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

Tuple Sieve Algorithmの並列化の提案
Study on Parallelizing the Tuple Sieve Algorithm

Keiichi Imai * Yuntao Wang * Eiichiro Fujisaki *

キーワード 格子暗号 並列化 TupleSieve

あらまし

現在大型の量子計算機が盛んに開発されており、より大規模な量子計算機が登場することによって現在広く利用されている素因数分解に安全性の根拠を持つ RSA や楕円曲線上の代数的性質を利用した楕円曲線暗号などが危殆化することが知られている。そこで次世代の暗号として格子上の最短ベクトルを見つける問題、最短ベクトル問題の困難さを利用した格子暗号が提案されている。しかし、実用化のためにパラメータの調整を行う必要がありその際大規模な計算器による攻撃や攻撃アルゴリズムの研究による知見が必要となる。そこで本研究では最短ベクトル問題の解法アルゴリズムの一つである TupleSieve[BLS16] を並列化したアルゴリズムの提案及び実装を行う。TupleSieve とは格子ベクトルを 3 つ以上を用いた簡約を何度も繰り返すことによって入力ベクトルより短いベクトルを次々に得るアルゴリズムである。TupleSieve とその基となったアルゴリズム GaussSieve[MV10] との主な違いとして TupleSieve の簡約の際 2 つだけベクトルを利用するという違いがある。TupleSieve の計算量は $2^{0.5662n+o(n)}$ と GaussSieve が $2^{0.52n+o(n)}$ であり、時間がかかる。しかし、同じベクトルの個数でより多くの線形結合による短いベクトルを得る試行を行うことが出来、空間複雑度は TupleSieve が $2^{0.1887n+o(n)}$ で GaussSieve が $2^{0.2n+o(n)}$ である。そのため、十分短いベクトルが得られるまでに必要なベクトルの量を減らせ、GaussSieve に比べて少ないメモリ空間で Sieve を実行出来る。

現在 GaussSieve に関しては並列化を施したアルゴリズム ParallelGaussSieve[IKMT14] が提案されている。しかし、TupleSieve においては未だ並列化の実装の提案はされておらず、研究の余地がある。そこで本研究では TupleSieve を利用した並列アルゴリズムを提案する。また、アルゴリズムの実装及び低次元における実験を通して TupleSieve の並列化アルゴリズムの有用性を示す。

参考文献

[BLS16] Shi Bai, Thijs Laarhoven, and Damien Stehlé. Tuple lattice sieving. *IACR Cryptol. ePrint Arch.*, page 713, 2016.

[IKMT14] Tsukasa Ishiguro, Shinsaku Kiyomoto, Yutaka Miyake, and Tsuyoshi Takagi. Parallel gauss sieve algorithm: Solving the SVP challenge over a 128-dimensional ideal lattice. In Hugo Krawczyk, editor, *Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings*, volume 8383 of *Lecture Notes in Computer Science*, pages 411–428. Springer, 2014.

[MV10] Daniele Micciancio and Panagiotis Voulgaris. Faster exponential time algorithms for the shortest vector problem. In Moses Charikar, editor, *Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2010, Austin, Texas, USA, January 17-19, 2010*, pages 1468–1480. SIAM, 2010.

* Japan Advanced Institute of Science and Technology (JAIST)