Titre : Codes Correcteurs et Crypto
Objectif : Implémentation d'une cryptanalyse
Encadrant : Guénaël Renault (guenael.renault@gmail.com)

L'objectif de ce projet est l'implémentation d'une attaque récente sur un cryptosystème basé sur les codes correcteurs.
L'étude de ces cryptosystèmes est très importante ce sont des représentants possibles des futurs standards du NIST.

Une partie importante du travail à réaliser sera la lecture et la compréhension de l'article de recherche (https://eprint.iacr.org/2016/858.pdf) avant de réaliser l'implémentation de l'attaque.