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　 ６ 月 ２１ 日現在

機関番号：３５３０２
研究種目：基盤研究(C)（一般）
研究期間：2020～2023
課題番号：２０Ｋ０３７４１

研究課題名（和文）最適化理論を用いた耐量子暗号の安全性解析と開発

研究課題名（英文）Security analysis and development of post-quantum cryptography using optimization theory

研究代表者
安田　貴徳（Yasuda, Takanori）

岡山理科大学・基盤教育センター・准教授

研究者番号：００４６４６０２

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：多変数公開鍵暗号の暗号方式の類似として格子ベース暗号の暗号方式を構成した。これは最適化理論を用いた構成法の応用である。また、多変数公開鍵暗号の署名方式 MQ-sign に対し、秘密鍵の脆弱性を発見し、それを利用した攻撃手法を提案した。それにより MQ-sign の一部は安全な使用が不可能となった。また、多変数多項式システムの線形変換による両側合成を利用した公開鍵暗号に対し、ある条件下で利用可能な攻撃手法と提案した。

研究成果の学術的意義や社会的意義
多変数公開鍵暗号では、様々な暗号方式や署名方式が提案されている。特に、UOVと呼ばれる署名方式は安全とされているが、その秘密鍵の鍵長削減などを行うと、必ずしも安全ではなくなくことを明らかにできた。また、これまであまり関連性がなかった多変数公開鍵暗号と格子ベース暗号であったが、どちらの特徴を持つ暗号方式を提案したことで、２つの中間の状態の公開鍵暗号が存在することを明らかにできた。

研究成果の概要（英文）：We constructed a lattice-based cryptosystem as an analogue of a multivariate public-key cryptosystem. This is an application of the construction method using optimization theory. We also found a vulnerability in the secret key of MQ-sign, a signature scheme for multivariate public-key cryptosystems, and proposed an attack method using it. This made it impossible to use some parts of MQ-sign securely. We also proposed an attack method that can be used under certain conditions against public-key cryptosystems based on two-sided composition by linear transformation of multivariate polynomial systems.

研究分野：暗号理論

キーワード：公開鍵暗号　耐量子暗号　多変数公開鍵暗号　最適化理論　格子ベース暗号

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

(1) 広く普及している暗号基盤技術（RSA 暗号と楕円曲線暗号）は、大規模な量子コンピュータが利用可能になると、多項式時間で解読可能であることが数学的に証明されている（ショアのアルゴリズム）。当時、量子アニーリングでは数千量子ビット、量子ゲートでは数十量子ビットの量子コンピュータが実現できており、まだ小規模ではあるものの、量子コンピュータ開発は着実に進展していた。

(2) 今後の量子コンピュータの大規模化に備えて、量子コンピュータに耐性を持つ暗号技術（耐量子暗号）を開発し、標準化しておく必要があった。米国標準技術研究所（NIST）は、2017 年に耐量子暗号の標準化候補の公募を行った。69 方式の暗号方式が投稿され、当時、26 方式まで絞り込まれていた。

(3) 耐量子暗号として候補に挙げられている公開鍵暗号の分類に、多変数公開鍵暗号、格子ベース暗号、符号ベース暗号、同種写像ベース暗号などがある。公開鍵暗号は、共通鍵暗号と並んで現代暗号の柱となっている基本技術であり、解読困難な数学問題を暗号安全性の根拠として利用する。すなわち、攻撃者が暗号を解読するには、対応する数学問題を解かなければならない。多変数公開鍵暗号では、MP 問題、MQ 問題といった数学問題が、格子ベース暗号では、SIS 問題、LWE 問題、最短ベクトル問題などが利用されている。

２．研究の目的

(1) 本研究の目的の１つ目は、最適化手法がもたらす耐量子暗号に対する脅威を定量的に評価することである。耐量子暗号に利用される数学問題は、最適化理論を用いた安全性解析が必要である。まず、どのような条件下で最適化理論の手法が暗号の脅威となるのかを明らかにしなければならない。そして、最適化理論を用いた攻撃の計算量を見積もる。

(2) 本研究の目的の２つ目は、最適化手法を耐量子暗号の効率的復号に応用する手法を開発することである。適化理論には様々な最適化テクニックがあり、良い処理効率や安定性を提供する最適化手法が他に存在する可能性がある。暗号の場合、解が常に整数値になるという特殊事情も考慮し、様々な最適化技術の実装と比較を行い、復号に適した最適化アルゴリズムを調査する。

３．研究の方法

(1) 耐量子暗号に現れる数学問題（SIS 問題、LWE 問題、最短ベクトル問題、MP 問題、MQ 問題など）に対し、最適化手法を用いた攻撃の計算量を見積もる。実験と理論の両面で評価する。また、この解析を下に、最適化攻撃に耐性を持つための数学問題の条件を記述する。

(2) 各暗号方式は、核となる数学問題に対する攻撃以外にも、方式固有の攻撃が存在する。最適化手法を用いた方式固有の攻撃の可能性を見極め、そのような攻撃が存在した場合、その計算量を評価する。128 ビット安全性レベルに対応する安全性パラメータなどを正確に見積もる。

(3) 申請者は最適化手法をトラップドアとする暗号方式を１つ提案しているが、効率性や鍵長の膨大さに課題がある。そのため、これらの課題を解決する新しい暗号方式や派生方式を開発する。

(4) 申請者は非線型方程式の求解手法として、いくつかの直線探索法を実装し、その中で Levenberg-Marquardt 法が最も効率的であることを既に示していた。しかし、信頼領域法や制約付き非線型方程式の求解手法などの実装と比較はまだ行っていない。最も効率的なアルゴリズムを実装と比較により特定する。

