様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月 １６ 日現在

機関番号：８２６２６
研究種目：基盤研究(B)（一般）
研究期間：2020～2022
課題番号：２０Ｈ０４１９０

研究課題名（和文）格子篩と格子点列挙を組み合わせた高速な格子基底簡約アルゴリズムの構築

研究課題名（英文）Efficient Lattice Basis Reduction with Sieving and Enumeration

研究代表者
照屋　唯紀（Teruya, Tadanori）

国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員

研究者番号：２０６３６９７２

交付決定額（研究期間全体）：（直接経費）　　7,800,000円

研究成果の概要（和文）：格子の最短ベクトル問題(SVP)および近似SVPの高速解法の部品として使用されるサンプリング法の効率化方法を提案した。この方法は、ランダムネス仮定に加えて新たに導入した最適探索仮定により、サンプリング法が出力する格子点の長さの分布とその統計量の間に関係が存在すると仮定し、サンプリング法が短い格子点を出力する確率を最大化するような探索空間を具体的に求める。
また、SVP Challengeの世界記録を達成しているSVPソルバーの実装であるG6KおよびそのGPU拡張について調査し、効率的に短い格子点を探索する方法についていくつかの着想を得た。

研究成果の学術的意義や社会的意義
格子暗号は、耐量子計算機暗号(PQC)の一つであり、格子問題の困難性を安全性の根拠とする。最短ベクトル問題(SVP)およびその緩和版である近似SVPは代表的な格子問題であり、（近似）SVPの高速解法として、格子基底簡約と格子ふるい、格子点列挙の三つの方法を組み合わせた解法が提案されている。本研究は、主に格子点列挙の亜種であるサンプリング法の効率化について研究成果を得た。これにより、（近似）SVPの解法のさらなる高速化と、格子暗号の安全性評価への貢献が期待される。

研究成果の概要（英文）：We proposed an efficient method for the sampling algorithm, which is used as a component of a fast solver for the shortest vector problem (SVP) and the approximate SVP of lattices. In addition to the randomness assumption, we introduce a new assumption called the best search assumption that assumes a relationship exists between the distribution of lengths of lattice points output by the sampling algorithm and the statistics of that distribution. Then we described a method to find a search space that maximizes the probability of the sampling algorithm outputting short lattice points.
We also studied G6K and its GPU extension called G6K-GPU, the world record solver implementations in the SVP Challenge. We considered some ideas for methods to find short lattice points.

研究分野：暗号技術

キーワード：格子暗号　格子基底簡約　格子点列挙　格子ふるい

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

いくつかの格子問題は、格子の次元数を大きくした時、量子計算機を使用したとしても効率的に解くアルゴリズムが知られていない。そのため、格子問題の求解困難性を安全性の根拠とする格子暗号は、耐量子計算機暗号の一つとして広く注目されている。実用的な格子暗号を実現するためには、安全性の根拠となっている格子問題の困難性を具体的に評価する必要がある。最短ベクトル問題(Shortest Vector Problem, SVP)およびその緩和版である近似 SVP は、格子暗号において取り扱われる代表的な格子問題であり、（近似）SVP を高速に解く方法の開発は、格子暗号の安全性を評価し、効率的な格子暗号方式を設計する上で重要な研究課題である。

（近似）SVP の効率的な解法は、大きく分けて、格子基底簡約、格子点列挙、格子ふるいの三つがある。本研究の代表者および分担者は、これまで格子基底簡約と格子点列挙の二つ、そしてランダムネス仮定に基づく理論的な確率的解析手法を利用した解法について研究を行なって来た。例えば、ランダムネス仮定を利用することで、格子点列挙の亜種であるサンプリング法が出力する格子点の長さの分布を推定する方法を示すなど、アルゴリズムの性質の解析に利用可能な理論の整備を行った。

2019 年に、Albrecht ら(EUROCRYPT 2019)により、格子基底簡約、格子点列挙そして格子ふるいを組み合わせた高速な（近似）SVP ソルバーの実装 G6K が発表され、ダルムシュタット工科大が主催する SVP 求解コンテストである SVP Challenge の世界記録が更新された。格子暗号の安全性評価は、最も高速な求解アルゴリズムや実装に基づき実施されることが望ましい。そのため、格子基底簡約、格子点列挙、格子ふるいの三つを組み合わせた SVP 求解アルゴリズムについて研究を行うことが重要であると考えられる。

