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　元 年　 ６ 月　 ６ 日現在

機関番号：１２６０１
研究種目：研究活動スタート支援
研究期間：2017～2018
課題番号：１７Ｈ０６５７１

研究課題名（和文）代表的な耐量子暗号に対する格子理論に基づく安全性解析

研究課題名（英文）Security Evaluation of Representative Post-quantum Cryptographic Scheme from Lattices

研究代表者
高安　敦（Takayasu, Atsushi）

東京大学・大学院情報理工学系研究科・助教

研究者番号：００８０８０８２

交付決定額（研究期間全体）：（直接経費）　　2,200,000円

研究成果の概要（和文）：来たる量子計算機の完成に備え、耐量子公開鍵暗号の安全性解析を行った。特に、その中でも最も注目されている格子暗号を対象とし、安全性の根拠となる最短ベクトル問題やlearning with errors（LWE）問題の困難性解析を行った。まず、代表的な近似最短ベクトル探索アルゴリズムとして知られるLLLアルゴリズムにおいて、低次元の場合に厳密な最短ベクトルを出力する条件を厳密に整理した。さらに、様々な変形方式のあるLWE問題を包括的に解く枠組みを整理し、その枠組みでの困難性を評価した。

研究成果の学術的意義や社会的意義
これまで、格子暗号の安全性を見積もるために、Kannanの埋め込み法とBai-Galbraithの埋め込み法の二つが広く用いられてきた。本研究は、格子暗号の安全性を見積もるためのLWE問題の一般的な定式化を捉え、従来よりもLWE問題の計算量解析をより統一的に行えるようになったという意味で学術的意義を持つ。さらに、本研究は、将来量子計算機が実用化された場合の情報社会の安全性を守るための耐量子公開鍵暗号の実用化へ向けて重要な社会的意義を持つ研究となった。

研究成果の概要（英文）：It is widely known that RSA/ECC is insecure in the presence of quantum computers. Thus, I work on the security estimation of post-quantum cryptography. In particular, I focus on lattice-based cryptography as the representative post-quantum scheme. Therefore, I study the hardness of the shortest vector problem and learning with errors problem in this project. I first find a necessary and sufficient condition when the LLL algorithm outputs the shortest non-zero lattice vector in small dimensions. Then, I further work on the learning with errors. I provide a generic framework to study the hardness of the learning with errors in general formulation.

研究分野：暗号理論

キーワード：耐量子暗号　格子　learning with errors問題　最短ベクトル問題　安全性解析

１．研究開始当初の背景

現在実用的に用いられている RSA 暗号や楕円曲線暗号の安全性は、それぞれ素因数分解や（楕円曲線上の）離散対数問題と密接な関連がある。ところが、これらの問題は、量子アルゴリズムによって多項式時間で解けることがわかっている。そのため、量子アルゴリズムに対しても安全な耐量子暗号の実用化は、暗号理論研究において喫緊に解決すべき課題である。格子暗号は、耐量子暗号の代表的な候補の一つとして知られており、属性ベース暗号や完全準同型暗号など、様々な実用的利点も知られている。格子公開鍵暗号方式の安全性が根拠を置く LWE（learning with errors）問題は、格子の次元・ノイズの大きさ・法の大きさ・サンプル数・秘密ベクトルの大きさなどの様々なパラメータによって定義されているため、その計算量解析は非常に複雑である。これまで、ある特殊ケースの場合についての知見が蓄えられており、Kannan の埋め込み法や Bai-Galbraith の埋め込み方が、それぞれ秘密ベクトルが大きい時と小さい時に有効であることが知られていた。ところが、これらの解析では、LWE サンプルが十分豊富に得られる場合についての考察が主であるなど、一般的な LWE 問題の定式化における困難性解析はあまり行われてこなかった。

