Development and Numerical Experiments of Massively Parallel Framework and Software for Shortest Vector Problem

立岩, 斉明

（様式３）

氏　　名　　：立岩 斉明

論 文 名　：Development and Numerical Experiments of Massively Parallel Framework and Software for Shortest Vector Problem
（最短ベクトル問題のための大規模並列フレームワークとソフトウェアの開発と数値実験）

区　　分　　：甲

論 文 内 容 の 要 旨

格子暗号は古典計算機や量子計算機による攻撃にも耐えうる次世代暗号として注目されている。格子暗号の本質的な安全性は、代表的な格子問題である最短ベクトル問題(SVP)の求解困難性に依存しており、暗号解析の観点から暗号のセキュリティレベルを評価するために高性能な並列計算によって SVP の求解困難性を正確に推定することが求められている。
複数の SVP 求解アルゴリズムがこれまで開発されているが、指数関数的な時間計算量や空間計量といった様々なデメリットがあり決定的に優れているアルゴリズムはない。 既存の有力な SVP 並列戦略は単一のアルゴリズムを共有メモリ空間やグローバルストレージを介した情報共有によって行われており、大規模な分散メモリ環境に適したものは我々の知る限りない。

我々は複数の異なる SVP 求解アルゴリズムが情報共有を伴いながら大規模な分散メモリ環境でも安定的な新しい並列スキームを提案し、同時にこのスキームを実現するフレームワークを開発した。 開発したフレームワークにより、異種アルゴリズムを大規模な分散システム上で非同期的に実行する並列戦略が実現可能になった。 制御プロセスへの情報集約により、少ない通信回数での効率的に情報共有と多くの計算時間を要する高次元の SVP 求解に不可欠なチェックポイントとリスタート機能が実現された。 フレームワークをベースに作成されたナイーブな SVP 求解ソフトウェアを用いた最大 103,680 コアによる SVP の求解実験により、フレームワークの安定性および実装された諸機能が SVP 求解性能を向上させることを示す。

さらに、作成したフレームワークの機能を最大限に活かした新しい分散非同期並列戦略およびそのソフトウェアを開発した。 このソフトウェアは block Korkine-Zolotarev(BKZ)基底簡約を拡張した DeepBKZ アルゴリズムの並列化のみに着目している。ランダマイズされた格子基底が複数のプロセスに配布され、それぞれのプロセスで独立して簡約処理が行われる一方、一部の基底ベクトルを全プロセス間で MPI により非同期に共有することでアルゴリズムが強化される。 基底のランダム性と情報共有の間にはトレードオフがあり、情報を共有しすぎるとすべてのプロセスが同じ問題を処理することになり、並列化の恩恵が失われてしまう。 そのため、このランダム性と情報共有のバランスを扱うために、基底集合の多様性を定量化する指標を提案しその有効性を示す。 これにより基底集合の多様性と求解性能のチューニングが可能になった。我々が提案する並列戦略とその実装の有効性をアルゴリズムの出力の質の向上とそのスケーラビリティの両方の観点から、最大 103,680 コアによる数値実験によって示す。