2 = k-1$, on pourra noter simplement A, car cet intervalle correspond aux relations non fixées par les blocs initiaux d'entrée et de sortie. Nous nous intéressons au nombre de séquences $\mathcal{R}$ comportant $A = A_{X^0, X^{k-1}}$ symboles $=$, ainsi qu'à la valeur du produit $N(d_1) \cdots N(d_{k-2})$. Ces deux éléments permettront d'établir des formules pour les coefficients H (sous-section A.1.3).

Intuitivement, et de manière très informelle, pour une séquence $\mathcal{R} \in \{=, \neq\}^k$, comportant A éléments correspondant au symbole $=$, le produit des $N(d_i), 1 \leq i \leq k-2$, devrait se rapprocher de la formule suivante :

$$\prod_{i=1}^{k-2} N(d_i) = 1^A \cdot (2^n - 1)^A \cdot 1^A \cdot (2^n - 2)^{k-2-3A}.$$

La raison pour cela est que chaque symbole $= \mathcal{R}_i$ de $\mathcal{R}$, force la valeur correspondante de d_i à valoir 0. D'après les propriétés mises en évidence à la sous-section A.1.1, d_{i+1} peut alors prendre toutes les valeurs non nulles et $d_{i+2} = d_{i+1}$. Pour les d_i restants, toutes les valeurs non nulles et différentes de d_{i-1} sont plus ou moins susceptibles d'être prises. Pour obtenir une formule précise, il faut cependant regarder en détail chaque cas, qui est l'objet des lemmes ci-dessous.
Remarque : Dans les formules des lemmes suivants, notamment dans l'expression de $N(d_1) \cdots N(d_k)$, certains exposants peuvent être négatifs, lorsque le nombre de tours k considéré est petit, typiquement $k = 1, 2$ ou 3.

Lemme 4 (cas $L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, S_1 \oplus S_2 = T_1 \oplus T_2$) *Dans ce cas, le nombre de séquences $\mathcal{R}$ dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$ est :*

$$\binom{k-2-2A}{A-1}.$$

Supposons fixée une séquence $\mathcal{R}$. Alors, le produit $N(d_1) \cdots N(d_{k-2})$ vaut :

i) *Si* $A > 0$ *:* $(2^n-1)^{A-1} \cdot (2^n-2)^{k-2-3A+1}$.

ii) *Si* $A = 0$ *:* $\sum_{j=0}^{\frac{k-3-\alpha}{2}} (2^n-2)^{j+\alpha}(2^n-3)^{k-3-\alpha-2j}\binom{k-3-\alpha-j}{j}$, *où* $\alpha = 1$ *si* $R_1 \oplus R_2 = S_1 \oplus S_2$, *0 sinon.*

Démonstration : Pour la partie du lemme concernant le nombre de séquences possibles avec A symboles $=$, comme $S_1 \oplus S_2 = T_1 \oplus T_2$, alors nécessairement, $\mathcal{R}_{k-2}$ est le symbole $=$. De plus, comme $L_1 = L_2$, nous avons que $\mathcal{R}_1$ est le symbole $\neq$. Il reste à fixer $A-1$ séquences de trois symboles $(=, \neq, \neq)$ dans la séquence $(\mathcal{R}_2, \ldots, \mathcal{R}_{k-3}$. La formule est donc $\binom{k-2-2-2(A-1)}{A-1}$, comme annoncé.
Concernant le produit des $N(d_i)$:

i) Si $A > 0$. L'égalité $L_1 = L_2$ implique $d_1 = R_1 \oplus R_2$. Soit $\mathcal{R}_{i_A}$ le dernier symbole $=$ de $\mathcal{R}$. Alors, pour $2 \leq i \leq i_A - 1$, si $\mathcal{R}_i$ est le symbole $=$, $d_i = 0$, et $d_{i+1} = d_{i+2}$ peuvent prendre $2^n - 1$ valeurs. Ensuite, comme $S_1 \oplus S_2 = T_1 \oplus T_2$, $i_A = k-2$, $d_{k-2} = 0$ et les d_i restant peuvent prendre $(2^n - 2)$ valeurs. On a dans ce cas : $N(d_1) \cdots N(d_{k-2}) = 1 \cdot 1^A \cdot (2^n-1)^{A-1} \cdot (2^n-2)^{k-2-1-3(A-1)-1}$, qui correspond à la formule annoncée.

ii) Supposons $A = 0$. Nous avons toujours $d_1 = R_1 \oplus R_2$. Pour obtenir la formule, nous sommons sur le nombre de d_i, $1 \leq i \leq k-2$, pouvant valoir $d_{k-1} = S_1 \oplus S_2$. Remarquons que pour tout d_i tel que $d_i = d_{k-1}$, d_{i+1} est différent de 0 et de d_{k-1}. Les d_i restant doivent être différents de d_{k-1}, de 0 et de d_{i-1}. Notons aussi que si $R_1 \oplus R_2 = d_{k-1}$, $j \geq 1$. S'il y a un nombre j de d_i valant d_{k-1}, alors le produit $N(d_1) \ldots N(d_{k-2})$ est $1^j(2^n-2)^j(2^n-3)^{k-2-2j}$. En multipliant cette valeur par le nombre de possibilités d'avoir j d_i valant d_{k-1}, puis en sommant sur j, on obtient, dans le cas où $R_1 \oplus R_2 = S_1 \oplus S_2$: $\sum_{j=1}^{\frac{k-1}{2}} (2^n-2)^j(2^n-3)^{k-2-2j}\binom{k-2-j-1}{j-1}$. Si $R_1 \oplus R_2 \neq S_1 \oplus S_2$, on obtient : $\sum_{j=0}^{\frac{k-2}{2}} (2^n-2)^j(2^n-3)^{k-2-2j}\binom{k-2-j-1}{j}$. Un changement de variable dans la première de ces deux formules permet d'obtenir la formule de l'énoncé.

□

Lemme 5 (cas $L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, S_1 \oplus T_1 \neq S_2 \oplus T_2$**)** *Le nombre de séquences* $\mathcal{R}$ *dont un nombre* A *d'éléments d'indice* i, $1 \leq i \leq k-2$, *correspondent au symbole* $=$, *est :*

$$\binom{k-2-2A}{A}.$$

Soit une telle séquence $\mathcal{R}$ *fixée. Le produit* $N(d_1) \cdots N(d_{k-2}$ *vaut :*

i) *Si* $A > 0$ *:* $(2^n-1)^{A-1} \cdot (2^n-2)^{k-2-3A}$.

ii) *Si* $A = 0$ *:* $\sum_{j=0}^{\frac{k-2-\alpha}{2}} (2^n-2)^{j+\alpha}(2^n-3)^{k-2-\alpha-2j}\binom{k-2-\alpha-j}{j}$, *où* $\alpha = 1$ *si* $R_1 \oplus R_2 = S_1 \oplus S_2$, *0 sinon.*

Démonstration : Il y a A symboles $=$ à fixer, dans la séquence $\mathcal{R}$ (rappelons que $\mathcal{R}_{-1}, \mathcal{R}_0, \mathcal{R}_{k-1}, \mathcal{R}_k$ sont fixés). Comme remarqué au paragraphe 2.12, un symbole $=$ dans cette séquence est forcément suivi (et précédé) de deux symboles $\neq$. Comme $L_1 = L_2$, alors nécessairement $\mathcal{R}_1$ est le symbole $\neq$. Comme $S_1 \oplus T_1 \neq S_2 \oplus T_2$, on a aussi nécessairement que $\mathcal{R}_{k-2}$ est le symbole $\neq$. Prenant ceci en compte et les contraintes du paragraphe 2.12, fixer A symboles $=$ dans $(\mathcal{R}_1, \ldots, \mathcal{R}_{k-2})$, revient alors à fixer A suites de trois symboles $(=, \neq, \neq)$ sur la sous-séquence $(\mathcal{R}_2, \ldots \mathcal{R}_{k-1})$ de $\mathcal{R}$. Ainsi, trouver une séquence $\mathcal{R}$ comme voulu, revient à trouver A places pour trois symboles consécutifs, dans une suite de symboles de longueur $k-2$. Le nombre de possibilités est bien $\binom{k-2-2A}{A}$.
Pour ce qui est du produit des $N(d_i)$:

i) Soit $A > 0$, notons $\mathcal{R}_{i_1}, \ldots \mathcal{R}_{i_A}$ les éléments de $\mathcal{R}$ correspondant au symbole $=$. L'égalité $L_1 = L_2$ implique $d_1 = R_1 \oplus R_2$. Pour $2 \leq i \leq i_l - 1$, si $\mathcal{R}_i$ est le symbole $=$, $d_i = 0$, et $d_{i+1} = d_{i+2}$ peuvent prendre $2^n - 1$ valeurs. Ensuite, $S_1 \oplus S_2 \neq T_1 \oplus T_2$, donc $i_\alpha < k-2$. Ainsi, $d_{i_A} = 0$, et d_{i_A+1} est fixée à la valeur d_{i_A+2}. Maintenant, soit $i_A + 2 = k-1$, $d_{i_A+1} = S_1 \oplus S_2$ et les d_i restant peuvent prendre $2^n - 2$ valeurs. Soit $i_A + 2 < k - 1$et $d_{i_A=2}$ peut prendre $2^n - 2$ valeurs, tout comme les d_i restant. On déduit $N(d_1) \cdots N(d_{k-2}) = 1 \cdot 1^A \cdot (2^n - 1)^{A-1} \cdot (2^n - 2)^{k-2-1-3(A-1)-2}$, qui correspond à la formule du lemme.

ii) La formule est similaire à celle du lemme 4. La démonstration est encore la même que celle des points *ii)* de ces deux lemmes, car $S_1 \oplus S_2 = T_1 \oplus T_2$ n'influence pas.

□

Lemme 6 (cas $L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, S_1 \oplus S_2 = T_1 \oplus T_2$) *Dans ce cas, le nombre de séquences $\mathcal{R}$ dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$, dépend de la relation entre $S_1 \oplus S_2$ et $T_1 \oplus T_2$:*

i) Si $S_1 \oplus S_2 = T_1 \oplus T_2$: $\binom{k-3-2(A-1)}{A-1}$.

ii) Si $S_1 \oplus S_2 \neq T_1 \oplus T_2$: $\binom{k-1-2A}{A}$.

Soit $\mathcal{R}$ une telle séquence fixée. Alors, le produit $N(d_1) \cdots N(d_{k-2}$ vaut :

i) Si $A \geq 1$: $(2^n - 1)^{A-1} \cdot (2^n - 2)^{k-1-3A+\beta}$, où $\beta = 1$ si $S_1 \oplus S_2 = T_1 \oplus T_2$, 0 sinon.

ii) Si $A = 0$: $\sum_{j=0}^{\frac{k-2-\alpha}{2}} (2^n-2)^{j+\alpha}(2^n-3)^{k-2-\alpha-2j}\binom{k-2-\alpha-j}{j}$, où $\alpha = 1$ si $R_1 \oplus R_2 = S_1 \oplus S_2$, 0 sinon.

Démonstration : Pour ce qui est du nombre de séquences, comme $S_1 \oplus S_2 = T_1 \oplus T_2$, alors nécessairement $\mathcal{R}_{k-2}$ est le symbole $=$. Il reste à fixer $A-1$ séquences de trois symboles $(=, \neq, \neq)$ dans la séquence $\mathcal{R}_1, \ldots, \mathcal{R}_{k-3}$. La première formule est donc $\binom{k-2-1-2(A-1)}{A-1}$, comme annoncé.
Pour ce qui est du produit des $N(d_i)$:

i) Supposons que $\mathcal{R}_{i_1}, \ldots, \mathcal{R}_{i_A}$ correspondent au symbole $=$ ($\alpha \geq 1$). Pour tout $1 \leq i \leq i_A - 1$, si $\mathcal{R}_i$ est le symbole $=$, $d_i = 0$, et $d_{i+1} = d_{i+2}$ peuvent prendre $2^n - 1$ valeurs. Ensuite, comme $S_1 \oplus S_2 = T_1 \oplus T_2$, $i_l = k - 2$, on a $d_{k-2} = 0$ et les d_i restant peuvent prendre $(2^n - 2)$ valeurs. On a : $N(d_1) \cdots N(d_{k-2}) = 1^A \cdot (2^n - 1)^{A-1} \cdot (2^n - 2)^{k-2-3(A-1)-1}$, qui correspond à la formule annoncée.

ii) Pour ce deuxième point, la formule annoncée est la même que dans le lemme 11. On pourra se référer au point *ii)* de la démonstration du lemme 4 dans ce cas.

□

Lemme 7 (cas $L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, S_1 \oplus S_2 \neq T_1 \oplus T_2$) *Dans ce cas, le nombre de séquences $\mathcal{R}$ dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$, est :*

$$\binom{k-1-2A}{A}.$$

Supposons une séquence R fixée. Alors, le produit $N(d_1) \cdots N(d_{k-2})$ vaut :

i) Si $A > 0$:

$$(2^n - 1)^{A-1} \cdot (2^n - 2)^{k-1-3A}.$$

ii) Si $A = 0$: $\sum_{j=0}^{\frac{k-3-\alpha}{2}} (2^n-2)^{j+\alpha}(2^n-3)^{k-3-\alpha-2j}\binom{k-3-\alpha-j}{j}$, où $\alpha = 1$ si $R_1 \oplus R_2 = S_1 \oplus S_2$, 0 sinon.

Démonstration : Commençons par la partie du lemme concernant le nombre de séquences. Il faut fixer A symboles $=$ dans la séquence $\mathcal{R}$, donc A séquences de trois symboles $(=, \neq, \neq)$ dans la sous-séquence $\mathcal{R}_1, \ldots \mathcal{R}_{k-1})$ (on inclut $\mathcal{R}_{k-1}$ car $S_1 \oplus S_2 \neq T_1 \oplus T_2$ implique que $\mathcal{R}_{k-2}$ est le symbole $\neq$, et $\mathcal{R}_{k-3}$ peut être $=$ ou $\neq$). Autrement dit, il faut trouver A places dans une séquence de longueur $k-1$, pour une suite de trois symboles consécutifs. La formule s'en déduit.
Concernant le produit $N(d_1) \cdots N(d_{k-2}$:

i) Supposons que $\mathcal{R}_{i_1}, \ldots, \mathcal{R}_{i_A}$ correspondent au symbole $=$ ($\alpha \geq 1$). Pour tout $1 \leq i \leq i_A - 1$, si $\mathcal{R}_i$ est le symbole $=$, $d_i = 0$, et $d_{i+1} = d_{i+2}$ peuvent prendre $2^n - 1$ valeurs. Ensuite, comme $S_1 \oplus S_2 \neq T_1 \oplus T_2$, donc $i_\alpha < k - 2$. Ainsi, $d_{i_A} = 0$, et $d_{i_A+1} = d_{i_A+2}$. Si $i_A + 2 = k - 2$, $d_{i_A+2} = S_1 \oplus S_2$ et les d_i restants peuvent prendre $2^n - 2$ valeurs. Si $i_A + 2 < k - 2$, d_{i_A+2} peut prendre $2^n - 2$ valeurs, tout comme les d_i restant. On déduit $N(d_1) \cdots N(d_{k-2}) = 1^A \cdot (2^n - 1)^{A-1} \cdot (2^n - 2)^{k-2-3(A-1)-2}$, qui correspond à la formule du lemme.

ii) Voir la démonstration du lemme 6 ou 4.

