SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

Bureau d'accueil des doctorants
15 rue de l'École de Médecine
75006 PARIS
email : scolarite.doctorat@upmc.fr

Spécialité :

INFORMATIQUE, TELECOMMUNICATIONS ET ELECTRONIQUE DE PARI

PROCES VERBAL ET RAPPORT de SOUTENANCE de THESE

Thèse soutenue le 17 Décembre 2019

Par **M. DEBRIS, THOMAS**

Sujet de la thèse

Cryptographie fondée sur les codes : nouvelles approches pour constructions et preuves ; contribution en cryptanalyse

Jury M. GABORIT PHILIPPE, Rapporteur, M. STEHLE DAMIEN, Rapporteur, M. DUCAS LEO, Rapporteu M. AUGOT DANIEL, Membre du jury, M. ZEMOR GILLES, Membre du jury, Mme VALIBOUZE ANNICK, Membre du jury, M. TILLICH JEAN-PIERRE, Directeur de thèse, M. SENDRIER NICOLAS, Membre du jury

Décision du jury

Conformément à l'article 18 de l'arrêté du 25 mai 2016 fixant le cadre national de la formation et les modalités conduisant à la délivrance du diplôme national de doctorat, le directeur de thèse participe au jury, mais ne prend pas part à la décision.

☐ Ajourné ☐ Admis ☐ Admis sous réserve de l'introduction de corrections majeures demandées par le jury ☒ Admis avec corrections mineures sous la responsabilité du docteur

Membre du jury (nom et prénom) désigné pour la vérification des corrections majeures :

Paris, le 17/12/2019

Le président du jury :
NOM : AUGOT
PRÉNOM : Daniel
Signature :

Seul le président du jury signe le procès-verbal de soutenance.
Utiliser le verso de ce document pour le rapport de soutenance. Tous les membres du jury, y compris le directeur de thèse, signent le rapport de soutenance et indiquent leur nom en toutes lettres. Si, exceptionnellement le rapport de soutenance est rédigé dans une autre langue que le français, la traduction en français de ce document devra être signée par le président du jury.
Mention : Conformément à la réglementation en vigueur, aucune mention n'est délivrée.

Thomas Debris-Alazard a donné un exposé pédagogique et bien mené en présentant ses nombreuses contributions tant en cryptanalyse qu'en cryptographie, dans le domaine de la cryptologie post-quantique fondée sur les codes correcteurs. Il s'est ensuite focalisé sur un résultat important: la conception d'un schéma de signature (WAVE) qui lui a valu le prix du "meilleur article" à la conférence Asiacrypt 2019. L'ensemble de ses travaux constitue une thèse exceptionnelle. Le jury a trouvé particulièrement remarquable que Thomas Debris-Alazard ait ouvert de nouvelles voies en introduisant le problème du décodage en grand poids. De surcroît, au delà de ces idées originales, le candidat a dû surmonter des obstacles très techniques, qu'il a su nous présenter de manière très didactique et intuitive.

Le candidat a répondu brillament aux questions, avec aisance, en convainquant le jury de sa maîtrise profonde de la cryptographie fondée sur les codes, mais aussi de sa compréhension de domaines connexes, en particulier la cryptographie fondée sur les réseaux euclidiens.

Le jury est certain qu'il a toutes les qualités requises pour faire un excellent chercheur ou enseignant-chercheur, et lui décerne le grade de docteur de Sorbonne Université en informatique

Gilles Zémor en visio

Philippe Gaborit en visio DA

Damien STEHLÉ

Nicolas SENDRIER

Léo DUCAS

Jean-Pierre TILLICH

Annick VALIBOUZE

AUGOT

ÉCOLE
NORMALE
SUPÉRIEURE
DE LYON

15 parvis René-Descartes
BP 7000, 69342 Lyon cedex 07
Tél. +33 (0)4 37 37 60 00
www.ens-lyon.fr

Damien STEHLÉ
Professeur des universités
Laboratoire de l'Informatique du Parallélisme (LIP)
École Normale Supérieure de Lyon
46 Allée d'Italie F69364 Lyon Cedex 07
damien.stehle@ens-lyon.fr

