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 ２５ 日現在

機関番号：１２１０１
研究種目：若手研究
研究期間：2020～2023
課題番号：２０Ｋ１９８０２

研究課題名（和文）多変数多項式暗号に対する理論的安全性解析

研究課題名（英文）Theoretical security analysis for multivariate cryptography

研究代表者
中村　周平（Nakamura, Shuhei）

茨城大学・理工学研究科（工学野）・助教

研究者番号：００８２４０３８

交付決定額（研究期間全体）：（直接経費）　　2,600,000円

研究成果の概要（和文）：本研究課題は多変数多項式暗号を対象しており，特にその安全性解析を行うことを目的としている．研究成果として，研究開始時活発に研究されていた多変数多項式署名方式 Rainbowに対する二つの攻撃で，新しい解析結果を得ることができた．また，多変数多項式暗号の安全性解析では連立代数方程式問題の求解計算量見積もりを行う必要があるが，この評価手法に対しても新しい手法を提案することができた．

研究成果の学術的意義や社会的意義
公開鍵暗号はインターネット等で秘匿な情報を安全に通信するための技術で広く身近に利用されている．しかしながら，現在利用されている公開鍵暗号は，大規模な量子計算機が実現した場合に容易に解かれることが予想されている．このため，量子計算機を用いても解読困難な耐量子計算機暗号を設計することは重要な課題となっている．現在耐量子計算機暗号の標準化を目的としたの世界的なプロジェクトが米国標準技術研究所により進められており，Rainbow方式をはじめとした多変数多項式暗号が活発に研究されている．本研究課題はこの多変数多項式暗号の安全性解析を目的としている．

研究成果の概要（英文）：This research project targets multivariate cryptography, and aims to analyze its security. As a result of this research, we were able to obtain new results in the analysis of two attacks against Rainbow, a multivariate signature scheme that was being actively researched at the time the research began. In addition, in analyzing the security of multivariate cryptography, it is necessary to estimate the complexity required to solve a system of polynomial equations, and we were able to propose a new method for this estimation.

研究分野：暗号

キーワード：多変数多項式暗号　耐量子計算機暗号　連立代数方程式問題

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

(1) NIST(米国標準技術研究所)により耐量子計算機暗号標準化プロジェクトが開始され，第 1 ラウンドが終了し，署名方式の有力な候補として多変数多項式署名方式 Rainbow, GeMSS などが残っていた．また，それぞれは多変数多項式暗号では長く研究されてきた方式を基にしている．

(2) 暗号において連立代数方程式問題の求解計算量評価においては，問題が準正則性を持つことを仮定し，1 変数形式的冪級数を用いてアルゴリズムの求解次数を評価していた．

２．研究の目的

(1) NIST 主催の耐量子計算機暗号標準化プロジェクトにおいて有力として考えられた候補である多変数多項式署名方式 Rainbow, GeMSS などの安全性解析を行う．特にこれらの署名方式への既存の攻撃の見積もりがどれくらい正確なものであるかを再検討し，その攻撃の有効性について正確に把握することを目指す．

(2) 連立代数方程式問題に対する求解アルゴリズムの計算量をより正確に見積もる．より具体的に，多変数多項式署名方式に対する攻撃において，秘密鍵や署名の偽造を連立代数方程式問題に帰着して行う攻撃で得られる問題に対して，その求解計算量見積もりを行う．このような攻撃において連立代数方程式問題を解く計算量は支配的となるため，これは攻撃の効率性を見積もることを意味する．

３．研究の方法

(1) 具体的な暗号方式に対してその攻撃を実際に実装し，振る舞いをさまざまな指標から計測する．

(2) 暗号解析において計算量見積もりの際に仮定している連立代数方程式問題の性質と実際に暗号への攻撃から得られる問題との性質の比較を行う．

４．研究成果

(1) Rainbow は UOV の多層化された変種として 2005 年に提案された方式であり，研究開始当初の NIST 耐量子計算機標準化プロジェクト第 1 ラウンドまで致命的な攻撃は見つかっていない状況であった．UOV に適用可能な攻撃は Rainbow に対しても適用できるが，Rainbow に対する特有の攻撃として 2008 年に見つかった Rainbow-Band-Separation 攻撃と呼ばれるものが知られている． Rainbow-Band-Separation 攻撃の有効性は攻撃が帰着させる連立代数方程式問題の計算量評価に依存しており，Rainbow の第 2 ラウンド仕様書ではある 1 変数形式的冪級数を用いて評価されていた． 本研究課題では Rainbow-Band-Separation 攻撃の帰着する連立代数方程式問題を 2 変数形式的冪級数を用いて評価する新たな評価方法を見つけることができた． これにより，Rainbow-Band-Separation 攻撃は仕様書で想定されていた場合より効率的に働くことがわかり，第 2 ラウンドでの Rainbow のパラメータは NIST 安全性基準を満たしていないことがわかった．このことにより，Rainbow は第 3 ラウンドでのパラメータ変更を行うこととなった．

