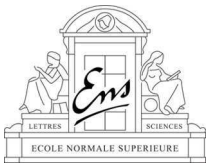
Cryptanalyse de Schémas Multivariés

Vivien Dubois



École normale supérieure
Département d'Informatique

Université Paris VI – Pierre et Marie Curie

Cryptanalyse de Schémas Multivariés

THÈSE

présentée et soutenue publiquement le 27 septembre 2007

pour l'obtention du

Doctorat de l'Université Paris VI
Spécialité : informatique

par

Vivien Dubois

Composition du jury

Directeur de thèse :	Jacques Stern (École normale supérieure)
Rapporteurs :	Jintai Ding (University of Cincinnati, USA) Henri Gilbert (France Télécom R&D) Louis Goubin (Université de Versailles Saint-Quentin)
Examinateurs :	Louis Granboulan (EADS Innovation Works) Reynald Lercier (DGA – Celar) Adi Shamir (Weizmann Institute of Science, Israel) Michèle Soria (Université Paris VI)

Travaux effectués au Laboratoire d'Informatique de l'École normale supérieure,
45 rue d'Ulm, 75230 Paris Cedex 05

Table des matières

Première partie

Introduction et préliminaires

Chapitre 1

Introduction à la Cryptographie Multivariée

La cryptographie multivariée peut être définie comme la cryptographie à clé publique basée sur la difficulté de résoudre des systèmes polynomiaux à plusieurs variables. Bien que la recherche de tels schémas soit apparue dès le début des années 80, elle s'est surtout développée depuis une dizaine d'années, et a conduit à l'émergence de plusieurs propositions jugées prometteuses. En particulier, deux schémas multivariés – SFLASH et QUARTZ – sont recommandés par le consortium européen NESSIE depuis 2003. Comparés aux schémas traditionnels, les schémas multivariés disposent de plusieurs atouts : ils sont généralement assez économiques en ressources de calcul, pouvant même être implantés sur carte sans cryptoprocesseur, et certains permettent la génération de signatures très courtes, d'une centaine de bits seulement. En contrepartie, leurs tailles de clés sont plus importantes, tout en restant raisonnables. Les schémas multivariés se posent ainsi en alternative possible aux schémas traditionnels basés sur des problèmes de théorie des nombres, et constituent des solutions efficaces à l'implantation des fonctionnalités de la cryptographie à clé publique.

Dans ce chapitre d'introduction, nous présentons les différents développements de la cryptographie multivariée, aussi bien sous l'angle constructif que cryptanalytique, et situons la présente thèse par rapport à ces développements. Nous commençons par un bref rappel des initiatives historiques qui ont donné naissance à la cryptographie multivariée ainsi que leurs motivations respectives. Nous décrivons ensuite brièvement les diverses constructions proposées et précisons les termes en lesquels la cryptographie multivariée se définit sous sa forme actuelle. Après cela, nous décrivons les différentes méthodes de résolution de systèmes polynomiaux et leur impact sur les instances particulières correspondant aux divers schémas proposés. Enfin, nous présentons les différents résultats développés durant la thèse et l'organisation du mémoire.

1.1 Les origines

Les premières tentatives de construction de schémas à clé publique basés sur des polynômes multivariés apparaissent dès le début des années 80 avec les travaux de Matsumoto et Imai [60, 47, 59], Fell et Diffie [38], et Ong, Schnorr, Shamir [65, 66, 77]. Si tous ces travaux partagent la motivation commune d'une recherche de performances supérieures à RSA, ils consistent toutefois en trois approches très différentes. L'approche de Ong, Schnorr, Shamir [65, 66] est probablement celle qui s'éloigne le moins de la construction RSA originale. Dans le schéma RSA, la vérification de signature consiste en l'évaluation d'un polynôme $P(x) = x^e$ sur $\mathbb{Z}_N$ où (N, e) est la clé publique et N est de factorisation pq inconnue ; le degré e de ce polynôme peut être choisi petit (environ 16 bits est le choix recommandé) afin de rendre cette opération de vérification efficace. En revanche, la génération de signature est relativement coûteuse car elle nécessite l'évaluation du polynôme inverse $P^{-1}(x) = x^d$ où d est la clé secrète et de taille comparable à N. Toutefois, pour un schéma de signature, rien n'impose que l'équation polynomiale $P(x) = m$ admette une unique solution dans $\mathbb{Z}_N$, il suffit seulement qu'une telle solution soit difficile à trouver. Dans [65, 66], Ong, Schnorr et Shamir proposent de substituer à l'équation $P(x) = m$ une équation multivariée $P(x_1, \ldots, x_k) = m$ sur $\mathbb{Z}_N$. Une signature consiste alors en un k-uplet $(s_1, \ldots, s_k)$ d'entiers modulo N, et vérifier la validité de cette signature est efficace lorsque P est de petit degré. Lorsque P admet une forme spécifique cachée, la génération de signature peut être également rendue efficace en utilisant les degrés de liberté supplémentaires : Ong, Schnorr et Shamir proposent de construire P comme la transformée par une matrice entière S inversible modulo N d'un polynôme de la forme $y_1.P'(y_2, \ldots, y_k)$; de cette façon, une signature pour un message m s'obtient en choisissant arbitrairement $y_2, \ldots, y_k$, en calculant $y_1 = m/P'(y_2, \ldots, y_k)$ modulo N (une valeur aléatoire de $\mathbb{Z}_N$ étant inversible avec forte probabilité lorsque N est grand), puis en appliquant le changement de variables inverse S^{-1} pour obtenir la signature $x_1, \ldots, x_k$. La sécurité de ce schéma se rapporte à la difficulté de calculer le changement de variables S sans la factorisation de N. Malheureusement, les deux instanciations proposées, pour lesquelles la condition de sécurité précédente admet des termes précis [65, 66], ont été cassées par Pollard, Schnorr [76], et Estes, Adleman, Kompella, McCurley et Miller [30]. Une réparation de la première instanciation [65] plus tard proposée par Shamir [77] a aussi été cassée par Coppersmith, Stern et Vaudenay [15].

Une autre tentative intéressante proposée par Fell et Diffie [38] avait pour motivation initiale de réduire l'écart entre cryptographie symétrique et asymétrique, autant sur le plan des mathématiques sous-jacentes que des performances. Ils proposaient alors de construire des fonctions à sens unique avec trappe comme composition itérée de permutations dépendant d'une fonction polynomiale secrète, d'une manière proche d'un schéma de Feistel. Chaque tour consiste en l'application de la permutation $(x_1 + g(x_2, \ldots, x_k), x_2, \ldots, x_k)$, où g est le polynôme secret, puis une rotation vers la droite des coordonnées, et est aisément inversé lorsque g est connu. La clé publique est le n-uplet de polynômes multivariés résultant de la composition

des multiples tours. Malheureusement, ce schéma possède deux défauts majeurs : le degré des polynômes multivariés formant la clé publique est exponentiel en le nombre de tours, ce qui oblige à limiter le nombre de tours afin de contenir sa taille, mais pire encore, l'inverse de la clé publique est de même degré que la clé publique elle-même. Il résulte de cette dernière observation que, lorsque le degré de la clé publique est effectivement pris petit, l'inverse de cette clé publique peut être déterminée en résolvant les coefficients de ces polynômes-coordonnées à partir de couples clair-chiffrés. Comme estimé par Fell et Diffie eux-mêmes [38], il est alors contradictoire d'obtenir de ce schéma à la fois sécurité et efficacité.

Une troisième voie, la plus ancienne en réalité, a été proposée par Matsumoto et Imai [60, 47, 59]. Au début des années 80, Matsumoto, Imai et leurs collaborateurs ont conçu plusieurs schémas à clé publique à partir de polynômes sur des corps finis sur le principe de la *représentation obscure* : la clé publique admet une représentation cachée sans laquelle il doit être impossible en pratique de déchiffrer. Pour l'un de ces schémas, appelé « Scheme A » [60, 47], la clé publique est un système de n polynômes quadratiques à n variables sur $\mathbb{F}_2$, consistant en la représentation obscure d'une fonction univariée sur $\mathbb{F}_{2^n}$ pouvant être aisément inversée. Comme $\mathbb{F}_{2^n}$ est un espace vectoriel de dimension n sur $\mathbb{F}_2$, tout choix d'une base définit un isomorphisme de $\mathbb{F}_{2^n}$ vers $(\mathbb{F}_2)^n$, et toute fonction univariée de $\mathbb{F}_{2^n}$ dans lui-même s'écrit sur cette base comme un système de n polynômes à n variables. En particulier, l'élévation à une puissance de 2 étant une application linéaire, elle s'écrit sur une telle base comme un système de n polynômes linéaires à n variables. De même, le degré des polynômes multivariés décrivant une fonction univariée correspond au plus fort poids de Hamming des puissances de x sur lesquelles elle s'écrit. Dans le schéma de Matsumoto et Imai, la fonction univariée cachée consiste en un simple monôme $P(x) = x^e$ sur $\mathbb{F}_{2^n}$ avec e de poids de Hamming 2. Afin de rendre $P(x)$ inversible, e est de plus choisi inversible modulo $2^n - 1$. La fonction $P(x)$ est ensuite dissimulée en composant son expression (quadratique) multivariée par deux applications affines inversibles S et T (d'une manière analogue à celle déjà employée dans le cryptosystème de McEliece [61]), ce qui produit la clé publique :

$$\boldsymbol{P} = T \circ P \circ S$$

Les transformations S et T sont choisies aléatoirement et constituent la clé secrète. Comme on peut le constater, ce schéma possède une certaine analogie avec RSA : la clé publique est une permutation résultant de l'élévation à une petite puissance inversible. Toutefois, la sécurité ne repose pas ici sur la secret de l'exposant inverse, mais sur la difficulté de restaurer la représentation secrète S, T permettant d'effectuer l'exponentiation inverse. Bien entendu, la sécurité du système repose également sur la difficulté de résoudre le système d'équations quadratiques associé à la clé publique ; bien que rien ne prouve que ce système ne possède pas de structure cachée permettant de le résoudre sans la clé secrète par une stratégie dédiée, résoudre un système quadratique (ou supérieur) sur un corps fini est un problème NP-dur [41] et réputé très difficile en pratique lorsque le nombre d'équations est

comparable au nombre de variables. De plus, comme pour RSA, l'exposant inverse de e est généralement très élevé, de poids de Hamming de l'ordre de n, et recomposer la fonction inverse de $\boldsymbol{P}$ est par conséquent infaisable en pratique. Notons que, bien que cet exposant inverse soit élevé, il existe de nombreuses optimisations dans les corps finis permettant de rendre une telle exponentiation très rapide ; à titre d'exemple, élever un élément de $\mathbb{F}_{2^n}$ à une puissance de 2 peut être effectué dans une base normale par de simples shifts. Du fait de ces propriétés avantageuses, et après l'échec de la méthode imaginée par Fell et Diffie, le « Scheme A », alors prototype parmi d'autres, a fait l'objet d'une véritable proposition présentée à Eurocrypt'88 sous le nom de C^* [59]. En particulier, Matsumoto et Imai proposent alors certaines optimisations pour des choix particuliers des paramètres, ainsi qu'une variante « par blocs » permettant d'améliorer encore les performances.

1.2 Le « baby-boom » multivarié

Malheureusement, C^* sera cassé par Patarin en 1995, par une approche inédite : Patarin montre que la structure particulière de C^* induit l'existence de relations bilinéaires entre couples clair-chiffré, qui une fois recomposées permettent de déduire l'essentiel du clair correspondant à un chiffré donné par algèbre linéaire [67]. Si la puissance de cette attaque aurait pu réduire à zéro les espoirs de concevoir un système sûr basé sur des polynômes multivariés, elle a bien au contraire marqué le début d'une période d'intense activité dans ce domaine. Patarin lui-même imaginera plusieurs contre-mesures possibles à son attaque ; de nouveaux schémas, dérivés ou non de C^*, seront alors proposés, avec en parallèle le développement de la cryptanalyse algébrique, visant à mettre en place des stratégies efficaces pour la résolution des systèmes de polynômes, inspirée de l'attaque de Patarin elle-même.

Le premier schéma proposé par Patarin est HFE, présenté à Eurocrypt'96 [69]. L'attaque de Patarin sur C^* reposant fortement sur le fait que la fonction univariée cachée est un monôme, celle-ci est remplacée dans HFE par un polynôme général sur la base des monômes de cette forme (i.e. dont l'exposant est de poids de Hamming 2, afin que l'expression multivariée associée soit de degré 2) mais dont *le degré est choisi petit* afin de permettre la recherche efficace de ses racines. Les opérations secrètes sont alors beaucoup moins efficaces, mais le système obtenu paraît toutefois beaucoup plus sûr. Une autre proposition originale de Patarin est le schéma Dragon, présenté à Crypto'96 [68]. La particularité de Dragon est que la fonction univariée cachée est définie implicitement, par une équation $F(x, y) = 0$, quadratique en x et linéaire en y. Toutefois, Patarin montre que toutes les instanciations de Dragon pour lesquelles l'application $x \mapsto F(x, y)$ est un monôme C^* peuvent être attaquées par une extension de son attaque originale. Une instanciation de Dragon basée sur HFE est alors proposée mais n'est d'aucun avantage sur HFE lui-même, avec le défaut d'une clé publique plus grosse, formée de polynômes cubiques. Une troisième proposition de Patarin est le schéma de signature *Oil and Vinegar* [70], qui rompt totalement avec la construction C^* originale mais rappelle

un peu le schéma de Ong-Schnorr-Shamir [66]. Dans OV, la fonction cachée est une fonction multivariée, linéaire en un certain nombre de variables appelées variables *huil*e, et quadratique en les variables restantes appelées variables *vinaigre*. Une signature est calculée en fixant arbitrairement les variables *vinaigre*, et ajustant les variables *huile* par algèbre linéaire. La sécurité du schéma repose sur l'impossibilité, une fois appliqué un changement de variables secret, de distinguer les deux types de variables. La proposition initiale, pour laquelle le nombre de variables *huile* était égal au nombre de variables *vinaigre*, a été cassée par Kipnis et Shamir [54] ; toutefois Kipnis, Patarin et Goubin en ont proposé une réparation immédiate appelée *Unbalanced Oil and Vinegar*, dans laquelle le nombre de variables *vinaigre* est très supérieur au nombre de variables *huil*e [53].

Parallèlement à ces nouvelles constructions, apparaissent des modificateurs génériques, appelés *variations*, visant à perturber la structure particulière des différents schémas. Une première telle variation, appelée *moins* et proposée par Shamir en 93 [77], consiste à supprimer un certain nombre de polynômes-coordonnées de la clé publique. Une variation symétrique, appelée *plus* et proposée par Patarin, Goubin et Courtois en 98 [73], consiste à combiner, par une application linéaire secrète, les coordonnées de la clé publique avec des polynômes quadratiques aléatoires. Une troisième variation importante, appelée *vinaigre* et inspirée du schéma *Oil and Vinegar* [70], consiste à « mélanger » la fonction cachée avec une fonction quadratique aléatoire en des variables distinctes. Ces simples modifications peuvent s'avérer des contre-mesures efficaces contre les attaques et leur utilisation n'implique généralement aucun surcoût pour un schéma de signature. Tout particulièrement, Patarin, Goubin et Courtois ont montré qu'appliquer la variation *moins* à C^* permettait de déjouer l'attaque de Patarin, même généralisée en degré supérieur, et constituait ainsi une réparation possible de C^* pour la signature [73]. Dès que le nombre de polynômes supprimés est suffisamment grand [73], cette famille de schémas est considérée très sûre, et ses performances, comme celles de C^*, sont très attractives. En particulier, l'un de ces schémas, appelé SFLASH, est recommandé par le consortium européen NESSIE depuis 2003 [64]. Un autre schéma, appelé QUARTZ, et dérivé de HFE par application couplée de *vinaigre* et *moins,* est également proposé par NESSIE pour des signatures courtes sur PC [64].

Malgré de nettes différences, ces divers schémas reposent tous sur un principe commun. La clé publique, notée $\boldsymbol{P}$, est toujours obtenue par représentation obscure (S, T) d'une fonction quadratique P admettant une forme spécifique permettant de l'inverser efficacement :

$$\boldsymbol{P} = T \circ P \circ S$$

La fonction interne P peut être l'expression multivariée d'une fonction univariée comme dans C^* ou HFE, et intégrer une variation comme *vinaigre*. D'autres variations peuvent ensuite être appliquées sur la clé publique comme *moins* ou *plus*. La sécurité du schéma repose sur l'infaisabilité de retrouver les applications S et T permettant d'inverser efficacement la clé publique, et bien sûr sur l'infaisabilité d'inverser directement la clé publique sans la connaissance de ces applications. Ré-

soudre le premier problème signifie restaurer la décomposition fonctionnelle $T \circ P \circ S$ sur la seule connaissance de $\boldsymbol{P}$ et de la forme spécifique de P. Lorsque cette forme spécifique définit complètement P, comme pour les schémas C^{*-}, ce problème est une instance du problème communément appelé IP2S, pour *isomorphismes de polynômes à deux secrets*, consistant à déterminer deux applications affines S et T associant deux systèmes de polynômes. Bien que ce problème ait été montré non NP-dur et que de significatifs progrès aient été accomplis pour le résoudre en pratique [74, 75, 34], aucune application positive de cette approche pour retrouver la clé secrète d'un schéma C^{*-} pour les paramètres d'intérêt n'a été rapportée. Le second problème signifie résoudre pour une valeur y donné, le système d'équations quadratiques multivariées $\boldsymbol{P}(x) = y$. Comme déjà mentionné, résoudre un système d'équations quadratiques multivariées sur un corps fini est un problème NP-dur (communément appelé MQ pour *multivariate quadratic*) [41] et les meilleurs algorithmes connus, utilisant les bases de Gröbner, sont exponentiels en moyenne à la fois en temps et en mémoire lorsque le nombre d'équations est comparable au nombre d'inconnues [2, 1]. Toutefois, rien ne prouve que les instances associées à tel ou tel cryptosystème ne constituent pas des instances faibles de MQ et c'est précisément le but des *attaques algébriques* (dont nous traiterons plus loin) que d'établir une telle vulnérabilité. Notons également que bien que les transformations S, T aient souvent été initialement définies affines, il a plus tard été montré que leurs termes constants pouvaient être retrouvés (au moins) pour les schémas C^{*-} et HFE [42, 37] ; la sécurité des schémas ne pouvant raisonnablement reposer sur la présence de ces termes constants, nous considérerons toujours les transformations S, T linéaires dans la suite.

Signalons, pour terminer et par souci d'information, l'existence de nombreuses autres propositions plus ou moins considérées. Il existe par exemple toujours une recherche active pour la conception de schémas basés sur la représentation obscure de fonctions quadratiques aux variables séquentiellement éliminées. Le premier tel schéma a été proposé par Shamir en 93 [77] et a été cassé par Coppersmith, Stern et Vaudenay [15] ; ceux-ci ont en effet montré qu'il était possible de restaurer un système aux variables séquentiellement éliminées par des combinaisons linéaires des formes publiques satisfaisant des conditions successives de rang minimal. D'autres schémas plus complexes ont plus tard été proposés [62, 79, 24], mais la plupart ont été cassés par des généralisations de l'attaque de Coppersmith *et al.* [46, 25, 5]. Enfin, les réparations de tentatives passées, par l'usage de deux tours de représentation obscure (la clé publique est alors de degré 4), proposées par Patarin et Goubin en 97 [46, 72, 71], se sont toutes avérées vaines [4, 80, 33].

1.3 Les attaques algébriques

Les schémas multivariés tentent de construire des fonctions à sens unique basées sur la difficulté, générique, de résoudre un système d'équations polynomiales multivariées sur un corps fini. Les clés publiques de ces systèmes comportent toutefois

quelque structure cachée et la difficulté de résoudre ces instances particulières ne saurait *a priori* être assimilée à la difficulté de résoudre des instances aléatoires de mêmes dimensions. Les *attaques algébriques* sont des stratégies de résolution des instances particulières associées aux cryptosystèmes. Le premier exemple d'une telle attaque est bien sûr l'attaque de Patarin sur C^* : la structure interne du schéma permet de prévoir l'existence de relations bilinéaires entre couples clair-chiffré qui permettent pour tout chiffré spécifié de déduire le clair par algèbre linéaire [67]. Des attaques comparables en degré supérieur ont également été employées par Patarin pour disqualifier certaines instanciations *a priori* envisageables de ses propres propositions [68, 69]. Le degré des relations trouvées est bien sûr de première importance car le nombre de couples clair-chiffrés nécessaires à la détermination de ces relations est exponentiel en ce paramètre. Toutefois, la forme de ces relations doit également permettre la résolution du message clair pour un chiffré donné. Lorsque la fonction interne possède une forme assez générale comme dans HFE, ou intègre une variation interne comme *vinegar*, il est assez peu probable que de telles relations particulières existent. De plus, on perçoit facilement que le degré de telles relations, supposant qu'elles existent, est nécessairement très élevé lorsque le nombre de préimages par la clé publique d'un message donné est très grand, comme c'est souvent le cas en signature. Il est donc clair que cette approche est impuissante à attaquer les schémas dont la fonction interne est de forme assez générale ou bien admet de nombreuses préimages pour une image donnée.

Toutefois, l'existence de relations implicites particulières $F(x, y) = 0$ de petit degré peut être alternativement vue, si l'on remplace les y_i par leurs expressions formelles que sont les polynômes-coordonnées p_i de la clé publique, comme des relations algébriques non-triviales et de petit degré en les p_i. De telles relations sont appelées *syzygies* dans la littérature et sont notamment exploitées par le calcul de bases de Gröbner dont l'un des objectifs est la résolution des systèmes polynomiaux. Bien que la notion de *base de Gröbner* s'exprime en référence à une relation d'ordre sur les monômes, il existe des algorithmes efficaces pour passer de la base associée à un ordre donné à celle associée à tout autre [31, 14]. Pour l'ordre lexicographique indépendant du degré, souvent noté *lex*, une base de Gröbner correspond à un système de polynômes aux variables séquentiellement éliminées, qui peut donc être aisément résolu. Le premier algorithme de calcul de base de Gröbner est dû à Buchberger [7, 8, 9], mais de nombreuses améliorations théoriques et pratiques ont été apportées par la suite notamment par Lazard [56] et Faugère [35, 36]. La stratégie générale des algorithmes modernes consiste à chercher, pour un degré croissant d, des dépendances linéaires parmi les multiples algébriques de degré d des polynômes donnés en entrée. Certaines de ces dépendances, dites triviales, existent toujours pour des raisons formelles et ne sont d'aucune utilité pour le calcul de la base de Gröbner. Le degré d en lequel il est nécessaire de monter pour obtenir les premières dépendances non-triviales est un paramètre important de la complexité du calcul car il est généralement très proche du degré final nécessaire. En particulier, nous voyons que pour les schémas multivariés attaqués par Patarin,

des dépendances non-triviales, associées aux relations implicites mises en évidence, existent en degré assez bas. L'approche « aveugle » par les bases de Gröbner est donc tout aussi apte à inverser les clés publiques des schémas attaqués par Patarin, et cela sans nécessiter la forme particulière de ces relations.

La puissance de cette approche s'est trouvée confirmée par le cassage du premier challenge HFE par Faugère en 2002 [51] avec son nouvel algorithme F5 [36]. Les raisons structurelles permettant le calcul d'une base de Gröbner pour un système HFE à un degré de recombinaisons algébriques relativement bas ont plus tard été mises en évidence par Faugère et Joux [32] ; malheureusement, le phénomène combinatoire responsable de ce résultat reste assez mal maîtrisé et ne permet pas de déduire la complexité du calcul pour des paramètres donnés. Cette complexité étant exponentielle (temps et mémoire) en le degré de recombinaisons algébriques nécessaire, la capacité de HFE à fournir la base d'un système sûr reste débattue.

L'attaque par les bases de Gröbner est maintenant devenue un test minimal de résistance des schémas multivariés. Une approche comparable, appelée XL, avait été plus tôt proposée par Courtois, Klimov, Patarin et Shamir [19], mais ne bénéficiait pas de la même assise théorique ni d'implémentation aussi efficace que l'algorithme de Faugère. Le défaut commun de telles approches reste toujours leur complexité en $n^{\mathcal{O}(d)}$, à la fois en temps et mémoire, où d est le degré maximal des recombinaisons algébriques considérées et n le nombre de variables. En particulier, la valeur de d nécessaire à l'attaque est généralement très élevée pour des systèmes sous-déterminés comme les clés publiques des divers schémas de signature.

1.4 Propos et organisation de la thèse

En 2004, Ding a introduit une nouvelle variation appelée *perturbation interne*, permettant de réparer C^* pour le chiffrement [20]. Cette modification rend C^* résistant aux attaques algébriques au prix d'un léger facteur de complexité au déchiffrement. Malheureusement, Fouque, Granboulan et Stern ont peu après proposé une approche totalement inédite permettant de supprimer efficacement la perturbation interne du schéma proposé par Ding [40]. Cette approche se fonde sur l'étude de la *différentielle* de la clé publique. Pour toute fonction quadratique P, l'application $x \mapsto P(a+x) - P(x)$ est affine de terme constant $P(a) - P(0)$. Sa partie linéaire est appelée la différentielle en a et notée DP_a :

$$DP_a(x) = P(a+x) - P(a) - P(x) + P(0)$$

Dans un schéma multivarié, la clé publique $\boldsymbol{P}$ et la fonction interne P sont deux fonctions quadratiques associées :

$$\boldsymbol{P} = T \circ P \circ S$$

et leurs différentielles se déduisent aisément l'une de l'autre :

$$D\boldsymbol{P}_a = T \circ DP_{S(a)} \circ S$$

Les applications linéaires S et T étant inversibles, la distribution du rang de la différentielle de la clé publique est identique à celle de la différentielle interne, et la nature de cette distribution est directement liée à la structure interne du schéma. En particulier, dans le schéma de Ding, la *perturbation interne* introduite induit une perturbation de la distribution du rang de la différentielle de C^* permettant de l'isoler puis de la supprimer de la clé publique [40].

L'approche proposée par Fouque *et al.* est fondatrice à plusieurs égards. Elle suggère tout d'abord d'exprimer la spécificité des fonctions quadratiques considérées par des propriétés linéaires, qui sont aisément calculables. L'idée de différentielle était auparavant apparue dans la littérature pour des causes isolées [72, 73, 80, 43] mais n'avait jamais été exprimée comme un invariant systématique des schémas multivariés ni considérée du point de vue de ses propriétés géométriques. Enfin, elle ouvre une nouvelle ligne d'attaque des schémas intégrant des variations par l'exploitation des propriétés différentielles spécifiques de la structure de base.

Au cours de cette thèse, nous avons développé la *méthodologie différentielle* engagée par Fouque *et al.* dans deux directions. La première consiste en le calcul combinatoire des distributions différentielles de HFE et de sa variation perturbée proposée par Ding-Schmidt en 2005 [23]. Ce traitement combinatoire nous a permis de construire un algorithme reconnaissant une clé publique HFE d'un système aléatoire en temps quasipolynomial [28], et de cryptanalyser la variation par *perturbation interne* de HFE [29] (travaux effectués en collaboration avec Louis Granboulan et Jacques Stern). Le second développement de la thèse est la découverte d'invariants fonctionnels de la différentielle de C^*, et nous a permis de cryptanalyser les schémas C^{*-} pour tous les paramètres raisonnables et en particulier pour les paramètres du schéma SFLASH, recommandé par NESSIE [27, 26] (travaux effectués en collaboration avec Pierre-Alain Fouque, Adi Shamir et Jacques Stern).

Le mémoire est donc naturellement divisé en deux parties, l'une concernant C^* et ses variations, et l'autre concernant HFE et ses variations. La première partie comprend trois chapitres :

1. Le premier chapitre est consacré à C^* lui-même et présente une cryptanalyse alternative à celle de Patarin [67] par l'utilisation des propriétés duales de sa différentielle.
2. Le second chapitre est consacré à la variation par *perturbation interne* de C^* proposée par Ding [20] ; nous y établissons la résistance de ce schéma aux attaque algébriques et présentons une cryptanalyse alternative à celle de Fouque *et al.* [40] par l'utilisation des propriétés ensemblistes des noyaux de la différentielle de C^*.
3. Le troisième chapitre est consacré aux schémas C^{*-} proposés par Patarin, Goubin et Courtois [73] et présente les deux attaques complémentaires établissant la faiblesse totale de ces schémas y compris pour les paramètres du schéma SFLASH, recommandé par NESSIE.

La seconde partie comprend quatre chapitres :

1. Le premier chapitre consiste en une introduction à HFE ; nous y décrivons le schéma HFE lui-même puis présentons une synthèse des résultats connus et des problèmes ouverts le concernant.
2. Le second chapitre décrit notre algorithme de reconnaissance des clés publiques HFE et détermine sa complexité.
3. Le troisième chapitre expose de façon détaillée les différentes stratégies d'attaques ayant été proposées contre le HFE ainsi que quelques notes complémentaires dans le prolongement de la cryptanalyse des schémas C^{*-}.
4. Le quatrième chapitre décrit notre attaque sur la variation par perturbation interne de HFE proposée par Ding et Schmidt [23] et détermine sa complexité.

Un chapitre consacré aux dénombrements dans les espaces vectoriels est proposé préalablement aux deux parties principales. La première partie de ce chapitre est une introduction recommandée pour la compréhension des chapitres suivants ; la seconde partie présente des résultats plus avancés nécessaires seulement à la compréhension des chapitres sur HFE.

Chapitre 2

Dénombrements dans les espaces vectoriels

La clé publique d'un schéma multivarié est une fonction quadratique à la structure particulière puisqu'elle admet une trappe permettant de l'inverser rapidement. À Eurocrypt 2005, Fouque, Granboulan et Stern ont proposé une nouvelle approche cryptanalytique consistant à étudier les propriétés différentielles de la clé publique [40]. La différentielle en un point donné est une application linéaire qui, du fait de la spécificité de la fonction quadratique dont elle est dérivée, admet elle-même des propriétés particulières, exprimées en termes de l'algèbre linéaire. Ces propriétés, telles la dimension du noyau ou la valeur du rang, ou plutôt leur comportement statistique en fonction du point considéré et de la clé secrète, révèlent parfois de l'information sur la structure secrète du système et cette information peut être exploitée pour une attaque. Il est donc très important, autant pour mesurer l'efficacité des attaques que celle des défenses, de savoir calculer précisément les répartitions statistiques des applications linéaires vérifiant des propriétés données.

Ce chapitre se divise en deux parties. La première partie consiste en l'introduction proprement dite aux dénombrements dans les espaces vectoriels, et permet de se familiariser avec les raisonnements énumératifs fondamentaux utilisés dans les chapitres suivants. La seconde partie consiste en des résultats plus avancés, prolongeant les premiers, qui peuvent être omis en première lecture. Les résultats les plus avancés sont des produits de cette thèse, développés pour les besoins des chapitres suivants, mais sont intéressants en soi. Notre motivation étant ici purement calculatoire, nous n'employons que le plus simple raisonnement énumératif, sans outils combinatoires sophistiqués.

2.1 Quantités élémentaires

On appelle *suite linéairement indépendante de longueur* r dans $(\mathbb{F}_q)^n$, une suite $v_1, \ldots, v_r$ de r éléments linéairement indépendants de $(\mathbb{F}_q)^n$. On construit une telle suite en choisissant un élément non-nul v_1, puis un élément v_2 hors de la droite

engendrée par v_1, puis un élément v_3 hors du plan engendré par v_1 et v_2, etc... Le nombre de suites linéairement indépendantes de longueur r dans $(\mathbb{F}_q)^n$, noté $S(n,r)$, est donc :

$$S(n,r) = (q^n-1)(q^n-q)\dots(q^n-q^{r-1}) = \prod_{i=0}^{r-1}(q^n-q^i)$$

Une telle suite engendre un sous-espace vectoriel de dimension r qui est également engendré par toute autre suite linéairement indépendante qu'il contient. Le nombre de sous-espaces vectoriels de dimension r, noté $E(n,r)$, est donc :

$$E(n,r) = \frac{S(n,r)}{S(r,r)} = \prod_{i=0}^{r-1}\frac{q^n-q^i}{q^r-q^i} = \prod_{i=0}^{r-1}\frac{q^{n-i}-1}{q^{r-i}-1} \tag{2.1}$$

Une autre façon d'obtenir ce nombre repose sur le raisonnement suivant. Un élément non-nul a de $(\mathbb{F}_q)^n$ est contenu dans autant de sous-espaces de dimension r qu'il existe de sous-espaces de dimension $r-1$ dans le quotient $(\mathbb{F}_q)^n/(\mathbb{F}_q\cdot a)$ par la droite engendrée par a. Formant pour chaque élément non-nul a une liste des sous-espaces de dimension r le contenant, et prenant la concaténation de ces listes, nous obtenons une liste de longueur $(q^n-1)E(n-1,r-1)$ dans laquelle chaque sous-espace de dimension r apparaît exactement (q^r-1) fois, soit autant de fois qu'il contient d'éléments non-nuls. Nous avons donc :

$$E(n,r) = \frac{q^n-1}{q^r-1}E(n-1,r-1)$$

Par récurrence descendante, nous retrouvons bien la formule (2.1) précédente.

Introduisant la suite :

$$\lambda(n) = \left(1-\tfrac{1}{q}\right)\left(1-\tfrac{1}{q^2}\right)\dots\left(1-\tfrac{1}{q^n}\right) = \prod_{i=1}^{n}\left(1-\tfrac{1}{q^i}\right)$$

valant 1 pour $n=0$, nous obtenons aisément :

$$S(n,r) = \frac{\lambda(n)}{\lambda(n-r)}q^{nr} \qquad \text{et} \qquad E(n,r) = \frac{\lambda(n)}{\lambda(n-r)\lambda(r)}q^{r(n-r)} \tag{2.2}$$

La suite $\lambda(n)$ décroissant de 1 vers une valeur croissante en q et minorée par 0.28 pour $q=2$ [39], les puissances q^{nr} et $q^{r(n-r)}$ sont les ordres de grandeur respectifs de $S(n,r)$ et $E(n,r)$. Nous constatons également la symétrie $E(n,r)=E(n,n-r)$.

Notons au passage qu'une suite aléatoire de $(\mathbb{F}_q)^n$ de longueur $r \ll n$ est linéairement indépendante avec probabilité :

$$\lambda(n)/\lambda(n-r) = (1-q^{-n}.q^{r-1})\dots(1-q^{-n}.1) = 1-q^{-n}\left(\frac{q^r-1}{q-1}\right)+\mathcal{O}(q^{-2n+r})$$

très proche de 1 à l'ordre q^{-n+r} près.

Les quantités $S(n,r)$ et $E(n,r)$ sont les analogues dans le contexte des espaces vectoriels des nombres d'arrangements et nombre de sous-ensembles de la combinatoire des ensembles ; en particulier, $E(n,r)$ est parfois appelé coefficient q-binomial dans la littérature. S'il est connu de longue date que les identités classiques telles la formule du binôme admettent des q-analogues, obtenues par le biais de la théorie des partitions ou la théorie des fonctions elliptiques, l'interprétation des q-quantités comme combinatoire des espaces vectoriels a été perçue tardivement, par Goldman et Rota en 1969 [44, 45]. Nombre de q-identités ont ainsi pu être redémontrées, par de simples arguments structurels. Les recherches ultérieures ont surtout contribué à approfondir l'analogie observée ; notamment, plusieurs développements classiques comme la fonction de Möbius ou les permutations à positions restreintes ont été transposés par Rota et ses collaborateurs au contexte des espaces vectoriels [44, 52, 13]. Cette analogie possède toutefois certaines limites : si $S(n,n)$ est l'analogue naturel de la factorielle de n, les expressions de $S(n,r)$ et $E(n,r)$ en fonction de cette quantité ne correspondent pas aux formules classiques.

2.2 Dénombrements élémentaires

Dans toute la suite, on note V_n tout espace vectoriel de dimension n sur $\mathbb{F}_q$.

2.2.1 Suites de vecteurs et applications linéaires

Étant donnée une base $e_1, \ldots, e_r$ de V_r, toute application linéaire de V_r dans V_n est uniquement déterminée par la suite des vecteurs $\ell(e_1), \ldots, \ell(e_r)$. Il existe donc autant d'applications linéaires de V_r dans V_n que de suites de r vecteurs dans V_n, soit q^{nr}. En particulier, un telle application est injective quand $\ell(e_1), \ldots, \ell(e_r)$ engendre un sous-espace de dimension r, soit quand cette suite est linéairement indépendante de longueur r. Le nombre d'applications injectives de V_r dans V_n est donc égal à $S(n,r)$. En complément de la remarque faite plus haut, une application linéaire aléatoire d'un petit espace V_r vers un grand espace V_n est injective avec probabilité très proche de 1 à l'ordre q^{-n+r} près.

2.2.2 Applications linéaires d'un rang donné

Soit F un sous-espace vectoriel de dimension d de V_n, et G un supplémentaire de F dans V_n. Toute application linéaire est définie uniquement sur V_n par sa restriction à F et G. Une application linéaire est de noyau F si et seulement si elle est nulle sur F et injective sur G. Le nombre d'applications linéaires à valeurs dans V_m de noyau F est donc $S(m, n-d)$. Le nombre de sous-espaces F de dimension d étant $E(n,d)$, le nombre d'applications linéaires de V_n dans V_m ayant un noyau de dimension d est :

$$E(n,d)S(m,n-d)$$

À titre d'exemple, nous montrons comment ce simple raisonnement permet de démontrer une identité analogue à la formule du binôme classique, comme observé dans [44]. Partitionnant les applications linéaires de V_n dans V_m selon la dimension de leur noyau, nous obtenons l'identité :

$$q^{nm} = \sum_{d=0}^{n} E(n,d)S(m,n-d)$$

Renommant $x = q^m$ le nombre d'éléments de V_m, cette identité se réécrit :

$$x^n = \sum_{d=0}^{n} E(n,d)(x-1)(x-q)\dots(x-q^{n-d-1})$$

L'identité ci-dessus est une équation polynomiale admettant une infinité de solutions $x = q^m$, elle est donc vraie pour toute valeur de x. L'analogie entre cette identité et la formule du binôme se perçoit en posant $x = 1+y$ et en faisant tendre q vers 1.

2.2.3 Applications linéaires envoyant un sous-espace dans un autre

Soit F un sous-espace de dimension r de V_n et G un sous-espace de dimension s de V_m. Étant donné une base $e_1, \dots, e_r$ de F complétée en une base $e_1, \dots, e_n$ de V_n, une application linéaire envoie F dans G si les vecteurs $\ell(e_1), \dots, \ell(e_r)$ sont des éléments de G ; il y a donc $q^{rs}q^{(n-r)m}$ telles applications. Une application linéaire injective envoie F dans G si $\ell(e_1), \dots, \ell(e_r)$ est une suite linéairement indépendante de G au lieu de V_m tout entier. Le nombre d'applications linéaires injectives envoyant F dans G est donc :

$$S(s,r)\frac{S(m,n)}{S(m,r)} = \prod_{i=0}^{r-1}(q^s - q^i)\prod_{i=r}^{n}(q^m - q^i)$$

2.2.4 Sous-espaces d'intersection zéro avec un sous-espace donné

Soit F un sous-espace de dimension r de V_n. Une suite linéairement indépendante $v_1, \dots, v_s$ de longueur $s \leq n-r$ engendre un espace d'intersection zéro avec F si et seulement si aucune combinaison linéaire non-triviale des v_i n'est un élément de F. Cette condition est satisfaite si et seulement si v_1 n'est pas dans F, v_2 n'est pas dans l'espace engendré par v_1 et F, v_3 n'est pas dans l'espace engendré par v_1, v_2 et F,... D'autre part, l'espace engendré par une suite linéairement indépendante dans un espace d'intersection zéro avec F est lui-même d'intersection zéro avec F. Par conséquent, le nombre de sous-espaces d'intersection zéro avec F est :

$$\frac{(q^n - q^r)(q^n - q^{r+1})\dots(q^n - q^{r+s-1})}{S(s,s)} = \frac{S(n,r+s)}{S(n,r)S(s,s)}$$

Autre dénombrement possible : les sous-espaces de dimension s d'intersection zéro avec F sont des sous-espaces de même dimension dans le quotient V_n/F. Soit $\bar{G}$ un sous-espace de dimension s de V_n/F ; on note $\bar{g}_1, \ldots, \bar{g}_s$ une base de $\bar{G}$. Pour tout i, les préimages de $\bar{g}_i$ par la surjection canonique $V_n \to V_n/F$ forment un sous-espace affine $g_i + F$. Par conséquent, les sous-espaces de dimension s et d'image $\bar{G}$ par la surjection canonique sont engendrés pas les vecteurs de la forme $g_1 + f_1, \ldots, g_s + f_s$ où les f_i sont des éléments de F. Il reste à remarquer que chaque choix $f_1, \ldots, f_s$ de s éléments de F définit un unique sous-espace de dimension s d'image $\bar{G}$, celui contenant à la fois $g_1 + f_1, \ldots, g_s + f_s$. Pour chaque sous-espace $\bar{G}$ de dimension s de V_n/F, il existe donc q^{ns} sous-espaces de V_n de dimension s d'image $\bar{G}$ par la surjection canonique. Comme il existe $E(n-r, s)$ choix d'un sous-espace $\bar{G}$, le nombre de sous-espaces de V_n de dimension s et d'intersection zéro avec F est :

$$q^{rs}.E(n-r,s) = \frac{q^{rs}(q^{n-r}-1)\ldots(q^{n-r}-q^{s-1})}{S(s,s)} = \frac{S(n,r+s)}{S(n,r)S(s,s)} \tag{2.3}$$

2.2.5 Sous-espaces contenant un sous-espace donné

Soit F un sous-espace de dimension r de V_n. Une suite linéairement indépendante $v_1, \ldots, v_s$ de longueur s engendre avec F un sous-espace de dimension $r+s$ si et seulement si l'espace engendré par $v_1, \ldots, v_s$ est d'intersection zéro avec F. Le nombre de suites de longueur s dans V_n engendrant un espace d'intersection zéro avec F a été calculé précédemment : $S(n, r+s)/S(n, r)$. De la même façon, étant donné un sous-espace G engendré par une telle suite et F, une suite linéairement indépendante de longueur s dans G engendre à nouveau G avec F si et seulement si elle engendre un espace d'intersection zéro avec F. Ce dernier nombre est donc $S(r+s, r+s)/S(r+s, r)$. Finalement, le nombre de sous-espaces de dimension $r+s$ contenant F est :

$$\frac{S(n,r+s)S(r+s,r)}{S(n,r)S(r+s,r+s)}$$

Autre dénombrement possible : les sous-espaces de dimension $r+s$ contenant F sont des sous-espaces de dimension s dans V_n/F. Pour chaque sous-espace de dimension s de V_n/F, il existe un unique sous-espace de dimension $r+s$ contenant F. Donc le nombre de sous-espaces de dimension $r+s$ contenant F est $E(n-r, s)$. Nous pouvons en effet vérifier, en utilisant l'identité (2.3), que la formule précédente est bien égale à ce nombre :

$$\frac{S(n,r+s)S(r+s,r)}{S(n,r)S(r+s,r+s)} = \frac{q^{rs}S(n-r,s)}{q^{rs}S(s,s)} = E(n-r,s)$$

2.2.6 Intersection de deux sous-espaces

Nous calculons le nombre de sous-espaces d'une certaine dimension ayant une intersection fixée avec un sous-espace donné.

Lemme 1. *Soit r, s, i des entiers, $i \leq r, s$. Étant donné un sous-espace F de dimension r de V_n et I un sous-espace de dimension i de F, le nombre de sous-espaces de dimension s d'intersection I avec F est :*

$$\frac{S(n, r+s-i)S(s, i)}{S(n, r)S(s, s)}$$

Démonstration. Soit F un sous-espace de dimension r de V_n et I un sous-espace de dimension i de F. Le nombre de suites linéairement indépendantes de longueur s engendrant un sous-espace d'intersection I avec F est le nombre de suites linéairement indépendantes de longueur $s-i$ engendrant un sous-espace d'intersection zéro avec F : $S(n, r+s-i)/S(n, r)$. Étant donné un sous-espace G de dimension s et d'intersection I avec F, le nombre de suites linéairement indépendantes de longueur s dans G engendrant un sous-espace disjoint de I est : $S(s, s)/S(s, i)$. Le nombre cherché s'obtient en prenant le quotient de ces deux quantités.
Autre dénombrement possible : Le nombre de sous-espaces G de dimension s d'intersection I avec F est le nombre de sous-espaces $\bar{G}$ de dimension $s-i$ disjoints de $\bar{F}$ dans V_n/I. Le nombre cherché est donc $q^{(r-i)(s-i)}.E(n-r, s-i)$. Nous pouvons vérifier, en utilisant (2.3), que la formule précédente est bien égale à ce nombre :

$$q^{(r-i)(s-i)}.E(n-r, s-i) = \frac{q^{r(s-i)}S(n-r, s-i)}{q^{i(s-i)}S(s-i, s-i)} = \frac{S(n, r+s-i)/S(n, r)}{S(s, s)/S(s, i)}$$

□

Le nombre de sous-espaces de dimension s ayant une intersection de dimension i avec F s'obtient en multipliant par le nombre $E(r, i)$ de choix possibles pour I. Divisant par le nombre total $E(n, s)$ de sous-espaces de dimension s, nous en déduisons le lemme suivant.

Lemme 2. *Soit r, s, i des entiers, $i \leq r, s$. Étant donné un sous-espace de dimension r de V_n, la probabilité qu'un sous-espace aléatoire de dimension s intersecte ce sous-espace avec dimension i est :*

$$\frac{S(r, i)S(n, r+s-i)S(s, i)}{S(n, r)S(i, i)S(n, s)}$$

Utilisant l'expression de S en fonction de λ, la probabilité du lemme est de l'ordre de $q^{-i(n-r-s+i)}$ et très rapidement décroissante avec i. Il en résulte que la valeur la plus probable de i est la valeur minimale, réalisant $i \geq r+s-n$. Ceci est une illustration d'un principe général que l'on pourrait appeler *principe d'intersection minimale*, selon lequel des sous-espaces aléatoires réalisent le plus probablement l'intersection minimale permise par les contraintes auxquelles ils sont soumis. L'explication intuitive d'un tel fait est qu'il existe toujours beaucoup plus d'éléments en dehors d'un sous-espace donné qu'à l'intérieur de ce sous-espace ; il existe en effet q^r éléments à l'intérieur d'un sous-espace de dimension r et $q^n - q^r = q^r(q^{n-r}-1)$ éléments à l'extérieur de ce sous-espace.

2.2.7 Dénombrement des polynômes $\mathbb{F}_q$-linéaires d'un degré donné

Rappelons que le corps à q^n éléments $\mathbb{F}_{q^n}$ est un espace vectoriel de dimension n sur $\mathbb{F}_q$. L'élévation à la puissance q est une application linéaire dans $\mathbb{F}_{q^n}$ ainsi que tout polynôme à coefficients dans $\mathbb{F}_{q^n}$ de la forme :

$$L(x) = \sum_{i=0}^{n-1} \lambda_i . x^{q^i}$$

Nous appellerons les polynômes de cette forme *polynômes $\mathbb{F}_q$-linéaires*. Comme il existe $(q^n)^n$ tels polynômes, il est clair que ces polynômes définissent l'ensemble des applications linéaires de $\mathbb{F}_{q^n}$ dans lui-même.

Le noyau, en tant qu'application linéaire, d'un polynôme $\mathbb{F}_q$-linéaire est l'ensemble de ses racines. En particulier, un polynôme $\mathbb{F}_q$-linéaire non-nul de degré q^D a au plus q^D racines et son noyau a donc dimension au plus D. Les probabilités qu'un polynôme $\mathbb{F}_q$-linéaire aléatoire de degré q^D ait un noyau de dimension $d \leq D$ sont données par le lemme suivant.

Lemme 3. *Les probabilités $p_D(0), \ldots, p_D(D)$ qu'un polynôme $\mathbb{F}_q$-linéaire aléatoire de degré q^D ait un noyau de dimension respectivement $0, \ldots, D$ satisfont le système triangulaire inversible suivant :*

$$d \in [0, D], \quad E(n, d) q^{-nd} = \sum_{m=d}^{D} E(m, d) p_D(m)$$

Démonstration. Le nombre de polynômes $\mathbb{F}_q$-linéaires de degré q^D est le nombre de choix possibles pour ses $D+1$ coefficients sachant que le coefficient principal doit être non-nul : $(q^n - 1)q^{nD}$. Étant donné un sous-espace de dimension $d \leq D$ de base $e_1, \ldots, e_d$, un polynôme $\mathbb{F}_q$-linéaire L de degré q^D s'annule sur ce sous-espace si et seulement si ses $D+1$ coefficients dans $\mathbb{F}_{q^n}$ vérifient les d contraintes linéaires : $L(e_1) = 0, \ldots, L(e_d) = 0$. Il en résulte que tout sous-espace de dimension d est contenu dans le noyau d'exactement $(q^n - 1)q^{n(D-d)}$ polynômes $\mathbb{F}_q$-linéaires de degré q^D. Formant pour tout sous-espace de dimension d une liste des polynômes $\mathbb{F}_q$-linéaires de degré q^D dont le noyau contient ce sous-espace, puis prenant le concaténation de ces listes, nous obtenons une liste de longueur $E(n, d)(q^n - 1)q^{n(D-d)}$ dans laquelle chaque polynôme $\mathbb{F}_q$-linéaire de degré q^D apparaît autant de fois que son noyau contient de sous-espaces de dimension d, soit $E(m, d)$ fois pour ceux dont le noyau est de dimension m. Les proportions $p_D(d)$ des polynômes $\mathbb{F}_q$-linéaires de degré q^D et de noyau de dimension d vérifient donc bien le système triangulaire annoncé. Ce système est inversible car les termes diagonaux $E(d, d)$ sont non-nuls. □

2.3 Dénombrements avancés

2.3.1 Intersection commune de trois sous-espaces

On calcule ici le nombre de sous-espaces H de dimension t dans V_n dont l'intersection avec deux sous-espaces donnés F et G de dimensions r et s est $F \cap G$:

$$H \cap F = H \cap G = F \cap G$$

Pour cela, nous allons procéder en plusieurs étapes. Une première étape consiste en le cas particulier suivant :

Lemme 4. *Soit r, s, t des entiers, $t \leq r, s$. Étant donnés deux sous-espaces F et G d'intersection zéro de dimensions respectivement r et s, le nombre de sous-espaces H de $F \oplus G$ de dimension t et d'intersection zéro à la fois avec F et G est :*

$$\frac{S(r,t)S(s,t)}{S(t,t)}$$

Démonstration. Soit $h_1, \ldots, h_t$ une base d'un sous-espace H vérifiant les conditions voulues ; nous avons alors nécessairement $t \leq r, s$. Comme H est un sous-espace de $F \oplus G$, tous les h_i s'écrivent de façon unique $f_i + g_i$ avec f_i dans F et g_i dans G. Comme de plus H est d'intersection zéro avec F et G, les suites (f_i) et (g_i) sont elles-mêmes linéairement indépendantes respectivement dans F et G. En effet, si ceci n'était pas vrai par exemple pour (f_i), nous pourrions alors trouver une dépendance linéaire non-triviale sur les f_i et par conséquent un élément non-trivial dans l'intersection de H et G, ce qui est exclu par hypothèse.