□

Lemme 8 (cas $L_1 \neq L_2, R_1 = R_2, S_1 \neq S_2, S_1 \oplus S_2 = T_1 \oplus T_2$) *Dans ce cas, le nombre de séquences $\mathcal{R}$ dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$, vaut :*

$$\binom{k-3-2A}{A-1}.$$

Soit une telle séquence $\mathcal{R}$ fixée. Le produit $N(d_1)\dots N(d_{k-2})$ vaut :

$$(2^n-1)^A \cdot (2^n-2)^{k-3-3A}.$$

Démonstration : Concernant la première partie du lemme, $S_1 \oplus S_2 = T_1 \oplus T_2$, alors nécessairement $\mathcal{R}_{k-2}$ est le symbole $=$. De plus, comme $R_1 = R_2$, nous avons que $\mathcal{R}_1$ et $\mathcal{R}_2$ sont le symbole $\neq$. Il reste à fixer $A-1$ séquences $(=, \neq, \neq)$ dans la séquence $\mathcal{R}_3, \dots, \mathcal{R}_{k-3}$. Ainsi, la première formule est $\binom{k-5-2(A-1)}{A-1}$, comme annoncé.
Passons au produit des $N(d_i)$. $S_1 \oplus S_2 = T_1 \oplus T_2$ implique $\mathcal{R}_{k-2}$ est le symbole $=$. Pour tout $2 \leq i \leq k-5$, si $\mathcal{R}_i$ est le symbole $=$, $d_i = 1$ et $d_{i+1} = d_{i+2}$ et les d_{i+2} peuvent prendre $2^n - 1$ valeurs. La valeur de d_1 est toujours celle de d_2 (qui peut prendre $2^n - 1$ valeurs) car $R_1 = R_2$. Pour tous les autres, il y a $2^n - 2$ valeurs possibles. Ainsi, $N(d_1)\dots N(d_{k-2}) = 1 \cdot (2^n-1) \cdot 1^A \cdot (2^n-1)^{A-1} \cdot (2^n-2)^{k-2-3(A-1)-2-1}$, qui est la formule annoncée. □

Lemme 9 (cas $L_1 \neq L_2, R_1 = R_2, S_1 \neq S_2, S_1 \oplus S_2 \neq T_1 \oplus T_2$) *Dans ce cas, le nombre de séquences $\mathcal{R}$ dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$, est :*

$$\binom{k-3-2A}{A}.$$

Soit une telle séquence $\mathcal{R}$ fixée, le produit $N(d_1)\cdots N(d_{k-2}$ vaut :

$$(2^n-1)^A \cdot (2^n-2)^{k-3-3A}.$$

Démonstration : $S_1 \oplus S_2 \neq T_1 \oplus T_2$, alors $\mathcal{R}_{k-2}$ est le symbole $\neq$. De plus, $R_1 = R_2$ implique que $\mathcal{R}_1$ et $\mathcal{R}_2$ sont le symbole $\neq$. Il reste à fixer A séquences $(=, \neq, \neq)$ dans la séquence $(\mathcal{R}_3, \dots, \mathcal{R}_{k-1})$ ($\mathcal{R}_{k-1}$ est inclus car $\mathcal{R}_{k-3}$ peut être le symbole $=$). On en déduit la formule annoncée pour le nombre de séquences.
Pour la seconde partie du lemme, commençons par raisonner dans le cas où pour $1 \leq i \leq k-2$, $\mathcal{R}_i$ est le symbole $\neq$. Tous les d_i, pour $2 \leq i \leq k-2$, peuvent prendre $(2^n - 2)$ valeurs : d_{k-2} doit être différent de $S_1 \oplus S_2$ et 0, d_{k-3} doit être différent de d_{k-2} et 0, etc. Quant à la valeur de d_1, celle-ci est fixée égale à d_2, car $R_1 = R_2$. D'où la formule dans ce cas : $N(d_1)\dots N(d_{k-2}) = (2^n-2)^{k-2-1}$.
Maintenant supposons qu'il y ait au moins un symbole $=$ dans la suite $\mathcal{R}$, disons $\mathcal{R}_{i_1}, \dots, \mathcal{R}_{i_A}$. Comme $S_1 \neq S_2$, tous les d_i, $k-2 \geq i > i_A + 1$, peuvent prendre $(2^n - 2)$ valeurs. Pour les autres, si $\mathcal{R}_i$ est le symbole $=$, $d_i = 1$ et

$d_{i+1} = d_{i+2}$ et les d_{i+2} peuvent prendre $2^n - 1$ valeurs (si $i + 2 < k - 1$). La valeur de d_1 est toujours celle de d_2 (qui peut prendre $2^n - 1$ valeurs) car $R_1 = R_2$. Pour tous les autres, il y a $2^n - 2$ valeurs possibles. Ainsi, $N(d_1) \dots N(d_{k-2}) = 1 \cdot (2^n - 1) \cdot 1^A \cdot (2^n - 1)^{A-1} \cdot (2^n - 2)^{k-2-3(A-1)-2-1}$, qui est la formule annoncée. □

Lemme 10 (cas $L_1 = L_2, R_1 \neq R_2, S_1 = S_2, T_1 \neq T_2$) *Dans ce cas, le nombre de séquences $\mathcal{R}$ dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$, est :*

$$\binom{k-3-2A}{A}.$$

Soit $\mathcal{R}$ une telle séquence fixée. Alors, le produit $N(d_1) \cdots N(d_{k-2})$ vaut :

$$(2^n - 1)^A \cdot (2^n - 2)^{k-3-3A}$$

Démonstration : Concernant la première partie du lemme, comme $L_1 = L_2$, alors nécessairement $\mathcal{R}_1$ est le symbole $\neq$. Il reste A symboles $=$ à fixer dans $\mathcal{R}$, soit A séquences de trois signes $(=, \neq, \neq)$ à fixer dans la séquence $(\mathcal{R}_2, \dots \mathcal{R}_{k-2})$. Il y a A places pour trois signes consécutifs à trouver, dans une suite de longueur $k-3$. On en déduit la formule.
Pour ce qui est du produit des $N(d_i)$, comme $L_1 = L_2$, d_1 est fixé et égal à $R_1 \oplus R_2$, non nul. Pour chaque $1 < i \leq k-2$, si $\mathcal{R}_i$ est le symbole $=$, alors la valeur de d_i est fixée et $d_{i+1} = d_{i+2}$ peuvent prendre $2^n - 1$ valeurs. Pour les autres indices, il y a $2^n - 2$ possibilités pour d_i. Ainsi, le produit $N(d_1) \cdot N(d_{k-2})$ vaut $1 \cdot 1^A \cdot (2^n - 1)^A \cdot 1^A \cdot (2^n - 2)^{k-2-1-3A}$. □

Lemme 11 (cas $L_1 \neq L_2, R_1 \neq R_2, S_1 = S_2, T_1 \neq T_2$) *Dans ce cas, le nombre de séquences $\mathcal{R}$ dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$, est :*

$$\binom{k-2-2A}{A.}$$

Soit $\mathcal{R}$ une telle séquence fixée. Alors, le produit $N(d_1) \cdots N(d_{k-2})$ vaut :

$$(2^n - 1)^A \cdot (2^n - 2)^{k-2-3A}.$$

Démonstration : Pour ce qui est de la première partie du lemme, il y a A symboles $=$ à fixer dans $\mathcal{R}$, soit A séquences $(=, \neq, \neq)$ à fixer dans la séquence $(\mathcal{R}_1, \dots \mathcal{R}_{k-2})$. Ainsi, il y a A places pour trois signes consécutifs à trouver, dans une suite de longueur $k-2$. On en déduit la formule pour le nombre de séquences.
Pour ce qui est du produit des $N(d_i)$, il n'y a pas d'égalité sur les deux premiers blocs. Pour chaque $1 \leq i \leq k-2$, si $\mathcal{R}_i$ est le symbole $=$, alors la valeur de d_i est fixée et $d_{i+1} = d_{i+2}$ peuvent prendre $2^n - 1$ valeurs. Pour les autres

indices, il y a $2^n - 2$ possibilités pour d_i. Ainsi, le produit $N(d_1) \cdot N(d_{k-2})$ vaut $1^A \cdot (2^n - 1)^A \cdot 1 \cdot (2^n - 2)^{k-2-3A}$, comme annoncé. □

Lemme 12 (cas $L_1 \neq L_2, R_1 = R_2, S_1 = S_2, T_1 \neq T_2$) *Dans ce cas, le nombre de séquences $\mathcal{R}$ dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$, est :*

$$\binom{k-4-2A}{A}.$$

Soit $\mathcal{R}$ une telle séquence fixée. Dans ce cas, le produit $N(d_1) \cdots N(d_{k-2})$ vaut :

$$(2^n - 1)^{A+1} \cdot (2^n - 2)^{k-4-3A}.$$

Démonstration : Pour la première partie du lemme, comme $R_1 = R_2$, nous avons nécessairement que $\mathcal{R}_1$ et $\mathcal{R}_2$ correspondent au symbole $\neq$. Il y a A symboles $=$ à fixer dans $\mathcal{R}$, donc A séquences de trois symboles $(=, \neq, \neq)$ à fixer dans la séquence $(\mathcal{R}_3, \ldots \mathcal{R}_{k-2})$. Ainsi, il y a A places pour trois symboles consécutifs à trouver, dans une séquence de longueur $k-4$. On en déduit la formule pour le nombre de séquences. Pour ce qui est du produit des $N(d_i)$, comme $R_1 = R_2$, d_1 peut prendre toutes les valeurs non nulles, et d_2 est égal à d_1. Pour chaque $2 < i \leq k-2$, si $\mathcal{R}_i$ est le symbole $=$, alors la valeur de d_i est fixée et $d_{i+1} = d_{i+2}$ peuvent prendre $2^n - 1$ valeurs. Pour les autres indices, il y a $2^n - 2$ possibilités pour d_i. Ainsi, le produit $N(d_1) \cdot N(d_{k-2})$ vaut $(2^n-1) \cdot 1 \cdot 1^A \cdot (2^n-1)^A \cdot 1 \cdot (2^n-2)^{k-2-2-3A}$, comme annoncé. □

A.1.3 Formules générales, Formule directe pour les coefficients H

Les lemmes de la sous-section A.1.2 précédente permettent à présent d'énoncer les résultats suivants :

Proposition 25 (Formule générale pour le nombre de séquences $\mathcal{R}$) *Le nombre de séquences $\mathcal{R}$ dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$, est :*

$$\binom{k-2-2 \cdot e(R) - e(L) + d(S) - 2A}{A-\beta},$$

où :

- $\beta = 1$ *si* $S_1 \oplus S_2 = T_1 \oplus T_2$, *et* 0 *sinon,*
- $e(R) = 1$ *si* $R_1 = R_2$, *et* 0 *sinon,*
- $e(L) = 1$ *si* $L_1 = L_2$, *et* 0 *sinon,*
- $d(S) = 1$ *si* $S_1 \neq S_2$, *et* 0 *sinon.*

Démonstration : Il suffit de vérifier que cette formule correspond bien à chacun des résultats des lemmes précédents. Pour $\beta = 0$, la formule est claire, d'après

les lemmes précédents. Lorsque $\beta = 1$, les lemmes précédents montrent que $\binom{k-2-\beta-2\cdot e(R)-e(L)-2(A-1)}{A-\beta}$ est une formule acceptable, or celle-ci est la même que celle énoncée. □

Proposition 26 (Formule générale pour le produit $N(d_1)\cdots N(d_{k-2})$) *Soit $\mathcal{R}$ une séquence de relations entre les blocs correspondant à deux entrées/sorties $[L_1, R_1]/[S_1, T_1]$ et $[L_2, R_2]/[S_2, T_2]$fixée. Notons :*

- *$e(L)$ vaut 1 si $L_1 = L_2$, 0 sinon,*
- *$e(R)$ vaut 1 si $R_1 = R_2$, 0 sinon,*
- *$d(S)$ vaut 1 si $S_1 \neq S_2$, 0 sinon,*
- *β vaut 1 si $S_1 \oplus S_2 = T_1 \oplus T_2$, 0 sinon,*
- *α vaut 1 si $R_1 \oplus R_2 = S_1 \oplus S_2$, 0 sinon.*

Le produit $N(d_1)\cdots N(d_{k-2})$ vaut :

$$(2^n-1)^{A+e(R)-d(S)}(2^n-2)^{k-2-2e(R)-e(L)-3(A-\beta)+(d(S)-\beta)-\beta},$$

sauf lorsque Lorsque $R_1 \neq R_2$ et $S_1 \neq S_2$ et que le nombre de $\mathcal{R}_i$ correspondant au symbole $=$ est nul. Dans ce second cas, $N(d_1)\cdots N(d_{k-2})$ vaut :

$$\sum_{j=0}^{\frac{k-2-e(L)-\alpha}{2}} \binom{k-2-e(L)-\alpha-j}{j}(2^n-2)^{j+\alpha}(2^n-3)^{k-2-\alpha-2j-e(L)}.$$

Démonstration : Il suffit de voir que l'une ou l'autre de ces formules (selon la situation), correspond aux formules données dans les lemmes 4 à 12 ci-dessus. □

Les formules pour H dépendent des cas distingués dans les lemmes 4 à 12. Il y a neuf lemmes correspondant à des cas différents, mais les lemmes 4, 5, 8 et 9 se subdivisent chacun en deux cas (selon que $R_1 \oplus R_2 = S_1 \oplus S_2$ ou non). Ceci mène à considérer treize cas, où chaque possibilité d'entrées/sorties est bien représentée. On note H_i le coefficient H dans le cas $i\,1 \leq i \leq 13$ (défini à la sous-section A.1.4 suivante). On a :