２．研究の目的

LWE 問題の計算量的困難性を解析することは、格子暗号実用化に向けて大きな意味を持つ重要な研究である。これまで、LWE 問題が漸近的に計算量的困難であることを利用し、LWE 問題の計算量的困難性に安全性の根拠を置く格子暗号の理論的構成については多くのことがわかっているが、LWE 問題の実パラメータの計算量的困難性があまりわかっていないため、格子暗号実用化のためのパラメータを上手く選ぶことができていなかった。このパラメータの設定は、格子暗号を実用化する際の効率に大きく関わる。そのため、実用化に向けて数多くの格子暗号があるにも関わらず、安全性・効率性の最適なトレードオフとなる実装パラメータが見つかっていなかった。つまり、安全性に重きを置いて非常に大きなパラメータを選ぶと、安全性は損なわないかもしれないが、計算時間が大きくなりすぎてしまう。対して、もし効率性を重視して小さなパラメータを選べば、安全性が損なわれてしまう危険性がある。実用的に計算が重すぎると、実社会のサービスにおいて利用することは難しいと考えられる。さらに、前述のように、これまで LWE 問題のパラメータは、ある特定の場合の解析が主に行われてきたが、近年、なるべく効率的な格子暗号を構成するために、これまであまり重視されてこなかったパラメータにおける LWE 問題の困難性に安全性の根拠を置く格子公開鍵暗号方式も提案されている。そのため、一般的定式化の LWE 問題の困難性解析という問題の解決は、来たる量子計算機完成後の情報社会の安全性を保証することを目的とする研究である。

