Cryptographie sur les codes correcteurs d'erreurs en métrique rang et applications

gaborit philippe, gaborit@unilim.fr
Tél : 0587506781
zemor gilles,
Tél : 0

Equipe : CRYPTIS, limoges

Mots clés : cryptographie, codes correcteurs d'erreurs

Résumé de la thèse :

Récemment des nouveaux systèmes de chiffrements ont été développés autour de la métrique rang et de la métrique de Hamming (les systèmes LRPC [1] et HQC[2]) , ces systèmes sont très efficaces et surtout bénéficient de très bonnes propriétés sémantiques. Le but de cette thèse est double, avec à la fois un coté très concret sur l'implémentation de cryptosystèmes efficaces basés sur les codes correcteurs d'erreurs pour le concours internatipnal du NIST pour la cryptographie post-quantique http://csrc.nist.gov/groups/ST/post-quantum-crypto/), et un coté plus théorique sur la sécurité et les applications de ces systèmes. Ces deux objectifs sont décrits ci-après.

Concours international du NIST :accompagnement de soumissions en codes correcteurs proposées par les directeurs de thèse, dans le cadre de l'appel à projet du NIST en cryptographie post-quantique . Comme on l'a vu les directeurs de cette thèse ont proposé des systèmes novateurs en théorie des codes en métrique de Hamming et en métrique rang. Le candidat à cette thèse aura normalement déjà fait son stage de M2 sur les implementations des systèmes basés sur les codes correcteurs pour l'appel au NIST, et devra continuer d'accompagner l'appel à projet au NIST pendant la compétition. Une partie du travail consistera à continuer à optimiser les implementations dévéloppées et à les mettre à jour, ainsi que regarder les attaques sur les autres soumissions au NIST.

Problème difficiles en théorie des codes pour la cryptographie. La deuxième partie , plus théorique, de cette thèse qui s'effectuera en parallèle de la première consistera à s'interesser plus à fond à la difficulté de problème en théorie des codes pour la cryptographie, et notamment de la difficulté intrinsèque des problèmes de syndrome décoding structurés comme les problèmes de décodage par syndrome basés sur les codes quasi-cycliques. A priori le problème est considéré comme difficile, mais il n'existe pas de preuve sous-jacente. Le sujet de thèse s'intéressera ausi à regarder la des problèmes basés sur la métrique rang et de regarder d'autres types de cryptosystèmes basés sur la métrique rang par exemple pour la signature et aussi d'autres applications pour des systèmes cryptographiques parfaitement surs basés sur la métrique rang comme dans [10].

The purpose of this thesis is the study of new cryptosystems based on code-based cryptography and in particular rank metric, a promising type of cryptography.

Objectifs :

Développer des nouveaux systèmes de cryptograohie basés sur la métrique rang.

Description complète du sujet de thèse :

Titre : Cryptographie sur les codes correcteurs d'erreurs en métrique rang et applications

directeurs : P. Gaborit (PR, univ. Limoges) et G. Zémor (PR, Univ. Bordeaux))

co-financement demandé : ½ bourse, une ½ bourse a deja été donné par le LABEX de Limoges.
étudiant pressenti : Nicolas Aragon (1er du master Cryptis-Info en M1, mention TB)

Contexte :

Limites de la cryptographie classique actuelle. 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.