Théorème 7 (Formule directe pour H)

$$
\begin{aligned}
H_1 &= \sum_{A=1}^{\frac{k-1}{3}} \binom{k-2+1-2A}{A}(2^n)^{k-2}. \\
&\quad (2^n-1)!^A(2^n-2)!^{k-A}(2^n-1)^{A-1}(2^n-2)^{k-1-3A} \\
&\quad + \sum_{j=0}^{\frac{k-2-\alpha}{2}} \binom{k-2-j}{j}(2^n-2)^j(2^n-3)^{k-2-2j}(2^n-2)!^k(2^n)^{k-2} \\
H_2 &= \sum_{A=0}^{\frac{k-3}{3}} \binom{k-3-2A}{A}(2^n)^{k-2}. \\
&\quad (2^n-1)!^{A+1}(2^n-2)!^{k-A-1}(2^n-1)^{A}(2^n-2)^{k-3-3A} \\
H_3 &= \sum_{A=0}^{\frac{k-2}{3}} \binom{k-2-2A}{A}(2^n)^{k-2}. \\
&\quad (2^n-1)!^{A+1}(2^n-2)!^{k-A-1}(2^n-1)^{A-1}(2^n-2)^{k-2-3A} \\
H_4 &= \sum_{A=1}^{\frac{k-1}{3}} \binom{k-2+1-2A}{A}(2^n)^{k-2}. \\
&\quad (2^n-1)!^{A}(2^n-2)!^{k-A}(2^n-1)^{A-1}(2^n-2)^{k-1-3A} \\
&\quad + \sum_{j=0}^{\frac{k-3}{2}} \binom{k-3-j}{j}(2^n-2)^{j+1}(2^n-3)^{k-3-2j}(2^n-2)!^k(2^n)^{k-2} \\
H_5 &= \sum_{A=0}^{\frac{k-2}{3}} \binom{k-2-2A}{A}(2^n)^{k-2}. \\
&\quad (2^n-1)!^{A+1}(2^n-2)!^{k-A-1}(2^n-1)^{A-1}(2^n-2)^{k-2-3A}
\end{aligned}
$$

$$
\begin{aligned}
H_6 &= \sum_{A=1}^{\frac{k-2}{3}} \binom{k-2-2A}{A}(2^n)^{k-2}. \\
&\quad (2^n-1)!^{A}(2^n-2)!^{k-A}(2^n-1)^{A+}(2^n-2)^{k-2-3A} \\
&\quad + \sum_{j=0}^{\frac{k-2}{2}} \binom{k-2-j}{j}(2^n-2)^j(2^n-3)^{k-2-2j}(2^n-2)!^k(2^n)^{k-2} \\
H_7 &= \sum_{A=0}^{\frac{k-4}{3}} \binom{k-4-2A}{A}(2^n)^{k-2}. \\
&\quad (2^n-1)!^{A+1}(2^n-2)!^{k-A-1}(2^n-1)^{A+1}(2^n-2)^{k-4-3A} \\
H_8 &= \sum_{A=0}^{\frac{k-3}{3}} \binom{k-3-2A}{A}(2^n)^{k-2}. \\
&\quad (2^n-1)!^{A+1}(2^n-2)!^{k-A-1}(2^n-1)^{A}(2^n-2)^{k-3-3A} \\
H_9 &= \sum_{A=1}^{\frac{k}{3}} \binom{k-2+1-2A}{A-1}(2^n)^{k-2}. \\
&\quad (2^n-1)!^{A}(2^n-2)!^{k-A}(2^n-1)^{A-1}(2^n-2)^{k-3A} \\
H_{10} &= \sum_{A=0}^{\frac{k-2}{3}} \binom{k-3-2A}{A-1}(2^n)^{k-2}. \\
&\quad (2^n-1)!^{A+1}(2^n-2)!^{k-A-1}(2^n-1)^{A}(2^n-2)^{k-2-3A} \\
H_{11} &= \sum_{A=0}^{\frac{k-1}{3}} \binom{k-2-2A}{A-1}(2^n)^{k-2}. \\
&\quad (2^n-1)!^{A+1}(2^n-2)!^{k-A-1}(2^n-1)^{A-1}(2^n-2)^{k-1-3A} \\
H_{12} &= \sum_{A=1}^{\frac{k}{3}} \binom{k-2+1-2A}{A-1}(2^n)^{k-2}. \\
&\quad (2^n-1)!^{A}(2^n-2)!^{k-A}(2^n-1)^{A-1}(2^n-2)^{k-3A} \\
H_{13} &= \sum_{A=0}^{\frac{k-1}{3}} \binom{k-2-2A}{A-1}(2^n)^{k-2}. \\
&\quad (2^n-1)!^{A+1}(2^n-2)!^{k-A-1}(2^n-1)^{A-1}(2^n-2)^{k-1-3A}
\end{aligned}
$$

A.1.4 Différents cas à considérer

Les coefficients H diffèrent selon les relations entre les blocs d'entrée et de sortie (cf. sous-section A.1.1). Les treize cas distingués, permettant à chaque possibilité d'entrées/sorties d'être bien représentée sont les suivants :

$$
\begin{aligned}
1 &: \ L_1{\neq}L_2, R_1{\neq}R_2, S_1{\neq}S_2, R_1{\oplus}R_2{\neq}S_1{\oplus}S_2, S_1{\oplus}S_2{\neq}T_1{\oplus}T_2\\
2 &: \ L_1{\neq}L_2, R_1{=}R_2, S_1{\neq}S_2, S_1{\oplus}S_2{\neq}T_1{\oplus}T_2\\
3 &: \ L_1{=}L_2, R_1{\neq}R_2, S_1{\neq}S_2, R_1{\oplus}R_2{\neq}S_1{\oplus}S_2, S_1{\oplus}S_2{\neq}T_1{\oplus}T_2\\
4 &: \ L_1{\neq}L_2, R_1{\neq}R_2, S_1{\neq}S_2, R_1{\oplus}R_2{=}S_1{\oplus}S_2, S_1{\oplus}S_2{\neq}T_1{\oplus}T_2\\
5 &: \ L_1{=}L_2, R_1{\neq}R_2, S_1{\neq}S_2, R_1{\oplus}R_2{=}S_1{\oplus}S_2, S_1{\oplus}S_2{\neq}T_1{\oplus}T_2\\
6 &: \ L_1{\neq}L_2, R_1{\neq}R_2, S_1{=}S_2, S_1{\oplus}S_2{\neq}T_1{\oplus}T_2\\
7 &: \ L_1{\neq}L_2, R_1{=}R_2, S_1{=}S_2, S_1{\oplus}S_2{\neq}T_1{\oplus}T_2\\
8 &: \ L_1{=}L_2, R_1{\neq}R_2, S_1{=}S_2, S_1{\oplus}S_2{\neq}T_1{\oplus}T_2\\
9 &: \ L_1{\neq}L_2, R_1{\neq}R_2, S_1{\neq}S_2, R_1{\oplus}R_2{\neq}S_1{\oplus}S_2, S_1{\oplus}S_2{=}T_1{\oplus}T_2\\
10 &: \ L_1{\neq}L_2, R_1{=}R_2, S_1{\neq}S_2, R_1{\oplus}R_2{\neq}S_1{\oplus}S_2, S_1{\oplus}S_2{=}T_1{\oplus}T_2\\
11 &: \ L_1{=}L_2, R_1{\neq}R_2, S_1{\neq}S_2, R_1{\oplus}R_2{\neq}S_1{\oplus}S_2, S_1{\oplus}S_2{=}T_1{\oplus}T_2\\
12 &: \ L_1{\neq}L_2, R_1{\neq}R_2, S_1{\neq}S_2, R_1{\oplus}R_2{=}S_1{\oplus}S_2, S_1{\oplus}S_2{=}T_1{\oplus}T_2\\
13 &: \ L_1{=}L_2, R_1{\neq}R_2, S_1{\neq}S_2, R_1{\oplus}R_2{=}S_1{\oplus}S_2, S_1{\oplus}S_2{=}T_1{\oplus}T_2
\end{aligned}
$$

Dans la section 4.1 sont données certaines valeurs exactes pour les coefficients H (section 4.1.4), mais nous nous intéresserons plus principalement aux valeurs des ε (définis comme $\frac{H \cdot 2^{4n}}{2^n e^n} \cdot \frac{2^{2n}}{2^{2n}(2^{2n}-1)}$), comme souligné à la remarque de la section 3.4 du chapitre 3, car de ces valeurs ε se déduisent facilement toutes les attaques deux points. Certaines des premières valeurs pour H et ε sont aussi données à la section A.3.

A.2 Calcul des Coefficients H dans le cas des schémas de Feistel avec permutations internes, Méthode Directe

Tout comme pour les schémas Misty L, commençons par voir les implications sur les blocs voisins, des différentes relations que l'on peut avoir entre deux blocs (sous-section A.2.1). Ceci permet de mieux cibler les possibilités de séquences $\mathcal{R}$, et d'évaluer les produit $N(d_1) \cdots N(d_{k-2})$ pour $\mathcal{R}$ donné (rappelons que nous nous basons sur la formule du théorème 1 de la sous-section 3.5.2). Une fois balayés tous les cas de paires d'entrées/sorties, nous déduisons une formule finale pour les coefficients H (sous-section A.2.3, théorèmes 8, 9, 10 et 11).

A.2.1 Restrictions sur les relations $\mathcal{R}$ entre les blocs

Soient $[L_1, R_1]/[S_1, T_1]$ et $[L_2, R_2]/[S_2, T_2]$ deux entrées/sorties distinctes de k tours de schémas du type Misty, On s'intéresse aux différentes séquences de relations $\mathcal{R}$ entre les blocs internes correspondant à ces deux entrées/sorties (voir le paragraphe 3.5.1.2 du chapitre 3). Afin de voir quelles restrictions sont imposées par le schéma, regardons à nouveau la figure A.2.

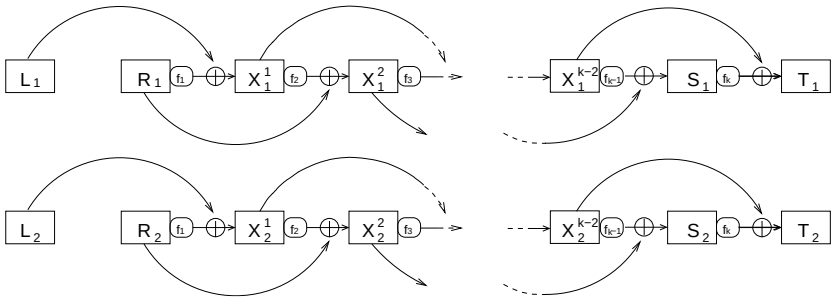

FIGURE A.2: $\psi^k(f_1, \ldots, f_k)([L_1, R_1]) = [S_1, T_1]$, $\psi^k(f_1, \ldots, f_k)([L_2, R_2]) = [S_2, T_2]$

On voit qu'il y a certaines contraintes pour les séquences $\mathcal{R}$ de relations entre les blocs valides :

1. Pour $-1 \leq i \leq k$, si $\mathcal{R}_i$ est le symbole $=$, alors $\mathcal{R}_{i+1}$, $\mathcal{R}_{i+2}$, $\mathcal{R}_{i-1}$ et $\mathcal{R}_{i-2}$ sont nécessairement tous égaux au symbole $\neq$ (lorsque tous ces éléments sont bien définis). De plus,(si l'on suppose fixer les blocs de la gauche vers la droite), si $d_i = 0$, alors $d_{i-1} = d_{i+1}$ et d_{i+2} peut prendre toutes les valeurs non nulles.
   En effet, pour la première assertion, on a $X^i = f_i(X^{i-1}) \oplus X^{i-2}$ et $X^{i+2} = f_{i+2}(X^{i+1}) \oplus X^i$. Si un des éléments de $\mathcal{R}$ ci-dessus est le symbole $=$ en plus de $\mathcal{R}_i$, alors les expressions précédentes impliquent que pour trois blocs successifs, nous avons $X_1 = X_2$ (rappelons que les fonctions sont bijectives). Autrement, tous les blocs correspondant à l'un ou à l'autre des messages sont égaux, ce qui est impossible.
   La première partie de la deuxième assertion est claire par définition du bloc X^{i+1}. Ensuite, $X^{i+2} = f_{i+2}(X^{i+1}) \oplus X^i$. Si $d_i = 0$, X^{i+2} est entièrement défini par l'image par f_{i+2} de X^{i+1}. Or $d_{i+1} \neq 0$ et f_{i+2} est une permutation. L'affirmation en découle.
2. Pour $-1 \leq i \leq k-2$, si $\mathcal{R}_i$, $\mathcal{R}_{i+1}$ et $\mathcal{R}_{i+2}$ correspondent au symbole $\neq$, alors $d_i \neq d_{i+2}$.
   Nous avons $X^{i+2} = f_{i+2}(X^{i+1}) \oplus X^i$. Alors, $d_i = d_{i+2}$ implique $f_{i+2}(X_1^{i+1}) = f_{i+2}(X_2^{i+1})$. f_{i+2} étant une permutation, ceci implique que $X_1^{i+1} = X_2^{i+1}$, ce qui est absurde.

Ces conditions impliquent différentes séquences $\mathcal{R}$ valides, selon les valeurs initiales de $\mathcal{R}_{-1}$, $\mathcal{R}_0$, $\mathcal{R}_{k-1}$ et $\mathcal{R}_k$. On voit ici encore, à cause de la formule du théorème 1 de la sous-section 3.5.2, que les valeurs de H de deux entrées/sorties distinctes $[L_1, R_1]/[S_1, T_1]$ et $[L_2, R_2]/[S_2, T_2]$ ne dépendent que des relations entre les blocs d'entrée et de sorties de ces deux messages (ce résultat a déjà annoncé pour les schémas du type Misty, théorème 6).

A.2.2 Séquences $\mathcal{R}$ possibles et produit des $N(d_i)$, $i = 1, \ldots k$

Une analyse similaire à celle faite pour les schémas du type Misty, basée sur les restrictions pour les séquences $\mathcal{R}$ et les valeurs de d_i (sous-section A.2.1 précédente),

nous permet d'arriver aux formules générales de la sous-section A.2.3. Nous donnons dans cette sous-section A.2.2 le détail du nombre de séquences $\mathcal{R}$ possibles, ainsi que du produit $N(d_1)\cdots N(d_{k-2})$, pour $\mathcal{R}$ fixé.

Séquences $\mathcal{R}$ possibles. On garde les mêmes notations que pour le cas des schémas Misty L : $A_{X^{i_1},X^{i_2}}$ correspond au nombre de relations d'égalités dans une séquence $\mathcal{R}$, correspondant à la relation entre deux blocs X_1^i et X_2^i, $i_1 < i < i_2$. Pour chaque cas significatif, on s'intéresse au nombre de séquences $\mathcal{R}$ comportant $A = A_{X^0,X^{k-1}}$ symboles $=$. Les résultats sont exposés dans les lemmes 13,14,15,16,17,18 suivants. Ceux-ci se démontrent comme les résultats analogues pour les schémas Misty L de la sous-section A.1.2, un simple raisonnement sur le nombre de possibilités de ranger A fois trois symboles consécutifs $(=,\neq,\neq)$ dans la séquence $\mathcal{R}$ considérée donne le résultat. Nous ne donnons pas le détail des démonstrations.

Lemme 13 (Cas $L_1 \neq L_2$, $R_1 \neq R_2$, $S_1 \neq S_2$, $T_1 \neq T_2$) *Le nombre de séquences $\mathcal{R}$, dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$, est :*

$$\binom{k-2A}{A}.$$

Lemme 14 (Cas $L_1 \neq L_2$, $R_1 = R_2$, $S_1 \neq S_2$, $T_1 \neq T_2$) *Le nombre de séquences $\mathcal{R}$, dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$, est :*

$$\binom{k-2-2A}{A}.$$

Lemme 15 (Cas $L_1 = L_2$, $R_1 \neq R_2$, $S_1 \neq S_2$, $T_1 \neq T_2$) *Le nombre de séquences $\mathcal{R}$, dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$, est :*

$$\binom{k-1-2A}{A}.$$

Lemme 16 (Cas $L_1 = L_2$, $R_1 \neq R_2$, $S_1 = S_2$, $T_1 \neq T_2$) *Le nombre de séquences $\mathcal{R}$, dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$, est :*

$$\binom{k-3-2A}{A}.$$

Lemme 17 (Cas $L_1 = L_2$, $R_1 \neq R_2$, $S_1 \neq S_2$, $T_1 = T_2$) *Le nombre de séquences $\mathcal{R}$, dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$, est :*

$$\binom{k-2-2A}{A}.$$

Lemme 18 (Cas $L_1 \neq L_2$, $R_1 = R_2$, $S_1 = S_2$, $T_1 \neq T_2$) *Le nombre de séquences $\mathcal{R}$, dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$, est :*

$$\binom{k-4-2A}{A}.$$

Nous avons encore besoin du lemme suivant, accompagnant le résultat du lemme 24 dans les formules générales pour H :

Lemme 19 *Le nombre de séquences $\mathcal{R}$, comportant $A = A_{X^0,X^{k-1}}$ éléments d'indice pair uniquement (respectivement impair uniquement) correspondant au symbole $=$ est :*

$$\binom{l+1-e(L)-e(R)-e(S)-e(T)-A}{A},$$

où l est le nombre d'indices pairs de $\mathcal{R}$ (respectivement impairs) entre 1 et $k-2$ inclus, et :

- $e(L) = 1$ *si* $L_1 = L_2$, 0 *sinon,*
- $e(R) = 1$ *si* $R_1 = R_2$, 0 *sinon,*
- $e(S) = 1$ *si* $S_1 = S_2$, 0 *sinon,*
- $e(T) = 1$ *si* $T_1 = T_2$, 0 *sinon.*

Remarque : Dans la suite, nous utilisons les notations :
- l_{pair} pour le nombre d'indices pairs de $\mathcal{R}$ entre 1 et $k-2$.
- l_{pair} pour le nombre d'indices pairs de $\mathcal{R}$ entre 1 et $k-2$.

