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　４ 年　 ５ 月 ３１ 日現在

機関番号：１７１０２
研究種目：基盤研究(B)（一般）
研究期間：2019～2021
課題番号：１９Ｈ０１８０４

研究課題名（和文）高機能な秘密計算暗号に向けた「弱い代数系」の組合せ論的群論に基づく研究

研究課題名（英文）Combinatorial group-theoretic study on "weak algebras" for advanced cryptosystems and secure computation

研究代表者

縫田　光司（Nuida, Koji）

九州大学・マス・フォア・インダストリ研究所・教授

研究者番号：２０４３５７６２

交付決定額（研究期間全体）：（直接経費）　　13,300,000円

研究成果の概要（和文）：完全準同型暗号とは、データを暗号化したままであらゆる演算を行うことのできる特殊な暗号化技術である。従来の完全準同型暗号のすべてに共通する複雑で非効率的な「ブートストラップ」と呼ばれる操作について、それを排した新しい完全準同型暗号の構成の枠組みを研究代表者が考案していたが、その構成に用いられる適切な性質を備えた数学的対象を具体的に特定できていなかった。本研究では、上記の具体的構成に必要となる適切な数学的対象の特定に向けて、前述の新たな構成の枠組みをより深く分析するとともに、関連する数学理論の整備を行った。

研究成果の学術的意義や社会的意義
完全準同型暗号とは、データを暗号化したままであらゆる演算を行うことのできる特殊な暗号化技術であり、企業秘密情報や個人のプライバシー情報を適切に秘匿したままでデータ利活用を行うプライバシー保護データ解析技術の主要な構成要素技術として期待されている。本研究は、この完全準同型暗号の既存の構成法に共通する複雑な操作を除去して効率性を大きく高めることを目標としており、プライバシー保護データ解析技術の効率化への貢献が期待されるとともに、本研究の過程で整備した種々の数学理論それ自体も学術的に意義深いものと考える。

研究成果の概要（英文）：Fully homomorphic encryption (FHE) is a special kind of encryption schemes that enable us to perform arbitrary operations on encrypted data. The existing FHE schemes commonly used some complicated and inefficient operation called "bootstrapping". In order to remove it, the principal researcher in this research has developed a new framework for constructing FHE schemes, but concrete construction of the suitable mathematical object realizing the framework was not achieved. In this research, towards concrete construction of the aforementioned suitable mathematical object, we analized the framework mentioned above more closely, and studied the related mathematical theory.

研究分野：暗号理論、組合せ論的群論

キーワード：完全準同型暗号　組合せ論的群論　宇宙際Teichmuller理論

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

完全準同型暗号とは、データを暗号化したままの状態であらゆる演算を行うことのできる特殊な暗号化技術である。この機能により、企業の秘密情報や個人のプライバシー情報といった機微情報を秘匿したままでデータ利活用を行う「プライバシー保護データ解析」の分野において、完全準同型暗号は主要な要素技術として高く期待されている。しかしながら、既存の完全準同型暗号の具体的構成法に共通する問題点として、「ブートストラップ」と呼ばれる複雑な操作を行う必要があり、そのために暗号化方式の効率が悪化してしまう。この問題点の解消に向けて、本研究代表者は、過去の研究において、このブートストラップ操作を必要としない新たな完全準同型暗号の構成原理を考案している。しかし、そうした新たな完全準同型暗号を安全かつ効率的に構成するうえで適した性質を備えた具体的な有限群を特定することには成功していなかった。

２．研究の目的

本研究の最終的な目的は、上記項目で述べた新たな完全準同型暗号の構成原理の具体化に必要となる適切な有限群（もしくはそれに類する何らかの数学的対象）を特定することである。その実現に向けて、暗号理論の立場からの研究を行うとともに、関連する数学理論の整備を行うことも本研究の目的である。

３．研究の方法

本研究では、主に以下の要領で研究を実施した。

(1) まず、上記構成原理（以下「当該構成原理」と記載）の具体化に必要な有限群を探しやすくするために、当該構成原理を整理し直し、その改良を試みた。また、当該構成原理を有限群以外の代数系に拡張することを考え、その可能性の検討を行った。

(2) 当該構成原理を実現するための有限群の構成に関する研究を行った。

(3) 当該構成原理の拡張の可能性として、有限ではない群に着目し、関連する数学理論の整備を行った。

(4) 当該構成原理の拡張の可能性として、群の公理系における条件の一部を緩和した代数系（以下「弱い代数系」と記載）に着目し、関連する数学理論の整備を行った。

４．研究成果

上記項目の(1)～(4)のそれぞれについて下記の成果を得た。またそれ以外にも、本研究に関連する群論など数学的理論の整備や、本研究成果の応用に向けた暗号理論およびアルゴリズム理論の研究も行った。