Réciproquement, soit $f_1, \ldots, f_t$ et $g_1, \ldots, g_t$ des suites linéairement indépendantes de longueur t respectivement de F et G. Comme F et G sont d'intersection zéro, le sous-espace engendré par $f_1 + g_1, \ldots, f_t + g_t$ est d'intersection zéro avec F et G ; en effet, si ceci n'était pas vrai, par exemple pour F, nous pourrions trouver une combinaison linéaire non-triviale des $f_i + g_i$ élément de F et cette même combinaison linéaire sur les g_i serait alors un élément non-trivial de $F \cap G$.

Par conséquent, le nombre de suites linéairement indépendantes de longueur t dans $F \oplus G$ engendrant un sous-espace H d'intersection zéro avec F et G est $S(r,t)S(s,t)$. Toute suite linéairement indépendante de longueur t de H vérifiant ces mêmes conditions, le nombre cherché s'obtient en divisant par $S(t,t)$. □

Le lemme précédent se généralise aisément au cas où F et G ne sont pas d'intersection zéro, ce qui donne le lemme suivant :

Lemme 5. *Soit r, s, t, i des entiers, avec $t \leq r, s$ et $i \leq r, s, t$. Étant donnés deux sous-espaces F et G de dimension r et s, le nombre de sous-espaces H de $F + G$ de dimension t et vérifiant $H \cap F = H \cap G = F \cap G$ est :*

$$\frac{S(r-i,t-i)S(s-i,t-i)}{S(t-i,t-i)}$$

où i est la dimension de $F \cap G$.

Démonstration. Il suffit de remarquer que les sous-espaces vérifiant les conditions voulues sont en bijection avec les sous-espaces $\bar{H}$ de $(F+G)/(F\cap G)$ de dimension $t-i$ et disjoints de $\bar{F}$ et $\bar{G}$ dont les dimensions sont respectivement $r-i$ et $s-i$. □

Le cas général peut maintenant s'obtenir en prolongeant un sous-espace J vérifiant les conditions du lemme précédent en dehors de $F+G$.

Lemme 6. *Soit n, r, s, t, i des entiers ; $r, s, t \leq n$, $i \leq r, s, t$. Dans V_n, étant donnés deux sous-espaces F et G de dimension r et s et d'intersection de dimension i, le nombre de sous-espaces H de dimension t vérifiant $H \cap F = H \cap G = F \cap G$ est :*

$$\sum_{i\leq j\leq r,s,t} \frac{S(r-i,t-i)S(s-i,t-i)}{S(t-i,t-i)} \frac{S(n,r+s-i+t-j)}{S(n,r+s-i)} \frac{S(t,j)}{S(t,t)}$$

Démonstration. Un sous-espace H de dimension t vérifie $H\cap F = H\cap G = F\cap G$ si et seulement si son intersection avec $F+G$ vérifie les conditions du lemme 5. Pour tout sous-espace J de $F+G$ de dimension j vérifiant les conditions du lemme 5, le nombre de sous-espaces H de dimension t d'intersection J avec $F+G$ s'obtient en appliquant le lemme 1 avec $r := r+s-i$, $i := j$, $s := t$. Le nombre total cherché s'obtient en sommant sur toutes les dimensions possibles pour J. □

2.3.2 Rang de la somme de deux applications linéaires

Le noyau de la somme $L+\ell$ de deux applications linéaires L et ℓ de noyaux respectifs F et G est un sous-espace H vérifiant : $H\cap F = H\cap G = F\cap G$. En effet, il est clair que $L+\ell$ s'annule sur l'intersection des noyaux de L et ℓ, que L s'annule sur l'intersection des noyaux de $L+\ell$ et ℓ, etc. Le lemme suivant donne la probabilité que le noyau de $L+\ell$ soit de dimension t lorsque L est une application fixée de noyau F et ℓ est une application aléatoire de noyau G.

Lemme 7. *Soit n, m, r, s, t, i des entiers, avec $r, s, t \leq n$, $i \leq r, s, t$ et $m \geq n - r, n-s, n-t$. Soit $L : V_n \to V_m$ une application linéaire dont le noyau F est de dimension r, et G un sous-espace de dimension s ayant une intersection de dimension i avec F. Notant $E_{r,s,i}(t)$ le nombre de sous-espaces H de dimension t vérifiant $H\cap F = H\cap G = F\cap G$ donné par le lemme 6, les probabilités $p_{r,s,i}(t)$ que $L+\ell$ ait un noyau de dimension t quand ℓ est une application aléatoire de noyau G satisfont le système triangulaire inversible suivant :*

$$\frac{E_{r,s,i}(t)}{S(m,t-i)} = \sum_{k\geq t}^{n} E(k,t)\frac{S(t,i)}{S(k,i)} p_{r,s,i}(k)$$

Démonstration. Étant donné un sous-espace H de dimension t et vérifiant $H\cap F = H\cap G = F\cap G$, nous comptons d'abord les applications linéaires ℓ de noyau G et telles que le noyau de $L+\ell$ contienne H. Toutes ces applications ont la même image sur le sous-espace $G+H$ de dimension $s+t-i$, et cette image est un sous-espace

W de V_m de dimension $t-i$. Fixant une base $e_{t+i},\dots,e_n$ d'un supplémentaire de $G+H$, ces applications sont donc définies par les suites linéairement indépendantes $\ell(e_{t+i}),\dots,\ell(e_n)$ de V_m engendrant un espace disjoint de W. Le nombre de choix possibles est donc :

$$(q^m-q^{t-i})\dots(q^m-q^{n-s-1})=\frac{S(m,n-s)}{S(m,t-i)}$$

Formant pour chaque sous-espace H de dimension t vérifiant $H\cap F=H\cap G=F\cap G$, une liste des applications ℓ de noyau G et telles que le noyau de $L+\ell$ contienne H, puis concaténant ces listes, nous obtenons une liste de longueur $E_{r,s,i}(t)S(m,n-s)/S(m,t-i)$, dans laquelle chaque application ℓ apparaît autant de fois que le noyau de $L+\ell$ contient de sous-espaces de dimensions t contenant $F\cap G$. Pour les applications ℓ telles que $L+\ell$ a un noyau de dimension k, ce dernier nombre est, utilisant le calcul 2.2.5, $E(k,t)S(t,i)/S(k,i)$. Le nombre total d'applications de noyau G étant $S(m,n-s)$, nous obtenons bien le système triangulaire annoncé. Ce système est inversible car les termes diagonaux sont non-nuls. □

Nous donnons maintenant une seconde démonstration dans le cas particulier où F et G sont supplémentaires dans V_n ; cette démonstration se généralise aisément au cas où F et G engendre V_n sans être nécessairement d'intersection zéro.

Lemme 8. *Soit n,m,r,s,t des entiers, avec $n=r+s$, $t\le r,s$ et $m\ge r,s,n-t$. Soit $L:V_n\to V_m$ une application linéaire dont le noyau F est de dimension r, et G un supplémentaire de F dans V_n. La probabilité $p_{r,n-r,0}(t)$ que $L+\ell$ ait un noyau de dimension t quand ℓ est une application aléatoire de noyau G est :*

$$p_{r,n-r,0}(t)=\frac{S(r,t)S(n-r,t)}{S(t,t)}\frac{S(m,n-t)}{S(m,r)S(m,n-r)}$$

Démonstration. Le noyau de $L+\ell$ est le sous-espace sur lequel L et $-\ell$ prennent les mêmes valeurs. Pour tout élément y dans l'intersection des images de L et ℓ, les préimages de y par L sont un sous-espace affine $u+F$ et les préimages de y par ℓ sont un sous-espace affine $v+G$. L'intersection des sous-espaces affines $u+F$ et $v+G$ est toujours non-vide quand $F+G=V_n$ et contient seulement $u+v$ quand F et G sont d'intersection zéro. Par conséquent, dans les conditions du lemme, le noyau de $L+\ell$ est isomorphe à l'intersection des images de L et ℓ.

Le nombre de sous-espaces de V_m de dimension $n-s=r$ d'intersection de dimension t avec l'image de L de dimension $n-r$ est, comme vu à la section 2.2.6 :

$$\frac{S(n-r,t)S(m,n-t)S(r,t)}{S(t,t)S(m,n-r)S(r,r)}=\frac{S(r,t)S(n-r,t)}{S(t,t)}\frac{S(m,n-t)}{S(m,n-r)S(r,r)}\qquad(2.4)$$

Pour tout sous-espace de dimension r de V_m, le nombre d'applications linéaires de noyau G et d'image ce sous-espace est le nombre de bases ordonnées dans ce sous-espace, soit $S(r,r)$. Multiplier par $S(r,r)$ le nombre (2.4) donne donc le nombre

d'applications linéaires de noyau G et telles que $L+\ell$ ait un noyau de dimension t. La probabilité qu'une application aléatoire de noyau G vérifie cette condition s'obtient en divisant par leur nombre total $S(m,r)$. □

Nous pouvons retrouver le lemme précédent par le raisonnement du lemme 7. Dans les conditions du lemme précédent, $E_{r,s,i}(t)$ est donnée par le lemme 4 :

$$E_{r,n-r,0}(t) = S(r,t)S(n-r,t)/S(t,t)$$

Pour chaque sous-espace H de dimension t et d'intersection zéro avec F et G, les applications linéaires ℓ de noyau G et telles que $L+\ell$ s'annule sur H ont la même image sur le sous-espace $G+H$ de dimension $n-r+t$, et cette image est un sous-espace W de l'image de L de dimension t. Comme nous l'avons remarqué lors de la preuve du lemme 8, lorsque F et G sont supplémentaires, le noyau de $L+\ell$ est en bijection avec l'intersection des images de L et ℓ. Il suffit donc que l'image de ℓ sur un supplémentaire de $G+H$ soit d'intersection zéro avec l'image de L pour garantir que $L+\ell$ ne s'annule pas en dehors de H. Le nombre d'applications linéaires ℓ de noyau G et telles que le noyau de $L+\ell$ soit exactement H est donc le nombre de suites linéairement indépendante de longueur $t-r$ dans V_m engendrant un sous-espace d'intersection zéro avec l'image de L, soit $S(m,n-r+r-t)/S(m,n-r)$. Le lemme 8 se retrouve en divisant par le nombre $S(m,r)$ d'applications de noyau G.

Deuxième partie

C^* et Variations

Chapitre 3

Le schéma C^*

Alors que les premières tentatives de construction de schémas multivariés par Fell et Diffie semblent vaines [38], Matsumoto et Imai proposent un nouveau schéma, C^*, construit sur un principe différent [59] : la clé publique C^* admet une représentation cachée sous la forme d'un polynôme univarié, permettant de l'inverser. Présentant certaines similitudes avec le RSA, dont une certaine élégance et la possibilité d'être utilisé à la fois en chiffrement et en signature, C^* admet des performances bien supérieures. Malheureusement, il admet également une attaque très efficace, révélée par Patarin en 1995 [67]. Malgré cela, de nombreuses réparations ont été proposées, dont certaines sont parmi les schémas les plus populaires de la cryptographie multivariée.

Après une brève description de C^*, nous rappellerons l'attaque de Patarin, puis nous décrirons une autre attaque basée sur des propriétés différentielles. Les schémas abordés dans la suite étant tous dérivés de C^*, les éléments introduits dans ce chapitre sont essentiels à la compréhension des chapitres suivants.

3.1 Description de C^*

Le corps à q^n éléments, noté $\mathbb{F}_{q^n}$, est un $\mathbb{F}_q$-espace vectoriel de dimension n, et tout choix d'une base de cet espace définit un isomorphisme de $\mathbb{F}_{q^n}$ vers l'espace-produit $(\mathbb{F}_q)^n$. Toute fonction de $(\mathbb{F}_q)^n$ dans $(\mathbb{F}_q)^n$, définie par n polynômes en n variables, admet donc une représentation comme un polynôme univarié sur $\mathbb{F}_{q^n}$, qui dépend de l'isomorphisme de $\mathbb{F}_{q^n}$ vers $(\mathbb{F}_q)^n$ choisi.

Dans C^*, la clé publique $\boldsymbol{P}$ est la transformée par deux bijections linéaires secrètes S, T d'une fonction P admettant une représentation univariée facilement inversible dans $\mathbb{F}_{q^n}$:

$$\boldsymbol{P} = T \circ P \circ S$$

La forme univariée de P quant à elle est

$$P(x) = x^{1+q^\theta}$$

où θ est un paramètre entier positif et x est un élément de $\mathbb{F}_{q^n}$. L'élévation à la

puissance q est une application linéaire dans $\mathbb{F}_{q^n}$ appelée Frobenius, et P étant le produit des deux telles applications linéaires, il est isomorphe à une fonction quadratique de $(\mathbb{F}_q)^n$ dans lui-même. Par ailleurs, lorsque $1+q^\theta$ admet un inverse h modulo q^n-1, P admet pour inverse l'élévation à la puissance h. Un tel inverse ne peut exister quand q est impair car alors $1+q^\theta$ et q^n-1 sont tous les deux pairs et leur pgcd l'est aussi. Lorsque q est pair, l'inverse existe si et seulement si $n/\mathrm{pgcd}(\theta,n)$ est impair, comme le montre le lemme 9 ci-après. Élever à la puissance h peut être effectué efficacement, plus rapidement même qu'une évaluation de clé publique pour certains paramètres [59]. Finalement, P définit une fonction quadratique bijective de $(\mathbb{F}_q)^n$ dans lui-même, et induit ces mêmes propriétés sur $\boldsymbol{P}$. De plus, lorsque l'inverse h de $1+q^\theta$ modulo q^n-1 est de poids de Hamming élevé, l'inverse de P est une fonction polynomiale de degré élevé et il en est de même pour l'inverse de $\boldsymbol{P}$. Par exemple, il est montré dans [59] que quand n est impair ≥ 3 et θ est premier avec n, l'inverse de $\boldsymbol{P}$ est de degré environ $(q-1)n/2$.

La clé publique étant bijective, le schéma peut être utilisé en chiffrement et en signature. Les paramètres associés à un monôme C^* bijectif sont donnés par le lemme suivant.

Lemme 9. *Notant d le pgcd de θ et n, le monôme x^{1+q^θ} est bijectif si et seulement si q est pair et n/d est impair.*

Démonstration. Élever à la puissance $1+q^\theta$ est bijectif si et seulement si $q^\theta+1$ est premier avec q^n-1. Si q est impair, alors $q^\theta+1$ et q^n-1 sont tous les deux pairs et leur pgcd est divisible par 2. Si q est pair, alors $q^\theta-1$ et $q^\theta+1$ sont premiers entre eux, et donc

$$\mathrm{pgcd}(q^{2\theta}-1,q^n-1)=\mathrm{pgcd}(q^\theta-1,q^n-1).\mathrm{pgcd}(q^\theta+1,q^n-1)$$

On note A,B et C les trois pgcds ci-dessus. On va d'abord calculer A et B, puis on en déduira C. Notant d le pgcd de θ et n, on a classiquement $B=q^d-1$. De la même façon, A vaut $q^{\mathrm{pgcd}(2\theta,n)}-1$. Comme

$$\mathrm{pgcd}(2\theta,n)=d.\mathrm{pgcd}(2\frac{\theta}{d},\frac{n}{d})$$

et puisque $\frac{\theta}{d}$ et $\frac{n}{d}$ sont premiers entre eux, le pgcd de droite vaut 2 quand $\frac{n}{d}$ est pair et 1 sinon. Ainsi, A vaut $q^{2d}-1$ quand $\frac{n}{d}$ est pair et q^d-1 si $\frac{n}{d}$ est impair. Finalement, C vaut q^d+1 si $\frac{n}{d}$ est pair et 1 si $\frac{n}{d}$ est impair. □

Le schéma de Cade

En 1985, Cade a proposé un schéma apparaissant comme un cas particulier de C^* associé aux choix de paramètres $\theta=1$, $n=3$ et q une grande puissance de 2 [10]. Ces choix de paramètres ne semblent pas présenter d'intérêt spécifique, hormis celui de simplifier le schéma. Si la publication de Cade est bien antérieure à celle de C^*, le prototype de C^* avait déjà été développé indépendamment par

Matsumoto et Imai sous le nom de "schéma A" dès 1983 [60, 47]. En 1986, James, Lidl et Niederreiter ont présenté une attaque sur le schéma de Cade, permettant de retrouver la clé secrète [49, 48]. Cette attaque est cependant très spécifique aux paramètres choisis par Cade, car elle exploite la très petite valeur de n, et ne s'étend pas au cas plus général de C^*. Peu après, Cade a proposé une réparation de son schéma [11], consistant en un cas particulier de la variante "par blocs" de C^* [59]. En 1995, les nouvelles idées développées par Patarin ont permis de cryptanalyser C^* ainsi que ses variantes par blocs [67].

3.2 L'attaque de Patarin

Lors de la conférence Crypto'95, Patarin a montré des propriétés induites par la forme spécifique du monôme interne de C^* rendant possible le déchiffrement sans la clé secrète [67]. Par définition, un élément x et son image y par P vérifient la relation :

$$y = x^{1+q^\theta} \tag{3.1}$$

En élevant cette équation à la puissance $q^\theta - 1$, on obtient alors :

$$y^{q^\theta - 1} = x^{q^{2\theta} - 1} \tag{3.2}$$

et par conséquent :

$$xy^{q^\theta} - x^{q^{2\theta}} y = 0 \tag{3.3}$$

Par linéarité de l'élévation à la puissance q, l'équation ci-dessus est bilinéaire en x, y. Après application d'un isomorphisme de $\mathbb{F}_{q^n}$ dans $(\mathbb{F}_q)^n$, elle s'écrit comme n équations multivariées bilinéaires en les coordonnées de x et y. L'application des bijections linéaires secrètes S et T transforment ces équations en n équations multivariées bilinéaires en les valeurs entrées et sorties de la clé publique $\boldsymbol{P}$, autrement dit entre messages clairs et chiffrés. Ces équations bilinéaires peuvent être déterminées à partir d'environ n^2 couples clair-chiffré en résolvant le système linéaire correspondant en leur coefficients. Une fois recomposées, ces équations bilinéaires induisent, pour chaque message chiffré y, des équations linéaires en le message clair x. Ces équations ne forment pas un système de rang plein mais pourvu que l'espace-solution de ces équations puisse être exhaustivement parcouru, le message clair peut être identifié comme le seul satisfaisant $\boldsymbol{P}(x) = y$.

Nous déterminons maintenant la dimension de l'espace-solution. Les solutions non nulles de l'équation (3.3) sont les solutions de l'équation (3.2). Cette dernière s'obtient par élévation à la puissance $q^\theta - 1$ de l'équation (3.1) et peut alternativement s'écrire :

$$y^{q^\theta - 1} = (x^{q^\theta - 1})^{q^\theta + 1} = P(x^{q^\theta - 1})$$

L'élément x antécédent de y par P est solution de cette équation, et comme P est une bijection, les autres solutions non-nulles sont multiples de cet élément x par les éléments d'ordre de $q^\theta - 1$, dits encore racines $(q^\theta - 1)$-ièmes de l'unité.

Leur nombre est $\gcd(q^\theta - 1, q^n - 1)$, soit $q^d - 1$ où d est le pgcd de θ et n. Les $q^d - 1$ solutions de l'équation (3.2) forment avec le vecteur nul l'espace-solution de l'équation (3.3), de dimension d.

Compte-tenu du calcul précédent, la complexité de l'attaque de Patarin est environ n^6 pour recomposer les équations bilinéaires clair-chiffré, puis $q^d n^3$ pour identifier le message clair correspondant à un chiffré donné utilisant la condition $\boldsymbol{P}(x) = y$. Bien que les équations bilinéaires puissent toujours être reconstruites pour les valeurs pratiques de n, la seconde phase peut ne pas être faisable si q et d sont grands. Dans [67], Patarin montre l'existence d'autres relations implicites entre clair et chiffré, qui sont d'ordre supérieur mais linéaires sur l'espace des messages clairs. Les équations linéaires correspondant à un chiffré donné ont pour unique solution le message clair original. Le degré de ces autres relations implicites est $(k + 1)/2$ où $k = n/d$, et la complexité pour les reconstruire est $n^{\frac{3}{2}(k+1)}$. Cette seconde attaque est donc efficace quand d est grand devant n, et permet généralement de traiter les cas où la première attaque échoue.

Il est apparu plus tard que C^* était également vulnérable à une attaque de déchiffrement par les bases de Gröbner [51]. Ceci peut effectivement être vu à partir de l'attaque de Patarin elle-même. Pour calculer une base de Gröbner d'un système de polynômes multivariés donnés en entrée, les algorithmes modernes tels que F4 ou F5 [35, 36] cherchent des dépendances linéaires entre les multiples algébriques de degré prescrit de ces polynômes. Certaines de ces dépendances sont triviales car elles proviennent de relations formelles vérifiées par tout système de polynômes. Les autres dépendances ont par contre des origines structurelles et l'apparition des premières d'entre elles annoncent généralement la fin du calcul de base de Gröbner. La complexité de l'algorithme est fonction du degré jusqu'auquel il est nécessaire de monter pour trouver ces dépendances non-triviales. Or, dans le cas de C^*, les équations bilinéaires de Patarin sont des relations non-triviales apparaissant au degré 3 puisqu'elles s'écrivent sur la base des multiples de degré 1 des coordonnées de $\boldsymbol{P}(x)$. Il n'est donc pas surprenant que C^* soit vulnérable aux attaques par bases de Gröbner ; être vulnérable aux attaques par bases de Gröbner et satisfaire des relations implicites de petit degré sont conceptuellement identiques. Ainsi, bien que l'inverse de la clé publique C^* soit de grand degré, elle n'en admet pas moins des relations algébriques de bas degré sur ses entrées-sorties.

3.3 Une attaque différentielle sur C^*

Lors de la conférence Eurocrypt 2005, Fouque, Granboulan et Stern ont montré une seconde cryptanalyse de C^* basée sur des propriétés de la différentielle [40]. Ces propriétés impliquent l'existence d'équations bilinéaires entre message chiffré et éléments du noyau dual de la différentielle, et entre éléments du noyau dual et le message clair. Ces équations bilinéaires permettent, comme dans l'attaque de Patarin, de déchiffrer sans la clé secrète avec complexité facteur de q^d. Présenter cette attaque sera l'occasion d'établir certaines propriétés remarquables de la

différentielle de C^*. Par ailleurs, la présentation ci-après a pour particularité par rapport à la description originale de l'attaque, d'utiliser la notion d'adjoint d'une application linéaire afin de caractériser les propriétés duales de la différentielle.

Le noyau de la différentielle d'un monôme C^* : Rappelons que la différentielle d'une application quadratique P en un élément a est l'application linéaire notée DP_a définie par :

$$DP_a(x) = P(a+x) - P(x) - P(a) + P(0)$$

Quand P est un monôme C^*, $P(x) = x^{1+q^\theta}$, sa différentielle en a est

$$DP_a(x) = ax^{q^\theta} + a^{q^\theta}x$$

Lorsque a est non-nul, cette différentielle peut se récrire :

$$DP_a(x) = a^{1+q^\theta} \cdot \left(\left(\frac{x}{a}\right) + \left(\frac{x}{a}\right)^{q^\theta} \right)$$

Notant M_a la multiplication par un élément a de $\mathbb{F}_{q^n}$, et L l'application linéaire $z \mapsto z + z^{q^\theta}$, la différentielle s'écrit alors comme la composition :

$$DP_a = M_{P(a)} \circ L \circ M_{a^{-1}} \tag{3.4}$$

Les deux multiplications étant des bijections linéaires, le noyau de DP_a est isomorphe au noyau de L. Plus exactement :

$$\ker DP_a = a.\ker L$$

Les éléments non-nuls du noyau de L vérifient $z^{q^\theta-1} = 1$, ceux sont donc les racines $(q^\theta-1)$-ièmes de l'unité, et leur nombre est q^d-1 où $d = \text{pgcd}(\theta, n)$. Par conséquent, le noyau de L et celui de DP_a sont de dimension d.

Le noyau *dual* de la différentielle d'un monôme C^* : On s'intéresse maintenant au noyau dual de DP_a, c'est-à-dire aux formes linéaires orthogonales à l'image de DP_a. On peut s'attendre au vu de l'équation (3.4) à ce qu'il existe une certaine relation entre ces éléments et $P(a)$.

La trace de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ est l'application linéaire à valeurs dans $\mathbb{F}_q$ définie par

$$tr(z) = z + z^q + z^{q^2} + \ldots + z^{q^{n-1}} = \textstyle\sum_{i=0}^{n-1} z^{q^i}$$

L'application bilinéaire $(x, y) \mapsto tr(xy)$, de $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ dans $\mathbb{F}_q$, définit un produit non-dégénéré [57]. Dans ces conditions, pour toute forme linéaire f, il existe un unique élément y tel que $f = tr(\cdot y)$, et l'espace des formes linéaires orthogonales à l'image de DP_a est isomorphe à l'espace des éléments y pour lesquels

$tr(DP_a(x).y) = 0$ pour tout x. Dans ces mêmes conditions, pour toute application linéaire A, il existe une unique application linéaire notée A^* satisfaisant

$$tr(A(x).y) = tr(x.A^*(y))$$

et cette application linéaire s'appelle l'adjoint de A. Les éléments y pour lesquels $tr(y.DP_a(x)) = 0$ pour tout x, sont donc les éléments du noyau de DP_a^*.

Calculons maintenant le noyau de DP_a^*. Il est immédiat de vérifier que l'adjoint d'une composition $A \circ B$ est la composition $B^* \circ A^*$. Il est également immédiat de voir que les multiplications sont leur propre adjoint. Nous avons donc :

$$DP_a^* = M_{a^{-1}} \circ L^* \circ M_{P(a)}$$

Finalement, en utilisant la commutativité de la trace avec les Frobenius :

$$tr(L(x).y) = tr(xy) + tr(x^{q^\theta} y) = tr(xy) + tr(xy^{q^{n-\theta}}) = tr(x.(y + y^{q^{n-\theta}}))$$

et par conséquent :

$$L^*(y) = y + y^{q^{n-\theta}}$$

Les éléments non-nuls du noyau de L^* vérifient $y^{q^{n-\theta}-1} = 1$. Élevant cette équation à la puissance $-q^\theta$, on obtient $y^{q^\theta - 1} = 1$ et nous avons donc : $\ker L^* = \ker L$. Finalement, on obtient :

$$\ker DP_a^* = P(a)^{-1}.\ker L \tag{3.5}$$

Attaque de déchiffrement : Comme le noyau de L est de dimension d, il existe $n - d$ formes linéaires indépendantes $f_1, \ldots, f_{n-d}$ qui lui sont orthogonales. De l'équation (3.5) précédente, on déduit que les éléments y du noyau de DP_a^* sont les solutions des $n - d$ équations linéaires :

$$f_i(P(a).y) = 0\,,\ i = 1, \ldots, n - d$$

Ces équations sont bilinéaires en $P(a)$ et y. En outre, comme par définition

$$tr(DP_a(x).y) = 0$$

pour tout x, et que $DP_a(x)$ est linéaire en a, il existe également des équations bilinéaires en y et a. Considérant ces équations sur une base $y_1, \ldots, y_d$ du noyau dual et une base $x_1, \ldots, x_n$ de $\mathbb{F}_{q^n}$, on forme des équations linéaires en a. Les solutions non-nulles de ces équations linéaires sont les éléments b non-nuls ayant le même noyau dual que a. D'après l'équation (3.5), ce sont ceux pour lesquels $P(b)$ est dans la même classe que $P(a)$ modulo les éléments non-nuls du noyau de L ; ces derniers éléments sont, comme nous l'avons vu, les racines $(q^\theta - 1)$-ième de l'unité, et forment un groupe multiplicatif. Comme P est une bijection, les éléments b cherchés sont au nombre de $q^d - 1$. Finalement, l'espace des solutions des équations linéaires en a considérées est de dimension d.

Nous obtenons donc deux ensembles d'équations bilinéaires B et B', reliant $P(a)$ et a par l'intermédiaire des éléments du noyau dual : $B(P(a), y) = 0$ et $B'(y, a) = 0$, pour tout y dans le noyau de DP_a^*. Ces équations bilinéaires induisent des équations du même type sur la clé publique $\boldsymbol{P}$. Celles-ci peuvent être recomposées de la clé publique en calculant, pour de l'ordre de n^2 éléments a, à la fois la valeur de $\boldsymbol{P}(a)$ et les formes linéaires orthogonales à $D\boldsymbol{P}_a$ (ou sous forme matricielle, le noyau de la transposée). Une fois ceci fait, pour tout chiffré, on détermine d vecteurs linéairement indépendants $y_1, \ldots, y_d$, puis évaluant le second jeu d'équations bilinéaires en ces éléments, on détermine un espace de dimension d contenant le message clair. Pourvu que ce sous-espace puisse être parcouru par recherche exhaustive (c'est-à-dire lorsque q^d n'est pas trop grand, comme pour l'attaque de Patarin), on identifie le message clair comme celui dont l'image par $\boldsymbol{P}$ est bien le message chiffré considéré. La complexité de l'attaque est identique à celle de l'attaque de Patarin [67].

Chapitre 4

PMI et PMI+

PMI et PMI+ sont des schémas de chiffrement introduits par Ding à PKC'04 [20] et Ding-Gower à PKC'06 [21]. Ils sont dérivés de C^* par *perturbation interne*, une méthode visant à renforcer un schéma multivarié vis-à-vis des attaques algébriques.

4.1 PMI

PMI signifie *Perturbed Matsumoto-Imai*. Il s'obtient à partir d'un C^* en ajoutant à la fonction interne une fonction quadratique aléatoire contrôlée par une fonction linéaire de petit rang. On note $P(x) = x^{1+q^\theta}$ la fonction interne C^* vue comme un polynôme sur $\mathbb{F}_{q^n}$. La perturbation se compose d'une fonction quadratique notée $\bar{P}$ choisie aléatoirement de $(\mathbb{F}_q)^n$ dans lui-même, et d'une fonction linéaire de petit rang r notée Z choisie aléatoirement de $(\mathbb{F}_q)^n$ dans lui-même. La fonction interne PMI notée $\tilde{P}$ est définie par

$$\tilde{P}(x) = P(x) + \bar{P} \circ Z(x)$$

Pourvu que q^r soit petit, cette fonction reste facile à inverser. Le terme $\bar{P} \circ Z(x)$ prend au plus q^r valeurs différentes, et trouver les antécédents par $\tilde{P}$ d'un y donné revient à résoudre un système

$$\left\{ \begin{array}{rcl} y & = & P(x) + z \\ z & = & \bar{P} \circ Z(x) \end{array} \right.$$

pour chacune des q^r valeurs z de l'image de $\bar{P} \circ Z$. Ce système se résout en calculant l'antécédent de $y - z$ par P et vérifiant s'il satisfait la seconde équation. Dans l'éventualité de solutions multiples, l'usage de redondance dans les messages permet d'identifier le message correct. La clé publique PMI est une fonction

$$\tilde{\boldsymbol{P}} = T \circ \tilde{P} \circ S$$

où S et T sont des bijections linéaires (ou affines) aléatoirement choisies. Dans [20], Ding propose pour PMI les paramètres $(q, n, \theta, r) = (2, 136, 40, 6)$. On notera que $d = \text{pgcd}(\theta, n)$ vaut 8 pour ces paramètres ; ce choix est justifié par Ding comme permettant une inversion plus rapide de la fonction interne C^*.

4.2 PMI et les attaques algébriques de déchiffrement

L'existence d'équations bilinéaires entre couple clair-chiffré est une propriété très particulière du C^*, et l'on ne s'attend bien sûr pas à ce que l'attaque de Patarin puisse – en l'état – s'appliquer à PMI. Généraliser l'attaque en degré supérieur aurait pu être envisagé, mais considérer la résistance de PMI aux attaques par bases de Gröbner, plus générales, a été préféré. Dans [22], temps de calcul et mémoire en utilisant l'algorithme F4 implémenté dans MAGMA ont été mesurés sur des exemples de tailles réduites, puis extrapolés pour plusieurs paramètres pratiques selon un modèle exponentiel et un modèle polynomial. Même si les estimations de complexité obtenues dans le modèle exponentiel sont sans doute largement surestimées, les complexités en mémoire restent hors de portée dans le modèle polynomial. Par conséquent, PMI résiste aux attaques algébriques.

Alternativement aux arguments expérimentaux cités précédemment, les complexités en temps et en mémoire utilisant F4 (ou F5) auraient pu être déterminées théoriquement de la façon suivante. On rappelle d'abord brièvement le fonctionnement de F4 (et F5). Pour simplifier, on considère toujours $q = 2$ dans la suite.

L'algorithme prend en entrée une suite de polynômes (supposés ici quadratiques) appelés générateurs et les multiplie par des monômes de degré $d-2$ pour d croissant. Pour chaque degré d, les polynômes ainsi obtenus s'écrivent sur la base des monômes de degré d comme une matrice appelée matrice de Macaulay de degré d et notée $\mathcal{M}_d$ dans la suite. Quand les monômes sont considérés sans carrés, le nombre de monômes de degré d, soit le nombre de colonnes de $\mathcal{M}_d$, est $\binom{n}{d}$. Lorsque les polynômes donnés en entrée sont quadratiques et au nombre de n, le nombre de lignes de $\mathcal{M}_d$ est $R_d = n.\binom{n}{d-2}$. On note $\mathcal{K}_d$ l'ensemble des dépendances linéaires entre les lignes de $\mathcal{M}_d$, c'est un sous-espace vectoriel de $(\mathbb{F}_2)^{R_d}$. Cet espace vectoriel est non-trivial au moins à partir de $d \geq 4$ puisqu'il contient alors les dépendances linéaires issues des relations de commutations entre générateurs $p_i p_j = p_j p_i$. Les relations triviales engendrent un espace de dimension

$$\tau_d = \frac{n(n-1)}{2}\binom{n}{d-4}$$

Le degré à partir duquel apparaissent les premières dépendances linéaires non triviales est appelé degré de régularité. Ces dépendances apparaissent généralement en grand nombre et le calcul se termine peu après. Ceci décrit schématiquement l'algorithme F4. Dans l'algorithme F5, les dépendances linéaires triviales sont identifiées et enlevées de façon à gagner du temps et de l'espace.

On cherche maintenant à déterminer le degré de régularité d'un système PMI. Comme celui-ci est conservé par changement de variables bijectif et opérations linéaires inversibles, il est équivalent de considérer le système interne. Pour tout d, la matrice $\mathcal{M}_d$ s'écrit comme la somme

$$\mathcal{M}_d = \mathcal{M}_d^* + \bar{\mathcal{M}}_d$$

où $\mathcal{M}_d^*$ est la matrice de Macaulay de degré d engendrée par les polynômes coordonnées de P, et $\bar{\mathcal{M}}_d$ est la matrice de Macaulay de degré d engendrée par les polynômes coordonnées de $\bar{P} \circ Z$. Les dépendances linéaires sur $\mathcal{M}_d^*$ forment un espace $\mathcal{K}_d^*$, celles sur $\bar{\mathcal{M}}_d$ forment un espace $\bar{\mathcal{K}}_d$. Le sous-espace $\mathcal{K}_d$ des dépendances linéaires sur $\mathcal{M}_d$ contient le sous-espace des dépendances triviales de dimension τ_d et les dépendances linéaires simultanées sur $\mathcal{M}_d^*$ et $\bar{\mathcal{M}}_d$. Compte-tenu des natures très différentes des générateurs de $\mathcal{M}_d^*$ et $\bar{\mathcal{M}}_d$, on peut raisonnablement supposer que les dépendances des deux types précédents sont d'intersection triviale et engendrent l'ensemble des dépendances sur $\mathcal{M}_d$. Sous cette hypothèse :

$$\dim \mathcal{K}_d = \tau_d + \dim(\mathcal{K}_d^* \cap \bar{\mathcal{K}}_d)$$

Lorsque $\bar{\mathcal{K}}_d$ est vu comme un espace aléatoire, son intersection avec $\mathcal{K}_d^*$ est minimale, et donc triviale jusqu'à ce que

$$\dim \mathcal{K}_d^* + \dim \bar{\mathcal{K}}_d > R_d - \tau_d$$

Il nous reste à déterminer les dimensions de $\mathcal{K}_d^*$ et $\bar{\mathcal{K}}_d$.

Lemme 10.

$$\dim \bar{\mathcal{K}}_d = R_d - \sum_{j=2}^{d} \binom{r}{j}\binom{n-r}{d-j}$$

Démonstration. On peut supposer que l'image de Z consiste en les r premières coordonnées. Alors, les fonctions coordonnées de $\bar{P} \circ Z$ sont n vecteurs aléatoires sur la base des monômes quadratiques sur $x_1, \ldots, x_r$, et au plus $r(r-1)/2$ de ces vecteurs sont linéairement indépendants. Ainsi, une base des lignes de $\bar{\mathcal{M}}_d$ sont les vecteurs obtenus en multipliant les $r(r-1)/2$ monômes $x_i x_j$ avec $1 \leq i < j \leq r$ par tous les monômes de degré $d-2$. On génère ainsi tous les monômes de degré d contenant au moins deux variables x_i et x_j dans $\{1, \ldots, r\}$. Le nombre de tels monômes ayant j variables dans $\{1, \ldots, r\}$ est $\binom{r}{j}\binom{n-r}{d-j}$ et la dimension de l'espace engendré par les lignes de $\bar{\mathcal{M}}_d$ est la somme de ces nombres pour j de 2 à d. □

Lemme 11. *Quand* $pgcd(\theta, n) = 1$*, on a*

$$\dim \mathcal{K}_d^* = R_d - \binom{n}{d} + \frac{n}{n-d}\binom{n-d}{d}$$

Démonstration. La fonction P est définie par un monôme x^{1+2^θ} sur $\mathbb{F}_{2^n}$. Sur une base normale $\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}$, nous avons :

$$P(x) = \textstyle\sum_{i=0}^{n-1} p_i(x)\alpha^{2^i} \qquad \text{et} \qquad x = \textstyle\sum_{i=0}^{n-1} x_i \alpha^{2^i}$$

On peut observer que la première coordonnée de P^{2^j} est p_j, et la première coordonnée de x^{2^i} est x_i. Ainsi, lorsque i et j varient, la première coordonnée des produits des P^{2^j} par tous les produits de $d-2$ Frobenius $x^{2^{i_1}} \ldots x^{2^{i_{d-2}}}$, décrit l'ensemble

des produits des p_j par tous les monômes de degré $d-2$, qui définissent les lignes de $\mathcal{M}_d^*$. La dimension de l'espace engendré par les lignes de $\mathcal{M}_d^*$ (soit le nombre de lignes distinctes) est donc égale au nombre de produits de d Frobenius dont 2 indices au moins sont décalés de θ. C'est encore le nombre de sous-ensembles de d entiers modulo n dont deux au moins sont décalés de θ. On calcule le complémentaire de ce nombre (le dénombrement est dû à Nicolas Gama). Comme θ est premier avec n, on peut le supposer égal à 1. Le nombre cherché correspond au nombre de façons de choisir d éléments sur un cercle de longueur n tels qu'aucun élément choisi ne soit consécutif à un autre. Les éléments choisis sont marqués par des 1 et les autres par des 0. Si le dernier élément du cercle n'est pas choisi, alors cela revient à placer d suites $(1,0)$ sur un segment de longueur n. On définit uniquement un tel placement en distinguant d indices dans la suite des $n-d$ zéros à placer ; nous avons donc $\binom{n-d}{d}$ possibilités. Si le dernier élément est choisi, le premier ne peut l'être, et cela revient à placer $d-1$ couples $(0,1)$ sur un segment de longueur $n-2$ soit $\binom{n-d-1}{d-1}$. La somme de ces deux nombres est $\frac{n}{n-d}\binom{n-d}{d}$. □

Finalement le degré de régularité noté δ d'un système PMI de paramètre r est estimé au plus petit entier d satisfaisant

$$\binom{n}{d} - \frac{n}{n-d}\binom{n-d}{d} + \sum_{j=2}^{d}\binom{r}{j}\binom{n-r}{d-j} < n\binom{n}{d-2} + \frac{n(n-1)}{2}\binom{n}{d-4}$$

La complexité de F4 est dominée par l'algèbre linéaire effectuée sur la matrice de Macaulay au degré δ. Les matrices de Macaulay étant creuse avec des lignes de poids $n(n+1)/2$, la complexité en temps de l'algèbre linéaire est en $n(n+1)R_\delta^2/2$ et la complexité en mémoire en $n(n+1)R_\delta/2$. La complexité de F5 s'obtient en remplaçant R_δ par $R_\delta - \tau_\delta$ dans les formules précédentes.

Dans la table ci-dessous, on compare les données expérimentales de [22] avec le calcul précédent. Les estimations du calcul précédent sont prises pour un entier θ premier avec n. Les temps et mémoires sont donnés par leur log en base 2.

	Calcul précédent			Données expérimentales	
(q,n,r)	δ	Temps (bin.op.)	Mém. (bits)	Temps (bin.op.)	Mém. (bits)
$(2,24,3)$	3	26.44	17.27	33.84	25.50
$(2,24,6)$	5	39.24	23.67	39.26	29.61
$(2,24,9)$	5	39.24	23.67	39.82	29.72
$(2,31,3)$	3	28.67	18.76	38.08	28.16
$(2,31,5)$	4	36.49	22.67	39.29	29.79
$(2,38,3)$	3	30.44	19.95	40.87	30.16

Comme on peut l'observer, notre estimation de complexité basée sur la taille de la matrice de Macaulay au degré δ est un peu optimiste, en particulier pour les petites valeurs de r. En pratique, et en particulier quand δ est petit, l'algorithme doit parfois construire la matrice de Macaulay de degré $\delta+1$, et plus rarement

au-delà, avant de pouvoir terminer le calcul de base de Gröbner. Une autre explication possible de ces différences tient au fait que nous avons estimé la complexité en mémoire à partir de la matrice de Macaulay au degré δ *avant* que l'algèbre linéaire soit effectuée sur cette matrice, et n'avons donc pas tenu compte de la densification conséquente aux opérations linéaires. D'autres divergences enfin, entre le calcul théorique et la complexité pratique observée, pourraient être dues à certaines variations de l'implémentation, consistant par exemple à ne mettre en œuvre la stratégie optimale (algèbre linéaire creuse, suppression de relations triviales) qu'à partir d'un certain degré. L'implémentation ayant servi aux expérimentations citées n'étant pas publique, il est difficile de s'avancer plus sur ce point.

Selon notre calcul, un système PMI a pour les paramètres suggérés $(2, 136, 6)$ un degré de régularité de 5. L'algorithme F4 devra donc monter en degré au moins 5 voire 6, ce qui requiert au moins $2^{64.63}$ opérations binaires (2^{70} estimées dans le modèle polynomial de [22]) et $2^{38.89}$ bits en mémoire pour en calculer une base de Gröbner. Considérant l'importante quantité de mémoire nécessaire à la mise en œuvre d'une telle attaque, PMI offre donc une certaine résistance (conforme aux standards cryptographiques ?) vis-à-vis des attaques par bases de Gröbner.

4.3 Un biais différentiel de perturbation

Résister aux attaques "frontales" par bases de Gröbner est le minimum pouvant être attendu d'un schéma multivarié, et ces méthodes ne sont pas nécessairement les plus efficaces pour attaquer un système. À Eurocrypt'05, Fouque-Granboulan-Stern ont présenté une attaque très efficace sur PMI utilisant des propriétés de sa différentielle [40]. On rappelle brièvement le principe de cette attaque, puis on présentera une autre attaque basée sur des propriétés plus fines de la différentielle.

4.3.1 L'attaque différentielle de Fouque-Granboulan-Stern

La fonction interne du PMI est

$$\tilde{P}(x) = P(x) + \bar{P} \circ Z(x)$$

avec P un monôme C^*, $\bar{P}$ quadratique aléatoire et Z linéaire de petit rang r. Notant $\mathcal{K}$ le noyau de Z, on observe que sur tout sous-espace affine parallèle à $\mathcal{K}$, $\tilde{P}$ coïncide avec la fonction P à une constante près – c'est d'ailleurs ce qui permet de déchiffrer. De la même façon, la clé publique $\tilde{\boldsymbol{P}} = T \circ \tilde{P} \circ S$ coïncide avec la fonction $T \circ P \circ S$ (qui est une clé publique C^*) à une constante près sur chaque parallèle au sous-espace $\boldsymbol{\mathcal{K}} = S^{-1}(\mathcal{K})$. Le secret du sous-espace $\boldsymbol{\mathcal{K}}$ est donc le seul qui importe, puisque la connaissance de ce sous-espace permet de partitionner la clé publique PMI en q^r clés publiques C^*, qui peuvent toutes être inversées comme montré par Patarin [67]. On appellera le sous-espace $\boldsymbol{\mathcal{K}}$ le *noyau de la perturbation*.

Considérant maintenant la différentielle de $\tilde{P}$ en un élément a,

$$D\tilde{P}_a = DP_a + D\bar{P}_{Z(a)} \circ Z$$

on remarque que cette différentielle n'est autre que celle de P quand a est dans $\mathcal{K}$, ce qui arrive avec probabilité q^{-r}. Par conséquent, pour tout a dans $\mathcal{K}$, la différentielle a un noyau de dimension $d = \text{pgcd}(\theta, n)$. Par contre, quand a n'est pas dans $\mathcal{K}$, le terme de perturbation intervient et d'autres dimensions, dans l'intervalle $[d-r, d+r]$, peuvent être atteintes. Ces propriétés sont conservées par bijections linéaires et se transposent à $\tilde{\boldsymbol{P}}$ et $\boldsymbol{\mathcal{K}}$. On rapporte ci-dessous les distributions expérimentales fournies dans [40] pour la dimension du noyau de la différentielle dans l'un et l'autre cas, pour les paramètres suggérés.

$\dim\ker D\tilde{\boldsymbol{P}}_a$	3	4	5	6	7	8	>8
$a \in \boldsymbol{\mathcal{K}}$						1	
$a \notin \boldsymbol{\mathcal{K}}$	≈ 0.686	≈ 0.290	≈ 0.023	$\approx 5e-4$	$\approx 2e-6$	≈ 0	≈ 0

Comme on peut le constater, la dimension du noyau de la différentielle et l'appartenance à $\boldsymbol{\mathcal{K}}$ sont très fortement corrélés ; un distingueur basé sur cette corrélation a un avantage très proche de 1 quand $d = \text{pgcd}(\theta, n)$ est grand. Utilisant le fait que $\boldsymbol{\mathcal{K}}$ est clos par linéarité, il est possible d'amplifier le biais par itération pour identifier des éléments de $\boldsymbol{\mathcal{K}}$ avec très faible probabilité d'erreur, et trouver environ n tels éléments permet de reconstruire $\boldsymbol{\mathcal{K}}$ avec forte probabilité. Dans [40], la complexité pour restaurer $\boldsymbol{\mathcal{K}}$ est estimée à nq^{3r} évaluations de la clé publique, soit environ 2^{49} opérations binaires. L'attaque ne nécessite pas de mémoire.

4.3.2 Une attaque alternative

La dimension constante égale à d n'est pas la seule propriété des noyaux de la différentielle d'un monôme C^*. Dans cette section, on montre une propriété ensembliste des noyaux C^*. Cette propriété permet de construire un distingueur alternatif à celui vu précédemment.

Comme on l'a vu au chapitre précédent, la différentielle de $P(x) = x^{1+q^\theta}$ en a non-nul s'écrit :

$$DP_a(x) = P(a) \cdot L\left(\frac{x}{a}\right)$$

où L est l'application linéaire $z \mapsto z + z^{q^\theta}$. Par conséquent, pour tout a non-nul, le noyau de DP_a est le sous-espace $a \cdot \ker L$. De par leur forme, les noyaux C^* satisfont pour tout a et b non-nuls la relation d'inclusion : $\ker DP_{a+b} \subset \ker DP_a + \ker DP_b$. Par ailleurs, les éléments non-nuls de $\ker L$ sont les racines $(q^\theta - 1)$-ièmes de l'unité et forment un groupe. En en déduit donc que les noyaux C^* en deux éléments a et b sont soit le même sous-espace, soit des espaces d'intersection zéro. Finalement pour tout couple (a, b) d'éléments distincts non-nuls, on a :

$$\ker DP_{a+b} \subset \ker DP_a \oplus \ker DP_b \tag{4.1}$$

Il s'agit là d'une propriété extrêmement forte : un tel cas de figure n'apparaît jamais pour des sous-espaces aléatoires – plus exactement, cela n'apparaît qu'avec probabilité négligeable $E(2d, d)/E(d, d) \simeq q^{-d(n-2d)}$ (voir le chapitre 2 pour les notations).

De même, une telle propriété ensembliste paraît extrêmement improbable sur des sous-espaces d'une nature plus aléatoire comme les noyaux de la différentielle de PMI. On peut donc utiliser cette propriété pour identifier des couples d'éléments a, b du noyau de la perturbation $\boldsymbol{\mathcal{K}}$. On s'attend à trouver deux tels éléments après q^{2r} tirages aléatoires. Utilisant l'un quelconque de ces deux éléments, on obtient un autre élément de $\boldsymbol{\mathcal{K}}$ après environ q^r tirages aléatoires. Finalement, on estime la complexité de cette attaque à $q^{2r} + nq^r$ évaluations de la clé publique. Bien que cette attaque soit estimée plus efficace que la précédente dans le cas général, elle ne permet pas d'attaquer les instances PMI pour lesquelles $d = 1$, puisqu'alors la propriété (4.1) est triviale.

4.4 PMI+

Lors de la conférence PKC 2006, Ding et Gower ont proposé une parade pour déjouer l'attaque de Fouque-Granboulan-Stern et un nouveau schéma, PMI+, en réparation de PMI [21]. La modification proposée permet de diminuer la corrélation entre la dimension du noyau de la différentielle et l'appartenance au noyau de la perturbation $\boldsymbol{\mathcal{K}}$, de façon à empêcher la reconstruction efficace de $\boldsymbol{\mathcal{K}}$ par la méthode décrite dans [40]. A première vue, la seconde attaque décrite à la section précédente est également déjouée et, même s'il serait intéressant de quantifier cela, le fait qu'elle ne s'applique pas aux schémas PMI+ pour lesquels $d = 1$ limite l'intérêt de poursuivre sur cette voie. On présente maintenant le schéma PMI+, puis on explique pourquoi ce schéma résiste à l'attaque de Fouque-Granboulan-Stern.

