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　２ 年　 ７ 月　 ６ 日現在

機関番号：９４３０５
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００００２７

研究課題名（和文）格子問題を解く量子アルゴリズムの耐量子暗号と量子人工知能への応用

研究課題名（英文）Application of Quantum Algorithms for Lattice Problems to Post-Quantum Cryptography and Quantum Artificial Intelligence

研究代表者

河野　泰人（Kawano, Yasuhito）

日本電信電話株式会社ＮＴＴコミュニケーション科学基礎研究所・メディア情報研究部・主任研究員

研究者番号：４０３９６１８０

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：量子コンピュータでも解読が困難とされる次世代公開鍵暗号（LWE暗号）の条件付き解読アルゴリズムを提案した。提案したアルゴリズムは三種類で、その内の二種類はゲート型量子コンピュータと古典コンピュータのハイブリッドアルゴリズム、もう一種類は量子アニーリングマシンと古典コンピュータのハイブリッドアルゴリズムである。また、これらのアルゴリズムの古典ニューラルネットワークの深層学習への応用方法を提案した。三種類の内の最後のアルゴリズムをハードウェア上で実装し、LWE問題のベンチマーク問題として知られるTU Darmstadt LWE Challengeの次元が最も小さい問題の解読に成功した。

研究成果の学術的意義や社会的意義
本研究は、量子コンピュータでは解読できないとされている次世代公開鍵暗号に対する条件付き解読アルゴリズムの研究を通して、次世代公開鍵暗号の量子コンピュータに対する弱点を明らかにする目的で行われた。研究の結果、量子コンピュータや量子アニーリングを用いた新たな攻撃方法が提案され、次世代公開鍵暗号の脆弱性に関する知見がもたらされた。また、提案された解読アルゴリズムの深層学習への応用方法が提案された。

研究成果の概要（英文）：We proposed algorithms for cryptanalyzing the LWE cryptography under certain conditions. The LWE cryptography is a candidate of the next-generation public-key cryptography and is considered as being secure against a quantum computer. Three algorithms are proposed. Two of them are hybrid algorithms for a gate-type quantum computer and a classical computer, and the other is a hybrid algorithm for a quantum annealing machine and a classical computer. In addition, we proposed a method of applying those algorithms to learning the deep neural networks. We implemented the third algorithm on a computer and succeeded in solving the smallest dimensional problem of TU Darmstadt LWE Challenge, which is a famous benchmark site of LWE problems.

研究分野：量子情報

キーワード：量子コンピュータ　量子アルゴリズム　量子人工知能　ニューラルネットワーク　深層学習　耐量子暗号　格子暗号　解読

様　式　C－１９、F－１９－1、Z－１９（共通）

１．研究開始当初の背景

1994 年、Shor（現 MIT 教授）は因数分解と離散対数問題を効率的に実行する量子アルゴリズムを発表し、RSA 暗号や楕円曲線暗号を含めて、現在使用されている公開鍵暗号の大部分が量子コンピュータにより解読されることを示した。この発表を契機に、量子コンピュータを用いても解読できない公開鍵暗号の研究が活発になった。量子コンピュータの攻撃に耐える公開鍵暗号は耐量子暗号またはポスト量子暗号と呼ばれる。Shor の発表から 20 年以上が経過した現在でも、インターネットで標準的に用いられる 1024 ビットの RSA 暗号は量子コンピュータで解読されていない。しかし、近年の量子情報技術の急速な進歩を受け、1024 ビットの RSA 暗号は 30 年以内には解読できるようになると予想されている。社会インフラとしての公開鍵暗号システムを更新するためには 20 年以上の時間を要するため、耐量子暗号は標準化作業がすでに始まっている。既存の公開鍵暗号に脅威が迫る中、耐量子暗号は暗号研究の主要な一分野を占めるようになっている。

耐量子暗号の中で最も有力とされている暗号方式が格子暗号である。格子暗号は、格子と呼ばれる古くから研究されてきた数学的対象を利用する公開鍵暗号で、数学における長年の研究蓄積が利用できる点に特徴がある。中でも、2006 年に提案された LWE 暗号は、最有力視されている次世代公開鍵暗号の一つである。LWE とは Learning With Errors の頭文字であり、学習に関係する概念である。平たく言えば、LWE 暗号とは学習の困難さをベースとする公開鍵暗号のことである。

LWE 暗号の量子コンピュータに対する安全性は、適当な仮定の下で証明されている。もう少し正確に言うと、ある仮定の下、十分鍵長を長くすれば、どのような量子アルゴリズムを用いても多項式時間で LWE 暗号を解読できないことが、理論的に証明できる。ただし、鍵長を決めるためにはコンピュータを用いた解読実験による安全性評価が不可欠だが、現時点では量子コンピュータが開発されていないため、これまで安全性評価は古典コンピュータを用いて行われおり、LWE 暗号の量子コンピュータに対する安全性評価としては不十分な点が問題である。また、鍵長以外にもパラメータが多数あり、パラメータの細かな設定と安全性との関係など未解明な部分も多い。