(1) 当該構成原理の整理と拡張可能性の検討

本項目では、まず、当該構成原理の性質とその実現可能性について過去の研究で得た知見の整理を行った。特に、当該構成原理に適した有限群の探索における失敗例の分析を行い、どのような数学的な性質が原因で成功しなかったのかについて考察を行った。具体的には、過去の研究において当該構成原理への適用を試した有限群の候補は、行列のなす群を用いて構成されたものであったが、そうした構成法では行列のなす群が自然に埋め込まれている行列のなす環を考えることで、得られる完全準同型暗号に対して線型代数の手法を用いた攻撃が可能となってしまう。そのため、そうした「線型代数的」でない構成が必要となるが、例えば（本研究代表者が専門としている）Coxeter 群のうち有限 Coxeter 群の範囲から「線型代数的」でない候補を探すのでは安全な構成が不可能であることを示した。こうした整理と考察の内容について国際ワークショップ MQC 2019 で招待講演を行い、予稿集にまとめた。
次に、当該構成原理の改良に関する研究を行った。具体的には、当該構成原理は、まずビットに対する種々の演算（AND, OR, NOT, XOR など）をある有限群 G に「埋め込み」、その群 G の元を「準同型暗号化」する、という 2 段階からなっている。ここで、例えばビット演算 AND を群 G に埋め込む、とは、ビット 0 と 1 に対応した G の異なる元σ_0 とσ_1、および G の元と G 上の群演算のみを用いて定義された関数（以降では「G-群関数」と呼ぶ）ｆ : G^2 → G で、AND 演算と整合的なもの、すなわち条件

ビット a と b について、f(σ_a,σ_b) = σ_{a AND b}

を満たすものを構成すること、と定義する（他の種類のビット演算についても同様である）。このような埋め込みを構成するには、G の位数 3 の元σおよび G-群関数 g : G → G で、条件

g(1) = 1 かつ g(σ) = g(σ^2) = σ

を満たすものを構成できれば充分であることがわかっている。過去の研究では、G を 5 次の対称群 S_5 として、上記の条件を満たす関数 g を機械的な探索によって構成していた。この点について、群 G をより小さな群に置き換えることができれば後の「群 G の元の準同型暗号化」がしやすいと期待され、また、同じ群 G であっても関数 g の構成がより簡潔であることが実用上望ましい。以上の考察を基に、上記の条件を満たす関数 g の構成可能性について系統的な研究を行い、G を 5 次交代群 A_5 とした場合に最小の表示を持つ関数 g の構成を与え、また 5 次交代群を同じまたはそれ以下の位数の群に取り替えるとそうした関数 g は存在しないことを示した。言い換えると、上記の条件を満たす関数 g の「最小の構成」を特定した。この成果は査読付国際論文誌に論文投稿中である。

(2) 当該構成原理の実現に向けた有限群の研究

本項目では、当該構成原理に適した有限群の探索を行った。特に、上述の「線型代数的」でない構成法の候補として、組合せ論的群論で取り扱うような生成元と基本関係による群の表示に基づく構成の可能性を考察し、自明な群の非自明な表示を用いて最終的に構成する群の表示を難読化するというアイデアを着想した。なお、このアイデアを具体的に実現するためには、難読化された群の表示に基づいて群演算を効率的に計算する手法が必要となるが、この点については今後研究を続ける予定である。

(3) 当該構成原理の実現に向けた無限群の研究および関連する数学理論の整備

上述のように当該構成原理に適した有限群の構成はまだ実現できていないことから、当該構成原理を有限群以外の代数系に拡張する可能性についても検討した。その可能性の一つとして無限群の利用が考えられる。上述のように有限群の場合には Coxeter 群の範囲では良い構成が不可能であるが、無限 Coxeter 群に範囲を広げれば適切な構成の可能性が残っている。本研究ではこのような観点から、無限 Coxeter 群の性質についての基礎研究を行い、特に、無限 Coxeter 群がどれだけ多様な群表示をもつか、という点についての研究を行い、査読付国際論文誌にて研究成果の論文発表を行った。

(4) 当該構成原理の実現に向けた「弱い代数系」および関連する数学理論の整備

前項目とは異なる拡張の可能性として、群よりも「弱い代数系」への当該構成原理の拡張が考えられる。この「弱い代数系」の候補としては、群の公理から結合法則を除いた loop や、さらに単位元の存在を除いた quasigroup などが考えられる。本研究ではこうした loop や quasigroup の性質について調査を行った。その結果として、群の組合せ群論的表示で用いられる自由群の、loop や quasigroup における類似物の性質を調べることで、組合せ論的群論の手法を「弱い代数系」に拡張する、という構想を得た。これについては今後研究を続ける予定である。
また、群に比べると「弱い代数系」の研究は全般的に不足していると考えられるが、本研究分担者の専門である宇宙際 Teichmuller 理論の「豊富な構造を忘れてより原始的な構造に移る」という視点がそうした「弱い代数系」の研究にも有益であると考え、宇宙際 Teichmuller 理論の研究も行った。具体的には、