Lyon, le 26 novembre 2019

Rapport sur le mémoire de thèse présenté par

Thomas DEBRIS-ALAZARD

« Codes correcteurs et cryptographie : conception, analyse et attaques »

Dans son manuscrit, Thomas Debris-Alazard étudie divers aspects de la cryptographie reposant sur les codes. Un code est un sous-espace vectoriel d'un $\mathbb{F}_q^n$. Le problème algorithmique central portant sur les codes est celui du décodage : étant donné un code $\mathcal{C}$, et un élément $\mathbf{y}$ de $\mathbb{F}_q^n$, trouver un élément de $\mathcal{C}$ a distance w de $\mathbf{y}$ (pour une certaine notion de distance). La sécurité du schéma de chiffrement McEliece est fondée en partie sur la difficulté présumée de ce problème pour la distance de Hamming. Ce schéma a été très robuste face à toutes les tentatives de cryptanalyse dont il a fait l'objet depuis son introduction en 1978. En terme de signatures reposant sur les codes, la situation est comparativement mauvaise : de nombreuses signatures proposées ont été cryptanalysées, et celles qui semblent résister ont des tailles prohibitives. Par exemple, aucune signature reposant sur les codes n'est parvenue au deuxième tour du processus de standardisation de la cryptographie post-quantique, lancé par le NIST.

Les travaux de doctorat de Thomas Debris-Alazard portent principalement sur les signatures reposant sur les codes. Le premier, chronologiquement, est une cryptanalyse de Ranksign, un schéma de signature soumise au processus de standardisation du NIST, et utilisant la métrique rang plutôt que la distance de Hamming. Le second est une proposition d'une signature, baptisée Wave, inspirée de la signature de Gentry, Peikert et Vaikuntanathan, reposant elle sur les réseaux euclidiens. N'étant pas spécialiste de la métrique rang, je me focaliserai, dans ce rapport, surtout sur les contributions liées à Wave. Comme je le détaillerai plus bas, il s'agit d'une contribution **exceptionnelle**.

Le manuscrit se décompose en quatre grandes parties, chacune contenant plusieurs chapitres. La première partie est un état de l'art. Les autres parties contiennent des contributions originales, qui sont parues dans les actes de conférences internationales : SAC 2019 et ISIT 2017 pour la Partie II, ASIACRYPT 2019 pour la Partie III (cet article a d'ailleurs obtenu le prix du meilleur papier de cette conférence), et ASIACRYPT 2018 pour la Partie IV. Le contenu du manuscrit est thématiquement cohérent, mais de niveau un peu hétérogène : par exemple, la Partie III est impressionnante en termes de nouveauté et d'impact, alors que la Partie II se détache

ÉCOLE
NORMALE
SUPÉRIEURE
DE LYON

15 parvis René-Descartes
BP 7000, 69342 Lyon cedex 07
Tél. +33 (0)4 37 37 60 00
www.ens-lyon.fr

moins nettement de l'état de l'art. Aussi, du fait de cette production scientifique importante, le manuscrit est long. Il est écrit en français, ce qui a nécessité de traduire les articles, en sus de la rédaction de contenus spécifiquement pour le manuscrit. Vu l'effort considérable investi dans la rédaction, le lecteur se serait cependant attendu à une introduction plus riche.

La Partie I est un état de l'art sur la cryptographie reposant sur les codes. Il traite en particulier du problème de décodage, en poids de Hamming et en métrique rang, des approches existantes pour obtenir un chiffrement à l'aide des codes correcteurs, et des signatures reposant sur les codes. Un chapitre entier est consacré aux algorithmes de décodage pour le poids de Hamming. Ces rappels sont très complets, et également très bien présentés. Ils peuvent sans aucun doute servir de support pour un cours de Master ou permettre à un novice d'être rapidement opérationnel.

La deuxième partie est consacrée aux algorithmes de décodage.

