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　６ 年　 ５ 月 ２８ 日現在

機関番号：１２６０１
研究種目：基盤研究(C)（一般）
研究期間：2020～2023
課題番号：２０Ｋ１１６６９

研究課題名（和文）最短ベクトル問題における新しいsieving計算の手法の開発

研究課題名（英文）Development of a new sieving algorithm for the shortest vector problem

研究代表者
柏原　賢二（Kashiwabara, Kenji）

東京大学・大学院総合文化研究科・助教

研究者番号：７０２８２５１４

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：格子の最短ベクトル問題の基底簡約アルゴリズムについて研究した。格子の最短ベクトル問題は、公開鍵暗号システムの一つである格子暗号の安全性の基礎となる問題である。最短ベクトル問題とは、基底行列によって張られる格子内のベクトルの中で、最も短いベクトルを見つけ出す問題である。
基底を簡約するためには、多くの短い格子ベクトルの候補を生成し、その中から効率的に簡約を行うベクトルを選び出す作業を繰り返す。この研究では、どのように基底ベクトルを簡約していくと効率的に処理できるかを探求した。開発したプログラムを用いて、最短ベクトル問題のチャレンジサイトでランキングすることに成功した。

研究成果の学術的意義や社会的意義
従来の公開鍵暗号技術は、主に素因数分解や離散対数問題に基づいて安全性が設計されてきた。これらの技術は、現在のコンピュータ技術では解読が非常に困難であるため、高い安全性を誇っている。しかし、量子コンピュータの登場により、これらの公開鍵暗号技術が脅かされる可能性が出てきた。量子コンピュータに耐性のある新しい公開鍵暗号システムとして、格子暗号システムが研究されてきている。格子暗号システムは、数学の格子理論を基にしている。システムの安全性の評価には解読アルゴリズムの研究が欠かせない。
この研究では、プロセス並列計算を用いた、格子の最短ベクトル問題に対する効率的なアルゴリズムを開発した。

研究成果の概要（英文）：I researched the basis reduction algorithm for the shortest vector problem in lattices. The shortest vector problem in lattices forms the foundation of security for lattice-based cryptosystems, which are a type of public-key cryptosystem. The shortest vector problem involves finding the shortest vector among those in a lattice generated by a basis matrix. To reduce the basis, one must generate many candidates of short lattice vectors and repeatedly select the most efficient vector for reduction from among them. This research explored how to process basis reduction efficiently. Using the developed program, we successfully ranked on a challenge site for the shortest vector problem.

研究分野：暗号理論

キーワード：公開鍵暗号理論　基底簡約アルゴリズム　格子の最短ベクトル問題　並列計算

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

現代の情報社会にとって、公開鍵暗号技術は、必要不可欠のものになっている。従来の公開鍵暗号技術は、主に素因数分解(RSA)や離散対数問題(楕円曲線暗号)に基づいて安全性が設計されてきた。これらの技術は、現在のコンピュータ技術では解読が非常に困難であるため、高い安全性を誇っている。しかし、量子コンピュータの登場により、これらの公開鍵暗号技術が脅かされる可能性が出てきた。量子コンピュータで効率的な解法が見つかっていない、量子アルゴリズムに対する耐性のある新しい公開鍵暗号システムのひとつとして、格子暗号システムが研究されてきている。格子暗号システムは、数学の格子理論を基にしている。暗号システムの安全性の評価には解読アルゴリズムの研究が欠かせない。格子暗号の解読には、与えられた基底行列によって張られた格子に対して、もっとも短いベクトルを探すという格子の最短ベクトル問題を考える必要がある。格子の最短ベクトル問題にアプローチする主な手法としては、基底簡約問題を考えるということがある。基底簡約問題とは、格子の基底行列を少しずつ扱いやすいものに基底変換することで、格子の短いベクトルを探しやすくしていこうというものである。格子の基底簡約問題に対するアルゴリズムとしては、近年は、sieving と呼ばれるアルゴリズムがもっとも有効とされていて注目を集めている。これは既知の大量の短い格子ベクトルを足したり引いたりして組み合わせて、新しい短い格子ベクトルを探す手法である。

