公開

（事後評価・研究者用）

研　究　報　告　書

「大規模並列計算に適した高速な格子基底簡約アルゴリズムの開発」

研究期間： 2018 年 10 月～2020 年 3 月
研究者番号： 50179
研 究 者： 照屋　唯紀

1．　研究のねらい

本研究のねらいは，高次元の格子問題を高速に求解するための格子基底簡約アルゴリズムの開発とその実装を行うことである．耐量子計算機暗号および次世代暗号の有力な候補である格子暗号の安全性は，格子問題の困難性を根拠とする．そのため，実用に耐えうる安全な格子暗号を実現するためには，最速の求解アルゴリズムとその高速な実装により，この困難性を可能な限り精密に評価する必要がある．

代表的な格子問題の一つは最短ベクトル問題(Shortest Vector Problem, SVP)であり，これは入力として格子を生成する基底が与えられて，非ゼロの格子点(位置ベクトル)のうち，最短の格子点を探索する問題である．また，最短の格子点に対してある程度長い格子点も解とみなす近似 SVP も研究の対象となっている．SVP の解法として，格子点列挙に基づく方法と格子篩に基づく方法が知られているが，どちらも格子の次元数に対して求解に要する計算時間が指数的に増加するため非効率的である．しかし，近似 SVP の解法である格子基底簡約と組み合わせる事で，互いの性能を飛躍的に向上させる事ができる．本研究では，これらアルゴリズムを組み合わせた，大規模並列計算機の性能を最大限引き出す事ができる高速な格子基底簡約法の開発を行う．

また，「SVP の求解に要する時間が次元数に対して指数的に増加する」という事は，次元数を大きくする事で直ちに安全な格子暗号を構築できる事を意味する．しかし，次元数が大きくなると効率性が著しく低下し，実用性が失われてしまう．そのため，安全性の達成に必要な困難性を持つ SVP を与える「丁度良い格子の次元数」を，可能な限り精密に推定する技術の開発も重要な研究課題である．本研究ではこのような推定技術の開発も並行して行う．

2．　研究成果

（1）概要

ランダムネス仮定と呼ばれる確率モデルの下で，Gram-Charlier A 型級数展開を利用して，格子点列挙法，サンプリングアルゴリズムおよび Babai の最近平面アルゴリズムが出力する格子点の長さの確率的推定法を構築し，項目 5-(1)-1 にて発表した．Babai の最近平面アルゴリズムは射影格子篩法で利用されており，この場合においても推定法を適用可能である．また，この推定法の入力は格子の基底であり，推定結果の良し悪しによって入力した基底の良さを評価する事も可能になると思われる．

（2）詳細

研究テーマ「SVP 困難性推定技術の開発」

格子点列挙法，サンプリングアルゴリズムおよび Babai の最近平面アルゴリズムは同じ種類のアルゴリズムであり，基底(と補助的な情報)を入力に取り，短い格子点を探索するために使用される．具体的には Gram-Schmidt 直交化した基底を使用して空間を格子点と一対一に対応する超直方体の集合で分割し，原点周辺のこれら超直方体内に包含される格子点を列挙する事で，短い格子点を探索する．ここで，もしも基底と列挙される超直方体の集合から，アルゴリズムが出力する格子点の長さの分布を確率的な分布とみなして推定する事ができれば，この確率を利用して(近似) SVP 求解に要する計算量を推定できる．しかし，確率を与えるようなランダムネスがアルゴリズムに存在しないため，そのような確率モデルを与えるヒューリスティックを導入する必要がある．

本研究では，ランダムネス仮定と呼ばれる確率モデルを採用し，Gram-Charlier A 型級数展開を利用して，アルゴリズムが出力する格子点の長さの確率的推定法を構築した．ランダムネス仮定とは，簡単に言えば，空間を分割した超直方体内に，格子点が連続的な独立一様分布に従って分布しているとする仮定であり，アルゴリズム内の変数の振る舞いに対して確率モデルを与える．Gram-Charlier A 型級数展開とは，確率分布に対する高次キュムラントを使用した漸近級数展開の一つである．これらの成果は項目 5-(1)-1 にて論文発表および登壇して口頭発表を行った．

研究テーマ「高速な格子基底簡約法の開発」

Babai の最近平面アルゴリズムは射影格子篩法においても利用されており，この場合においても項目 5-(1)-1 にて発表した推定法を適用可能である．また，この推定法の入力の一部は基底であり，推定結果として得られる確率の値を利用する事で，その基底の良さを評価する事も可能となり，そしてこれを利用する事で，格子基底簡約の改良も可能になると思われる．これら射影格子篩法と格子基底簡約は，現在世界最速の SVP 求解アルゴリズムの実装である G6K で使用されているアルゴリズムのうち主要なものである．よって，本研究により，さらに高速なアルゴリズムの開発について研究を行う際の理論的なツールを構築できたと考えられる．

3. 今後の展開

アメリカ国立標準技術研究所(National Institute of Standards and Technology)では，現在，耐量子計算機暗号の標準化プロジェクトを実施しており，2022 年から 2024 年頃に標準規格を決める予定としている．このプロジェクトには様々な暗号方式が世界中から提案されており，第 2 ラウンドに選出された 26 件のうち，格子暗号に属する方式の数は 12 件であり最も多い．この事から，格子暗号は耐量子計算機暗号の有力な候補と見なされていると考えられる．さらに，格子暗号は完全準同型暗号や関数暗号，効率的な秘密計算などの高機能暗号を実現可能にする要素技術でもある．その応用として，より高度な情報システムやサービスの実現が期待されている．最初に述べたように，格子暗号の安全性は SVP の困難性を根拠とする．しかし，SVP の実際の困難性は，計算機技術や SVP 求解技術，暗号解読技術の発展により変わる．すなわち，格子暗号の安全性が失われていないかを継続的に監視し評価できる技術や状況を確立しなければならない．本研究で得られた知見を元に，このような大きな目標

や関連するプロジェクトなどへの貢献を目指して，今後も研究活動を継続する予定である．

4. 自己評価

本研究の独創性・挑戦性と達成状況および波及効果については，最速の SVP 求解アルゴリズムの開発という挑戦的な目標を設定し，格子点列挙・格子篩・格子基底簡約を組み合わせた，大規模並列計算機に適した高速なアルゴリズムを開発するという方針で研究開発を行った．しかし，具体的な成果を得るには至っておらず，十分に目的を達成できたとは言い難い．しかし，SVP の困難性を評価するための推定方法を提案する事ができた．また，この推定方法はランダムネス仮定に基づく方法であり，この仮定はこれまであまり注目されていなかったため，高速な SVP 求解アルゴリズムの研究開発ついて，他の研究とは異なるアプローチの一つを提示できた．このように，安全な格子暗号の実現という大きな目標に対してある程度の貢献ができたと考えられる．

本研究の進め方について．本研究の目的を達成するために，研究費は主に大規模計算機利用料として使用した．大規模計算機における実装技術については，専門家である池上努氏から助言を得られる体制を構築でき，様々なノウハウを得る事ができた．この場を借りて池上氏に深く感謝します．

5. 主な研究成果リスト

（1）論文（原著論文）発表

1. Yoshitatsu Matsuda, Tadanori Teruya, Kenji Kashiwabara. “Efficient Estimation of Number of Short Lattice Vectors in Search Space under Randomness Assumption.” The 6th ACM ASIA Public-Key Cryptography Workshop (APKC 2019). 2019, p.13-22, doi: 10.1145/3327958.3329543

（2）特許出願

なし

（3）その他の成果（主要な学会発表、受賞、著作物、プレスリリース等）

なし