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　 ９ 月 １１ 日現在

機関番号：３３９１９
研究種目：若手研究
研究期間：2019～2023
課題番号：１９Ｋ２０２７０

研究課題名（和文）耐量子計算機暗号の多項式数理における安全性評価手法の確立

研究課題名（英文）Mathematical properties of multivariate polynomial cryptosystems and their application to security analysis

研究代表者

伯田　恵輔（Hakuta, Keisuke）

名城大学・理工学部・准教授

研究者番号：９０５８７０９９

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）：従来の公開鍵暗号は量子計算機によって多項式時間で解読可能であることが知られており、量子計算機に耐性を持つ暗号技術（耐量子計算機暗号）は国内外を問わず学術・産業界において実用化に向けた研究開発が活発に行われている。耐量子計算機暗号の一つとして多変数多項式暗号があり、格子暗号など他の方式と比べて処理性能が高速であることが特徴である。ところが多変数多項式暗号の安全性評価は多岐にわたる。本研究では、多変数多項式暗号で利用される多項式同型群およびその部分群についての数学的性質を明らかにし、本性質を、多変数多項式暗号の解読困難性の根拠である数学計算問題の安全性評価に適用するための理論的方法を考察した。

研究成果の学術的意義や社会的意義
従来の公開鍵暗号は量子計算機によって多項式時間で解読可能であることが知られており、現在、量子計算機に耐性を持つ暗号技術（耐量子計算機暗号）の標準化が進められている。上記の標準化活動における安全性評価のみならず、ウェブブラウザのセキュアプロトコルであるSSL/TLSなどインフラとして利用されている暗号技術の高安全化に貢献できる可能性があるため、本研究成果は、学術的意義だけでなく、社会的意義も高いと考えられる。

研究成果の概要（英文）：The multivariate polynomial cryptosystems have emerged as one of the candidates of post-quantum cryptography. Most of the multivariate polynomial cryptosystems make use of the fact that solving a random multivariate polynomial system over a finite field is an NP-complete problem. However, multivariate polynomials with special properties are used to construct public key encryption schemes and digital signature schemes. For this reason, we need a detailed understanding of mathematical properties of multivariate polynomial cryptosystems. In this research, we showed some mathematical properties of subgroups of the polynomial automorphism groups over finite fields.

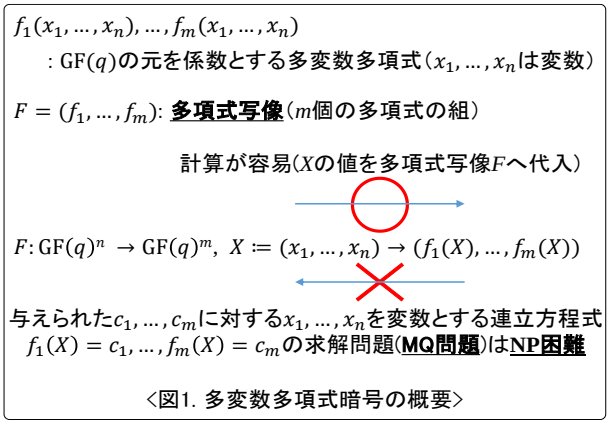
研究分野：計算代数幾何学

キーワード：アフィン代数幾何学　多変数多項式暗号　耐量子計算機暗号　有限体　置換群

１．研究開始当初の背景

（１）RSA 暗号や楕円曲線暗号など従来の公開鍵暗号は、量子計算機によって多項式時間で解読可能となることが Peter Shor 氏に示されていた（1994 年）。そのため、量子計算機に耐性を持つ暗号・署名方式（耐量子計算機暗号）は学術界・産業界において実用化に向けた研究開発が活発に行われている。

（２）耐量子計算機暗号の一つに多変数多項式暗号があり、格子暗号など他の方式と比べて処理性能が高速であることが特徴である。要素数が q の有限体を GF(q)と表す。多項式写像 F とは有限体 GF(q)上の線形空間 $GF(q)^n$ から線形空間 $GF(q)^m$ への多項式の組 $F = (f_1,\cdots,f_m)$で表される写像であり、各 f_i は 2 次の多項式を利用する。$GF(q)^n$ の元を多項式写像 F に代入する計算は容易である。多変数多項式暗号の安全性は、多変数多項式の求解問題（MQ 問題）の困難性を安全性の根拠にしている。



<図1. 多変数多項式暗号の概要>

（３）多変数多項式暗号の安全性評価の研究は、これまで MQ 問題を直接計算する攻撃手法（グレブナ基底攻撃、XL 攻撃など）に主眼が置かれていた。一方、暗号学的には鍵復元攻撃のほうがより強い攻撃であり、鍵復元攻撃に対する安全性評価も不可欠である。多変数多項式暗号の構成要素として多項式同型写像（多項式写像であって、その逆写像も多項式写像であるもの）が利用されている。また、いくつかの多項式同型写像の組を秘密鍵とし、その合成写像を公開鍵としている多変数多項式の暗号・署名方式も提案されている。これらの方式では、与えられた公開鍵 F から合成前の多項式同型写像を直接計算する数学計算問題（TDP と呼ぶ）が困難でなければならない。鍵復元攻撃についても多くの結果が報告されているが、従来の攻撃手法は特定方式にのみ適用可能な手法であり、汎用的な鍵復元攻撃手法とその安全性評価指標は確立されていないという課題があった。