(2) Rainbow や HFE 方式の変種である GeMSS などへの攻撃では，直接的に連立代数方程式問題に帰着するような攻撃だけではなく， 一度 MinRank 問題を経由するような攻撃もいくつか知られている． このため， 多変数多項式暗号の安全性解析に関連して， MinRank 問題がどれくらい効率的に解かれるかを評価することは重要な課題の一つとなっている． MinRank 問題を解く手法の一つとして Kipnis-Shamir 手法と呼ばれるものが知られており，MinRank 問題を連立代数方程式問題に帰着することで解く手法である． Kipnis-Shamir 手法が帰着する連立代数方程式問題に対する既存評価は， 1 変数形式的冪級数を用いた手法を利用していたが， 本研究課題では一般に多変数形式的冪級数を用いた評価手法を新たに導入した．Kipnis-Shamir 手法は MinRank 問題で解く行列の列を選択して解くが， 選択する列の個数により得られる連立代数方程式問題の性質は異なる． 新たに導入した手法により， 最も効率的な列の選択個数に対しても知ることが可能となった． さらに本研究成果の応用として， Rainbow に対する MinRank 攻撃に新たな手法を適用して計算量評価も行なっている． 結果として， Rainbow に対するこの攻撃の有効性は既存より高いことがわかったが，NIST による安全性基準を下回るほどではないことがわかった．

(3) 上記の研究成果(1),(2)で得られた新しい連立代数方程式問題の評価手法は，具体的に解く多項式系が多重次数付け可能であることが影響している．通常の次数は非負整数に値を取るが，多重次数は非負整数を成分としたベクトルに値を取る次数である． 暗号分野における安全性評価のためには実際には多重次数付け可能であることがわかるだけでは十分ではなく， その多項式系の定義する多変数 Hilbert 級数が入力パラメータから形式的冪級数で近似できることが必

要である．本研究課題では，通常の次数付けで考えられる多項式系の準正則性の類似として多重次数付けに対する多項式系の多重準正則性の概念を導入することで，一般にランダム係数の多重次数付け可能な多項式系で定められる連立代数方程式問題の評価を可能にした．

５．主な発表論文等

〔雑誌論文〕　計7件（うち査読付論文　7件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 S. Nakamura, Y. Whang, Y. Ikematsu	４．巻 E106-A(3)
２．論文標題 A New Analysis of the Kipnis-Shamir Method Solving the MinRank Problem	５．発行年 2023年
３．雑誌名 IEICE Transactions	６．最初と最後の頁 203,211
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 －

１．著者名 B. Santoso , Y. Ikematsu , S. Nakamura, T. Yasuda	４．巻 -
２．論文標題 Three-Pass Identification Scheme Based on MinRank Problem with Half Cheating Probability	５．発行年 2023年
３．雑誌名 ISITA 2022	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） 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 －

１．著者名 Y. Ikematsu, S. Nakamura, T. Takagi	４．巻 -
２．論文標題 Recent Progress in the Security Evaluation of Multivariate Public-Key Cryptography	５．発行年 2023年
３．雑誌名 IET Information Security	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） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Shuhei Nakamura, Yasuhiko Ikematsu, Yacheng Wang, Jintai Ding, Tsuyoshi Takagi	４．巻 896
２．論文標題 New complexity estimation on the Rainbow-Band-Separation attack	５．発行年 2021年
３．雑誌名 Theoretical Computer Science	６．最初と最後の頁 1-18
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2021.09.043	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 and Shuhei Nakamura	４．巻 1412
２．論文標題 Security Analysis via Algebraic Attack Against "A New Encryption Scheme for Multivariate Quadratic System"	５．発行年 2021年
３．雑誌名 Proceedings of the Seventh International Conference on Mathematics and Computing	６．最初と最後の頁 9-21
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 －

１．著者名 Ikematsu Y., Nakamura S., Santoso B., Yasuda T.	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 Inscrypt 2021. Lecture Notes in Computer Science	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 Hiroki Furue, Shuhei Nakamura and Tsuyoshi Takagi	４．巻 12841
２．論文標題 Improving Thomae-Wolf Algorithm for Solving Underdetermined Multivariate Quadratic Polynomial Problem	５．発行年 2021年
３．雑誌名 PQCrypto 2021, Lecture Notes in Computer Science	６．最初と最後の頁 65-78
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-81293-5_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4件（うち招待講演　1件／うち国際学会　0件）

１．発表者名 中村周平，横溝恭平
２．発表標題 暗号における連立代数方程式問題を評価する新しい不変量の検討
３．学会等名 第41回数理科学講演会
４．発表年 2022年

１．発表者名
中村周平

２．発表標題
多変数多項式暗号における連立代数方程式の求解計算量評価

３．学会等名
総務省プロジェクト「5G等のための耐量子計算機暗号の機能付加技術等（耐量子　コンピュータセキュリティ技術）」招待講演（招待講演）

４．発表年
2021年

１．発表者名
Shuhei Nakamura

２．発表標題
New Complexity Estimation on the Rainbow-Band-Separation attack

３．学会等名
コンピュータセキュリティシンポジウム2020

４．発表年
2020年

１．発表者名
中村周平

２．発表標題
暗号分野における連立代数方程式問題の解析

３．学会等名
CRESTクリプトマス2023年度第2回全体会議

４．発表年
2023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