4.4.1 Description

La fonction interne PMI+ s'obtient en ajoutant à la suite des n polynômes-coordonnées définissant la fonction $\tilde{P}$ un petit nombre s de polynômes choisis aléatoirement où s est un nouveau paramètre. La fonction interne PMI+, notée $\tilde{P}^+$, est donc une fonction de $(\mathbb{F}_q)^n$ dans $(\mathbb{F}_q)^{n+s}$. Pour inverser cette fonction, on inverse la fonction $\tilde{P}$ puis, en cas de solutions multiples, on identifie le message correct en utilisant la redondance fournie par les fonctions aléatoires supplémentaires, ou une redondance interne au message comme pour PMI. La clé publique est une fonction $T^+ \circ \tilde{P}^+ \circ S$ où T^+ est une bijection linéaire de $(\mathbb{F}_q)^{n+s}$ dans lui-même et S une bijection linéaire de $(\mathbb{F}_q)^n$ dans lui-même. Pourvu qu'ils restent en petit nombre, l'ajout de polynômes supplémentaires aléatoires à la fonction interne ne change pas la difficulté d'inverser la clé publique par les bases de Gröbner.

4.4.2 Fonctionnement de la contre-mesure

Voyons maintenant pourquoi la parade de Ding et Gower permet de contrer l'attaque de Fouque-Granboulan-Stern. Une telle explication peut être trouvée dans [21], on en donne ici une autre plus simple. La différentielle de $\tilde{P}^+$ en a est une matrice à $n + s$ lignes et n colonnes, dont les n premières lignes sont les lignes de

$D\tilde{P}_a$ et les s suivantes sont des vecteurs aléatoires orthogonaux à a. Quand l'espace engendré par les lignes de $D\tilde{P}_a$ n'est pas de dimension maximale $n-1$, l'ajout de vecteurs aléatoires va contribuer à combler cette dimension, et finalement, pour s assez grand, le rang de la différentielle est égal à $n-1$ avec forte probabilité. Dit autrement, le noyau de la différentielle de PMI+ est trivial de dimension égale à 1 en tout point avec forte probabilité. Cette probabilité doit cependant rester légèrement corrélée à l'appartenance à $\mathcal{K}$, et nous allons maintenant estimer la valeur de cette corrélation. On cherche à calculer la probabilité que l'espace engendré par les lignes de la différentielle en a ait une dimension strictement plus petite que $n-1$, lorsque a est dans $\mathcal{K}$ et lorsque a n'est pas dans $\mathcal{K}$.

Commençons par le cas où a est dans $\mathcal{K}$. L'espace engendré par les lignes de $D\tilde{P}_a$ est de dimension $n-d$ avec $d = \text{pgcd}(\theta, n)$ et orthogonal à a. L'espace engendré par la lignes supplémentaires aléatoires est un espace aléatoire orthogonal à a, qui est de dimension s sauf probabilité négligeable environ $q^{-(n-s)}$. L'espace engendré par les lignes de la différentielle est la somme de ces deux sous-espaces, et a une dimension strictement inférieure à $n-1$ quand leur intersection est de dimension $i > s-d+1$. Utilisant le lemme 2 démontré à la section 2.2.6 en remplaçant n, r et s respectivement par $n-1$, $n-d$ et s, et utilisant l'approximation 2.2, la probabilité que l'intersection soit de dimension i est de l'ordre de $q^{-i(d-s-1+i)}$. L'intersection minimale étant toujours le cas le plus probable, la probabilité que la différentielle soit de rang inférieur à $n-1$ quand a est dans $\mathcal{K}$ est approximée par la probabilité ci-dessus avec $i = s-d+2$ soit environ $q^{d-1}q^{-s-1}$.

On considère maintenant le cas où a n'est pas dans $\mathcal{K}$. Dans ce cas, quand $d \leq r$, $D\tilde{P}_a$ est de rang $n-1$ ou $n-2$ avec probabilité environ $\frac{1}{q}$ pour le second cas. La différentielle PMI+ ne peut avoir un rang inférieur à $n-1$ que dans le second cas. Ainsi, utilisant le calcul précédent avec $d=2$, la probabilité que la différentielle soir de rang inférieur à $n-1$ quand a n'est pas dans $\mathcal{K}$ est $\simeq q^{-s-1}$.

Finalement, il est environ q^{d-1} fois plus probable que la différentielle ne soit pas de rang maximal quand a est dans $\mathcal{K}$ que dans le cas contraire. Un distingueur qui déciderait en faveur de l'appartenance à $\mathcal{K}$ quand le rang n'est pas maximal et le contraire sinon, aurait pour avantage environ

$$Adv = q^{d-1}q^{-s-1}$$

Basé sur ce distingueur, l'algorithme de reconstruction de $\mathcal{K}$ par linéarité de [40] a pour complexité (voir section 9.6 pour une démonstration) :

$$nq^{3r}/Adv^4 = nq^{3r+4(s-d+2)}$$

évaluations de la clé publique. Comme, pour les paramètres de PMI, nq^{3r} évaluations de la clé publique correspondent déjà à 2^{49} opérations binaires, choisir $s = d+10$ suffit à déjouer cette attaque, comme prescrit dans [21].

Conclusion : Alors que PMI est vulnérable à une attaque différentielle et MI+ vulnérable à l'attaque de Patarin [73], l'utilisation couplée des deux variations produit un système qui ne connaît pas d'attaque à ce jour.

Chapitre 5

Les schémas C^{*-}

La variation *moins* consiste à ne publier qu'une partie de la clé publique. D'abord suggérée par Shamir [77], elle est l'une des contre-mesures les plus populaires en cryptographie multivariée. Même lorsque le schéma de base est faible, appliquer le *moins* semble une défense imparable. Les variations *moins* de C^* ou schémas C^{*-} ont été proposées par Patarin-Goubin-Courtois à Asiacrypt'98 [73]. En raison des performances attractives de ces schémas, ces mêmes auteurs ont plus tard proposé deux instanciations, FLASH et SFLASH, comme candidats à la sélection de primitives cryptographiques du consortium européen NESSIE [64] organisée en 2001. Aucune faille critique n'ayant été trouvée sur ces schémas, SFLASH a été choisi, et recommandé depuis 2003 comme algorithme de signature pour les dispositifs cryptographiques aux capacités de calcul limitées.

5.1 Définition

Un schéma C^{*-} s'obtient à partir d'un schéma C^* en supprimant un certain nombre des polynômes définissant la clé publique. Plus précisément, pour un certain paramètre r, la génération de clé construit un schéma C^* puis supprime de la clé publique les r derniers polynômes. Par la suite, on notera $\boldsymbol{P}$ la clé publique C^* et on notera $\tilde{\boldsymbol{P}}$ une clé publique C^{*-} dérivée.

Pour calculer une préimage par la fonction $\tilde{\boldsymbol{P}}$ d'un élément $\tilde{y}$ de $(\mathbb{F}_q)^{n-r}$, l'utilisateur légitime doit d'abord concaténer à $\tilde{y}$ un élément arbitraire k de $(\mathbb{F}_q)^r$, puis calculer l'inverse de $(\tilde{y}, k)$ par $\boldsymbol{P}$ à l'aide de sa clé secrète. Il est donc assez peu commode d'utiliser un schéma C^{*-} pour faire du chiffrement : il faut en effet alors passer en revue toutes les valeurs possibles de k, et pour chacune inverser la fonction $\boldsymbol{P}$, pour récupérer le message clair, ce qui limite les valeurs de r. En revanche, les schémas C^{*-} peuvent fort bien être utilisés en signature, même pour de grandes valeurs de q et r, puisqu'alors l'une quelconque des q^r préimages est une signature valide. Ainsi, pour signer un message $\tilde{y}$, l'utilisateur choisit un vecteur arbitraire k de longueur r et calcule une signature comme l'inverse de $(\tilde{y}, k)$ par la fonction $\boldsymbol{P}$.

Étrangement, aucun argument théorique n'est offert dans [73] permettant de constater que l'attaque de Patarin est effectivement empêchée par la méthode *moins*. On pourrait toutefois avancer les arguments suivants, montrant que l'attaque de Patarin, même généralisée en degré supérieur, ne peut fonctionner sur les schémas C^{*-} dès que q^r est grand devant n. Comme on l'a vu, un message $\tilde{y}$ a q^r préimages par la fonction $\tilde{\boldsymbol{P}}$. En général, aucune linéarité n'est susceptible d'exister entre ces préimages, de sorte que le plus petit sous-espace contenant tous ces éléments doit être de dimension proche de q^r (quand cette quantité est inférieure à n). Quand q^r est grand devant n (ce qui est le cas, pour toutes les instanciations considérées en pratique comme nous le verrons plus tard), ce plus petit sous-espace doit être l'espace $(\mathbb{F}_q)^n$ tout entier. Ainsi, il ne peut exister d'équations bilinéaires entre $\tilde{y}$ et ses préimages, car cela impliquerait que ces préimages sont contenues dans un sous-espace strictement plus petit que $(\mathbb{F}_q)^n$. En fait, ce même argument montre qu'il ne peut pas exister non plus d'équations implicites entre $\tilde{y}$ et ses préimages qui soient linéaires sur l'ensemble des préimages. Même s'il n'est pas impossible que des équations implicites de degré plus élevé sur l'ensemble des préimages existent (pour r pas trop grand), leur intérêt est limité car pour un $\tilde{y}$ donné il nous faudrait résoudre un système non-linéaire pour trouver une préimage.

5.2 Choix de paramètres

Le paramètre q est une puissance de 2 pour qu'il existe des C^* bijectifs. Dans [73], Patarin-Goubin-Courtois décrivent une technique pouvant potentiellement permettre de reconstruire une clé publique C^* à partir d'une clé publique C^{*-} avec complexité faisant intervenir un facteur q^r. Afin d'éviter cette attaque potentielle, il est donc recommandé de choisir q^r de l'ordre de 2^{80} ; la notation illustrative C^{*--} est alors parfois utilisée quand cette condition est réalisée. Aucune condition spécifique n'apparaît dans la littérature en ce qui concerne le choix du paramètre θ, si ce n'est de définir un monôme C^* bijectif. Comme nous l'avons vu au chapitre 3, les monômes C^* bijectifs sont ceux pour lesquels θ a un pgcd d avec n tel que $\frac{n}{d}$ soit impair. Comme noté par Ding dans [20], choisir un θ avec un d assez grand permet une inversion plus rapide du monôme C^*, et peut donc être un choix attractif.

Les schémas FLASH et SFLASH sont des instanciations de schémas C^{*-} proposées par Patarin-Goubin-Courtois à la sélection NESSIE en 2001. La première version de SFLASH présentait une particularité malheureuse ouvrant la voie à une attaque présentée par Gilbert et Minier à Eurocrypt'01 [43]. Il avait été proposé de choisir les applications linéaires secrètes S et T à coefficients dans $\mathbb{F}_2$ au lieu de $\mathbb{F}_q$. Comme le monôme interne définit également une permutation de $\mathbb{F}_{2^n}$, la clé publique était alors elle-même à coefficients dans $\mathbb{F}_2$ au lieu de $\mathbb{F}_q$ et occupait $\log_2 q$ fois moins d'espace. L'objection soulevée par Gilbert et Minier était que, par ce fait même, le schéma pouvait être entièrement considéré sur $\mathbb{F}_2$ au lieu de $\mathbb{F}_q$, et qu'alors le critère de sécurité pertinent n'était plus $q^r \simeq 2^{80}$ mais bien $2^r \simeq 2^{80}$, ce qui n'était pas vérifié pour la valeur de r choisie. Une attaque alternative à celle

à l'origine de ce critère [73] est également proposée par Gilbert et Minier [43] ; cette attaque exploite la petite valeur de 2^r ainsi que celle de 2^n. Sa particularité supprimée, SFLASH devenait alors très similaire à FLASH mais de paramètres légèrement avantageux, et seul SFLASH fut plus tard considéré dans le processus d'évaluation de NESSIE, pour finalement être sélectionné en 2003. Pour des raisons mal identifiées, une troisième version de SFLASH fut proposée par la suite par Patarin-Goubin-Courtois bien que la seconde, acceptée à NESSIE, continuât d'être la version recommandée. La table ci-dessous réunit les paramètres des trois schémas explicitement proposés.

	q	n	θ	d	r	Taille Signatures	Taille Clé Publique
FLASH	2^8	29	11	1	11	296 bits	18 Ko
SFLASHv2	2^7	37	11	1	11	259 bits	15 Ko
SFLASHv3	2^7	67	33	1	11	469 bits	112 Ko

La quasi-inexistence d'attaques sur les schémas C^{*-} autorise une large gamme de paramètres qui tous peuvent prétendre à la même sécurité. La non-justification des paramètres choisis pour les propositions ci-dessus reflète bien cet état de fait. Pour autant, l'absence d'attaque ne saurait garantir la sécurité des schémas.

5.3 Vers une cryptanalyse des schémas C^{*-}

Soit $\boldsymbol{P}$ une clé publique C^* et $\tilde{\boldsymbol{P}}$ la clé publique C^{*-} qui en est dérivée en supprimant les r derniers polynômes. La fonction $\boldsymbol{P}$ est définie par une suite de polynômes $\boldsymbol{p_1}, \ldots, \boldsymbol{p_n}$ et $\tilde{\boldsymbol{P}}$ par les $n-r$ premiers de ces polynômes. Comme la fonction $\boldsymbol{P}$ est une fonction $T \circ P \circ S$ avec P un monôme C^* et S, T des bijections linéaires secrètes, les polynômes $\boldsymbol{p_1}, \ldots, \boldsymbol{p_n}$ sont des combinaisons linéaires des n polynômes $p_1, \ldots, p_n$ définissant $P \circ S$. Par ailleurs, ces combinaisons linéaires sont indépendantes puisque T est inversible. La fonction $\tilde{\boldsymbol{P}}$ est donc formée des $n-r$ premières de ces combinaisons, qui correspondent à la sous-matrice $\tilde{T}$ des $n-r$ premières lignes de T. Ainsi, quand on applique la transformation "moins" à $\boldsymbol{P}$, on ne perd pas r polynômes quadratiques indépendants, mais r combinaisons linéaires indépendantes des polynômes secrets $p_1, \ldots, p_n$. Si, par un certain procédé, on pouvait régénérer r nouvelles combinaisons linéaires de ces polynômes, formant un système de rang plein avec les lignes de $\tilde{T}$, alors cela recomposerait une clé publique C^*, éventuellement différente de la fonction initiale $\boldsymbol{P}$, mais pouvant tout autant être inversée par l'attaque de Patarin. Le point de départ d'une attaque pourrait donc être la capacité à générer de nouvelles combinaisons linéaires des polynômes secrets $p_1, \ldots, p_n$ par une certaine opération sur la clé publique $\tilde{\boldsymbol{P}}$.

Une telle opération pourrait consister en la composition par une application linéaire bien choisie : on cherche une application linéaire $\boldsymbol{M}$ telle que la composition de $\tilde{\boldsymbol{P}}$ par cette application résulte en une transformation linéaire M' sur les

polynômes coordonnées de P. Plus précisément, on cherche $\boldsymbol{M}$ et M' satisfaisant :

$$\tilde{T} \circ (P \circ S) \circ \boldsymbol{M} = \tilde{T} \circ M' \circ (P \circ S)$$

Notant M la fonction linéaire $S \circ \boldsymbol{M} \circ S^{-1}$, cela peut se récrire :

$$\tilde{T} \circ (P \circ M) \circ S = \tilde{T} \circ (M' \circ P) \circ S$$

En d'autres termes, les candidats possibles M, M' doivent satisfaire une forme de commutation avec P. Rappelons-nous la forme de P :

$$P(x) = x^{1+q^\theta}$$

Comme nous le voyons, au moins deux classes d'applications commutantes peuvent être considérées. Les Frobenius, tout d'abord, commutent avec P. Une autre classe exploite la multiplicativité de P : multiplier par α l'entrée de P revient à multiplier par $P(\alpha)$ la sortie de P :

$$P(\alpha \cdot x) = P(\alpha) \cdot P(x)$$

Notant M_α la multiplication par α, cela peut se récrire :

$$P \circ M_\alpha = M_{P(\alpha)} \circ P$$

Malheureusement, composer le monôme interne par de telles applications M ne peut être opéré que par la composition de la clé publique par leurs conjuguées $\boldsymbol{M} = S^{-1} \circ M \circ S$ qui dépendent de la clé secrète S. Dans la suite, nous cherchons des applications M dont l'action sur la différentielle du monôme C^* est spécifique et permet de déterminer leurs conjuguées de l'équation publique correspondante.

5.4 Applications antisymétriques vis-à-vis de la différentielle de C^*

La différentielle en a d'une fonction quadratique P est la fonction linéaire :

$$DP_a(x) = P(a + x) - P(x) - P(a) + P(0)$$

En réalité, cette expression étant symétrique en a et x, la différentielle est une application bilinéaire symétrique en (a, x) ; nous la noterons $DP(a, x)$.

La différentielle du monôme C^*, $P(x) = x^{1+q^\theta}$, est :

$$DP(a, x) = a.x^{q^\theta} + a^{q^\theta}.x$$

qui peut se réécrire, pour a non-nul :

$$DP(a, x) = P(a).L_\theta\left(\frac{x}{a}\right)$$

où L_θ est l'application linéaire $z \mapsto z + z^{q^\theta}$. De cette expression, nous voyons directement que, pour tout élément ξ dans le noyau de L_θ, nous avons l'identité :

$$DP(a, \xi.a) = 0$$

pour tout élément a. Autrement dit, les multiplications M_ξ associées aux éléments du noyau de L_θ, sont les solutions de l'équation linéaire :

$$DP(a, M(a)) = 0$$

Une caractérisation équivalente, mais plus élégante de ces multiplications, est obtenue en prenant la différentielle de l'application quadratique $a \mapsto DP(a, M(a))$:

$$DP(M(a), x) + DP(a, M(x)) = 0$$

de laquelle, nous voyons que ces multiplications, associées aux éléments du noyau de L_θ, sont des applications *antisymétriques* par rapport à la différentielle. Le théorème suivant assure qu'elles sont bien les seules à satisfaire cette propriété :

Théorème 1. *Soit M une application linéaire ; M est anti-symétrique par rapport à la différentielle DP d'un C^* de paramètre θ, si et seulement si M est la multiplication par un élément ξ satisfaisant $\xi^{q^\theta} + \xi = 0$.*

Démonstration. Une application linéaire M sur $\mathbb{F}_{q^n}$ est une somme de Frobenius : $M(x) = \sum_{i=0}^{n-1} \lambda_i x^{q^i}$. Quand DP est la différentielle d'un C^* de paramètre θ, l'application M est anti-symétrique par rapport à DP si et seulement si

$$\sum_{i=0}^{n-1} \lambda_i a^{q^\theta} x^{q^i} + \sum_{i=0}^{n-1} \lambda_i^{q^\theta} a\, x^{q^{i+\theta}} + \sum_{i=0}^{n-1} \lambda_i a^{q^i} x^{q^\theta} + \sum_{i=0}^{n-1} \lambda_i^{q^\theta} a^{q^{i+\theta}} x = 0$$

Les monômes $a^{q^u} x^{q^v}$ formant un base de l'espace des applications bilinéaires sur $\mathbb{F}_{q^n}$, on obtient les équations suivantes pour les divers éléments de la base

$$\begin{array}{ll} \lambda_0 + \lambda_0^{q^\theta} = 0 & (\text{coefficient of } a x^{q^\theta}) \\ \lambda_i = 0,\ i \neq 0, \theta & (\text{coefficient of } a^{q^i} x^{q^\theta},\ i \neq 0, \theta) \\ (\lambda_\theta)^{q^\theta} = 0 & (\text{coefficient of } a x^{q^{2\theta}}) \end{array}$$

Le sens réciproque a déjà été obtenu. □

Les applications linéaires antisymétriques vis-à-vis de la différentielle d'un monôme C^* de paramètre θ forment un sous-espace isomorphe au noyau de L_θ, noté $\mathcal{K}_\theta$, dont nous avons vu au chapitre 3 que la dimension est $d = \text{pgcd}(\theta, n)$. En particulier, quand $d = 1$, $\mathcal{K}_\theta$ est réduit aux multiples scalaires de l'unité, et les multiplications antisymétriques sont les multiples scalaires de l'identité. Or, de telles multiplications sont triviales car elles sont antisymétriques par rapport à tout produit bilinéaire symétrique. Par conséquent, il existe des multiplications antisymétriques non-triviales seulement quand $d > 1$.

Soit maintenant $\boldsymbol{P} = T \circ P \circ S$ une clé publique C^*. Sa différentielle est

$$D\boldsymbol{P}(a, x) = T \circ DP(S(a), S(x))$$

Comme T est inversible, les applications antisymétriques par rapport à $D\boldsymbol{P}$ sont les applications antisymétriques par rapport à $DP(S(a), S(x))$. Cette dernière application bilinéaire étant isomorphe par S à la différentielle DP d'un C^*, les applications qui lui sont-antisymétriques sont les applications

$$\boldsymbol{M}_\xi = S^{-1} \circ M_\xi \circ S$$

Bien que ces applications soient fonction d'une partie de la clé secrète, elles satisfont le système d'équations publiques

$$D\boldsymbol{P}(\boldsymbol{M}(a), x) + D\boldsymbol{P}(a, \boldsymbol{M}(x)) = 0$$

pour tout (a, x), linéaire en l'inconnue $\boldsymbol{M}$. En réalité, comme $D\boldsymbol{P}$ a n coordonnées, chaque choix de a, x dans cette équation impose n contraintes linéaires sur les coefficients de $\boldsymbol{M}$. Pour chacune des n coordonnées de $D\boldsymbol{P}$, évaluer cette équation sur une base bilinéairement indépendante de (a, x) (avec $a \neq x$ car alors l'équation est triviale) impose $n(n-1)/2$ contraintes linéaires sur les n^2 coefficients de $\boldsymbol{M}$. On voit donc que la condition d'antisymétrie est largement surdéfinie : une seule coordonnée de $D\boldsymbol{P}$ nous fournit presque autant d'équations que nous avons d'inconnues. Sauf dégénérescence imprévue des équations générées, on s'attend donc à être capable de retrouver les applications antisymétriques $\boldsymbol{M}_\xi$ même à partir d'un très petit nombre de coordonnées de la clé publique $\boldsymbol{P}$.

5.5 Cryptanalyse des C^{*-} avec $d > 1$

Une clé publique $\tilde{\boldsymbol{P}}$ d'un schéma C^{*-} est la donnée de $n - r$ coordonnées d'une clé publique C^*. Compte tenu des observations précédentes, les équations

$$D\tilde{\boldsymbol{P}}(\boldsymbol{M}(a), x) + D\tilde{\boldsymbol{P}}(a, \boldsymbol{M}(x)) = 0$$

pour des choix indépendants de a et x, forment un système de $(n-r)n(n-1)/2$ équations linéaires en les n^2 coefficients de $\boldsymbol{M}$. Ce système a au moins pour solution l'espace des $\boldsymbol{M}_\xi$ avec ξ dans $\mathcal{K}_\theta$, de dimension $d = \text{pgcd}(\theta, n)$. Si l'on suppose que toutes les équations du système sont bien indépendantes, il n'y en a pas d'autres jusqu'à r satisfaisant :

$$(n-r)\frac{n(n-1)}{2} \geq n^2 - d$$

Sous cette approximation, la valeur r_{max} de r jusqu'à laquelle les $\boldsymbol{M}_\xi$ sont les seules solutions du système correspond à

$$r^*_{max} = n - \left\lceil 2\frac{n^2 - d}{n(n-1)} \right\rceil = n - 3$$

Bien que ce raisonnement soit assez naïf, on constate expérimentalement qu'il donne une bonne approximation de la valeur réelle de r_{max} : la table ci-dessous fournit cette valeur, déterminée expérimentalement, pour quelques paramètres proches de ceux de SFLASHv2, à comparer avec la valeur heuristique $r^*_{max} = n - 3$.

n	36	36	38	39	39	40	42	42	44
θ	8	12	10	13	9	8	12	14	12
d	4	12	2	13	3	8	6	14	4
r_{max}	33	32	35	35	36	37	39	38	41
r^*_{max}	33	33	35	36	36	37	39	39	41

Comme on peut le remarquer, la valeur réelle de r_{max} diffère de la valeur heuristique (d'une unité au plus) quand d est grand. Une explication possible serait que des choix indépendants de a, x n'engendrent pas $n(n-1)/2$ équations indépendantes, mais une quantité du même ordre décroissante en d.

Alors que pour les instanciations proposées en pratique, r est beaucoup plus petit que n – environ $n/3$ pour FLASH et SFLASHv2, environ $n/6$ pour SFLASHv3 – nous voyons qu'il suffit de 3 ou 4 coordonnées de la clé publique pour restaurer l'espace des applications antisymétriques. Pour des paramètres pratiques, retrouver ces applications en résolvant leur équation caractéristique prend seulement quelques secondes sur une machine standard (AMD Opteron 2GHz). Lorsque $d > 1$, cette stratégie nous permet donc de déceler des multiplications non-triviales.

5.5.1 Reconstruire une clé publique C^*

Pour toute application $\boldsymbol{M}_\xi$ non-triviale, on considère la transformée de la clé publique $\tilde{\boldsymbol{P}} \circ \boldsymbol{M}_\xi$. On va maintenant montrer que, quand r est plus petit que $n/2$, compléter $\tilde{\boldsymbol{P}}$ par r coordonnées arbitraires de $\tilde{\boldsymbol{P}} \circ \boldsymbol{M}_\xi$ reconstruit une clé publique C^* avec forte probabilité. La technique se généralise jusqu'à $r \leq n(1 - \frac{1}{d})$ en utilisant $d - 1$ applications $\boldsymbol{M}_\xi$ non-triviales et linéairement indépendantes.

La composition de $\tilde{\boldsymbol{P}}$ par une $\boldsymbol{M}_\xi$ s'écrit

$$\tilde{\boldsymbol{P}} \circ \boldsymbol{M}_\xi = (\tilde{T} \circ P \circ S) \circ (S^{-1} \circ M_\xi \circ S) = \tilde{T} \circ P \circ M_\xi \circ S$$

Utilisant la multiplicativité de P, on obtient

$$\tilde{\boldsymbol{P}} \circ \boldsymbol{M}_\xi = \tilde{T} \circ M_{P(\xi)} \circ P \circ S$$

Quand M_ξ est non-triviale, ξ n'est pas colinéaire à 1, et puisque l'inverse de P est une exponentiation, $P(\xi)$ n'est pas non plus colinéaire à 1. Ainsi, $M_{P(\xi)}$ est non-triviale et les matrices $\tilde{T}$ et $\tilde{T} \circ M_{P(\xi)}$ sont bien distinctes.

Les $n - r$ polynômes quadratiques définissant $\tilde{\boldsymbol{P}}$ sont des combinaisons linéaires encodées par les lignes de $\tilde{T}$ des n polynômes quadratiques définissant $P \circ S$, tandis que les polynômes quadratiques définissant $\tilde{\boldsymbol{P}} \circ \boldsymbol{M}_\xi$ sont des combinaisons linéaires

encodées par les lignes $\tilde{T} \circ M_{P(\xi)}$ de ces mêmes polynômes. Ajouter r polynômes de $\tilde{\boldsymbol{P}} \circ \boldsymbol{M}_\xi$ à $\tilde{\boldsymbol{P}}$ reconstruit une clé publique C^* si et seulement si les lignes correspondantes de $\tilde{T} \circ M_{P(\xi)}$ forment avec les lignes $\tilde{T}$ un système de rang plein. Choisissons par exemple les r premières lignes de $\tilde{T} \circ M_{P(\xi)}$. Les lignes de $\tilde{T}$ engendrent un sous-espace de dimension $n - r$ de $(\mathbb{F}_q)^n$. Un vecteur aléatoire est dans un sous-espace de dimension $n - k$ de $(\mathbb{F}_q)^n$ avec probabilité q^{-k}. Donc, si on suppose que les r lignes de $\tilde{T} \circ M_{P(\xi)}$ sont des vecteurs aléatoires, la probabilité qu'elles forment avec les lignes de $\tilde{T}$ un système de rang plein est

$$\left(1 - \tfrac{1}{q^r}\right)\left(1 - \tfrac{1}{q^{r-1}}\right) \ldots \left(1 - \tfrac{1}{q}\right) \simeq 1 - \tfrac{1}{q}$$

Selon cet argument, ajouter les r premiers polynômes de $\tilde{\boldsymbol{P}} \circ \boldsymbol{M}_\xi$ à $\tilde{\boldsymbol{P}}$ recompose une clé publique C^* (non nécessairement identique à la clé publique initialement tronquée) avec probabilité environ $1 - 1/q$. Cette clé publique correspond à une clé secrète T obtenue en ajoutant aux lignes de $\tilde{T}$ les r premières lignes de $\tilde{T} \circ M_{P(\xi)}$. La clé publique recomposée peut ensuite être attaquée comme montré par Patarin [67]. Si ajouter les r premiers polynômes a échoué à recomposer une clé publique C^* complète, on réessaye avec r autres polynômes de $\tilde{\boldsymbol{P}} \circ \boldsymbol{M}_\xi$. La probabilité de succès en t essais indépendants est environ $1 - q^{-(t-1)}$.

La table ci-dessous fournit les temps de calcul (en secondes) d'une implémentation concrète de l'attaque pour plusieurs choix de paramètres proches de ceux de SFLASHv2 et avec la même valeur $q = 2^7$.

n	36	36	38	39	39	40	42	42	44
θ	8	12	10	13	9	8	12	14	12
d	4	12	2	13	3	8	6	14	4
r	11	11	11	12	12	12	13	13	13
$C^{*-} \mapsto C^*$	$57s$	$57s$	$94s$	$105s$	$90s$	$105s$	$141s$	$155s$	$155s$

La technique précédente se généralise jusqu'à $r \leq n(1 - \frac{1}{d})$ en utilisant une base $\boldsymbol{M}_{\xi_1}, \ldots, \boldsymbol{M}_{\xi_{d-1}}$ d'un supplémentaire des multiples scalaires de l'identité dans le sous-espace des multiplications antisymétriques. Nous allons alors utiliser les coordonnées des transformées de la clé publique par ces multiplications,

$$\tilde{\boldsymbol{P}} \circ \boldsymbol{M}_{\xi_1}, \ldots, \tilde{\boldsymbol{P}} \circ \boldsymbol{M}_{\xi_{d-1}}$$

pour recomposer une clé publique C^* complète. Comme le nombre total de coordonnées disponibles est $d(n-r)$, on ne pourra pas recomposer une clé publique C^* complète si r est plus grand que $n(1 - \frac{1}{d})$. Quand toutes les coordonnées sont linéairement indépendantes, on récupère une clé C^* complète jusqu'à $r = n(1 - \frac{1}{d})$. Dans la table ci-dessous, on donne des timings pour plusieurs paramètres et la plus grande valeur de r autorisant l'attaque. Cette dernière valeur est bien sûr le minimum de r_{max} – afin de pouvoir restaurer l'espace des applications antisymétriques

à partir de la différentielle – et de $n(1-\frac{1}{d})$ – afin d'avoir assez de coordonnées pour restaurer une clé publique C^* complète. Dans la table, le symbole étoile indique quand la valeur considérée correspond à r_{max}.

n	36	36	38	39	39	40	42	42	44
θ	8	12	10	13	9	8	12	14	12
d	4	12	2	13	3	8	6	14	4
$r = \min\{r_{max}, n(1-\frac{1}{d})\}$	27	32^*	19	35^*	26	35	35	38^*	33
$C^{*-} \mapsto C^*$	$65s$	$51s$	$112s$	$79s$	$107s$	$95s$	$134s$	$117s$	$202s$

5.6 Action des multiplications sur la différentielle de C^*

Pour cryptanalyser les schémas C^{*-}, notre objectif est de découvrir des multiplications. En effet, ces applications particulières réalisent une forme de commutation avec le monôme interne et peuvent être utilisées pour régénérer des coordonnées supprimées de la clé publique C^* originale. Une classe particulière de ces multiplications est constituée des applications antisymétriques par rapport à la différentielle. Ceux sont les applications linéaires M satisfaisant

$$DP(M(a), x) + DP(a, M(x)) = 0$$

Malheureusement, de telles applications sont toujours triviales lorsque $d = 1$, comme c'est notamment le cas pour les instanciations FLASH, SFLASHv2 et SFLASHv3. Notre but à présent est de trouver d'autres propriétés dont les solutions sont des multiplications non-triviales.

Une généralisation de la propriété ci-dessus s'obtient en évaluant le membre de gauche en une multiplication arbitraire M_ξ. Formant

$$DP(M_\xi(a), x) + DP(a, M_\xi(x)) = \xi^{q^\theta} a^{q^\theta} x + \xi a x^{q^\theta} + \xi a^{q^\theta} x + \xi^{q^\theta} a x^{q^\theta}$$

on reconnaît en le second membre le produit $(\xi + \xi^{q^\theta}).DP(a, x)$, et notant $L_\theta(\xi)$ le terme multiplicatif, on obtient :

$$DP(M_\xi(a), x) + DP(a, M_\xi(x)) = M_{L_\theta(\xi)} \circ DP(a, x) \tag{5.1}$$

On note que $L_\theta(\xi)$ est linéaire en ξ et que les éléments de son noyau correspondent précisément aux applications antisymétriques par rapport à la différentielle DP du monôme C^*. Pour tous les autres ξ, l'identité (5.1) n'en est pas moins remarquable. Elle induit la propriété que chaque coordonnée de la fonction bilinéaire $DP(M(a), x) + DP(a, M(x))$ est une combinaison linéaire des coordonnées de DP lorsque M est une multiplication. Or, lorsque M est une application linéaire aléatoire, chaque coordonnée de $DP(M(a), x) + DP(a, M(x))$

– assimilée à une forme bilinéaire symétrique aléatoire – est dans l'espace de dimension n engendré par les formes coordonnées de DP avec probabilité environ q^{-k} où $k = n(n-1)/2 - n$, et il est alors hautement improbable que même trois des coordonnées de $DP(M(a), x) + DP(a, M(x))$ soient dans cet espace. Il s'agit donc là d'une propriété très spécifique aux multiplications.

Dans la suite, on cherche à exploiter cette propriété pour développer une autre cryptanalyse des schémas C^{*-} qui soit également valable lorsque $d = 1$. Bien que le cas $d > 1$ ait déjà été traité, on garde d quelconque afin d'observer quelle est l'influence de ce paramètre dans cette seconde approche.

5.7 Cryptanalyse des C^{*-} avec d quelconque

Il est clair que l'identité (5.1) précédente induit une identité similaire sur la clé publique C^*. Considérant $\boldsymbol{P} = T \circ P \circ S$, on obtient

$$D\boldsymbol{P}(\boldsymbol{M}_\xi(a), x) + D\boldsymbol{P}(a, \boldsymbol{M}_\xi(x)) = \boldsymbol{N}_{L_\theta(\xi)} \circ D\boldsymbol{P}(a, x) \tag{5.2}$$

où $\boldsymbol{M_\xi}$ et $\boldsymbol{N}_{L_\theta(\xi)}$ sont conjuguées de M_ξ et $M_{L_\theta(\xi)}$ respectivement par S et T :

$$\boldsymbol{M}_\xi = S^{-1} \circ M_\xi \circ S \qquad \text{et} \qquad \boldsymbol{N}_{L_\theta(\xi)} = T \circ M_{L_\theta(\xi)} \circ T^{-1}$$

Introduisant la notation

$$\boldsymbol{\Sigma}[\boldsymbol{M}](a, x) = D\boldsymbol{P}(\boldsymbol{M}(a), x) + D\boldsymbol{P}(a, \boldsymbol{M}(x))$$

une conséquence de l'identité (5.2) est que pour tout ξ chaque coordonnée de $\boldsymbol{\Sigma}[\boldsymbol{M}_\xi]$ est dans l'espace engendré par les coordonnées de $D\boldsymbol{P}$, noté V.

Voyons maintenant ce qui arrive lorsque seulement les $n-r$ premières coordonnées de $\boldsymbol{P}$ sont données. Alors, chacune des $n-r$ premières coordonnées de $\boldsymbol{\Sigma}[\boldsymbol{M}_\xi]$ est encore effectivement dans l'espace V engendré par $D\boldsymbol{P}$, mais cet espace est à présent seulement partiellement connu : on ne connaît que le sous-espace engendré par les $n-r$ premières coordonnées, noté $\tilde{\boldsymbol{V}}$. Néanmoins, un vecteur aléatoire de V se trouve dans $\tilde{\boldsymbol{V}}$ avec probabilité q^{-r}, et parmi les q^n multiplications disponibles, on peut donc s'attendre à ce qu'une coordonnée fixée de $\boldsymbol{\Sigma}$ soit dans ce sous-espace pour environ q^{n-r} d'entre elles. Considérant k coordonnées fixées de $\boldsymbol{\Sigma}$ au lieu d'une seule, on s'attend à ce qu'il existe environ q^{n-kr} multiplications pour lesquelles ces mêmes coordonnées sont dans $\tilde{\boldsymbol{V}}$. Si cette condition est assez contraignante pour ne pas admettre d'autres solutions, alors on va ainsi découvrir un sous-espace de multiplications. On décrit maintenant les détails de l'attaque.

Dimension de l'espace des solutions : On considère k coordonnées de $\boldsymbol{\Sigma}[\boldsymbol{M}]$, par exemple les k premières. Pour chacune de ces coordonnées, la condition d'appartenir au sous-espace $\tilde{\boldsymbol{V}}$ (de dimension $n-r$) s'exprime comme l'annulation de $n(n-1)/2 - (n-r)$ formes linéaires. Les applications $\boldsymbol{M}$ pour lesquelles les k premières coordonnées de $\boldsymbol{\Sigma}[\boldsymbol{M}]$ sont dans $\tilde{\boldsymbol{V}}$ sont donc les solutions d'un système

de $k(n(n-1)/2-(n-r))$ équations linéaires en les n^2 coefficients inconnus de $\boldsymbol{M}$. Quand ces équations sont linéairement indépendantes, l'espace des solutions, noté $E(1,\ldots,k)$, est donc de dimension $n^2-k(n(n-1)/2-(n-r))$. Cet espace contient un sous-espace de multiplications, dont on calcule maintenant la dimension.

Dimension des solutions multiplicatives : L'application $N_i(\eta)$ qui à tout η associe la coordonnée i de $\boldsymbol{N}_\eta = T \circ M_\eta \circ T^{-1}$ est linéaire de $\mathbb{F}_{q^n}$ dans $(\mathbb{F}_q)^n$. Les éléments de son noyau sont les η pour lesquels la i-ème ligne de $\boldsymbol{N}_\eta$ est nulle. Or, $\boldsymbol{N}_\eta$ étant toujours inversible pour η non-nul, il ne peut donc s'agir que de 0, ce qui montre que l'application $N_i(\eta)$ est bijective. Par suite, pour chaque coordonnée i, l'application qui à tout η associe la i-ème ligne de $\boldsymbol{N}_\eta \circ D\boldsymbol{P}(a,x)$ est une bijection linéaire de $\mathbb{F}_{q^n}$ dans V. L'image réciproque de $\tilde{\boldsymbol{V}}$ par la i-ème ligne de $\boldsymbol{N}_\eta \circ D\boldsymbol{P}(a,x)$ est un sous-espace de même dimension noté F_i. L'ensemble des éléments η pour lesquels les k premières coordonnées de $\boldsymbol{N}_\eta \circ D\boldsymbol{P}(a,x)$ sont dans $\tilde{\boldsymbol{V}}$ est donc l'espace intersection des $F_1,\ldots,F_k$. Les sous-espaces $F_1,\ldots,F_k$ étant tous de dimension $n-r$, leur intersection est au minimum de dimension $n-kr$; de plus, assimilant ces sous-espaces à des sous-espaces aléatoires de même dimension, leur intersection est de dimension minimale $n-kr$ avec forte probabilité. Parmi les éléments η de cette intersection, ceux qui correspondent à des valeurs-images de L_θ sont un sous-espace qui a dimension $n-kr-d$ avec forte probabilité. L'image réciproque par L_θ de ce sous-espace est de dimension $d+n-kr-d$ lorsque $n-kr-d>0$ et de dimension d sinon, ne contenant alors que les éléments du noyau de L_θ. Les applications $\boldsymbol{M}_\xi$ pour lesquelles les k premières coordonnées de $\boldsymbol{\Sigma}[\boldsymbol{M}_\xi]$ sont dans $\tilde{\boldsymbol{V}}$ forment un espace isomorphe $E_\xi(1,\ldots,k)$ de dimension $n-kr$ lorsque $n-kr-d>0$ et de dimension d sinon, ne contenant alors que les multiplications antisymétriques.

Dimension finale de l'espace des solutions : Finalement, sauf dégénérescence imprévue, le dimension de l'espace-solution $E(1,\ldots,k)$, contenant le sous-espace de multiplications $E_\xi(1,\ldots,k)$ qui lui-même contient le sous-espace des multiplications antisymétriques de dimension d, est estimée à :

$$\dim\, E(1,\ldots,k) = \max\{\, n^2 - k(n(n-1)/2-(n-r))\,,\, n-kr\,,\, d\,\}$$

Trouver des multiplications non-triviales pour $r \leq (n-2)/3$: On observe que le premier terme est négatif pour $k=3$, pour tout r et les valeurs pratiques de n. On en déduit que $E(1,\ldots,3)$ se réduit très probablement au sous-espace $E_\xi(1,\ldots,3)$. Les solutions sont alors toutes des multiplications, dont certaines sont non-triviales quand la dimension de $E_\xi(1,\ldots,3)$ est strictement supérieure à 1. Cette dernière condition est toujours vérifiée pour $d>1$. Elle n'est vérifiée quand $d=1$ que pour r satisfaisant $n-3r>1$. L'attaque présentée ici est donc une extension de celle décrite en 5.5, permettant d'attaquer aussi le cas $d=1$ pour des valeurs de $r \leq (n-2)/3$. On montre à la section suivante qu'elle peut être étendue à des valeurs de r allant jusqu'à environ $n/2$, en procédant à des raffinements sur les espaces-solutions obtenus pour plusieurs paires de coordonnées.

5.7.1 Extension de l'attaque par distillation de sous-espaces

Dans cette section, nous proposons une extension de l'attaque permettant de trouver des multiplications non-triviales jusqu'à

$$r \leq (n-3)/2$$

Le paramètre d est maintenant toujours considéré égal à 1. La technique qui suit vise à construire à partir d'espaces-solutions associés à une ou deux coordonnées, et par le jeu de sommes et intersections, d'autres sous-espaces dont la concentration en multiplications est croissante jusqu'à ne contenir que de tels éléments. On applique d'abord cette idée à des espaces-solutions associés à deux coordonnées, puis associés à une seule coordonnée.

Pour toute paire de coordonnées (i, j), la dimension attendue de l'espace des solutions $E(i, j)$ est selon la formule précédente $3n - 2r$. Il contient un sous-espace de multiplications $E_\xi(i, j)$ qui, s'il n'est pas trivial, est de dimension $n - 2r$; ce sous-espace est toujours trivial si $n - 2r \leq 1$, et nous nous plaçons donc sous la condition $2r + 1 \leq n - 1$. On définit $\delta = n - 2r - 1$, qui est la dimension de multiplications non-triviales dans un sous-espace $E_\xi(i, j)$, et vaut toujours au moins 1 sous la condition précédente. En outre, la dimension de non-multiplications dans un espace-solution $E(i, j)$ est $(3n - 2r) - (n - 2r) = 2n$. Considérons la somme Σ_l de l espaces solutions $E_1, \ldots, E_l$ associés à plusieurs paires de coordonnées. Quand Σ_l n'est pas tout l'espace, il est de dimension $l(2n) + l.\delta + 1$, car les intersections deux à deux des E_i ne contiennent que les multiplications triviales avec forte probabilité. Σ_l contient un sous-espace de multiplications qui, s'il n'est l'espace des multiplications tout entier, est de dimension $l.\delta + 1$. Soit λ la première valeur de l pour laquelle Σ_l contient tout l'espace des multiplications : $\lambda\delta \geq n - 1 > (\lambda - 1)\delta$. L'intersection I de Σ_λ avec un $(\lambda + 1)$-ième espace-solution E contient toutes les multiplications de E et, on l'espère, moins de non-multiplications que E. Plus exactement, I ne contient que les multiplications de E si $\lambda(2n) + 2n + n \leq n^2$, soit $2\lambda + 3 \leq n$, et en contient moins que E dès que $\lambda(2n) + n < n^2$, soit $2\lambda + 1 < n$. Si la première condition est vérifiée, on va directement restaurer un sous-espace non-trivial de multiplications. Si seule la seconde condition est vérifiée, alors il faudra itérer le procédé sur une famille de sous-espaces ainsi construits ; la dimension de ces espaces décroissant et leur dimension de multiplications restant constante, on est assuré que le procédé va ainsi converger vers l'obtention d'un sous-espace non-trivial de multiplications. Utilisant les inégalités précédentes, la première valeur de δ pour laquelle le procédé de distillation décrit fonctionne est 3. La valeur de λ est alors $\lceil (n-1)/3 \rceil$ et il n'est pas nécessaire d'itérer. La plus grande valeur de r pouvant être ainsi attaquée est donc la dernière vérifiant $r \leq (n-4)/2$.

Une variante de cette technique de distillation consiste à chercher la première valeur λ' pour laquelle l'intersection de $\Sigma_{\lambda'}$ et E contient un sous-espace non-trivial ; c'est donc la première valeur satisfaisant $(\lambda' + 1)\delta \geq n$. Sans le détail des calculs, on obtient alors directement un sous-espace de multiplications si $2(\lambda' + 1) \leq n - 1$, et un sous-espace contenant moins de non-multiplications que E si $2(\lambda' + 1) < n + 1$.

La première valeur de δ pour laquelle ce second procédé de distillation fonctionne est 2. La valeur de λ' est alors $\lfloor n/2 \rfloor - 1$; le sous-espace obtenu contient encore des non-multiplications mais en codimension moindre que E. La plus grande valeur de r pouvant être ainsi attaquée est donc la dernière vérifiant $r \leq (n-3)/2$.

La technique de distillation ne peut s'appliquer pour des espaces solutions $E(i)$ associés à une seule coordonnée, car la somme de deux tels sous-espaces engendrent toujours l'espace tout entier. De plus, le surplus de dimension (égal à $2n$) est trop grand pour pouvoir envisager de tronquer arbitrairement ces deux sous-espaces : il ne resterait alors plus de multiplications dans leurs troncatures.

5.7.2 Reconstruire une clé publique C^*

Une fois déterminé des multiplications non-triviales, nous pouvons restaurer une clé publique C^* exactement tel que décrit à la section 5.5.1. La présente attaque ne permettant de découvrir des multiplications non-triviales que pour $r \leq n/2$, une seule multiplication non-triviale est suffisante pour restaurer une clé publique C^* complète. La table ci-dessous donne les temps de calcul de l'attaque pour plusieurs paramètres sur un AMD Opteron 2GHz ; les valeurs en gras correspondent aux paramètres de FLASH, SFLASHv2 et SFLASHv3. Le symbole † indique quand la technique de distillation de sous-espaces est utilisée.

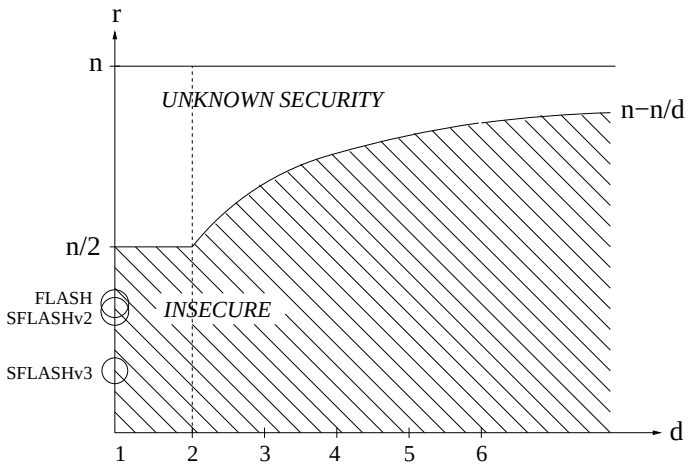
n	29	29	**29**	37	37	**37**	67	67	**67**
θ	11	11	**11**	11	11	**11**	33	33	**33**
q	2	2	$\mathbf{2^8}$	2	2	$\mathbf{2^7}$	2	2	$\mathbf{2^7}$
r	$11^\dagger$	$13^\dagger$	$\mathbf{11}^\dagger$	11	$17^\dagger$	**11**	11	$32^\dagger$	**11**
$C^{*-} \mapsto C^*$	$6s$	$8s$	$\mathbf{183}\boldsymbol{s}$	$7s$	$19s$	$\mathbf{92}\boldsymbol{s}$	$141s$	$742s$	$\mathbf{1}\boldsymbol{h}$

5.8 Conclusion et perspectives

La variation *moins* est une modification générique couramment appliquée aux schémas multivariés, consistant à supprimer un certain nombre des polynômes de la clé publique. Cette variation permet en effet souvent de contrer les attaques existantes sur les schémas de base. Pour autant, la sécurité présumée du *moins* tient surtout au fait que l'on ne sait pas l'attaquer. Cet absence d'attaque a progressivement instauré une certaine confiance comme en témoigne la sélection de SFLASH, une variation *moins* de C^*, par le consortium européen NESSIE, et l'usage récurrent de cette variation sur divers schémas multivariés.

Dans ce chapitre, nous avons proposé une nouvelle stratégie pour attaquer le *moins* visant à reconstruire les polynômes supprimés en composant la clé publique par certaines applications linéaires associées à des invariants algébriques de la fonction interne. La découverte préalable de ces applications particulières à partir de la

clé publique tronquée reste évidemment le problème principal. Dans le cas des schémas C^{*-}, nous avons montré que certaines de ces applications linéaires pouvaient être détectées par leurs propriétés vis-à-vis de la différentielle. Une première classe de telles applications existent pour tous les schémas C^{*-} pour lesquels le pgcd d des paramètres n et θ est plus grand que 1 ; ces applications satisfont une propriété différentielle massivement surdéfinie permettant de les calculer même lorsque le système est très fortement tronqué. La reconstruction d'une clé publique C^* complète sur ces schémas peut alors être réalisée à partir de seulement n/d polynômes de la clé publique. Dans le cas des schémas C^{*-} pour lesquels $d = 1$, un invariant plus général est considéré, mais seule une proportion des applications particulières qui lui sont associées peut être détectée à partir de la différentielle de la clé publique tronquée. Cette proportion peut être estimée par des arguments combinatoires en fonction des paramètres et contient des éléments non-triviaux tant qu'environ la moitié des polynômes de la clé publique sont connus. L'un quelconque de ces éléments non-triviaux permet la reconstruction d'une clé complète. La portée des deux attaques est résumée par la figure suivante, sur laquelle r désigne le nombre de polynômes supprimés.



Sur cette figure, les paramètres correspondants aux propositions FLASH, SFLASHv2 et SFLASHv3 sont marqués par des cercles ($d = 1$ pour ces trois schémas).