Bien que ces algorithmes répondent en pratique aux besoins cryptographiques actuels, ils ont leur limite :
− une première limite vient de la difficulté intrinsèque des problèmes liés à la théorie des nombres, en effet ces problèmes ne font pas partie des problèmes les plus durs connus. En particulier des résultats de P. Shor en 1994 ont montré qu'à la condition qu'il existe un ordinateur quantique suffisamment puissant, il était possible de résoudre le problème de la factorisation en temps polynomial (résultats qui se généralisent au problème du logarithme discret). Il n'existe pas aujourd'hui un tel ordinateur quantique - et pas de perspective à court terme d'en construire un - néanmoins son existence reste toujours une possibilité et conduirait à la chute totale de tous les systèmes utilisés actuellement en pratique en clé publique.
− une deuxième limite vient du fait que les algorithmes basés sur la théorie des nombres sont relativement couteux d'un point de vue calcul, et sont donc difficilement utilisables sur des support à ressources réduites comme par exemple les tags RFID ou les capteurs.
− enfin une dernière limite de principe vient du fait qu'il est toujours risqué de mettre tous ses oeufs dans le même panier, car on ne sait jamais ce qui peut arriver. Sans parler nécessairement d'un ordinateur quantique éventuel, par exemple très récemment des nouveaux résultats ont amélioré de manière très significative les attaques pour certains cas du problème du logarithme discret (le cas des extensions sur une petite caractéristique), même s'il ne s'agit pas de cas de logarithme discret utilisés en pratique, ces résultats en sont relativement proches.

Il existe plusieurs alternatives possibles: la cryptographie basée sur les réseaux euclidiens, la cryptographie multivariée ou encore la cryptographie basée sur les codes, regroupées sous la dénomination de cryptographie post-quantique, en ce sens que les problèmes difficiles sous-jacents sont NP-dur et a priori résistant à l'ordinateur quantique. Parmi ces alternatives, la cryptographie basée sur les codes présente beaucoup d'avantages. Le but de cette thèse est de proposer et d'implémenter en vue du concours international du NIST sur la cryptographie post-quantique des systèmes efficaces de cryptographie basés sur les codes correcteurs et de considérer leur sécurité et leurs applications.

Descriptif du sujet:

Cryptographie basée sur les codes. La cryptographie basée sur les codes a été introduite par McEliece en 1978 peu de temps après l'algorithme RSA. Au cours du temps de nombreuses variantes ont été proposées avec des familles de codes différentes. Cependant, bien que le système proposé à l'origine avec les codes de Goppa soit toujours considéré comme sûr et rapide, ces systèmes ont le gros désavantage d'avoir une taille de clé très importante: plusieurs centaines de milliers de bits.
Au milieu des années 2000, des premiers travaux ont vu le jour pour faire baisser la taille des clés via des matrices structurées [3] qui permettent potentiellement de faire baisser la taille des clés à quelques milliers de bits. Bien que potentiellement toujours intéressants les instances proposés dans [3] ont fait l'objet d'attaques structurelles [4]. Suite à ces premiers résultats utilisant des matrices compactes les codes MDPC ont été introduits dans [5] et permettent d'obtenir des systèmes (à la NTRU) moins structurés que les systèmes basés sur les codes alternants de [3].

Cryptographie en métrique rang. En parallele des systèmes basés sur les codes en distance de Hamming, Gabidulin a présenté dans [6], des systèmes basés sur la métrique rang. Les problèmes définis pour la métrique de Hamming peuvent aussi être définis de manière analogue en métrique rang. L'intérêt de la métrique rang est qu'à sécurité donnée, les tailles des paramètres sont beaucoup plus petits sans ajout de structure comme la cyclicité. Les systèmes proposés par Gabidulin dans [6] avaient des tailles de clés de seulement quelques milliers de bits. Malheureusement, tous ces systèmes et leur variations ont fait l'objet d'attaques structurelles dans les années 2000 liées à la structure du code sous-jacent, le code de Gabidulin, très dur à masquer (voir l'HDR de P. Loidreau pour tous les détails [7]).