２．研究の目的

上述した TDP に対する汎用的な鍵復元攻撃手法としてアフィン代数幾何学に基づく Tame 分解理論が知られている。本研究の目的は、Tame 分解理論を用いた多変数多項式暗号の汎用的な鍵復元攻撃手法とその安全性評価指標を確立することである。Tame 分解とはアフィン代数幾何と呼ばれる数学理論に基づく新たな攻撃手法であり、従来の鍵復元攻撃とは異なるため、学術的に新しい研究課題として Tame 分解理論を考察する必要がある。

３．研究の方法

（１）標数 2 の有限体上定義されたアフィン自己同型群および一つの非線形な基本自己同型で生成される多項式同型群の部分群（Derksen 群）が順部分群と一致しないこと（Derksen の定理が成立しないこと）の証明に取り組む。

（２）標数 2 の素体上定義された translation automorphism によって生成される正規部分群が特殊線形群を含む特殊多項式同型群の最小の正規部分群と一致するかどうかを考察する。

（３）上記（１）の類似問題として、標数 2 の素体上定義された弱 Derksen 群によって誘導される置換群と順部分群によって誘導される置換群が一致するという弱 Derksen の定理が知られている。この定理の証明は長く、非常にテクニカルで複雑なものである。そこで、この定理の別証明を考察する。

（４）標数 2 の有限体上の多項式同型群から誘導される置換群と標数 2 の有限体上の順部分群から誘導される置換群の間に存在する具体的な部分群を考察する。

４．研究成果

（１）〔学会発表〕④では、標数 2 の有限体上定義されたアフィン自己同型群および一つの非線形な基本自己同型で生成される多項式同型群の部分群（Derksen 群）が順部分群と一致しないこと（Derksen の定理が成立しないこと）を証明した。本研究成果を学術論文としてまとめ、〔雑誌論文〕③として発表した。

（２）〔学会発表〕③では、標数 2 の素体上定義された translation automorphism によって生成される正規部分群が特殊線形群を含む特殊多項式同型群の最小の正規部分群と一致するかどう

かを考察し、2 次元の場合に両者は一致しないこと、および 3 次元以上の場合には両者は一致することを証明した。なお、本成果を学術論文としてまとめ、学術雑誌に投稿した。
（３）〔学会発表〕②では、標数 2 の素体上定義された弱 Derksen 群によって誘導される置換群と順部分群によって誘導される置換群が一致するという弱 Derksen の定理の別証明を与えた。なお、本成果を学術論文としてまとめ、学術雑誌に投稿した。
（４）〔学会発表〕①では、標数 2 の有限体上の多項式同型群から誘導される置換群と標数 2 の有限体上の順部分群から誘導される置換群の間に存在する部分群を発見した。本研究成果は、この研究分野において長年の未解決問題である Maubach Conjecture にアプローチする際に有効と考えられる。なお、本成果を学術論文としてまとめ、学術雑誌に投稿した。
（５）また、上記研究成果（１）～（４）に関する研究の副次的な結果として〔雑誌論文②〕の成果も得た。

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　1件）

１．著者名 Kano Hiroyuki、Hakuta Keisuke	４．巻 4
２．論文標題 Efficiency improvement techniques for private intersection-sum protocol using Bloom filter	５．発行年 2022年
３．雑誌名 SN Applied Sciences	６．最初と最後の頁 1-15
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s42452-021-04910-z	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 Hakuta Keisuke	４．巻 46
２．論文標題 Permutation Groups Induced by Derksen Groups in Characteristic Two	５．発行年 2020年
３．雑誌名 Acta Mathematica Vietnamica	６．最初と最後の頁 123～132
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s40306-020-00391-1	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 Hakuta Keisuke	４．巻 26
２．論文標題 Semilinear groups contained in alternating group on a finite-dimensional linear space	５．発行年 2023年
３．雑誌名 Journal of Discrete Mathematical Sciences and Cryptography	６．最初と最後の頁 1051～1062
掲載論文のDOI（デジタルオブジェクト識別子） 10.1080/09720529.2021.1974649	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　0件／うち国際学会　0件）

１．発表者名 伯田恵輔
２．発表標題 標数2の素体における弱Derksenの定理の別証明
３．学会等名 SCIS2023
４．発表年 2023年

１．発表者名
伯田恵輔

２．発表標題
translation automorphismによって生成される正規部分群の性質

３．学会等名
SCIS2021

４．発表年
2021年

１．発表者名
伯田恵輔

２．発表標題
標数2のDerksen群に関連する置換群の性質

３．学会等名
SCIS2020

４．発表年
2020年

１．発表者名
伯田恵輔

２．発表標題
有限体上の多項式同型群の部分群に関連する置換群の性質

３．学会等名
SCIS2024

４．発表年
2024年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

researchmap
https://researchmap.jp/hakuta

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