２．研究の目的

ドイツのダルムシュタット大学によって 2010 年より運営されている SVP Challenge と呼ばれる格子の問題サイトがある。https://www.latticechallenge.org/svp-challenge/
そこでは次元ごとに基底行列が与えられて、それに対して、各次元でより短い格子ベクトルを探すということを競うサイトである。高次元の基底行列ほど短いベクトルを探すのが難しい。高次元の問題にエントリーするには、並列コンピュータなどを用いて大規模な計算を行う必要がある。並列アルゴリズムを用いて、基底簡約問題に対する効率的なアルゴリズムを開発し、SVP Challenge にエントリーするのがこの研究の主な目的である。元々は、Enumeration という格子ベクトル生成手法を用いて、われわれのグループが SVP Challenge のもっとも高次元の問題にエントリーしていた。しかし、2018 年に Ducas らのグループによる sieving のアルゴリズムを用いた計算によりもっとも高い次元の記録を奪われた。彼らの並列計算においては、CPU によるスレッド並列の計算を用いたり、GPU による並列計算を用いたものであった。われわれは、利用している計算機の環境により合致する、プロセス並列によるアルゴリズムを開発することで、対抗しようとした。複数の CPU 間でメモリを共有する必要があるスレッド並列よりも、CPU 間でメモリを共有しないプロセス並列のほうが、より計算の規模を容易に増やすことができ、幅広い計算機環境に対応することができる。

３．研究の方法

基底簡約アルゴリズムは、既知の格子ベクトルを用いた大量の短い格子ベクトルの生成の部分のステップと、そのなかで有効な格子ベクトルを選択して、基底行列をよりよいものに基底変換する部分のステップの繰り返しからなる。もともとはすべて独自に書いた C++のプログラムを開発していた。記録が抜かれたときに、格子ベクトルの生成方式として、sieving を利用したものに切り替えようとして、独自にプログラムを書いた。しかし、そのプログラムは思うような性能を出すことができなかった。そこでベクトル生成部分は、Ducas らが GitHub にソースを公開している G6K と言われるシステムを採用し、そのベクトルの選択部分だけを独自に、われわれの並列計算機環境に合うように書き換えることに方針転換した。われわれのシステムはそれぞれのプロセスが独自の基底をもち、有用な短いベクトルが得られたときは、ファイルシステムを通じて、プロセス間で情報をやり取りするというものである。さらにわれわれのアルゴリズムの特徴として、基底変換に使えるような格子ベクトルが見つかってもすぐに基底簡約に適用せずに、候補として保持し、より短い格子ベクトルが見つかるまで更新を保留するという工夫を行なった。長さの更新幅がどのくらいかを評価関数で表して、そのときどきでもっとも評価のよい格子ベクトルを基底簡約に用いた。これは、基底行列の前のほうのインデックスで基底簡約を行うとそれ以降のインデックスの直交基底ベクトルを短くしていてもリセットされてしまうからである。
われわれの利用している計算機環境は、東京大学等が運用している OakBridge CX などであった。並行して一部、パソコンも計算に用いた。科研費の予算を利用して大型計算機を借りて、計算をおこなった。

４．研究成果

我々は Ducas らが開発した G6K のプログラムの基底簡約部分を大幅に改造した。彼らのプログラムのベクトル生成部分は C++で書かれ、基底簡約部分は、Python で書かれていたが、主に基底簡約部分に関して改良を加えた。プロセス並列を利用した計算により並列プロセス間で、よい基底行列の情報を交換する基底簡約プログラムを作成した。スーパーコンピュータ上で実行することにより、SVP Challenge のサイトに 162 次元や 166 次元などの記録をエントリーすることができた。166 次元のエントリーベクトルを見つけた後に、168 次元の問題に対して、計算を行ったが、残念ながら期間中にエントリーベクトルを見つけることができなかった。168 次元の問題に対して、パソコンによる計算は続けているが、スーパーコンピュータとの能力差は大きく、エントリーベクトルが見つかりそうな状況ではない。現在は Wang らのグループが 186 次元という高い次元の計算に成功しているが、これは GPU を用いた計算を行っているということと主にメモリの大きさの差と思われる。sieving は、非常に大きなメモリを利用したほうが、大量の格子ベクトルを一気に生成することができるので有利なアルゴリズムになっている。
プロセス並列計算により、高次元で短い格子ベクトルを見つけたことにより、格子の簡約問題の安全性の評価において、一定の貢献をすることができた。

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　0件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 柏原賢二	４．巻 -
２．論文標題 格子の最短ベクトル問題に対する離散的考察と並列計算アルゴリズム	５．発行年 2022年
３．雑誌名 Jxiv プレプリントサーバー	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.51094/jxiv.60	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 柏原賢二
２．発表標題 大規模並列計算による格子の最短ベクトル問題の効率化について
３．学会等名 日本応用数理学会
４．発表年 2021年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

SVP Challenge https://www.latticechallenge.org/svp-challenge/

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

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