(A)虚数乗法をもつ楕円曲線に対する宇宙際 Teichmuller 理論の拡張とその応用、
(B)楕円曲線のモジュライにおける無限遠点での宇宙際 Teichmuller 理論と見なすことのできる発展的理論、

の研究を望月新一氏と行った。
(A)については、虚数乗法をもつ楕円曲線に対しては(a)楕円曲線から生じる Galois 表現の像が小さくなる、(b)(古典的宇宙際 Teichmuller 理論において中心的役割を果たすテータ値を生む)悪還元をもつ有限素点が存在しなくなる、という問題が生じる。また、関連して(c)例外集合をどの様に定めるか、という問題も生じる。これら及び(d)虚 2 次体の Dirichlet 指標に対する L 関数の Siegel 零点への応用、について望月氏と議論をした。(a)については、Hodge 舞台の構造を適切に修正すること、(b)については、無限素点での悪還元という概念を導入して無限素点

でのエタール・テータの理論を構築すること、で困難を克服した。その結果、(d)により、L 関数の零点解明への宇宙際幾何学の初めての応用が得られた。これは(理論的な包含関係はないものの)次の(B)を研究する上で大きな進歩であった。また、単テータ環境の代わりにテータ・モノイドを使うなど、理論の簡略化も進んだ。

(B)について。遠 Abel 幾何的にテータ関数を復元し、Jacobi の三重積公式を用いて、ある加法(具体的には 1 と 3q の和)の"乗法的な分解"が得られる、という望月氏の発案をもとに同氏とともに(B)の発展的理論の構築を進めている。古典的な宇宙際 Teichmuller 理論及び上記(A)の拡張においては幾何的/組み合わせ論的次元が 2 であるのに対して、(B)の発展的理論においては幾何的/組み合わせ論的次元が 3 であることが大きく違う。これにより、Galois 評価写像・対数 Kummer 対応・第 3 不定性が(古典的な宇宙際 Teichmuller 理論及びその拡張(A)と異なり)それぞれ 2 種類生じる。この意味でより複雑になっているが、その一方、無限遠点(つまり Tate 曲線)においては Hodge 舞台における"仮想的な"大域的乗法部分空間及び±生成元が標準的に存在していて Hodge 舞台の構造は簡単になっている。引き続きこの発展的理論の構築を研究する。

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　1件／うちオープンアクセス　1件）

１．著者名 Koji Nuida	４．巻 -
２．論文標題 An elementary linear-algebraic proof without computer-aided arguments for the group law on elliptic curves	５．発行年 2021年
３．雑誌名 International Journal of Mathematics for Industry	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） 10.1142/S2661335221500015	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 Koji Nuida	４．巻 -
２．論文標題 Towards Constructing Fully Homomorphic Encryption without Ciphertext Noise from Group Theory	５．発行年 2020年
３．雑誌名 in: Proceedings of International Symposium on Mathematics, Quantum Theory, and Cryptography	６．最初と最後の頁 57-78
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-981-15-5191-8_8	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 Bernhard Muhlherr, Koji Nuida	４．巻 225
２．論文標題 Locally finite continuations and Coxeter groups of infinite ranks	５．発行年 2021年
３．雑誌名 Journal of Pure and Applied Algebra	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） 10.1016/j.jpaa.2020.106464	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 該当する

１．著者名 Go Yamashita	４．巻 54
２．論文標題 An introduction to p-adic Hodge theory for open varieties via syntomic cohomology	５．発行年 2019年
３．雑誌名 in: Une promenade dans la theorie de Hodge p-adique: des fondements aux developpements recents, Panoramas et Syntheses	６．最初と最後の頁 131-157
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4件（うち招待講演　1件／うち国際学会　2件）

１．発表者名
Go Yamashita

２．発表標題
A Motivation of Theta-Link from Hodge-Arakelov Theory

３．学会等名
Inter-universal Teichmuller Theory Summit 2021（国際学会）

４．発表年
2021年

１．発表者名
小田川 拓利，縫田 光司

２．発表標題
Optimal DeepLLL系基底簡約の停止性の証明と計算量評価

３．学会等名
暗号と情報セキュリティシンポジウム2021（SCIS 2021）

４．発表年
2021年

１．発表者名
品川 和雅，江利口 礼央，縫田 光司

２．発表標題
平方剰余に基づくPrivate Simultaneous Messagesについて

３．学会等名
暗号と情報セキュリティシンポジウム2021（SCIS 2021）

４．発表年
2021年

１．発表者名
Koji Nuida

２．発表標題
Towards Constructing Fully Homomorphic Encryption without Ciphertext Noise from Group Theory

３．学会等名
International Symposium on Mathematics, Quantum Theory, and Cryptography (MQC 2019)（招待講演）（国際学会）

４．発表年
2019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
研究分担者	山下　剛 (Yamashita Go) (70444453)	京都大学・数理解析研究所・講師 (14301)	

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			
ドイツ	University of Giessen			