２．研究の目的

本研究の目的は、LWE 暗号を条件付きで解読する量子アルゴリズムを新たに提案し、その効率を解析することにより、LWE 暗号の量子コンピュータに対する安全性を再評価することである。この安全性評価により LWE 暗号の量子コンピュータに対する脆弱性を明らかにし、標準化に反映させることで、次世代公開鍵暗号の安全性向上が期待できる。また、LWE 暗号が学習の困難さをベースとする公開鍵暗号であることを利用し、LWE 暗号を解読する量子アルゴリズムを深層学習に応用し、古典コンピュータ上で動作する従来のアルゴリズムに比べて高速な深層ニューラルネットワークの学習アルゴリズムの開発も期待できる。

３．研究の方法

LWE 暗号解読アルゴリズムの提案､提案した解読アルゴリズムのコンピュータ上での実装、実装した解読アルゴリズムを用いた LWE ベンチマークの解読実験、提案した解読アルゴリズムの深層学習への応用、の 4 種類に分けて説明する。

（１）LWE 暗号解読アルゴリズムの提案

日本学術振興会科研費 基盤研究(C) 20500024「行列分解を用いた量子回路設計とその応用」、および日本学術振興会科研費基盤研究(C) 25330021「非可換群上の量子フーリエ変換とその応用」における研究成果を利用し、新しい解読アルゴリズムを提案する。科研費で購入したコンピュータを用いてシミュレーション実験を行い、アルゴリズムの開発に役立てる。近年、注目を集めている量子アルゴリズムと古典アルゴリズムを組み合わせたハイブリッド型アルゴリズムなども視野に入れ、研究を行う。

（２）提案した解読アルゴリズムのコンピュータ上での実装

科研費で購入したコンピュータ、および現時点で利用可能な量子コンピュータ類（NISC、量子アニーリングマシン、コヒーレント・イジング・マシンなど）上に、提案アルゴリズムを実装する。古典コンピュータ上で量子アルゴリズムを実装する場合にはシミュレータを利用する。量子コンピュータが開発された場合に簡単に移植できるようにすること、および将来の量子人工知能への応用を考慮し、Python など人工知能研究で広く利用される言語を用いる。

（３）実装した解読アルゴリズムを用いた LWE ベンチマークの解読実験

実装した解読アルゴリズムを用いて、LWE ベンチマークとして有名な TU Darmstadt LWE Challenge の問題を解く。LWE Challenge の問題は最低次元が 40 次元だが、現在利用可能な量子コンピュータの上でこのクラスの問題を解くことは難しい。そこで、同サイトに掲載されている練習問題である LWE Toy Challenge を利用する。LWE Toy Challenge は 2,5,10 次元の問題である。また、これら以外にも、ランダムに生成した LWE 問題を解かせ、解読アルゴリズムの性能を検証する。

（４）提案した解読アルゴリズムの深層学習への応用

LWE 暗号を解読するアルゴリズムを学習アルゴリズムと見なして、深層ニューラルネットワークの教師あり学習に応用する。深層ニューラルネットワークの学習に用いられるバックプロパゲーションを改良する。最終的には、実装した解読アルゴリズムを利用し、深層ニューラルネットワークの学習アルゴリズムの実装と、簡単な学習実験を目指す。

４．研究成果

上記、研究の方法に記載した（１）—（４）のそれぞれについて、研究成果をまとめる。

（１） LWE 暗号解読アルゴリズムの提案

期間中、全部で三種類の解読アルゴリズムを提案した。それぞれ、量子フーリエ変換を利用する解読手法、量子スワップテストを利用する解読手法、インターポレーションと呼ばれる方法を利用する解読手法である。第一の解読手法は、ゲート型量子コンピュータの使用を前提としており、実装が難しい反面、高速な解読が期待できる。この手法は、電子情報通信学会第 36 回量子情報技術研究会（QIT36) 「格子問題を解く量子アルゴリズムについて」、量子 ICT フォーラム「格子暗号解読に向けた量子アルゴリズム研究の取り組みについて」、電子情報通信学会第 37 回量子情報技術研究会（QIT37)「格子暗号の安全性について」にて発表した。また、国内出願特許「変換装置、判定装置、および計算装置」（特願 2017-205011)、および海外出願特許 “TRANSFORMATION APPARATUS, DECISION APPARATUS, QUANTUM COMPUTATION APPARATUS AND QUANTUM MACHINE LEARNING SYSTEM”（出願番号 16/168014）で特許出願を行った。第二の解読手法は、実装しやすい反面、解読速度が遅いという欠点があるため学会での発表は行わず、特許出願のみを行った。出願先は、海外出願特許 “TRANSFORMATION APPARATUS, DECISION APPARATUS, QUANTUM COMPUTATION APPARATUS AND QUANTUM MACHINE LEARNING SYSTEM”（出願番号 16/168014)、および国内出願特許「判定装置、計算装置、および学習システム」（特願 2019-047931）である。第三の解読手法は、量子アニーリングマシンの使用を想定した解読手法で、解読に関する理論的な保証がない反面、現時点でも比較的高次元の LWE 暗号解読に適用できる。この方式は、国際会議 CNC 2019 “Computer Simulation of Quantum Algorithms for Lattice Problems”、電子情報通信学会第 41 回量子情報技術研究会（QIT41)「LASOLV を用いた次世代公開鍵暗号の攻撃方法について」、および国際会議 FQST 2020 “On Attacking the Next-Generation Public-Key Cryptography by Using LASOLV”にて発表した。