Des améliorations ou variantes de ces attaques pourraient considérer d'autres invariants de la fonction interne comme par exemple celui associé aux Frobenius, qui sont également des applications commutant avec le monôme central. Une autre approche en cours d'étude consiste en une exploitation différente des applications linéaires particulières décelées visant à extraire de l'information sur la clé secrète. Plus précisément, les applications satisfaisant les propriétés différentielles cherchées vis-à-vis de la clé publique sont associées par la clé secrète à celles réalisant cette propriété vis-à-vis de la fonction interne. Par exemple, les applications antisymétriques vis-à-vis de la fonction interne forment un petit groupe de multiplica-

tions M_ξ et les applications antisymétriques vis-à-vis de la clé publique sont :

$$\boldsymbol{M}_\xi = S^{-1} \circ M_\xi \circ S$$

Lorsque $\boldsymbol{M}_\xi$ et M_ξ sont connus, les applications S possibles sont les solutions inversibles de l'équation linéaire :

$$S \circ \boldsymbol{M}_\xi = M_\xi \circ S$$

Il peut cependant arriver que cette équation possède un nombre négligeable de solutions inversibles. Lorsque $\boldsymbol{M}_\xi$ et M_ξ sont effectivement associés, il existe au moins une telle solution S et les autres solutions S' satisfont :

$$(S' \circ S^{-1}) \circ M_\xi = M_\xi \circ (S' \circ S^{-1})$$

Il existe donc autant de solutions que d'applications linéaires qui commutent avec la multiplication par ξ. Ces dernières peuvent être dénombrées en considérant les contraintes résultantes sur les coefficients de leur expression en tant que polynôme sur $\mathbb{F}_{q^n}$. On peut vérifier en particulier que le nombre des telles applications linéaires est grand lorsque l'ordre de ξ est divisible par $q-1$, comme c'est le cas pour les éléments du groupe antisymétrique vis-à-vis de la différentielle. En revanche, l'équation doit admettre une solution inversible unique lorsque ξ est d'ordre premier avec $q-1$, comme c'est le cas avec une certaine probabilité pour un élément aléatoire non nul de $\mathbb{F}_{q^n}$.

Au-delà des schémas C^{*-}, les résultats présentés dans ce chapitre ont une incidence probable sur la sécurité d'autres schémas basés sur C^*. En particulier, il serait intéressant d'étudier l'influence sur ces attaques de l'usage supplémentaire de variation *plus* comme suggéré dans [73]. Si ceci ne devait pas gêner l'existence des propriétés considérées, certaines extensions pourraient sans doute s'appliquer aux schémas PMI et PMI+ qui apparaissent comme des cas particuliers de ces précédents schémas. Enfin, au delà même des schémas basés sur C^*, l'approche développée dans ce chapitre consiste en une exploitation de la structure différentielle différente de celle que nous considérions jusqu'alors, basée sur l'étude d'invariants fonctionnels de la différentielle. Les perspectives offertes par une telle approche sont vastes, et son application à HFE est particulièrement intéressante.

Troisième partie

HFE et Variations

Chapitre 6

Introduction à HFE

HFE (*Hidden Field Equation*) est une généralisation de C^* proposée par Patarin à Eurocrypt'96 [69]. Si les particularités indésirables de ce dernier schéma semblent ainsi évitées, les opérations nécessaires au déchiffrement sont aussi plus complexes et font de HFE un schéma moins attractif sur le plan des performances. Cet inconvénient est compensé par un potentiel jugé prometteur à fournir la base d'un système sûr qui dans son évaluation actuelle, permet d'envisager des choix de paramètres autorisant des tailles de bloc ou de signature d'une centaine de bits. Par la suite, plusieurs variations ont été proposées pour renforcer la sécurité du système, pouvant potentiellement autoriser un déchiffrement plus efficace en compensation.

6.1 Description de HFE

Dans la suite, nous appellerons *polynômes $\mathbb{F}_q$-linéaires* les polynômes sur $\mathbb{F}_{q^n}$ s'écrivant sur la base des monômes x^{q^i}, et *$\mathbb{F}_q$-quadratiques* ceux s'écrivant sur la base des monômes $x^{q^i+q^j}$. En particulier, les monômes C^* sont des polynômes $\mathbb{F}_q$-quadratiques. Ces dénominations proviennent du fait que les premiers se transposent, par un isomorphisme de $\mathbb{F}_{q^n}$ vers $(\mathbb{F}_q)^n$, en applications linéaires de $(\mathbb{F}_q)^n$ dans lui-même, et les seconds en applications quadratiques de $(\mathbb{F}_q)^n$ dans lui-même, définies par n polynômes de degré 2 en n variables sur $\mathbb{F}_q$.

Dans HFE, la fonction interne est un polynôme $\mathbb{F}_q$-quadratique de petit degré :

$$P(x) = \sum_{i=0}^{D} \sum_{j=0}^{D} p_{ij}\, x^{q^i+q^j}$$

où D est le premier entier tel que q^{D+1} majore strictement le degré. Cette contrainte sur le degré rend possible le calcul des préimages par P de toute valeur y par la recherche des racines de $P(x) - y$, qui peut être effectuée efficacement lorsque D est petit, en temps polynomial quand q^{D+1} est polynomial en n, en utilisant les algorithmes classiques [57, 78]. Pour construire un schéma HFE, l'algorithme de génération de clés choisit aléatoirement un polynôme P de la forme spécifiée ainsi

que deux bijections linéaires S et T, puis transforme le polynôme P en une fonction quadratique de $(\mathbb{F}_q)^n$ dans lui-même via un isomorphisme de $\mathbb{F}_{q^n}$ vers $(\mathbb{F}_q)^n$, et forme la composition :

$$\boldsymbol{P} = T \circ P \circ S$$

La clé publique consiste en la fonction $\boldsymbol{P}$ et la clé secrète en les fonctions T, P et S. HFE peut être utilisé en chiffrement et en signature mais, la fonction interne n'étant pas une permutation en général, certains aménagements doivent être apportés dans l'un et l'autre cas.

En chiffrement : on pallie à la non-injectivité de P par l'ajout de redondance interne au message. Comme P est de degré borné par q^{D+1}, chaque valeur image correspond à au plus q^{D+1} préimages par P. Il est donc nécessaire d'ajouter $(\log_2 q)(D+1)$ bits de redondance pour pouvoir identifier le message original. Une solution alternative consiste à compléter la fonction interne P par un petit nombre de polynômes quadratiques aléatoires comme redondance externe, ce qui a pour effet de rendre la clé publique presque partout injective, au prix d'une clé publique légèrement plus grosse. Cette modification est connue sous le nom de variation *plus* et a déjà été rencontrée au chapitre 4.

En signature : on pallie à la non-surjectivité de P par l'ajout de degrés de liberté dans l'espace des messages à signer. Comme les valeurs image de P admettent au plus q^{D+1} préimages, l'ensemble image de P couvre une proportion au moins q^{-D-1} de l'espace d'arrivée et en pratique une proportion beaucoup plus large. Ainsi, ajouter aux messages à signer $(\log_2 q)(D+1)$ degrés de liberté doit permettre en pratique de trouver des coordonnées supplémentaires adéquates pour lesquelles le message à signer est dans l'espace image de $\boldsymbol{P}$. Plusieurs réalisations de cette idée sont proposées dans [69]. La plus simple consiste à supprimer de l'ordre de $D+1$ polynômes de la clé publique afin de laisser libre le choix des coordonnées correspondantes ; cette modification, connue sous le nom de variation *moins*, a déjà été rencontré au chapitre 5. Une autre possibilité est offerte par la variation *vinaigre* de HFE [53], dont un avantage potentiel est de permettre une génération de signature plus rapide à niveau de sécurité égal.

6.2 Instances HFE proposées en pratique

On rapporte ici les tailles de paramètres proposées dans la littérature ainsi que les variations principales envisagées pour utiliser HFE en pratique.

Les challenges HFE : En 1998, Patarin a proposé deux challenges HFE avec une récompense de 500$ pour chacun. Ces challenges sont décrits dans la version étendue de son article d'Eurocrypt [69]. Les paramètres de ces deux challenges sont donnés dans la table ci-dessous. Le premier challenge est un HFE standard mettant

en jeu des paramètres q et n minimaux. Pour ces paramètres, le déchiffrement (ou la génération de signature) prend environ une seconde sur un PC à 500MHz. Le second challenge est une variation *moins* de HFE, ou HFE$^-$, dans lequel $r = 4$ polynômes ont été supprimés de la clé publique. En outre, cette instance est prise sur $\mathbb{F}_{16}$ plutôt que $\mathbb{F}_2$; prendre un corps de base plus gros permet de diminuer la taille de la clé publique à taille de bloc constante.

TAB. 6.1 – Paramètres d'instances pratiques de HFE

	q	n	D	r	v	Taille Signature	Taille Clé Publique
HFE Challenge 1	2	80	6	*	*	80 bits	32 Ko
HFE Challenge 2	2^4	36	3	4	*	144 bits	11 Ko
HFEv	2	77	5	*	3	80 bits	32 Ko
HFEv$^-$ (Quartz)	2	103	7	7	4	128 bits	71 Ko
IPHFE	2	89	3	*	2	89 bits	50 Ko

HFE avec Vinaigre : La variation *vinaigre* de HFE, couramment notée HFEv, a été introduite par Kipnis, Patarin et Goubin à Eurocrypt'99 [53]. Informellement, la variation *vinaigre* consiste à entrelacer un système HFE avec un système aléatoire à v nouvelles variables. Cette hybridation est supposée rendre le système plus sûr, sans diminution des performance lorsque le schéma est utilisé en signature. HFEv constitue donc une possibilité de rendre HFE plus performant en autorisant des valeurs de D plus faibles à sécurité présumée comparable. Des paramètres pour HFEv sont proposés dans [53] et donnés dans la table ci-dessus.

Les variations *moins* et *vinaigre* peuvent aussi être utilisées conjointement ; le schéma résultant est couramment noté HFEv$^-$. Un tel schéma, appelé QUARTZ, a été proposé par Patarin, Goubin et Courtois à NESSIE et est recommandé pour des signatures courtes sur PC. La génération de signatures nécessite environ 10 secondes sur un PC à 500 MHz pour les paramètres donnés dans la table. Un autre schéma générant des signatures très courtes est le McEliece-signature proposé par Courtois, Finiasz et Sendrier [18]. Ce dernier schéma offre des performances comparables à QUARTZ mais sa clé publique est de taille environ 15 fois supérieure, faisant plus d'un Mo. À titre de comparaison : signer avec RSA est environ 1000 fois plus rapide qu'avec QUARTZ pour des signatures 10 fois plus longues ; signer avec ECDSA est aussi 1000 fois plus rapide pour des signatures 3 fois plus longues.

HFE avec Perturbation Interne : Une nouvelle variation d'HFE, dite par *perturbation interne* et appelée IPHFE, a été proposée par Ding et Schmidt à PKC'06 [23]. La modification suggérée se veut une amélioration d'HFEv dans laquelle les variables de vinaigre ne sont plus libres mais dépendent des variables internes du HFE par une fonction gardée secrète. Cette idée rend le système po-

tentiellement plus sûr, mais elle induit un surcoût à la fois en chiffrement et en signature, ce qui n'était justement pas l'inconvénient d'HFEv dont les performances en signature sont identiques à celles de HFE. Pour IPHFE, diminuer le paramètre D de degré du HFE n'est alors plus seulement une possibilité mais une nécessité imposée par des contraintes de performances.

6.3 Résultats connus et problèmes ouverts

Le principal résultat connu concernant la sécurité de HFE est sa relative vulnérabilité aux attaques de déchiffrement par les bases de Gröbner. Les algorithmes de calcul de bases de Gröbner sont des algorithmes généraux pour la résolution des systèmes polynomiaux. La portée pratique de ces algorithmes, traditionnellement très limitée, s'est récemment étendue grâce aux innovations dues notamment à Faugère et dont l'algorithme F5, publié en 2001, est le résultat [35, 36]. La complexité de cet algorithme reste toutefois exponentielle en temps et mémoire et n'est pratique pour des systèmes quadratiques sur $\mathbb{F}_2$ que pour une vingtaine d'équations et variables environ. Faugère a donc suscité un certain étonnement après qu'il a annoncé en 2002 avoir cassé le premier challenge HFE, un système quadratique sur $\mathbb{F}_2$ de 80 équations et 80 variables, par calcul d'une base de Gröbner avec F5 [50]. À l'origine de ce résultat, il est constaté expérimentalement que le degré des recombinaisons algébriques nécessaire au calcul d'une base de Gröbner est bien inférieur dans le cas d'un système HFE à celui génériquement requis pour des systèmes de mêmes dimensions. Plus précisément, il est constaté que ce degré est fonction du paramètre D et non du paramètre n comme pour le cas générique. Les origines structurelles de ce phénomène ont plus tard été mises en évidence par Faugère et Joux [32], grâce à un changement de représentation du problème laissant paraître la spécificité des systèmes HFE. Toutefois, si ce changement de représentation offre une base privilégiée à la détermination combinatoire du degré de recombinaisons nécessaire, ce calcul en lui-même n'est pas résolu, et on ne sait pas déterminer la valeur de ce degré en fonction des paramètres. Cette valeur est cependant cruciale pour évaluer la portée de l'attaque, car la complexité de l'algorithme au degré d est en $n^{\mathcal{O}(d)}$ à la fois en temps et en mémoire. La valeur du paramètre cherché a été déterminée expérimentalement par Faugère pour certains paramètres sur $\mathbb{F}_2$ [51], mais l'implantation de l'attaque n'est pas disponible et le cas des systèmes définis sur des corps plus gros reste non résolu. Les limites rencontrées ici rendent également difficile l'évaluation de l'influence des variations sur cette attaque.

L'unique résultat obtenu concernant la sécurité de HFE laisse donc de multiples questions en suspens. Paradoxalement, bien que certains paramètres puissent être cassés comme montré par Faugère [51], on ne sait pas différencier un système HFE d'un système aléatoire autrement qu'en constatant, au bout du compte, la possibilité d'en calculer une base de Gröbner, en une complexité indéterminée. Un autre aspect intéressant concerne la possibilité de supprimer les variations. Nous avons

vu lors de la partie II des attaques permettant de supprimer les variations *perturbation interne* et *moins* d'une clé publique C^* ; la possibilité de faire de même dans le cas de HFE est une question déterminante pour l'intérêt de ces variations.

6.4 Résultats et organisation de cette partie

Au chapitre 7, nous montrerons qu'il est possible de reconnaître un système HFE d'un système quadratique aléatoire en temps quasipolynomial. Ce distingueur se base sur des propriétés différentielles de HFE et sa complexité est prouvée au moyen de dénombrements dans les espaces vectoriels, qui ont été introduits au chapitre 2. Nous proposons ensuite, au chapitre 8, une synthèse des différentes approches de cryptanalyse ayant été proposées contre HFE ainsi que leurs résultats. Enfin, au chapitre 9, nous présentons une cryptanalyse de la variation par *perturbation interne* de HFE, proposée par Ding et Schmidt à PKC 2005 [23]. Cette attaque permet de supprimer la perturbation interne de la clé publique et repose sur une analyse précise de la distribution différentielle du schéma au moyen (à nouveau) de dénombrements dans les espaces vectoriels.

Chapitre 7

Algorithme de reconnaissance des clés publiques HFE

The system should possess no apparent features.
In a sense, the system should be a nearly random one.

T.Matsumoto, H.Imai [59]

Dans ce chapitre, nous nous intéressons à la difficulté de distinguer des clés publiques HFE de systèmes quadratiques aléatoires. Bien que ne constituant pas une attaque à proprement parler, la question est fondamentale en ce qu'elle invalide l'argument de sécurité classique fondé sur la difficulté générique de la résolution des systèmes quadratiques. Par ailleurs, aucune des approches précédentes de Kipnis et Shamir [55], Courtois [17], et enfin Faugère et Joux [51, 32] n'est parvenue à donner une réponse théorique à cette question, et seule la dernière donne une réponse pratique sans toutefois pouvoir fournir de complexité asymptotique. Dans ce chapitre, nous montrons une propriété différentielle élémentaire de HFE à partir de laquelle on construit un algorithme qui distingue un système HFE d'un système quadratique aléatoire en temps quasipolynomial.

7.1 Une propriété différentielle élémentaire de HFE

Rappelons que pour toute fonction quadratique P de $(\mathbb{F}_q)^n$ dans lui-même, et tout élément a de $(\mathbb{F}_q)^n$, la différentielle de P en a, notée DP_a, est une application linéaire de $(\mathbb{F}_q)$ dans lui-même définie par :

$$DP_a(x) = P(a+x) - P(x) - P(a) + P(0)$$

Dans un schéma multivarié, la fonction quadratique $\boldsymbol{P}$ définissant la clé publique est transformée d'une fonction quadratique P par deux bijections linéaires S et T :

$\boldsymbol{P} = T \circ P \circ S$. Les différentielles se correspondent de la façon suivante :

$$D\boldsymbol{P}_a = T \circ DP_{S(a)} \circ S$$

Il en résulte que les propriétés invariantes par bijections linéaires de la différentielle de la fonction interne vont se transmettre à la différentielle de la clé publique. En particulier, la dimension des noyaux de $D\boldsymbol{P}_a$ et $DP_{S(a)}$ sont les mêmes.

Dans la suite, nous montrons que la dimension du noyau de la différentielle de HFE est bornée supérieurement, alors qu'elle peut prendre des valeurs arbitrairement grandes pour une fonction quadratique aléatoire. Dans toute la suite, q est une puissance de 2.

7.1.1 Dimension du noyau de la différentielle pour une fonction quadratique aléatoire

Pour une fonction quadratique aléatoire, la dimension du noyau de la différentielle en un élément non-nul suit une loi donnée par la théorème suivant.

Théorème 2. *Soit q une puissance de 2, et a un élément de $\mathbb{F}_{q^n}$. La différentielle en a d'une fonction quadratique aléatoire de $(\mathbb{F}_q)^n$ dans lui-même est une application linéaire aléatoire de $(\mathbb{F}_q)^n$ dans lui-même s'annulant en a. Dans ces conditions, cette différentielle a un noyau de dimension t avec probabilité $\alpha_{q,t}.q^{-t(t-1)}$ où $\alpha_{q,t}$ est une constante dans l'intervalle* $[0.16, 3.58]$.

Démonstration. Soit $a = (a_1, \ldots, a_n)$ un élément non-nul de $\mathbb{F}_q^n$ et L une application linéaire qui s'annule en a : $\sum_{i=1}^n l_i a_i = 0$ où les l_i sont les vecteurs-colonnes de L. Une fonction quadratique $P(x_1, \ldots, x_n) = \sum_{i=1}^n \sum_{j=i+1}^n p_{ij} x_i x_j$ a pour différentielle en a

$$DP_a(x_1, \ldots, x_n) \quad = \sum_{i=1}^n \left(\sum_{j=1}^{i-1} p_{ji} a_j + \sum_{j=i+1}^n p_{ij} a_j \right) x_i$$

Donc, l'équation $DP_a = L$ équivaut à

$$\begin{bmatrix} l_1 \\ \\ \vdots \\ \\ l_n \end{bmatrix} = \begin{bmatrix} 0 & p_{12} & p_{13} & \ldots & p_{1n} \\ p_{12} & 0 & p_{23} & \ldots & p_{2n} \\ p_{13} & p_{23} & 0 & & p_{3n} \\ \vdots & \vdots & & \ddots & \vdots \\ p_{1n} & p_{2n} & p_{3n} & \ldots & 0 \end{bmatrix} \begin{bmatrix} a_1 \\ \\ \vdots \\ \\ a_n \end{bmatrix}$$

À un réordonnement des coordonnées près, on peut supposer a_n non-nul. Alors, tout choix de coefficients p_{ij} pour $i < j < n$ peut être complété en une fonction quadratique telle que $DP_a = L$. En effet, on définit pour tout i dans $[1, n-1]$,

$$p_{in} = l_i + \sum_{j=1}^{i-1} p_{ji} a_j + \sum_{j=i+1}^{n-1} p_{ij} a_j$$

et on peut vérifier que la dernière équation $\sum_{i=1}^{n-1} p_{in} a_i = l_n$ est bien satisfaite, en utilisant l'annulation en a à la fois de L et DP_a. Ainsi, le nombre de fonctions

quadratiques P telles que $DP_a = L$ est indépendant de a et L, ce qui établit la première partie du théorème.

Les notations utilisées ici ont été introduites à la section 2.1 du chapitre 2. Pour tout t entre 1 et n, le nombre de sous-espaces de dimension t et contenant a est égal au nombre de sous-espaces de dimension $t-1$ dans $(\mathbb{F}_q)^n/(\mathbb{F}_q.a) : E(n-1,t-1)$. Le nombre d'applications linéaires s'annulant en a dont le noyau est de dimension t est alors $E(n-1,t-1)S(n,n-t)$, comme vu à la section 2.2.2. Le nombre total d'applications linéaires s'annulant en a étant $q^{n(n-1)}$, celles dont le noyau est de dimension t sont une proportion

$$\Pr_{L:L(a)=0}[\dim\ker L = t] = \alpha_{q,t}.q^{-t(t-1)} \quad \text{avec} \quad \alpha_{q,t} = \frac{\lambda(n)\lambda(n-1)}{\lambda(t)\lambda(t-1)\lambda(n-t)}$$

où $\lambda(n) = (1-\frac{1}{q})(1-\frac{1}{q^2})\dots(1-\frac{1}{q^n})$. La suite $\lambda(n)$ décroît de la valeur 1 et converge vers une valeur croissante en q et minorée par 0.28 pour $q = 2$ [39]. Il en résulte que $\alpha_{q,t}$ est dans l'intervalle $[0.16, 3.58]$. □

7.1.2 Borne sur la dimension du noyau de la différentielle de HFE

Comme déjà mentionné, la distribution de la dimension des noyaux de la différentielle est la même pour la clé publique et pour la fonction interne. La fonction interne est un polynôme $\mathbb{F}_q$-quadratique de degré inférieur à q^{D+1} :

$$P(x) = \sum_{i=0}^{D}\sum_{j=0}^{D} p_{ij}x^{q^i+q^j}$$

Sa différentielle est alors un polynôme $\mathbb{F}_q$-linéaire de degré inférieur ou égal à q^D :

$$DP_a(x) = \sum_{i=0}^{D}\sum_{j=0}^{D} p_{ij}(a^{q^i}x^{q^j} + a^{q^j}x^{q^i})$$

Les racines de ce polynôme $\mathbb{F}_q$-linéaire forment les éléments du noyau de l'application linéaire qu'il définit. En particulier, comme DP_a est de degré borné par q^D, il a au plus q^D racines (sauf à être le polynôme nul), et son noyau en tant qu'application linéaire est de dimension bornée par D.

$$\dim\ker DP_a \leq D$$

En contrepartie, la différentielle d'une application quadratique aléatoire a un noyau de dimension supérieure à D avec probabilité de l'ordre de $q^{-D(D+1)}$ (théorème 2).

Définissons le test T_D qui pour un élément non-nul a et une fonction quadratique P calcule la différentielle DP_a et répond 1 si la dimension du noyau est supérieure à D et 0 sinon. La complexité de cet algorithme est environ n^3. Cet algorithme définit un distingueur qui répond `HFE` quand T_D vaut 0 et `random` sinon. L'avantage de ce distingueur est la probabilité qu'il donne la bonne la réponse

déduit de la probabilité qu'il se trompe quand il lui est donné en entrée avec équiprobabilité une clé publique HFE ou une fonction aléatoire. Utilisant le théorème 2, le distingueur répond `random` avec probabilité de l'ordre de $q^{-D(D+1)}$, et ne se trompe jamais dans ce cas. L'avantage du distingueur est donc égal à cette probabilité. En outre, pour que le déchiffrement soit polynomial en le paramètre de sécurité n, le degré q^{D+1} du polynôme interne HFE doit être polynomial en n, ou encore D doit être logarithmique en n. L'avantage du distingueur est donc quasipolynomial en n, de la forme $1/exp\left((\log n)^2\right)$.

On va maintenant transformer ce distingueur par itération en un distingueur de complexité quasipolynomiale et avantage très proche de 1.

7.2 Amélioration de l'avantage par itération

Pour tout entier N, définissons le test T_D^N qui prend en entrée N éléments non-nuls distincts $a_1, \ldots, a_N$ et une fonction quadratique P, calcule toutes les valeurs $T_D(P, a_i)$, et renvoie 1 si l'une au moins de ces valeurs est 1, et 0 sinon. La complexité de l'algorithme est donc Nn^3. L'idée du test est d'augmenter la probabilité de détecter un système non-HFE en essayant plusieurs points. Tout choix de $a_1, \ldots, a_N$ définit un nouveau distingueur dont l'avantage est vraisemblablement amélioré par rapport au distingueur simple. On calcule maintenant cet avantage.

Pour tout choix de $a_1, \ldots, a_N$ non-nuls distincts, on définit la variable aléatoire

$$S_N^D(P) = \sum_{i=1}^{N} T_D(P, a_i)$$

définie sur l'ensemble des fonctions quadratiques. Toute les valeurs sommées sont 0 ou 1 et l'avantage du distingueur amélioré correspond à la probabilité

$$\Pr_{rand(P)}[S_N^D(P) \geq 1] = 1 - \Pr_{rand(P)}[S_N^D(P) = 0]$$

où $rand(P)$ désigne une fonction quadratique aléatoire. Pour minorer l'avantage, nous allons chercher à majorer la probabilité que $S_N^D(P) = 0$.

On sait par le théorème 2 que les variables $T_D(\cdot, a_i)$ sont toutes de loi binomiale de paramètre $\mu_D \simeq q^{-D(D+1)}$. Par suite, la moyenne de S_N^D, notée A_N^D, vaut $N\mu_D$. La probabilité que S_N^D soit égal 0 est majorée par la probabilité que S_N^D soit à distance de A_N^D supérieure à A_N^D :

$$\Pr_{rand(P)}[S_N^D(P) = 0] \leq \Pr_{rand(P)}[|S_N^D(P) - A_N^D| \geq A_N^D]$$

Il serait facile de trouver une borne supérieure de cette dernière probabilité si les variables sommées $T_D(\cdot, a_i)$ étaient indépendantes (avec la borne de Chernoff par exemple), malheureusement ces variables ne sont même pas indépendantes deux-à-deux. On peut en effet le voir de la symétrie de DP : les différentielles de P en a_i et a_j vérifient $DP_{a_i}(a_j) = DP_{a_j}(a_i)$, et par conséquent, l'annulation (ou non)

de DP_{a_i} en a_j est directement corrélé à l'annulation (ou non) de DP_{a_j} en a_j. Il s'ensuit que les distributions de la dimension du noyau de DP_{a_i} et DP_{a_j} ne sont pas indépendantes. Toutefois, cette corrélation entre DP_{a_i} et DP_{a_j} est la seule. Définissant l'ensemble $D(a,b)$ des couples d'applications linéaires (L,L') tels que $L(a)=0$, $L'(b)=0$ et $L(b)=L'(a)$, on a le lemme suivant.

Lemme 12. *Soient a et b deux éléments non-nuls et distincts de $(\mathbb{F}_q)^n$. Quand P est une fonction quadratique aléatoire, (DP_a, DP_b) est aléatoire dans $D(a,b)$.*

Démonstration. La preuve est similaire à celle du théorème 2. Soit (L,L') dans $D(a,b)$: $\sum_{i=1}^{n} l_i a_i = 0$, $\sum_{i=1}^{n} l'_i b_i = 0$ et $\sum_{i=1}^{n} l_i b_i = \sum_{i=1}^{n} l'_i a_i$; l_i, l'_j sont dans $\mathbb{F}_q^n$ et a_i, b_j dans $\mathbb{F}_q$. Puisque $a \neq b$ et $a \neq 0$, on peut supposer à un changement de coordonnées près que $a_n = 0$, $b_n = 1$ and $a_{n-1} = 1$. Tout choix de p_{ij} pour $i < j \leq n-2$ peut être uniquement complété en une fonction quadratique P telle que $(DP_a, DP_b) = (L, L')$, en prenant

$$\text{pour } i \text{ de 1 à } n-2 \qquad \begin{cases} p_{i\,n-1} &= l_i + \sum_{j=1}^{i-1} p_{ji} a_j + \sum_{j=i+1}^{n-2} p_{ij} a_j \\ p_{in} &= l'_i + \sum_{j=1}^{i-1} p_{ji} b_j + \sum_{j=i+1}^{n-1} p_{ij} b_j \end{cases}$$
$$\text{et} \qquad p_{n-1\,n} = l_n + \sum_{j=1}^{n-2} p_{jn} a_j$$

Le nombre de fonctions P telle que $(DP_a, DP_b) = (L, L')$ est donc indépendant de a, b, L, L', ce qui établit le lemme. □

À partir de ce lemme, nous allons pouvoir calculer la distribution jointe des dimensions des noyaux de DP_{a_i} et DP_{a_j} comme donnée par les probabilités

$$\Pr_{rand(P)}\left[\begin{array}{l} \dim\ker DP_{a_i} = r \\ \dim\ker DP_{a_j} = s \end{array}\right] = \Pr_{(L,L')\in D(a_i,a_j)}\left[\begin{array}{l} \dim\ker L = r \\ \dim\ker L' = s \end{array}\right] \tag{7.1}$$

et en particulier la probabilité que $T_D(P, a_i)$ et $T_D(P, a_j)$ valent simultanément 1. Nous en déduirons alors la variance de la variable aléatoire S_N^D.

7.2.1 Calcul de la distribution jointe

Notons $N_k(r)$ le nombre d'applications linéaires dont le noyau de dimension r contient un espace donné de dimension k. Comme montré à la section 2.2.5 et avec les notations du chapitre 2, le nombre de sous-espaces de $(\mathbb{F}_q)^n$ de dimension r contenant un espace donné de dimension k est $E(n-k, r-k)$. Pour chaque tel sous-espace, le nombre d'applications l'ayant pour noyau est $S(n, n-r)$. Nous avons donc

$$N_k(r) = E(n-k, r-k)S(n, n-r)$$

Ces notations introduites, la probabilité de droite dans l'équation 7.1 est donnée par lemme suivant.

Lemme 13. *Soit a, b deux éléments non-nuls et distincts de $(\mathbb{F}_q)^n$. Pour tout entiers r et s, la proportion des paires d'applications linéaires (L, L') dans $D(a, b)$ ayant des noyaux de dimensions (r, s) est :*

$$\frac{1}{q^{n(2n-3)}} \times \left(N_2(r)N_2(s) + \frac{1}{2^n - 1}(N_1(r) - N_2(r))(N_1(s) - N_2(s)) \right)$$

Démonstration. Une paire (L, L') dans $D(a, b)$ satisfait $L(a) = 0$,$L'(b) = 0$,$L(b) = L'(a)$, qui sont trois contraintes linéaires indépendantes sur les $2n$ coefficients dans $\mathbb{F}_2^n$ définissant L et L'. Par conséquent, $D(a, b)$ possède $q^{n(2n-3)}$ éléments. On définit l'ensemble V_a des applications linéaires qui s'annulent en a et l'ensemble $V_{a,b}$ des applications linéaires qui s'annulent sur le sous-espace engendré par a et b. Deux fonctions (L, L') dans $D(a, b)$ sont toutes deux dans $V_{a,b}$ ou bien toutes deux hors de $V_{a,b}$. Dans le second cas, pour tout L dans V_a et hors de $V_{a,b}$, le nombre de L' dans $D(a, b)$ tels que $L'(a) = L(b)$ représente une fraction $1/(q^n - 1)$ de tous les éléments de V_b et hors de $V_{a,b}$ puisque $L(b)$ est l'une des $q^n - 1$ valeurs autrement possibles pour $L'(a)$. □

La probabilité que $T_D(P, a_i)$ et $T_D(P, a_j)$ vaillent simultanément 1 se déduit du lemme précédent avec $r = s = D + 1$. Observant que :

$$N_1(D + 1) = N_2(D + 1)(q^{n-1} - 1)/(q^D - 1)$$

cette probabilité vaut :

$$\frac{N_1(D+1)^2}{q^{n(2n-3)}} \left(\left(\frac{q^D - 1}{q^{n-1} - 1} \right)^2 + \frac{1}{q^n - 1} \left(1 - \frac{q^D - 1}{q^{n-1} - 1} \right)^2 \right) \tag{7.2}$$

Par ailleurs, le nombre d'applications linéaires s'annulant en un élément donné et ayant un noyau de dimension $D + 1$ vaut $N_1(D + 1)/q^{n(n-1)}$, et correspond à la valeur de μ_D. Le facteur de l'expression ci-dessus vaut donc $\mu_D^2 q^n$, et après quelques étapes de calcul, on obtient pour la probabilité 7.2 :

$$\mu_D^2(1 + \epsilon_D) \qquad \text{où} \quad \epsilon_D = \frac{1}{q^n - 1} \left(\frac{q^n(q^D - 1)}{q^{n-1} - 1} - 1 \right)^2$$

Remarquons que comme le nombre de paires d'applications linéaires dans $V_a \times V_b$ est μ_D^2, le facteur $1 + \epsilon_D$ est un terme correctif mesurant la différence entre les distributions des dimensions des noyaux dans $V_a \times V_b$ et $D(a, b)$ à $(D + 1, D + 1)$. Mettant ϵ_D sous la forme

$$\epsilon_D = \frac{1}{q^n - 1} \left(q^{D+1} - 1 - q \left(1 - \frac{q^D - 1}{q^{n-1} - 1} \right) \right)^2$$

on constate que

$$\epsilon_D \leq \frac{q^{2(D+1)}}{q^n - 1}$$

7.2.2 Calcul de la variance

On peut maintenant calculer la variance, notée $(\sigma_N^D)^2$, de S_N^D. Notant $\mathrm{E}_{rand(P)}$ l'espérance pour P aléatoire, nous avons par définition

$$(\sigma_N^D)^2 = \mathrm{E}_{rand(P)}[(S_N^D)^2] - (A_N^D)^2$$

Par linéarité de l'espérance, et puisque les variables $T_D(P, a_i)$ ne valent toujours que 0 ou 1, nous avons

$$E[(S_N^D)^2] = A_N^D + \sum_{i=1}^{N} \sum_{j \neq i} \mathrm{E}_{rand(P)}[T_D(P, a_i).T_D(P, a_j)]$$

Or, pour chaque couple $i \neq j$,

$$\mathrm{E}_{rand(P)}[T_D(P, a_i).T_D(P, a_j)] = \mathrm{Pr}_{rand(P)} \left[\begin{array}{l} \dim \ker DP_{a_i} = D + 1 \\ \dim \ker DP_{a_j} = D + 1 \end{array} \right]$$

qui vaut, selon la section précédente : $\mu_D^2(1 + \epsilon_D)$. On en déduit que

$$(\sigma_N^D)^2 = A_N^D + N(N-1)\mu_D^2(1 + \epsilon_D) - (A_N^D)^2$$

puis, comme $A_N^D = N\mu_D$,

$$(\sigma_N^D)^2 = N\mu_D - N\mu_D^2(1 + \epsilon_D) + \epsilon_D N^2 \mu_D^2$$

7.2.3 Minoration de l'avantage

Par l'inégalité de Tchebycheff, on a pour tout t dans l'intervalle $]0, A_N^D/\sigma_N^D]$:

$$\mathrm{Pr}_{rand(P)}[|S_N^D - A_N^D| \geq t\sigma_N^D] \leq \frac{1}{t^2}$$

Par conséquent, pour $t = A_N^D/\sigma_N^D$, on obtient la majoration

$$\mathrm{Pr}_{rand(P)}[S_N^D(P) = 0] \leq \mathrm{Pr}_{rand(P)}[|S_N^D(P) - A_N^D| \geq A_N^D] \leq \frac{(\sigma_N^D)^2}{(A_N^D)^2}$$

En remplaçant A_N^D et $(\sigma_N^D)^2$ par leurs valeurs respectives, on obtient

$$\frac{(\sigma_N^D)^2}{(A_N^D)^2} = \frac{1}{N\mu_D} - \frac{1}{N}(1 + \epsilon_D) + \epsilon_D < \frac{1}{N\mu_D} + \epsilon_D$$

Finalement, posant $N\mu_D = q^a$, l'avantage du distingueur est

$$\mathrm{Pr}_{rand(P)}[S_N^D(P) \geq 1] > 1 - q^{-a} - \epsilon_D$$

Ainsi, prenant $N = q^D/\mu_D$, notre distingueur a pour complexité $q^{D(D+2)}$ et pour avantage

$$1 - q^{-D} - q^{-(n-2D-2)}$$

Pour $N = q^{D^2}/\mu_D$, la complexité devient $q^{D(2D+1)}$ et l'avantage

$$1 - q^{-D^2} - q^{-(n-2D-2)}$$

Comme q^D est polynomial en le paramètre de sécurité n, l'une et l'autre complexités sont quasipolynomiales, de la forme $exp((\log n)^2)$.

7.3 Conclusion

Nous avons montré qu'une clé publique HFE pouvait être distinguée d'un système quadratique aléatoire en temps quasipolynomial. Observons que, par ailleurs, la faisabilité d'inverser un système HFE par bases de Gröbner pour des tailles qui seraient hors de portée pour des systèmes aléatoires, montrée expérimentalement par Faugère [50], est en soi un autre distingueur de systèmes HFE. En réalité, il est même possible de distinguer un système HFE d'un système aléatoire légèrement avant la fin du calcul de base de Gröbner [51], car l'observation des premières dépendances linéaires non triviales dans la matrice de Macaulay est une détermination expérimentale du degré de régularité du système, un paramètre suffisant pour distinguer le système en présence d'un système aléatoire. Récemment, Granboulan-Joux-Stern ont montré une borne théorique sur le degré de régularité d'un système HFE, qui prouve que le calcul de base de Gröbner sur un système HFE jusqu'au degré de régularité est quasipolynomial, de complexité équivalente au distingueur présenté dans ce chapitre [58]. Le degré de régularité étant généralement très proche du degré maximal nécessaire au calcul de la base de Gröbner, la complexité estimée par Granboulan-Joux-Stern est également une bonne estimation de la complexité de l'attaque de Faugère sur un système HFE. Le distingueur différentiel présenté dans ce chapitre et le distingueur par bases de Gröbner diffèrent en la manière dont est exploitée la propriété de petit degré de HFE. En outre, le distingueur différentiel admet une preuve mathématique simple et ne requiert pas de mémoire.

Chapitre 8

La cryptanalyse de HFE

Dans ce chapitre, nous décrivons les principales stratégies d'attaques ayant été proposées contre HFE. Ces attaques appartiennent trois catégories. Les attaques de déchiffrement, cherchant à inverser la clé publique par l'exploitation de faiblesses structurelles, seront considérées en première partie. Les attaques sur la clé secrète, cherchant à extraire de l'information sur la clé secrète à partir de propriétés de la clé publique, seront considérées en deuxième partie. Enfin, quelques réflexions préliminaires concernant la recherche d'invariants fonctionnels de la différentielle seront présentées en troisième partie ; de tels invariants peuvent potentiellement être utilisés pour supprimer les variations et retrouver la clé secrète, comme vu au chapitre 5 dans le cas des schémas C^{*-}, toutefois leur existence dans le cas le plus général de HFE et leur exploitation concrète dans ce contexte sont encore inconnus.

8.1 Attaques de déchiffrement

Nous décrivons les différentes approches proposées dans l'ordre historique.

8.1.1 Attaque par multiple affine

Patarin a montré dans son article introduisant HFE quelques cas particuliers de HFE pouvant être attaqués par une généralisation simple de son attaque sur C^* [69]. L'attaque consiste à trouver une expression $A(x, y) = 0$ affine en x, vérifiée par les entrées et sorties de la clé publique x, $y = \boldsymbol{P}(x)$. Lorsqu'une telle expression est connue, les préimages par $\boldsymbol{P}$ d'une valeur spécifiée y sont contenues dans un sous-espace affine que l'on peut calculer, et qui, si sa dimension est suffisamment faible, peut être parcouru exhaustivement. Lorsque la forme de $A(x, y)$ n'est pas connue, on doit deviner son degré en y et déterminer ses coefficients par algèbre linéaire utilisant plusieurs valeurs x et $y = \boldsymbol{P}(x)$. Le nombre de coefficients de $A(x, y)$ étant de l'ordre de n^{k+1} lorsque A est de degré k en y, la complexité pour résoudre ce système linéaire est $n^{3(k+1)}$. L'attaque fonctionne donc si la clé publique $\boldsymbol{P}$ admet un multiple affine $A(x, y)$ de petit degré k en y, ou de façon équivalente, si le polynôme interne P satisfait cette même propriété.

Malheureusement, les conditions du succès de cette attaque ne sont pas claires. Bien que Patarin montre plusieurs cas concrets de polynômes internes pour lesquels cette attaque fonctionne, il est difficile d'en extraire un schéma général permettant d'isoler une famille de clés faibles. Il apparaît que les exemples attaqués par Patarin sont presque tous de la forme $P(x) = L_1(x)L_2(x)$ où L_1 et L_2 sont des polynômes $\mathbb{F}_q$-linéaires, mais on ne voit cependant pas la corrélation entre les formes spécifiques de L_1 et L_2 et la complexité de l'attaque. Les cas concrets attaqués par Patarin permettent toutefois d'exclure quelques permutations remarquables dont l'usage en tant que polynôme interne aurait pu présenter un intérêt particulier. D'autres permutations de la forme $L_1(x)L_2(x)$ sont connues [6] et n'ont pas été étudiées. Bien que les conditions d'existence d'un multiple affine d'un degré donné ne soient pas identifiées, il est conjecturé que pour un polynôme aléatoire de degré (univarié) d le plus petit multiple affine est de degré (multivarié) linéaire en d, ce qui porte la complexité de calculer ce multiple affine par ses valeurs entrées-sorties à $n^{\mathcal{O}(d)}$. Comme d doit être polynomial en n, la complexité conjecturée par Patarin pour cette attaque est donc exponentielle, de la forme $exp(n \log n)$.

8.1.2 Équations implicites de bas degré

Dans la version étendue de son article sur HFE [69], Patarin propose une généralisation de l'attaque précédente consistant à chercher des multiples quadratiques ou cubiques, c'est-à-dire des expressions $A(x, y) = 0$ quadratiques ou cubiques en x. Pour toute valeur spécifiée y, le système $A(x, y) = 0$ n'est alors plus linéaire, mais il pourrait être surdéterminé, et il serait alors possible par linéarisation de diminuer l'espace de recherche exhaustive, voire si ce système était suffisamment surdéterminé, retrouver le message initial. À nouveau, cette approche ne semble pas avoir fait l'objet d'une étude poussée et son intérêt n'est pas établi. Toutefois, sa généralisation par Courtois a porté certains fruits préfigurant des résultats plus tard reformulés dans le langage des bases de Gröbner.

Dans la continuité de l'approche proposée par Patarin, Courtois considère des relations implicites $A(x, y) = 0$ de formes prescrites et classifiées d'un point de vue formel [17, 16]. L'intérêt de considérer des relations implicites particulières plutôt que l'ensemble de celles de degrés donnés en x et y se justifie par la tentative de constater l'existence de certaines relations et non d'autres, qui révélerait ainsi certaines propriétés algébriques non évidentes. L'existence ou non de telles relations est établie sur une base expérimentale : comme pour l'attaque par multiple affine, on tente de déterminer ces relations par des valeurs (x, y) avec $y = P(x)$, et pour des raisons pratiques seules les relations de degré relativement faible en x et y sont considérées ; ainsi les tables données par Courtois ne répertorient que des relations de degré au plus 4 conjointement en x et y. Certaines relations implicites existent toutefois toujours ; ces relations appelées triviales sont des conséquences formelles de relations de commutation entre les y_i vus comme expressions quadratiques en les x_j et leur nombre est connu à l'avance. Par ailleurs, l'existence de relations non-triviales d'un degré donné est extrêmement improbable pour une

fonction quadratique aléatoire dès que n est suffisamment grand ; ceci est confirmé expérimentalement dans [16] pour le degré 4 en x, y sur $\mathbb{F}_2$ et dès que $n \geq 20$. Or, dans le cas des systèmes HFE, Courtois constate l'existence de relations implicites non-triviales de degré 4 en x, y pour ces mêmes valeurs de n et différentes valeurs du paramètre de degré d de HFE, avec un degré pour ces relations devenant de plus en plus élevé à mesure que d croît. Bien que d'une portée modeste, l'existence de ces relations constitue bien un distingueur de clés publiques HFE. L'exploitation de ces relations pour une attaque de déchiffrement n'est, en revanche, pas claire.

En marge de ce résultat, l'hypothèse initiale de l'existence pour un système HFE de relations implicites de types particuliers n'est pas observée : l'existence des relations implicites dépend de leur degré et non de leur forme particulière. En outre, Courtois observe un effet de seuil dans l'existence ou non de ces relations : les mêmes relations existent pour toute valeur de d entre deux puissances de 2 successives, en nombre décroissant avec d. Basé sur cette dernière observation, il conjecture que le degré des premières relations implicites non-triviales d'un HFE est logarithmique en d, soit linéaire en $D = \log_2(d)$. Comme les y_i sont implicitement des expressions quadratiques en les x_i, ces relations implicites de degré $\mathcal{O}(D)$ sont contenues dans l'ensemble des produits de y_i par des monômes en les x_j de degré $\mathcal{O}(D) - 2$. Le nombre de coefficients de ces relations est donc en $n^{\mathcal{O}(D)}$, ainsi que le coût de déterminer ces coefficients par algèbre linéaire. Comme D est lui-même logarithmique en n pour que le déchiffrement soit asymptotiquement polynomial, la complexité estimée du distingueur est $n^{\mathcal{O}(\log n)}$, soit une complexité quasi-polynomiale de la forme $exp((\log n)^2)$. En pratique toutefois, la complexité de l'attaque reste très élevée, notamment en mémoire. La méthode consistant à résoudre les coefficients des relations à partir de leurs évaluations sur des couples x, y ne semble pas permettre de tirer parti à l'avance du caractère éventuellement creux de ces équations et nécessite l'usage des méthodes d'algèbre linéaire pleine. Dans ces conditions, la complexité de calculer ces relations implicites pour le premier challenge HFE est estimée par Courtois à 2^{62} opérations et 33 To de mémoire [17]. Afin de diminuer la complexité en mémoire, Courtois propose des techniques de *distillation* et *reconciliation* visant à calculer ces relations par morceaux ; l'utilisation de ces techniques permettrait de réduire la complexité en mémoire pour le premier challenge HFE à 390 Go.

8.1.3 Attaques par les bases de Gröbner

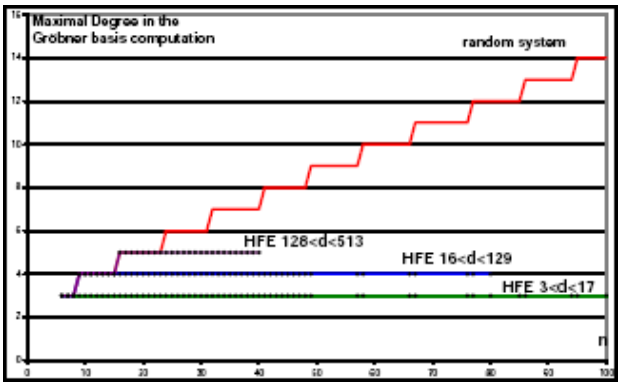
Comme pour les systèmes linéaires, les solutions d'un système d'équations polynomiales $p_1 = 0, \ldots, p_n = 0$ peuvent être calculées via des recombinaisons algébriques qui conduisent à une élimination progressive des variables. Une base de Gröbner est un ensemble générateur de l'ensemble des combinaisons algébriques des p_i formés de polynômes aux variables échelonnées (voir section 1.3 pour plus de précisions). Afin de calculer une telle base, les algorithmes modernes considèrent l'ensemble des multiples algébriques des p_i d'un degré donné, représentés comme des vecteurs sur la base des monômes du degré considéré, puis cherchent des dépen-

dances linéaires sur ces vecteurs par algèbre linéaire ; ces dépendances permettent précisément de calculer la base de Gröbner. La matrice formée de ces vecteurs est appelée matrice de Macaulay. Malheureusement, un grand nombre des dépendances trouvées proviennent de relations formelles entre générateurs du type $p_i p_j = p_j p_i$ et ne sont d'aucune utilité pour le calcul de la base de Gröbner. Le degré des multiples algébriques nécessaire à l'observation des premières dépendances linéaires *non-triviales* est un paramètre important appelé degré de régularité qui dépend du système de polynômes considéré. Récemment, Faugère a proposé un critère pour éliminer les dépendances linéaires triviales, conduisant à un algorithme particulièrement optimisé, appelé F5 [36]. Le fonctionnement courant de l'algorithme F5 est alors le suivant : l'algorithme construit les matrices de Macaulay de degré croissant jusqu'à rencontrer les premières dépendances linéaires non-triviales, puis termine rapidement le calcul (parfois un degré de plus est nécessaire). La complexité de l'algorithme correspond approximativement au coût de l'algèbre linéaire sur la matrice de Macaulay correspondant au degré de régularité. La taille de cette matrice est exponentielle en le degré de régularité, qui lui-même vaut asymptotiquement $n/11$ pour un système quadratique aléatoire de n équations en n variables sur $\mathbb{F}_2$ [2]. En pratique, F5 permet de calculer des bases de Gröbner pour des systèmes de l'ordre de 25 équations et inconnues, ce qui est bien meilleur que ce que permettaient les algorithmes précédents.

En 2002, Faugère a montré que le degré de régularité des systèmes HFE était bien inférieur à la valeur générique $n/11$ des systèmes aléatoires [51]. Il établit cette propriété expérimentalement avec l'algorithme F5 et fournit la valeur du degré de régularité pour plusieurs paramètres HFE sur $\mathbb{F}_2$; ces valeurs sont données dans la figure ci-après empruntée à [51]. Il apparaît sur la figure que la valeur du degré de régularité ne dépend que du paramètre de degré HFE pour n assez grand ; la complexité du calcul peut alors être estimée en fonction de n comme le coût de l'algèbre linéaire sur la matrice de Macaulay au degré de régularité, noté δ. Les lignes de cette matrice correspondant aux multiples des p_i par des monômes de degré $\delta - 2$, le nombre de lignes de cette matrice est $n.\binom{n}{\delta-2} = \mathcal{O}(n^{\delta-1})$ et leur poids est $n(n+1)/2$; le coût de l'algèbre linéaire creuse sur cette matrice est alors $\mathcal{O}(n^{2\delta})$ en temps et $\mathcal{O}(n^{\delta+1})$ en mémoire. Pour le paramètre de degré $d = 96$ du premier challenge HFE, celle-ci est $\mathcal{O}(n^8)$ en temps et $\mathcal{O}(n^5)$ en mémoire. En pratique, Faugère réussit à résoudre le premier challenge HFE, un système de 80 équations quadratiques à 80 variables sur $\mathbb{F}_2$, par le calcul d'une base de Gröbner avec F5, en une centaine d'heures et quelques Go de mémoire [50].

L'observation de Faugère d'un petit degré de régularité des systèmes HFE est clairement équivalente à celle de Courtois de l'existence de relations implicites de bas degré [17, 16]. En outre, Courtois avait lui aussi observé que le degré considéré restait constant sur les plages de valeurs du degré HFE comprises entre deux puissances de 2. Toutefois, la méthode de Faugère est beaucoup plus efficace algorithmiquement et sait transformer l'invariant algébrique détecté en une attaque de déchiffrement. La méthode de Courtois, cherchant à déterminer des relations

implicites à partir de valeurs entrées-sorties, ne sait mettre à profit des stratégies creuses comme c'est le cas de la méthode constructive employée par les algorithmes de bases de Gröbner, ce qui explique l'importante différence de portée pratique.