Le premier chapitre de cette Partie II adapte et analyse les algorithmes de décodage existants (rappelés dans la Partie I), dans le cas spécifique où la distance au code est grande. Typiquement, ces algorithmes existants et leurs analyses s'intéressent au cas où la distance au code est petite, de telle sorte qu'on s'attend à très peu de solutions. Cela est dû à l'application à l'estimation de la sécurité des protocoles existants. Cependant, il convient de noter que ces protocoles utilisent souvent des poids d'erreurs sous-linéaires en la longeur du code, mais que ces algorithmes et leurs analyses se focalisent sur des poids linéaires. Il peut donc paraître encore plus étrange d'étudier ces algorithmes quand le poids des erreurs est très grand. La justification est la signature Wave, présentée dans la Partie III, dont la sécurité repose justement sur la difficulté présumée du décodage pour de grandes distances. Ce premier chapitre de la Partie II est donc essentiel, pour déterminer si ce problème du décodage pour de grandes distances a une chance d'être en effet difficile à résoudre.

Le second chapitre de la Partie II analyse une approche moins usuelle pour le décodage, consistant à se servir de vecteurs courts dans le code orthogonal pour "annuler" le mot du code dans les instances du problèmes de décodage et ainsi "révéler" l'erreur. Dans le cas des réseaux euclidiens, l'approche analogue, consistant à trouver des vecteurs courts dans le réseau dual, est très fréquemment utilisée, et, dans certains cas, préférable. L'analyse effectuée dans ce chapitre montre que la situation est à ce stade moins favorable dans le cas des codes, l'utilisation du code orthogonal ne semblant amener à des algorithmes compétitifs.

La troisième partie présente le schéma de signature Wave. Cette partie contient trois chapitres : le premier décrit Wave ; le second montre que Wave est sûr dans le modèle de l'oracle aléatoire, sous les hypothèses qu'une variante du problème du décodage est difficile, et qu'un code $(U, U+V)$ généralisé permuté est calculatoirement indistinguable d'un code aléatoire ; et le troisième est une étude la difficulté algorithmique de ce dernier problème, pour les approches algorithmiques existantes.

Une des techniques centrales de design cryptographique à l'aide de réseaux euclidiens est la fonction de Gentry, Peikert et Vaikuntanathan. L'idée est de se servir une trappe pour échantillonner des vecteurs courts (pour la norme euclidienne) ayant un syndrôme donné, de telle sorte que la distribution jointe d'un syndrôme uniforme et d'un vecteur court lui correspondant ne dépende pas de la trappe. Plus formellement, il faut que cette distribution jointe puisse être simulée sans la trappe. Dans ce chapitre, Thomas Debris-Alazard introduit la première adaptation de cette technique à la cryptographie reposant sur les codes. Pour cela, il propose une famille de codes pour lesquels il montre qu'il est possible de résoudre le problème du décodage pour des poids inatteignables avec des codes génériques (c'est la trappe), et il propose une distribution des préimages d'un syndrôme donné qui est échantillonnable à l'aide de la trappe, et telle que la distribution jointe d'un syndrôme

ÉCOLE
NORMALE
SUPÉRIEURE
DE LYON

15 parvis René-Descartes
BP 7000, 69342 Lyon cedex 07
Tél. +33 (0)4 37 37 60 00
www.ens-lyon.fr

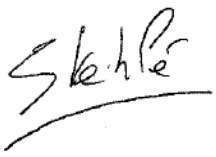
uniforme et d'une préimage de celui-ci peut être publiquement simulée. Il y a une quantité fort conséquente de méthodes nouvelles dans cette construction : utilisations des codes généralisés $(U, U+V)$ et du module $q = 3$, fondement de la sécurité sur la difficulté du problème de décodage pour des mots de poids forts, étude algorithmique de ce problème (dans la Partie II), échantillonnage de la distribution des préimages à l'aide de rejet. C'est un résultat très novateur, ayant le potentiel de changer significativement le domaine. Il amène un nombre de questions ouvertes important, incluant par exemple le design de protocoles cryptorgaphiques plus avancés, et l'algorithmique (classique et quantique) pour résoudre les problèmes utilisés comme fondements de sécurité. C'est très certainement à ce jour la signature reposant sur les codes qui est la plus viable, et sans aucun doute la plus élégante.

