Algorithmes ISD et jeu d'instructions AVX512

Pascal Véron

23 octobre 2023

1 Sujet

Les avancées récentes dans le domaine du développement des ordinateurs quantiques ont considérablement bouleversé la sécurité de la cryptographie. Par conséquent, le National Institute of Standards and Technology (NIST) a lancé en décembre 2016 un projet visant à normaliser les primitives cryptographiques destinées à contrer les menaces quantiques, que l'on désigne sous le nom de "cryptographie post-quantique". Parmi les domaines les plus prometteurs de cette cryptographie post-quantique, les codes correcteurs d'erreurs occupent une place centrale. Tous les protocoles post-quantiques se fondent sur un problème fondamental hérité de la théorie des codes, à savoir le problème de décodage de syndrome (SD). Ce dernier s'énonce très simplement.

> Soit H une matrice $k \times n$ définie sur $\mathbb{F}_2$, soit s un vecteur colonne de $\mathbb{F}_2^k$ et soit p un entier. Existe-t-il un vecteur colonne $e \in \mathbb{F}_{2^n}$ ne comportant que p composantes non nulles tel que $He = s$?

Malgré de nombreux efforts sur cette question, les meilleurs algorithmes demeurent exponentiels et sont essentiellement des améliorations de l'algorithme original conçu par Prange en 1962 [Pra62]. Ces algorithmes sont couramment désignés sous le terme "Information Set Decoding" (ISD). L'un des principaux défis dans l'élaboration de protocoles post-quantiques basés sur les codes correcteurs d'erreurs consiste à choisir des ensembles de paramètres sécurisés qui répondent aux normes de sécurité établies par le NIST. Par conséquent, il est impératif de mesurer de manière pratique l'efficacité des différents algorithmes de résolution du problème SD.
Le jeu d'instructions AVX512 proposent des instructions vectorielles permettant d'effectuer une même opération sur plusieurs données à la fois stockées dans un registre 512 bits (par exemple 8 mots de 64 bits). Bien que désactivé par INTEL sur ses dernières générations de processeur, la technologie a été reprise et améliorée par AMD dans la série des processeurs Ryzen 7000.
L'objectif principal de ce stage consistera, dans un premier temps, à analyser et à acquérir une compréhension approfondie des différents algorithmes appartenant à la famille ISD. Dans un second temps, il s'agira de réaliser une implémentation en utilisant le jeu d'instructions AVX512 de l'algorithme jugé le plus adapté. Cette démarche nous permettra d'obtenir des mesures concrètes des progrès réalisés dans le domaine de la résolution du problème SD.

2 Bibliographie

[Pra62] Eugene Prange. *The use of information sets in decoding cyclic codes.* IEEE Transactions on Information Theory, 8(5) :5–9, 1962.
[BBCPG19] Baldi, M., Barenghi, A., Chiaraluce, F., Pelosi, G., Santini, P., *A finite regime analysis of information set decoding algorithms.* Algorithms 12(10), 209 (2019).