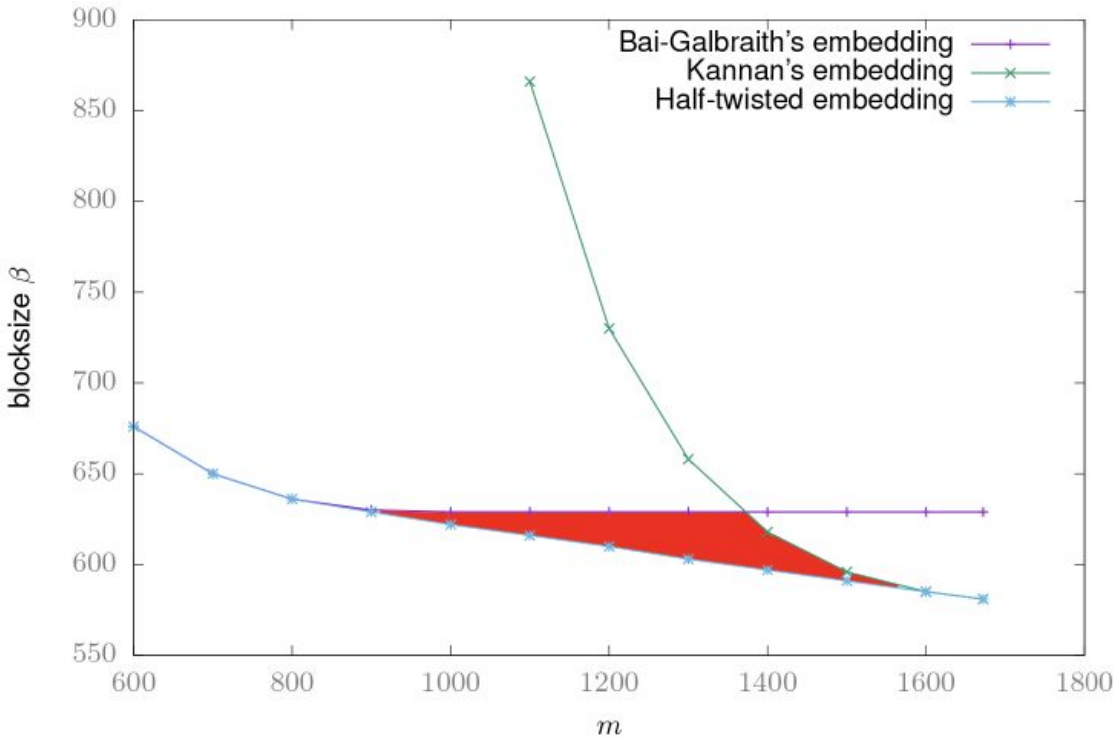
３．研究の方法

従来の研究と一線を画し、本研究では、LWE 問題の計算量的困難性を統一的に解析することを目指す。例として、これまでは、LWE 問題を定義するパラメータとして、秘密ベクトルの定義域の大きさは事前に固定され、その大きさによって Kannan の埋め込み法を用いるのか、Bai-Galbraith の埋め込み法を用いるのかが分かれていた。現在行われている研究は、同じパラメータのもとで、Kannan の埋め込み法や Bai-Galbraith の埋め込み法をより効率的に実装することを目指すものが主である。また、これまでの解析では、サンプル数も十分得られることを仮定して研究されていた。だが、数学的に LWE 問題を考えるのではなく、暗号学的に考えれば、このように豊富に LWE サンプルが得られるという状況はあまり考えられない。よって、本研究では、秘密ベクトルの定義域のみならず、格子の次元・ノイズの大きさ・法の大きさをも一般的な扱いを目指す。ただし、従来の研究のように、LWE 問題のインスタンスを埋め込み法によって格子の unique-SVP 問題として定式化し、その格子問題は、既存の BKZ アルゴリズムを用いて解くことで LWE 問題の解を求める。BKZ アルゴリズムの改良は、多くの研究で活発に行われている。本研究では、一般的定式化のもとでの LWE 問題に対する埋め込み法に注目し、その最適な構成を目指す。

４．研究成果

本研究では、まず、Bai-Galbraithの埋め込み法は、Kannanの埋め込み法にある種のtwistを作用させた形をしていることに着目した。前述のように、Kannanの埋め込み法は、秘密ベクトルが大きい場合、そして、Bai-Galbraithの埋め込み法は、秘密ベクトルが小さい場合に有効である。よって、本研究では、この二つを補間するように一般化した、half-twisted埋め込み法と呼ぶ新たな埋め込み法を提案し、一般的な定式化のもとでのLWE問題の困難性を評価する。次元nのLWEサンプルをm個もらうとき、Kannanの埋め込み法では(m+1)×(m+1)行列を、Bai-Galbraith埋め込み法では(n+m+1)×(n+m+1)行列を構成し、それらの行列が貼る格子の最短ベクトル(unique-shortest vector)を計算することにより、LWE問題の秘密ベクトルを計算していた。だ

が、本研究のhalf-twisted埋め込み法では、まず、twistパラメータ tを0からnの間の整数として設定し、(t+m+1)×(t+m+1)行列を構成し、それらの行列が貼る格子の最短ベクトルを計算することにより、LWE問題の秘密ベクトルを計算する。このとき、twistパラメータがt=0のときにはhalf-twisted埋め込み法はKannanの埋め込み法と一致し、twistパラメータがt=nのときにはhalf-twisted埋め込み法はBai-Galbraith埋め込み法と一致する。これにより、我々は、パラメータが与えられたあとにtwistパラメータtを最適化することで、事前に秘密ベクトルの大きさやサンプル数を固定することなく、包括的なLWE問題の困難性解析が可能になった。つまり、最初からKannanの埋め込み法やBai-Galbraithの埋め込み法として解析を行うのではなく、half-twisted埋め込み法として解析した後にtwistパラメータtを最適化することで、欲しい最適な埋め込み法を得ることができる。また、このような埋め込み法を提案した意図として、これまであまり考えられてこなかったが、秘密ベクトルの大きさが中間的な値となるとき、half-twisted埋め込み法がKannanの埋め込み法やBai-Galbraithの埋め込み法よりも効率的になることを期待したためである。