ここで、G6K が実装している（近似）SVP ソルバーの概要について解説する。SVP 求解にかかる時間計算量は、格子点列挙は$2^{O(n\log n)}$、格子ふるいは$2^{O(n)}$であり、格子ふるいの方が高速である。しかし、空間計算量はそれぞれ$O(\mathrm{poly}(n))$、$2^{O(n)}$であり、格子ふるいの実行には非常に膨大なメモリ空間が必要である。G6K は、格子基底簡約、格子点列挙、格子ふるいそれぞれの長所と短所を考慮しつつ、高速な SVP ソルバーが実現できるようにこれら三つを組み合わせていると考えられる。特に、格子点列挙の亜種である Babai-lift と呼ばれるアルゴリズムと Gram-Schmidt 直交化基底を使用して、低次元の射影空間上で格子ふるいを実行することで、格子ふるいを改良し、高速な SVP ソルバーを実現している。なお、この射影空間上の格子ふるいは、射影格子ふるいと呼ばれる。

２．研究の目的

本研究の目的は、これまでに行ってきた格子基底簡約と格子点列挙に加えて、（射影）格子ふるいを加えた三つの方法を組み合わせることにより、効率的な格子基底簡約法を構成すること、そして、これを使用して効率的な（近似）SVP 求解アルゴリズムを構成することである。これにより、格子暗号の安全性評価および効率的な格子暗号方式の設計に貢献することを目指す。

３．研究の方法

上で解説したように、格子基底簡約、格子点列挙、（射影）格子ふるいは、それぞれが（近似）SVP を解くための重要なビルディングブロックである。これら三つを組み合わせた（近似）SVP 求解アルゴリズムを構築する上で、それぞれの効率化方法について研究を行いつつ、それぞれの性質を明らかにすることが重要であると考えられる。そのため、まずはこれら三つそれぞれについて効率化の研究を試みる。これに加えて、Albrecht ら(EUROCRYPT 2019)が公開している G6K について文献調査を行いつつ、ABCI などのスーパーコンピュータを用いて G6K を実際に動かすなどの調査も行い、実装されている格子基底簡約、格子点列挙、そして（射影）格子ふるいの組み合わせ方法を分析し、さらなる効率化を試みる。

４．研究成果

まず始めに、IWSEC 2020 で発表した、格子点列挙の効率化について得られた成果を解説する。この研究成果では、box-type と呼ばれるサンプリング法に入力する探索空間について、ランダムネス仮定と確率的推定法や実験により得られた知見を応用し、サンプリング法の効率化方法を提案した。ここで言う効率化とは、長さが短い格子点をサンプリング法が出力する確率を向上させることを指し、提案方法は、確率が向上するようなサンプリング法に入力する探索空間を求める。

研究成果の概要を解説する。上記の背景で述べたように、Matsuda ら(APKC 2019)による既存研究において、ランダムネス仮定に基づき、Gram-Charlier A 型級数展開を用いて、box-type と

呼ばれる探索空間と基底を入力に取った場合にサンプリング法が出力する格子点の長さの分布を推定する方法を提案し、この推定が実際に精度良く長さの分布を推定できることを実験により確認した。この既存研究により得られた知見を応用してサンプリング法を効率化するために、この研究成果ではランダムネス仮定に加えて、新たに最適探索仮定(Best Search Assumption, BSA)を導入した。BSA は次のような仮定である：ランダムネス仮定を導入することにより、入力される基底 B と探索空間 Y に対してサンプリング法が出力する格子点の長さの分布 F を推定することができる。この時、分布 F の平均や分散、歪度、尖度などの高次統計量(cumulant)も算出することができる。BSA とは、統計量のうち、次数が 2 次以上の統計量を無視し、平均が最小となるような探索空間 Y を入力した時に、長さが短い格子点をサンプリング法が出力する確率が最大となる、とする仮定である。この BSA を導入することにより、サンプリング法の効率化を、平均が最小となるような探索空間 Y を求める問題に置き換えることができる。この研究成果では、格子の基底 B と、サンプリング法が出力する格子点の個数が与えられた時、この最小化問題を解いて box-type の探索空間 Y を求めるアルゴリズムを提案した。