La quatrième partie présente des cryptanalyses d'une signature et d'un chiffrement reposant sur l'identité, qui faisaient intervenir la métrique rang plutôt que la distance de Hamming. Cela est plus éloigné de mon domaine d'expertise, et j'ai compris que ces contributions sont discutées par un autre rapporteur. Je me contenterai donc d'observer qu'il s'agit d'un résultat important, en le sens qu'il a mis à mal une approche qui paraissait pourtant prometteuse pour obtenir des signatures efficaces reposant sur les codes.

Conclusion. Le manuscrit de thèse de Thomas Debris-Alazard contient des contributions novatrices, pertinentes et ouvrant de nombreuses perspectives de recherche. La signature Wave est en rupture avec les approches existantes en cryptographie reposant sur les codes, et ce pour de multiples raisons. Cette contribution justifierait à elle seule l'obtention du diplôme de doctorat. Le candidat ne s'est pas arrêté là, et le manuscrit contient d'autres contributions importantes, notamment sur la cryptographie reposant sur les codes en métrique rang. Le manuscrit témoigne d'une maîtrise technique impressionnante et d'une compréhension large du domaine.

En conclusion, j'exprime un avis très favorable à la soutenance de cette thèse devant le jury.

Damien Stehlé



institut de recherche
UMR 7252

Rapport sur le mémoire de thèse

de Thomas Debris-Alazard
« Codes correcteurs et cryptographie : conception, analyse et attaques»
Sorbonne Université
sous la direction de Jean-Pierre Tillich

par Philippe Gaborit, Professeur en Informatique à l'Université de Limoges

Dans ce mémoire de thèse de cryptographie, Thomas Debris-Alazard s'intéresse à la cryptographie à clé publique post-quantique et en particulier à la cryptographie basée sur les codes correcteurs d'erreurs. Il présente dans ce mémoire d'excellents résultats à la fois variés et très originaux sur des aspects touchant tant la cryptographie, la cryptanalyse que la complexité du décodage.

La cryptographie à clé publique s'est développée à partir du célèbre algorithme RSA en 1977. Au fur et à mesure des années et notamment avec le développement d'internet, la cryptographie est devenue un outil indispensable au développement de la société numérique. En effet la cryptographie est la pierre angulaire de la sécurité numérique actuelle et on la retrouve partout : des cartes à puce aux transactions bancaires en passant par le courrier électronique. La très grande majorité des algorithmes cryptographiques à clé publique utilisés en pratique actuellement, reposent sur des problèmes difficiles liés à la théorie des nombres comme le problème de la factorisation pour RSA ou encore le problème du logarithme discret sur le groupe Z/pZ ou sur le groupe des courbes elliptiques pour des chiffrements de type El Gamal. Les résultats de Peter Shor en 1994 ont montré que sous l'hypothèse de l'existence d'un ordinateur quantique suffisamment puissant il était possible d'attaquer facilement tous les problèmes basés sur la théorie de nombres utilisés dans les applications au quotidien, menaçant potentiellement, par la même, l'équilibre mondial de la sécurité des communications. Devant le développement des résultats pratiques sur les ordinateurs quantiques, en 2015 la NSA (l'agence de renseignements américaine), a encouragé le passage à des algorithmes dit post-quantiques, résistants *a priori* aux attaques par ordinateur quantique. Les problèmes alternatifs les plus mis en avant aujourd'hui sont les problèmes basés sur les réseaux euclidiens ou les codes correcteurs d'erreurs. Le sujet général de cette thèse est de s'intéresser aux systèmes basés sur les codes dont le développement est un point crucial pour la cryptographie de demain.

Le mémoire de thèse se décline en quatre parties principales.

