SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Multi-Parallel MMT アルゴリズムによる高次元 SDP の解読
Multi-Parallel MMT Algorithm for Solving High-Dimensional SDP

成定　真太郎 *　　福島 和英 *　　清本 晋作 *
Shintaro Narisada　　Kazuhide Fukishima　　Shinsaku Kiyomoto

キーワード　シンドローム復号問題 (SDP)，符号暗号，Information Set Decoding (ISD), Graphics Processing Unit (GPU)

あらまし

シンドローム復号問題 (SDP: Syndrome Decoding Problem) は，符号暗号の安全性の根拠となっている問題である．シンドローム復号問題を効率的に求解するアルゴリズムとして，Information Set Decoding (ISD) が知られている．ISD は，組み合わせ理論に基づいて SDP の解となる符号を確率的に求める手法の総称であり，これまでに Dumer [1]，May–Meurer–Thomae (MMT) [2]，Both–May [3] といった多くの ISD が提案されてきた．これらの論文においては，各アルゴリズムの漸近計算量の解析が行われており，例えば Full Distance Decoding と呼ばれる問題設定においては，SDP の問題次元 n に対して，Both–May の計算量が $2^{0.0885n}$ となり，提案された ISD の中で最も高速となる．一方で，実際の符号暗号に関連付けられる実用的な問題サイズの SDP に対して，ISD の計算量を解析する Estimator に関する研究も行われている [4].

符号暗号の安全なパラメータセットを見積もるためには，攻撃者が SDP をどの程度の難しさまで解読できるかに関して，理論面のみならず実装面においても検証することが大切である．ISD の高速実装に関しては，Dumer のアルゴリズムの FPGA 実装 [5] および GPU 実装 [6] に関する既存研究があるが，計算量の面に関して，他の ISD との比較検討が不十分であった．本稿では，いくつかの実際の SDP インスタンスに対して，メモリを制限した場合における各 ISD の最適な計算量を解析する．結果として，漸近計算量の結果に反して，最近傍 (NN: Nearest Neighbor) 法を使用しない手法では MMT が，NN を使用する手法では May–Ozerov [7] が最も計算量が小さくなる場合があることがわかった．さらに，MMT に対して，多並列最適化の検討を行い，MMT に対する GPU アルゴリズムである Multi-Parallel MMT を提案する．Multi-Parallel MMT は，著者らの知る限りでは MMT に対する最初の GPU アルゴリズムである．また，GPU 上で Multi-Parallel MMT による SDP の解読実験を行い，SDP の解読状況のベンチマークである符号暗号の暗号解読コンテスト [8] における SDP Challenge において，新記録となる 510 次元および 530 次元の解読に初めて成功したことを報告する．

参考文献

[1] Ilya Dumer. On minimum distance decoding of linear codes. In *Proc. 5th Joint Soviet-Swedish Int. Workshop Inform. Theory*, pp. 50–52, 1991.

[2] Alexander May, Alexander Meurer, and Enrico Thomae. Decoding random linear codes in $\tilde{\mathcal{O}}(2^{0.054n})$. In *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 107–124, 2011.

[3] Leif Both and Alexander May. Decoding linear codes with high error rate and its impact for lpn security. In *International Conference on Post-Quantum Cryptography*, pp. 25–46, 2018.

[4] Andre Esser and Emanuele Bellini. Syndrome decoding estimator. Cryptology ePrint Archive, Report 2021/1243, 2021.

[5] Stefan Heyse, Ralf Zimmermann, and Christof Paar. Attacking code-based cryptosystems with information set decoding using special-purpose hardware. In *PQCrypto 2014*, pp. 126–141, 2014.

[6] Shintaro Narisada, Kazuhide Fukushima, and Shinsaku Kiyomoto. Fast GPU implementation of dumer's algorithm solving the syndrome decoding problem. In *IEEE ISPA 2021*, pp. 971–977, 2021.

[7] Alexander May and Ilya Ozerov. On computing nearest neighbors with applications to decoding of binary linear codes. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 203–228, 2015.

[8] Nicolas Aragon, Julien Lavauzelle, and Matthieu Lequesne. decodingchallenge.org, 2019. http://decodingchallenge.org.

* KDDI 総合研究所, KDDI Research, Inc.