Très récemment des nouveaus systèmes basés sur des instances aléatoires quasi-cycliques (et donc difficilement attaquables sur leur structure) ont été proposés par les directeurs de cette thèse dans [1] et [2]. Ces systèmes permettent pleinement de profiter des avantages de la métrique rang sans avoir à souffrir des problemes des systèmes précédents liés à la structure des Gabidulin. En parallèle, des travaux de fond sur la difficulté pratique et intrinsèque de la métrique rang ont été publiés par les directeurs de cette thèse dans [8] et [9] dans la revue de référence IEEE trans. on Information Theory. Concrétement et toute proportions gardées les codes en métrique rang sont à la métrique de Hamming, un peu l'équivalent de ce qu'est le logarithme discret sur les courbes elliptiques par rapport au logarithme discret sur Z/nZ. Ainsi bien qu'il y a probablement encore des études à faire sur ce sujet (dont l'étude remonte déjà à plus de 25 ans), la métrique rang présente un très grand potentiel pour la cryptographie que les travaux récents ne font que révéler un peu plus.

Concours du NIST. Enfin en 2015 la NSA a annoncé qu'elle encourageait l'administration américaine à passer aux systèmes post-quantique et en novembre 2016 un appel à proposition a démarré (sur les modèles des ceux de l'AES et de SHA3 – mais avec probablement plusieurs candidats retenus). L'appel à contribution du NIST a retenu 3 types de cryptosystèmes : le chiffrement, l'échange de clés et la signature.

Objectifs de la thèse et programme: Récemment des nouveaux systèmes de chiffrements ont été développés autour de la métrique rang et de la métrique de Hamming (les systèmes LRPC [1] et HQC[2]) , ces systèmes sont très efficaces et surtout bénéficient de très bonnes propriétés sémantiques. Le but de cette thèse est double, avec à la fois un coté très concret sur l'implémentation de cryptosystèmes efficaces basés sur les codes correcteurs d'erreurs pour le concours internatipnal du NIST pour la cryptographie post-quantique http://csrc.nist.gov/groups/ST/post-quantum-crypto/), et un coté plus théorique sur la sécurité et les applications de ces systèmes. Ces deux objectifs sont décrits ci-après.

Concours international du NIST :accompagnement de soumissions en codes correcteurs proposées par les directeurs de thèse, dans le cadre de l'appel à projet du NIST en cryptographie post-quantique . Comme on l'a vu les directeurs de cette thèse ont proposé des systèmes novateurs en théorie des codes en métrique de Hamming et en métrique rang. Le candidat à cette thèse aura normalement déjà fait son stage de M2 sur les implementations des systèmes basés sur les codes correcteurs pour l'appel au NIST, et devra continuer d'accompagner l'appel à projet au NIST pendant la compétition. Une partie du travail consistera à continuer à optimiser les implementations dévéloppées et à les mettre à jour, ainsi que regarder les attaques sur les autres soumissions au NIST.

Problème difficiles en théorie des codes pour la cryptographie. La deuxième partie , plus théorique, de cette thèse qui s'effectuera en parallèle de la première consistera à s'interesser plus à fond à la difficulté de problème en théorie des codes pour la cryptographie, et notamment de la difficulté intrinsèque des problèmes de syndrome décoding structurés comme les problèmes de décodage par syndrome basés sur les codes quasi-cycliques. A priori le problème est considéré comme difficile, mais il n'existe pas de preuve sous-jacente. Le sujet de thèse s'intéressera ausi à regarder la des problèmes basés sur la métrique rang et de regarder d'autres types de cryptosystèmes basés sur la métrique rang par exemple pour la signature et aussi d'autres applications pour des systèmes cryptographiques parfaitement surs basés sur la métrique rang comme dans [10].

Synthèse : Le sujet de cette thèse est un projet ambitieux pour des systèmes cryptographiques parmi les plus concurrenciels de ce qui se fait aujourd'hui en cryptographie post-quantique et qui ont probablement de bonne chance de très bien figurer dans le cadre de l'appel international du NIST, avec à la fois un coté très pratique sur la cryptographie sur les codes correcteurs d'erreurs et aussi un volet théorique ambitieux, proposé par des directeurs de thèse

très reconnus mondialement dans le domaine de la cryptographie basée sur les codes correcteurs.