Produit des $N(d_i)$, $i = 1, \ldots k$. Pour ce qui est du produit des $N(d_i)$, $i = 1, \ldots, k-2$, la stratégie est légèrement différente que dans le cas des schémas Misty L. Nous considérons, dans le cas des schémas de Feistel avec permutations internes, les sous-séquences formées seulement des blocs X^i avec i pair, ou des blocs X^i avec i impairs. En effet, d'après la sous-section A.2.1, on voit que les contraintes sur une valeur d_i ne dépend que de d_{i-2} et d_{i+2} (lorsque ceux-ci sont bien définis). On peut ensuite fusionner les résultats pour obtenir le produit des $N(d_i)$ dans chacun des cas à considérer.

Pour ne pas avoir à spécifier si nous considérons la sous-séquence des blocs pairs ou impairs, nous considérons dans les lemmes suivants des séquences de blocs longueur $l+2$, $(B^0, \ldots, B^{l+1})$, où B^0 et B^{l+1} sont fixés. Nous notons $N(d_{B^i})$ le nombre de possibilités de $d_{B^i} = B^i - 1 \oplus B_2^i$, pour ne pas confondre avec $N(d_i)$ correspondant aux possibilités pour $X_1^i \oplus X_2^i$. Cependant B^0 doit être vu comme X^{-1} ou X_0, B^{l+1} comme X^{k+1} ou X^{k+2}, et $l+1$ correspond le nombre d'indices impairs ou pairs, selon que l'on considère la sous-séquence de blocs impairs ou pairs.

Lemme 20 (Cas $B_1^0 \neq B_2^0$, $B_1^{l+1} = B_2^{l+1}$) *Supposons fixée une séquence $\mathcal{R}$. Soit $A(B) = A(B)_{B^0,B^{l+1}}$ le nombre de relations d'égalité correspondant à deux blocs B_1^i et B_2^i, $i = 1, \ldots, l$. Le produit $N(d_{B^1} \cdots N(d_{B^l})$ vaut :*

$$(2^n - 1)^{A(B)} \cdot (2^n - 2)^{l - A_{B^0,B^{L+1}} - A(B)}.$$

Démonstration : Nous avons $A(B)$ d_{B^i} qui sont fixés à zéro, et pour chaque tel i, $d_{B^{i+1}}$ peut prendre toutes les $2^n - 1$ valeurs non nulles. De plus, il existe alors $A_{B^0,B^{l+1}} - A(B)$ symboles = dans la sous-séquence formée des blocs X^i non contenus dans B et strictement entre B^0 et B^{l+1}. Ceci signifie autant de blocs B^i tels que $d_{B^i} = d_{B^{i-1}}$. Pour les blocs restants, ceux-ci doivent vérifier $d_{B^i} \neq 0$ et $d_{B^i} \neq d_{B^{i-1}}$. On obtient $1^{A(B)+A_{B^0,B^{l+1}}-A(B)} \cdot (2^n - 1)^{A(B)} \cdot (2^n - 2)^{l-2A(B)-(A_{B^0,B^{l+1}}-A(B))}$, comme annoncé. □

Pour les lemmes suivants, le détail de la démonstration n'est pas donné. Le raisonnement est très similaire à celui du lemme 20, ou aux différents raisonnements faits dans le cas de schémas Misty L, aux lemmes 2.12 à 2.12.

Lemme 21 (Cas $B_1^0 = B_2^0$, $B_1^{l+1} \neq B_2^{l+1}$) *Supposons fixée une séquence $\mathcal{R}$. Soit $A(B) = A(B)_{B^0,B^{l+1}}$ le nombre de relations d'égalité correspondant à deux blocs B_1^i et B_2^i, $i = 1, \ldots, l$. Le produit $N(d_{B^1} \cdots N(d_{B^l})$ vaut :*

$$(2^n - 1)^{A(B)} \cdot (2^n - 2)^{l - A_{B^0,B^{l+1}} - A(B)}.$$

Lemme 22 (Cas $B_1^0 = B_2^0$, $B_1^{l+1} = B_2^{l+1}$) *Supposons fixée une séquence $\mathcal{R}$. Soit $A(B) = A(B)_{B^0,B^{l+1}}$ le nombre de relations d'égalité correspondant à deux blocs B_1^i et B_2^i, $i = 1, \ldots, l$. Le produit $N(d_{B^1} \cdots N(d_{B^l})$ vaut :*

$$(2^n - 1)^{A(B)+1} \cdot (2^n - 2)^{l - A_{B^0,B^{l+1}} - A(B) - 1}.$$

Lemme 23 (Cas $B_1^0 \neq B_2^0$, $B_1^{l+1} \neq B_2^{l+1}$ et $A(B) > 0$) *Supposons fixée une séquence $\mathcal{R}$. Soit $A(B) = A(B)_{B^0,B^{l+1}} > 0$ le nombre de relations d'égalité correspondant à deux blocs B_1^i et B_2^i, $i = 1, \ldots, l$. Le produit $N(d_{B^1} \cdots N(d_{B^l})$ vaut :*

$$(2^n - 1)^{A(B)-1} \cdot (2^n - 2)^{l - A_{B^0,B^{l+1}} - A(B) + 1}.$$

Lorsque, pour ce cas $B_1^0 \neq B_2^0$ et $B_1^{l+1} \neq B_2^{l+1}$, le nombre $A(B) = A(B)_{B^0,B^{l+1}}$ est nul, il faut être un peu plus précautionneux dans le raisonnement. Le dénombrement est à rapprocher de celui fait aux lemmes 4,5,6 ou 7,*ii*) de la section A.1. Sans démontrer ce point, on obtient :

Lemme 24 (Cas $B_1^0 \neq B_2^0$, $B_1^{l+1} \neq B_2^{l+1}$ et $A(B) = 0$) *Supposons fixée une séquence $\mathcal{R}$. Supposons nul le nombre $A(B) = A(B)_{B_0,B_{l+1}}$ de relations d'égalité correspondant à deux blocs B_1^i et B_2^i, $i = 1, \ldots, l$. Le produit $N(d_{B^1} \cdots N(d_{B^l})$ vaut :*

i) Si $B_1^0 \oplus B_2^0 = B_0^{l+1} \oplus B_1^{l+1}$ *:*

$$\sum_{j=0}^{(l-1-A_{B^0,B^{l+1}})/2} \binom{l - A_{B^0,B^{l+1}} - j - 1}{j} \cdot (2^n-2)^{j+1} \cdot (2^n-3)^{l-A_{B^0,B^{l+1}}-2j-1}.$$

ii) Si $B_1^0 \oplus B_2^0 = B_0^{l+1} \oplus B_1^{l+1}$ *:*

$$\sum_{j=0}^{(l-A_{B^0,B^{l+1}})/2} \binom{l - A_{B^0,B^{l+1}} - j}{j} \cdot (2^n-2)^{j} \cdot (2^n-3)^{l-A_{B^0,B^{l+1}}-2j}.$$

Remarque : Dans le suite, nous utilisons les notations :
- Lorsque k est pair :
  - α_{pair} vaut 1 lorsque $R_1 \oplus R_2 = T_1 \oplus T_2$, 0 sinon.
  - α_{imp} vaut 1 lorsque $L_1 \oplus L_2 = S_1 \oplus S_2$, 0 sinon.
- Lorsque k est impair :
  - α_{pair} vaut 1 lorsque $R_1 \oplus R_2 = S_1 \oplus S_2$, 0 sinon.
  - α_{imp} vaut 1 lorsque $L_1 \oplus L_2 = T_1 \oplus T_2$, 0 sinon.

A.2.3 Formules générales, formules générales pour H

Des lemmes 13 à 18, nous avons :

Proposition 27 (Nombre de séquences $\mathcal{R}$) *Le nombre de séquences $\mathcal{R}$, dont un nombre A d'éléments d'indice i, $1 \leq i \leq k-2$, correspondent au symbole $=$, est :*

$$\binom{k - 2(e(R)+e(S)) - e(L) - e(T) - 2A}{A},$$

où :
- $e(L) = 1$ *si* $L_1 = L_2$, 0 *sinon,*
- $e(R) = 1$ *si* $R_1 = R_2$, 0 *sinon,*
- $e(S) = 1$ *si* $S_1 = S_2$, 0 *sinon,*
- $e(T) = 1$ *si* $T_1 = T_2$, 0 *sinon.*

Pour calculer le produit $N(d_1) \cdots N(d_k)$ correspondant à une séquence $\mathcal{R}$ fixée, il suffit d'utiliser les résultats des lemmes 20 à 24 précédents. Plus précisément, pour chacune des sous-séquences pair et impair, on applique un des lemmes précédents, en remplaçant B^0 par L ou R, et B^l par S ou T. Le produit cherché s'obtient en multipliant les deux résultats. Nous utilisons les notations spécifiées dans les remarques ou propositions précédentes.

Proposition 28 (Formule générale 1 pour le produit $N(d_1) \cdots N(d_{k-2})$) *Soit $\mathcal{R}$ une séquence fixée de relations possibles, avec A symboles $=$ et telle qu'ils existent $i, j \in \{-1, \ldots, k+2\}$, i pair, j impair tels que $\mathcal{R}_i$ et $\mathcal{R}_j$ correspondent au symbole $=$. Alors, le produit $N(d_1) \cdots N(d_{k-2})$ vaut :*

$$\Pi_1 = (2^n-1)^{A-2}(2^n-2)^{k-3A+e(R)+e(S)+2(e(L)+e(T))} .$$

Proposition 29 (Formule générale 2 pour le produit $N(d_1)\cdots N(d_{k-2})$)
Soit $\mathcal{R}$ une séquence fixée de relations possibles, avec A symboles $=$ et telle qu'il existe $i \in \{-1,\ldots,k+2\}$, i pair tel que $\mathcal{R}_i$ corresponde au symbole $=$ et $\forall j$ impair, $\mathcal{R}_j$ soit le symbole $\neq$. Alors, le produit $N(d_1)\cdots N(d_{k-2})$ vaut :

$$\Pi_2 = \left\{ \sum_{j=0}^{M_{imp}} C_{j,imp}\cdot(2^n-2)^{j+\alpha_{imp}}(2^n-3)^{P_{j,imp}} \right\} \cdot (2^n-1)^{e(s)-1}(2^n-2)^{Q_{imp}},$$

où :

$$\begin{array}{lcl} M_{imp} & = & \frac{l_{imp}-\alpha_{imp}-A-e(R)-e(S)}{2}, \\ C_{j,imp} & = & \binom{l_{imp}-A-e(R)-e(S)-\alpha_{imp}-j}{j}, \\ P_{j,imp} & = & l_{imp}-A-e(R)-e(S)-\alpha_{imp}-2j, \\ Q_{imp} & = & l_{pair}-2A-(e(L)+e(R)+e(S)+e(T))+1. \end{array}$$

Proposition 30 (Formule générale 3 pour le produit $N(d_1)\cdots N(d_{k-2})$)
Soit $\mathcal{R}$ une séquence fixée de relations possibles, avec A symboles $=$ et telle qu'il existe $i \in \{-1,\ldots,k+2\}$, i impair tel que $\mathcal{R}_i$ corresponde au symbole $=$ et $\forall j$ pair, $\mathcal{R}_j$ soit le symbole $\neq$. Alors, le produit $N(d_1)\cdots N(d_{k-2})$ vaut :

$$\Pi_3 = \left\{ \sum_{j=0}^{M_{pair}} C_{j,pair}\cdot(2^n-2)^{j+\alpha_{pair}}(2^n-3)^{P_{j,pair}} \right\} \cdot (2^n-1)^{A-1}(2^n-2)^{Q_{pair}},$$

où :

$$\begin{array}{lcl} M_{pair} & = & \frac{l_{pair}-\alpha_{pair}-A-e(R)-e(S)}{2}, \\ C_{j,pair} & = & \binom{l_{pair}-A-e(R)-e(S)-\alpha_{pair}-j}{j}, \\ P_{j,pair} & = & l_{pair}-A-e(R)-e(S)-\alpha_{pair}-2j, \\ Q_{pair} & = & l_{pair}-2A-(e(L)+e(R)+e(S)+e(T))+1. \end{array}$$

Proposition 31 (Formule générale 4 pour le produit $N(d_1)\cdots N(d_{k-2})$)
Soit $\mathcal{R}$ une séquence fixée de relations possibles, telle que $\forall i$, $\mathcal{R}_i$ soit le symbole $\neq$. Alors avec les notations des propositions précédentes, le produit $N(d_1)\cdots N(d_{k-2})$ vaut :

$$\Pi_4 = \left\{ \sum_{j=0}^{M_{pair}} C_{j,pair}\cdot(2^n-2)^{j+\alpha_{pair}}\cdot(2^n-3)^{P_{j,pair}} \right\} \cdot \left\{ \sum_{j=0}^{M_{imp}} C_{j,imp}\cdot(2^n-2)^{j+\alpha_{imp}}\cdot(2^n-3)^{P_{j,imp}} \right\}.$$

Passons aux formules pour les coefficients H. Ces formules se déduisent des propositions 28 à 31 pour le produit des $N(d_i)\, i = 1,\ldots k$ et de la proposition 27, mais aussi du lemme 19.

Remarque : En fait, ces formules sont vraies sous certaines conditions, pour un nombre de tours petit, 1, 2 ou 3 tours. Nous les spécifions dans les formules générales pour les coefficients H suivantes.

