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　元 年　 ６ 月 １３ 日現在

機関番号：１５２０１
研究種目：若手研究(B)
研究期間：2016～2018
課題番号：１６Ｋ１６０６６

研究課題名（和文）耐量子計算機暗号の多項式数理

研究課題名（英文）Mathematical Properties of Multivariate Polynomial Cryptosystems

研究代表者
伯田　恵輔（Hakuta, Keisuke）

島根大学・学術研究院理工学系・助教

研究者番号：９０５８７０９９

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）：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。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は、安全性評価が不十分な状況にある。本研究では、多変数多項式暗号に関するいくつかの数学的性質を証明し、さらに、これらの性質を利用して、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に関する理論的な性質を明らかにした。

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 multivariate polynomial cryptosystems. In addition, we proved relations between computational problems within the multivariate polynomial cryptosystems (so-called the Tame automorphism Decomposition Problem, TDP for short). These results may be able to provide a better understanding of the security of the multivariate polynomial cryptosystems.

研究分野：暗号理論，応用数学，情報セキュリティ

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

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

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る。要素数が q の有限体を GF(q)と書く。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。

（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、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が、その困難性を評価するための手法が明らかに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 Tame 分解問題は数学のアフィン代数幾何学と密接な関わりがある。本研究の目的は、アフィン代数幾何学の分野の知見を積極的に取り入れつつ、上述した TDP の困難性を評価するための基礎理論を構築することである。

３．研究の方法

（１）有限体上定義されたアフィン自己同型、基本自己同型など多変数多項式暗号で利用されている多項式同型写像に対し、その線形空間上の置換としての符号を求める一般公式を導出する。また、変数の個数が少ない場合の多項式同型写像写像に対し、その Tame 分解を具体的に計算し、置換としての符号を明らかにする。

（２）座標の各成分に p 乗 Frobenius 写像を施す多項式写像を考察し、上記多項式写像に対し、その線形空間上の置換の符号を求める一般公式を導出する。また、順多項式同型写像に対し、上記で述べた座標の各成分に Frobenius 写像を施した多項式写像を合成することによる多変数多項式暗号の安全性強化手法が知られているが、上記の安全性強化手法に対する安全性を再考し、暗号学的に妥当と考えられる条件下において、上記手法の安全性が実際に強化されるための必要条件を導く。

（３）有限次 Galois 拡大 K/k（拡大次数 m）に対し、K 上の n 変数多項式同型を、k 上の mn 変数多項式同型に変形することで、与えられた K 上の tame automorphism に対し、K 上のアフィン自己同型と基本自己同型の合成の形に分解する数学計算問題である Tame automorphism Decomposition Problem（TDP）と k 上の TDP の間の関係を明らかにする。

（４）TDP を解く素朴なアルゴリズムのメモリ使用量は膨大になることが予想される。そのため、上記のメモリ使用量を抑えるには、アフィン代数幾何学の結果として知られている Derksen の定理が有限体の場合にも成立することが望ましい。そのため、有限体の場合に Derksen の定理が成り立つか否かの初期検討を行う。

４．研究成果

（１）〔雑誌論文〕③では、有限体上定義されたアフィン自己同型、基本自己同型など多変数多項式暗号で利用されている多項式同型写像に対し、置換としての符号を求める一般公式を導出した。これにより、有限体上のアフィン自己同型や基本自己同型の置換としての符号は以下になることを明らかにした。

表 1. 有限体上定義された多項式同型写像の置換としての符号

有限体$\mathbb{F}_q$の種別	置換としての偶奇性			
	基本自己同型写像	アフィン自己同型写像	strictly triangular automorphism	順自己同型写像
標数2, 素体	偶/奇	偶	偶	偶/奇
標数2, 拡大体	偶	偶	偶	偶
奇標数	偶	偶/奇	偶	偶/奇