8.1.4 Explication de la cryptanalyse algébrique

Si les approches de Courtois et Faugère font toutes deux la preuve expérimentale d'une moindre complexité algébrique des systèmes HFE par rapport aux systèmes aléatoires, aucune ne propose en revanche d'explication de ce phénomène. Dans [32, 58], Joux *et al.* proposent un changement de représentation du problème permettant de comprendre qualitativement l'origine du phénomène observé.

Observons tout d'abord que le degré de régularité du système est invariant par composition par des applications linéaires inversibles et il est donc suffisant de calculer le degré de régularité du système associé à la fonction interne. La fonction interne est définie par un polynôme $P(X)$ sur $\mathbb{F}_{q^n}$:

$$P(X) = \sum_{i=0}^{D} \sum_{j=0}^{D} p_{ij} X^{q^i+q^j}$$

où D est un paramètre définissant une borne sur le degré. Pour toute base de $\mathbb{F}_{q^n}$, on peut représenter cette fonction par ses coordonnées $p_0, \ldots, p_{n-1}$ qui sont des formes quadratiques en les coefficients $x_0, \ldots, x_{n-1}$ de X. La matrice de Macaulay au degré d du système engendré par $p_0, \ldots, p_{n-1}$ a pour lignes les multiples par les monômes de degré $d-2$ des générateurs $p_0, \ldots, p_{n-1}$ vus comme des vecteurs sur la base des monômes de degré d. Le degré de régularité du système est la plus petite valeur de d pour laquelle la matrice de Macaulay admet des dépendances linéaires non-triviales (au sens précisé à la section précédente).

Quitte à appliquer un changement de coordonnées, qui ne change pas le degré de régularité, on peut considérer P dans une base normale $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$:

$$P(X) = \sum_{k=0}^{n-1} p_k(x_0, \ldots, x_{n-1}) \alpha^{q^k}$$

Dans une telle représentation, élever à la puissance q revient à faire une permutation circulaire des coordonnées vers la droite. Ainsi, la première coordonnée de $P(X)^{q^i}$ est p_i et la première coordonnée de X^{q^j} est x_j. Notant P_i la puissance q^i-ième de P et X_j la puissance q^j-ième de X, la projection sur la première coordonnée de P_i est p_i et celle de X_j est x_j. Comme toute projection s'écrit comme une trace, les p_i s'écrivent comme des combinaisons linéaires à coefficients dans $\mathbb{F}_{q^n}$ des $P_0, \ldots, P_{n-1}$ et les x_j comme des combinaisons linéaires à coefficients dans $\mathbb{F}_{q^n}$ des $X_0, \ldots, X_{n-1}$. En outre, les P_k sont des polynômes quadratiques en les X_k ; par exemple :

$$P(X) = \sum_{i=0}^{D} \sum_{j=0}^{D} p_{ij} X_i X_j$$

Nous en déduisons que les multiples des $p_0, \ldots, p_{n-1}$ par des monômes de degré $d-2$ en $x_0, \ldots, x_{n-1}$ s'écrivent comme des combinaisons linéaires à coefficients dans $\mathbb{F}_{q^n}$ des multiples des $P_0, \ldots, P_{n-1}$ par des monômes de degré $d-2$ en $X_0, \ldots, X_{n-1}$; ces derniers polynômes sont eux-mêmes de degré d. La matrice de Macaulay au degré d, notée $\mathcal{M}_d$, peut donc se réécrire comme une matrice M_d à coefficients dans $\mathbb{F}_{q^n}$ dont les lignes correspondent à des polynômes de degré d sur $X_0, \ldots, X_{n-1}$. Toute dépendance linéaire sur les lignes de $\mathcal{M}_d$ est une dépendance linéaire à coefficients dans $\mathbb{F}_q$ des lignes de M_d. En outre, la multiplication par un élément de $\mathbb{F}_{q^n}$ étant elle-même une opération linéaire sur $\mathbb{F}_q$, toute opération linéaire à coefficients dans $\mathbb{F}_{q^n}$ sur les lignes de M_d se transforme en opérations linéaires à coefficients dans $\mathbb{F}_q$ sur les lignes de $\mathcal{M}_d$. Le degré de régularité du système est donc la première valeur de d pour laquelle il existe des dépendances non-triviales à coefficients dans $\mathbb{F}_{q^n}$ des lignes de M_d.

Transformé en ces termes, le problème laisse mieux paraître la spécificité des systèmes HFE. Calculer une base de Gröbner pour un tel système revient à effectuer les opérations correspondantes sur les polynômes $P_0, \ldots, P_{n-1}$ quadratiques en $X_0, \ldots, X_{n-1}$ qui dans le cas d'un HFE possèdent une forme spécifique : pour tout k, le polynôme P_k s'exprime en les seules variables $X_k, \ldots, X_{D+k}$. Le fait que chacun de ces polynômes s'exprime sur un petit nombre de variables consécutives implique que la résolution de seulement $D+1$ variables, par exemple $X_0, \ldots, X_D$, permet d'en déduire toutes les autres, puisque celles-ci sont séquentiellement éliminées dans les expressions de $P_2, \ldots, P_{n-1}$. Généralisant cela comme décrit dans [32], chaque sous-système de λD polynômes $P_1, \ldots, P_{\lambda D}$ s'écrit sur $(\lambda+1)D$ variables ; le rapport du nombre de variables sur le nombre d'équations est donc $1+1/\lambda \simeq 1$. De façon informelle, un système HFE de paramètre (n, D) peut donc être vu comme une suite de $\mathcal{O}(n/D)$ petits systèmes quadratiques de dimensions $\mathcal{O}(D)$. De façon plus formelle, le degré de régularité δ du système est inférieur à celui de tout sous-système, et en particulier inférieur à celui δ_λ du sous-système formé des λD premiers polynômes, car toute dépendance linéaire non-triviale sur les lignes de la sous-matrice M_d^λ de M_d associée à ce sous-système est une dépendance non-triviale sur les lignes de M_d. Prenant par exemple $\lambda = 1$, nous avons donc δ borné par δ_1, qui est une fonction de D indépendante de n.

Détermination du degré de régularité en fonction des paramètres : Outre le fait d'expliquer le phénomène observé, à savoir que le degré de régularité d'un système HFE est une fonction de D et non de n, le changement de représentation proposé par Joux *et al.* offre également une base favorable à la détermination précise du degré de régularité pour des paramètres donnés. Pour toute valeur de d, le rang de la matrice de Macaulay au degré d peut être calculé en dénombrant le nombre de polynômes distincts obtenus en multipliant $P_0, \ldots, P_{n-1}$ par tous les monômes de degré $d-2$ en $X_0, \ldots, X_{n-1}$. Le nombre de polynômes ainsi formés dépend bien sûr de la forme spécifique des P_k ; en particulier, il apparaît clairement que ce nombre augmente d'autant plus vite avec d que les polynômes P_k s'expriment sur peu de variables. Notons également, que lorsque nous cherchons à calculer une base de Gröbner pour les solutions à coefficients dans $\mathbb{F}_q$, le dénombrement proposé doit s'effectuer sur la base des monômes sans puissance de q. Supposant maintenant que nous sachions résoudre ce problème combinatoire, le degré de régularité δ du système est la première valeur de d à laquelle le rang de la matrice de Macaulay n'est pas maximal, soit inférieur au nombre total de lignes de la matrice diminué de la dimension de l'espace des dépendances linéaires triviales dont les valeurs respectives ne dépendent pas du système considéré. Nous ne connaissons malheureusement pas de traitement mathématique de ce problème ; il ne fait cependant nul doute que résoudre le dénombrement proposé serait d'une grande utilité pour évaluer la complexité pratique de l'attaque en fonction des paramètres et affiner notre compréhension du phénomène combinatoire sous-jacent.

Expression asymptotique du degré de régularité de HFE pour $q = 2$: La représentation précédente permet également, par un simple argument formel et dans le cas où $q = 2$, de déduire la forme asymptotique du degré de régularité en fonction du paramètre D. Le résultat, présenté par Joux *et al.* dans [58], s'obtient sur la base des résultats asymptotiques généraux démontrés pour les systèmes quadratiques surdéterminés par Bardet *et al.* [2].

L'algorithme F5 est un algorithme général de calcul de bases de Gröbner, dont le calcul ne s'effectue pas nécessairement sur la base des monômes sans puissance de q, comme on le souhaiterait lorsque l'on cherche à calculer une base de Gröbner associée à des solutions à coordonnées dans $\mathbb{F}_q$. Une solution à ce problème lorsque $q = 2$ est d'adjoindre au système en entrée les polynômes supplémentaires $x_0^2 - x_0, \ldots, x_{n-1}^2 - x_{n-1}$, qui permettent de simuler le calcul d'une base de Gröbner sur la base des monômes sans carrés. Dans ce cas, le degré de régularité du système sur $\mathbb{F}_2$ quand le calcul s'effectue sur la base des monômes sans carrés coïncide avec le degré de régularité du système obtenu par adjonction de $x_0^2 - x_0, \ldots, x_{n-1}^2 - x_{n-1}$ quand le calcul s'effectue sur la base générale, avec l'algorithme F5. Ceci n'est pas vrai en général lorsque q est supérieur à 2, car ajouter les polynômes supplémentaires $x_0^q - x_0, \ldots, x_{n-1}^q - x_{n-1}$ ne permet de simuler le calcul d'une base de Gröbner sur la base des monômes sans puissance de q qu'à partir du degré q. Afin d'utiliser les résultats de Bardet *et al.* sur la complexité de F5, il convient

donc d'appliquer le changement de représentation décrit à la section précédente également aux polynômes supplémentaires $x_0^2 - x_0, \ldots, x_{n-1}^2 - x_{n-1}$. Élevant X_i à la puissance 2 (qui est une opération linéaire) et comparant à la valeur de X_{i+1}, nous obtenons :

$$X_i^2 - X_{i+1} = \left(\sum_{k=0}^{n-1} x_k \alpha^{2^{k+i}}\right)^2 - \left(\sum_{k=0}^{n-1} x_k \alpha^{q^{k+i+1}}\right) = \sum_{k=0}^{n-1} (x_k^2 - x_k)\alpha^{q^{k+i+1}}$$

Il s'ensuit que les images des polynômes supplémentaires $x_0^2 - x_0, \ldots, x_{n-1}^2 - x_{n-1}$ sont $X_0^2 - X_1, \ldots, X_{n-1}^2 - X_0$. Nous pouvons alors à nouveau remarquer que le degré de régularité δ du système $P_0, \ldots, P_{n-1}, X_0^2 - X_1, \ldots, X_{n-1}^2 - X_0$ est borné par celui de tout système, et en particulier par celui δ_λ associé au sous-système s'exprimant en les seules $(\lambda+1)D$ premières variables :

$$\begin{cases} P_0, \ldots, P_{\lambda D-1}, \\ X_0^2 - X_1, \ldots, X_{(\lambda+1)D-2}^2 - X_{(\lambda+1)D-1} \end{cases}$$

formé de $(2\lambda+1)D$ équations quadratiques en $(\lambda+1)D$ variables. Le degré de régularité δ_λ de ce sous-système ne dépend que de λ et D, et supposant que ce sous-système vérifie les hypothèses de généricité dans lesquels sont établis les résultats de Bardet *et al.* pour les systèmes quadratiques surdéterminés [2], l'expression asymptotique de δ_λ est :

$$\delta_\lambda = c_\lambda . D + \mathcal{O}(D^{1/3})$$

où la constante

$$c_\lambda = (\tau - \frac{1}{2} - \sqrt{\tau(\tau-1)})$$

est fonction du taux de surdétermination $\tau = (2\lambda+1)/(\lambda+1)$. Fixant une quelconque valeur de λ, il résulte de $\delta \leq \delta_\lambda$ que δ est asymptotiquement linéaire en D. De ceci, nous pouvons en déduire la complexité asymptotique du calcul de bases de Gröbner pour les systèmes HFE sur $\mathbb{F}_2$: celle-ci s'évalue comme le coût de l'algèbre linéaire sur la matrice de Macaulay au degré de régularité δ, qui comprend de l'ordre de $n^{\delta-1}$ lignes ; la complexité du calcul s'élève donc à $n^{2\delta} = n^{\mathcal{O}(D)}$. Finalement, lorsque $D = \log_2 n$ comme requis pour un déchiffrement polynomial du cryptosystème en fonction du seul paramètre n, la complexité de l'attaque est quasipolynomiale en n, de la forme $exp((\log_2 n)^2)$.

8.1.5 Conclusion

Les résultats présentés dans cette section représentent l'état de l'art actuel concernant les attaques de déchiffrement sur HFE. Nous renvoyons le lecteur à la section 6.3 pour des commentaires et perspectives quant à cette approche.

8.2 Attaques sur la clé secrète

À la section précédente, nous nous sommes intéressés au caractère à sens unique de la fonction de chiffrement. Dans cette section, notre objectif est d'extraire de la clé publique de l'information sur la clé secrète. Plus précisément, nous cherchons à extraire des contraintes algébriques sur les coefficients du masquage linéaire (S, T) transformant la fonction interne P de forme connue en la clé publique $\boldsymbol{P}$:

$$\boldsymbol{P} = T \circ P \circ S$$

8.2.1 Attaque de Kipnis et Shamir

Une première approche, proposée par Kipnis et Shamir en 1999 [55], vise à dériver des contraintes sur les coefficients de T à partir de l'équation équivalente

$$T^{-1} \circ \boldsymbol{P} = P \circ S \tag{8.1}$$

en utilisant la contrainte de petit degré de P. Pour cela, nous exprimons la relation précédente comme une identité polynomiale sur $\mathbb{F}_{q^n}$ en la variable x. Étant donné un isomorphisme de $\mathbb{F}_{q^n}$ dans $(\mathbb{F}_q)^n$, la clé publique $\boldsymbol{P}$ se réécrit comme un polynôme sur $\mathbb{F}_{q^n}$ de la forme :

$$\boldsymbol{P}(x) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \boldsymbol{p}_{ij} x^{q^i+q^j}$$

Pour ce même isomorphisme, nous pouvons supposer que la fonction interne P admet une représentation univariée de cette forme et de degré borné en fonction du paramètre D :

$$P(x) = \sum_{i=0}^{D} \sum_{j=0}^{D} p_{ij} x^{q^i+q^j}$$

Nous savons en effet que pour l'isomorphisme de $\mathbb{F}_{q^n}$ dans $(\mathbb{F}_q)^n$ choisi par l'utilisateur légitime, P admet une telle expression, et supposer que P admet cette même expression pour l'isomorphisme de l'attaquant revient à un changement de S et T.

L'attaque de Kipnis-Shamir se reformule de manière non-ambiguë en terme de différentielle. La différentielle de la clé publique

$$D\boldsymbol{P}(a, x) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \boldsymbol{p}_{ij} (a^{q^i} x^{q^j} + a^{q^j} x^{q^i})$$

est une forme bilinéaire symétrique sur la base des $A_i = a^{q^i}$ et $X_j = x^{q^j}$:

$$D\boldsymbol{P}(a, x) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \boldsymbol{p}_{ij} (A_i X_j + A_j X_i)$$

associée uniquement à une matrice symétrique de taille $n \times n$ à coefficients dans $\mathbb{F}_{q^n}$ notée $\boldsymbol{M}$. Notant $\underline{A}$ le vecteur $(A_0, \ldots, A_{n-1})$ et $\underline{X}$ le vecteur $(X_0, \ldots, X_{n-1})$,

$$D\boldsymbol{P}(a, x) = \underline{A} \,.\, \boldsymbol{M} \,.\, \underline{X}^t$$

De la même façon, l'application linéaire T^{-1} s'écrit comme un polynôme sur $\mathbb{F}_{q^n}$,

$$T^{-1}(x) = \sum_{k=0}^{n-1} t_k . x^{q^k}$$

et la composition $T^{-1} \circ D\boldsymbol{P}(a, x)$ se réécrit :

$$T^{-1} \circ D\boldsymbol{P}(a, x) = \sum_{k=0}^{n-1} t_k . (D\boldsymbol{P}(a, x))^{q^k}$$

Pour tout k, $(D\boldsymbol{P}(a, x))^{q^k}$ est encore une forme bilinéaire symétrique en les A_i et X_j, associée à la matrice $\boldsymbol{M}_k$ obtenue de $\boldsymbol{M}$ par élévation des coefficients à la puissance q^k et translation de k indices. Finalement, $T^{-1} \circ D\boldsymbol{P}$ est une forme bilinéaire symétrique associée à la matrice : $\sum_{k=0}^{n-1} t_k . \boldsymbol{M}_k$.

Nous procédons maintenant à une transformation similaire sur le membre de droite de l'équation (8.1). La fonction interne $P(x)$ est un polynôme de la même forme que $\boldsymbol{P}(x)$ mais écrit sur la base des seuls monômes $x^{q^i+q^j}$ avec $i, j \leq D$. Sa différentielle $DP(a, x)$ définit une forme bilinéaire symétrique sur la base des A_i et X_j, qui du fait de la borne D est associé à une matrice symétrique M dont seul le premier bloc de taille $(D+1) \times (D+1)$ comprend des entrées non-nulles. On obtient maintenant la différentielle de $P \circ S$, soit $DP(S, S)$, en évaluant M sur les vecteurs $(S(A_0), \ldots, S(A_{n-1}))$ et $(S(X_0), \ldots, S(X_{n-1}))$. Pour tout k, $S(A_k)$ est une forme linéaire en les $A_0, \ldots, A_{n-1}$, et le vecteur $(S(A_0), \ldots, S(A_{n-1}))$ est l'évaluation en $(A_0, \ldots, A_{n-1})$ d'une certaine matrice W de taille $n \times n$ à coefficients dans $\mathbb{F}_{q^n}$. La matrice de la forme bilinéaire symétrique $DP(S, S)$ est donc $W.M.W^t$:

$$DP(S, S)(a, x) = \underline{A} \,.\, W.M.W^t \,.\, \underline{X}^t$$

Finalement, l'égalité des formes bilinéaires symétriques associées aux deux membres de l'équation (8.1) consiste en l'identité matricielle :

$$\sum_{k=0}^{n-1} t_k . \boldsymbol{M}_k = W.M.W^t \tag{8.2}$$

dans laquelle les matrices $\boldsymbol{M}_k$ sont connues et le membre de droite est une matrice de rang au plus $D+1$. Les coefficients $t_0, \ldots, t_{n-1}$ sont donc solutions du problème d'optimisation linéaire consistant à trouver une combinaison linéaire des matrices $\boldsymbol{M}_k$ qui soit de rang inférieur à $D+1$. Dans sa forme générale, ce problème est connu en théorie des codes sous le nom de MinRank et prouvé NP-complet [3, 12, 16]. Toutefois, lorsque $D \ll n$, Kipnis et Shamir montrent que le problème se ramène à la résolution d'un système quadratique largement surdéterminé [55].

Retrouver T par résolution algébrique du problème MinRank associé : Le problème MinRank exprime que le sous-espace engendré par les vecteurs lignes de la matrice $\sum_{k=0}^{n-1} t_k.\boldsymbol{M}_k$ est de dimension au plus $D+1$. Supposant que pour les valeurs des t_k correspondant à T^{-1} les $D+1$ premiers vecteurs lignes sont linéairement indépendants, ceci revient à exprimer que les $n-(D+1)$ vecteurs lignes restants sont des combinaisons linéaires de ces $D+1$ premiers vecteurs. Les coefficients de ces combinaisons linéaires sont autant de nouvelles inconnues, en nombre $(n-(D+1))(D+1)$, et l'équation associée à chaque vecteur se décline en n équations sur ses coefficients. Ces derniers coefficients étant eux-mêmes des formes linéaires des inconnues initiales $t_0, \ldots, t_{n-1}$, nous obtenons un système de $n(n-(D+1))$ équations quadratiques en $n+(n-(D+1))(D+1)$ variables sur $\mathbb{F}_{q^n}$. Ce système est nettement surdéfini, avec pour rapport du nombre d'équations sur le nombre de variables

$$\tau = \frac{n(n-(D+1))}{n+(n-(D+1))(D+1)} < \frac{n}{D+1}$$

Malheureusement, il ne l'est pas suffisamment pour pouvoir être résolu par simple linéarisation : observant que les monômes quadratiques de ce système sont tous le produit d'un t_k et d'un coefficient d'une des combinaisons linéaires, ce système se linéarise en $n(n-(D+1))(D+1)$ variables, ce qui est $D+1$ fois plus que le nombre d'équations dont nous disposons. Dans [55], Kipnis et Shamir proposent une technique de *relinéarisation*, consistant à ajouter des équations de degré supérieur exprimant la commutation des monômes linéarisés, mais son succès n'est pas établi. La complexité de résoudre ce système par les bases de Gröbner peut s'estimer, sous hypothèse de généricité, par les formules de Bardet *et al.* [1, 2]. Le degré de régularité d'un système quadratique surdéterminé de rapport τ est asymptotiquement $(\tau - \frac{1}{2} - \sqrt{\tau(\tau-1)})$ fois le nombre de variables. Par un développement limité, le coefficient vaut environ $1/8\tau$. Le système considéré ayant environ Dn variables et un taux de surdétermination d'environ n/D, son degré de régularité est, sous hypothèse de généricité toujours, environ $\delta = D^2/8$. La complexité du calcul de base de Gröbner sur un tel système est donc environ $(Dn)^{2\delta}$; lorsque $D = \mathcal{O}(\log n)$ comme requis pour que le déchiffrement soit polynomial, cette complexité est quasipolynomiale de la forme $exp\left((\log n)^3\right)$. Malheureusement, pour les paramètres pratiques, cette complexité est totalement hors de portée. Bien sûr, il est possible que la forme spécifique du système d'équations considéré permette une résolution par les bases de Gröbner avec une complexité plus faible, mais ceci n'a jamais été rapporté. Finalement, l'intérêt de cette approche reste théorique.

8.2.2 Une autre approche

Une autre approche beaucoup plus simple que celle de Kipnis et Shamir consiste à dériver des contraintes sur S, plutôt que sur T, à partir de l'équation :

$$\boldsymbol{P} \circ S^{-1} = T \circ P$$

Les deux membres de l'équation sont des polynômes sur la base des monômes $x^{q^i+q^j}$, dont l'identité expriment des contraintes sur les coefficients de S^{-1}, P et T. Qui plus est, le polynôme $T \circ P$ est creux, avec pour seuls coefficients non-nuls ceux correspondant aux indices i, j de différence au plus D, et identifier ses coefficients nuls à ceux de $\boldsymbol{P} \circ S^{-1}$ fournit autant de contraintes en les seuls coefficients de S^{-1}. Plus précisément, notant $s_0, \ldots, s_{n-1}$ les coefficients de S^{-1} et $(\boldsymbol{p}_{ij})$ les coefficients de $\boldsymbol{P}$, on peut vérifier que le coefficient de $x^{q^i+q^j}$ dans $\boldsymbol{P} \circ S^{-1}$ est :

$$\sum_{k=0}^{n-1} \sum_{l=0}^{n-1} \boldsymbol{p}_{i-k,j-l} \cdot s_k^{q^{i-k}} s_l^{q^{j-l}}$$

où les valeurs $i-k$ et $j-l$ sont prises modulo n, et cette expression est donc nulle pour tous les indices i, j de différence supérieur à D. Tenant compte de la symétrie en i, j de $x^{q^i+q^j}$, le nombre de tels indices est $(n-D-1)(n-D)/2$, et pour chacun d'eux, l'équation en les coefficients $s_0, \ldots, s_{n-1}$ correspond à n équations quadratiques en leurs coordonnées sur $\mathbb{F}_q$. Les coefficients de S^{-1} sont donc solutions d'un système d'équations quadratiques surdéterminé, avec pour rapport du nombre d'équations sur le nombre de variables :

$$\tau = \frac{n(n-D-1)(n-D)}{2n^2} < \frac{n}{2}\left(1 - \frac{D}{n}\right)^2$$

Le rapport de surdétermination de ce système est supérieur à celui du système obtenu par Kipnis et Shamir, mais le nombre de variables est également beaucoup plus grand. Le degré de régularité d'un tel système est génériquement $\delta = n^2/8\tau = \mathcal{O}(n)$ et la complexité du calcul de bases de Gröbner est alors exponentielle. Cette approche est donc finalement moins intéressante que celle de Kipnis et Shamir.

8.3 Recherche d'invariants multiplicatifs

Dans cette dernière section, nous proposons quelques réflexions concernant une possible nouvelle voie de recherche sur la sécurité de HFE : la recherche d'invariants fonctionnels de la différentielle. En termes abstraits, nous pourrions définir un tel invariant comme le comportement particulier de la différentielle sous l'action spécifique de certaines applications linéaires ; les termes « comportement », « action » et « certaines » restant les grandes inconnues du problème. Bien que ceci laisse de grandes libertés à l'imagination, nous ne considérerons ici que des extensions simples de telles propriétés mises en évidence sur le C^* au chapitre 5. L'exploitation de ces propriétés a notamment permis de cryptanalyser la variation *moins* de C^* ; une autre application considérée vise à retrouver la clé secrète.

8.3.1 Action antisymétrique des multiplications sur HFE

Nous avons montré au chapitre 5 une propriété remarquable de la différentielle de C^* vis-à-vis des applications linéaires correspondant à des multiplications par

des éléments de $\mathbb{F}_{q^n}$. On note $\pi_\theta(x) = x^{1+q^\theta}$ le monôme C^* de paramètre θ, et M_ξ la multiplication par l'élément ξ de $\mathbb{F}_{q^n}$. Nous avons alors l'identité suivante sur la différentielle $D\pi_\theta$ de π_θ, pour tout couple d'éléments (a, x) :

$$D\pi_\theta(M_\xi(a), x) + D\pi_\theta(a, M_\xi(x)) = M_{\ell_\theta(\xi)} \circ D\pi_\theta(a, x) \tag{8.3}$$

où l'on a posé $\ell_\theta(\xi) = \xi + \xi^{q^\theta}$. Un caractéristique importante de cette identité est que les applications linéaires M_ξ et $M_{\ell_\theta(\xi)}$ y interviennent linéairement : les couples $(M_\xi, M_{\ell_\theta(\xi)})$ sont les solutions de l'équation linéaire en (M, N) :

$$D\pi_\theta(M(a), x) + D\pi_\theta(a, M(x)) = N \circ D\pi_\theta(a, x)$$

De la même façon, l'identité induite sur la clé publique $T \circ \pi_\theta \circ S$ est linéaire en les transformées $S^{-1} \circ M \circ S$ et $T \circ N \circ T^{-1}$ des inconnues (M, N) de cette équation par le masquage secret S, T. Celles-ci peuvent donc être cherchées par algèbre linéaire à partir de l'équation publique correspondante ; comme il existe environ $n^2/2$ choix de couples (a, x) linéairement indépendants, l'ensemble des équations induites par les n coordonnées de la clé publique forme un système de $\simeq n^3/2$ équations linéaires en les $2n^2$ coefficients inconnus, qui rend aisément possible la résolution des applications linéaires cherchées, comme constaté en pratique.

Considérons à présent les conséquences de l'identité ci-dessus sur la différentielle de HFE. Un polynôme interne HFE, noté $P(x)$, s'écrit de façon unique :

$$P(x) = \sum_{i=0}^{D-1} \sum_{j>i}^{D} p_{ij}\, x^{q^i+q^j}$$

Un tel polynôme s'écrit comme une combinaison fonctionnelle de C^* de paramètre k valant respectivement $1, \ldots, D$:

$$P(x) = \sum_{i=0}^{D-1} \sum_{j>i}^{D} p_{ij}(x^{1+q^{j-i}})^{q^i} = \sum_{k=1}^{D} \left[\sum_{i=0}^{D-k} p_{i,i+k}(x^{1+q^k})^{q^i} \right] = \sum_{k=1}^{D} L_k \circ \pi_k(x)$$

Dans cette expression, les applications L_k sont linéaires. Par suite, la différentielle de P s'écrit :

$$DP(a, x) = \sum_{k=1}^{D} L_k \circ D\pi_k(a, x) \tag{8.4}$$

Définissons alors, pour toute application linéaire M, la fonction bilinéaire

$$\Sigma[M](a, x) = DP(M(a), x) + DP(a, M(x))$$

que l'on appelle l'*action antisymétrique* de M sur DP. De même, on note $\sigma_k[M]$ l'action antisymétrique de M sur $D\pi_k$:

$$\sigma_k[M](a, x) = D\pi_k(M(a), x) + D\pi_k(a, M(x))$$

L'expression (8.4) de DP en fonction des $D\pi_k$ donne alors :

$$\Sigma[M](a,x) = \sum_{k=1}^{D} L_k \circ \sigma_k[M](a,x)$$

En particulier, lorsque M est la multiplication par un élément ξ, la propriété remarquable (8.3) de C^* se réécrit pour tout k,

$$\sigma_k[M_\xi](a,x) = M_{\ell_k(\xi)} \circ D\pi_k(a,x)$$

où l'on rappelle que $\ell_k(\xi) = \xi + \xi^{q^k}$, et par conséquent, l'action antisymétrique de M_ξ sur DP admet l'expression :

$$\Sigma[M_\xi](a,x) = \sum_{k=1}^{D} L_k \circ M_{\ell_k(\xi)} \circ D\pi_k(a,x) \tag{8.5}$$

Si l'on considère maintenant la clé publique $\boldsymbol{P} = T \circ P \circ S$, sa différentielle s'obtient en composant l'expression (8.4) par S et T :

$$D\boldsymbol{P}(a,x) = T \circ DP(S(a),S(x)) = \sum_{k=1}^{D} (T \circ L_k \circ T^{-1}) \circ (T \circ D\pi_k(S(a),S(x)))$$

que l'on peut encore réécrire :

$$D\boldsymbol{P}(a,x) = \sum_{k=1}^{D} \boldsymbol{L}_k \circ D\boldsymbol{\pi}_k(a,x)$$

où l'on a noté $\boldsymbol{L}_k = T \circ L_k \circ T^{-1}$ et $\boldsymbol{\pi}_k$ la clé publique C^* obtenue de π_k par composition par S et T. De la même façon, l'action antisymétrique des conjuguées $\boldsymbol{M}_\xi = S^{-1} \circ M_\xi \circ S$ des multiplications sur la différentielle de la clé publique s'obtient en composant l'expression (8.5) par S et T :

$$\boldsymbol{\Sigma}[\boldsymbol{M}_\xi](a,x) = \sum_{k=1}^{D} \boldsymbol{L}_k \circ \boldsymbol{N}_{\ell_k(\xi)} \circ D\boldsymbol{\pi}_k(a,x) \tag{8.6}$$

où l'on a posé $\boldsymbol{N}_{\ell_k(\xi)} = T \circ M_{\ell_k(\xi)} \circ T^{-1}$.

Il apparaît de cette relation que, si les clés publiques C^* associées $\boldsymbol{\pi}_1, \ldots, \boldsymbol{\pi}_D$ étaient connues, il serait évidemment très facile de déterminer les applications $\boldsymbol{M}_\xi$ conjuguées des multiplications par le masquage secret. En effet, les uplets d'applications linéaires $(\boldsymbol{M}_\xi, \boldsymbol{L}_1 \circ \boldsymbol{N}_{\ell_1(\xi)}, \ldots, \boldsymbol{L}_D \circ \boldsymbol{N}_{\ell_D(\xi)})$ pour tout ξ sont les solutions de l'équation linéaire d'inconnue notée $(\boldsymbol{M}, \boldsymbol{N}_1, \ldots, \boldsymbol{N}_D)$:

$$\boldsymbol{\Sigma}[\boldsymbol{M}](a,x) = \sum_{k=1}^{D} \boldsymbol{N}_k \circ D\boldsymbol{\pi}_k(a,x)$$

À nouveau, comme il existe $\simeq n^2/2$ choix de couples (a, x) linéairement indépendants, l'ensemble des équations pour les n coordonnées de la différentielle forme un système de $\simeq n^3/2$ équations linéaires en les $(D+1)n^2$ coefficients inconnus. Malheureusement, nous ne connaissons pas ces clés publiques C^* associées $\boldsymbol{\pi}_1, \ldots, \boldsymbol{\pi}_D$, nous n'en connaissons qu'une combinaison fonctionnelle : la différentielle $D\boldsymbol{P}$.

Dans la suite, nous montrons qu'il existe cependant des cas spécifiques de HFE pour lesquels il est très facile de déterminer des multiplications non-triviales. Ces cas particuliers sont fonction de la factorisation de n, un aspect qui n'était jusqu'alors jamais apparu comme pouvant influer sur la sécurité de HFE. Nous montrerons ensuite une interprétation de l'identité (8.6) conduisant à une propriété distinctive des multiplications, mais que l'on ne sait pas exprimer par des conditions linéaires.

8.3.2 Influence de la factorisation de n

Considérant la factorisation de n, nous pouvons regrouper les termes $\boldsymbol{L}_k \circ \boldsymbol{\pi}_k$ selon le plus petit facteur premier commun de leur paramètre respectif k et de n. Nous nous intéressons ici au cas des polynômes HFE qui sont des sommes de C^* dont les paramètres ont tous un même facteur commun $d > 1$ avec n. Le polynôme HFE considéré s'écrit donc :

$$P(x) = \sum_{d|k\,,\,k\leq D} L_k \circ \pi_k(x)$$

L'action antisymétrique d'une multiplication M_ξ sur sa différentielle s'écrit :

$$\Sigma[M_\xi](a, x) = \sum_{d|k\,,\,k\leq D} L_k \circ M_{\ell_k(\xi)} \circ D\pi_k(a, x)$$

Or, pour tout k multiple de d, le noyau de l'application linéaire $\ell_k(\xi) = \xi + \xi^{q^k}$ contient le noyau de ℓ_d qui est de dimension d, et par conséquent pour tout élément ξ de ce sous-espace commun, nous avons :

$$\Sigma[M_\xi](a, x) = 0$$

Ces applications vérifient une équation linéaire et leurs conjuguées peuvent donc être aisément restaurées à partir de l'équation publique correspondante. De tels polynômes HFE, pour lesquels les paramètres C^* admettent un facteur commun non-trivial de n, constituent donc des instances faibles de HFE.

Curieusement, les polynômes HFE pour lesquels les paramètres C^* sont tous premiers avec n constituent aussi des instances faibles de HFE lorsque n est pair, en caractéristique 2. Lorsque n est pair, nous pouvons en effet montrer que l'équation $\xi + \xi^q = 1$ admet des solutions : considérant un quelconque élément z de trace 1, la demi-trace constituée des puissances paires (ou impaires) de q est une telle solution. Les autres solutions s'en déduisent par l'ajout d'un multiple scalaire de l'unité, qui sont les solutions de $\xi + \xi^q = 0$. Notons maintenant, qu'en

caractéristique 2, un élément ξ satisfaisant $\xi + \xi^q = 1$ satisfait aussi $\xi + \xi^{q^2} = (\xi+\xi^q)+(\xi+\xi^q)^q = 1+1 = 0$, et plus généralement $\ell_k(\xi) = 0$ pour toute valeur de k paire ; par le même argument, un tel élément vérifie $\ell_k(\xi) = 1$ pour toute valeur de k impaire. En particulier, les entiers k premiers avec n sont tous impairs lorsque n est pair. Par conséquent, l'action de M_ξ avec ξ satisfaisant $\xi + \xi^q = 1$, sur la différentielle d'un polynôme HFE dont tous les paramètres C^* sont premiers avec n,

$$\Sigma[M_\xi](a,x) = \sum_{k\wedge n=1\, k\leq D} L_k \circ M_{\ell_k(\xi)} \circ D\pi_k(a,x) = \sum_{k\wedge n=1\, k\leq D} L_k \circ M_1 \circ D\pi_k(a,x)$$

n'est autre que l'identité :

$$\Sigma[M_\xi](a,x) = DP(a,x)$$

Cette équation linéaire induit une équation analogue sur la clé publique à partir de laquelle on restaure par algèbre linéaire les conjuguées des multiplications M_ξ avec $\xi + \xi^q = 1$. Ces polynômes HFE, de paramètres C^* tous premiers avec n où n est pair, constituent donc également des instances faibles de HFE.

8.3.3 Un invariant multiplicatif non-linéaire de HFE

Revenant au cas général, nous proposons ici une caractérisation des multiplications, déduite de l'identité :

$$\boldsymbol{\Sigma}[\boldsymbol{M}_\xi](a,x) = \sum_{k=1}^{D} \boldsymbol{L}_k \circ \boldsymbol{N}_{\ell_k(\xi)} \circ D\boldsymbol{\pi}_k(a,x) \tag{8.7}$$

Comme nous l'avons vu, la différentielle $D\boldsymbol{P}$ d'un HFE est une combinaison fonctionnelle des différentielles $D\boldsymbol{\pi}_1, \ldots, D\boldsymbol{\pi}_D$:

$$D\boldsymbol{P}(a,x) = \sum_{k=1}^{D} \boldsymbol{L}_k \circ D\boldsymbol{\pi}_k(a,x)$$

La propriété distinctive des multiplications, exprimée par l'identité (8.7) ci-dessus, est qu'il en est de même des fonctions $\boldsymbol{\Sigma}[\boldsymbol{M}_\xi]$ pour tout ξ, avec toutefois des facteurs linéaires différents. Malheureusement, ceci ne nous fournit pas directement un moyen de calculer les applications $\boldsymbol{M}_\xi$, car la base $D\boldsymbol{\pi}_1, \ldots, D\boldsymbol{\pi}_D$ sur laquelle s'écrivent ces combinaisons fonctionnelles n'est pas connue. Cependant, considérant D éléments linéairement indépendants $\xi_1, \ldots, \xi_D$, il existe un espoir raisonnable que les fonctions $\boldsymbol{\Sigma}[\boldsymbol{M}_{\xi_1}], \ldots, \boldsymbol{\Sigma}[\boldsymbol{M}_{\xi_D}]$ constituent une base équivalente, ou tout au moins engendrent un large sous-ensemble des combinaisons fonctionnelles des $D\boldsymbol{\pi}_1, \ldots, D\boldsymbol{\pi}_D$. En particulier, il existe très probablement de nombreux choix d'un D-uplet $(\xi_1, \ldots, \xi_D)$ tel que $\boldsymbol{\Sigma}[\boldsymbol{M}_{\xi_1}], \ldots, \boldsymbol{\Sigma}[\boldsymbol{M}_{\xi_D}]$ engendrent $D\boldsymbol{P}$. Ces multiplications sont donc des solutions possibles de la condition :

$$\boldsymbol{\Sigma}[\boldsymbol{M}_1], \ldots, \boldsymbol{\Sigma}[\boldsymbol{M}_D] \text{ engendrent } D\boldsymbol{P}$$

qui s'expriment à partir de la clé publique, en les inconnues $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_D$. D'un autre côté, cette condition a très probablement extrêmement peu de chances d'être satisfaite pour un choix aléatoire de $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_D$: assimilant alors les fonctions bilinéaires symétriques $\boldsymbol{\Sigma}[\boldsymbol{M}_k]$ à des n-uplets de formes bilinéaires symétriques aléatoires, l'espace engendré par les n coordonnées respectives des $\boldsymbol{\Sigma}[\boldsymbol{M}_1], \ldots, \boldsymbol{\Sigma}[\boldsymbol{M}_D]$ est de dimension Dn avec forte probabilité, et la probabilité qu'il contienne les n coordonnées de $D\boldsymbol{P}$ est égal à la proportion des sous-espaces de dimension nD contenant l'espace de dimension n engendré par les coordonnées de $D\boldsymbol{P}$, soit en utilisant les résultats du chapitre 2 :

$$S(nD, n)/S(n^2/2, n) \simeq q^{-n^3/2+n^2D}$$

Selon ces arguments, la propriété considérée est donc bien caractéristique des multiplications. Malheureusement, on ne voit pas comment exprimer une telle condition autrement qu'en faisant des facteurs linéaires de la décomposition de $D\boldsymbol{P}$ des inconnues supplémentaires du problème ; nous aurions alors à résoudre un système quadratique surdéterminé d'environ $n^3/2$ équations en $2Dn^2$ inconnues.

Chapitre 9

HFE avec Perturbation Interne

HFE avec Perturbation Interne, aussi appelé IPHFE, est une variation de HFE introduite par Ding et Schmidt à PKC 2005 [23]. La modification proposée consiste à bruiter la structure HFE d'origine par des termes quadratiques de degrés arbitraires contrôlés par une fonction linéaire de petit rang. Le but recherché est de permettre une résistance supérieure aux attaques par bases de Gröbner, au prix d'une moindre efficacité des opérations secrètes.

Un schéma apparenté à IPHFE est le schéma PMI, proposé par Ding en 2004, et résultant de l'application d'une idée similaire à C^* [20]. Si PMI résiste effectivement aux attaques par bases de Gröbner pour les paramètres recommandés [22], il admet cependant une grave vulnérabilité, révélée par Fouque, Granboulan et Stern [40]. La perturbation interne, dépendant d'une fonction linéaire de petit rang, s'annule sur un gros sous-espace appelé le noyau de la perturbation. La restriction de la clé publique à tout sous-espace parallèle au noyau de la perturbation est une clé publique C^*, et il est par conséquent essentiel à la sécurité de PMI que ce sous-espace ne puisse être découvert. Malheureusement, Fouque *et al.* ont montré que la perturbation interne induisait des propriétés différentielles qui, contrastant fortement avec celles de C^*, permettaient de distinguer l'appartenance ou non d'un élément donné au noyau de la perturbation, rendant alors possible sa détection.

Le secret du noyau de la perturbation est également un enjeu vital pour IPHFE. Pareillement, la connaissance de ce sous-espace permet de transformer la clé publique en une partition de clés publiques HFE, dont les paramètres ont souvent été affaiblis afin de compenser le surcoût au déchiffrement dû à la perturbation interne. Toutefois, la plus grande généricité de HFE par rapport à C^* et l'application d'une perturbation plus élaborée que celle de PMI posent un obstacle technique à l'analyse différentielle de IPHFE et rendent même hypothétique l'existence d'une généralisation de l'attaque sur PMI fonctionnant pour toutes les clés. L'hypothèse d'une telle attaque n'est d'ailleurs même pas envisagée par Ding et Schmidt [23].

Dans ce chapitre, nous montrons que la structure différentielle de IPHFE admet une caractérisation simple en moyenne sur les clés et constatons l'existence d'un biais différentiel de perturbation. Le calcul précis de ce biais peut être effectué, sur

la base de résultats combinatoires démontrés à la section 2.3. Le reste de l'attaque est une généralisation de l'attaque de Fouque *et al.* sur PMI. La complexité globale de l'attaque peut être précisément estimée ; l'attaque n'est pas pratique pour les paramètres recommandés, mais reste bien plus rapide qu'un déchiffrement par recherche exhaustive, préalablement évalué comme la meilleure attaque, tout en restaurant une clé secrète équivalente.

9.1 Description de IPHFE

La définition d'un schéma IPHFE fait intervenir trois paramètres (n, D, r) où n est le nombre de variables du système, D est le paramètre HFE et r est le paramètre de perturbation. La fonction interne est définie par un quadruplet $(P, M, \bar{P}, Z)$ dont les constituants sont des types suivants. Les trois premiers, $P, M, \bar{P}$ sont des polynômes à coefficients dans $\mathbb{F}_{2^n}$ respectivement en les variables x, (x, y) et y. Le polynôme $P(x)$ est $\mathbb{F}_2$-quadratique de degré inférieur à 2^{D+1}, de la forme :

$$P(x) = \sum_{i=0}^{D} \sum_{j=0}^{D} p_{ij} x^{2^i+2^j}$$

Le polynôme $M(x, y)$ est $\mathbb{F}_2$-bilinéaire de degré en x inférieur à 2^D, de la forme :

$$M(x, y) = \sum_{i=0}^{D} \sum_{j=0}^{n-1} m_{ij} x^{2^i} y^{2^j}$$

Le polynôme $\bar{P}(y)$ est un polynôme $\mathbb{F}_2$-quadratique quelconque, de la forme :

$$\bar{P}(y) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \bar{p}_{i,j} y^{2^i+2^j}$$

On note $\ddot{P}(x, y)$ la somme de ces trois polynômes :

$$\ddot{P}(x, y) = P(x) + M(x, y) + \bar{P}(y)$$

Enfin, Z est une application linéaire de rang r de $\mathbb{F}_{2^n}$ dans lui-même. La fonction interne IPHFE, notée $\tilde{P}$, est alors la fonction à une variable :

$$\tilde{P}(x) = \ddot{P}(x, Z(x))$$

Bien que cette fonction soit de grand degré en général, ses racines peuvent être calculées indirectement lorsque r est petit. Pour chacune des 2^r valeurs b de l'image de Z, on cherche les racines du polynôme $\ddot{P}(x, b)$ qui, par construction, est de petit degré inférieur à 2^{D+1}, puis on filtre ces racines par la condition $Z(x) = b$. Ceci rend possible l'inversion de la fonction $\tilde{P}$, au prix de 2^r inversions d'un polynôme HFE de paramètre D.

On construit un schéma IPHFE en choisissant aléatoirement un quadruplet $(P, M, \bar{P}, Z)$ et deux bijections linéaires S et T, constituant ensemble la clé secrète, puis calculant la clé publique :

$$\tilde{\boldsymbol{P}} = T \circ \tilde{P} \circ S$$

Les paramètres recommandés dans [23] pour IPHFE sont $(n, D, r) = (89, 3, 2)$. Comparant ces paramètres avec ceux du premier challenge HFE, $(n, D) = (80, 6)$, nous voyons qu'à valeur de n comparable, le paramètre D choisi pour IPHFE est beaucoup plus faible que celui du premier challenge HFE. La raison de ce choix est une question de performance. Afin de compenser le surcoût au déchiffrement dû à la perturbation interne, il a été nécessaire de diminuer la valeur du paramètre HFE. D'une façon générale, le coût du déchiffrement d'un IPHFE de paramètre (n, D, r) est comparable à celui d'un HFE de paramètre $(n, D + r/2)$ car la complexité de trouver les racines d'un polynôme est typiquement quadratique en le degré (avec l'algorithme Berlekamp-trace [57] par exemple). En particulier, IPHFE avec les paramètres proposés est de performance comparable au premier challenge HFE.

Par l'application d'une perturbation interne, les concepteurs de IPHFE visent à produire un schéma résistant mieux que le HFE aux attaques par bases de Gröbner. Il est maintenant établi que, du fait de sa structure particulière, une clé publique HFE peut être inversée par calcul d'une base de Gröbner, avec l'algorithme F5 par exemple, beaucoup plus rapidement qu'un système aléatoire. En particulier, le premier challenge HFE est apparu à portée d'une attaque pratique et cassé par Faugère en 2002 [50]. Toutefois, même sur les systèmes HFE, les performances des algorithmes actuels reste en pratique très limitée du fait de leur importante complexité en mémoire et il peut toujours être envisagé d'augmenter les paramètres tout en gardant une efficacité raisonnable. L'opportunité de IPHFE est de permettre une résistance supérieure à HFE à performance égale. Bien que cet avantage possible de IPHFE n'ait cependant jamais été démontré ni quantifié, l'exemple de PMI suggère que l'ajout de perturbation interne améliore en effet considérablement la résistance aux attaques par bases de Gröbner. Dans [23], les concepteurs de IPHFE prévoient que pour les paramètres proposés la meilleure attaque est la recherche exhaustive dans l'espace des messages, en 2^{89} évaluations de la clé publique.

9.2 Le noyau de la perturbation

Par construction, la restriction de la fonction interne $\tilde{P}$ à tout sous-espace affine parallèle au noyau $\mathcal{K}$ de Z est un polynôme $\mathbb{F}_2$-quadratique de degré inférieur à 2^{D+1}. Il en résulte que la restriction de la clé publique $\tilde{\boldsymbol{P}}$ à tout sous-espace affine parallèle au noyau $\boldsymbol{\mathcal{K}}$ de $Z \circ S$ est une clé publique HFE de paramètre D. Ainsi, parmi les nombreux composants formant la clé secrète, le sous-espace $\boldsymbol{\mathcal{K}}$ est d'un intérêt particulier car sa connaissance permet de réduire le problème de l'inversion de la clé publique IPHFE à celui de l'inversion de 2^r clés publiques HFE de paramètre D. Notons, de plus, que ces restrictions HFE sont plus faibles qu'un HFE

de performance égale au schéma IPHFE original, du fait de l'arbitrage entre leur paramètre D et le paramètre r de perturbation. En particulier, pour les paramètres proposés, ces restrictions sont des HFE de paramètres $(89, 3)$ qui, comparant aux paramètres $(80, 6)$ du premier challenge HFE cassé par Faugère, doivent être à portée d'une attaque pratique. Dans ces conditions, le sous-espace $\boldsymbol{\mathcal{K}}$ consiste en une clé secrète équivalente puisqu'il rend possible l'inversion de la clé publique. Nous appelons le sous-espace $\boldsymbol{\mathcal{K}}$ le *noyau de la perturbation.*

9.2.1 L'exemple de PMI

Un schéma apparenté à IPHFE est le schéma PMI proposé par Ding en 2004 [20]. PMI résulte de l'application de l'idée de perturbation interne à C^*. Avec nos notations, PMI se définit en prenant le polynôme P de la forme $x^{2^i+2^j}$ où i et j sont choisis tels que $2^i + 2^j$ et $2^n - 1$ soient premiers entre eux, et en prenant nul le polynôme M. Le choix particulier du polynôme P permet une inversion plus efficace que la recherche de racines mise en œuvre dans HFE : P est ici une permutation et s'inverse en élevant à la puissance inverse de $2^i + 2^j$ modulo $2^n - 1$. Toutefois, ce mode d'inversion interdit l'usage d'une perturbation interne avec un terme M, car le polynôme $\ddot{P}(x, b)$ obtenu pour une valeur image b de Z ne serait alors pas un monôme. Finalement, la fonction interne PMI est :

$$\tilde{P}(x) = P(x) + \bar{P}(Z(x))$$

Comme pour IPHFE, sur tout espace affine $Z^{-1}(b)$ parallèle au noyau $\mathcal{K}$ de Z, la fonction interne PMI est un monôme C^* avec terme constant, $P(x) + \bar{P}(b)$. Par conséquent, la restriction de la clé publique PMI à tout sous-espace affine parallèle au noyau de la perturbation $\boldsymbol{\mathcal{K}} = \ker(Z \circ S)$ est une clé publique C^*. Pareillement, le noyau de la perturbation consiste ici en une clé secrète équivalente car toute clé publique C^* peut être inversée en temps polynomial par l'attaque de Patarin [67].