Théorème 8 (Formule 1 pour H) *Soient les cas suivants :*

$$\begin{array}{rccl} & k & \text{pair} & \text{et } L_1 = L_2,\ R_1 \neq R_2,\ S_1 \neq S_2,\ T_1 = T_2, \\ \text{ou} & k & \text{pair} & \text{et } L_1 \neq L_2,\ R_1 = R_2,\ S_1 = S_2,\ T_1 \neq T_2, \\ \text{ou} & k & \text{impair} & \text{et } L_1 = L_2,\ R_1 \neq R_2,\ S_1 = S_2,\ T_1 \neq T_2, \\ \text{ou} & k & \text{impair} & \text{et } L_1 \neq L_2,\ R_1 = R_2,\ S_1 \neq S_2,\ T_1 = T_2. \end{array}$$

Dans ces conditions, nous avons l'expression suivante pour le coefficient H, valable pour $k \geq 2$:

$$H = \sum_{A=0}^{M} (2^n-1)!^{A+e(R)+e(S)} \cdot (2^n-2)!^{k-A-e(R)-e(S)} \cdot 2^{n(k-2)} \cdot \binom{k-2(e(R)+e(S))-e(L)-e(T)-2A}{A} \cdot \Pi_1.$$

Théorème 9 (Formule 2 pour H) *Soient les cas suivants :*

$$\begin{array}{rccl} & k & \text{pair} & \text{et } L_1 \neq L_2,\ R_1 = R_2,\ S_1 \neq S_2,\ T_1 = T_2, \\ \text{ou} & k & \text{pair} & \text{et } L_1 \neq L_2,\ R_1 = R_2,\ S_1 \neq S_2,\ T_1 \neq T_2, \\ \text{ou} & k & \text{pair} & \text{et } L_1 \neq L_2,\ R_1 \neq R_2,\ S_1 \neq S_2,\ T_1 = T_2, \\ \text{ou} & k & \text{impair} & \text{et } L_1 \neq L_2,\ R_1 \neq R_2,\ S_1 = S_1,\ T_1 \neq T_2, \\ \text{ou} & k & \text{impair} & \text{et } L_1 \neq L_2,\ R_1 = R_2,\ S_1 \neq S_2,\ T_1 \neq T_2, \\ \text{ou} & k & \text{impair} & \text{et } L_1 \neq L_2,\ R_1 = R_2,\ S_1 = S_2,\ T_1 \neq T_2. \end{array}$$

Dans ces conditions, nous avons l'expression suivante pour le coefficient H, valable pour[1] *$k > 2$:*

$$\begin{aligned} H \quad = \quad & \sum_{A=0}^{M} (2^n-1)!^{A+e(R)+e(S)} \cdot (2^n-2)!^{k-A-e(R)-e(S)} \cdot 2^{n(k-2)} \cdot \\ & \Big[\ \binom{l_{pair}+1-A-e(L)-e(R)-e(S)-e(T)}{A} \cdot \Pi_2 \ + \Big[\binom{k-2(e(R)+e(S))-e(L)-e(T)-2A}{A} - \\ & \binom{l_{pair}+1-A-e(L)-e(R)-e(S)-e(T)}{A} \Big] \cdot \Pi_1 \ \Big]. \end{aligned}$$

Théorème 10 (Formule 3 pour H) *Soient les cas suivants :*

$$\begin{array}{rccl} & k & \text{pair} & \text{et } L_1 \neq L_2,\ R_1 \neq R_2,\ S_1 = S_2,\ T_1 \neq T_2, \\ \text{ou} & k & \text{pair} & \text{et } L_1 = L_2,\ R_1 \neq R_2,\ S_1 \neq S_2,\ T_1 \neq T_2, \\ \text{ou} & k & \text{pair} & \text{et } L_1 = L_2,\ R_1 \neq R_2,\ S_1 = S_2,\ T_1 \neq T_2, \\ \text{ou} & k & \text{pair} & \text{et } L_1 = L_2,\ R_1 \neq R_2,\ S_1 \neq S_2,\ T_1 \neq T_2, \\ \text{ou} & k & \text{pair} & \text{et } L_1 \neq L_2,\ R_1 \neq R_2,\ S_1 \neq S_2,\ T_1 = T_2, \\ \text{ou} & k & \text{pair} & \text{et } L_1 = L_2,\ R_1 \neq R_2,\ S_1 \neq S_2,\ T_1 = T_2. \end{array}$$

Dans ces conditions, nous avons l'expression suivante pour le coefficient H, valable

1. et pour $k = 2$ lorsque l'on suppose la somme dans Π_2 égale à 1 quand $\alpha_{odd} = e(L)$

pour[2] $k > 2$ *:*

$$H = \sum_{A=0}^{M} (2^n-1)!^{A+e(R)+e(S)} \cdot (2^n-2)!^{k-A-e(S)} \cdot 2^{n(k-2)} \cdot \Big[\binom{l_{imp}+1-A-e(L)-e(R)-e(S)-e(T)}{A} \cdot \Pi_3 + \Big[\binom{k-2(e(R)+e(S))-e(L)-e(T)-2A}{A} - \binom{l_{imp}+1-A-e(L)-e(R)-e(S)-e(T)}{A}\Big] \cdot \Pi_1 \Big].$$

Théorème 11 (Formule 4 pour H) *Soient les cas suivants :*

$$k \in \mathbb{N}^*,\ L_1 \neq L_2,\ R_1 \neq R_2,\ S_1 \neq S_2,\ T_1 \neq T_2.$$

Dans ces conditions, nous avons l'expression suivante pour le coefficient H, valable pour[3] $k > 3$ *:*

$$H = (2^n-2)!^k \cdot (2^n)^{k-2} \cdot \Pi_4 + \sum_{A=1}^{k/3} (2^n-1)!^A \cdot (2^n-2)!^{k-A} \cdot 2^{n(k-2)} \cdot \Big[\binom{l_{pair}+1-A}{A}\Pi_2 + \binom{l_{imp}+1-A}{A}\Pi_3 + \Big[\binom{k-2A}{A} - \binom{l_{pair}+1-A}{A} - \binom{l_{imp}+1-A}{A}\Big] \cdot \Pi_1\Big].$$

A.2.4 Différents cas à considérer

Ci-dessous les différents cas à considérer, selon que le nombre de tours de schémas de Feistel considérés est pair ou impair. Ces cas correspondent aux cas distingués dans la sous-section A.2.2. Chaque possibilité d'égalités entre blocs d'entrée et de sortie de deux messages est bien prise en compte.

Pour un nombre k de tours *impair* :

1 : $L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq T_1 \oplus T_2, R_1 \oplus R_2 \neq S_1 \oplus S_2$
2 : $L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 = T_1 \oplus T_2, R_1 \oplus R_2 \neq S_1 \oplus S_2$
3 : $L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq T_1 \oplus T_2, R_1 \oplus R_2 = S_1 \oplus S_2$
4 : $L_1 \neq L_2, R_1 \neq R_2, S_1 = S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq T_1 \oplus T_2, R_1 \oplus R_2 \neq S_1 \oplus S_2$
5 : $L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq T_1 \oplus T_2, R_1 \oplus R_2 \neq S_1 \oplus S_2$
6 : $L_1 = L_2, R_1 \neq R_2, S_1 = S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq T_1 \oplus T_2, R_1 \oplus R_2 \neq S_1 \oplus S_2$
7 : $L_1 \neq L_2, R_1 \neq R_2, S_1 = S_2, T_1 \neq T_2, L_1 \oplus L_2 = T_1 \oplus T_2, R_1 \oplus R_2 \neq S_1 \oplus S_2$
8 : $L_1 \neq L_2, R_1 = R_2, S_1 = S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq T_1 \oplus T_2, R_1 \oplus R_2 = S_1 \oplus S_2$
9 : $L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 \neq T_1 \oplus T_2, R_1 \oplus R_2 = S_1 \oplus S_2$
10 : $L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 = T_2, L_1 \oplus L_2 = T_1 \oplus T_2, R_1 \oplus R_2 \neq S_1 \oplus S_2$
11 : $L_1 \neq L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 \neq T_2, L_1 \oplus L_2 = T_1 \oplus T_2, R_1 \oplus R_2 = S_1 \oplus S_2$
12 : $L_1 \neq L_2, R_1 = R_2, S_1 = S_2, T_1 \neq T_2, L_1 \oplus L_2 = T_1 \oplus T_2, R_1 \oplus R_2 = S_1 \oplus S_2$
13 : $L_1 = L_2, R_1 \neq R_2, S_1 \neq S_2, T_1 = T_2, L_1 \oplus L_2 = T_1 \oplus T_2, R_1 \oplus R_2 = S_1 \oplus S_2$

2. Et pour $k = 2$ lorsque la somme dans Π_3 vaut 1 quand $e(L) + e(S) = 1$, et $\alpha_{pair} = e(S)$.
3. Et pour $k = 2, 3$ si l'on suppose
   – la somme dans Π_4, majorée par M_{pair} vaut 1, quand $k = 2$ et $\alpha_{pair} = 0$,
   – la somme dans Π_4, majorée par M_{imp} vaut 1, quand $k = 2$ et $\alpha_{pair} = 0$,
   – la somme dans Π_3 vaut 1, quand $k = 3$ et $\alpha_{pair} = 1 = A$.

Pour un nombre k de tours *pair* :

$$
\begin{aligned}
1 &: \; L_1{\neq}L_2, R_1{\neq}R_2, S_1{\neq}S_2, T_1{\neq}T_2, L_1{\oplus}L_2{\neq}S_1{\oplus}S_2, R_1{\oplus}R_2{\neq}T_1{\oplus}T_2 \\
2 &: \; L_1{\neq}L_2, R_1{=}R_2, S_1{\neq}S_2, T_1{\neq}T_2, L_1{\oplus}L_2{\neq}S_1{\oplus}S_2, R_1{\oplus}R_2{\neq}T_1{\oplus}T_2 \\
3 &: \; L_1{=}L_2, R_1{\neq}R_2, S_1{\neq}S_2, T_1{\neq}T_2, L_1{\oplus}L_2{\neq}S_1{\oplus}S_2, R_1{\oplus}R_2{\neq}T_1{\oplus}T_2 \\
4 &: \; L_1{\neq}L_2, R_1{\neq}R_2, S_1{\neq}S_2, T_1{\neq}T_2, L_1{\oplus}L_2{=}S_1{\oplus}S_2, R_1{\oplus}R_2{\neq}T_1{\oplus}T_2 \\
5 &: \; L_1{=}L_2, R_1{\neq}R_2, S_1{\neq}S_2, T_1{=}T_2, L_1{\oplus}L_2{\neq}S_1{\oplus}S_2, R_1{\oplus}R_2{\neq}T_1{\oplus}T_2 \\
6 &: \; L_1{\neq}L_2, R_1{=}R_2, S_1{=}S_2, T_1{\neq}T_2, L_1{\oplus}L_2{\neq}S_1{\oplus}S_2, R_1{\oplus}R_2{\neq}T_1{\oplus}T_2 \\
7 &: \; L_1{\neq}L_2, R_1{=}R_2, S_1{\neq}S_2, T_1{=}T_2, L_1{\oplus}L_2{\neq}S_1{\oplus}S_2, R_1{\oplus}R_2{=}T_1{\oplus}T_2 \\
8 &: \; L_1{\neq}L_2, R_1{=}R_2, S_1{\neq}S_2, T_1{\neq}T_2, L_1{\oplus}L_2{=}S_1{\oplus}S_2, R_1{\oplus}R_2{\neq}T_1{\oplus}T_2 \\
9 &: \; L_1{\neq}L_2, R_1{\neq}R_2, S_1{\neq}S_2, T_1{=}T_2, L_1{\oplus}L_2{=}S_1{\oplus}S_2, R_1{\oplus}R_2{\neq}T_1{\oplus}T_2 \\
10 &: \; L_1{\neq}L_2, R_1{\neq}R_2, S_1{\neq}S_2, T_1{\neq}T_2, L_1{\oplus}L_2{=}S_1{\oplus}S_2, R_1{\oplus}R_2{=}T_1{\oplus}T_2 \\
11 &: \; L_1{\neq}L_2, R_1{=}R_2, S_1{\neq}S_2, T_1{=}T_2, L_1{\oplus}L_2{=}S_1{\oplus}S_2, R_1{\oplus}R_2{=}T_1{\oplus}T_2
\end{aligned}
$$

A.3 Calculs des Coefficients H pour les schémas du type Misty, Méthode par récurrence

Dans cette section, nous montrons comment les coefficients H pour les schémas M_L^k peuvent être obtenus par récurrence. Ceci permet également de valider les formules directes obtenues précédemment, à la section A.1.

A.3.1 Coefficients H pour un tour et deux tours

A.3.1.1 Un tour

Dans le cas de M_L^1, nous avons (voir aussi figure A.3) :

$$\begin{cases} S = R \\ T = R \oplus f_1(L) \end{cases}$$

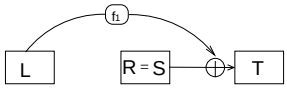

FIGURE A.3: Un tour de Misty L

Dans le cadre d'une attaque deux points, pour M_L^1, on a nécessairement :

$$\begin{cases} S_1 = R_1, \; S_2 = R_2 \\ L_1 = L_2 \Leftrightarrow T_1 \oplus R_1 = T_2 \oplus R_2. \end{cases}$$

Ainsi, si ces conditions ne sont pas vérifiées, $H = 0$. Lorsqu'elles le sont, comme f_1 s'applique sur le blocs L, si $L_1 = L_2$, on a $H = \frac{|B_n|}{2^n}$, et $H = \frac{|B_n|}{2^n(2^n-1)}$, sinon.

Revenons aux 13 cas distingués (voir sous-sectionA.1.4). Notons H_c la valeur de H pour le cas c. On obtient, pour un tour de schéma du type Misty :

$$\begin{aligned}
&H_1 = 0,\\
&H_2 = 0,\\
&H_3 = 0,\\
&H_4 = \tfrac{|B_n|}{2^n(2^n-1)},\\
&H_5 = 0,\\
&H_6 = 0,\\
&H_7 = \tfrac{|B_n|}{2^n(2^n-1)},\\
&H_8 = 0,\\
&H_9 = 0,\\
&H_{10} = 0,\\
&H_{11} = 0,\\
&H_{12} = 0,\\
&H_{13} = \tfrac{|B_n|}{2^n}.
\end{aligned}$$

A.3.1.2 Deux tours

Pour deux tours, on a les relations suivantes (voir aussi figure A.4) :

$$\begin{cases} S = R \oplus f_1(L) \\ T \oplus S = f_2(R). \end{cases}$$

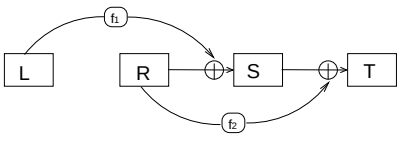

FIGURE A.4: Deux tours de Misty L

On a les valeurs suivantes pour le coefficient H pour deux tours (H_c le coefficient

H dans le cas c) :

$$
\begin{aligned}
H_1 &= \tfrac{|B_n|^2}{2^{2n}(2^n-1)^2},\\
H_2 &= 0,\\
H_3 &= 0,\\
H_4 &= 0,\\
H_5 &= \tfrac{|B_n|^2}{2^{2n}(2^n-1)},\\
H_6 &= \tfrac{|B_n|^2}{2^{2n}(2^n-1)^2},\\
H_7 &= 0,\\
H_8 &= 0,\\
H_9 &= 0,\\
H_{10} &= \tfrac{|B_n|^2}{2^{2n}(2^n-1)},\\
H_{11} &= 0,\\
H_{12} &= 0,\\
H_{13} &= 0.
\end{aligned}
$$

A.3.2 Formules de récurrence pour les coefficients H

Pour $k \geq 3$ tours, nous allons établir des formules permettant d'obtenir les valeurs pour H pour le tour $k+1$, à partir des valeurs de H le tour k.

Pour établir ces formules, il suffit de remarquer que M_L^{k+1} avec permutations internes $(f_1, \ldots, f_{k+1})$ appliqué à $[L, R]$, est composé de M_L^1 avec permutation interne f_1 appliqué à $[L, R]$, et de M_L^k avec permutations internes $(f_2, \ldots, f_{k+1})$ appliqué à $[R, X^1]$ (figure A.5 pour M_L^k).

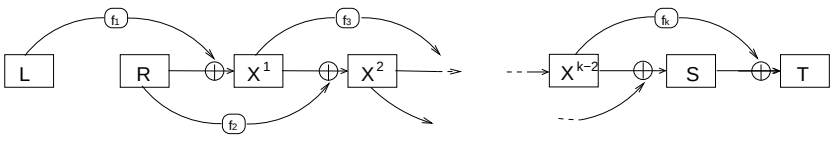

FIGURE A.5: $M_L^k(f_1, \ldots, f_k)([L, R]) = [S, T]$

Pour $k \geq 2$, notons H'_{c} la valeur de H dans le cas c pour $k+1$ tours, et H_{c} cette

valeur pour k tours. Les formules de récurrence sont les suivantes :

$$\begin{cases} H'_1 = \frac{|B_n|}{2^n-1}[(2^n-3)H_1 + H_2 + H_4] \\ H'_2 = \frac{|B_n|}{2^n-1}[(2^n-2)H_3 + H_5] \\ H'_3 = \mid B_n \mid \cdot H_1 \\ H'_4 = \frac{1}{2^n-1}[(2^n-2)H_1 + H_2] \\ H'_5 = \mid B_n \mid \cdot H_4 \\ H'_6 = \frac{|B_n|}{2^n-1}[(2^n-2)H_6 + H_7] \\ H'_7 = \mid B_n \mid \cdot H_8 \\ H'_8 = \mid B_n \mid \cdot H_6 \\ H'_9 = \frac{|B_n|}{2^n-1}[(2^n-3)H_9 + H_{10} + H_{12}] \\ H'_{10} = \frac{|B_n|}{2^n-1}[(2^n-2)H_{11} + H_{13}] \\ H'_{11} = H_9 \\ H'_{12} = \frac{|B_n|}{2^n-1}[(2^n-2)H_9 + H_{10}] \\ H'_{13} = \mid B_n \mid \cdot H_{12} \end{cases}$$

Notons que les formules données ci-dessus ne sont valables que pour un nombre de tours supérieur ou égale à 3. En effet, lors de l'établissement de ces formule, on suppose les blocs de sortie S_1, T_1, S_2, T_2 de M_L^{k+1} distincts des blocs de sortie de M_L^1 (ou des blocs d'entrée de M_L^k), dans la décomposition de M_L^{k+1} en M_L^1 et M_L^k.

