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　５ 年　 ６ 月 １２ 日現在

機関番号：２２６０４
研究種目：基盤研究(C)（一般）
研究期間：2019～2022
課題番号：１９Ｋ０３６４０

研究課題名（和文）代数的手法を用いたポスト量子暗号の安全性解析及び設計

研究課題名（英文）Security analysis and design of post-quantum cryptography using algebraic methods

研究代表者
内山　成憲（Uchiyama, Shigenori）

東京都立大学・理学研究科・教授

研究者番号：４０４３３１７２

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：耐量子計算機暗号の代表例である多変数公開鍵暗号の安全性解析及びパラメータ生成としてのいくつかの素数判定法について考察を行った。グレブナー基底計算アルゴリズムの基礎となるブッフバーガーアルゴリズムの高速化手法の一つであるF4の実用的な改良とその高速実装を与えた。多変数公開鍵暗号の安全性評価の国際的コンテストであるFukuoka MQ Challengeで公開されている問題でType II及びIIIに分類される問題に提案法を使用して、37変数の問題に挑戦し世界記録を更新した。また、2次フロベニウステストや強リュカテストと呼ばれる確率的素数判定アルゴリズムとミラー-ラビンテストについて比較を行った。

研究成果の学術的意義や社会的意義
現在広く利用されている公開鍵暗号方式は、素因数分解問題等の計算困難性に基づく。一方、これらの問題は量子計算機を用いて効率的に解かれてしまうことが知られている。実用的な量子計算機が実現し際に、社会に与える影響を軽減するため、現在、量子計算機を用いた攻撃に対して耐性を持つ暗号方式（耐量子計算機暗号、ポスト量子暗号）についての研究や標準化が進められている。本研究ではその代表例の一つである多変数公開鍵暗号の安全性について考察を与えた。これは実用的なパラメータサイズ評価に対する一つの指針を与えるものでもあり、理論的な観点のみならず実用的にも十分意義があると考えられる。

研究成果の概要（英文）：We discussed the security analysis for multivariate public-key cryptography, which is one of the representative examples of post quantum cryptography with resistance to quantum computers, and some prime number testing algorithms as parameter settings for post quantum cryptography. We proposed a practical improvement of F4, one of the practical speed-up methods of the Buchberger algorithm, which is the basis of the Groebner basis algorithm. We also succeeded in implementing the proposed method in the world record breaking 37-variable problem using the proposed method for problems classified as Type II and III in the Fukuoka MQ Challenge, an international contest for security evaluation of multivariable public-key cryptography. Also, we discussed the efficiency of some probabilistic prime number testing algorithms, such as the quadratic Frobenius test and the strong Lucas test, by comparing between these algorithms and the Miller-Rabin test.

研究分野：暗号理論

キーワード：暗号・認証等　アルゴリズム

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

現在世界中で広く利用されている公開鍵暗号方式の安全性根拠となる数学的問題は、素因数分解問題等の数論的問題であり、これらには量子計算機と呼ばれる近未来型の計算機を用いた効率的な解法の存在が知られている。つまり、実用的かつ大規模サイズの量子計算機が実現した暁には、現在利用されている公開鍵暗号方式は安全ではなくなってしまう。量子計算機の実現による社会への影響を軽減するため、現在、量子計算機を用いた攻撃に対して耐性を持つ暗号方式（耐量子計算機暗号、ポスト量子暗号）についての研究や標準化が進められている。実際、2015 年に米国国家安全保障局（NSA）はポスト量子暗号への移行を表明し、2016 年から米国標準技術研究所（NIST）はその標準化を進めている。現在、耐量子計算機暗号の候補とされているものとしては、符号理論、格子理論や楕円曲線同種写像に基づく方式及び多変数公開鍵暗号等が知られている。これらは、いずれも現在までのところ量子計算機を用いても効率的には解けないと考えられている。NIST の標準化の計画では現在広く使用されている方式の移行措置も考慮し 2030 年までを目安として標準方式を選定しようとしている。