L'importance fondamentale du noyau de la perturbation a d'abord été remarquée par Fouque, Granboulan et Stern, et est la première de deux observations ayant conduit à une attaque très efficace sur PMI [40]. La seconde observation offre un moyen de déceler le noyau de la perturbation à partir de la clé publique : la différentielle de la clé publique en un élément a est structurellement différente selon l'appartenance ou non de a au noyau de la perturbation. Ceci peut effectivement être vu à partir de la différentielle du polynôme interne ; la différentielle de $\tilde{P}$ en a est :

$$D\tilde{P}_a = DP_a + D\bar{P}_{Z(a)} \circ Z$$

Cette différentielle se réduit à $D\tilde{P}_a = DP_a$ lorsque a est dans $\mathcal{K} = \ker(Z)$. Ainsi, quand a est dans $\mathcal{K}$, la différentielle est simplement la différentielle du monôme C^*, tandis que quand a n'est pas dans $\mathcal{K}$, elle comprend le terme additionnel de perturbation. Ces différences structurelles peuvent être perçues en considérant la dimension du noyau. Dans [40], il est montré que le noyau de la différentielle d'un

monôme C^* est toujours de dimension égale à $\text{pgcd}(j-i,n)$, en tout élément non-nul. En revanche, quand le terme de perturbation interfère, d'autres dimensions sont possibles. À titre d'exemple, on rapporte dans la table ci-dessous les probabilités expérimentales fournies dans [40] pour les paramètres recommandés (nous avons alors $\text{pgcd}(j-i,n)=8$).

$a \in \boldsymbol{\mathcal{K}}$						1	
$a \notin \boldsymbol{\mathcal{K}}$	≈ 0.686	≈ 0.290	≈ 0.023	$\approx 5e-4$	$\approx 2e-6$	≈ 0	≈ 0
$\dim\ker D\tilde{\boldsymbol{P}}_a$	3	4	5	6	7	8	>8

Nous voyons ici que la dimension du noyau de la différentielle laisse fuir énormément d'information sur l'appartenance ou non à $\mathcal{K}$. Cette information peut être exploitée pour détecter des éléments de $\mathcal{K}$ avec très faible probabilité d'erreur, et détecter n tels éléments restaure le noyau $\mathcal{K}$ tout entier avec forte probabilité [40].

9.2.2 Application à IPHFE

Suivant l'exemple de PMI, la question se pose d'un biais différentiel de perturbation dans IPHFE. Celui-ci diffère de PMI à deux égards : il est basé sur HFE au lieu de C^* et sa perturbation interne est plus complexe, avec un terme mixte M. Nous allons voir que si la première différence s'avère d'impact mineur, la seconde a des conséquences plus graves. Sans terme mixte M, nous nous trouvons effectivement dans une situation assez analogue à la précédente : la différentielle en un élément a de $\mathcal{K}$ est la différentielle du polynôme P de degré inférieur à 2^{D+1}, dont le noyau est de dimension au plus D comme nous l'avons vu au chapitre 7 ; en revanche, quand a n'est pas dans $\mathcal{K}$, le terme de perturbation interfère, et des dimensions supérieures peuvent être atteintes avec une probabilité non nulle. Notons toutefois, que le terme de perturbation étant linéaire de rang r, la dimension du noyau est toujours inférieure à $D+r$. À nouveau, nous avons donc un critère simple pour détecter des éléments hors de $\mathcal{K}$, qui peuvent être exploités pour restaurer le noyau de la perturbation selon la stratégie proposée dans [40]. En revanche, avec un terme de mixte M, la différentielle prend la forme générale suivante :

$$D\tilde{P}_a(x) = DP_a(x) + M(x, Z(a)) + M(a, Z(x)) + D\bar{P}_{Z(a)}(Z(x))$$

Son expression en un élément a de $\mathcal{K}$, n'est plus la différentielle du polynôme HFE en a mais s'accompagne d'un terme de perturbation :

$$a \in \mathcal{K}, \quad D\tilde{P}_a(x) = DP_a(x) + M(a, Z(x))$$

La conséquence de cette observation est que le même spectre de dimensions va pouvoir être atteint que a soit dans $\mathcal{K}$ ou non. La différentielle a de plus une forme très similaire dans les deux cas. Dans les deux cas, la différentielle est la somme

d'un polynôme $\mathbb{F}_2$-linéaire de degré au plus 2^D et d'une application linéaire de rang au plus r. Nous avons en effet, quand a est dans $\mathcal{K}$:

$$a \in \mathcal{K}, \quad D\tilde{P}_a(x) = L_a^+(x) + \ell_a^+(x)$$

avec $L_a^+(x) = DP_a(x)$ de degré inférieur à 2^D et $\ell_a^+ = M(a, Z(x))$ de rang inférieur à r. Dans l'autre cas, quand a n'est pas dans $\mathcal{K}$, nous avons :

$$a \notin \mathcal{K}, \quad D\tilde{P}_a(x) = L_a^-(x) + \ell_a^-(x)$$

avec $L_a^-(x) = DP_a(x) + M(x, Z(a))$ de degré inférieur à 2^D et $\ell_a^- = M(a, Z(x)) + D\bar{P}_{Z(a)}(Z(x))$ de rang inférieur à r. En caractéristique 2, la différentielle en a s'annulant toujours en a, les deux composantes L_a^+, ℓ_a^+ et L_a^-, ℓ_a^- prennent respectivement les mêmes valeurs en a :

$$L_a^+(a) = \ell_a^+(a) \quad ; \quad L_a^-(a) = \ell_a^-(a)$$

Il existe toutefois une différence entre les deux cas : cette valeur commune est 0 dans le premier cas, et non-nulle avec très forte probabilité dans le second :

$$\begin{cases} a \in \mathcal{K}, & L_a^+ = \ell_a^+ = 0 \\ a \notin \mathcal{K}, & L_a^- = \ell_a^- = M(a, Z(a)) \neq 0 \end{cases}$$

Ceci constitue bien un biais différentiel de perturbation de IPHFE. Toutefois, même si ce biais existe, nous ne savons toujours pas comment le détecter. Nous pourrions étudier les deux distributions :

$$\begin{cases} \Pr_a[\dim \ker D\tilde{P}_a = t \,|\, a \in \mathcal{K}] \\ \Pr_a[\dim \ker D\tilde{P}_a = t \,|\, a \notin \mathcal{K}] \end{cases}$$

pour tout t, mais celles-ci doivent dépendre des composants secrets $(P, M, \bar{P}, Z)$ de la fonction interne. Dans la suite, nous montrons que ces probabilités peuvent être déterminées en moyenne sur les choix possibles de $(P, M, \bar{P}, Z)$; ceci nous permettra de définir un distingueur de $\mathcal{K}$ correspondant à une stratégie gagnante en moyenne pour une instance aléatoire du cryptosystème.

9.3 Caractérisation différentielle de IPHFE

À la section précédente, nous avons vu que pour tout élément a, la différentielle en a est une somme de deux applications linéaires de types distincts, L_a^+, ℓ_a^+ lorsque a est dans $\mathcal{K}$, L_a^-, ℓ_a^- lorsque a n'est pas dans $\mathcal{K}$. Dans cette section, nous montrons que lorsque $(P, M, \bar{P}, Z)$ sont aléatoirement choisis, ces applications linéaires sont aléatoires des types respectivement prescrits. Ceci nous permettra de transformer les probabilités sur $(P, M, \bar{P}, Z)$ en des probabilités sur les paires (L, ℓ) où L est un polynôme $\mathbb{F}_2$-linéaire aléatoire de degré 2^D et ℓ est une application linéaire aléatoire de rang r. Le calcul effectif de ces probabilités sera l'objet de la prochaine section.

Le choix d'un quadruplet $(P, M, \bar{P}, Z)$ définit un polynôme interne $\tilde{P}$ et un noyau de perturbation $\mathcal{K} = \ker(Z)$. Pour tout élément non-nul a, l'ensemble des quadruplets $(P, M, \bar{P}, Z)$ se divise en deux classes : ceux pour lesquels Z a un noyau contenant a, et ceux pour lesquels Z a un noyau de contenant pas a. Le théorème suivant montre que la proportion de quadruplets pour lesquels le noyau de $D\tilde{P}_a$ est de dimension t dans l'une et l'autre classe s'écrit comme une proportion associée sur l'espace des paires (L, ℓ).

Théorème 3. *Soit a un élément non-nul de $(\mathbb{F}_2)^n$. Un quadruplet $(P, M, \bar{P}, Z)$ définit un polynôme interne $\tilde{P}$ et un sous-espace $\mathcal{K} = \ker(Z)$. On note L un polynôme $\mathbb{F}_2$-linéaire aléatoire de degré 2^D et ℓ une application linéaire aléatoire de rang r. Pour une proportion $1 - \epsilon_{n,r}$ des choix de $(P, M, \bar{P}, Z)$, nous avons :*

$$\Pr\left[\dim\ker D\tilde{P}_a = t \mid a \in \mathcal{K}\right] = \Pr_{(L,\ell)}[\dim\ker(L+\ell) = t \mid L(a) = \ell(a) = 0]$$

et

$$\Pr\left[\dim\ker D\tilde{P}_a = t \mid a \notin \mathcal{K}\right] = \Pr_{(L,\ell)}[\dim\ker(L+\ell) = t \mid L(a) = \ell(a) \neq 0]$$

où $\epsilon_{n,r} = 2^{-n+r} + \mathcal{O}(2^{-2n+r})$

Il apparaîtra clairement dans la suite que la quantité $\epsilon_{n,r}$ est bien heureusement négligeable devant les probabilités cherchées. Ce facteur correspond à la proportion de quadruplets $(P, M, \bar{P}, Z)$ pour lesquels les applications L_a^+, ℓ_a^+ (respectivement L_a^-, ℓ_a^-) ne seraient pas de degré exactement 2^D ou de rang exactement r. Dans la suite, on notera π^+ et π^- les deux distributions cherchées (indépendantes de a) :

$$\pi^+(t) = \Pr_{(L,\ell)}[\dim\ker(L+\ell) = t \,|\, L(a) = \ell(a) = 0]$$
$$\pi^-(t) = \Pr_{(L,\ell)}[\dim\ker(L+\ell) = t \,|\, L(a) = \ell(a) \neq 0]$$

La preuve du théorème n'est pas difficile mais un peu longue ; nous l'isolons dans la sous-section suivante, elle peut être omise en première lecture.

9.3.1 Preuve du théorème 3

La preuve du théorème revient essentiellement à montrer, dans chaque cas, l'existence d'une surjection uniforme d'un sous-ensemble quasi-exhaustif des quadruplets $(P, M, \bar{P}, Z)$ vers un sous-ensemble déterminé des paires (L, ℓ).

Les deux briques essentielles de la preuve sont les deux lemmes suivants.

Lemme 14. *Soit a un élément non-nul de $\mathbb{F}_{2^n}$. Quand P est un polynôme $\mathbb{F}_2$-quadratique aléatoire de degré inférieur à 2^{D+1}, DP_a est un polynôme $\mathbb{F}_2$-linéaire aléatoire de degré inférieur ou égal à 2^D et s'annulant en a.*

Démonstration. On montre que l'application $P \mapsto DP_a$ est une surjection uniforme des ensembles décrits dans l'énoncé. Soit L un polynôme $\mathbb{F}_2$-linéaire de degré $\leq 2^D$ qui s'annule en a : $\sum_{i=0}^{D} l_i a^{2^i} = 0$. Le polynôme $\mathbb{F}_2$-quadratique

$$P(x) = \sum_{i=0}^{D} \sum_{j=i+1}^{D} p_{ij} x^{2^i+2^j}$$

a pour différentielle en a :

$$\sum_{i=0}^{D} \left(\sum_{j=0}^{i-1} p_{ji} a^{2^j} + \sum_{j=i+1}^{D} p_{ij} a^{2^j} \right) x^{q^i}$$

Tout choix des coefficients p_{ij} pour $i < j < D$ peut être complété uniquement de façon à satisfaire $DP_a = L$, il suffit en effet de choisir pour les D derniers coefficients p_{iD} pour $i = 0$ à $D-1$, les valeurs

$$p_{iD} = (a^{-1})^{2^D} \left(l_i + \sum_{j=0}^{i-1} p_{ji} a^{2^j} + \sum_{j=i+1}^{D-1} p_{ij} a^{2^j} \right)$$

On peut vérifier que l_D est bien égal au coefficient correspondant de DP_a en utilisant l'annulation de L et DP_a en a. Finalement, le nombre de P tels que $DP_a = L$ est indépendant de a et L et le lemme s'en déduit. □

Lemme 15. *Soit a un élément non-nul de $\mathbb{F}_{2^n}$. Quand M est un polynôme $\mathbb{F}_2$-bilinéaire aléatoire de degré $\leq 2^D$ en la première variable, $M(a,\cdot)$ est un polynôme $\mathbb{F}_2$-linéaire aléatoire.*

Démonstration. Soit L un polynôme $\mathbb{F}_2$-linéaire de coefficients $l_0, \ldots, l_{n-1}$. Tout choix des coefficients m_{ij} pour $j < D$ peut être complété uniquement de façon à satisfaire $M(a,\cdot) = L$, il suffit de choisir pour les n derniers coefficients m_{iD} les valeurs

$$m_{iD} = (a^{-1})^{2^D} \left(l_i + \sum_{j=0}^{D-1} m_{ij} a^{2^j} \right)$$

Ainsi, pour tout L, le nombre de M tel que $M(a,\cdot)$ est indépendant de a et L et le lemme s'en déduit. □

Appliquant les lemmes 14 et 15, nous pouvons alors facilement montrer :

Proposition 1. *Soit a, b deux éléments de $\mathbb{F}_{2^n}$ avec a non-nul. On note $\mathcal{L}$ l'ensemble des polynômes $\mathbb{F}_2$-linéaires sur $\mathbb{F}_{2^n}$ et $\mathcal{L}^D$ le sous-espace de ceux de degré inférieur à 2^D. Un triplet $(P, M, \bar{P})$ choisi lors de la génération de clés de IPHFE définit la fonction :*

$$\ddot{P}(x,y) = P(x) + M(x,y) + \bar{P}(y)$$

Selon que b est nul ou non, la différentielle $D\ddot{P}$ de $\ddot{P}$ en (a,b) a la forme suivante :

i. Si $b = 0$: pour tout $\bar{P}$ et P, M aléatoires, $D\ddot{P}(x,y) = L(x) + \ell(y)$ où L est un élément aléatoire de $\mathcal{L}^D$ s'annulant en a et ℓ est aléatoire dans $\mathcal{L}$.

ii. Si $b \neq 0$: pour tout M et $P, \bar{P}$ aléatoires, $D\ddot{P}(x,y) = L(x) + \ell(y)$ où L et ℓ sont des éléments aléatoires respectivement dans $\mathcal{L}^D$ et $\mathcal{L}$ prenant la même valeur $M(a,b)$ resp. en a et b.

Démonstration. Si $b = 0$: La différentielle s'écrit $D\ddot{P}(x, y) = L(x) + \ell(y)$ avec $L(x) = DP_a(x)$ et $\ell(y) = M(a, y)$. D'après le lemme 14, quand P est choisi aléatoirement, L est un élément aléatoire de $\mathcal{L}^D$ s'annulant en a. D'après le lemme 15, quand M est choisi aléatoirement, ℓ est un élément aléatoire de $\mathcal{L}$.

Si $b \neq 0$: La différentielle s'écrit $D\ddot{P}(x, y) = L(x)+\ell(y)$ avec $L(x) = DP_a(x)+M(x, b)$ et $\ell(y) = M(a, y) + D\bar{P}_b(y)$. A M fixé, $M(x, b)$ est un élément fixé de $\mathcal{L}^D$. Utilisant le lemme 14, quand P est aléatoire, L est un élément aléatoire de $\mathcal{L}^D$ valant $M(a, b)$ en a. Toujours à M fixé, $M(a, y)$ est un élément fixé de $\mathcal{L}$. Utilisant le lemme 14 avec $D = n - 1$, quand $\bar{P}$ est aléatoire, ℓ est un élément aléatoire de $\mathcal{L}$ valant $M(a, b)$ en b. □

Les choix aléatoires de Z se divisent en deux classes selon que $Z(a) = 0$ ou non. Pour tout Z tel que $Z(a) = 0$, il résulte de la proposition 1 que pour tout $\bar{P}$ et P, M aléatoires, la différentielle de $\tilde{P}$ en a s'écrit : $D\tilde{P}_a = L + \ell \circ Z$, avec $L(a) = \ell \circ Z(a) = 0$. Dans l'autre cas, pour tout Z tel que $Z(a) \neq 0$, il résulte de la proposition 1 que pour tout M et $P, \bar{P}$ aléatoires, la différentielle de $\tilde{P}$ en a s'écrit : $D\tilde{P}_a = L + \ell \circ Z$, avec $L(a) = \ell \circ Z(a) = M(a, Z(a))$. Les deux lemmes suivants montrent que, dans les deux cas, l'application $\ell \circ Z$ est de noyau $\ker(Z)$ avec forte probabilité quand ℓ est aléatoire.

Le premier lemme établit la probabilité en question :

Lemme 16. *Soit Z une application linéaire de rang r.*

i. La proportion des applications linéaires ℓ vérifiant $\ker(\ell) \cap Im(Z) = \{0\}$ *est* $(1 - \alpha_{n,r})$ *avec* $\alpha_{n,r} = (2^r - 1)2^{-n} + \mathcal{O}(2^{-2n+r})$.

ii. La proportion des ℓ telles que $\ell \circ Z(a)$ prend une valeur non-nulle quelconque v_a vérifiant la condition précédente est $(1 - \alpha_{n,r})/(1 - 2^{-n})$.

Démonstration. La quantité $S(n, r)$, introduite à la section 2.1, est le nombre de suites linéairement indépendantes de longueur r : $S(n, r) = (2^n - 1) \dots (2^n - 2^r)$.

Une application linéaire ℓ vérifie $\ker(\ell) \cap Im(Z) = \{0\}$ si et seulement si $\ell(Im(Z))$ est de dimension r. Fixant une base $e_1, \dots, e_r$ de $Im(Z)$, ceci est encore équivalent à ce que la suite $\ell(e_1), \dots, \ell(e_r)$ soit linéairement indépendante. La proportion cherchée est donc :

$$S(n, r)/2^{nr} = \left(1 - 2^{-n}\right) \dots \left(1 - 2^{-n+r-1}\right) = 1 - (2^{r-1} + \dots + 1)2^{-n} + \mathcal{O}\left(2^{-2n+r}\right)$$

soit encore $1 - \alpha_{n,r}$ avec $\alpha_{n,r} = (2^r - 1)2^{-n} + \mathcal{O}(2^{-2n+r})$.

La condition $\ell \circ Z(a) = v_a$ est une contrainte linéaire non-triviale sur les coefficients de ℓ. Par conséquent, le nombre total des applications linéaires vérifiant cette condition est $2^{n(n-1)}$. Pouvant supposer $e_1 = Z(a)$, le nombre d'applications linéaires telles que $\ell(e_1) = v_a$ et $\ell(e_1), \dots, \ell(e_r)$ est linéairement indépendante est $S(n, r)2^{n(n-r)}/(2^n - 1)$. La proportion cherchée s'en déduit. □

Le second lemme établit la surjection uniforme cherchée :

Lemme 17. *Soit Z une application linéaire de rang r.*

i. Quand ℓ est une application linéaire aléatoire vérifiant $\ker(\ell) \cap Im(Z) = \{0\}$, alors $\ell \circ Z$ est une application linéaire aléatoire de noyau $\ker(Z)$.

ii. Quand ℓ est une application linéaire aléatoire vérifiant $\ker(\ell) \cap Im(Z) = \{0\}$ et $\ell \circ Z(a) = v_a$ pour une valeur v_a donnée, alors $\ell \circ Z$ est une application linéaire aléatoire de noyau $\ker(Z)$ valant v_a en a.

Démonstration. Pour toute application ℓ_r de noyau $\ker(Z)$, la condition $\ell \circ Z = \ell_r$ définit r contraintes linéaires sur les coefficients de ℓ. Quand $\ker(\ell) \cap Im(Z) = \{0\}$, ces contraintes sont linéairement indépendantes. Le nombre d'applications linéaires ℓ est $2^{n(n-r)}$, indépendamment du choix de ℓ_r. La seconde partie du lemme se montre pareillement. □

Nous pouvons maintenant conclure la preuve du théorème :

Cas où $\mathcal{K}$ contient a : La différentielle de $\tilde{P}$ en a s'écrit : $D\tilde{P}_a = L + \ell \circ Z$ où :

1. L est un polynôme $\mathbb{F}_2$-linéaire aléatoire de degré inférieur à 2^D s'annulant en a pour P aléatoire, et de degré exactement 2^D pour une proportion $(1 - 2^{-n})$ des choix aléatoires de P.
2. $\ell \circ Z$ est une application linéaire aléatoire de noyau $\ker(Z)$ pour une proportion $(1 - \alpha_{n,r})$ des choix aléatoires de M, et $\ker(Z) = \mathcal{K}$ est un sous-espace aléatoire contenant a pour tout choix aléatoire de Z avec $Z(a) = 0$.

Donc, pour une proportion $(1 - \epsilon_{n,r}) = (1 - 2^{-n})(1 - \alpha_{n,r})$ des choix aléatoires de $(P, M, \bar{P}, Z)$, nous avons :

$$\Pr\left[\dim \ker D\tilde{P}_a = t \,|\, a \in \mathcal{K}\right] = \Pr_{(L,\ell)}[\dim \ker(L + \ell) = t \,|\, L(a) = \ell(a) = 0]$$

où L est un polynôme $\mathbb{F}_2$-linéaire aléatoire de degré 2^D et ℓ est une application linéaire aléatoire de rang r.

Cas où $\mathcal{K}$ ne contient pas a : La différentielle s'écrit : $D\tilde{P}_a = L + \ell \circ Z$, où :

1. L est un polynôme $\mathbb{F}_2$-linéaire aléatoire de degré inférieur à 2^D prenant la valeur $M(a, Z(a))$ en a pour P aléatoire, et de degré exactement 2^D pour une proportion $(1 - 2^{-n})$ des choix aléatoires de P.
2. $\ell \circ Z$ est une application linéaire aléatoire de noyau $\ker(Z)$ et prenant la valeur $M(a, Z(a))$ en a pour une proportion $(1 - \alpha_{n,r})/(1 - 2^{-n})$ des choix aléatoires de $\bar{P}$.

La valeur commune $M(a, Z(a))$ est aléatoire pour M aléatoire, et non-nulle pour une proportion $(1 - 2^{-n})$ des choix aléatoires de M. Enfin, quand Z est aléatoire vérifiant $Z(a) \neq 0$, $\ker(Z) = \mathcal{K}$ est un sous-espace aléatoire ne contenant pas a.

Donc, pour une proportion $(1-2^{-n})^2(1-\alpha_{n,r})/(1-2^{-n}) = (1-\epsilon_{n,r})$ des choix aléatoires de $(P, M, \bar{P}, Z)$, nous avons :

$$\Pr\left[\dim\ker D\tilde{P}_a = t \,|\, a \notin \mathcal{K}\right] = \Pr_{(L,\ell)}[\dim\ker(L+\ell) = t \,|\, L(a) = \ell(a) \neq 0]$$

où L est un polynôme $\mathbb{F}_2$-linéaire aléatoire de degré 2^D et ℓ est une application linéaire aléatoire de rang r.

9.4 Distribution différentielle de IPHFE

À la section précédente, nous avons établi que pour tout élément a, la proportion des clés secrètes $(P, M, \bar{P}, Z)$ telles que la différentielle en a ait un noyau de dimension t est, respectivement quand a est dans ou hors du noyau $\mathcal{K}$ de Z, et à des termes négligeables près :

$$\pi^+(t) = \Pr_{(L,\ell)}[\dim\ker(L+\ell) = t \,|\, L(a) = \ell(a) = 0]$$
$$\pi^-(t) = \Pr_{(L,\ell)}[\dim\ker(L+\ell) = t \,|\, L(a) = \ell(a) \neq 0]$$

où ces deux probabilités sont prises sur les couples (L, ℓ) avec L un polynôme $\mathbb{F}_2$-linéaire de degré 2^D et ℓ une application linéaire de rang r. Dans cette section, nous montrons comment calculer effectivement les distributions π^+ et π^-. Précisons que dans les définitions de π^+ et π^-, l'élément a désigne un élément quelconque non nul.

Comme première étape de calcul, nous considérons la distribution :

$$\pi(t) = \Pr_{(L,\ell)}[\dim\ker(L+\ell) = t]$$

de laquelle les distributions π^+ et π^- diffèrent par leur contrainte respective en a. La dimension du noyau de $L+\ell$ dépend de la dimension i de $\ker(L) \cap \ker(\ell)$, qui lui-même dépend de la dimension d de $\ker(L)$. Rappelons que comme L est $\mathbb{F}_2$-linéaire de degré 2^D, la dimension d de son noyau est au plus D. La probabilité que le noyau de $L+\ell$ soit de dimension t à i et d donnés est notée $\pi_{d,i}(t)$:

$$\pi_{d,i}(t) = \Pr_{(L,\ell)}\left[\dim\ker(L+\ell) = t \,;\, \left\{ \begin{array}{l} \dim\ker(L) = d \\ \dim(\ker(L)\cap\ker(\ell)) = i \end{array} \right.\right] \tag{9.1}$$

et la probabilité $\pi(t)$ s'obtient en sommant sur toutes les valeurs possibles de i et d :

$$\pi(t) = \sum_{d=0}^{D}\sum_{i=0}^{d}\pi_{d,i}(t)$$

Le calcul de la probabilité $\pi_{d,i}(t)$ est détaillé à la section 2.3, nous en rappelons brièvement le principe. Pour une fonction L donnée, la proportion d'applications linéaires ℓ de rang r satisfaisant les conditions voulues est indépendante du choix de cette même fonction L. Notant $\lambda_{d,i}(t)$ cette proportion, et $\Lambda_D(d)$ la proportion de polynômes $\mathbb{F}_2$-linéaires de degré 2^D dont le noyau est de dimension d, nous

avons : $\pi_{d,i}(t) = \Lambda_D(d).\lambda_{d,i}(t)$. La proportion $\Lambda_D(d)$ se calcule en remarquant que l'annulation sur un espace de dimension d donné d'un polynôme $\mathbb{F}_2$-linéaire de degré 2^D s'écrit comme d contraintes linéaires indépendantes sur les D coefficients dans $\mathbb{F}_{2^n}$ le définissant. La proportion $\lambda_{d,i}(t)$ se calcule en fixant une application L, calculant la probabilité qu'un espace G de dimension $n-r$ intersecte $\ker(L)$ avec dimension i, puis calculant le nombre d'applications ℓ de noyau G tel que le noyau de $L+\ell$ soit de dimension t. Cette dernière quantité est l'objet d'un calcul assez avancé, que nous ne commentons pas ici.

Déterminer les distributions π^+ et π^- consiste à refaire l'énumération précédente en tenant compte des contraintes respectives en a : par exemple, pour $\pi^+_{d,i}$, nous calculons la proportion $\Lambda^+_D(d)$ de polynômes $\mathbb{F}_2$-linéaires de degré 2^D s'annulant en a dont le noyau est de dimension d, puis la proportion $\lambda^+_{d,i}(t)$ des applications linéaires ℓ dont le noyau G contient a vérifiant les conditions voulues. À d et i fixés, il est possible d'extraire des facteurs correctifs dans chaque cas, donnés par la proposition suivante :

Proposition 2. *Soit $\pi_{d,i}(t)$ la probabilité donnée par l'équation 9.1 où L est un polynôme $\mathbb{F}_2$-linéaire aléatoire de degré 2^D et ℓ est une application linéaire aléatoire de rang r. Pour tout élément non-nul a, les probabilités $\pi^+_{d,i}(t)$ et $\pi^-_{d,i}(t)$ du même événement pris sur les couples (L,ℓ) vérifiant respectivement $L(a)=\ell(a)=0$ et $L(a)=\ell(a)\neq 0$ sont :*

$$\begin{aligned}\pi^+_{d,i}(t) &= (2^i-1)2^r(1+\epsilon_{n,r}).\pi_{d,i}(t)\\ \pi^-_{d,i}(t) &= (2^t-2^i)/(1-2^{-r}).\pi_{d,i}(t)\end{aligned}$$

où $\epsilon_{n,r} = 2^{-n+r} + \mathcal{O}(2^{-2n+2r})$, en moyenne sur a.

La preuve de la proposition détaille les modifications apportées au calcul de la distribution $\pi_{d,i}$ proposé à la section 2.3 ; nous l'isolons dans la sous-section 9.4.1 suivante, qui peut être omise en première lecture. Notons toutefois que le résultat de la proposition traduit une certaine intuition : quand $L(a)=\ell(a)=0$, a est un élément non-nul de l'intersection des deux noyaux qui a dimension i, d'où l'extraction du facteur (2^i-1) ; quand $L(a)=\ell(a)\neq 0$, a est un élément du noyau de $L+\ell$ (de dimension t) mais qui n'est pas dans l'intersection des deux noyaux (de dimension i), d'où le facteur (2^t-2^i). Quant aux facteurs 2^r et $1/(1-2^{-r})$, ce sont les inverses des probabilités d'appartenance et non-appartenance à $\mathcal{K} = \ker \ell$.

Utilisant les formules donnant $\pi_{d,i}(t)$ à la section 2.3 et négligeant les termes d'ordre 2^{-n+r}, nous pouvons en déduire les valeurs de $\pi^+(t)$ et $\pi^-(t)$:

$$\begin{aligned}\pi^+(t) &= \tfrac{1}{2^{-r}} \cdot \textstyle\sum_{d=0}^{D}\sum_{i=0}^{d}(2^i-1)\pi_{d,i}(t)\\ \pi^-(t) &= \tfrac{1}{1-2^{-r}} \cdot \textstyle\sum_{d=0}^{D}\sum_{i=0}^{d}(2^t-2^i)\pi_{d,i}(t)\end{aligned}$$

La table ci-dessous rapporte les valeurs de π^+ et π^- pour les paramètres recommandés $(n, D, r) = (89, 3, 2)$ pour IPHFE :

dimension t	π^+	π^-	signe$(\pi^+ - \pi^-)$
1	$\simeq 0.57764$	$\simeq 0.57756$	$+$
2	$\simeq 0.38495$	$\simeq 0.38507$	$-$
3	$\simeq 0.036718$	$\simeq 0.036662$	$+$
4	$\simeq 0.00069427$	$\simeq 0.00070045$	$-$
5	$\simeq 0.0000025431$	$\simeq 0.0000029064$	$-$

Comme on peut le constater, la valeur de $\pi^+(t)$ est supérieure à celle de $\pi^-(t)$ pour les dimensions 1 et 3. Revenant à l'interprétation de π^+ et π^- en terme de clés IPHFE, il en résulte que si la différentielle en a a un noyau de dimension $t = 1$ ou 3, il est plus probable que le noyau de perturbation $\mathcal{K} = \ker(Z)$ contienne a pour une clé $(P, M, \bar{P}, Z)$ aléatoire que l'événement contraire. À la section 9.5, nous en déduisons un distingueur d'éléments de $\mathcal{K}$ et calculons son avantage.

9.4.1 Preuve de la proposition 2

La preuve de la proposition 2 consiste en des modifications des calculs présentés à la section 2.3 et est construite en référence à ceux-ci ; elle peut être omise en première lecture.

Facteurs correctifs lorsque L et ℓ s'annulent tout deux en a

Modification du lemme 3 : Le nombre de polynômes $\mathbb{F}_2$-linéaires de degré 2^D s'annulant en a est $(2^n-1)2^{n(D-1)}$. Par ailleurs, une proportion $(2^d-1)/(2^n-1)$ des sous-espaces de dimension d de $(\mathbb{F}_2)^n$ contient a et une proportion $(2^d-1)/(2^m-1)$ des sous-espaces de dimension d contenus dans un sous-espace de dimension m contenant a contiennent eux-mêmes a. Donc la proportion $\Lambda_D^+(d)$ des polynômes $\mathbb{F}_2$-linéaires de degré 2^D ayant un noyau de dimension d contenant a satisfait le système triangulaire inversible suivant :

$$d \in [1, D], \quad E(n, d)2^{-nd} = \sum_{m=d}^{D} E(m, d)(1 - 2^{-n})\frac{\Lambda_D^+(m)}{2^m - 1}$$

Les quantités $(1 - 2^{-n})/(2^m - 1)\Lambda_D^+(m)$ satisfont le même système inversible que les probabilités $\Lambda_D(1), \ldots, \Lambda_D(D)$; nous en déduisons qu'elles sont égales :

$$d \in [1, D], \quad \Lambda_D^+(d) = \frac{(2^d - 1)}{(1 - 2^{-n})}\Lambda_D(d) \tag{9.2}$$

Modification du lemme 2 : Soit L un polynôme $\mathbb{F}_2$-linéaire de degré 2^D de noyau F de dimension d. Comme F contient a par hypothèse, les sous-espaces

contenant a ayant une intersection de dimension i avec F sont ceux dont l'intersection avec F contient a ; parmi les sous-espaces de dimension i de F, ceux contenant a sont en proportion $(2^i-1)/(2^d-1)$. Enfin, parmi les sous-espaces de dimension $n-r$, ceux contenant a sont une proportion $(2^{n-r}-1)/(2^n-1)$. La proportion $p_d^+(i)$ des sous-espaces de dimension $n-r$ contenant a qui ont une intersection de dimension i avec F est donc :

$$p_d^+(i) = \frac{(2^i-1)(2^n-1)}{(2^d-1)(2^{n-r}-1)} p_d(i) \tag{9.3}$$

où $p_d(i)$ est la proportion de sous-espaces de dimension $n-r$ qui ont une intersection de dimension i avec F.

Modification du lemme 6 : Soit G un sous-espace de dimension $n-r$ contenant a et d'intersection de dimension i avec F. Le nombre de sous-espaces H de dimension t tels que $H \cap F = H \cap G = F \cap G$ ne dépend pas des éléments de $F \cap G$ tel a. La proportion résultante reste donc inchangée.

Modification du lemme 7 : Le nombre de sous-espaces d'une certaine dimension vérifiant $H \cap F = H \cap G = F \cap G$ n'étant pas affecté pour a dans $F \cap G$, ce dénombrement reste également inchangé :

$$p_{d,i}^+(t) = p_{d,i}(t) \tag{9.4}$$

Facteur global Utilisant les équations (9.2), (9.3) et (9.4), nous avons :

$$\pi_{d,i}^+(t) = \Lambda_D^+(d).p_d^+(i).p_{d,i}^+(t) = (2^i-1)2^r \frac{1}{(1-2^{-n+r})} \Lambda_D(d).p_d(i).p_{d,i}(t)$$

où nous reconnaissons $\pi_{d,i}(t) = \Lambda_D(d).p_d(i).p_{d,i}(t)$.

Facteurs correctifs lorsque ni L ni ℓ ne s'annulent en a

Modification du lemme 3 : Parmi les polynômes $\mathbb{F}_2$-linéaires de degré 2^D, ceux qui ne s'annulent pas en a sont en proportion $(1-2^{-n})$. Le nombre de polynômes $\mathbb{F}_2$-linéaires de degré 2^D ayant un noyau de dimension d est $(2^n-1)2^{nD}\Lambda_D(d)$ et le nombre de ceux s'annulant en a est $(2^n-1)2^{n(D-1)}\Lambda_D^+(d)$. La proportion des polynômes $\mathbb{F}_2$-linéaires de degré 2^D ne s'annulant pas en a dont le noyau est de dimension d est donc :

$$\Lambda_D^-(d) = \frac{(2^n-1)2^{nD}(1-(2^d-1)/(2^n-1))\Lambda_D(d)}{(2^n-1)2^{nD}(1-2^{-n})} = \frac{2^n(2^n-2^d)}{(2^n-1)^2}\Lambda_D(d) \tag{9.5}$$

Modification du lemme 2 : Soit L un polynôme $\mathbb{F}_2$-linéaire de degré 2^D de noyau F de dimension d ne contenant pas a. Pour tout sous-espace I de dimension i de F, la proportion des sous-espaces de dimension $n-r$ qui sont d'intersection I avec F et contiennent a sont une proportion $(2^{n-r}-1)/(2^n-2^d)$ et ceux ne contenant pas a sont la proportion complémentaire. De même, parmi tous les sous-espaces de dimension $n-r$, ceux contenant a sont une proportion $(2^{n-r}-1)/(2^n-1)$ et ceux qui ne contiennent pas a sont la proportion complémentaire. Par conséquent, la proportion des sous-espaces de dimension $n-r$ ne contenant pas a ayant une intersection avec F de dimension i est :

$$p_d^-(i) = \frac{(2^n - 2^{n-r} - 2^d + 2^i)}{(2^n - 2^d)} \frac{(2^n - 1)}{(2^n - 2^{n-r})} p_d(i) \tag{9.6}$$

Modification du lemme 6 : Soit G un sous-espace de dimension $n-r$ ne contenant pas a ayant une intersection de dimension i avec F, lui-même ne contenant pas a. Nous énumérons le nombre de sous-espaces H de dimension t contenant a et tels que $H \cap F = H \cap G = F \cap G$. Comme pour le lemme 2.3.1, nous comptons d'abord le nombre de sous-espaces J de $F+G$ de dimension j vérifiant la condition précédente, puis nous comptons le nombre de sous-espaces H de dimension t dont l'intersection avec $F+G$ est J. Toutefois, nous voyons qu'en fonction de la position de a relativement à $F+G$, le calcul est différemment affecté.

1. Si a est dans $(F+G) \setminus (F \cap G)$ **:** seul le premier dénombrement est affecté ; le nombre de sous-espace J de $F+G$ de dimension j contenant a et tels que $J \cap F = J \cap G = F \cap G$ est le nombre de sous-espaces $\bar{J}$ de dimension $j-i$ contenant $\bar{a}$ et tels que $\bar{J} \cap \bar{F} = \bar{J} \cap \bar{G} = \{0\}$ dans l'espace quotienté par $F \cap G$. Parmi les suites linéairement indépendantes de longueur $j-i$ générant un espace d'intersection $\{0\}$ avec $\bar{F}$ et $\bar{G}$, celles contenant $\bar{a}$ sont une fraction $(2^{d-i}-1)^{-1}(2^{n-r-i}-1)^{-1}$. Par ailleurs, parmi les suites engendrant un même sous-espace de dimension $j-i$, celles contenant $\bar{a}$ sont une fraction $(2^{j-i}-1)^{-1}$. Notant $E_{d,i}(j,t)$ le nombre de sous-espaces H de dimension t dont l'intersection avec $F+G$ est de dimension j et vérifiant $H \cap F = H \cap G = F \cap G$, le nombre de tels sous-espaces contenant un élément a de $(F+G) \setminus (F \cap G)$ est :

$$\frac{(2^{j-i}-1)}{(2^{d-i}-1)(2^{n-r-i}-1)} E_{d,i}(j,t)$$

2. Si a n'est pas dans $F+G$: seul le second dénombrement est affecté ; pour tout sous-espace J de $F+G$ de dimension j vérifiant $J \cap F = J \cap G = F \cap G$, la proportion des sous-espaces H contenant a parmi ceux de dimension t et d'intersection J avec $F+G$ (la condition $H \cap F = H \cap G = F \cap G$ étant alors vérifiée) est $(2^t - 2^j)/(2^n - 2^{n-r+d-i})$. Le nombre cherché est donc :

$$\frac{(2^t - 2^j)}{(2^n - 2^{n-r+d-i})} E_{d,i}(j,t)$$

Par ailleurs, le nombre d'éléments de $(F+G)\backslash(F\cap G)$ est $2^i(2^{d-i}-1)(2^{n-r-i}-1)$ et le nombre d'éléments hors de $F+G$ est $(2^n-2^{n-r+d-i})$. Donc, en moyenne sur l'ensemble des points a hors de F et G, la proportion de sous-espaces H contenant a parmi ceux de dimension t, d'intersection de dimension j avec $F+G$ et vérifiant $H\cap F = H\cap G = F\cap G$ est :

$$E^-_{d,i}(j,t) = \frac{(2^t-2^i)}{(2^n-2^{n-r}-2^d+2^i)} E_{d,i}(j,t)$$

Le nombre total de sous-espaces H de dimension t et $H\cap F = H\cap G = F\cap G$ et contenant a s'obtient en sommant sur toutes les valeurs j :

$$E^-_{d,i}(t) = \sum_{j=i}^{d} E^-_{d,i}(j,t)$$

Modification du lemme 7 : Parmi les applications linéaires ℓ de noyau G, celles pour lesquelles le noyau de $L+\ell$ contient un élément a hors de F et G sont une fraction $1/(2^n-1)$. Par ailleurs, la proportion de sous-espaces contenant a parmi les sous-espaces de dimension t contenant $F\cap G$ dans un sous-espace de dimension m contenant $F\cap G$ et a est $(2^t-2^i)/(2^m-2^i)$. Finalement, parmi les applications linéaires ℓ de noyau G telles que le noyau de $L+\ell$ contienne un élément aléatoire a en dehors de F et G, la proportion $p^-_{d,i}(t)$ de celles pour lesquelles le noyau de $L+\ell$ est de dimension t satisfait le système triangulaire inversible suivant :

$$t\in[i,r+i],\quad \frac{E_{d,i}(t)}{S(n,t-i)} = \sum_{m=t}^{r+i} E(m,t)\frac{S(t,i)}{S(m,i)}\left[\frac{(2^n-2^{n-r}-2^d+2^i)}{(2^n-1)(2^m-2^i)}\,p^-_{d,i}(t)\right]$$

Les quantités entre crochets vérifient le même système inversible que les probabilités $p_{d,i}(t)$ déterminées par le lemme 7 ; nous en déduisons qu'elles sont égales :

$$p^-_{d,i}(t) = \frac{(2^n-1)(2^t-2^i)}{(2^n-2^{n-r}-2^d+2^i)}\,p_{d,i}(t) \tag{9.7}$$

Facteur global Utilisant les équations (9.5), (9.6) et (9.7), nous avons :

$$\pi^-_{d,i}(t) = \Lambda^-_D(d).p^-_d(i).p^-_{d,i}(t) = \frac{(2^t-2^i)}{(1-2^{-r})}\Lambda_D(d).p_d(i).p_{d,i}(t)$$

où nous reconnaissons $\pi_{d,i}(t) = \Lambda_D(d).p_d(i).p_{d,i}(t)$.

9.5 Un distingueur d'éléments du noyau

Sur la base du calcul des distributions π^+ et π^- effectué à la section précédente, nous pouvons définir un distingueur d'éléments du noyau de la perturbation.

Définition du distingueur

Soit $\tilde{\boldsymbol{P}}$ la clé publique d'une instance donnée $(P, M, \bar{P}, Z)$ de IPHFE, et soit $\boldsymbol{\mathcal{K}}$ le sous-espace isomorphe à $\mathcal{K} = \ker(Z)$ par le masquage linéaire S. Pour un élément non-nul a choisi aléatoirement, nous calculons la dimension du noyau de la différentielle de $\tilde{\boldsymbol{P}}$ et a et trouvons la valeur t. Si pour cette dimension t nous avons $\pi^+(t) > \pi^-(t)$, alors la proportion des clés $(P, M, \bar{P}, Z)$ pour lesquelles a est dans $\boldsymbol{\mathcal{K}}$ est supérieure à celle des clés pour lesquelles a n'est pas dans $\mathcal{K}$, et nous devons donc supposer que a est dans $\boldsymbol{\mathcal{K}}$ pour la clé inconnue $(P, M, \bar{P}, Z)$ donnée. Suivant ce raisonnement, nous définissons la fonction :

$$T : \begin{cases} T(a) = 1, \text{ si } \dim\ker(D\tilde{\boldsymbol{P}}_a) = t \text{ avec } \pi^+(t) > \pi^-(t) \\ T(a) = 0, \text{ si } \dim\ker(D\tilde{\boldsymbol{P}}_a) = t \text{ avec } \pi^+(t) < \pi^-(t) \end{cases}$$

T est notre distingueur d'éléments de $\boldsymbol{\mathcal{K}}$; nous calculons maintenant son avantage.

Avantage du distingueur

L'avantage de T pour un élément a aléatoire non-nul et une une clé $(P, M, \bar{P}, Z)$ aléatoire est par définition :

$$Adv = |\Pr[T(a) = 1 | a \in \boldsymbol{\mathcal{K}}] - \Pr[T(a) = 1 | a \notin \boldsymbol{\mathcal{K}}]|$$

La différence entre valeur absolue se développe en :

$$\sum_{t:\pi^+(t)>\pi^-(t)} \Pr\left[\dim\ker(D\tilde{\boldsymbol{P}}_a) = t \,|\, a \in \boldsymbol{\mathcal{K}}\right] - \Pr\left[\dim\ker(D\tilde{\boldsymbol{P}}_a) = t \,|\, a \notin \boldsymbol{\mathcal{K}}\right]$$

Les termes de la somme valent $\pi^+(t) - \pi^-(t)$ selon la théorème 3 (à des termes négligeables près) et sont positifs pour les valeurs de t considérées. Finalement, l'avantage de T s'écrit :

$$Adv = \sum_{t:\pi^+(t)>\pi^-(t)} \pi^+(t) - \pi^-(t)$$

ou encore :

$$Adv = \frac{1}{2} \sum_t \left|\pi^+(t) - \pi^-(t)\right|$$

La table ci-dessous fournit les valeurs de Adv pour plusieurs choix de paramètres. Les valeurs en gras correspondent aux paramètres recommandés pour IPHFE. Comme nous pouvons le remarquer, l'avantage est environ deux fois plus sensible à l'augmentation du paramètre D qu'à celle du paramètre r.

TAB. 9.1 – Avantage du distingueur en fonction des paramètres IPHFE

(n, D, r)	$-\log_2(Adv)$	(n, D, r)	$-\log_2(Adv)$	(n, D, r)	$-\log_2(Adv)$
$(89, 2, 2)$	7.49	**(89,3,2)**	**12.95**	$(89, 4, 2)$	19.66
$(89, 2, 3)$	9.73	$(89, 3, 3)$	16.17	$(89, 4, 3)$	23.87
$(89, 2, 4)$	11.84	$(89, 3, 4)$	19.28	$(89, 4, 4)$	27.97

9.6 La reconstruction du noyau

Dans cette section, nous montrons comment extraire du distingueur précédent une information sûre quant à l'appartenance ou non d'un élément donné. La technique mise en œuvre est une généralisation de celle proposée pour l'attaque contre PMI [40] ; elle consiste à tirer parti d'un comportement moyen différent du distingueur vis-à-vis de la linéarité selon l'appartenance ou non des éléments sommés au noyau de la perturbation $\boldsymbol{\mathcal{K}}$. Tester sur une large assemblée de points la clôture par linéarité du distingueur vis-à-vis d'un élément donné fournit une probabilité d'appartenance à $\boldsymbol{\mathcal{K}}$ de cet élément qui tend vers 0 quand celui-ci n'est pas dans $\boldsymbol{\mathcal{K}}$.

9.6.1 Comportement du distingueur vis-à-vis de la linéarité

L'ensemble $\boldsymbol{\mathcal{K}}$ possède une propriété que son complémentaire ne possède pas : il est clos par linéarité. Ainsi, lorsque x est dans $\boldsymbol{\mathcal{K}}$, tout y et $x + y$ doivent être tous les deux dans $\boldsymbol{\mathcal{K}}$ ou tous les deux hors de $\boldsymbol{\mathcal{K}}$, alors qu'il peut en être différemment lorsque x n'est pas dans $\boldsymbol{\mathcal{K}}$. Par analogie, la probabilité pour un élément aléatoire y, que y et $x + y$ soient détectés tous deux dans $\boldsymbol{\mathcal{K}}$ ou tous deux hors de $\boldsymbol{\mathcal{K}}$ par le distingueur T doit être supérieure en moyenne sur les éléments x de $\boldsymbol{\mathcal{K}}$ que sur ceux qui ne sont pas dans $\boldsymbol{\mathcal{K}}$.

Pour tout élément y, on note μ_y^+ la probabilité que $T(x + y) = T(y)$ quand x est dans $\boldsymbol{\mathcal{K}}$ et μ_y^- la même probabilité quand x n'est pas dans $\boldsymbol{\mathcal{K}}$.

$$\begin{aligned} \mu_y^+ &= \Pr_x[\, T(x+y) = T(y) \,|\, x \in \boldsymbol{\mathcal{K}} \,] \\ \mu_y^- &= \Pr_x[\, T(x+y) = T(y) \,|\, x \notin \boldsymbol{\mathcal{K}} \,] \end{aligned}$$

Les valeurs moyennes de μ_y^+ et μ_y^- sur tous les éléments y sont notées μ^+ et μ^-.

$$\begin{aligned} \mu^+ &= \Pr_{x,y}[\, T(x+y) = T(y) \,|\, x \in \boldsymbol{\mathcal{K}} \,] \\ \mu^- &= \Pr_{x,y}[\, T(x+y) = T(y) \,|\, x \notin \boldsymbol{\mathcal{K}} \,] \end{aligned} \tag{9.8}$$

Suivant notre raisonnement précédent, nous attendons un écart positif entre les valeurs de μ^+ et μ^-. La moyenne de cet écart sur les clés est donnée par la proposition suivante.

Proposition 3. *L'écart entre les probabilités μ^+ et μ^- données par l'équation (9.8) est, en moyenne sur les clés $(P, M, \bar{P}, Z)$:*

$$\Delta\mu = \mu^+ - \mu^- = 2.\frac{Adv^2}{2^r}$$

à des termes d'ordre $2^{-n+\max\{2D,r\}}$ près.

Une preuve simplifiée est présentée à la section suivante ; la preuve complète se trouve à l'appendice A. La suite de l'attaque est décrite à la section 9.6.3.

9.6.2 Preuve simplifiée de la proposition 3

Nous présentons ici une preuve simple de l'écart entre les deux probabilités μ^+ et μ^- basée sur une hypothèse d'uniformité. L'intuition est que cette hypothèse d'uniformité est satisfaite en moyenne sur les clés (à des termes négligeables près). Une preuve rigoureuse de ce résultat est donnée à l'appendice A.

En plus des probabilités μ^+ et μ^-, on définit la probabilité :

$$\mu = \Pr_{x,y}[T(x+y) = T(y)]$$

Notant $\beta = 2^{-r}$ la probabilité qu'un élément aléatoire appartienne à $\mathcal{K}$, les trois probabilités vérifient la relation : $\mu = \beta\mu^+ + (1-\beta)\mu^-$. Nous calculons d'abord μ et μ^+, puis nous en déduisons μ^- et $\mu^+ - \mu^-$.