Ces formules de récurrence permettent de trouver toutes les valeurs des coefficients H, pour tout $k \geq 3$, à partir des formules de H pour M_L^1 et M_L^{k-1}.

A.3.3 Évaluation asymptotique du comportement des ε

On note :

$$\varepsilon = \frac{H \cdot 2^{4n}}{\mid B_n \mid^k} - \frac{2^{2n}}{2^{2n}-1}.$$

Nous avons vu à la section 3.4 du chapitre 3, qu'à partir de la valeur ε_c (ε dans le cas c), il est possible de déduire rapidement la complexité de l'attaque deux points correspondant au cas c. On peut aussi voir que c'est cette valeur ε qui a servi lors des attaques sur 6 tours (section 3.2 du chapitre 3).

Dans la remarque de cette section 3.4, nous avons vu qu'une attaque donne une meilleure complexité pour ε grand et un nombre d'égalités sur les blocs d'entrée et de sortie demandées par l'attaque (n_e) petit. Plus précisément, le cas c donnant la meilleure complexité d'attaque est le cas permettant de réaliser le meilleur compromis entre une valeur ε_c grande et une valeur de n_e petite.

Les valeurs peuvent être obtenues directement à partir des valeurs de H, mais dans cette partie, nous allons prouver que ces valeurs décroissent (globalement, dans le sens où le sup de tous les ε décroît) d'un facteur au moins $\frac{1}{2^n}$ tous les deux tours. Ceci permet de justifier théoriquement que la complexité des attaques augmente bien avec le nombre de tours de schémas Misty L utilisés.

A.3.3.1 Formules de récurrence pour les ε

Les formules de récurrence données pour H dans la partie A.3.2, s'adaptent naturellement pour donner des formules de récurrence pour les ε.

Nous avons, pour deux tours :

$$\begin{aligned}
\varepsilon_1 &= \tfrac{2\cdot 2^{2n}}{(2^n-1)^2(2^n+1)} \simeq \tfrac{2}{2^n}\\
\varepsilon_2 &= -\overset{\circ}{1} = \tfrac{-2^{2n}}{(2^n-1)(2^n+1)} \simeq -1\\
\varepsilon_3 &= -\overset{\circ}{1} \simeq -1\\
\varepsilon_4 &= -\overset{\circ}{1} \simeq -1\\
\varepsilon_5 &= \tfrac{2^{3n}}{(2^n-1)(2^n+1)} \simeq 2^n\\
\varepsilon_6 &= \tfrac{2\cdot 2^{2n}}{(2^n-1)^2(2^n+1)} \simeq \tfrac{2}{2^n}\\
\varepsilon_7 &= -\overset{\circ}{1} \simeq -1\\
\varepsilon_8 &= -\overset{\circ}{1} \simeq -1\\
\varepsilon_9 &= -\overset{\circ}{1} \simeq -1\\
\varepsilon_{10} &= \tfrac{2^{3n}}{(2^n-1)(2^n+1)} \simeq 2^n\\
\varepsilon_{11} &= -\overset{\circ}{1} \simeq -1\\
\varepsilon_{12} &= -\overset{\circ}{1} \simeq -1\\
\varepsilon_{13} &= -\overset{\circ}{1} \simeq -1
\end{aligned}$$

Les formules de récurrence de la sous-section A.3.2 deviennent :

$$\left\{\begin{array}{rcl}
\varepsilon'_1 &=& \tfrac{1}{2^n-1}[(2^n-3)\varepsilon_1+\varepsilon_2+\varepsilon_4]\\
\varepsilon'_2 &=& \tfrac{1}{2^n-1}[(2^n-2)\varepsilon_3+\varepsilon_5]\\
\varepsilon'_3 &=& \varepsilon_1\\
\varepsilon'_4 &=& \tfrac{1}{2^n-1}[(2^n-2)\varepsilon_1+\varepsilon_2]\\
\varepsilon'_5 &=& \varepsilon_4\\
\varepsilon'_6 &=& \tfrac{1}{2^n-1}[(2^n-2)\varepsilon_6+\varepsilon_7]\\
\varepsilon'_7 &=& \varepsilon_8\\
\varepsilon'_8 &=& \varepsilon_6\\
\varepsilon'_9 &=& \tfrac{1}{2^n-1}[(2^n-3)\varepsilon_9+\varepsilon_{10}+\varepsilon_{12}]\\
\varepsilon'_{10} &=& \tfrac{1}{2^n-1}[(2^n-2)\varepsilon_{11}+\varepsilon_{13}]\\
\varepsilon'_{11} &=& \varepsilon_9\\
\varepsilon'_{12} &=& \tfrac{1}{2^n-1}[(2^n-2)\varepsilon_9+\varepsilon_{10}]\\
\varepsilon'_{13} &=& \varepsilon_{12}
\end{array}\right.$$

Le but est d'essayer de calculer l'évolution de chacun de ces ε. Continuons l'évaluation.

Nous avons, pour tous S_1, T_1, S_2, T_2 fixés :

$$\begin{aligned}
& \sum_{L_1,R_1,L_2,R_2} H =\mid B_n \mid^k \\
\Leftrightarrow \quad & \sum_{L_1,R_1,L_2,R_2} \frac{H \cdot 2^{4n}}{\mid B_n \mid^k} = 2^{4n} \\
\Leftrightarrow \quad & \sum_{L_1,R_1,L_2,R_2} \varepsilon + 2^{2n}(2^{2n}-1) \cdot \overset{\circ}{1} = 2^{4n} \\
\Leftrightarrow \quad & 2^{2n}(2^{2n}-1) \cdot \frac{2^{2n}}{2^{2n}-1} + \sum_{L_1,R_1,L_2,R_2} \varepsilon = 2^{4n} \\
\Leftrightarrow \quad & \sum_{L_1,R_1,L_2,R_2} \varepsilon = 0.
\end{aligned}$$

De manière symétrique, pour tous L_1, R_1, L_2, R_2 fixés :

$$\begin{aligned}
& \sum_{S_1,T_1,S_2,T_2} H =\mid B_n \mid^d \\
\Leftrightarrow \quad & \sum_{S_1,T_1,S_2,T_2} \varepsilon = 0.
\end{aligned}$$

A.3.3.2 Évaluation asymptotique du comportement des ε

Cas $S_1 \neq S_2$ et $S_1 \oplus S_2 \neq T_1 \oplus T_2$ (indices $1, 2, 3, 4, 5$) Les formules de récurrence pour les ε donnent :

$$\left\{ \begin{array}{lcl}
\varepsilon'_1 & = & \frac{1}{2^n-1}[(2^n-3)\varepsilon_1 + \varepsilon_2 + \varepsilon_4] \\
\varepsilon'_2 & = & \frac{1}{2^n-1}[(2^n-2)\varepsilon_3 + \varepsilon_5] \\
\varepsilon'_3 & = & \varepsilon_1 \\
\varepsilon'_4 & = & \frac{1}{2^n-1}[(2^n-2)\varepsilon_1 + \varepsilon_2] \\
\varepsilon'_5 & = & \varepsilon_4.
\end{array} \right.$$

Par ailleurs, l'équation précédente correspondant à la somme des ε sur les entrées possibles donne :

$$\begin{aligned}
& (2^n-1)(2^n-2)\varepsilon_1 + (2^n-1)\varepsilon_2 + (2^n-2)\varepsilon_3 + (2^n-1)\varepsilon_4 + \varepsilon_5 = 0 \\
\Leftrightarrow \quad & (2^n-2)\varepsilon_3 + \varepsilon_5 = -(2^n-1)(2^n-2)\varepsilon_1 + (2^n-1)\varepsilon_2 + (2^n-1)\varepsilon_4.
\end{aligned}$$

On déduit :

$$\left\{ \begin{array}{lcl}
\varepsilon'_1 & = & \frac{(2^n-3)\varepsilon_1}{2^n-1} + \frac{\varepsilon_2}{2^n-1} + \frac{\varepsilon_4}{2^n-1} \\
\varepsilon'_2 & = & (-2^n+2)\varepsilon_1 - \varepsilon_2 - \varepsilon_4 \\
\varepsilon'_4 & = & \frac{(2^n-2)\varepsilon_1}{2^n-1} + \frac{\varepsilon_2}{2^n-1} \\
\varepsilon'_3 & = & \varepsilon_1 \\
\varepsilon'_5 & = & \varepsilon_4
\end{array} \right.$$

En passant aux ε'' correspondant à M_L^{k+2} :

$$\left\{\begin{array}{lcl} \varepsilon''_1 & = & \frac{-\varepsilon_1-2\varepsilon'_1+\varepsilon'_4}{2^n-1} \\ \varepsilon''_2 & = & \varepsilon_1+\varepsilon'_1+\varepsilon'_4 \\ \varepsilon''_4 & = & \frac{-\varepsilon_1-\varepsilon'_1}{2^n-1} \\ \varepsilon'_3 & = & \varepsilon_1 \\ \varepsilon'_5 & = & \varepsilon_4 \end{array}\right.$$

De ces deux ensembles d'égalités, on déduit que ε_1 au tour décroît d'un facteur au moins 2^n tous les deux tours (ε_1 au tour k décroît de 2^n par rapport à la plus grande valeur de $\varepsilon_1, \varepsilon_2, \varepsilon_4$, au tour $k-2$). On peut observer le même phénomène pour ε_4. L'expression pour ε''_2, associée aux autres expression ci-dessus, permet encore de déduire la même chose. L'évolution de ε_3 est la même que ε_1 et celle de ε_5 la même que ε_4.

Cas $S_1 = S_2$ et $S_1 \oplus S_2 \neq T_1 \oplus T_2$ (indices 6,7,8) Les formules de récurrence pour les ε donnent :

$$\left\{\begin{array}{lcl} \varepsilon'_6 & = & \frac{1}{2^n-1}[(2^n-2)\varepsilon_6+\varepsilon_7] \\ \varepsilon'_7 & = & \varepsilon_8 \\ \varepsilon'_8 & = & \varepsilon_6 \end{array}\right.$$

Par ailleurs, l'équation précédente correspondant à la somme des ε sur les entrées possibles donne :

$$\begin{array}{cl} & (2^n-1)\varepsilon_6+\varepsilon_7+\varepsilon_8 = 0 \\ \Leftrightarrow & \varepsilon_8 = -(2^n-1)\varepsilon_6-\varepsilon_7 \end{array}$$

On déduit :

$$\left\{\begin{array}{lcl} \varepsilon'_6 & = & \frac{-\varepsilon_6-\varepsilon_8}{2^n-1} \\ \varepsilon'_8 & = & \varepsilon_6 \\ \varepsilon'_7 & = & \varepsilon_8 \end{array}\right.$$

L'équation pour ε'_6 montre que ε_6 décroît au moins d'un facteur 2^n par rapport à la plus grande des valeurs de ε_6 et ε_8 du tour précédent. ε_8 et ε_7 évoluent comme ε_6.

Cas $S_1 \oplus S_2 = T_1 \oplus T_2$ et $S_1 \neq S_2$ (indices 9,10,11,12,13) Les formules de récurrence pour les ε donnent :

$$\left\{\begin{array}{lcl} \varepsilon'_9 & = & \frac{1}{2^n-1}[(2^n-3)\varepsilon_9+\varepsilon_{10}+\varepsilon_{12}] \\ \varepsilon'_{10} & = & \frac{1}{2^n-1}[(2^n-2)\varepsilon_{11}+\varepsilon_{13}] \\ \varepsilon'_{11} & = & \varepsilon_9 \\ \varepsilon'_{12} & = & \frac{1}{2^n-1}[(2^n-2)\varepsilon_9+\varepsilon_{10}] \\ \varepsilon'_{13} & = & \varepsilon_{12} \end{array}\right.$$

Par ailleurs, l'équation précédente correspondant à la somme des ε sur les entrées possibles donne :

$$\begin{array}{cl} & (2^n-1)(2^n-2)\varepsilon_9+(2^n-1)\varepsilon_{10}+(2^n-2)\varepsilon_{11}+(2^n-1)\varepsilon_{12}+\varepsilon_{13} = 0 \\ \Leftarrow & (2^n-2)\varepsilon_{11}+\varepsilon_{13} = -(2^n-1)(2^n-2)\varepsilon_9-(2^n-1)\varepsilon_{10}-(2^n-1)\varepsilon_{12} \end{array}.$$

On déduit :

$$\left\{\begin{array}{rcl} \varepsilon'_9 & = & \frac{1}{2^n-1}[(2^n-3)\varepsilon_9+\varepsilon_{10}+\varepsilon_{12}] \\ \varepsilon'_{10} & = & (-2^n+2)\varepsilon_9-\varepsilon_{10}-\varepsilon_{12} \\ \varepsilon'_{12} & = & \frac{2^n-2}{2^n-1}\varepsilon_9+\frac{\varepsilon_{10}}{2^n-1} \\ \varepsilon'_{11} & = & \varepsilon_9 \\ \varepsilon_{13} & = & \varepsilon_{12} \end{array}\right.$$

Remarquons maintenant que pour deux tours, $\varepsilon_9 = \varepsilon_{12}$. Les relations de récurrence précédentes impliquent alors que pour tout $k \geq 2$, la valeurs de ε_9 au tour k et la même que celle de ε_{12}. L'ensemble de formules de récurrence se réécrit alors :

$$\left\{\begin{array}{rcl} \varepsilon'_9 & = & \frac{1}{2^n-1}[(2^n-2)\varepsilon_9+\varepsilon_{10}] \\ \varepsilon'_{10} & = & (-2^n+1)\varepsilon_9-\varepsilon_{10}=\varepsilon_{11} \\ \varepsilon'_{11} & = & \varepsilon_9 \\ \varepsilon'_{13} & = & \varepsilon_9 \\ \varepsilon_{12} & = & \varepsilon_9 \end{array}\right.$$

En passant aux ε'' correspondant à M_L^{k+2}, on obtient : $\varepsilon''_9 = -\frac{2\cdot\varepsilon_9}{2^n-1} + \frac{\varepsilon_9}{(2^n-1)^2}\frac{\varepsilon_{10}}{(2^n-1)^2}$. On en déduit que ε_9 au tour k, décroît d'un facteur au moins 2^n par rapport à ε_9 et ε_{10} du tour $k-2$. ε_{11}, ε_{12} et ε_{13} évoluent comme ε_9 et par suite ε_{10} également.

Finalement, les ε décroissent globalement d'un facteur au moins 2^n tous les deux tours.

A.3.3.3 Les ε pour trois et quatre tours

Ci-dessous les valeurs de ε pour trois et quatre tours. On peut aussi les calculer à partir des valeurs exactes de H (section 4.1.4 de la section 4.1).

