# Sujet de Thèse

- **Titre :** Étude et conception de nouvelles primitives de chiffrement fondées sur les codes correcteurs d'erreur en métrique rang.
- **Unité de recherche :** IRMAR, UMR-6625
- **Thème :** Codes correcteurs d'erreurs et cryptographie.
- **Mots clefs :** Polynômes de Ore, Codes de Gabidulin, métrique rang, cryptosystème de McEliece.
- **Les noms, prénoms et courriel du directeur de thèse**

  *Directeur* Pierre Loidreau

  *Courriel :* Pierre.Loidreau@univ-rennes1.fr

## Objectif de la thèse

L'usage de codes correcteurs d'erreurs en cryptographie remonte à l'origine de la cryptographie à clé publique en 1978, [5]. Au départ ce fut McEliece qui proposa un système de chiffrement à clé publique utilisant comme clé privée un code que l'on sait décoder (un code de Goppa binaire). La sécurité de ce système repose sur la difficulté de trouver le plus petit mot de code en terme de métrique de Hamming ou bien de trouver le mot de code le plus proche d'un vecteur donné. Sur ce principe, reposent la plupart des primitives de chiffrement dites post-quantiques utilisant des réseaux euclidiens (la métrique considérée est alors la métrique euclidienne) ou bien des codes correcteur d'erreur. À l'heure actuelle ce type de cryptographie connaît un regain d'intérêt fort depuis l'appel du NIST (*National Institute of Standard and Technologies*) à standardiser de telles primitives de chiffrement pour se préparer à l'avènement plus ou moins proche de l'ordinateur quantique.

Dans les années 90's, Gabidulin, Paramonov et Tretjakov proposèrent un système de chiffrement de type McEliece reposant sur la difficulté de décoder un code linéaire en métrique rang, [3]. Comme la complexité du décodage en métrique rang est exponentiellement plus coûteuse à paramètres fixés que le décodage en métrique de Hamming, l'utilisation de cette métrique permet d'imaginer concevoir des systèmes de chiffrement avec des clés plus compactes. La famille de codes sous-jacente utilisée est la famille de codes de Gabidulin, [2]. Ce sont des codes d'évaluation de l'anneau des polynômes de Ore sur des corps finis, et ils ont la propriété d'être optimaux pour la métrique rang (*Maximum Rank Distance*). Á l'image des codes GRS, optimaux pour la métrique de Hamming, il est indispensable de casser leur structure afin de préserver la sécurité des primitives conçues. Jusqu'à présent, toutes les variantes proposées ont été cassées par l'attaque des *sous-espaces invariants*, encore appelées attaques de *Overbeck*, [6].

L'objectif de cette thèse est d'étudier et de concevoir de nouvelles primitives de chiffrement utilisant des codes en métrique rang Pour ce faire on étudiera la structure d'une nouvelle famille de codes, dérivée des codes de Gabidulin. Celle-ci est construite en utilisant l'idée qui a prévalu à la conception des systèmes utilisant des LRPC (*low-rank parity-check codes*), [4]. On casse la structure du code en lui appliquant l'action d'un sous-espace vectoriel du corps fini qui constitue l'alphabet du code. Ce sous-espace n'étant pas invariant par l'action de l'automorphisme de Frobenius, l'attaque par *sous-espaces invariants*, n'est pas applicable. L'intérêt de cette technique est que l'on construit des codes qui ne sont plus des objets combinatoires optimaux, on les rend indistinguable d'un code aléatoire. Un autre intérêt est que cela permet de s'affranchir de techniques compliquées et donc suspectes de masquage de la clé publique. On s'appuiera sur l'abondante littérature scientifique concernant la conception de primitives de chiffrement basées sur les codes, ainsi que sur les articles traitant de codes de Gabidulin et de la métrique rang, [1].

# References


[1] Lionel Chaussade, Pierre Loidreau, and Felix Ulmer. Skew codes of prescribed distance or rank. *Des. Codes Cryptography*, 50(3):267–284, 2009.

[2] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.

[3] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their applications to cryptography. In *Advances in Cryptology - EUROCRYPT'91*, number 547 in Lecture Notes in Comput. Sci., pages 482–489, Brighton, April 1991.

[4] P. Gaborit, G. Murat, O. Ruatta, and G. Zémor. Low rank parity check codes and their application to cryptography. In *Proceedings of the Workshop on Coding and Cryptography WCC'2013*, Bergen, Norway, 2013. Available on `www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf`.

[5] R. J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, pages 114–116. Jet Propulsion Lab, 1978. DSN Progress Report 44.

[6] R. Overbeck. A new structural attack for GPT and variants. In *Mycrypt*, volume 3715 of *Lecture Notes in Comput. Sci.*, pages 50–63, 2005.