La première partie propose un bref état de l'art sur les codes correcteurs d'erreurs et la cryptographie avec deux sous-parties sur les notions principales de cryptographie pour les codes correcteurs ainsi qu'une deuxième partie plus spécifique sur un état de l'art sur le décodage par ensemble d'information en métrique de Hamming. Cette partie du mémoire donne une très bonne vision de l'état de l'art actuel tant pour la métrique de Hamming que pour la métrique rang en prenant le temps de bien détailler les parties qui serviront de repères pour la suite du mémoire comme par exemple les signatures ou encore les algorithmes les plus récents de décodage de codes aléatoires. Globalement les résultats de cette partie sont présentés de manière très harmonieuse et montre la grande maîtrise de compréhension et le recul qu'a pu atteindre M. Thomas Debris-Alazard durant sa thèse.

La deuxième partie considère différents aspects de méthodes de décodage. Tout d'abord dans le premier chapitre de cette partie l'auteur introduit la notion de décodage en grand poids. Cette notion très originale et contre-intuitive a priori, trouve des applications importantes en cryptographie comme on le verra par la suite. L'idée consiste à trouver des pré-images de grands poids de Hamming pour un syndrome donné plutôt que de petit poids comme c'est le cas classiquement. En particulier cette notion fait particulièrement sens pour des codes sur le corps GF(3) plutôt que sur le corps GF(2) pour lequel elle ne présente pas d'intérêt. Les travaux présentés dans ce chapitre adaptent les algorithmes classiques sur GF(2) et montrent bien l'intérêt qu'il peut y avoir à considérer cette approche dans certains cas. Le deuxième chapitre de cette partie s'intéresse au décodage statistique pour lequel l'auteur propose une analyse asymptotique détaillée. Même si les résultats obtenus montrent que cette approche ne peut améliorer l'approche classique de Prange, ces résultats permettent de montrer les limites d'un tel décodage et font appel à des notions d'une grande complexité technique que l'auteur explique très clairement.

La troisième partie et les chapitres 5, 6 et 7 constituent le résultat le plus marquant de ce mémoire. Ces chapitres décrivent un nouveau schéma de signature appelé WAVE, pour les codes dans l'esprit du schéma de signature GPV, un schéma de référence pour la cryptographie basée sur les réseaux euclidiens. Ce schéma est basé sur l'indistingabilité d'une structure de type (U|U+V) généralisée sur des codes ternaires et le décodage des mots de gros poids, abordé dans les chapitres précédents. En particulier la signature reprend la notion de *rejection sampling* qui permet de filtrer les signatures afin d'obtenir une preuve sur le fait que donner des signatures n'implique pas de fuite d'information sur la clé secrète. Ces trois chapitres proposent un travail remarquable sur l'analyse et la conception de ce protocole de signature, un problème majeur en théorie de la cryptographie basée sur les

123, avenue Albert-Thomas - 87060 LIMOGES Cedex France
Tél. : (33) 05 55 45 72 50 - Fax : (33) 05 55 45 76 97
Courriel : dir@xlim.fr - Site web : http://www.xlim.fr
Site de Brive : IUT GEII - 7, rue Jules-Vallès - 19100 BRIVE - Tél. 05 55 86 73 18
Site de Poitiers : Bd Pierre-et-Marie-Curie - BP 30179 - 86962 FUTUROSCOPE Cedex - Tél. 05 49 49 65 67

codes, où ce schéma très novateur marque assurément une étape majeure. Ces résultats ont d'ailleurs obtenu le prix du meilleur article à la conférence de référence ASIACRYPT 2019.

Enfin la dernière partie s'intéresse à la cryptanalyse de schémas sur les codes en métrique rang. Les deux derniers chapitres considèrent le schéma de signature RankSign et un protocole d'IBE (chiffrement basé sur l'identité) en métrique rang. La cryptanalyse de RankSign repose sur l'utilisation des contraintes liées à la signature impliquées par le décodage pour retrouver la clé secrète directement à partir de la clé publique. L'attaque, effectuée en pratique par l'auteur, paraît difficilement réparable à moindre coût, tant les contraintes sur la structure du code considéré pour le schéma paraissent fortes. Enfin le dernier chapitre considère les contraintes théoriques pour pouvoir utiliser un schéma d'IBE en métrique rang basé sur une signature de type *hash and sign* et montre qu'il n'existe qu'une petite zone théorique pour pouvoir appliquer la construction de l'IBE en métrique rang. Ces résultats parus dans la conférence de référence ASIACRYPT 2017 sont d'un très bon niveau, puisque en particulier le schéma RankSign était soumis à la standardisation post-quantique du NIST (l'organisme de standardisation américain) et n'était pas attaqué depuis sa parution en 2014.