Calcul de μ : La probabilité μ se scinde en $\mu_0 + \mu_1$ selon la valeur commune de $T(x+y)$ et $T(y)$. Quand x et y sont aléatoires, $x+y$ et y sont indépendants et :

$$\mu_1 = \Pr_{x,y}[T(x+y) = 1; T(y) = 1] = \alpha^2$$

où $\alpha = \Pr_y[T(y) = 1]$. De même, $\mu_0 = (1-\alpha)^2$, et finalement

$$\mu = 1 - 2\alpha + 2\alpha^2 \tag{9.9}$$

Calcul de μ^+ : Comme précédemment, μ^+ se scinde en $\mu_0^+ + \mu_1^+$ selon la valeur commune de $T(x+y)$ et $T(y)$. Soit γ la proportion des éléments y qui sont à la fois dans $\mathcal{K}$ et satisfont $T(y) = 1$. Pour chaque tel élément y, l'application $x \mapsto x + y$ est une permutation de $\mathcal{K}$ et donc la proportion des éléments x de $\mathcal{K}$ pour lesquels $T(x) = 1$ est γ/β. La proportion des éléments y qui ne sont pas dans $\mathcal{K}$ et tels que $T(y) = 1$ est $\alpha - \gamma$. Pour chaque tel élément y, l'application $x \mapsto x + y$ est une bijection de $\mathcal{K}$ vers le sous-espace affine $y + \mathcal{K}$. Malheureusement, la proportion des éléments de $y+\mathcal{K}$ pour lesquels $T = 1$ est une inconnue dépendant de y. Nous allons toutefois *supposer que cette valeur est indépendante de y*. Intuitivement, lorsque l'on fait varier les coefficients de la clé secrète, chaque élément y hors de $\mathcal{K}$ est équivalent à un autre, et cette hypothèse d'uniformité doit donc être satisfaite en moyenne sur les clés de noyau $\mathcal{K}$. Toutefois, comme les probabilités que $T(x+y) = 1$ et

$T(y) = 1$ dépendent toutes deux de T qui lui-même dépend de la clé secrète, il est nécessaire pour être rigoureux d'étudier d'abord la distribution jointe pour une clé secrète aléatoire, *puis* de considérer cette probabilité en fonction de x et y ; nous renvoyons le lecteur à l'appendice A pour les détails. *Sous l'hypothèse considérée*, comme les éléments de $y + \mathcal{K}$ sont une proportion $\beta/(1-\beta)$ du complémentaire de $\mathcal{K}$, la proportion des éléments de $y + \mathcal{K}$ pour lesquels $T = 1$ est $(\alpha - \gamma)\beta/(1-\beta)$. Finalement, nous obtenons :

$$\mu_1^+ = \frac{1}{\beta}\gamma^2 + \frac{1}{1-\beta}(\alpha - \gamma)^2$$

De même, nous trouvons :

$$\mu_0^+ = \frac{1}{\beta}(\beta - \gamma)^2 + \frac{1}{1-\beta}(1 - \beta - (\alpha - \gamma))^2$$

Après quelques simplifications, nous obtenons :

$$\mu^+ = 1 - 2\alpha + 2\left(\frac{\gamma^2}{\beta} + \frac{(\alpha-\gamma)^2}{1-\beta}\right) \tag{9.10}$$

Par ailleurs, l'avantage Adv s'écrit en fonction de α, β et γ :

$$Adv = |\Pr_x[T(x) = 1 | x \in \mathcal{K}] - \Pr_x[T(x) = 1 | x \notin \mathcal{K}]| = \left|\frac{\gamma}{\beta} - \frac{\alpha - \gamma}{1-\beta}\right|$$

Élevant au carré, on peut aisément vérifier :

$$\beta(1-\beta)Adv^2 = \frac{\gamma^2}{\beta} + \frac{(\alpha-\gamma)^2}{1-\beta} - \alpha^2$$

À partir des expressions (9.9) et (9.10) de μ et μ^+, nous en déduisons alors :

$$\mu^+ = \mu + 2\beta(1-\beta)Adv^2$$

De la relation entre μ, μ^+ et μ^-, nous obtenons $\mu^- = \mu - 2\beta^2 Adv^2$ et finalement :

$$\mu^+ - \mu^- = 2\beta Adv^2$$

9.6.3 Construire un test fiable d'appartenance au noyau

Pour tout élément y, on définit la variable aléatoire $\delta_y(x)$ valant 1 quand x vérifie $T(x + y) = T(y)$ et 0 sinon. La valeur moyenne de δ_y sur $\boldsymbol{\mathcal{K}}$ est μ_y^+ et sa valeur moyenne sur le complémentaire de $\boldsymbol{\mathcal{K}}$ est μ_y^-.

Définition du test : Pour tous N éléments distincts quelconques $y_1, \ldots, y_N$, nous définissons la variable aléatoire :

$$S_N(x) = \sum_{i=1}^{N} \delta_{y_i}(x)$$

Pour toute variable aléatoire S_N ainsi définie, on définit un test d'appartenance à $\boldsymbol{\mathcal{K}}$ de la façon suivante. Étant donné un élément x, on calcule la valeur de $S_N(x)$; si $S_N(x) \geq N\mu^+$, le test répond `oui`, et `non` sinon.

L'intention à l'origine de ce test est la suivante. Comme $\delta_{y_i}(x)$ vaut plus probablement 1 quand x est dans $\boldsymbol{\mathcal{K}}$ que quand x n'est pas dans $\boldsymbol{\mathcal{K}}$, on s'attend à une plus grande valeur de $S_N(x)$ quand x est dans $\boldsymbol{\mathcal{K}}$ que quand x n'est pas dans $\boldsymbol{\mathcal{K}}$. Quand N croît, on s'attend à ce que l'intersection entre les valeurs de S_N sur $\boldsymbol{\mathcal{K}}$ et les valeurs de S_N sur $\boldsymbol{\mathcal{K}}$ diminue. Finalement, pour N suffisamment grand, on s'attend à ce que la probabilité que $S_N(x) \geq N\mu^+$ soit élevée lorsque x est dans $\boldsymbol{\mathcal{K}}$ et très faible lorsque x n'est pas dans $\boldsymbol{\mathcal{K}}$.

Analyse du test : Considérons d'abord la variable S_N sur $\boldsymbol{\mathcal{K}}$. Pour tout y_i, la valeur moyenne de δ_{y_i} sur $\boldsymbol{\mathcal{K}}$ est $\mu^+_{y_i}$. Cette dernière valeur n'est pas connue, toutefois nous savons qu'elle suit une distribution de valeur moyenne μ^+ quand y_i est aléatoire. De même, la valeur moyenne de S_N sur $\boldsymbol{\mathcal{K}}$, notée A^+_N, suit une distribution sur les N-uplets $(y_1, \ldots, y_N)$ de valeur moyenne $N\mu^+$. Ainsi, pour la moitié des choix d'un N-uplet $(y_1, \ldots, y_N)$, nous avons $A^+_N \geq N\mu^+$. Quand ceci est vérifié, nous avons :

$$\Pr_x \left[S_N(x) \geq N\mu^+ \,|\, x \in \boldsymbol{\mathcal{K}} \right] \geq \Pr_x \left[S_N(x) \geq A^+_N \,|\, x \in \boldsymbol{\mathcal{K}} \right] = \frac{1}{2}$$

Donc, pour au moins la moitié des choix d'un N-uplet $(y_1, \ldots, y_N)$, plus de la moitié des éléments de $\boldsymbol{\mathcal{K}}$ passera le test, quelle que soit la valeur de N.

Considérons maintenant S_N sur le complémentaire de $\boldsymbol{\mathcal{K}}$. Nous voulons trouver une valeur de N pour laquelle la probabilité qu'un élément du complémentaire de $\boldsymbol{\mathcal{K}}$ passe le test soit très faible. Nous pouvons remarquer comme précédemment, que la valeur moyenne de S_N sur le complémentaire de $\boldsymbol{\mathcal{K}}$, notée A^-_N, suit une distribution sur les N-uplets $(y_1, \ldots, y_N)$ de valeur moyenne $N\mu^-$. Par conséquent, pour la moitié des choix d'un N-uplet $(y_1, \ldots, y_N)$, nous avons $A^-_N \leq N\mu^-$. Quand ceci est vérifié, nous avons :

$$\Pr_x \left[S_N(x) \geq N\mu^+ \,|\, x \notin \boldsymbol{\mathcal{K}} \right] \leq \Pr_x \left[S_N(x) - A^-_N \geq N\Delta\mu \,|\, x \notin \boldsymbol{\mathcal{K}} \right] \tag{9.11}$$

où $\Delta\mu = \mu^+ - \mu^-$, et notre but est maintenant de majorer la probabilité de droite.

Observons que quand les y_i sont choisis aléatoirement, les variables aléatoires δ_{y_i} sont indépendantes entre elles. Les suites de variables aléatoires binaires, indépendantes, non-identiquement distribuées sont connues dans la littérature sous le nom

d'épreuves de Poisson (« Poisson trials » dans la littérature anglophone). Nous pouvons alors appliquer la borne de Chernoff [63], pour obtenir :

$$\Pr_x \left[S_N(x) - A_N^- \geq N\Delta\mu \,|\, x \notin \boldsymbol{\mathcal{K}} \right] \leq \exp\left(-\frac{1}{4} \frac{N^2 \Delta\mu^2}{A_N^-} \right)$$

Par ailleurs, comme $A_N^- \leq N\mu^-$ et $\mu^- \leq \mu$ où μ est la probabilité pour x et y aléatoires que $T(x+y) = T(y)$, nous pouvons majorer A_N^- par $N\mu$. Finalement, utilisant l'inégalité (9.11), nous obtenons la borne suivante sur la probabilité de faux-positif :

$$\Pr_x \left[S_N(x) \geq N\mu^+ \,|\, x \notin \boldsymbol{\mathcal{K}} \right] \leq \exp\left(-\frac{N}{4} \frac{\Delta\mu^2}{\mu} \right)$$

La probabilité μ est égale à la probabilité que deux éléments aléatoires x, y aient la même valeur de T ; sa valeur de l'ordre de $1/2$. Finalement, la probabilité de faux-positif est inférieure à ϵ pour :

$$N = \frac{2}{\Delta\mu^2} \ln\left(\frac{1}{\epsilon}\right)$$

Remplaçant $\Delta\mu$ par sa valeur en moyenne sur les clés (lemme 3), on obtient :

$$N = \frac{2^{2r-1}}{Adv^4} \ln\left(\frac{1}{\epsilon}\right) \tag{9.12}$$

Complexité de reconstruire le noyau : Un élément aléatoire x est dans $\boldsymbol{\mathcal{K}}$ avec probabilité 2^{-r} et détecté en tant que tel par le test avec probabilité $1/2$. Calculer chaque valeur $\delta_{y_i}(x)$ nécessite de calculer la différentielle en $x + y_i$ et y_i, puis de calculer la dimension de leurs noyaux. La complexité de calculer une différentielle et la dimension de son noyau est n^3, la même qu'une évaluation de la clé publique. Enfin, n éléments de $\boldsymbol{\mathcal{K}}$ engendrent le sous-espace tout entier avec forte probabilité. La complexité de reconstruire $\boldsymbol{\mathcal{K}}$ est donc $2^{r+1}Nn$ évaluations de clé publique. Prenant pour N la valeur donnée par l'équation (9.12), celle-ci vaut :

$$\frac{n2^{3r}}{Adv^4} \ln\left(\frac{1}{\epsilon}\right) \tag{9.13}$$

évaluations de la clé publique. Notons que la valeur de N donnée par l'équation (9.12) résulte de la borne supérieure de Chernoff ; bien que cette borne donne souvent une estimation fine, il n'est pas impossible que l'attaque puisse être réalisée pour des valeurs inférieures de N. La valeur de ϵ doit être choisie de manière à ce que la probabilité de faux-positifs parmi les n éléments sélectionnés soit faible. La probabilité de réussite est $(1-\epsilon)^n \simeq 1 - n\epsilon$, donc lorsque n vaut 100, choisir $\epsilon = 0.001$ assure le succès de l'attaque avec probabilité 0.9. La table ci-dessous donne le logarithme en base 2 des complexités correspondantes pour plusieurs paramètres et $\epsilon = 0.001$. Les valeurs en gras correspondent aux paramètres recommandés pour IPHFE.

(n, D, r)	Restaurer $\mathcal{K}$	(n, D, r)	Restaurer $\mathcal{K}$	(n, D, r)	Restaurer $\mathcal{K}$
$(89, 2, 1)$	32.26	$(89, 3, 1)$	50.20	$(89, 4, 1)$	73.15
$(89, 2, 2)$	45.25	**(89,3,2)**	**67.09**	$(89, 4, 2)$	93.93
$(89, 2, 3)$	57.19	$(89, 3, 3)$	82.98	$(89, 4, 3)$	113.76
$(89, 2, 4)$	68.65	$(89, 3, 4)$	98.41	$(89, 4, 4)$	133.16

9.7 Inverser la clé publique à partir du noyau

Une fois le noyau $\mathcal{K}$ de la perturbation découvert, on détermine des formes linéaires indépendantes $l_1, \ldots, l_r$ orthogonales à $\mathcal{K}$. Un élément $(x_1, \ldots, x_n)$ appartient à $\mathcal{K}$ si et seulement si pour tout k entre 1 et r, $l_k(x_1, \ldots, x_n) = 0$.

Chaque parallèle à $\mathcal{K}$ est caractérisé par des valeurs cibles 0 ou 1 pour les l_k. Comme nous l'avons déjà remarqué, la clé publique IPHFE est une clé publique HFE sur tout sous-espace parallèle à $\mathcal{K}$. Pour tout tel sous-espace, nous appelons $p_1, \ldots, p_n$ les coordonnées multivariées de la clé publique IPHFE, et $p'_1, \ldots, p'_n$ celles de la clé publique HFE équivalente sur ce sous-espace. Les formes linéaires l_k sont constantes sur ce sous-espace ; par exemple, elles prennent toutes la valeur 0 (le sous-espace considéré est alors $\mathcal{K}$). Pour toute valeur image $(b_1, \ldots, b_n)$, les systèmes d'équations multivariés $\{p_i = b_i, i \in [1, n]\} \cap \{l_k = 0, k \in [1, r]\}$ et $\{p'_i = b_i, i \in [1, n]\} \cap \{l_k = 0, k \in [1, r]\}$ ont les mêmes solutions. Comme tout idéal est radical dans l'anneau $R_n = \mathbb{F}_2[x_1, \ldots, x_n]/\{x_1^2 - x_1, \ldots, x_n^2 - x_n\}$, l'idéal engendré par $p_1 - b_1, \ldots, p_n - b_n$ et les formes linéaires $l_1, \ldots, l_r$ est donc le même que l'idéal engendré par $p'_1 - b_1, \ldots, p'_n - b_n$ et $l_1, \ldots, l_r$. Notons I cet idéal et J l'idéal engendré par $p'_1 - b_1, \ldots, p'_n - b_n$ sans les formes linéaires du noyau.

L'idéal J est engendré par des polynômes provenant d'un cryptosystème HFE. Faugère et Joux ont montré que calculer une base de Gröbner pour un tel idéal était bien plus facile que pour un idéal aléatoire de R_n [32]. En particulier, Faugère réussit à casser le premier challenge HFE de paramètre $(n, D) = (80, 6)$ en une centaine d'heures, alors que les paramètres HFE suggérés pour une réalisation pratique de IPHFE sont $(n, D) = (89, 3)$. Le calcul étant polynomial en D, il est donc clair que calculer une base de Gröbner pour l'idéal J peut être réalisé en pratique. Or, calculer une base de Gröbner pour l'idéal I, comme c'est notre objectif, ne peut pas être plus difficile que calculer une base de Gröbner pour J. En effet, I et J ne diffèrent que par des générateurs de degré 1, et calculer une base de Gröbner pour ces générateurs peut être effectué par algèbre linéaire. Au contraire, l'ajout de ces générateurs revient à la suppression d'autant de variables et accélère le calcul. C'est bien ce qui est constaté expérimentalement : pour toute instance IPHFE testée de paramètres $(n, D, r) = (60, 3, 2)$, la calcul d'une base de Gröbner de l'idéal engendré par les polynômes de la clé publique et les formes linéaires du noyau requiert environ 2h10, contre 2h45 pour le HFE correspondant, utilisant l'algorithme F4 implanté dans MAGMA et sur un AMD Opteron à 2GHz.

Dans la pratique, les valeurs $b_1, \ldots, b_n$ sont des variables supplémentaires et le calcul de base de Gröbner n'est fait qu'une fois. Nous obtenons alors des polynômes $g_1, \ldots, g_L$ de la forme $g_l = f_l(x_1, \ldots, x_{i_l}) - h_l(b_1, \ldots, b_n)$ où f_l ne dépend que des i_l premières variables x_i. Ces polynômes permettent alors de résoudre le système $\{p_1 = b_1, \ldots, p_n = b_n, l_1 = 0, \ldots, l_r = 0\}$ pour toute valeur $(b_1, \ldots, b_n)$ en résolvant les équations $f_l(x_1, \ldots, x_{i_l}) = h_l(b_1, \ldots, b_n)$ par ordre croissant de i_l.

9.8 Conclusion

IPHFE est conçu pour offrir une résistance aux attaques par bases de Gröbner supérieure à HFE à performance égale. Toutefois, l'entière sécurité du schéma repose sur le secret du *noyau de la perturbation*, puisque la connaissance de ce sous-espace permet de partitionner la clé publique à un petit nombre de clés publiques HFE de paramètres affaiblis. Dans ce chapitre, nous avons montré qu'il existe une corrélation entre l'appartenance d'un élément au noyau de la perturbation et la dimension du noyau de la différentielle en cet élément. Cette corrélation peut être exactement calculée sur la base des résultats combinatoires exposés au chapitre 2, et peut être exploitée par un algorithme pour reconstruire le noyau de la perturbation. Pour les paramètres proposés, la complexité de l'attaque s'élève à 2^{67} évaluations de la clé publique, soit 2^{22} fois moins que la recherche exhaustive dans l'espace des messages préalablement conjecturée comme la meilleure attaque, tout en restaurant une clé secrète équivalente.

Annexe A

Compléments au chapitre 9 : preuve de la proposition 3

La proposition suivante valide l'hypothèse d'uniformité faite à la section 9.6.2 et achève ainsi la preuve de la proposition 3 :

Proposition 4. *Soit a et b deux éléments de $(\mathbb{F}_2)^n$ et δ_a, δ_b valant 0 ou 1. Les probabilités sur les clés $(P, M, \bar{P}, Z)$ que $T(a)$ et $T(b)$ valent respectivement δ_a et δ_b sont indépendantes et leurs valeurs ne dépendent pas de a et b mais de leur appartenance respective à $\mathcal{K}$, à des termes négligeables d'ordre $2^{-n+\max\{2D,r\}}$ près.*

Afin de montrer la proposition, il suffit de montrer que pour une clé aléatoire, les dimensions des noyaux des différentielles en a et b sont indépendantes et de valeurs ne dépendant que de l'appartenance respective à $\mathcal{K}$ de a et b, à des termes d'ordre $2^{-n+\max\{2D,r\}}$ près. Nous avons vu au théorème 3 que les probabilités sur les clés $(P, M, \bar{P}, Z)$

$$p_a^+(t) = \Pr\left[\dim\ker D\tilde{P}_a = t \,|\, a \in \mathcal{K}\right] \quad \text{et} \quad p_a^-(t) = \Pr\left[\dim\ker D\tilde{P}_a = t \,|\, a \notin \mathcal{K}\right]$$

sont indépendantes de a et respectivement égales aux probabilités $\pi^+(t)$ et $\pi^-(t)$ définies ci-dessous à des termes d'ordre 2^{-n+r} près. Plus précisément, nous avons, selon l'appartenance ou non à $\mathcal{K}$ de a :

$$p_a^+(t) = \pi^+(t) + \mathcal{O}(2^{-n+r}) \quad \text{et} \quad p_a^-(t) = \pi^-(t) + \mathcal{O}(2^{-n+r})$$

où

$$\pi^+(t) = \Pr_{(L,\ell)}\left[\dim\ker(L+\ell) = t \,|\, L(a) = \ell(a) = 0\right]$$
$$\pi^-(t) = \Pr_{(L,\ell)}\left[\dim\ker(L+\ell) = t \,|\, L(a) = \ell(a) \neq 0\right]$$

avec L un polynôme $\mathbb{F}_2$-linéaire aléatoire de degré 2^D et ℓ une application linéaire aléatoire de rang r.

De même, nous définissons ici avec des notations évidentes les probabilités $p_{a,b}^{++}(t,t')$, $p_{a,b}^{+-}(t,t')$ et $p_{a,b}^{--}(t,t')$ sur les clés $(P, M, \bar{P}, Z)$; par exemple :

$$p_{a,b}^{++}(t,t') = \left[\begin{array}{c|c} \dim\ker D\tilde{P}_a = t & a \in \mathcal{K} \\ \dim\ker D\tilde{P}_b = t' & b \in \mathcal{K} \end{array}\right]$$

Similairement, nous montrons que ces probabilités ne dépendent pas de a et b mais seulement de leur appartenance respective à $\mathcal{K}$. Par exemple, nous montrons que

$$p_{a,b}^{++}(t,t') = \pi^{++}(t,t') + \mathcal{O}(2^{-n+r})$$

où

$$\pi^{++}(t,t') = \Pr_{(L,L',\ell,\ell')}\left[\begin{array}{l|l;{}} \dim\ker(L+\ell)=t & L(a)=0 \\ \dim\ker(L'+\ell')=t' & L'(b)=0 \end{array} ; L(b)+L'(a)=0\right]$$

Cette première simplification est l'objet de la section A.1.

La seconde étape de la preuve consiste à montrer que la corrélation entre les dimensions des noyaux de $L+\ell$ et $L'+\ell'$ due aux conditions croisées telles la condition $L(b)+L'(a)=0$ ci-dessus, est négligeable d'ordre 2^{-n+2D}. Plus précisément, nous montrons que

$$\pi^{++}(t,t') = \pi^{+}(t)\pi^{+}(t') + \mathcal{O}(2^{-n+2D})$$

Ce résultat est l'objet de la section A.2.

A.1 Caractérisation de la distribution jointe

La preuve suit la même méthodologie que celle du théorème 3. En particulier, les deux lemmes suivants sont des généralisations des lemmes 14 et 15.

Lemme 18. *Soient a, b deux éléments non-nuls distincts de $\mathbb{F}_{2^n}$. Quand P est un polynôme $\mathbb{F}_2$-quadratique aléatoire de degré inférieur à 2^{D+1}, DP_a, DP_b sont des polynômes $\mathbb{F}_2$-linéaires aléatoires L, L' de degré inférieur à 2^D tels que $L(a)=0$, $L(b)=0$ et $L(b)+L'(a)=0$.*

Démonstration. On montre que l'application $P \mapsto (DP_a, DP_b)$ est une surjection uniforme pour les ensembles décrits dans l'énoncé. Soit (L, L') verifiant les conditions de l'enonce ; les coefficients de L et L' sont respectivement les (l_i) et (l'_i) pour i entre 0 et D. Un polynôme $\mathbb{F}_2$-quadratique

$$P(x) = \textstyle\sum_{i=0}^{D}\sum_{j=i+1}^{D} p_{ij}.x^{2^i+2^j}$$

vérifie $(DP_a, DP_b) = (L, L')$ si et seulement si les (p_{ij}) vérifient :

$$\begin{bmatrix} l_0 \\ \\ \vdots \\ \\ l_D \end{bmatrix} = \begin{bmatrix} 0 & p_{01} & p_{02} & \cdots & p_{0D} \\ p_{01} & 0 & p_{12} & \cdots & p_{1D} \\ p_{01} & p_{12} & 0 & & p_{2D} \\ \vdots & \vdots & & \ddots & \vdots \\ p_{0D} & p_{1D} & p_{2D} & \cdots & 0 \end{bmatrix} \begin{bmatrix} a^{2^0} \\ \\ \vdots \\ \\ a^{2^D} \end{bmatrix}$$

ainsi que l'équation correspondante en les (l'_i) et (b^{2^j}). Pour tout $i \leq D-2$, tout choix des coefficients p_{ij} pour $i < j \leq D-2$ définit uniquement les coefficients $p_{i,D-1}$ et $p_{i,D}$. En effet, ces coefficients satisfont le système linéaire suivant :

$$\begin{cases} p_{i,D-1}.a^{2^{D-1}} + p_{i,D}.a^{2^D} = l_i - c_i(a) \\ p_{i,D-1}.b^{2^{D-1}} + p_{i,D}.b^{2^D} = l'_i - c_i(b) \end{cases} \quad \text{où} \quad c_i(a) = \sum_{j=0}^{i-1} p_{ji} a^{2^j} + \sum_{j=i+1}^{D-2} p_{ij} a^{2^j}$$

qui est inversible, puisque son déterminant $(ab^2 - a^2b)^{2^{D-1}}$ est non-nul lorsque a et b sont non-nuls et distincts. Il nous reste à définir le coefficient $p_{D-1,D}$, selon :

$$p_{D-1,D}.a^{2^D} = l_{D-1} - \textstyle\sum_{j=0}^{D-2} p_{j,D-1}.a^{2^j} \tag{A.1}$$

et à vérifier que cette définition est bien compatible avec les contraintes restantes. L'équation en l_D s'obtient en utilisant $L(a) = 0$; nous avons :

$$l_D.a^{2^D} = \textstyle\sum_{j=0}^{D-2} l_j.a^{2^j} + l_{D-1}.a^{2^{D-1}}$$

Remplaçant les l_j, $j \leq D-2$ par leurs expressions et utilisant la symétrie :

$$l_D.a^{2^D} = \textstyle\sum_{j=0}^{D-2} (p_{j,D-1}.a^{2^{D-1}} + p_{j,D}.a^{2^D})a^{2^j} + l_{D-1}.a^{2^{D-1}}$$

L'équation (A.1) donnant l_{D-1} permet alors d'obtenir le résultat attendu :

$$l_D.a^{2^D} = (\textstyle\sum_{j=0}^{D-1} p_{j,D}.a^{2^j}).a^{2^D}$$

De même, les équations en l'_{D-1} et l'_D s'obtiennent des conditions $L'(b) = 0$ et $L'(a) = L(b)$. Finalement, le nombre de P pour lesquels $(DP_a, DP_b) = (L, L')$ est bien indépendant de L, L', a, b. □

Lemme 19. *Soit a, b deux éléments non-nuls distincts de $\mathbb{F}_{2^n}$. Quand M est un polynôme $\mathbb{F}_2$-bilinéaire aléatoire de degré $\leq 2^D$ en la première variable, $M(a, \cdot)$ et $M(b, .)$ sont deux polynômes $\mathbb{F}_2$-linéaires aléatoires et indépendants.*

Démonstration. Soit L et L' deux applications linéaires de coefficients respectivement (l_i) et (l'_i) pour i entre 0 et $n-1$. Un polynôme $\mathbb{F}_2$-bilinéaire M de degré $\leq 2^D$ en la première variable vérifie $M(a, \cdot) = L$ et $M(b, \cdot) = L'$ si et seulement si ces coefficients m_{ij} vérifient :

$$\begin{bmatrix} l_0 \\ \vdots \\ l_{n-1} \end{bmatrix} = \begin{bmatrix} m_{0,1} & \dots & m_{0,D} \\ \vdots & & \vdots \\ m_{n-1,0} & \dots & m_{n-1,D} \end{bmatrix} \begin{bmatrix} a^{2^0} \\ \vdots \\ a^{2^D} \end{bmatrix}$$

ainsi que l'équation correspondante en les (l'_i) et b^{2^j}. Pour tout i, tout choix des coefficients m_{ij} pour $j \leq D-2$ définit uniquement les coefficients $m_{i,D-1}$ et $m_{i,D}$. En effet, ces coefficients satisfont le système linéaire suivant :

$$\begin{cases} m_{i,D-1}.a^{2^{D-1}} + m_{i,D}.a^{2^D} = l_i - c_i(a) \\ m_{i,D-1}.b^{2^{D-1}} + m_{i,D}.b^{2^D} = l'_i - c_i(b) \end{cases} \quad \text{où} \quad c_i(a) = \sum_{j=0}^{D-2} m_{ij}.a^{2^j}$$

qui est inversible, puisque son déterminant $(ab^2 - a^2b)^{2^{D-1}}$ est non-nul lorsque a et b sont non-nuls et distincts. □

Appliquant les lemmes 18 et 19, nous pouvons alors facilement montrer :

Proposition 5. *Soit a, b, α, β des éléments de $\mathbb{F}_2^n$ avec a, b non-nuls. On note $\mathcal{L}$ l'ensemble des polynômes $\mathbb{F}_2$-linéaires sur $\mathbb{F}_{2^n}$ et $\mathcal{L}^D$ le sous-espace de ceux de degré inférieur à 2^D. Un triplet $(P, M, \bar{P})$ choisi lors de la génération de clés IPHFE définit la fonction a deux variables :*

$$\ddot{P}(x, y) = P(x) + M(x, y) + \bar{P}(y)$$

Les différentielles $D\ddot{P}_{(a,\alpha)}, D\ddot{P}_{(b,\beta)}$ de $\ddot{P}$ en (a, α) et (b, β) s'écrivent :

$$\begin{cases} D\ddot{P}_{(a,\alpha)}(x, y) & = L(x) + l(y) \\ D\ddot{P}_{(b,\beta)}(x, y) & = L'(x) + l'(y) \end{cases}$$

avec, selon que α et β sont nuls ou non :

i. Si $\alpha = 0$ et $\beta = 0$: pour tout $\bar{P}$ et P, M aléatoires, L, L' et l, l' sont respectivement aléatoires dans $\mathcal{L}^D$ et $\mathcal{L}$ tels que $L(a) = 0$, $L'(b) = 0$ et $L(b)+L'(a) = 0$.

ii. Si $\alpha = 0$ et $\beta \neq 0$: pour $P, M, \bar{P}$ aléatoires, L, L' et l, l' sont respectivement aléatoires dans $\mathcal{L}^D$ et $\mathcal{L}$ tels que $L(a) = 0$, $L'(b) = l'(\beta)$ et $L(b)+L'(a) = l(\beta)$ et ces deux valeurs communes sont aléatoires et indépendantes.

iii. Si $\alpha \neq 0$ et $\beta \neq 0$: pour $P, M, \bar{P}$ aléatoires, L, L' et l, l' sont respectivement aléatoires dans $\mathcal{L}^D$ et $\mathcal{L}$ tels que $L(a) = l(\alpha)$, $L'(b) = l'(\beta)$ et $L(b) + L'(a) = l(\beta) + l'(\alpha)$ et ces valeurs communes sont aléatoires et indépendantes.

Démonstration. i. Lorsque $\alpha = 0$ et $\beta = 0$, nous avons $L = DP_a$, $L' = DP_b$, $l = M(a, \cdot)$, $l' = M(b, \cdot)$ et le résultat vient des lemmes 18 et 19.

ii. Lorsque $\alpha = 0$ et $\beta \neq 0$, nous avons :

$$\begin{cases} L(x) = DP_a(x) \\ l(y) = M(a, y) \end{cases} \quad \text{et} \quad \begin{cases} L'(x) = DP_b(x) + M(x, \beta) \\ l'(y) = M(b, y) + D\bar{P}_\beta(y) \end{cases}$$

À M fixé, $M(x, \beta)$ est un élément fixé de $\mathcal{L}^D$. Par le lemme 18, quand P est aléatoire, L, L' sont des éléments aléatoires de $\mathcal{L}^D$ vérifiant :

$$\begin{cases} L(a) = 0 \\ L'(b) = M(b, \beta) \\ L(b) + L'(a) = M(a, \beta) \end{cases}$$

Toujours par le lemme 18, quand $\bar{P}$ est aléatoire, l' est un élément aléatoire de $\mathcal{L}$ vérifiant $l'(\beta) = M(b, \beta)$. Par conséquent, à M fixé et $P, \bar{P}$ aléatoires, L, L' et l' sont des éléments aléatoires de $\mathcal{L}^D$ et $\mathcal{L}$ vérifiant :

$$\begin{cases} L(a) = 0 \\ L'(b) = l'(\beta) = M(b, \beta) \\ L(b) + L'(a) = M(a, \beta) \end{cases}$$

Enfin, par le lemme 19, quand M est aléatoire, $l = M(a, \cdot)$ est un élément aléatoire de $\mathcal{L}$ tel que $l(\beta) = L(b) + L'(a)$ et $M(b, \beta)$ est une valeur aléatoire.

iii. Lorsque $\alpha \neq 0$ et $\beta \neq 0$, nous avons :

$$\left\{ \begin{array}{rcl} L(x) & = & DP_a(x) + M(x, \alpha) \\ l(y) & = & M(a, y) + D\bar{P}_\alpha(y) \end{array} \right. \quad \text{et} \quad \left\{ \begin{array}{rcl} L'(x) & = & DP_b(x) + M(x, \beta) \\ l'(y) & = & M(b, y) + D\bar{P}_\beta(y) \end{array} \right.$$

À M fixé, $M(x, \alpha)$ et $M(x, \beta)$ sont deux éléments fixés de $\mathcal{L}^D$. Par les lemmes 18 et 19, quand P et $\bar{P}$ sont aléatoires, L, L' et l, l' sont des éléments aléatoires respectivement de $\mathcal{L}^D$ et $\mathcal{L}$ vérifiant :

$$\left\{ \begin{array}{l} L(a) = \ell(\alpha) = M(a, \alpha) \\ L'(b) = l'(\beta) = M(b, \beta) \\ L(b) + L'(a) = l(\beta) + l'(\alpha) = M(b, \alpha) + M(a, \beta) \end{array} \right.$$

Quand M est aléatoire, $M(a, \beta), M(a, \alpha), M(b, \beta), M(\alpha, \beta)$ sont quatre valeurs aléatoires independantes, et par conséquent, les valeurs $L(a) = l(\alpha)$, $L'(b) = l'(\beta)$ et $L(b) + L'(a) = l(\beta) + l'(\alpha)$ sont aléatoires et indépendantes. □

Nous pouvons maintenant conclure la caractérisation cherchée, à l'aide des lemmes 16 et 17 du chapitre 9 :

Cas ou $\mathcal{K}$ contient a et b : alors $D\tilde{P}_a = L + l \circ Z$ et $D\tilde{P}_b = L' + l' \circ Z$, où :

1. L et L' sont des polynômes $\mathbb{F}_2$-linéaires aléatoires de degré inférieur à 2^D avec $L(a) = 0$, $L'(b) = 0$, $L(b) + L'(a) = 0$ pour P aléatoire, et de degré exactement 2^D pour une proportion $(1 - 2^{-n})^2$ des choix aléatoires de P.
2. $l \circ Z$ et $l' \circ Z$ sont des applications linéaires aléatoires de noyau $\ker(Z)$ pour une proportion $(1 - \alpha_{n,r})^2$ des choix aléatoires de M ou $\alpha_{n,r} = (2^r - 1)2^{-n} + \mathcal{O}(2^{-2n+r})$, et $\ker(Z) = \mathcal{K}$ est un sous-espace aléatoire contenant a et b pour tout choix aléatoire de Z avec $Z(a) = 0$ et $Z(b) = 0$.

Donc, pour une proportion $(1-2^{-n})^2(1-\alpha_{n,r})^2 = 1+\mathcal{O}(2^{-n+r})$ des choix aléatoires de $(P, M, \bar{P}, Z)$, nous avons :

$$\Pr\left[\begin{array}{l} \dim\ker D\tilde{P}_a = t \\ \dim\ker D\tilde{P}_b = t' \end{array} \middle| \begin{array}{l} a \in \mathcal{K} \\ b \in \mathcal{K} \end{array} \right] = \Pr\left[\begin{array}{l} \dim\ker(L + \ell) = t \\ \dim\ker(L' + \ell') = t' \end{array} \middle| \begin{array}{l} L(a) = \ell(a) = 0 \\ L'(b) = \ell'(b) = 0 \\ L(b) + L'(a) = 0 \\ \ker(\ell) = \ker(\ell') \end{array} \right]$$

où L, L' sont des polynômes $\mathbb{F}_2$-linéaires aléatoire de degré 2^D et ℓ, ℓ' sont des applications linéaires aléatoires de rang r. On note $\pi^{++}(t, t')$ la probabilité de droite.

Cas ou $\mathcal{K}$ contient a mais non b : $D\tilde{P}_a = L + l \circ Z$ et $D\tilde{P}_b = L' + l' \circ Z$, où :

1. L et L' sont des polynômes $\mathbb{F}_2$-linéaires aléatoires de degré inférieur à 2^D avec $L(a) = 0$ pour P aléatoire, et de degré exactement 2^D pour une proportion $(1-2^{-n})^2$ des choix aléatoires de P. De plus, $L'(b)$, $L(b)+L'(a)$ et leur somme sont non-nuls pour une proportion $(1-2^{-n})(1-2^{-n+1})$ de ces derniers choix de P. Considérer ces éléments non-nuls permettra certaines simplifications ci-après ainsi qu'à la section suivante.
2. $l \circ Z$ et $l' \circ Z$ sont des applications linéaires aléatoires vérifiant $l'(Z(b)) = L'(b)$ et $l(Z(b)) = L(b) + L'(a)$ et de noyau $\ker(Z)$ pour une proportion $(1-\alpha_{n,r})^2/(1-2^{-n})^2$ des choix aléatoires de M et $\bar{P}$; $\ker(Z) = \mathcal{K}$ est un sous-espace aléatoire contenant a et non b pour tout choix aléatoire de Z avec $Z(a) = 0$ et $Z(b) \neq 0$.

Donc, pour une proportion $(1-2^{-n})(1-2^{-n+1})(1-\alpha_{n,r})^2 = 1 + \mathcal{O}(2^{-n+r})$ des choix aléatoires de $(P, M, \bar{P}, Z)$, nous avons :

$$\Pr\left[\begin{array}{l|l} \dim\ker D\tilde{P}_a = t & a \in \mathcal{K} \\ \dim\ker D\tilde{P}_b = t' & b \notin \mathcal{K} \end{array}\right] = \Pr\left[\begin{array}{l|l} \dim\ker(L+\ell) = t & L(a) = \ell(a) = 0 \\ \dim\ker(L'+\ell') = t' & L'(b) = \ell'(b) \neq 0 \\ & L(b) + L'(a) \\ & \quad = \ell(b) \neq 0 \\ & L'(b) + L(b) \\ & \quad + L'(a) \neq 0 \\ & \ker(\ell) = \ker(\ell') \end{array}\right]$$

où L, L' sont des polynômes $\mathbb{F}_2$-linéaires aléatoire de degré 2^D et ℓ, ℓ' sont des applications linéaires aléatoires de rang r. On note $\pi^{+-}(t, t')$ la probabilité de droite.

Cas ou $\mathcal{K}$ ne contient ni a ni b : $D\tilde{P}_a = L + l \circ Z$ et $D\tilde{P}_b = L' + l' \circ Z$, où :

1. L et L' sont des polynômes $\mathbb{F}_2$-linéaires aléatoires de degré inférieur a 2^D pour P aléatoire, et de degré exactement 2^D pour une proportion $(1-2^{-n})^2$ des choix aléatoires de P. De plus, $L(a)$, $L'(b)$, $L(b)+L'(a)$, $L(a)+L(b)+L'(a)$, et $L'(b)+L(b)+L'(a)$ sont non-nuls pour une proportion $(1-2^{-n})(1-2^{-n+1})^2$ de ces derniers choix de P.
2. $l \circ Z$ et $l' \circ Z$ sont applications linéaires aléatoires vérifiant $l(Z(a)) = L(a)$, $l'(Z(b)) = L'(b)$ et $l(Z(b)) + l'(Z(a)) = L(b) + L'(a)$ et de noyau $\ker(Z)$ pour une proportion $(1-\alpha_{n,r})^2/(1-2^{-n})^3$ des choix aléatoires de M et $\bar{P}$; $\ker(Z) = \mathcal{K}$ est un sous-espace aléatoire ne contenant ni a ni b pour tout choix aléatoire de Z avec $Z(a) \neq 0$ et $Z(b) \neq 0$.

Donc, pour une proportion $(1-2^{-n+1})^2(1-\alpha_{n,r})^2 = 1+\mathcal{O}(2^{-n+r})$ des choix aléatoires de $(P, M, \bar{P}, Z)$, nous avons :

$$\Pr\left[\begin{array}{l|l} \dim\ker D\tilde{P}_a = t & a \in \mathcal{K} \\ \dim\ker D\tilde{P}_b = t' & b \notin \mathcal{K} \end{array}\right] = \Pr\left[\begin{array}{l|l} \dim\ker(L+\ell) = t & L(a)=\ell(a)\neq 0 \\ \dim\ker(L'+\ell') = t' & L'(b)=\ell'(b)\neq 0 \\ & L(b)+L'(a) \\ & =\ell(b)+\ell'(a)\neq 0 \\ & L(a)+L(b) \\ & \qquad +L'(a)\neq 0 \\ & L'(b)+L(b) \\ & \qquad +L'(a)\neq 0 \\ & \ker(\ell)=\ker(\ell') \end{array}\right]$$

où L, L' sont des polynômes $\mathbb{F}_2$-linéaires aléatoire de degré 2^D et ℓ, ℓ' sont des applications linéaires aléatoires de rang r. On note $\pi^{--}(t,t')$ la probabilité de droite.

A.2 Estimation du facteur de corrélation

Étant donné des conditions $\mathcal{C}$, on note $\pi^{\mathcal{C}}(t,t')$ la probabilité

$$\pi^{\mathcal{C}}(t,t') = \Pr_{(L,L',\ell,\ell')}\left[\begin{array}{l} \dim\ker(L+\ell) = t \\ \dim\ker(L'+\ell') = t' \end{array}\;\middle|\; \mathcal{C}\right]$$

Pour tout $d, d' \leq D$, $i \leq d$ et $i' \leq d'$, on note $\pi^{\mathcal{C}}_{d,d',i,i'}(t,t')$ la probabilité intersection avec les propriétés additionnelles :

$$\left\{\begin{array}{l} \dim\ker(L) = d \\ \dim\ker(L') = d' \end{array}\right. \qquad \left\{\begin{array}{l} \dim(\ker(L)\cap\ker(\ell)) = i \\ \dim(\ker(L')\cap\ker(\ell')) = i' \end{array}\right.$$

Pour calculer la probabilité $\pi^{\mathcal{C}}_{d,d',i,i'}(t,t')$, on dénombre d'abord la proportion des paires L, L' de polynômes $\mathbb{F}_2$-linéaires de degré 2^D vérifiant les conditions $\mathcal{C}$ pour lesquelles les noyaux sont de dimensions respectivement d et d'. On note cette proportion $\Lambda^{\mathcal{C}}_{2,D}(d,d')$:

$$\Lambda^{\mathcal{C}}_{2,D}(d,d') = \Pr_{(L,L')}\left[\begin{array}{l} \dim\ker(L) = d \\ \dim\ker(L') = d' \end{array}\;\middle|\; \mathcal{C}\right]$$

Pour L et L' fixés vérifiant ces conditions, on dénombre ensuite la proportion des sous-espaces $\mathcal{K}, \mathcal{K}'$ de dimension $n-r$ vérifiant les conditions $\mathcal{C}$ qui vérifient également les conditions sur i, i'. On note cette proportion $\mathcal{S}^{\mathcal{C}}_{L,L'}(i,i')$:

$$\mathcal{S}^{\mathcal{C}}_{2,L,L'}(i,i') = \Pr_{(\mathcal{K},\mathcal{K}')}\left[\begin{array}{l} \dim(\ker(L)\cap\mathcal{K}) = i \\ \dim(\ker(L')\cap\mathcal{K}') = i' \end{array}\;\middle|\; \mathcal{C}\right]$$

Pour L, L' et $\mathcal{K}, \mathcal{K}'$ fixés, on calcule enfin la proportion des applications linéaires ℓ, ℓ' de rang r vérifiant les conditions $\mathcal{C}$ qui vérifient également les conditions sur t, t' :

$$\lambda^{\mathcal{C}}_{L,L',\mathcal{K},\mathcal{K}'}(t,t') = \Pr_{(\ell,\ell')}\left[\begin{array}{ll} \dim\ker(L+\ell) = t & \ker(\ell) = \mathcal{K} \\ \dim\ker(L'+\ell') = t' & , \ \ker(\ell') = \mathcal{K}' \end{array}\;\middle|\; \mathcal{C}\right]$$

A.2.1 Calcul de $\pi^{++}(t, t')$

Dans ce cas, nous avons :

$$\mathcal{C} : \left\{ \begin{array}{lll} L(a) = \ell(a) = 0 & , & L(b) + L'(a) = 0 \\ L'(b) = \ell'(b) = 0 & , & \ker(\ell) = \ker(\ell') \end{array} \right.$$

Ce jeu de conditions se scinde en :

$$\mathcal{C}_\Lambda : \left\{ \begin{array}{l} L(a) = 0 \\ L'(b) = 0 \\ L(b) + L'(a) = 0 \end{array} \right. \quad \text{et} \quad \mathcal{C}_\mathcal{S} : \left\{ \begin{array}{l} a \in \mathcal{K} \\ b \in \mathcal{K}' \\ \mathcal{K} = \mathcal{K}' \end{array} \right.$$

affectant respectivement $\Lambda^{++}_{2,D}(d, d')$ et $\mathcal{S}^{++}_{2,L,L'}(i, i')$.

Calcul de $\Lambda^{++}_{2,D}(d, d')$

La proportion $\Lambda^{++}_{2,D}(d, d')$ est le rapport du nombre $N^{++}_{2,D}(d, d')$ de paires L, L' vérifiant les conditions $\mathcal{C}_\Lambda$ ainsi que les conditions sur d, d', sur le nombre total $N^{++}_{2,D}$ de paires vérifiant les conditions $\mathcal{C}_\Lambda$. Soit $N^{+}_{D}(d)$ le nombre de polynômes $\mathbb{F}_2$-linéaires de degré 2^D dont le noyau est de dimension d et contient un point fixé non-nul, et $N^{++}_{D}(d)$ le nombre de polynômes $\mathbb{F}_2$-linéaires de degré 2^D dont le noyau est de dimension d et contient un sous-espace fixé de dimension 2. Le lemme suivant fournit l'expression de $N^{++}_{2,D}(d, d')$ en termes de $N^{+}_{D}(d)$ et $N^{++}_{D}(d)$:

Lemme 20. *Soit a, b deux éléments non-nuls et distincts de $(\mathbb{F}_2)^n$. Pour tout entiers $d, d' \leq D$, nous avons :*

$$N^{++}_{2,D}(d, d') = N^{++}_{D}(d) N^{++}_{D}(d') + \frac{1}{2^n - 1}(N^{+}_{D}(d) - N^{++}_{D}(d))(N^{+}_{D}(d') - N^{++}_{D}(d'))$$

Démonstration. On définit l'ensemble V_a des polynômes $\mathbb{F}_2$-linéaires de degré 2^D qui s'annulent en a et l'ensemble $V_{a,b}$ des polynômes $\mathbb{F}_2$-linéaires de degré 2^D qui s'annulent sur le sous-espace engendré par a et b. Deux fonctions L, L' verifiant les conditions prescrites sont toutes deux dans $V_{a,b}$ ou bien toutes deux hors de $V_{a,b}$. Dans le second cas, pour tout L dans V_a et hors de $V_{a,b}$, le nombre de L' dans V_b satisfaisant la condition $L'(a) = L(b)$ représente une fraction $1/(2^n - 1)$ des éléments de V_b hors de $V_{a,b}$ puisque $L(b)$ est l'une des $2^n - 1$ valeurs autrement possibles pour $L'(a)$. □

Le lemme suivant permet de se ramener à une expression en le seul $N^{+}_{D}(d)$.

Lemme 21.

$$N^{++}_{D}(d) = \frac{2^d - 2}{2^n - 2}.N^{+}_{D}(d)$$

Démonstration. Selon le théorème 3, le nombre $N_D(m)$ de polynômes $\mathbb{F}_2$-linéaires de degré 2^D dont le noyau est de dimension $m = 0, \ldots, D$ vérifie le système :

$$E(n,d)(2^n-1)2^{n(D-d)} = \sum_{m=d}^{D} E(m,d)N_D(m)$$

Le nombre de sous-espaces de dimension d dans un espace de dimension n qui contiennent un élément fixé non-nul est une fraction $(2^d-1)/(2^n-1)$ du nombre total. Par conséquent, le nombre $N_D^+(d)$ pour $d = 1, \ldots, D$ vérifie

$$\frac{2^d-1}{2^n-1}E(n,d)(2^n-1)2^{n(D-d)} = \sum_{m=d}^{D} E(m,d)\frac{2^d-1}{2^n-1}N_D(m)$$

d'où l'on déduit : $N_D^+(d) = (2^d-1)/(2^n-1).N_D(d)$, et on obtient similairement :

$$N_D^{++}(d) = (2^d-2)/(2^n-2).N_D^+(d)$$

□

Des lemmes 20 et 21, nous obtenons :

$$N_{2,D}^{++}(d,d') = N_D^+(d)N_D^+(d')\left(\frac{2^d-2}{2^n-2}.\frac{2^{d'}-2}{2^n-2} + \frac{1}{2^n-1}.\frac{2^n-2^d}{2^n-2}.\frac{2^n-2^{d'}}{2^n-2}\right)$$

Nous calculons maintenant le dénominateur $N_{2,D}^{++}$. Les trois conditions $\mathcal{C}_\Lambda$ consistent en trois contraintes linéaires sur les $2(D+1)$ coefficients de L et L'. Comme les coefficients dominants de ces deux polynômes sont non-nuls quand ceux-ci sont de degré 2^D, le nombre de tels polynômes est :

$$N_{2,D}^{++} = (2^n-1)^2 2^{n(2D-3)}$$

De la même façon, le nombre total N_D^+ des polynômes $\mathbb{F}_2$-linéaires de degré 2^D s'annulant en un point prescrit non-nul est $(2^n-1)2^{n(D-1)}$. Nous avons donc :

$$N_{2,D}^{++} = 2^{-n}(N_D^+)^2$$

Nous obtenons donc finalement pour $\Lambda_{2,D}^{++}(d,d')$ l'expression :

$$\Lambda_{2,D}^{++}(d,d') = \Lambda_D^+(d)\Lambda_D^+(d')(1+\epsilon_{\Lambda,D})$$

où $\Lambda_D^+(d)$ est la proportion des polynômes $\mathbb{F}_2$-linéaires de degré 2^D et s'annulant en un point prescrit non-nul pour lesquels le noyau est de dimension d, et

$$1+\epsilon_{\Lambda,D} = 2^n\left(\frac{2^d-2}{2^n-2}.\frac{2^{d'}-2}{2^n-2} + \frac{1}{2^n-1}.\frac{2^n-2^d}{2^n-2}.\frac{2^n-2^{d'}}{2^n-2}\right)$$

Les termes dominants de cette expression sont :

$$1 + 2^n.\frac{2^d-2}{2^n-2}.\frac{2^{d'}-2}{2^n-2}$$

d'où nous déduisons que $\epsilon_{\Lambda,D} = \mathcal{O}(2^{-n+2D})$.

Calcul de $\mathcal{S}^{++}_{2,L,L'}(i,i')$

Au préalable, on note que les noyaux de L et L' sont d'intersection zéro avec forte probabilité $1-\mathcal{O}(2^{-n+2D})$. En effet, la probabilité que deux sous-espaces aléatoires de dimension d et d' soient d'intersection de dimension j est d'après le lemme 2 de l'ordre de $2^{-j(n-d-d'+j)}$, et donc celle que ces deux sous-espaces soient d'intersection non-nulle est de l'ordre de $2^{-n+d+d'}=\mathcal{O}(2^{-n+2D})$. Quitte à remplacer $\Lambda^{++}_{2,D}(d,d')$ par son intersection avec la condition $\ker(L)\cap\ker(L')=\{0\}$ dont la valeur est la même à des termes d'ordre 2^{-n+2D} près, nous pouvons donc supposer que cette condition est réalisée.