２．研究の目的

本研究の目的は、１．で述べた耐量子計算機暗号のうち、落とし戸つき一方向性関数の候補となる種類も少ないがその中でも高速処理を特徴とした実用的な方式の一つである多変数公開鍵暗号に着目し、その安全性の根拠となる連立多変数代数方程式の求解問題の計算量的困難性について、理論および計算機実装の両面から解析を行うことである。安全性解析について具体的には、多変数連立代数方程式の解法で一般的に利用される汎用性の高いグレブナー基底計算アルゴリズムについて、多変数公開鍵暗号でよく用いられる 2 次の多変数連立代数方程式系に入力を絞り、その計算アルゴリズムの理論的解析及び最適化について考察することで、高速化を行うことである。この結果はポスト量子暗号の実用的なパラメータ生成と言う観点から見ると、現状の計算機を用いた場合でもどの程度のセキュリティパラメータのサイズを推奨すべきかの判断は重要であり、そのための一定の評価基準となり得ると考えられる。また、耐量子計算機暗号でも従来の数論ベースの公開鍵暗号と同様にパラメータ生成として素数を用いるものがあり、パラメータ生成手法としての素数判定法についての解析も行った。

３．研究の方法

グレブナー基底計算の基本となるアルゴリズムはブッフバーガーアルゴリズムと呼ばれるものである。このアルゴリズムの実用的な高速化手法についてはすでにいくつか提案されているが、ここではその中でも F4 と呼ばれるある種の並列計算を用いた手法やその亜種の一つである M4GB と呼ばれるアルゴリズムに着目し、その理論的な解析に基づく最適化を行い、それに基づく高速実装により提案手法の効果を確かめるものである。具体的には MQ Challenge と呼ばれる多変数公開鍵暗号の安全性評価を目的とする国際的なコンテストで与えられている問題に対して、どの程度の時間で解が求められるかを測ることでその性能を評価を行った。耐量子計算機暗号のパラメータ生成としていくつかの確率的素数判定法の実用的な観点からの性能評価を行った。

４．研究成果

主結果としては、グレブナー基底計算アルゴリズムの基礎となるブッフバーガーアルゴリズムの実用的な高速化手法の一つである F4 の実用的な改良を行い、その提案手法による高速実装に成功した。多変数公開鍵暗号の安全性評価に関する国際的なコンテストである Fukuoka MQ Challenge で公開されているいくつかの問題に対して挑戦し、その効果を確かめた。具体的には、Fukuoka MQ Challenge において、Type II 及び III に分類される 2 次多変数連立代数方程式に特化したアルゴリズムとプログラムを開発し、従来予測されていた計算時間よりも計算時間が約 5 倍速く、メモリ使用量を最良の場合では約 8 分の 1 に減少することに成功した。この改良は、まずいわば確率的な手法として、ブッフバーガーアルゴリズムの中心となる S 多項式と呼ばれる多項式の別の多項式での割り算回数を極力減らすため、数値実験等に基づき、多項式としての 0 になる場合には早めに止めるチェックを用いたこと。次に、単項式順序について通常は先頭項の順序に注目するがそれだけでなく次の 2 番目の順序の項等まで考慮する最適化を行ったこと。さらには実際の実装の際にどういう順番で多項式を選んでいくかについても最適化を行ったことにより。本手法を使用して、37 変数の問題に挑戦した。この 37 変数の問題を解くためには、MQ Challenge の資料を参考にすると、23 変数の問題を解く場合の約 15 万倍の時間がかかり、汎用ソフトを使用した場合は 4 年から 16 年はかかると考えられる。今回提案したアルゴリズムとプログラムを汎用サーバ（CPU: Intel Xenon CPU E5-4669 v4 (2.20GHz/22Core)×4、メモリ: 1TB）で使うことで、Type II の 37 変数については 75.7 日、Type III の 37 変数については 56.1 日で解くことに成功した。これらは当時の世界記録を与えるものである。これらの手法は F4 の亜種とも考えられる M4GB と呼ばれるアルゴリズムにも適用し、同様の高速化が可能となることが数値実験により確かめられた。ただし、サイズの大きなパラメータによる実装につ

いては出来ておらず今後の課題となる。また、パラメータ生成としての素数判定については、確率的なアルゴリズムとして知られるいくつかの手法についてその実用的な効果について考察を与えた。具体的には 2 次フロベニウステストや強リュカテストと呼ばれる確率的素数判定アルゴリズムに対して、代表的かつ実用的な素数判定法であるミラー-ラビンテストと比較を行った。つまり、合成数に対して基底と呼ばれるパラメータを小さな素数から順に選んでテストを行う際にどこまでパスするかについて調べた。2 次フロベニウステストについてはパラメータに条件を付けている制限付きではあるが先行研究として知られているものよりも少ない試行回数で判定が可能となることが示されたが、強リュカテストについては適用範囲の狭さもありミラー-ラビンテストとほぼ同様となった。