４．研究成果

(1) 多変数公開鍵暗号の暗号方式の格子ベース暗号への応用

申請者は pq 法と呼ばれる最適化理論と関わる数学問題を安全性の根拠とする多変量公開鍵暗号システムを提案していた。これは、既存の多変数公開鍵暗号方式からより安全な方式を構成する方法である。この安全性は MQ 問題と呼ばれる多変数多項式の数学問題に基づく。本課題では、その方式にノイズ要素を追加することで暗号システムを改良した。さらに多変数多項式部分を線形写像にすることで格子ベース暗号に応用し、3 つの暗号方式を提案した。そのうち１つは格子ベース暗号の暗号方式である NTRU を応用したものである。

(2) 特殊な Isomorophism of Polynomial 問題に対する安全性解析

多変数公開鍵暗号には、２つの線形変換の両側合成で移りあう多変数多項式システムに関する数学問題が存在する。その多変数多項式システムから２つの線形写像を見つける問題であり、こ

れを IP2S 問題と呼ぶ。これは公開鍵暗号の安全性の根拠として利用されている。2020 年に、Santoso が IP2S に由来する問題を提案した。この問題は BIPC 問題と呼ばれる。BIPC 問題は IP2S を線形化し、秘密の線形写像をサーキュラント行列で表現される線形写像に限定することで得られる。サーキュラント行列の積の可換性を利用して、BIPC 問題に基づく ElGamal のような暗号化方式が構成できる。本課題では、BIPC 問題の線形性を利用することで、ElGamal ライクな暗号化方式の等価鍵を見つける新しい攻撃を提案した。この攻撃は、多項式時間アルゴリズムであり、ElGamal-like 暗号方式の 128 ビット提案パラメータを標準的な PC で 10 時間以内で破ることができた。

(3) MQ-sign の解読

多変数公開鍵暗号の署名方式 UOV は安全性が高いと思われている。そのため、その変種の提案が非常に多い。多変数署名方式 MQ-Sign は、Shim らによって提案された UOV 署名方式の一種である。韓国の耐量子暗号標準化プロジェクト KpqC の耐量子標準化候補として提案されている。UOV は２つの線形変換を利用するが、その係数はランダムに選ばれる。一方、MQ-sign はその２つの線形変換を疎にするという選択も考えた。組み合わせとしては 4 種類である。（1 つはオリジナルの UOV を含む）本課題では、そのうち、１つの線形変換を疎にしたものは脆弱性を持つことを発見した。そのことを利用し実用的な鍵回復攻撃を提案した。

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3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 Wang Yuntao、Ikematsu Yasuhiko、Yasuda Takanori	４．巻 13600
２．論文標題 Lattice-Based Public Key Cryptosystems Invoking Linear Mapping Mask	５．発行年 2022年
３．雑誌名 Lecture Notes in Computer Science book series	６．最初と最後の頁 88～104
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-20917-8_7	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 Yasuhiko Ikematsu, Shuhei Nakamura, Bagus Santoso, Takanori Yasuda	４．巻 13007
２．論文標題 Security Analysis on an ElGamal-Like Multivariate Encryption Scheme Based on Isomorphism of Polynomials	５．発行年 2021年
３．雑誌名 Lecture Notes in Computer Science book series	６．最初と最後の頁 235-250
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-88323-2_12	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 Ikematsu Yasuhiko、Jo Hyungrok、Yasuda Takanori	４．巻 14402
２．論文標題 A Security Analysis on?MQ-Sign	５．発行年 2024年
３．雑誌名 Lecture Notes in Computer Science book series	６．最初と最後の頁 40～51
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-981-99-8024-6_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 －

〔学会発表〕　計7件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 安田 貴徳
２．発表標題 Construction of pairing using elliptic curves
３．学会等名 高度化する暗号技術と数学的技法の進展
４．発表年 2022年

１．発表者名
Bagus Santoso, Yasuhiko Ikematsu, Shuhei Nakamura, Takanori Yasuda

２．発表標題
MinRank Based Three-Pass Identification Scheme with Half Cheating Probability

３．学会等名
コンピュータセキュリティシンポジウム 2021（CSS2021）

４．発表年
2021年

１．発表者名
Yasuhiko Ikematsu, Shuhei Nakamura, Bagus Santoso, Takanori Yasuda

２．発表標題
New Post-Quantum Digital Signature Scheme based on MinRank Problem

３．学会等名
2022年暗号と情報セキュリティシンポジウム（SCIS2022）

４．発表年
2022年

１．発表者名
安田 貴徳，石井 将大，照屋 唯紀

２．発表標題
ペアリング高速計算に適した楕円曲線における群所属判定

３．学会等名
2022年暗号と情報セキュリティシンポジウム（SCIS2022）

４．発表年
2022年

１．発表者名
石井 将大，照屋 唯紀，安田 貴徳

２．発表標題
3次ツイストを利用した効率的なペアリングアルゴリズム

３．学会等名
コンピュータセキュリティシンポジウム 2020（CSS2020）

４．発表年
2020年

１．発表者名 Yasuhiko Ikematsu, Shuhei Nakamura, Bagus Santoso, Takanori Yasuda
２．発表標題 Security analysis on an El-Gamal-like multivariate encryption scheme based on a generalization of IP2S problem
３．学会等名 2021年暗号と情報セキュリティシンポジウム（SCIS2021）
４．発表年 2021年

１．発表者名 Yuntao Wang, Yasuhiko Ikematsu, Takanori Yasuda
２．発表標題 Public Key Cryptosystems Combining Lattice and Multivariate Polynomial
３．学会等名 2021年暗号と情報セキュリティシンポジウム（SCIS2021）
４．発表年 2021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