Pour conclure le travail présenté par Thomas Debris Alazard est un travail remarquable d'un excellent niveau scientifique qui a permis de proposer une nouvelle signature de type *hash and sign* en codes correcteurs avec des paramètres très raisonnables et des techniques de preuves très abouties, ainsi que l'introduction du nouveau problème de décodage des gros poids, problème qui sera sans aucun doute repris comme problème de référence pour de nouveaux protocoles en cryptographie basée sur les codes correcteurs. Le mémoire très dense et imposant est très bien rédigé, montrant l'étendue des connaissances que Thomas Debris-Alazard a su s'approprier durant sa thèse. Pour toutes ces raisons je donne un avis très favorable et enthousiaste pour la soutenance de cette thèse.

Limoges le 27/11/2019,

P. Gaborit.

Philippe Gaborit
Professeur en Informatique
Université de Limoges

123, avenue Albert-Thomas - 87060 LIMOGES Cedex France
Tél. : (33) 05 55 45 72 50 - Fax : (33) 05 55 45 76 97
Courriel : dir@xlim.fr - Site web : http://www.xlim.fr

Site de Brive : IUT GEII - 7, rue Jules-Vallès - 19100 BRIVE - Tél. 05 55 86 73 18
Site de Poitiers : Bd Pierre-et-Marie-Curie - BP 30179 - 86962 FUTUROSCOPE Cedex - Tél. 05 49 49 65 67

Rapport sur la Thèse de Thomas Debris-Alazard

«Codes correcteurs et cryptographie : conception, analyse et attaques»

Ce travail est consacré à differents aspects de la cryptographie fondée sur les codes, traitant à la fois des questions de cryptanalyse et des questions de constructions cryptographiques aux propriétés de sécurité mathématiquement prouvées. Deux types de codes correcteurs sont étudiés dans différents chapîtres, les codes dits «U+V» (généralisés), et les codes en «métrique rang». Étant donnée la longueur du manuscrit et mon expertise limitée, mon rapport fait l'impasse sur l'étude des codes en métrique rang, pour laquelle je ne peux que souligner leur publication à Asiacrypt 2018, l'une des trois conférences les plus séléctive en cryptographie.

Ainsi, de mon point de vue, le résultat le plus impressionnant de cette thèse demeure la construction d'un schéma de signature de type «trappe-GPV» fondée sur les codes U+V généralisés. En effet, la construction originale de Gentry, Peikert et Vaikutanathan (GPV) pour les réseaux euclidiens a eu un impact fort et durable dans le domaine de la cryptographie fondée sur les réseaux, et son adaptation aux codes semblait donc être un problème ouvert majeure. Il aura fallu plus de dix ans pour enfin voir une telle adaptation. La solution proposée dans ce manuscrit est particulièrement créative, et fait appel à des technique plus courramment utilisées en cryptanalyse qu'en construction. À mes yeux, cela démontre la capacité du candidat à faire interagir différents sous-domaines de recherche, une qualité qui laisse entrevoir la résolution future de nombreux autres problèmes centraux en cryptographie. En effet, les plus grand bonds en avant de la cryptographie partagent cette approche : s'approprier les outils de la cryptanalyse. Ce résultat a par ailleurs été récompensé par le *prix du meilleur article* à Asiacrypt 2019.

Le manuscrit commence avec un chapître introductif très détaillé sur l'état de l'art de la cryptographie fondée sur les codes, et propose un exposé presque exhaustif des idées du domaine. En particulier, la thèse mentionne les tentatives ratées de constructions de cryptosystème fondées sur les codes; en effet ce domaine de recherche s'est heurté par le passé a de nombreux échecs qu'il est important de bien connaître afin de les prévenir. Cette introduction, en plus de démontrer une connaissance encyclopédique du domaine, est donc particulièrement pertinente avant de s'attaquer à un problème ouvert telle que la réalisation de trappes-GPV fondé sur les codes.