次に、この提案アルゴリズムの性質や性能を評価するために行った実験の概要について解説する。SVP Challenge で出題されている 100 次元、128 次元、150 次元格子の基底を使用し、出力する格子点の個数を2^{28}に固定して、提案アルゴリズムで求めた探索空間と、Schnorr (STACS 2003)が提案したオリジナルのサンプリング法が使用している探索空間の性能を比較した。まず、それぞれの探索空間をサンプリング法に入力した際に出力される格子点の長さの分布を Gram-Charlier A 型級数展開により推定した。その結果、提案アルゴリズムにより求めた探索空間の方が、長さが短い格子点を出力する確率が高いことを確認した。次に、サンプリング法が実際に出力した格子点の長さの分布のうち、長さが短い格子点の分布を比較した。この実験を行った範囲ではその分布に大きな違いは認められなかったが、簡約された基底を入力した場合に多くの格子点が出力されていることがわかった。よって、簡約された基底においては、提案アルゴリズムによる効率化が期待できると考えられる。また、出力する格子点の個数を変更した場合に、提案アルゴリズムが求める探索空間の性質を分布の平均値を計算し BSA に基づいて考察した。上記実験と同じ基底を使用したところ、個数が約2^{20}個以下の場合には Schnorr (STACS 2003)の探索空間と同様の探索空間を得るが、この個数を超えた場合には、異なる探索空間を出力し、その違いが大きくなる傾向にあることがわかった。このことから、多くの格子点をサンプリング法により出力する場合には、提案アルゴリズムを使用して求めた探索空間の方が効率的となる可能性が示された。

次に、G6K に関する調査について述べる。なお、2021 年に Ducas ら(EUROCRYPT 2021)は G6K を GPU 向けに拡張した G6K-GPU-Tensor (G6K-GPU)を発表し、この実装により SVP Challenge の世界記録が再び更新された。上記の背景で述べたように、最も高速な求解アルゴリズムやその実装に基づき研究を行うことが重要であるため、この G6K-GPU についても調査を行った。G6K-GPU も G6K と同様に格子基底簡約、格子点列挙、射影格子ふるいを組み合わせた構成となっているが、GPU に適したアルゴリズムが新しく導入されている。ABCI 上で、SVP Challenge で出題されている 140 次元から 150 次元の格子に対して G6K-GPU を実行したところ、G6K よりも約 10 倍の速度で解を求めることを確認した。これら調査と実験結果をまとめ、本研究の代表者である照屋が組織委員の一人として参加した九州大 IMI 共同利用・共同研究プロジェクト（代表：王イントウ）の内部討論会にて発表した。また、参加した研究者と情報交換および議論を行い、SVP 求解アルゴリズムのさらなる効率化について着想を得た。なお、このプロジェクトの報告書などは下記 URL にて公開されている：

https://joint1.imi.kyushu-u.ac.jp/research_chooses/view/20210002

その後も引き続き G6K と G6K-GPU に対する調査および実験を継続した。G6K および G6K-GPU に導入されている近似計算アルゴリズムを参考に、これまでの格子点列挙に対する研究で得られた知見に基づき、アルゴリズムの効率化について検討した。その結果、射影格子ふるいの出力に対して Babai-lift を実行する際に行う長さが短い格子点の探索について、近似計算アルゴリズムにより探索する方法の着想を得た。

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 Matsuda Yoshitatsu
２．発表標題 Optimization of Search Space for Finding Very Short Lattice Vectors
３．学会等名 Advances in Information and Computer Security - 15th International Workshop on Security, IWSEC 2020（国際学会）
４．発表年 2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

照屋は、九州大IMI共同利用・共同研究プロジェクト（代表：王イントウ）に組織委員の一人として参加し、このプロジェクトの内部討論会にて、本研究で行った調査および実験について発表した。このプロジェクトの報告書などは https://joint1.imi.kyushu-u.ac.jp/research_chooses/view/20210002 にて公開されている。

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	松田　源立 (Matsuda Yoshitatsu) (40433700)	成蹊大学・理工学部・准教授 (32629)	
研究分担者	池上　努 (Ikegami Tsutomu) (80245612)	国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員 (82626)	

６．研究組織（つづき）

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	柏原　賢二 (Kashiwabara Kenji) (70282514)	東京大学・大学院総合文化研究科・助教 (12601)	2021年度まで参加

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	柏原　賢二 (Kashiwabara Kenji) (70282514)	東京大学・大学院総合文化研究科・助教 (12601)	2022年度から参加

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関