（２）提案した解読アルゴリズムのコンピュータ上での実装

現段階で最も実装の容易な第三の解読手法を実装した。第三の解読手法は、古典コンピュータと量子アニーリングマシンのハイブリッドタイプで、量子アニーリングマシンにはアルゴリズムがないため、主として古典コンピュータ上での古典アルゴリズムの実装を行った。実装は、Mathematica および Python で行った。Mathematica を利用したのは、処理が非常に重く、高次元の LWE 問題を解かせた場合、Python で書いた処理系だけでは計算が終了しないためである。

（３）実装した解読アルゴリズムを用いた LWE ベンチマークの解読実験

実装した第三の解読手法を用いて、TU Darmstadt LWE Challenge に掲載されている 2 次元 LWE 問題を解き、量子コンピュータを用いた LWE 暗号の解読に成功した。この成果を、電子情報通信学会第 41 回量子情報技術研究会（QIT41)「LASOLV を用いた次世代公開鍵暗号の攻撃方法について」にて発表した。また、この成果を発展させ、20 次元の LWE 暗号の解読方法を国際会議 FQST 2020 “On Attacking the Next-Generation Public-Key Cryptography by Using LASOLV”にて発表した。

（４）提案した解読アルゴリズムの深層学習への応用

LWE 暗号の解読アルゴリズムの深層学習への応用方法を考案し、電子情報通信学会　第 39 回量子情報技術研究会（QIT39)「教師あり深層学習のための量子アルゴリズムについて」にて発表した。また、同手法を特許出願した。出願先は、海外出願特許 “TRANSFORMATION APPARATUS, DECISION APPARATUS, QUANTUM COMPUTATION APPARATUS AND QUANTUM MACHINE LEARNING SYSTEM”（出願番号 16/168014)、および国内出願特許「判定装置、計算装置、および学習システム」（特願 2019-047931）である。現段階では問題の次元が高すぎて量子コンピュータでの処理が難しいという問題点も明らかになった。処理方法を工夫して、量子コンピュータで処理できるようにするためにはさらに工夫が必要であり、今後に残された課題となった。

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計7件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 河野　泰人，関川浩
２．発表標題 格子問題を解く量子アルゴリズムについて
３．学会等名 電子情報通信学会　第36回量子情報技術研究会（QIT36）
４．発表年 2017年

１．発表者名 河野泰人，関川浩
２．発表標題 格子暗号解読に向けた量子アルゴリズム研究の取り組みについて
３．学会等名 量子ICTフォーラム
４．発表年 2017年

１．発表者名 河野泰人，関川浩
２．発表標題 格子暗号の安全性について
３．学会等名 電子情報通信学会　第37回量子情報技術研究会（QIT37）
４．発表年 2017年

１．発表者名 河野泰人，関川浩
２．発表標題 教師あり深層学習のための量子アルゴリズムについて
３．学会等名 電子情報通信学会　第39回量子情報技術研究会（QIT39）
４．発表年 2018年

１．発表者名 Yasuhito Kawano, Hiroshi Sekigawa
２．発表標題 Computer Simulation of Quantum Algorithms for Lattice Problems
３．学会等名 Coherent Network Computing (CNC 2019)（国際学会）
４．発表年 2019年

１．発表者名 河野泰人，関川浩
２．発表標題 LASOLVを用いた次世代公開鍵暗号の攻撃方法について
３．学会等名 電子情報通信学会　第41回量子情報技術研究会（QIT41）
４．発表年 2019年

１．発表者名 Yasuhito Kawano, Hiroshi Sekigawa
２．発表標題 On Attacking the Next-Generation Public-Key Cryptography by Using LASOLV
３．学会等名 FQST 2020（国際学会）
４．発表年 2020年

〔図書〕　計0件

〔出願〕　計3件

産業財産権の名称	発明者	権利者
変換装置、判定装置、および計算装置	河野泰人，関川浩	NTT，東京理科大学
産業財産権の種類、番号	出願年	国内・外国の別
特許、特願2017-205011	2017年	国内

産業財産権の名称	発明者	権利者
TRANSFORMATION APPARATUS, DECISION APPARATUS, QUANTUM COMPUTATION APPARATUS AND QUANTUM MACHINE LEARNING SYSTEM	Y. Kawano, H. Sekigawa	NTT
産業財産権の種類、番号	出願年	国内・外国の別
特許、16/168014	2018年	外国

産業財産権の名称	発明者	権利者
判定装置、計算装置、および学習システム	河野泰人，関川浩	NTT，東京理科大学
産業財産権の種類、番号	出願年	国内・外国の別
特許、特願2019-047931	2019年	国内

〔取得〕　計0件

〔その他〕

―

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	関川　浩 (Sekigawa Hiroshi) (00396178)	東京理科大学・理学部第一部応用数学科・教授 (32660)	