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 ２７ 日現在

機関番号：１２６０１
研究種目：若手研究
研究期間：2019～2023
課題番号：１９Ｋ２０２６７

研究課題名（和文）量子アルゴリズムを活用した耐量子公開鍵暗号の安全性解析

研究課題名（英文）Security Analysis of Post-quantum Public Key Cryptography by Utilizing Quantum Algorithms

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・准教授

研究者番号：００８０８０８２

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：本プロジェクトは耐量子計算機暗号の量子アルゴリズムを用いた安全性解析を主眼としたものであり、本テーマに関わる複数の成果を得た。
主たる成果として、扱える量子ビットが少ないときの符号暗号に対する量子アルゴリズムの高速化を行ない、査読付き国際会議ACISP 2023で発表した。これは本プロジェクトのテーマに合致し、かつ、国際的に評価される画期的な成果である。
他にも、量子アルゴリズムを活用した公開鍵暗号への攻撃や耐量子計算機暗号への攻撃に関する成果をあげ、これらは本プロジェクトの周辺分野として、主テーマを進めるにあたり重要な成果となった。

研究成果の学術的意義や社会的意義
耐量子計算機暗号は今後必須とされる暗号技術であり、世界的にその実用化に向けた研究が活発に行われており、来る量子時代に安全な情報社会を維持する社会的意義の大きな研究である。
学術的には、主結果である扱える量子ビット数が制限されたときの符号暗号への量子攻撃の高速化には大きな意義がある。量子コンピュータは物理的な実現が困難であるとされており、大きな量子ビットすうを扱うのは困難であると考えられており、このような状況で符号暗号の量子安全性解析を行なった初の研究である。
その他の成果に関しても、査読付き国際会議等での発表されている画期的なものである。

研究成果の概要（英文）：The main topic of this project is quantum security analysis of post-quantum crytographic algorithms. We obtain several results that relate to the topic.
The main result is the faster quantum information set decoding algorithm to break code-based cryptography when the number of qubits is bounded. This result was presented at the peer-reviewed international conference ACISP 2023. This is an impressive achievement that is consistent with the theme of this project and has been internationally recognized.
We have also achieved results on quantum attacks on public-key cryptographyand attacks on quantum computer cryptography, which are important results in advancing the main theme of this project as a peripheral field.

研究分野：暗号理論

キーワード：耐量子計算機暗号　量子アルゴリズム　符号暗号　格子暗号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景
現在広く実用的に用いられている公開鍵暗号方式である RSA 暗号や楕円曲線暗号の安全性は、それぞれ素因数分解問題や離散対数問題の困難性と関連がある。そして、これらの数論問題を多項式時間で解くアルゴリズムが未知であるという事実に基づき、既存の公開鍵暗号は安全であると考えられている。だが、1994 年に Shor は、これらの数論問題を多項式時間で解く量子アルゴリズムを提案した。
Shor の論文以降、量子計算機にも耐性を持つ耐量子計算機暗号方式の設計は、暗号研究の主たる動機の一つであった。さらに、量子計算機の構成や実装に関する研究の進展に伴い、耐量子計算機暗号方式の実用化は喫緊の課題となってきた。事実、アメリカ国家安全保障局(NSA)は、2015 年 8 月に耐量子計算機暗号への移行を表明し、さらに、米国標準技術研究所(NIST)は、耐量子計算機暗号の標準化計画を発表している（L. Chen et al., Report on post-quantum cryptography, NIST Interagency Report (NISTIR) 8105, 2016）。この標準化計画では、暗号方式・鍵交換方式・ディジタル署名方式を対象として 2017 年 11 月末を締め切りとした公募を行い、50 件を超える公募があった。さらに、3-5 年かけてその安全性・実装性能を評価する計画である。
これまで、格子問題・符号問題・多変数多項式問題・同種写像問題などの困難性に安全性の根拠を多く耐量子暗号が開発されてきた。これらの方式は、量子アルゴリズムでも解読できないように設計されているため、現在実用化されている方式より効率が悪い。さらに、その実装は、既存の古典計算機においても十分効率的でなければならない。それは、量子計算機が完成した直後には、他国の諜報機関・大規模な犯罪者グループなどが大金をかけて量子計算機を手にしたいても、一般に普及するまでにタイムラグがあることが予想されるからである。そのため、耐量子暗号の安全性・効率性を両立する最適なパラメータの導出は、実用化に向けて核となる研究である。
ただし、これまでのところ、真に量子計算機の存在を仮定したパラメータ解析は、精密には行われていない。具体的には、従来のパラメータ解析は、なるべく効率的な``古典"解読アルゴリズムの構成や、大規模実装に基づくその漸近的な挙動解析が主であり、量子アルゴリズムを活用した高速化としては、全探索を高速化する Grover 探索アルゴリズムを内部で``素朴に"用いているにすぎない。

