Une réduction pire cas-cas moyen pseudoaléatoire pour le problème de décodage

Etienne Burle, doctorant d'Ayoub Otmani

La théorie des codes correcteurs d'erreurs sert à corriger les erreurs apparaissant lors des transmissions de signaux numériques dans un canal. Cette théorie trouve également des applications en cryptographie. En effet, en 1978 est créé le premier schéma de chiffrement basé sur les codes correcteurs d'erreurs [McE78]. Celui-ci s'appuie notamment sur l'hypothèse que le problème de décodage d'un code aléatoire est difficile, problème qui deviendra la base de toute la cryptographie basée sur les codes. Aucun algorithme quantique connu ne permettant de résoudre plus rapidement ce problème que les algorithmes fonctionnant sur les ordinateurs classiques, cette cryptographie apparaît comme d'autant plus prometteuse qu'elle est post-quantique.

Par ailleurs, le problème de décodage est un problème bien connu et étudié depuis des décennies, ce qui laisse supposer que les algorithmes existant pour le résoudre donnent une bonne idée de sa complexité intrinsèque et que le problème est réellement difficile. Cependant, donner des preuves théoriques de la difficulté du problème de décodage permettra de crédibiliser encore d'avantage la cryptographie basée sur les codes correcteurs d'erreur. Il a rapidement été prouvé [BMvT78] que le problème de décodage est NP-complet, ce qui a pour conséquence qu'il existe des instances difficiles du problème de décodage. Mais en cryptographie, les instances de décodage sont générées aléatoirement, et le fait qu'il existe des instances difficile ne signifie pas qu'en moyenne le problème de décodage est difficile. Pour résumer, s'il a déjà été montré que le pire cas du problème de décodage est difficile, il reste à démontrer théoriquement qu'il est difficile dans le cas moyen, qui est celui utilisé en pratique en cryptographie.

L'outil pour arriver à un tel résultat est la réduction du pire cas vers le cas moyen, qui permet de montrer que si un algorithme parvient à résoudre le problème du décodage pour une instance aléatoire, alors il arrive à le résoudre pour une instance arbitrairement choisie. De tels réductions ont longtemps été absentes pour le problème de décodage, jusqu'en 2019 [BLVW19]. C'en est suivi quelques autres travaux sur le même thème [YZ21, DR22, BCD22] améliorant et développant le premier résultat de 2019. Tous utilisent la méthode du "smoothing" inspirées des réductions pour les réseaux euclidiens. Cependant, ces premières réductions pour les codes imposent des paramètres non utilisables en cryptographie.

Nous avons construit une nouvelle réduction pire cas-cas moyen pour le problème de décodage qui, en utilisant de nouvelles méthodes, parvient à obtenir des paramètres utilisables en pratique. Une des grandes différences avec les réductions précédentes est que lors de la réduction, l'instance du pire cas n'est pas transformée vers une instance proche de l'uniforme par la *distance statistique*, mais par la *distance calculatoire*. Notre réduction contient donc une hypothèse (qui est sur la difficulté calculatoire de la version décision du décodage), elle est donc pseudoaléatoire. Ce type de réduction a été présenté et théorisé pour la première fois récemment par Hirahara et Santhanam [HS17]. Il est à noter que dans notre cas, même si l'hypothèse calculatoire s'avérait fausse, notre réduction exhibe malgré tout une distribution intéressante d'instances difficiles du décodage, qui ne serait juste plus considérée comme uniforme.

References

[BCD22] Maxime Bombar, Alain Couvreur, and Thomas Debris-Alazard. On Codes and Learning With Errors over Function Fields. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO*, Santa Barbara, CA, USA, August 2022. Springer.

[BLVW19] Zvika Brakerski, Vadim Lyubashevsky, Vinod Vaikuntanathan, and Daniel Wichs. Worst-case hardness for LPN and cryptographic hashing via code smoothing. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *LNCS*, pages 619–635. Springer, 2019.

[BMvT78] Elwyn Berlekamp, Robert McEliece, and Henk van Tilborg. On the inherent intractability of certain coding problems. *IEEE Trans. Inform. Theory*, 24(3):384–386, May 1978.

[DR22] Thomas Debris-Alazard and Nicolas Resch. Worst and average case hardness of decoding via smoothing bounds. preprint, December 2022. eprint.

[HS17] Shuichi Hirahara and Rahul Santhanam. On the Average-Case Complexity of MCSP and Its Variants. In Ryan O'Donnell, editor, *32nd Computational Complexity Conference (CCC 2017)*, volume 79 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 7:1–7:20, Dagstuhl, Germany, 2017. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[McE78] Robert J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, pages 114–116. Jet Propulsion Lab, 1978. DSN Progress Report 44.

[YZ21] Yu Yu and Jiang Zhang. Smoothing out binary linear codes and worst-case sub-exponential hardness for LPN. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part III*, volume 12827 of *LNCS*, pages 473–501. Springer, 2021.