Le chapître 3, lui aussi très précis et exhaustif, se concentre spécifiquement sur les téchniques de cryptanalyses connues de décodage par ensemble d'information. Cet exposé est loin d'être gratuit : premièrement ces considérations seront curciales pour determiner la sécurité des schémas nouvellement proposés dans la suite de cette thèse. Deuxièmement, ce sont précisement ces techniques qui seront au centre de l'invention de trappe-GPV pour les codes. Ce chapître adapte aussi ces résultats connus à une nouvelle variation du problème de décodage, le décodage en grande distance. Bien que peu naturel d'un point de vue de la correction d'erreur, cette variation sera l'une des clefs de voûte pour la construction de trappes-GPV fondées sur les codes.

Le chapître 4 traite lui aussi de décodage, mais cette fois ci par une autre approche dîte statistique. Cette approche, bien que naturelle n'à été l'objet que de très peu de travaux, qui

sont revisités dans ce chapître. En particulier, une analyse plus fine de l'éfficacité de cette approche est proposée en exploitant les polynômes de Krawtchouk, ce qui permet de conclure que les résultats précedents faisaient des hypothèses trop optimistes. Cette clarification importante a été publiée ISIT 2017.

Enfin, les chapîtres 5, 6 et 7 traitent respectivement la construction de trappes-GPV pour les codes U+V, leur utilisation prouvablement-sûr pour la construction de schéma de signatures, et enfin leur résistance à la cryptanalyse. Un premier point important mis en avant est la nécéssité d'aller au delà des codes binaires, pour lesquels la structure U+V est facilement détéctable. L'utilisation proposée de codes ternaires permet au contraire de généraliser les codes U+V, de tel sorte qu'ils gardent des propriétés utiles pour qui connait leur structures, mais semblent empécher la détection de cette structure cachée. De plus, il est noté qu'une plus grande marge de maneuvre est offerte du côté du décodage en grande distance : bien que peu naturel ce choix s'avère bénéfique.

Le manuscrit explique ensuite comment la structure U+V géneralisée peut être exploitée pour efféctuer un décodage éfficace au delà de de linterval offert par le décodage générique. En bref, il s'agit de décoder dans U génériquement, puis de décoder dans V génériquement de façon biaisée et dépendante du décodage dans U. Celà donne déjà une trappe, mais cette trappe laisse fuiter de l'information sur la structure U+V secrète. Il s'en suit donc une modification de cet algorithme naïf, afin de palier a ce biais. La solution proposée est inspirée de la cryptographie à base de réseaux (mais étrangère à l'article GPV lui même), et consiste à effectuer des rejets probabilistes finement calibrés afin de réctifier la distribution de sortie de l'algorithme, et de la rendre indépendente de toute informations secrètes. Ce dernier passage est particulièrement technique et je n'ai malheuresement pas eu le temps d'en apprécier tout les détails.

Appréciation et Conclusion. Je ne peux qu'être impressionné par le nombre d'obstacles surmontés pour en arriver à ce dernier résultat. Le candidat a non seulement su adopter des techniques venant d'autres sous-domaines (GPV, rejet), mais a aussi et surtout exploré de nouveaux territoires en cryptographie fondée sur les codes (codes U+V, codes ternaires, décodage en grand poids). Cette combinaison d'une grande technicité mène à un résultat faisant date dans le domaine de la cryptographie fondée sur les codes, et ouvre de nouvelles voies vers des schémas de plus en plus sophistiqués.

Ainsi, Thomas Debris-Alazard à fait preuve d'une grande maîtrise technique du sujet, mais aussi d'une compréhension plus large des domaines connexes, et enfin d'un grande créativité scientifique. Je recommande sans réserve sa soutenance.

Amsterdam, le 24 Novembre 2019
Dr. Léo Ducas

Chercheur au Centrum Wiskunde & Informatica