２．研究の目的
本プロジェクトは、量子アルゴリズムを用いた耐量子計算機暗号の安全性解析を行うものである。本テーマは、耐量子計算機暗号の実用化のための必須のものであり、量子コンピュータ完成後の情報社会の安全性を維持するための社会的に意義があるテーマである。さらに、耐量子計算機暗号は現在の暗号理論研究の中心的研究対象であり、学術的にも大きな意味を持つ。

３．研究の方法
本研究は、基本的に指導する学生と連携することで進めていく。また、より画期的な成果を生むために他組織の研究者とも連携する。

４．研究成果
本研究のメインテーマとして、シンドローム復号問題を解く量子アルゴリズムで使用する量子ビット数を削減した。シンドローム復号問題は、符号暗号の安全性の根拠となる数学的問題であり、符号暗号はNISTの標準化候補の最終候補に入っている方式が複数あるなど注目されている耐量子計算機暗号である。そのため、シンドローム復号問題を効率的に解くアルゴリズムを構成することは大きな意義がある。耐量子性を考慮に、これまでシンドローム復号問題を解く様々な量子アルゴリズムが提案されてきたが、高速化のためには指数的に大きな量子ビット数が必要となっていた。量子コンピュータでは大きな量子ビット数を搭載するのは物理的に困難であろうと考えられているため、なるべく計算速度を落とさずに量子ビット数を削減することは重要な課題である。本研究では、既存のアルゴリズムより必ずしも速いわけではないが、量子ビット数が制限されているときには最も高速なアルゴリズムを提案した。本研究成果は査読付き国際会議ACISP 2023で発表済みである。
さらに、その他の成果について簡潔にまとめる。
量子攻撃者に対して安全な鍵付き完全準同型性暗号の構成を提案した。鍵付き完全準同型性暗号は、暗号文を復号することなく任意の計算が可能な完全準同型性を保つために安全なデータ

活用などの応用が期待される暗号技術であり、準同型演算に演算鍵が必要であることから従来の完全準同型性暗号では実現できなかった選択暗号文攻撃に対する安全性を保証することができる。鍵付き完全準同型性暗号は、これまで識別不可能性難読化と呼ばれる非常に非効率な暗号技術を用いた構成しか知られていなかったが、初めて識別不可能性難読化を用いない方式を構成した。本研究成果は査読付き国際会議 ACNS 2022 で発表済みである。
量子アルゴリズムを用いた離散対数計算アルゴリズムの改良を行なった。量子離散対数計算アルゴリズムは量子 GCD 逆元計算アルゴリズムと量子 FLT 逆元計算アルゴリズムのいずれかを用いる必要があり、前者はより量子ビットを削減することができ、後者はより計算を高速化することができる。本プロジェクトでは量子 FLT 逆元計算アルゴリズムの改良を行なった。まず、これまでの量子 FLT 逆元計算アルゴリズムの計算過程を加法連鎖の観点より見直し、より適切な加法連鎖を選ぶことで量子ビット数・計算時間をいずれも削減できることを示した。本研究成果は査読付き国際会議 CT-RSA 2023 で発表済みである。この成果では依然として量子 GCD 逆元計算アルゴリズムより圧倒的に多くの量子ビットが必要であったが、さらに追加の計算を行うことでほぼ同等の量子ビット数で逆元計算が可能である改良アルゴリズムを提案した。さらに、計算時間は依然として量子 GCD 逆元計算アルゴリズムより圧倒的に少ない。本研究成果は査読付き国際会議 ACNS 2024 で発表済みである。

５．主な発表論文等

〔雑誌論文〕　計6件（うち査読付論文　6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 Ren Taguchi and Atsushi Takayasu	４．巻 23
２．論文標題 Concrete quantum cryptanalysis of binary elliptic curves via addition chain	５．発行年 2024年
３．雑誌名 Quantum Information Processing	６．最初と最後の頁 122
掲載論文のDOI（デジタルオブジェクト識別子） 10.48550/ARXIV.QUANT-PH/9806084	査読の有無 有
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 －

１．著者名 Ren Taguchi and Atsushi Takayasu	４．巻 14584
２．論文標題 On the Untapped Potential of the Quantum FLT-based Inversion	５．発行年 2024年
３．雑誌名 Applied Cryptography and Network Security	６．最初と最後の頁 79-100
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-54773-7_4	査読の有無 有
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 －