Nous estimons maintenant le nombre

$$\eta^{++}_{2,L,L'}(i,i')=\#\left\{\mathcal{K},\dim(\mathcal{K})=n-r\;\middle|\;\begin{array}{l}\dim(\ker(L)\cap\mathcal{K})=i\\ \dim(\ker(L')\cap\mathcal{K})=i'\end{array}\quad\text{et}\quad a,b\in\mathcal{K}\right\}$$

où $\ker(L)$ et $\ker(L')$ sont d'intersection zéro. L'intersection I de $\ker(L)$ et $\mathcal{K}$ est un sous-espace de dimension contenant a : il y a donc

$$(2^i-1)/(2^d-1).E(d,i)$$

choix pour un tel sous-espace. De même, il y a $(2^{i'}-1)/(2^{d'}-1).E(d',i')$ choix pour l'intersection I' de $\ker(L')$ et $\mathcal{K}$. Le sous-espace somme des intersections de $\mathcal{K}$ avec $\ker(L)$ et $\ker(L')$ est un sous-espace de dimension $i+i'$ de $\mathcal{K}$. Le nombre de sous-espaces de dimension $n-r$ d'intersection I avec $\ker(L)$ et I' avec $\ker(L')$ est donné par le lemme suivant.

Lemme 22. *Étant donnés F et F' deux sous-espaces de dimension $d,d'\leq D$, et deux sous-espaces I et I' de dimension i et i' respectivement de F et F', le nombre de sous-espace $\mathcal{K}$ de dimension $n-r$ ayant I pour intersection avec F et I' pour intersection avec F' est :*

$$\frac{S(n,n-r)S(n-r,i+i')}{S(n,i+i')S(n-r,n-r)}\left(1+\mathcal{O}(2^{-n+2D})\right)$$

Démonstration. Une borne supérieure du nombre cherché est le nombre de sous-espaces de dimension $n-r$ contenant $I+I'$. Le nombre de tels sous-espaces est

$$\frac{S(n,n-r)}{S(n,i+i')}\frac{S(n-r,i+i')}{S(n-r,n-r)}$$

Une borne inférieure du nombre cherché est le nombre de sous-espaces de dimension $n-r$ contenant $I+I'$ et d'intersection zéro avec $F+F'$. Le nombre de tels sous-espaces est :

$$\frac{S(n,n-r+(d-i)+(d'-i'))}{S(n,d+d')}\frac{S(n-r,i+i')}{S(n-r,n-r)}$$

Le facteur de gauche dans l'expression ci-dessus s'écrit :

$$\frac{S(n,n-r)}{S(n,i+i')}\frac{(1-\alpha)\dots(1-\alpha^{k-1})}{(1-\beta)\dots(1-\beta^{k-1})}$$

avec $\alpha = 2^{-r}$, $\beta = 2^{-n+i+i'}$ et $k = (d-i)+(d'-i') \leq 2D$. Le lemme provient de :

$$\frac{(1-\alpha)\dots(1-\alpha^{k-1})}{(1-\beta)\dots(1-\beta^{k-1})} \leq 1+\beta+\mathcal{O}(\beta^2) = 1+\mathcal{O}(2^{-n+2D})$$

□

Notons maintenant $\eta_L^+(i)$ le nombre de sous-espaces de dimension $n-r$ dont l'intersection avec $\ker(L)$ est de dimension i et contient a. Nous obtenons aisément :

$$\eta_L^+(i) = \left(\frac{2^i-1}{2^d-1}\right) E(d,i) \frac{S(n,n-r)S(n-r,i)}{S(n,i)S(n-r,n-r)}$$

Par ailleurs, nous pouvons facilement montrer que :

$$S(n,i+i') = S(n,i)S(n,i')(1+\mathcal{O}(2^{-n+2D}))$$

Il suffit en effet de voir que :

$$\frac{S(n,i+i')}{S(n,i)} = \left(1-\frac{2^i-1}{2^n-1}\right)\dots\left(1-\frac{2^i-1}{2^{n-i'}-1}\right) = 1+\mathcal{O}(2^{-n+2D})$$

Par conséquent, nous obtenons finalement pour le nombre $\eta_{2,L,L'}^{++}(i,i')$:

$$\eta_{2,L,L'}^{++}(i,i') = \eta_L^+(i)\eta_{L'}^+(i')\frac{S(n,n-r)}{S(n-r,n-r)}(1+\mathcal{O}(2^{-n+2D}))$$

Nous calculons maintenant le nombre total η_2^{++} de sous-espaces de dimension $n-r$ contenant a et b. Nous obtenons aisément :

$$\eta_2^{++} = \frac{(2^{n-r}-1)(2^{n-r}-2)}{(2^n-1)(2^n-2)} E(n,n-r)$$

Par ailleurs, le nombre η^+ de sous-espaces de dimension $n-r$ contenant a est :

$$\eta^+ = \frac{2^{n-r}-1}{2^n-1} E(n,n-r)$$

Comme

$$\frac{2^{n-r}-2}{2^n-2} = \frac{2^{n-r}-1}{2^n-1}(1+\mathcal{O}(2^{-n+r}))$$

Nous obtenons :

$$\eta_2^{++} = (\eta^+)^2 E(n,n-r)(1+\mathcal{O}(2^{-n+r}))$$

Notant $S_L^+(i)$ la probabilité qu'un sous-espace aléatoire de dimension $n-r$ ait une intersection de dimension i contenant a avec $\ker(L)$, la probabilité $\mathcal{S}_{2,L,L'}^{++}(i,i')$ s'écrit en fonction de $S_L^+(i)$ et $S_{L'}^+(i')$:

$$\mathcal{S}_{2,L,L'}^{++}(i,i') = S_L^+(i)S_{L'}^+(i')(1+\epsilon_S)$$

avec $\epsilon_S = \mathcal{O}(2^{-n+\max\{2D,r\}})$.

Résultat du calcul de $\pi^{++}(t,t')$

Finalement, nous obtenons :

$$\pi^{++}(t,t') = \pi^{+}(t)\pi^{+}(t')(1+\mathcal{O}(2^{-n+\max\{2D,r\}}))$$

A.2.2 Calcul de $\pi^{+-}(t,t')$

Dans ce cas, nous avons :

$$\mathcal{C} : \begin{cases} L(a) = \ell(a) = 0 & , \quad L(b) + L'(a) = \ell(b) \neq 0 \\ L'(b) = \ell'(b) \neq 0 & , \quad L'(b) + L(b) + L'(a) \neq 0 \\ \ker(\ell) = \ker(\ell') \end{cases}$$

Ce jeu de conditions se séparent en :

$$\mathcal{C}_\Lambda : \begin{cases} L(a) = 0 \\ L'(b) \neq 0 \\ L(b) + L'(a) \neq 0 \\ L'(b) + L(b) \\ \qquad + L'(a) \neq 0 \end{cases} \quad \mathcal{C}_\mathcal{S} : \begin{cases} a \in \mathcal{K} \\ b \notin \mathcal{K}' \\ \mathcal{K} = \mathcal{K}' \end{cases} \quad \mathcal{C}_\lambda : \begin{cases} \ell(b) = L(b) + L'(a) \\ \ell'(b) = L'(b) \end{cases}$$

affectant respectivement $\Lambda^{+-}_{2,D}(d,d')$, $\mathcal{S}^{+-}_{2,L,L'}(i,i')$ et $\lambda^{+-}_{L,L',\mathcal{K},\mathcal{K}'}(t,t')$.

Calcul de $\Lambda^{+-}_{2,D}(d,d')$

Soit $N^1_D(d)$ le nombre de polynômes $\mathbb{F}_2$-linéaires de degré 2^D dont le noyau est de dimension d et prenant une valeur fixé non-nulle en un point donné. Soit $N^2_D(d)$ le nombre de polynômes $\mathbb{F}_2$-linéaires de degré 2^D dont le noyau de dimension d est d'intersection zéro avec un sous-espace fixé de dimension 2 sur lequel ces applications prennent des valeurs fixées. Enfin, on note $N^{1+}_D(d)$ le nombre de polynômes $\mathbb{F}_2$-linéaires de degré 2^D dont le noyau est de dimension d contient un élément fixé non-nul et ne contient pas un élément fixé non-nul en lequel ces applications prennent une valeur fixée non-nulle.

Le lemme suivant fournit l'expression de $N^{+-}_{2,D}(d,d')$:

Lemme 23. *Soit a, b deux éléments non-nuls et distincts de $(\mathbb{F}_2)^n$. Pour tout entiers $d, d' \leq D$, nous avons :*

$$N^{+-}_{2,D}(d,d') = (2^n-1)(2^n-2)\left(N^{++}_D(d)N^2_D(d') + N^{1+}_D(d)N^{1+}_D(d') + \frac{1}{2^n-2}(N^+_D(d) - N^{++}_D(d) - N^{1+}_D(d))(N^1_D(d') - N^2_D(d') - 2N^{1+}_D(d'))\right)$$

Démonstration. Soit v_b et $v_{a,b}$ non-nuls tels que $v_b + v_{a,b}$ soit non-nul. Le nombre de choix de deux tels éléments est $(2^n - 1)(2^n - 2)$. Pour tout choix, nous définissons les conditions

$$\mathcal{C}_\Lambda(v_b, v_{a,b}) = \begin{cases} L(a) = 0 \\ L'(b) = v_b \\ L(b) + L'(a) = v_{a,b} \end{cases}$$

L'union disjointe de ces conditions forme la condition $\mathcal{C}_\Lambda$.

La troisième condition de $\mathcal{C}_\Lambda(v_b, v_{a,b})$ a pour symétrie : $L(b) \in Vect(v_{ab})$ si et seulement si $L'(a) \in Vect(v_{ab})$. Plus précisément, lorsque $L(b) = 0$, nous avons $L'(a) = v_{ab}$, et comme $v_{ab} + v_b$ est non-nul le nombre de telles applications L et L' est respectivement $N_D^{++}(d)$ et $N_D^2(d')$. Lorsque $L(b) = v_{ab}$, nous avons $L'(a) = 0$, et le nombre de telles applications L et L' est respectivement $N_D^{1+}(d)$ et $N_D^{1+}(d')$. Lorsque $L(b)$ n'est ni 0 ni v_{ab}, nous avons également $L'(a) \neq 0$ et $L'(a) \neq v_{ab}$; le nombre de telles applications L est $N_D^+(d) - N_D^{++}(d) - N_D^{1+}(d)$, et pour tout L, le nombre d'applications L' vérifiant $L'(a) = L(b) + v_{a,b}$ est une proportion $1/(2^n - 2)$ du nombre d'applications L' vérifiant $L'(b) = v_b$ et $L'(a) \neq 0, v_{a,b}$. Dans l'ensemble des applications vérifiant $L'(b) = v_b$, celles pour lesquelles $L'(a) = 0$ sont au nombre de $N_D^{1+}(d')$ et celles pour lesquelles $L'(a) = v_{a,b}$ se répartissent en fonction de la valeur de $L'(a + b)$ en $N_D^2(d)$ et $N_D^{1+}(d)$. □

Le lemme suivant permet, avec le lemme 21, de se ramener à une expression en les seuls $N_D^+(d)$ et $N_D^1(d)$.

Lemme 24.

$$N_D^{1+}(d) = \frac{2^n - 2^d}{(2^n - 1)(2^n - 2)} N_D^+(d)$$

$$N_D^2(d) = \frac{2^n - 2^{d+1}}{(2^n - 2)^2} N_D^1(d) \qquad N_D^{1+}(d) = \frac{2^d - 1}{2^n - 2} N_D^1(d)$$

Préalablement à la démonstration, soit $N_D^-(d)$ le nombre de polynômes $\mathbb{F}_2$-linéaires de degré 2^D dont le noyau de dimension d ne contient pas un point prescrit. Soit également $N_D^{--}(d)$ le nombre de ceux dont le noyau de dimension d est d'intersection zéro avec un sous-espace prescrit de dimension 2. Soit enfin $N_D^{+-}(d)$ le nombre de polynômes $\mathbb{F}_2$-linéaires de degré 2^D dont le noyau de dimension d contient un point point prescrit et n'en contient pas un autre.

Démonstration. Le nombre $N_D^1(d)$ est une fraction $1/(2^n - 1)$ du nombre $N_D^-(d)$. Par le lemme 21, nous avons :

$$N_D^-(d) = N_D(d) - N_D^+(d) = \frac{2^n - 2^d}{2^n - 1} N_D(d)$$

et donc :

$$N_D^1(d) = \frac{1}{2^n - 1} N_D^-(d) = \frac{2^n - 2^d}{(2^n - 1)^2} N_D(d)$$

De la même façon,

$$N_D^{1+}(d) = \frac{1}{2^n-1} N_D^{-+}(d) = \frac{1}{2^n-1}(N_D^{+}(d) - N_D^{++}(d)) = \frac{2^n - 2^d}{(2^n-1)(2^n-2)} N_D^{+}(d)$$

ou encore

$$N_D^{1+}(d) = \frac{2^d-1}{2^n-2} N_D^{1}(d)$$

Enfin, nous avons :

$$N_D^{--}(d) = N(d) - 3N_D^{+}(d) + 2N_D^{++}(d) = \frac{(2^n-2^d)(2^n-2^{d+1})}{(2^n-1)(2^n-2)} N_D(d)$$

et donc :

$$N_D^{2}(d) = \frac{N_D^{--}(d)}{(2^n-1)(2^n-2)} = \frac{(2^n-2^d)(2^n-2^{d+1})}{(2^n-1)^2(2^n-2)^2} N_D(d) = \frac{2^n-2^{d+1}}{(2^n-2)^2} N_D^{1}(d)$$

□

Des lemmes 23, 21 et 24, nous obtenons :

$$N_{2,D}^{+-}(d,d') = N_D^{+}(d) N_D^{1}(d')(2^n-1)\left(\frac{(2^d-2)(2^n-2^{d'+1})}{(2^n-2)^2} + \frac{(2^n-2^d)(2^{d'}-1)}{(2^n-1)(2^n-2)} + \frac{(2^n-2^d)(2^n-2^{d'+1})}{(2^n-1)(2^n-2)}\left(1 - \frac{1}{2^n-2}\right)\right)$$

Par ailleurs, le nombre total $N_{2,D}^{+-}$ de paires de polynômes $\mathbb{F}_2$-linéaires L, L' de degré 2^D vérifiant les conditions $\mathcal{C}_\Lambda$ est

$$N_{2,D}^{+-} = (2^n-1)^2 2^{n(2D-3)}(2^n-1)(2^n-2)$$

Le nombre total N_D^+ de polynômes $\mathbb{F}_2$-linéaire de degré 2^D dont le noyau contient a est, comme on l'a calculé à la section A.2.1, $(2^n-1)2^{n(D-1)}$. Enfin, le nombre N_D^- de polynômes $\mathbb{F}_2$-linéaires de degré 2^D ne s'annulant pas en b est lui : $(2^n-1)2^{n(D-1)}(2^n-1)$. Nous avons donc :

$$N_{2,D}^{+-} = N_D^{+} N_D^{-} 2^{-n}(2^n-2)$$

Finalement, nous obtenons :

$$\Lambda_{2,D}^{+-}(d,d') = \Lambda_D^{+}(d)\Lambda_D^{-}(d')(1+\epsilon'_{\Lambda,D})$$

où $\Lambda_D^+(d)$ et $\Lambda_D^-(d)$ sont respectivement les proportions de polynômes $\mathbb{F}_2$-linéaires de degré 2^D et s'annulant/ne s'annulant pas en un point prescrit pour lesquels le noyau est de dimension d, et

$$1 + \epsilon'_{\Lambda,D} = 1 - \frac{2^{d'}-1}{2^n-1} + \mathcal{O}(2^{-n}) = 1 + \mathcal{O}(2^{-n+D})$$

Calcul de $\mathcal{S}^{+-}_{2,L,L'}(i,i')$

Comme vu lors du calcul de $\mathcal{S}^{++}_{2,L,L'}(i,i')$, nous pouvons supposer que les noyaux de L et L' sont d'intersection zéro aux termes d'ordre 2^{-n+2D} près. Le point b n'est pas dans $\ker(L')$ et supposer que b n'est pas non plus dans $\ker(L)$ n'affecte que des termes d'ordre 2^{-n+D}. La condition $a \in \mathcal{K}$ avec le nombre de sous-espaces intersection avec $\ker(L)$ d'un facteur $(2^i-1)/(2^d-1)$. La condition $b \notin \mathcal{K}$ affecte le nombre de choix d'un sous-espace $\mathcal{K}$ de dimension $n-r$ d'intersections fixées de dimensions i, i' avec $\ker(L)$ et $\ker(L')$ d'un facteur $(2^n - 2^{i+i'})/(2^n - 2^{n-r})$. Par conséquent,

$$\eta^{+-}_{2,L,L'}(i,i') = \left(\frac{2^i-1}{2^d-1}\right) E(d,i)E(d',i') \left(\frac{2^n-2^{n-r}}{2^n-2^{i+i'}}\right) \frac{S(n,n-r)S(n-r,i+i')}{S(n,i+i')S(n-r,n-r)}$$

aux termes d'ordre 2^{-n+2D} près.

Par ailleurs, le nombre $\eta^{-}_{L'}(i')$ de sous-espaces de dimension $n-r$ ne contenant pas b et d'intersection de dimension i' avec $\ker(L')$ est :

$$\eta^{-}_{L'}(i') = E(d',i') \left(\frac{2^n-2^{n-r}}{2^n-2^{i'}}\right) \frac{S(n,n-r)S(n-r,i)}{S(n,i)S(n-r,n-r)}$$

Comme

$$2^n - 2^{i+i'} = (2^n - 2^{i'}) \left(1 - \frac{2^{i+i'}-2^{i'}}{2^n-2^{i'}}\right) = (2^n-2^{i'})(1+\mathcal{O}(2^{-n+2D}))$$

et nous avons déjà montré que

$$S(n,i+i') = S(n,i)S(n,i')(1+\mathcal{O}(2^{-n+2D}))$$

nous obtenons finalement :

$$\eta^{+-}_{2,L,L'}(i,i') = \eta^{+}_{L}(i)\eta^{-}_{L'}(i') \frac{S(n,n-r)}{S(n-r,n-r)}(1+\mathcal{O}(2^{-n+2D}))$$

Soit maintenant η^{+-}_2 le nombre total de sous-espaces de dimension $n-r$ contenant a et ne contenant pas b :

$$\eta^{+-}_2 = \frac{(2^{n-r}-1)(2^n-2^{n-r})}{(2^n-1)(2^n-2)} E(n,n-r)$$

Le nombre η^{+} de sous-espaces de dimension $n-r$ contenant a est :

$$\eta^{+} = \frac{2^{n-r}-1}{2^n-1} E(n,n-r)$$

et le nombre η^{-} de sous-espaces de dimension $n-r$ ne contenant pas b est :

$$\eta^{-} = \frac{2^n-2^{n-r}}{2^n-1} E(n,n-r)$$

Nous avons donc :

$$\eta_2^{+-} = \eta^+\eta^- E(n, n-r)(1 + \mathcal{O}(2^{-n}))$$

Finalement, notant $S^-_{L'}(i')$ la probabilité qu'un sous-espace aléatoire de dimension $n-r$ ne contenant pas b ait une intersection de dimension i' avec $\ker(L')$, nous obtenons :

$$S^{+-}_{2,L,L'}(i,i') = S^+_L(i) S^-_{L'}(i')(1 + \epsilon'_{\mathcal{S}})$$

avec $\epsilon'_{\mathcal{S}} = \mathcal{O}(2^{-n+2D})$.

Calcul de $\lambda^{+-}_{L,L',\mathcal{K},\mathcal{K}'}(t,t')$

Les conditions sur ℓ et ℓ' sont indépendantes. Par conséquent :

$$\lambda^{+-}_{L,L',\mathcal{K},\mathcal{K}'}(t,t') = \lambda^+_{L,\mathcal{K}}(t)\lambda^-_{L',\mathcal{K}'}(t')$$

Résultat du calcul de $\pi^{+-}(t,t')$

Finalement, nous obtenons :

$$\pi^{+-}(t,t') = \pi^+(t)\pi^-(t')(1 + \mathcal{O}(2^{-n+\max\{2D,r\}}))$$

A.2.3 Calcul de $\pi^{--}(t,t')$

Dans ce cas, nous avons :

$$\mathcal{C} : \begin{cases} L(a) = \ell(a) \neq 0 & , \quad L(a) + L(b) + L'(a) \neq 0 \\ L'(b) = \ell'(b) \neq 0 & , \quad L'(b) + L(b) + L'(a) \neq 0 \\ \ker(\ell) = \ker(\ell') & , \quad L(b) + L'(a) = \ell(b) + \ell'(a) \neq 0 \end{cases}$$

Ce jeu de conditions se séparent en :

$$\mathcal{C}_\Lambda : \begin{cases} L(a) \neq 0 \\ L'(b) \neq 0 \\ L(b) + L'(a) \neq 0 \\ L(a) + L(b) \\ \qquad + L'(a) \neq 0 \\ L'(b) + L(b) \\ \qquad + L'(a) \neq 0 \end{cases} \quad \mathcal{C}_\mathcal{S} : \begin{cases} a \notin \mathcal{K} \\ b \notin \mathcal{K}' \\ \mathcal{K} = \mathcal{K}' \end{cases} \quad \mathcal{C}_\lambda : \begin{cases} \ell(a) = L(a) \\ \ell'(b) = L'(b) \\ \ell(b) + \ell'(a) \\ = L(b) + L'(a) \end{cases}$$

affectant respectivement $\Lambda^{--}_{2,D}(d,d')$, $\mathcal{S}^{--}_{2,L,L'}(i,i')$ et $\lambda^{--}_{L,L',\mathcal{K},\mathcal{K}'}(t,t')$.

Calcul de $\Lambda^{--}_{2,D}(d,d')$

Le lemme suivant fournit l'expression de $N^{--}_{2,D}(d,d')$:

Lemme 25. *Soit a,b deux éléments non-nuls et distincts de $(\mathbb{F}_2)^n$. Pour tout entiers $d,d' \leq D$, nous avons :*

$$N^{--}_{2,D}(d,d') = (2^n-1)(2^n-2)^2 \left(N^{1+}_D(d)N^2_D(d') + N^2_D(d)N^{1+}_D(d') + \frac{1}{2^n-2}(N^1_D(d) - 2N^{1+}_D(d) - N^2_D(d))(N^1_D(d') - 2N^{1+}_D(d') - N^2_D(d')) \right)$$

Démonstration. Soit v_a, v_b et $v_{a,b}$ non-nuls tels que $v_a + v_{a,b}$ et $v_b + v_{a,b}$ sont non-nuls. Le nombre de choix de deux tels éléments est $(2^n-1)(2^n-2)^2$. Pour tout choix, nous définissons les conditions

$$\mathcal{C}_\Lambda(v_a, v_b, v_{a,b}) = \begin{cases} L(a) = v_a \\ L'(b) = v_b \\ L(b) + L'(a) = v_{a,b} \end{cases}$$

L'union disjointe de ces conditions forme la condition $\mathcal{C}_\Lambda$.

Lorsque $L(b) = 0$, nous avons $L'(a) = v_{a,b}$, et comme $v_{a,b} + v_b$ est non-nul le nombre de telles applications L et L' est respectivement $N^{1+}_D(d)$ et $N^2_D(d')$. Lorsque $L(b) = v_{a,b}$, nous avons $L'(a) = 0$, et comme $v_{a,b}+v_a$ est non-nul le nombre de telles applications L et L' est respectivement $N^2_D(d)$ et $N^{1+}_D(d')$. Lorsque $L(b)$ n'est ni 0 ni v_{ab}, nous avons également $L'(a) \neq 0$ et $L'(a) \neq v_{ab}$; le nombre de telles applications L est $N^1_D(d) - 2N^{1+}_D(d) - N^2_D(d)$, et pour tout L, le nombre d'applications L' vérifiant la troisième condition est $(N^1_D(d') - 2N^{1+}_D(d') - 2N^2_D(d'))/(2^n-2)$. □

Des lemmes 25, 21 et 24, nous obtenons :

$$N^{--}_{2,D}(d,d') = N^1_D(d)N^1_D(d')(2^n-1)^2 \left(\frac{(2^d-1)(2^n-2^{d'+1})}{(2^n-1)(2^n-2)} + \frac{(2^n-2^{d+1})(2^{d'}-1)}{(2^n-1)(2^n-2)} + \frac{(2^n-2^{d+1})(2^n-2^{d'+1})}{(2^n-2)^2}\left(1 - \frac{1}{2^n-2}\right)^2 \right)$$

Par ailleurs, le nombre total $N^{--}_{2,D}$ de paires de polynômes $\mathbb{F}_2$-linéaires L, L' de degré 2^D vérifiant les conditions $\mathcal{C}_\Lambda$ est

$$N^{--}_{2,D} = (2^n-1)^2 2^{n(2D-3)}(2^n-1)(2^n-2)^2$$

Le nombre N^-_D de polynômes $\mathbb{F}_2$-linéaires de degré 2^D ne s'annulant pas en b est $(2^n-1)2^{n(D-1)}(2^n-1)$. Nous avons donc :

$$N^{--}_{2,D} = N^-_D N^-_D 2^{-n}(2^n-2)^2/(2^n-1)$$

Finalement, nous obtenons :

$$\Lambda^{--}_{2,D}(d,d') = \Lambda^{-}_{D}(d)\Lambda^{-}_{D}(d')(1+\epsilon''_{\Lambda,D})$$

où $\Lambda^{-}_{D}(d)$ est la proportion de polynômes $\mathbb{F}_2$-linéaires de degré 2^D et ne s'annulant pas en un point prescrit pour lesquels le noyau est de dimension d, et

$$1+\epsilon''_{\Lambda,D} = 1 - \left(\frac{2^d-1}{2^n-1} + \frac{2^{d'}-1}{2^n-1}\right) + \mathcal{O}(2^{-n}) = 1+\mathcal{O}(2^{-n+D})$$

Calcul de $\mathcal{S}^{--}_{2,L,L'}(i,i')$

Comme vu lors du calcul de $\mathcal{S}^{++}_{2,L,L'}(i,i')$, nous pouvons supposer que les noyaux de L et L' sont d'intersection zéro aux termes d'ordre 2^{-n+2D} près. L'élément a n'est pas dans $\ker(L)$ et supposer qu'il n'est pas non plus dans $\ker(L')$ n'affectent que des termes d'ordre 2^{-n+D} ; de même pour b. Supposer que le point $a+b$ n'est ni $\ker(L)$ ni dans $\ker(L')$ n'affectent que des termes d'ordre 2^{-n+2D}. Finalement, nous pouvons supposer $Vect(a,b)$ d'intersection zéro avec $\ker(L)$ et $\ker(L')$.

Les sous-espaces $\mathcal{K}$ de dimension $n-r$ ne contenant pas a et b se séparent en deux catégories : ceux ne contenant pas non plus $a+b$ et ceux contenant $a+b$. Dans le premier cas, la condition affecte le nombre de sous-espaces de dimension $n-r$ d'intersections fixées de dimensions i,i' avec $\ker(L)$ et $\ker(L')$ d'un facteur :

$$\frac{(2^n-2^{n-r})(2^n-2^{n-r+1})}{(2^n-2^{i+i'})(2^n-2^{i+i'+1})}$$

Dans l'autre cas, la condition affecte le nombre de sous-espaces de dimension $n-r$ d'intersections fixées de dimensions i,i' avec $\ker(L)$ et $\ker(L')$ d'un facteur :

$$\frac{(2^n-2^{n-r})(2^{n-r}-2^{i+i'})}{(2^n-2^{i+i'})(2^n-2^{i+i'+1})}$$

La somme des deux facteurs distinguant ces deux proportions est

$$2^n-2^{n-r}-2^{i+i'} = (2^n-2^{n-r})\left(1-\frac{2^{i+i'}}{2^n-2^{n-r}}\right) = (2^n-2^{n-r})(1+\mathcal{O}(2^{-n+2D}))$$

Par conséquent,

$$\eta^{--}_{2,L,L'}(i,i') = E(d,i)E(d',i')\frac{(2^n-2^{n-r})^2}{(2^n-2^{i+i'})(2^n-2^{i+i'+1})}\frac{S(n,n-r)S(n-r,i+i')}{S(n,i+i')S(n-r,n-r)}$$

aux termes d'ordre 2^{-n+2D} près. Comme

$$\eta^{-}_{L}(i) = E(d',i')\left(\frac{2^n-2^{n-r}}{2^n-2^{i'}}\right)\frac{S(n,n-r)S(n-r,i)}{S(n,i)S(n-r,n-r)}$$

et nous avons montré précédemment que

$$2^n - 2^{i+i'} = (2^n - 2^{i'})(1+\mathcal{O}(2^{-n+2D})) \quad \text{et} \quad S(n, i+i') = S(n,i)S(n,i')(1+\mathcal{O}(2^{-n+2D}))$$

nous obtenons :

$$\eta^{--}_{2,L,L'}(i,i') = \eta^{-}_{L}(i)\eta^{-}_{L'}(i')\frac{S(n,n-r)}{S(n-r,n-r)}(1+\mathcal{O}(2^{-n+2D}))$$

De même, le nombre total η^{--}_2 de sous-espaces de dimension $n-r$ ne contenant pas a et b est :

$$\eta^{--}_2 = \left(\frac{(2^n-2^{n-r})(2^n-2^{n-r+1})}{(2^n-1)(2^n-2)} + \frac{(2^n-2^{n-r})(2^n-2^{n-r+1})}{(2^n-1)(2^n-2)}\right) E(n,n-r)$$

soit encore :

$$\eta^{--}_2 = \frac{(2^n-2^{n-r})^2}{(2^n-1)(2^n-2)} E(n,n-r)(1+\mathcal{O}(2^{-n}))$$

Nous avons donc, en fonction du nombre η^- introduit lors du calcul de $\mathcal{S}^{+-}_{2,L,L'}(i,i')$,

$$\eta^{--}_2 = (\eta^-)^2 E(n,n-r)(1+\mathcal{O}(2^{-n}))$$

Finalement, notant $S^-_{L'}(i')$ la probabilité qu'un sous-espace aléatoire de dimension $n-r$ ne contenant pas b ait une intersection de dimension i' avec $\ker(L')$, nous obtenons :

$$S^{--}_{2,L,L'}(i,i') = S^-_L(i)S^-_{L'}(i')(1+\epsilon''_{\mathcal{S}})$$

avec $\epsilon''_{\mathcal{S}} = \mathcal{O}(2^{-n+2D})$.

Calcul de $\lambda^{--}_{L,L',\mathcal{K},\mathcal{K}'}(t,t')$

La corrélation entre les choix de ℓ et ℓ' provient de la condition $(L'+\ell')(a) = (L+\ell)(b) \neq 0$. Pour tout ℓ, cette condition fixe la valeur en a de ℓ', ce qui affecte le nombre de ces applications d'un facteur $1/(2^n-1)$, indépendamment de la dimension du noyau de $L+\ell$ qui ne contient pas a. Par conséquent, la proportion $\lambda^{--}_{L,L',\mathcal{K},\mathcal{K}'}(t,t')$ est strictement égale au produit des deux proportions $\lambda^-_{L,\mathcal{K}}(t)$ et $\lambda^-_{L',\mathcal{K}'}(t')$ dont le calcul a été effectué à la section 9.4.1.

Résultat du calcul de $\pi^{--}(t,t')$

Finalement, nous obtenons :

$$\pi^{--}(t,t') = \pi^-(t)\pi^-(t')(1+\mathcal{O}(2^{-n+\max\{2D,r\}}))$$

Bibliographie

[1] M. Bardet. *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie.* PhD thesis, Université Paris 6, 2004.

[2] M. Bardet, J.-C. Faugère, and B. Salvy. On the Complexity of Gröbner Basis Computation of Semi-Regular Overdetermined Algebraic Equations. In *ICPSS International Conference on Polynomial System Solving*, 2004.

[3] A. Barg. *Handbook of Coding Theory*, chapter 7, Complexity Issue in Coding Theory. North Holland, 1999.

[4] E. Biham. Cryptanalysis of Patarin's 2-Round Public Key System with S-Boxes (2R). In *EUROCRYPT*, pages 408–416, 2000.

[5] O. Billet and H. Gilbert. Cryptanalysis of Rainbow. In R. D. Prisco and M. Yung, editors, *SCN*, volume 4116 of *Lecture Notes in Computer Science*, pages 336–347. Springer, 2006.

[6] A. Blokhuis, R. Coulter, M. Henderson, and C. O'Keefe. Permutations amongst the Dembowski-Ostrom polynomials. In *Proceedings of the Fifth International Conference on Finite Fields and Applications*, pages 37–42, 2001.

[7] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassnringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Innsbruck, 1965.

[8] B. Buchberger. An Algorithmical Criterion for the Solvability of Algebraic Systems. *Aequationes Mathematicae*, 4 :374–383, 1970.

[9] B. Buchberger. A criterion for detecting unnecessary reductions in the construction of Groebner bases. In E. W. Ng, editor, *EUROSAM*, volume 72 of *Lecture Notes in Computer Science*, pages 3–21. Springer, 1979.

[10] J. J. Cade. A Public Key Cipher which allows Signatures. In *2nd SIAM Conference on Applied Linear Algebra*, 1985.

[11] J. J. Cade. A Modification of a Broken Public-Key Cipher. In A. M. Odlyzko, editor, *CRYPTO*, volume 263 of *Lecture Notes in Computer Science*, pages 64–83. Springer, 1986.

[12] F. Chabaud and J. Stern. The Cryptographic Security of the Syndrome Decoding Problem for Rank Distance Codes. In K. Kim and T. Matsumoto, editors, *ASIACRYPT*, volume 1163 of *Lecture Notes in Computer Science*, pages 368–381. Springer, 1996.

[13] W. Y. Chen and G.-C. Rota. q-Analogs of the Inclusion-Exclusion Principle and Permutations with Restricted Positions. *Discrete Mathematics*, 104 :7–22, 1992.

[14] S. Collart, M. Kalkbrener, and D. Mall. Converting Bases with the Gröbner Walk. *J. Symb. Comput.*, 24(3/4) :465–469, 1997.

[15] D. Coppersmith, J. Stern, and S. Vaudenay. The Security of the Birational Permutation Signature Schemes. *J. Cryptology*, 10(3) :207–221, 1997.

[16] N. Courtois. *La sécurité des primitives cryptographiques basées sur des problèmes algébriques multivariables*. PhD thesis, Université Paris 6, 2001.

[17] N. Courtois. The Security of Hidden Field Equations (HFE). In D. Naccache, editor, *CT-RSA*, volume 2020 of *Lecture Notes in Computer Science*, pages 266–281. Springer, 2001.

[18] N. Courtois, M. Finiasz, and N. Sendrier. How to Achieve a McEliece-Based Digital Signature Scheme. In C. Boyd, editor, *ASIACRYPT*, volume 2248 of *Lecture Notes in Computer Science*, pages 157–174. Springer, 2001.

[19] N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In *EUROCRYPT*, pages 392–407, 2000.

[20] J. Ding. A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation. In F. Bao, R. H. Deng, and J. Zhou, editors, *Public Key Cryptography*, volume 2947 of *Lecture Notes in Computer Science*, pages 305–318. Springer, 2004.

[21] J. Ding and J. E. Gower. Inoculating Multivariate Schemes Against Differential Attacks. In M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, editors, *Public Key Cryptography*, volume 3958 of *Lecture Notes in Computer Science*, pages 290–301. Springer, 2006.

[22] J. Ding, J. E. Gower, D. Schmidt, C. Wolf, and Z. Yin. Complexity Estimates for the F_4 Attack on the Perturbed Matsumoto-Imai Cryptosystem. In N. P. Smart, editor, *IMA Int. Conf.*, volume 3796 of *Lecture Notes in Computer Science*, pages 262–277. Springer, 2005.

[23] J. Ding and D. Schmidt. Cryptanalysis of HFEv and Internal Perturbation of HFE. In S. Vaudenay, editor, *Public Key Cryptography*, volume 3386 of *Lecture Notes in Computer Science*, pages 288–301. Springer, 2005.

[24] J. Ding and D. Schmidt. Rainbow, a New Multivariable Polynomial Signature Scheme. In J. Ioannidis, A. D. Keromytis, and M. Yung, editors, *ACNS*, volume 3531 of *Lecture Notes in Computer Science*, pages 164–175, 2005.

[25] J. Ding, D. Schmidt, and Z. Yin. Cryptanalysis of the new TTS scheme in CHES 2004. *Int. J. Inf. Sec.*, 5(4) :231–240, 2006.

[26] V. Dubois, P.-A. Fouque, A. Shamir, and J. Stern. Practical Cryptanalysis of SFLASH. In A. Menezes, editor, *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2007.

[27] V. Dubois, P.-A. Fouque, and J. Stern. Cryptanalysis of SFLASH with Slightly Modified Parameters. In *Proceedings of Eurocrypt 2007*, volume LNCS 4515, pages 264–275, 2007.

[28] V. Dubois, L. Granboulan, and J. Stern. An Efficient Provable Distinguisher for HFE. In M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, editors, *ICALP (2)*, volume 4052 of *Lecture Notes in Computer Science*, pages 156–167. Springer, 2006.

[29] V. Dubois, L. Granboulan, and J. Stern. Cryptanalysis of HFE with Internal Perturbation. In *Proceedings of PKC 2007*, volume LNCS 4450, pages 249–265. Springer, 2007.

[30] D. Estes, L. M. Adleman, K. Kompella, K. S. McCurley, and G. L. Miller. Breaking the Ong-Schnorr-Shamir Signature Scheme for Quadratic Number Fields. In H. C. Williams, editor, *CRYPTO*, volume 218 of *Lecture Notes in Computer Science*, pages 3–13. Springer, 1985.

[31] J.-C. Faugère, P. M. Gianni, D. Lazard, and T. Mora. Efficient Computation of Zero-Dimensional Gröbner Bases by Change of Ordering. *J. Symb. Comput.*, 16(4) :329–344, 1993.

[32] J.-C. Faugère and A. Joux. Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases. In D. Boneh, editor, *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 44–60. Springer, 2003.

[33] J.-C. Faugère and L. Perret. Cryptanalysis of $2R^-$ Schemes. In C. Dwork, editor, *CRYPTO*, volume 4117 of *Lecture Notes in Computer Science*, pages 357–372. Springer, 2006.

[34] J.-C. Faugère and L. Perret. Polynomial Equivalence Problems : Algorithmic and Theoretical Aspects. In S. Vaudenay, editor, *EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 30–47. Springer, 2006.

[35] J.-C. Faugère. A New Efficient Algorithm for Computing Gröbner Bases (F4). *Journal of Pure and Applied Algebra*, 139 :61–88, 1999.

[36] J.-C. Faugère. A New Efficient Algorithm for Computing Gröbner Bases without Reductions to Zero $F5$. In *ISSAC*, pages 75–83, 2002.

[37] P. Felke. On the Affine Transformations of HFE-Cryptosystems and Systems with Branches. In Ø. Ytrehus, editor, *WCC*, volume 3969 of *Lecture Notes in Computer Science*, pages 229–241. Springer, 2005.

[38] H. J. Fell and W. Diffie. Analysis of a Public Key Approach Based on Polynomial Substitution. In H. C. Williams, editor, *CRYPTO*, volume 218 of *Lecture Notes in Computer Science*, pages 340–349. Springer, 1985.

[39] S. Finch. *Mathematical Constants*, pages 354–361. Cambridge, 2003.

[40] P.-A. Fouque, L. Granboulan, and J. Stern. Differential Cryptanalysis for Multivariate Schemes. In R. Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 341–353. Springer, 2005.

[41] M. R. Garey and D. S. Johnson. *Computer and Intractability : A Guide to the Theory of NP-Completeness*. Freeman, 1979.

[42] W. Geiselmann, R. Steinwandt, and T. Beth. Attacking the Affine Parts of SFLASH. In B. Honary, editor, *IMA Int. Conf.*, volume 2260 of *Lecture Notes in Computer Science*, pages 355–359. Springer, 2001.

[43] H. Gilbert and M. Minier. Cryptanalysis of SFLASH. In L. R. Knudsen, editor, *EUROCRYPT*, volume 2332 of *Lecture Notes in Computer Science*, pages 288–298. Springer, 2002.

[44] J. Goldman and G.-C. Rota. The Number of Subspaces of a Vector Space. In W.T.Tutte, editor, *Recent Progress in Combinatorics*, pages 75–83. Academic Press, 1969.

[45] J. Goldman and G.-C. Rota. On the Foundations of Combinatorial Theory. IV. Finite Vector Spaces and Eulerian Generating Functions. *Studies in Applied Mathematics*, 49 :239–258, 1970.

[46] L. Goubin and N. Courtois. Cryptanalysis of the TTM Cryptosystem. In T. Okamoto, editor, *ASIACRYPT*, volume 1976 of *Lecture Notes in Computer Science*, pages 44–57. Springer, 2000.

[47] H. Imai and T. Matsumoto. Algebraic Methods for Constructing Asymmetric Cryptosystems. In J. Calmet, editor, *AAECC*, volume 229 of *Lecture Notes in Computer Science*, pages 108–119. Springer, 1985.

[48] N. S. James, R. Lidl, and H. Niederreiter. A Cryptanalytic Attack on the Cade Cryptosystem. In *EUROCRYPT*, page 27, 1986.

[49] N. S. James, R. Lidl, and H. Niederreiter. Breaking the Cade Cipher. In A. M. Odlyzko, editor, *CRYPTO*, volume 263 of *Lecture Notes in Computer Science*, pages 60–63. Springer, 1986.

[50] Jean-Charles Faugère. HFE Challenge 1 broken in 96 hours. Announcement that appeared in news ://sci.crypt, 19 of April 2002.

[51] Jean-Charles Faugère. Algebraic Cryptanalysis of HFE using Gröbner Bases. Technical Report 4738, INRIA, 2003.

[52] S. A. Joni and G.-C. Rota. A Vector Space Analog of Permutations with Restricted Position. *J. Comb. Theory, Ser. A*, 29(1) :59–73, 1980.

[53] A. Kipnis, J. Patarin, and L. Goubin. Unbalanced Oil and Vinegar Signature Schemes. In *EUROCRYPT*, pages 206–222, 1999.

[54] A. Kipnis and A. Shamir. Cryptanalysis of the Oil & Vinegar Signature Scheme. In H. Krawczyk, editor, *CRYPTO*, volume 1462 of *Lecture Notes in Computer Science*, pages 257–266. Springer, 1998.

[55] A. Kipnis and A. Shamir. Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In M. J. Wiener, editor, *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 1999.

[56] D. Lazard. Gröbner-Bases, Gaussian Elimination and Resolution of Systems of Algebraic Equations. In J. A. van Hulzen, editor, *EUROCAL*, volume 162 of *Lecture Notes in Computer Science*, pages 146–156. Springer, 1983.

[57] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its applications*. Cambridge University Press, 1997.

[58] Louis Granboulan and Antoine Joux and Jacques Stern. Inverting HFE Is Quasipolynomial. In C. Dwork, editor, *CRYPTO*, volume 4117 of *Lecture Notes in Computer Science*, pages 345–356. Springer, 2006.

[59] T. Matsumoto and H. Imai. Public Quadratic Polynominal-Tuples for Efficient Signature-Verification and Message-Encryption. In *EUROCRYPT*, pages 419–453, 1988.

[60] T. Matsumoto, H. Imai, H. Harashima, and H. Miyakawa. An Asymmetric Bijective Cryptosystem using a System of Polynomials in Several Indeterminates as a Public Key. In *Proc. of the 6th Symposium on Information Theory and its Applications*, pages 263–268, nov. 1983. (in japanese).

[61] R. J. McEliece. A Public-Key Cryptosystem based on Algebraic Coding Theory. In *JPL DSN Progress Report*, pages 114–116, California Inst. Technol., Pasadena, 1978.

[62] T. T. Moh. A Fast Public Key System with Signature and Master Key Functions. In *Proceedings of CrypTEC'99, International Workshop on Cryptographic Techniques and E-commerce*, pages 63–69, 1999.

[63] R. Motwani and P. Raghavan. *Randomized Algorithms*, chapter 4, pages 67–74. Cambridge University Press, 1995.

[64] NESSIE. *Portfolio of Recommended Cryptographic Primitives.* `http://www.nessie.eu.org/index.html`.

[65] H. Ong, C.-P. Schnorr, and A. Shamir. An Efficient Signature Scheme Based on Quadratic Equations. In *STOC*, pages 208–216. ACM, 1984.

[66] H. Ong, C.-P. Schnorr, and A. Shamir. Efficient Signature Schemes Based on Polynomial Equations. In *CRYPTO*, pages 37–46, 1984.

[67] J. Patarin. Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88. In D. Coppersmith, editor, *CRYPTO*, volume 963 of *Lecture Notes in Computer Science*, pages 248–261. Springer, 1995.

[68] J. Patarin. Asymmetric Cryptography with a Hidden Monomial. In N. Koblitz, editor, *CRYPTO*, volume 1109 of *Lecture Notes in Computer Science*, pages 45–60. Springer, 1996.

[69] J. Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP) : Two New Families of Asymmetric Algorithms. In *EUROCRYPT*, pages 33–48, 1996.

[70] J. Patarin. The Oil and Vinegar Signature Scheme. Presented at the Dagstuhl Workshop on Cryptography (transparencies), september 1997.

[71] J. Patarin and L. Goubin. Asymmetric cryptography with S-Boxes. In Y. Han, T. Okamoto, and S. Qing, editors, *ICICS*, volume 1334 of *Lecture Notes in Computer Science*, pages 369–380. Springer, 1997.

[72] J. Patarin and L. Goubin. Trapdoor One-Way Permutations and Multivariate Polynominals. In Y. Han, T. Okamoto, and S. Qing, editors, *ICICS*, volume 1334 of *Lecture Notes in Computer Science*, pages 356–368. Springer, 1997.

[73] J. Patarin, L. Goubin, and N. Courtois. ${C^*}_{-+}$ and HM : Variations Around Two Schemes of T. Matsumoto and H. Imai. In K. Ohta and D. Pei, editors, *ASIACRYPT*, volume 1514 of *Lecture Notes in Computer Science*, pages 35–49. Springer, 1998.

[74] J. Patarin, L. Goubin, and N. Courtois. Improved Algorithms for Isomorphisms of Polynomials. In *EUROCRYPT*, pages 184–200, 1998.

[75] L. Perret. A Fast Cryptanalysis of the Isomorphism of Polynomials with One Secret Problem. In R. Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 354–370. Springer, 2005.

[76] J. M. Pollard and C.-P. Schnorr. An Efficient Solution of the Congruence $x^2+ky^2 = m \mod n$. *IEEE Transactions on Information Theory*, 33(5) :702–709, 1987.

[77] A. Shamir. Efficient Signature Schemes Based on Birational Permutations. In D. R. Stinson, editor, *CRYPTO*, volume 773 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 1993.

[78] J. von zur Gathen and V. Shoup. Computing Frobenius Maps and Factoring Polynomials (Extended Abstract). In *STOC*, pages 97–105. ACM, 1992.

[79] B.-Y. Yang, J.-M. Chen, and Y.-H. Chen. TTS : High-Speed Signatures on a Low-Cost Smart Card. In M. Joye and J.-J. Quisquater, editors, *CHES*, volume 3156 of *Lecture Notes in Computer Science*, pages 371–385. Springer, 2004.

[80] D. Ye, K.-Y. Lam, and Z.-D. Dai. Cryptanalysis of "2R" Schemes. In M. J. Wiener, editor, *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 315–325. Springer, 1999.

Résumé

La cryptographie multivariée peut être définie comme la cryptographie à clé publique basée sur la difficulté de résoudre des systèmes polynomiaux à plusieurs variables. Bien que la recherche de tels schémas soit apparue dès le début des années 80, elle s'est surtout développée depuis une dizaine d'années, et a conduit à l'émergence de plusieurs propositions jugées prometteuses, telles que le cryptosystème HFE et le schéma de signature SFLASH ; ce dernier est notamment l'un des trois schémas de signature recommandés par le consortium européen NESSIE avec RSA-PSS et ECDSA. Les shémas multivariés se posent ainsi en alternative possible aux schémas traditionnels basés sur des problèmes de théorie des nombres, et constituent des solutions efficaces pour l'implantation des fonctionnalités de la cryptographie à clé publique.

Lors d'Eurocrypt 2005, Fouque, Granboulan et Stern ont proposé une nouvelle approche cryptanalytique pour les schémas multivariés basée sur l'étude d'invariants liés à la *différentielle*, et ont démontré la pertinence de cette approche par la cryptanalyse du schéma PMI proposé par Ding.

Au cours de cette thèse, nous avons développé l'approche différentielle proposée par Fouque *et al.* dans deux directions. La première consiste en un traitement combinatoire des invariants dimensionnels de la différentielle. Ceci nous a permis de montrer qu'une clé publique HFE pouvait être distinguée d'un système quadratique aléatoire en temps quasipolynomial, invalidant ainsi l'argument de sécurité classique fondé sur la difficulté générique de la résolution d'un tel système. Une seconde application de cette même approche nous a permis de cryptanalyser une variation de HFE proposée par Ding et Schmidt à PKC 2005. Le second développement de la thèse est la découverte d'invariants fonctionnels de la différentielle et nous a permis de montrer la faiblesse du schéma SFLASH recommandé par NESSIE ; l'attaque permet en effet de forger des signatures en quelques minutes pour ces paramètres.

Mots-clés : cryptologie, cryptographie à clé publique, cryptogtaphie multivariée, cryptanalyse, différentielle, HFE, SFLASH.

Abstract

Multivariate Cryptography can be defined as public key cryptography based on the computational hardness of solving a system of polynomial equations in several variables. Although research on such schemes appeared in the early 80s, it has really been developed over the last ten years, and has given rise to several promising proposals, such as the HFE cryptosystem and the SFLASH signature scheme. Notably, the latter is one of only three signature schemes recommended by the NESSIE European consortium along with RSA-PSS and ECDSA. Multivariate schemes therefore stand as possible alternatives to the traditional schemes based on problems from number theory, and as efficient solutions for the implementation of public key functionality.

At the Eurocrypt 2005 conference, Fouque, Granboulan and Stern proposed a new cryptanalytic approach for multivariate schemes based on the analysis of invariants related to the differential of the public key, and demonstrated the relevance of this approach by cryptanalyzing the PMI scheme proposed by Ding.

In this thesis, we develop the differential approach proposed by Fouque *et al.* in two directions. The first one consists of a combinatorial treatment of the dimensional invariants of the differential, which enables us to show that an HFE public key can be distinguished from a random system of quadratic equations in quasipolynomial time, countering the classical security argument based on the generic intractability of solving such a system of equations. A second application of the same approach leads to a cryptanalysis of a variation of HFE proposed by Ding and Schmidt at PKC 2005. The second development of this thesis is the exposure of functional invariants of the differential, which enables us to completely cryptanalyze the SFLASH scheme with the parameters recommended by NESSIE ; the attack makes it possible to forge a signature for an arbitrary message within a few minutes on a single PC.

Keywords : cryptology, public key cryptography, multivariate cryptography, cryptanalysis, differential, HFE, SFLASH.