3 tours.

$$\begin{array}{rcrcl} \varepsilon_1 & = & \frac{-4\cdot 2^{2n}}{(2^n-1)^3(2^n+1)} & \simeq & \frac{-4}{2^{2n}} \\ \varepsilon_2 & = & \frac{2\cdot 2^{2n}}{(2^n-1)^2(2^n+1)} & \simeq & \frac{2}{2^n} \\ \varepsilon_3 & = & \frac{2\cdot 2^{2n}}{(2^n-1)^2(2^n+1)} & \simeq & \frac{2}{2^n} \\ \varepsilon_4 & = & \frac{2^{2n}(2^n-3)}{(2^n-1)^3(2^n+1)} & \simeq & \frac{1}{2^n} \\ \varepsilon_5 & = & -\overset{\circ}{1}=\frac{-2^{2n}}{(2^n-1)(2^n+1)} & \simeq & -1 \\ \varepsilon_6 & = & \frac{2^{2n}(2^n-3)}{(2^n-1)^3(2^n+1)} & \simeq & \frac{1}{2^n} \\ \varepsilon_7 & = & -\overset{\circ}{1}=\frac{-2^{2n}}{(2^n+1)(2^n-1)} & \simeq & -1 \\ \varepsilon_8 & = & \frac{2\cdot 2^{2n}}{(2^n-1)^2(2^n+1)} & \simeq & \frac{2}{2^n} \\ \varepsilon_9 & = & \frac{2\cdot 2^{2n}}{(2^n-1)^2(2^n+1)} & \simeq & \frac{2}{2^n} \\ \varepsilon_{10} & = & -\overset{\circ}{1}=\frac{-2^{2n}}{(2^n-1)(2^n+1)} & \simeq & -1 \\ \varepsilon_{11} & = & -\overset{\circ}{1} & \simeq & -1 \\ \varepsilon_{12} & = & \frac{2\cdot 2^{2n}}{(2^n-1)^2(2^n+1)} & \simeq & \frac{2}{2^n} \\ \varepsilon_{13} & = & -\overset{\circ}{1} & \simeq & -1 \end{array}$$

4 tours

$$
\begin{array}{lcll}
\varepsilon_1 & = & \frac{-2^{2n}(2^n-7)}{(2^n-1)^4(2^n+1)} & \backsimeq \frac{-1}{2^{2n}} \\
\varepsilon_2 & = & \frac{2^{2n}(2^n-3)}{(2^n-1)^3(2^n+1)} & \backsimeq \frac{1}{2^n} \\
\varepsilon_3 & = & \frac{-4\cdot 2^{2n}}{(2^n-1)^3(2^n+1)} & \backsimeq \frac{-4}{2^{2n}} \\
\varepsilon_4 & = & \frac{-2\cdot 2^{2n}(2^n-3)}{(2^n-1)^4(2^n+1)} & \backsimeq \frac{-2}{2^{2n}} \\
\varepsilon_5 & = & \frac{2^{2n}(2^n-3)}{(2^n-1)^3(2^n+1)} & \backsimeq \frac{1}{2^n} \\
\varepsilon_6 & = & \frac{-2^{2n}(3\cdot 2^n-5)}{(2^n-1)^4(2^n+1)} & \backsimeq \frac{-3}{2^{2n}} \\
\varepsilon_7 & = & \frac{2\cdot 2^{2n}}{(2^n+1)(2^n-1)^2} & \backsimeq \frac{2}{2^n} \\
\varepsilon_8 & = & \frac{2^{2n}(2^n-3)}{(2^n-1)^3(2^n+1)} & \backsimeq \frac{1}{2^n} \\
\varepsilon_9 & = & \frac{2^{2n}(2^n-3)}{(2^n-1)^3(2^n+1)} & \backsimeq \frac{1}{2^n} \\
\varepsilon_{10} & = & \overset{\circ}{-1} & \backsimeq -1 \\
\varepsilon_{11} & = & \frac{2\cdot 2^{2n}}{(2^n-1)^2(2^n+1)} & \backsimeq \frac{2}{2^n} \\
\varepsilon_{12} & = & \varepsilon_9 & \backsimeq \frac{2}{2^n} \\
\varepsilon_{13} & = & \varepsilon_{11} & \backsimeq \frac{2}{2^n}
\end{array}
$$

A.4 Calcul des Coefficients H pour les schémas de Feistel avec permutations internes, Méthode par Récurrence

Dans cette section, nous montrons comment les coefficients H pour les schémas de Feistel avec permutations internes peuvent être obtenus par récurrence. Ceci permet également de valider les formules directes obtenues à la section A.2.

A.4.1 Coefficients H pour un tour et deux tours

A.4.1.1 Un tour

Dans le cas de ψ^1, nous avons (voir aussi figure A.6) :

$$
\begin{cases}
S = R \\
T = R \oplus f_1(L)
\end{cases}
$$

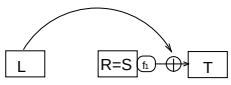

FIGURE A.6: Un tour de Schéma de Feistel

Dans le cadre d'une attaque deux points, pour ψ^1, on a nécessairement :

$$
\begin{cases}
S_1 = R_1,\ S_2 = R_2 \\
R_1 = R_2 \Leftrightarrow T_1 \oplus R_1 = L_2 \oplus L_2.
\end{cases}
$$

Ainsi, si ces conditions ne sont pas vérifiées, $H = 0$. Lorsqu'elles le sont, comme f_1 s'applique sur le bloc L, si $L_1 = L_2$, on a $H = \frac{|B_n|}{2^n}$, et $H = \frac{|B_n|}{2^n(2^n-1)}$, sinon.

Revenons aux 13 cas distingués pour un nombre de tours $k = 1$ impair (voir sous-section A.2.4). Notons H_c la valeur de H pour le cas c. On obtient, pour un tour de schéma du type Misty :

$$\begin{aligned}
H_1^{\text{imp}} &= 0,\\
H_2^{\text{imp}} &= 0,\\
H_3^{\text{imp}} &= \tfrac{|B_n|}{2^n(2^n-1)},\\
H_4^{\text{imp}} &= 0,\\
H_5^{\text{imp}} &= 0,\\
H_6^{\text{imp}} &= 0,\\
H_7^{\text{imp}} &= 0,\\
H_8^{\text{imp}} &= 0,\\
H_9^{\text{imp}} &= 0,\\
H_{10}^{\text{imp}} &= 0,\\
H_{11}^{\text{imp}} &= 0,\\
H_{12}^{\text{imp}} &= \tfrac{|B_n|}{2^n},\\
H_{13}^{\text{imp}} &= 0.
\end{aligned}$$

A.4.1.2 Deux tours

Pour deux tours, on a les relations suivantes (voir aussi figure A.7) :

$$\begin{cases} S = f_1(R) \oplus L \\ T = f_2(S) \oplus R. \end{cases}$$

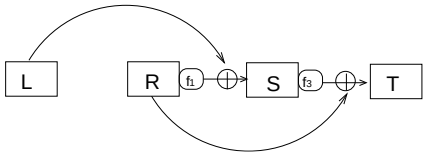

FIGURE A.7: Deux tours de schémas de Feistel

Considérons les onze cas distingués pour un nombre de tours $k = 2$ pair (voir sous-sectionA.2.4). On a les valeurs suivantes pour le coefficient H pour deux tours et pour chaque cas

$$
\begin{aligned}
H_1^{\text{pair}} &= \tfrac{|B_n|^2}{2^{2n}(2^n-1)^2},\\
H_2^{\text{pair}} &= 0,\\
H_3^{\text{pair}} &= \tfrac{|B_n|^2}{2^{2n}(2^n-1)^2},\\
H_4^{\text{pair}} &= 0,\\
H_5^{\text{pair}} &= \tfrac{|B_n|^2}{2^{2n}(2^n-1)^2},\\
H_6^{\text{pair}} &= 0,\\
H_7^{\text{pair}} &= 0,\\
H_8^{\text{pair}} &= \tfrac{|B_n|^2}{2^{n}(2^n-1)\cdot 2^n},\\
H_9^{\text{pair}} &= 0,\\
H_{10}^{\text{pair}} &= 0,\\
H_{11}^{\text{pair}} &= 0.
\end{aligned}
$$

A.4.2 Formules de récurrence pour les coefficients H

Pour $k \geq 3$ tours, nous allons établir des formules permettant d'obtenir les valeurs pour H pour le tour $k+1$, à partir des valeurs de H le tour k.

Pour établir ces formules, il suffit de remarquer que ψ^{k+1} avec permutations internes $(f_1, \ldots, f_{k+1})$ appliqué à $[L, R]$, est composé de $\psi^k 1$ avec permutation interne $(f_1, \ldots, f_k)$ appliqué à $[L, R]$, et de ψ^1 avec permutation interne f_{k+1} appliqué à $[X^{k-3}, S]$. (figure A.8 pour M_L^k).

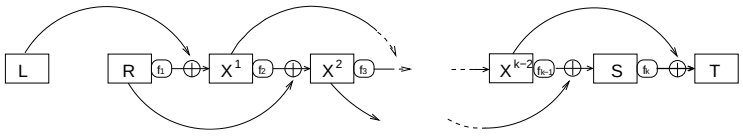

FIGURE A.8: $\psi^k(f_1, \ldots, f_k)([L, R]) = [S, T]$

Pour $k \geq 2$, notons H'_{c} la valeur de H dans le cas c pour $k+1$ tours, et H_{c} cette valeur pour k tours. Les formules de récurrence sont les suivantes :

Pour les cas impairs :

$$
\begin{aligned}
H_1^{\text{imp}} &= \frac{\mid B_n \mid}{2^n-1}\left[(2^n-3)\,H_1^{\text{pair}} + H_2^{\text{pair}} + H_4^{\text{pair}}\right] \\
H_2^{\text{imp}} &= \frac{\mid B_n \mid}{2^n-1}\left[(2^n-2)\,H_1^{\text{pair}} + H_2^{\text{pair}}\right] \\
H_3^{\text{imp}} &= \frac{\mid B_n \mid}{2^n-1}\left[(2^n-3)\,H_4^{\text{pair}} + H_8^{\text{pair}} + H_{10}^{\text{pair}}\right] \\
H_4^{\text{imp}} &= \frac{\mid B_n \mid}{2^n-1}\left[(2^n-3)\,H_2^{\text{pair}} + H_6^{\text{pair}} + h_8^{\text{pair}}\right] \\
H_5^{\text{imp}} &= \frac{\mid B_n \mid}{2^n-1}\left[(2^n-2)\,H_1^{\text{pair}} + H_4^{\text{pair}}\right] \\
H_6^{\text{imp}} &= \frac{\mid B_n \mid}{2^n-1}\left[(2^n-2)\,H_2^{\text{pair}} + H_8^{\text{pair}}\right] \\
H_7^{\text{imp}} &= \frac{\mid B_n \mid}{2^n-1}\left[(2^n-2)\,H_2^{\text{pair}} + H_6^{\text{pair}}\right] \\
H_8^{\text{imp}} &= H_7^{\text{pair}} \\
H_9^{\text{imp}} &= \frac{\mid B_n \mid}{2^n-1}\left[(2^n-2)\,H_4^{\text{pair}} + H_{10}^{\text{pair}}\right] \\
H_{10}^{\text{imp}} &= \mid B_n \mid \cdot H_3^{\text{pair}} \\
H_{11}^{\text{imp}} &= \frac{\mid B_n \mid}{2^n-1}\left[(2^n-2)\,H_4^{\text{pair}} + H_8^{\text{pair}}\right] \\
H_{12}^{\text{imp}} &= \mid B_n \mid \cdot H_{11}^{\text{pair}} \\
H_{13}^{\text{imp}} &= \mid B_n \mid \cdot H_9^{\text{pair}}
\end{aligned}
$$

Pour les cas pairs :

$$
\begin{aligned}
H_1^{\text{pair}} &= \frac{\mid B_n \mid}{2^n-1}\left[(2^n-3)\,H_1^{\text{imp}} + H_3^{\text{imp}} + H_4^{\text{imp}}\right] \\
H_2^{\text{pair}} &= \mid B_n \mid \cdot H_5^{\text{imp}} \\
H_3^{\text{pair}} &= \frac{\mid B_n \mid}{2^n-1}\left[(2^n-2)\,H_1^{\text{imp}} + H_3^{\text{imp}}\right] \\
H_4^{\text{pair}} &= \frac{\mid B_n \mid}{2^n-1}\left[(2^n-2)\,H_1^{\text{imp}} + H_4^{\text{imp}}\right] \\
H_5^{\text{pair}} &= \frac{\mid B_n \mid}{2^n-1}\left[(2^n-2)\,H_5^{\text{imp}} + H_9^{\text{imp}}\right] \\
H_6^{\text{pair}} &= \mid B_n \mid \cdot H_6^{\text{imp}} \\
H_7^{\text{pair}} &= \mid B_n \mid \cdot H_{10}^{\text{imp}} \\
H_8^{\text{pair}} &= \mid B_n \mid \cdot H_9^{\text{imp}} \\
H_9^{\text{pair}} &= \frac{\mid B_n \mid}{2^n-1}\left[(2^n-2)\,H_5^{\text{imp}} + H_6^{\text{imp}}\right] \\
H_{10}^{\text{pair}} &= \frac{\mid B_n \mid}{2^n-1}\left[(2^n-2)\,H_2^{\text{imp}} + H_7^{\text{imp}}\right] \\
H_{11}^{\text{pair}} &= \mid B_n \mid \cdot H_{13}^{\text{imp}}
\end{aligned}
$$

Ces relations de récurrence permettent d'obtenir toutes les valeurs des coefficients H pour n'importe quel nombre de tours. Nous avons également pu valider, pour les premiers tours, les formules directes de la section A.2. L'analyse du comportement asymptotique global des ε n'a pas été faite pour les schémas de Feistel avec permutations internes. L'analyse semble plus délicate que pour le cas de schémas du type Misty. Par exemple, pour ces schémas Misty L, on peut voir dans les tableaux de la section 4.2 que l'évolution des ε ou de la complexité des attaques est assez régulière. Par contre, dans le cas des schémas de Feistel avec permutations internes, cette évolution est plus complexe. Des formules de récurrence permettant de prouver la décroissance des ε doivent cependant pouvoir être établies.