１．著者名 Yen-Ting Kuo and Atsushi Takayasu	４．巻 14561
２．論文標題 A Lattice Attack on CRYSTALS-Kyber with Correlation Power Analysis	５．発行年 2024年
３．雑誌名 Information Security and Cryptology	６．最初と最後の頁 202-220
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-981-97-1235-9_11	査読の有無 有
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 －

１．著者名 Naoto Kimura, Atsushi Takayasu, and Tsuyoshi Takagi	４．巻 13915
２．論文標題 Memory-Efficient Quantum Information Set Decoding Algorithm	５．発行年 2023年
３．雑誌名 Information Security and Privacy	６．最初と最後の頁 452-468
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-35486-1_20	査読の有無 有
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 －

1．著者名 Ren Taguchi and Atsushi Takayasu	4．巻 13871
2．論文標題 Concrete Quantum Cryptanalysis of Binary Elliptic Curves via Addition Chain	5．発行年 2023年
3．雑誌名 Topics in Cryptology - CT-RSA 2023	6．最初と最後の頁 57-83
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-30872-7_3	査読の有無 有
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 －

1．著者名 Naoto Kimura, Atsushi Takayasu, and Tsuyoshi Takagi	4．巻 未発行
2．論文標題 Memory-Efficient Quantum Information Set Decoding Algorithm	5．発行年 2023年
3．雑誌名 ACISP 2023	6．最初と最後の頁 未発行
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
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15件（うち招待講演　2件／うち国際学会　4件）

1．発表者名 Ren Taguchi
2．発表標題 On the Untapped Potential of the Quantum FLT-based Inversion
3．学会等名 ACNS 2024（国際学会）
4．発表年 2024年

1．発表者名 Yen-Ting Kuo
2．発表標題 A Lattice Attack on CRYSTALS-Kyber with Correlation Power Analysis
3．学会等名 ICISC 2023（国際学会）
4．発表年 2023年

１．発表者名
Atsushi Takayasu

２．発表標題
Memory-Efficient Quantum Information Set Decoding Algorithm

３．学会等名
ACISP 2023（国際学会）

４．発表年
2023年

１．発表者名
Yen-Ting Kuo

２．発表標題
A Lattice Attack on CRYSTALS-Kyber with Correlation Power Analysis (from ICISC 2023)

３．学会等名
情報セキュリティ研究会（招待講演）

４．発表年
2024年

１．発表者名
瀬戸友暁

２．発表標題
UOV系署名に対する部分鍵導出攻撃

３．学会等名
情報セキュリティ研究会

４．発表年
2024年

１．発表者名
Yen-Ting Kuo

２．発表標題
Improved Lattice Analysis on Correlation Power Analysis of CRYSTALS-Kyber

３．学会等名
SCIS 2024

４．発表年
2024年

１．発表者名
田口廉

２．発表標題
量子FLT逆元計算アルゴリズムの深さ削減

３．学会等名
SCIS 2024

４．発表年
2024年

１．発表者名
西村佑介

２．発表標題
Module-LWE問題における格子の回転構造を利用した列挙法の計算量解析

３．学会等名
SCIS 2024

４．発表年
2024年

１．発表者名
櫻井徳吾

２．発表標題
Module-LWE問題に対する格子の回転構造を利用したBDD列挙法

３．学会等名
情報セキュリティ研究会

４．発表年
2023年

１．発表者名
田口廉

２．発表標題
Concrete Quantum Cryptanalysis of Binary Elliptic Curves via Addition Chain (from CT-RSA 2023)

３．学会等名
情報セキュリティ研究会（招待講演）

４．発表年
2023年

１．発表者名
田口廉

２．発表標題
量子FLT逆元計算アルゴリズムの改良

３．学会等名
2022年コンピュータセキュリティシンポジウム(CSS2022),

４．発表年
2023年

１．発表者名
田口廉

２．発表標題
バイナリECDLPに対するShorのアルゴリズムの量子ビット削減

３．学会等名
2023年暗号と情報セキュリティシンポジウム(SCIS 2023)

４．発表年
2023年

１．発表者名
枝村天真

２．発表標題
適応的シミュレーション安全なIDベース内積関数型暗号の構成

３．学会等名
2023年暗号と情報セキュリティシンポジウム(SCIS 2023)

４．発表年
2023年

１．発表者名
Shingo Sato, Keita Emura, Atsushi Takayasu

２．発表標題
Keyed-Fully Homomorphic Encryption without Indistinguishability Obfuscation

３．学会等名
20th International Conference on Applied Cryptography and Network Security (ACNS 2022)（国際学会）

４．発表年
2022年

１．発表者名 木村直人
２．発表標題 メモリ制限下における量子Information Set Decodingアルゴリズムの高速化
３．学会等名 情報セキュリティ研究会
４．発表年 2020年

〔図書〕　計0件

〔産業財産権〕

〔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

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