基本自己同型に依存

アフィン自己同型に依存

多変数多項式暗号で利用

また、〔雑誌論文〕①、②では、アフィン代数幾何学で有名な Nagata 自己同型、Anick 自己同型、及び Nagata-Anick 自己同型は、有限体上の線形空間としての符号を具体的に計算し、いずれの写像も、有限体が標数 2 の素体の場合には奇置換となり、その他の場合には偶置換となることを明らかにした。
（２）〔学会発表〕④では、座標の各成分に p 乗 Frobenius 写像を施す有限体上の多項式写像の置換としての符号を計算し、特殊な状況では奇置換となるが、その他の場合には偶置換となることを明らかにした。また、Frobenius 写像を施した多項式写像を合成することによる多変数多項式暗号の安全性強化手法が知られているが、上記の安全性強化手法に対する安全性を再考し、ある一つの暗号学的に妥当と考えられる仮定のもとで、上記手法の安全性が実際に強化されるための必要条件を導いた。また、上記仮定を含む 2 つの仮定のもとで、上記手法の安全性が実際に強化されていることを証明した。
（３）有限次 Galois 拡大 K/k（拡大次数 m）に対し、K 上の n 変数多項式同型を、k 上の mn 変数多項式同型に変形することで、与えられた K 上の tame automorphism に対し、K 上の TDP を、k 上の TDP に変換可能であることを証明した。また、上記の系として、一般の有限体 K における TDP が、その素体上の TDP に変換可能であることを明らかにした。これにより、素体上の TDP の計算困難性のみを評価すればよいことが明らかになった。
（４）TDP を解く素朴なアルゴリズムのメモリ使用量は膨大になることが予想される。そのため、上記のメモリ使用量を抑えるには、アフィン代数幾何学の結果として知られている Derksen の定理が有限体の場合にも成立することが望ましい。〔雑誌論文〕④では、標数 2 の素体の場合において、Derksen の定理が成立しないことを証明した。

５．主な発表論文等

〔雑誌論文〕（計４件）

① Keisuke Hakuta, Generalization of a counterexample to Derksen's theorem in characteristic two, Beiträge zur Algebra und Geometrie / Contributions to Algebra and Geometry, 査読有, in press
DOI: 10.1007/s13366-019-00436-z
② Keisuke Hakuta, On permutations induced by tame automorphisms over finite fields, Acta Mathematica Vietnamica, 査読有, Vol.43, No.2, 2018, pp.309-324
DOI: 10.1007/s40306-017-0217-0
③ Keisuke Hakuta and Tsuyoshi Takagi, Sign of permutations induced by Nagata automorphisms over finite fields, Journal of Mathematics Research, 査読有, Vol.9, No.5, 2017, pp.54-60
DOI: 10.5539/jmr.v9n5p54
④ Keisuke Hakuta, Sign of permutations induced by Anick and Nagata-Anick automorphisms over finite fields, Journal of Mathematics Research, 査読有, Vol.9, No.4, 2017, pp.23-29
DOI: 10.5539/jmr.v9n4p23

〔学会発表〕（計６件）

① 伯田 恵輔, 標数 2 の素体上定義された Derksen 群の性質, 2019 年暗号と情報セキュリティシンポジウム（SCIS2019）, 大津市, 2019 年 1 月.
② 伯田 恵輔, Tame Automorphism Decomposition Problem に関する一考察, コンピュータセキュリティシンポジウム 2018（CSS2018）, 長野市, 2018 年 10 月.
③ 伯田 恵輔, Tame Transformation Method の安全性強化手法に対する安全性再考, コンピュータセキュリティシンポジウム 2017（CSS2017）, 山形市, 2017 年 10 月.
④ 伯田 恵輔, アフィン代数幾何に基づく多変数多項式暗号, 代数幾何学と暗号数理の展開, 福岡市, 2017 年 2 月.
⑤ 伯田 恵輔, 有限体上の tame automorphism の置換としての符号, 2017 年暗号と情報セキュリティシンポジウム（SCIS2017）, 那覇市, 2017 年 1 月.
⑥ 伯田 恵輔, 有限体上の Anick automorphism の置換としての符号, コンピュータセキュリティシンポジウム 2016（CSS2016）, 秋田市, 2016 年 10 月.

〔図書〕（計０件）

〔産業財産権〕
○出願状況（計０件）

○取得状況（計０件）

〔その他〕
ホームページ等
https://www.staffsearch.shimane-u.ac.jp/kenkyu/search/f9744d5cdf8b80135d91ac82c2

5fb108/detail?page=research

６．研究組織

(1)研究分担者　なし

(2)研究協力者
研究協力者氏名：高木 剛
ローマ字氏名：(TAKAGI, Tsuyoshi)

海外研究協力者氏名：丁 津秦
ローマ字氏名：(DING, Jintai)