Bibliographie

[AB96] R. Anderson and E. Biham. Two Practical and Provably Secure Block Ciphers : BEAR and LION, 1996. 4

[AIK+00] K. Aoki, T. Itchikawa, M. Kanda, M. Matsui, J. Nakajima S. Moriai, and T. Tokita. Camellia : A 128-bit Block Cipher Suitable for Multiple Platforms - Design and Analysis. In *SAC 2000*, volume 2012, pages 39–56. Springer, 2000. 4

[AV96] W. Aiello and R. Venkatesan. Foiling Birthday Attacks in Length-Doubling Transformations - Benes : A Non-Reversible Alternative to Feistel. In *Advances in Cryptology – EUROCRYPT 1996*, volume 1070 of *Lecture Notes in Computer Science*, pages 307–320. Springer-Verlag, 1996. 16

[Bar04] M. Bardet. *Étude des Systèmes Algébriques Surdéterminés. Applications aux Codes Correcteurs et à la Cryptographie.* PhD thesis, Université de Paris VI, 2004. 88, 90, 91, 130

[BCP97] W. Bosma, J. J. Cannon, and C. Playoust. The Magma Algebra System I : The User Language. *Journal of Symbolic Computation*, 24(3/4) :235–265, 1997. 104, 130, 131

[BFFP10] C. Bouillaguet, J.-C. Faugère, P.-A. Fouque, and L. Perret. Isomorphism of Polynomials : New Results, October 2010. Unpublished manuscript. 93

[BFJT09] C. Bouillaguet, P.-A. Fouque, A. Joux, and J. Treger. A Family of Weak Keys for HFE and the Practical Corresponding Key Recovery. In *SCC 2010*, 2009. Submitted at the Journal of Mathematical Cryptology. 77, 90, 92, 111, 134, 139

[BFSY05] M. Bardet, J.-C. Faugère, B. Salvy, and B.-Y. Yang. Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems. In *MEGA 2005*, 2005. 90, 91, 111, 130

[BGP06] Côme Berbain, H. Gilbert, and J. Patarin. QUAD : A Practical Stream Cipher with Provable Security. In Vaudenay [Vau06], pages 109–128. 140

[Bih97] E. Biham. Cryptanalysis of Ladder-DES. In *FSE 1997*, volume 1267, pages 134–138. Springer, 1997. 4

[Buc65] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem Nulldimensionalen Polynomideal.* PhD thesis, University of Innsbruck, 1965. 84, 88, 89

[BWP05] A. Braeken, C. Wolf, and B. Preneel. A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes. In *CT-RSA 2005*, volume 3376 of *LNCS*, pages 29–43. Springer, February 2005. 112, 139

[CKPS00] N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In *Advances in Cryptology – EUROCRYPT 2000*, pages 392–407, 2000. 88

[CLO07] D. A. Cox, J. B. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007. 84, 86, 89

[Cou01] N. Courtois. The Security of Hidden Field Equations (HFE). In *CT-RSA 2001*, volume 2020, pages 156–167. Springer, 2001. 114

[DFS07] V. Dubois, P.-A. Fouque, and J. Stern. Cryptanalysis of SFLASH with Slightly Modified Parameters. In *Advances in Cryptology – EUROCRYPT 2007*, volume 4515, pages 264–275. Springer, 2007. 95, 115

[DFSS07] V. Dubois, P.-A. Fouque, A. Shamir, and J. Stern. Practical Cryptanalysis of SFLASH. *Advances in Cryptology - CRYPTO'07*, 4622 :1–12, 2007. 95, 115, 139

[DGF06] V. Dubois, L. Granboulan, and P.-A. Fouque. An Efficient Provable Distinguisher for HFE. In *ICALP 2006*, volume 4052, pages 156–167. Springer, 2006. 115, 139

[DSW08] J. Ding, D. Schmidt, and F. Werner. Algebraic Attack on HFE Revisited. In Tzong-Chen Wu, Chin-Laung Lei, Vincent Rijmen, and Der-Tsai Lee, editors, *ISC 2008*, volume 5222 of *Lecture Notes in Computer Science*, pages 215–227. Springer, 2008. 111

[Dub07] V. Dubois. *Cryptanalyse de Schémas Multivariés*. PhD thesis, Université Paris VI, 2007. 95, 115

[Fau99] J.-C. Faugère. A New Efficient Algorithm for Computing Gröbner Bases (F4). *Journal of Pure and Applied Algebra*, 139 :61–88, June 1999. 88

[Fau02] J.-C. Faugère. A New Efficient Algorithm for Computing Gröbner Bases Without Reduction to Zero (F5). In *ISSAC 2002*, pages 75–83. ACM Press, July 2002. isbn : 1-58113-484-3. 88, 89, 110, 111, 114

[FGLm93] J.-C. Faugère, P. Gianni, D. Lazard, and T. mora. Efficient Computation of Zero-Dimensional Gröbner Bases. *Journal of Symbolic Computation*, 16 :329 – 344, 1993. 91

[FGS05] P.-A. Fouque, L. Granboulan, and J. Stern. Differential Cryptanalysis for Multivariate Schemes. In *Advances in Cryptology – EUROCRYPT 2005*, volume 3494, pages 341 – 353. Springer, 2005. 114, 115

[FJ03a] J.-C. Faugère and A. Joux. Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 44–60. Springer, 2003. 83, 95, 111, 114, 115

[FJ03b] J.-C. Faugère and A. Joux. Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases. In *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *LNCS*, pages 44–60. Springer, 2003. 97

[FJPT10] J.-C. Faugère, A. Joux, L. Perret, and J. Treger. Cryptanalysis of the Hidden Matrix Cryptosystems. In *LATINCRYPT 2010*, 2010. 77, 90, 97, 100, 138

[FMR10] P.-A. Fouque and G. Macariot-Rat. Pencils, Kernels and Differentials : Revisited Tools for Multivariate Cryptology, 2010. Unpublished Manuscript - Submitted to CRYPTO 2010. 95

[FMRS08] P.-A. Fouque, G. Macario-Rat, and J. Stern. Key Recovery on Hidden Monomial Multivariate Schemes. In Nigel P. Smart, editor, *Advances in Cryptology – EUROCRYPT 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 2008. 92

[FP06] J.-C. Faugère and L. Perret. Polynomial Equivalence Problems : Algorithmic and Theoretical Aspects. In Vaudenay [Vau06], pages 30–47. 93

[FY30] A. Fraenkel and Y. Yesha. Complexity of Problems in Games, Graphs and Algebraic Equations. *Discrete Appl. Maths*, 1 :369–380, 15-30. 79

[Gan59] F. G. Gantmacher. *The Theory of Matrices*, volume 1. Chelsea Publishing Company, 1959. 98

[GJS06] L. Granboulan, A. Joux, and J. Stern. Inverting HFE Is Quasipolynomial. In *Advances in Cryptology – CRYPTO 2006*, pages 345–356, 2006. 95, 97, 114, 115, 139

[GM01] H. Gilbert and M. Minier. New Results on the Pseudorandomness of Some Blockcipher Constructions. In *FSE 2001*, volume 2355 of *Lecture Notes in Computer Science*, pages 248–266. Springer-Verlag, 2001. 7, 9, 27

[GM02] H. Gilbert and M. Minier. Cryptanalysis of SFLASH. In L. R. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 288–298. Springer, 2002. 95, 112, 139

[Goz97] Y. Gozard. *Théorie de Galois*. Ellipses Marketing, 1997. 81, 82

[GP97] L. Goubin and J. Patarin. Assymetric Cryptography with S-Boxes. In *ICICS 1997*, volume 1334, pages 369–380. Lecture Notes in Computer Science, 1997. 79

[Hir64] H. Hironaka. Resolution of Singularities of an Algebraic Variety over a Field of Characteristic Zero. *Ann. Math.*, 79 :109–326, 1964. 84

[IM85] H. Imai and T. Matsumoto. Algebraic Methods for Constructing Asymmetric Cryptosystems. In *AAECC-3 1985*, volume 229, pages 108–119. Lecture Notes in Computer Science, 1985. 98, 104, 138

[Jou09] A. Joux. *Algorithmic Cryptanalysis*, volume 1 of *1*. Chapman & Hall, 2009. 84, 88

[Jut98] C. S. Jutla. Generalised Birthday Attacks on Unbalanced Feistel Networks. In *Advances in Cryptology – CRYPTO 1998*, volume 1462, pages 186–199. Springer, 1998. 3, 9

[Ka] Specification of the 3GPP Confidentiality and Integrity Algorithm KASUMI. 7

[Knu98] L. R. Knudsen. DEAL - A 128-bit Block Cipher. Technical report, Technical report number 151, University of Bergen, Norway – NIST AES Proposal, 1998. Available at `http ://www2.mat.dtu.dk/people/Lars.R.Knudsen/newblock.html`. 4

[Knu02] L. R. Knudsen. The Security of Feistel Ciphers with Six Rounds or Less. *Journal of Cryptology*, 15 :207–222, 2002. 4, 12, 17

[Kob98] N. Koblitz. *Algebraic Aspects of Cryptography.*, volume 3 of *Algorithms and Computation in Mathematics*. Springer-Verlag, 1998. 80

[KPG99] A. Kipnis, J. Patarin, and L. Goubin. Unbalanced Oil and Vinegar Signature. In *Advances in Cryptology – EUROCRYPT 1999*, volume 1592 of *Lecture Notes in Computer Science*, pages 206–222. Springer-Verlag, 1999. 96, 112, 140

[KS98] A. Kipnis and A. Shamir. Cryptanalysis of the Oil and Vinegar Signature Scheme. In *CRYPTO 98*, volume 1462, pages 257–266. Springer, 1998. 96

[KS99] A. Kipnis and A. Shamir. Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In Michael J. Wiener, editor, *Advances in Cryptology – CRYPTO 1999*, volume 1666 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 1999. 114

[KW02] L. Knudsen and D. Wagner. Integral Cryptanalysis. In *FSE 2002*, volume 2365 of *Lecture Notes in Computer Science*, pages 112–127. Springer-Verlag, 2002. 7, 27

[Laz83] D. Lazard. Gaussian Elimination and Resolution of Systems of Algebraic Equations. *EUROCAL 83*, 162 :146–157, 1983. 88

[LM91] Xuejia Lai and James. L Massey. A Proposal for a New Block Encrytption Standard. In *Advances in Cryptology – EUROCRYPT 1990*, volume 473 of *Lecture Notes in Computer Science*, pages 389–404. Springer-Verlag, 1991. 6

[LN96] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 1996. 81, 82

[LR88] M. Luby and C. Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM Journal on Computing*, 17 n.2 :373–386, 1988. 3, 12, 16

[Mac16] F. S. Macaulay. The Algebraic Theory of Modular Systems. In *Cambridge Mathematical Library*. Cambridge University Press, 1916. 88

[Mat97] M. Matsui. New Block Encrytpion Algorithm MISTY. In *FSE 1997*, volume 1267 of *Lecture Notes in Computer Science*, pages 54–68. Springer-Verlag, 1997. 6, 7

[MI88] T. Matsumoto and H. Imai. Public Quadratic Polynomial-tuples for Efficient Signature-Verification and Message-Encryption. In *Advances in Cryptology – EUROCRYPT 1988*, volume 330 of *LNCS*, pages 419–453. Springer–Verlag, 1988. 93, 94, 111, 139

[Nac01] David Naccache, editor. *Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, April 8-12, 2001, Proceedings*, volume 2020 of *Lecture Notes in Computer Science*. Springer, 2001. 180

[NPT09] V. Nachef, J. Patarin, and J. Treger. Generic Attacks on Misty Schemes, Extended Version. Cryptology eprint Archive, Report 2009-405, 2009. 35

[NPT10] V. Nachef, J. Patarin, and J. Treger. Generic Attacks on Misty Schemes. In *LATINCRYPT 2010*, 2010. 7, 9, 11, 19, 47, 138

[Nyb96] K. Nyberg. Linear Approximation of Block Ciphers. In *Advances in Cryptology – EUROCRYPT 1994*, volume 950, pages 439–444. Springer, 1996. 4

[Pat91] J. Patarin. *Étude des Générateurs de Permutations Pseudo-Aléatoires Basés sur le Schéma du DES*. PhD thesis, Université de Paris VI, 1991. 44, 137

[Pat95] J. Patarin. Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88. *Advances in Cryptology - CRYPTO'95*, 963 :248–261, 1995. 94, 95, 99, 111, 116, 122, 139

[Pat96] J. Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP) : Two new families of asymmetric algorithms. In *Advances in Cryptology – EUROCRYPT 1996*, volume 1070 of *LNCS*, pages 33–48. Springer–Verlag, 1996. 77, 84, 92, 94, 97, 111, 113, 114, 132, 133, 139

[Pat97] J. Patarin. The Oil and Vinegar Signature Scheme. presented at the Dagstuhl Workshop on Cryptography, 1997. 80

[Pat01] J. Patarin. Generic Attacks on Feistel Schemes. In *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 222–238. Springer-Verlag, 2001. 9, 12, 14, 15, 16, 19, 22, 59, 70

[PCG98a] J. Patarin, N. Courtois, and L. Goubin. C^*_{-+} and HM : Variations on Two Schemes of T.Matsumoto and H.Imai. In *Advances in Cryptology – ASIACRYPT 1998*, volume 1514, pages 35–50. Springer, 1998. 77, 95, 98, 99, 100, 103, 104, 138

[PCG98b] J. Patarin, N. Courtois, and L. Goubin. C^{*-+} and HM : Variations on Two Schemes of T.Matsumoto and H.Imai, Extended Version. Available From the Authors, 1998. 101, 104

[PCG01a] J. Patarin, N. Courtois, and L. Goubin. FLASH, a Fast Multivariate Signature Algorithm. In Naccache [Nac01], pages 298–307. 80, 115

[PCG01b] J. Patarin, N. Courtois, and L. Goubin. QUARTZ, 128-Bit Long Digital Signatures. In Naccache [Nac01], pages 282–297. 80, 113

[PGC98] J. Patarin, L. Goubin, and N. Courtois. Improved Algorithms for Isomorphisms of Polynomials. In *Advances in Cryptology – EUROCRYPT 1998*, pages 184–200, 1998. 92

[Pir06] G. Piret. Luby-Rackoff revisited : On the Use of Permutations as Inner Functions of a Feistel Scheme. *Designs, Codes and Cryptography*, 39, no.2 :233–245, 2006. 4, 9

[PM06] J. Patarin and A. Montreuil. Benes and Butterfly Schemes Revisited. In *ICISC 2006*, volume 3935, pages 92–116. Springer, 2006. 9

[PNB06a] J. Patarin, V. Nachef, and C. Berbain. Generic Attacks on Unbalanced Feistel Schemes with Contracting Functions. In *Advances in Cryptology – ASIACRYPT 2006*, volume 4284, pages 396–411. Springer, 2006. 4, 9, 31, 47

[PNB06b] J. Patarin, V. Nachef, and C. Berbain. Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions, Extended Version, 2006. Available from the authors. 4, 9, 47

[PQ05] G. Piret and J.-J. Quisquater. Security of the MISTY Structure in the Luby-Rackoff Model : Improved results. In *SAC 2005*, volume 3357 of *Lecture Notes in Computer Science*, pages 100–115. Springer-Verlag, 2005. 7

[RPW97] R. Rijmen, B. Preneel, and E. De Win. On Weakness of Non-Surjective Round Functions. *Designs, Codes and Criptography*, 12, no.3 :253–266, 1997. 4, 137

[SFL] SFLASH, a Fast Asymetric Signature Scheme for Low Cost Smart Cards. `http://www.nessie.org`. 95

[SK96] B. Schneier and J. Kelsey. Unbalanced Feistel Networks and Block Cipher Design. In *FSE 1996*, volume 1039, pages 121–144. Springer, 1996. 3

[Suga] M. Sugita. Pseudorandomness of a Block Cipher MISTY. Technical report, Technical Report of IEIECE, ISEC 96-9. 7

[Sugb] M. Sugita. Pseudorandomness of a Block Cipher with Recursive Strictures. Technical report, Technical Report of IEIECE, ISEC 97-9. 7

[SZ97] K. Sakurai and Y. Zheng. On Non-Pseudorandomness from Block Ciphers with Provable Immunity Against Linear Cryptanalysis. In *IEICE 1997*, volume E80-A,n.1, 1997. 7, 22, 24

[TP09] J. Treger and J. Patarin. Generic Attacks on Feistel Networks with Internal Permutations. In *Progresses in Cryptology – AFRICACRYPT 2009*, Lecture Notes in Computer Science. Springer-Verlag, 2009. 4, 9, 11, 12, 19, 31, 47, 137, 138

[Vau06] Serge Vaudenay, editor. *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in Computer Science*. Springer, 2006. 175, 177

[WDGY05] Z. Wu, J. Ding, J. E. Gower, and D. Ye. Perturbed Hidden Matrix Cryptosystems. *ICCSA*, 1462 :595–602, 2005. 138

[WP05a] C. Wolf and B. Preneel. Large Superfluous Keys in Multivariate Quadratic Asymmetric Systems. In Serge Vaudenay, editor, *PKC 2005*, volume 3386 of *Lecture Notes in Computer Science*, pages 275–287. Springer, 2005. 113

[WP05b] C. Wolf and B. Preneel. Taxonomy of Public Key Schemes Based on the Problem of Multivariate Quadratic Equations. Cryptology ePrint Archive, Report 2005/077, 2005. `http://eprint.iacr.org/`. 80