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　0件／うちオープンアクセス　3件）

１．著者名 Kurokawa Takashi、Ito Takuma、Shinohara Naoyuki、Yamamura Akihiro、Uchiyama Shigenori	４．巻 7
２．論文標題 Selection Strategy of F4-Style Algorithm to Solve MQ Problems Related to MPKC	５．発行年 2023年
３．雑誌名 Cryptography	６．最初と最後の頁 1-25
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/cryptography7010010	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 Ito Takuma、Yuuta Hoshi、Shinohara Naoyuki、Uchiyama Shigenori	４．巻 14
２．論文標題 Polynomial Selection of F4 for solving the MQ problem	５．発行年 2022年
３．雑誌名 JSIAM Letters	６．最初と最後の頁 135-138
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 Takuma Ito, Atsushi Nitta, Yuta Hoshi, Naoyuki Shinohara, Shigenori Uchiyama	４．巻 13
２．論文標題 Polynomial Selection for Computing Goroebner bases	５．発行年 2021年
３．雑誌名 JSIAM Letters	６．最初と最後の頁 72-75
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 ITO Takuma、SHINOHARA Naoyuki、UCHIYAMA Shigenori	４．巻 E104.A
２．論文標題 Solving the MQ Problem Using Gr?bner Basis Techniques	５．発行年 2021年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 135～142
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10件（うち招待講演　1件／うち国際学会　1件）

１．発表者名
小林耕太郎，伊藤琢真，篠原直之，内山成憲

２．発表標題
M4GBアルゴリズムを基にしたグレブナー基底計算について

３．学会等名
2022年日本応用数理学会連合発表会

４．発表年
2022年

１．発表者名
市川守，篠原直之，黒川貴司，内山成憲

２．発表標題
Lucas chainを用いた強Lucasテストとその判定効率について

３．学会等名
2022年日本応用数理学会連合発表会

４．発表年
2022年

１．発表者名
T. Ito, N. Shinohara, T. Kurokawa and S. Uchiyama

２．発表標題
Polynomial Selection to Compute an F4-style algorithm for MQ 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
Takuma Ito, Naoyuki Shinohara, Shigenori Uchiyama

２．発表標題
Polynomial Selections to Compute Grobner Basis for Security Evaluation of Multivariate Public Key Cryptosystems

３．学会等名
2021年暗号と情報セキュリティシンポジウム

４．発表年
2021年

１．発表者名
伊藤琢真，篠原直之，内山成憲

２．発表標題
F4-style アルゴリズムによるMQ問題の求解

３．学会等名
電子情報通信学会 情報セキュリティ研究会（ISEC）（招待講演）

４．発表年
2020年

１．発表者名
星雄大，伊藤琢真，篠原直之，内山成憲

２．発表標題
F4アルゴリズムにおける多項式選択について

３．学会等名
2021年日本応用数理学会連合発表会

４．発表年
2021年

１．発表者名
伊丹洸陽，篠原直之，内山成憲

２．発表標題
2次強Frobeniusテストとその判定効率について

３．学会等名
2021年日本応用数理学会連合発表会

４．発表年
2021年

１．発表者名
Takuma Ito, Naoyuki Shinohara, Shigenori Uchiyama

２．発表標題
An Efficient F4-style Based Algorithm to Solve MQ Problems

３．学会等名
14th International Workshop on Security, IWSEC 2019（国際学会）

４．発表年
2019年

１．発表者名 稲生裕太，伊藤琢真，篠原直之，内山成憲
２．発表標題 MQ問題に対するM4GBアルゴリズムの多項式選択について
３．学会等名 日本応用数理学会第19回研究部会連合発表会
４．発表年 2023年

１．発表者名 伊藤琢真，篠原直之，黒川貴司，内山成憲
２．発表標題 空間計算量を考慮したM4GBアルゴリズム
３．学会等名 2023年暗号と情報セキュリティシンポジウム
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