Bibliographie

[1] P.Gaborit , O. Ruattan J. Schrek and G. Zémor: New Results for Rank-Based Cryptography. AFRICACRYPT 2014: 1-12
[2] Carlos Aguilar, O. Blazy, JC. Deneuville, P. Gaborit and G. Zémor : Efficient Encryption from Random Quasi-Cyclic Codes. (2016)
[3] T. Berger, PL Cayrel , P. Gaborit and A. Otmani:
Reducing Key Length of the McEliece Cryptosystem. AFRICACRYPT 2009: 77-97
[4] JC Faugère, A. Otmani, L. Perret, JP Tillich , Ayoub Otmani:
Algebraic Cryptanalysis of McEliece Variants with Compact Keys. EUROCRYPT 2010: 279-298
[5] R. Misoczki, JP Tillich , N. Sendrier P. Barreto,
MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes. ISIT 2013: 2069-2073
[6] Ernst M. Gabidulin, A. Paramonov and O. Tretjakov , :
Ideals over a Non-Commutative Ring and thier Applications in Cryptology. EUROCRYPT 1991: 482-489
[7] https://perso.univ-rennes1.fr/pierre.loidreau/Habilitation/HDR.ps
[8] Philippe Gaborit, O. Ruatta, J. Schrek
On the Complexity of the Rank Syndrome Decoding Problem. IEEE Trans. Information Theory 62(2): 1006-1019 (2016)
[9] Philippe Gaborit, Gilles Zémor:
On the Hardness of the Decoding and the Minimum Distance Problems for Rank Codes. IEEE Trans. Information Theory 62(12): 7245-7252 (2016)
[10] G.Spini,G.Zémor:
Perfectly Secure Message Transmission in Two Rounds. TCC (B1) 2016: 286-304

Réferences bibliographiques des encadrants P. Gaborit et G. Zémor liés au sujet de la cryptographie post-quantique et des codes correcteurs : publications dans les meilleures revues et conférences du domaine :

1 - Philippe Gaborit, Olivier Ruatta, Julien Schrek:
On the Complexity of the Rank Syndrome Decoding Problem. IEEE Trans. Information Theory 62(2): 1006-1019 (2016)

2 - Philippe Gaborit, Gilles Zémor:
On the Hardness of the Decoding and the Minimum Distance Problems for Rank Codes. IEEE Trans. Information Theory 62(12): 7245-7252 (2016)

3- G.Spini,G.Zémor:
Perfectly Secure Message Transmission in Two Rounds. TCC (B1) 2016: 286-304

4 - Anthony Leverrier, Jean-Pierre Tillich, Gilles Zémor:
Quantum Expander Codes. FOCS 2015: 810-824

5 - Philippe Gaborit, Olivier Ruatta, Julien Schrek, Gilles Zémor:
New Results for Rank-Based Cryptography. AFRICACRYPT 2014: 1-12

6 - Carlos Aguilar Melchor, Philippe Gaborit, Javier Herranz:
Additively Homomorphic Encryption with d-Operand Multiplications. CRYPTO 2010: 138-154

7 - Thierry P. Berger, Pierre-Louis Cayrel, Philippe Gaborit, Ayoub Otmani:
Reducing Key Length of the McEliece Cryptosystem. AFRICACRYPT 2009: 77-97

Compétences à l'issue de la thèse :

compétences en cryptographie et en programmation

Présentation de l'équipe d'accueil :

Cryptis est une équipe qui travaille dans les domaines de la sécurité de l'information et la cryptographie, très reconnue internationalement.

Financement : Lot1: Sujet financé sur crédits institutionnels (sujets fléchés)

Spécialité de Doctorat : Sciences et Technologies de l'Information et de la Communication

Domaine de compétences principal: Informatique-Electronique

Domaine de compétences secondaire: Mathématiques

Candidat :
Compétences souhaitées : profil math-info / ingénieur

Conditions restrictives de candidature : Aucune

Date Limite de candidature : 8 juin 2017 - 18H