先に期待として述べたように、提案したhalf-twisted埋め込み法の利点は、単にKannanの埋め込み法をBai-Galbraithの埋め込み法を一般化しただけに止まらないことを確認した。これまであまり注目されてこなかったが、サンプル数が限られたときには、Kannanの埋め込み法やBai-Galbraithの埋め込み法よりも効率的になる場合があることを示した。つまり、twistパラメータtが、t=0やt=nではなく、0<t<nの範囲で最適化される場合があることを示した。これによって、特定のパラメータにおいてLWE問題の困難性を評価するためのより高速な埋め込み法を見つけるという先進的な成果を得ることができた。これは、LWE問題を単に数学的問題として捉えるのではなく、暗号学的に意味のある設定でより良い結果を得ることができたと考えている。
添付のグラフは、サンプル数mのLWE問題の困難性を既存のBKZアルゴリズムの実行時間シミュレータによって評価したものである。縦軸のβは、BKZアルゴリズム内のアルゴリズムパラメータであるブロックサイズを表しており、BKZアルゴリズムの計算量は、（格子の次元がほとんど変わらない場合には)ブロックサイズβが小さくなればなるほど小さくなると考えることができる。このグラフから分かるように、ある特定のパラメータにおいては、Kannanの埋め込み法や

Bai-Galbraith埋め込み法よりも、提案したhalf-twisted埋め込み法の方が小さなブロックサイズβにおいてLWE問題を解けることを示しており、つまり、より高速にLWE問題を解くことができるパラメータ（赤い領域）が存在することが確認できる。

５．主な発表論文等

〔雑誌論文〕（計　2　件）

① Kotaro Matsuda, Atsushi Takayasu, and Tsuyoshi Takagi. Explicit Relation between Low-dimensional LLL-reduced Bases and Shortest Vectors. IEICE Transactions on Fundamenals of Electronics, Communications and Computer Sciences. (to appear)
② Weiyao Wang, Yuntao Wang, Atsushi Takayasu, and Tsuyoshi Takagi. Estimated Cost for Solving Generalized Learning with Errors Problem via Embedding Techniques. Advances in Information and Computer Security, pp. 87-103, Lecture Notes in Computer Science, volume 11049, Springer, 2018.

〔学会発表〕（計　4　件）

① Weiyao Wang, Yuntao Wang, Atsushi Takayasu, and Tsuyoshi Takagi. Estimated Cost for Solving Generalized Learning with Errors Problem via Embedding Techniques. The 13th International Workshop on Security. Sendai, Japan. September 3rd-5th, 2018.
② Kotaro Matsuda, Atsushi Takayasu, and Tsuyoshi Takagi. Explicit Relation between Low-dimensional LLL-reduced Bases and the Shortest Vectors. The 11th Annual Meeting of the Asian Association for Algorithms and Computation. Beijing, China. May 18th-20th, 2018.
③ 井上晶登，王イントウ，高安敦，高木剛．少ないサンプル数の LWE 問題に対する kannan の埋め込み法の挙動評価．2019 年暗号と情報セキュリティシンポジウム，2B4-1, 2019 年 1 月 22 日-25 日.
④ Weiyao Wang, Yuntao Wang, Atsushi Takayasu, and Tsuyoshi Takagi. A New Embedding Method for Generalized LWE. 情報セキュリティ研究会，2018 年 7 月 25-26 日.

〔図書〕（計　　件）

〔産業財産権〕
○出願状況（計　0　件）

名称：
発明者：
権利者：
種類：
番号：
出願年：
国内外の別：

○取得状況（計　0　件）

名称：
発明者：
権利者：
種類：
番号：
取得年：
国内外の別：

〔その他〕
ホームページ等

６．研究組織

(1)研究分担者
研究分担者氏名：
ローマ字氏名：
所属研究機関名：

部局名：

職名：

研究者番号（8 桁）：

(2)研究協力者

研究協力者氏名：

ローマ字氏名：

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。