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　 ５ 月 ２６ 日現在

機関番号：１１３０１
研究種目：基盤研究(C)（一般）
研究期間：2019～2022
課題番号：１９Ｋ０３６１２

研究課題名（和文）非可換な代数構造を利用した公開鍵暗号方式の一般的構成方法の提案

研究課題名（英文）A proposal for general constructions of public key cryptosystems based on noncommutative algebraic structures

研究代表者

小泉　英介（Koizumi, Eisuke）

東北大学・データ駆動科学・AI教育研究センター・助教

研究者番号：３０４００４４３

交付決定額（研究期間全体）：（直接経費）　　1,500,000円

研究成果の概要（和文）：非可換な代数構造を利用した暗号方式は，量子計算機が実用化されたとしても安全性を担保できると考えられている．しかし，既存の暗号方式の多くはいくつかの安全上の問題を抱えており，ただちに実用化することは困難である．本研究では，WICS2018で研究代表者らが構成した非アーベル群上の暗号方式について，それが抱えている安全性の問題を解決することを目指した．その結果，ある種の半直積上で，元の暗号方式の利点を残しつつより高い安全性を有する方式を構成することができた．

研究成果の学術的意義や社会的意義
これまでの暗号方式はアーベル群，特に素数位数の巡回群を利用して構成されることがほとんどであった．そのため，量子計算機の脅威から逃れるという意味で，アーベル群以外の代数構造を利用した暗号方式を構成するという意義は多分に大きい．また，暗号方式を構成するために，本研究を通して半直積の構造を詳しく調査した．その調査結果を利用することで，暗号方式の安全性の根拠となる諸問題の難しさについて，より詳細に解析することが可能になると考えられる．

研究成果の概要（英文）：Cryptographic schemes based on noncommutative algebraic structures are considered to be secure even if quantum computers are put into practical use. However, many of the existing schemes include some security problems, and it is difficult to put them into practical use immediately. In this research, we tried to solve the security problems of our protocol proposed in WICS2018. As a result, we succeeded in constructing a protocol with desirable security on some specific semidirect product which maintains some advantages of the original protocol.

研究分野：情報セキュリティに関連する数学

キーワード：公開鍵暗号方式　非可換群

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

現代の公開鍵暗号方式の多くは，素因数分解問題や離散対数問題およびこれらから派生した様々な数論的問題の難しさにその安全性の根拠を置いている．しかし，量子計算機上でこれらの問題を効率的に解くアルゴリズムが発見されているため，量子計算機が実用化されると，これらの問題に安全性を依存する暗号方式は安全ではなくなる．

したがって，量子計算機が実用化されたとしても安全性を担保できるような暗号方式を構成することは非常に重要である．そのためのアプローチの一つとして，非アーベル群や群環など，アーベル群以外の代数構造とその上の問題を利用した暗号方式が研究されている．これまでの暗号方式はアーベル群，特に素数位数の巡回群を利用して構成されることがほとんどであったため，量子計算機の脅威から逃れるという意味でアーベル群以外の代数構造を利用する利点は小さくないと考えられる．また，これらの代数構造を利用した暗号方式は暗号学の研究者のみならず，数学（特に代数学）の研究者からも注目されている．

一方で，非可換な代数構造を利用した既存の暗号方式の多くは以下の二つの問題を抱えているため，ただちに実用化することは困難であると考えられる．

問題 1. 安全性証明がない．既存の暗号方式の中には，代数的な興味で構成されたものも数多く存在する．そのためか，安全性証明が与えられていないものが多い．このことは，たとえ安全性の根拠となる問題を解くことが難しいとしても，暗号方式に対する攻撃が成功する可能性があることを意味する．したがって，これらの方式をそのまま実用化することはできない．

問題 2. 暗号方式自体の都合による可換性要件を必要とする．ここでいう「可換性要件」とは，例えば暗号方式のアルゴリズム内の「パラメータ a と b については，$ab = ba$ を満たすように選ぶ」というような要件のことである．可換性を利用することで，秘密情報（秘密鍵や乱数など）の共有が容易になり，暗号方式が作りやすくなる．また，従来のアーベル群を利用した暗号方式に似た仕組みを適用することができる．しかし，アーベル群を利用した方式に対する既知の攻撃（およびその変形）を活用することにより，これらの方式の安全性が失われる可能性がある．

したがって，非可換な代数構造を利用した暗号方式が量子計算機の実用化に対する現実的な対抗手段になるためには，これら二つの問題を解決した方式を構成する必要がある．

２．研究の目的

本研究では問題 1 および 2 を解決する，すなわち以下の二つの条件を満たす非可換な代数構造を利用した公開鍵暗号方式の一般的構成方法を提案することを目指した:

条件 1. 安全性証明を有している．
条件 2. 暗号方式自体の都合による可換性要件を必要としない．

３．研究の方法

研究代表者らはこれまでに，Anshel らの鍵共有方式（AAG 鍵共有方式，Math. Res. Lett. 1999）から非アーベル群を利用した暗号方式（AAG 暗号方式）を構成している（WICS 2018）．しかし，この方式は本来望まれる安全性よりも少し弱い安全性しか有していない．また，その安全性を達成するために利用する非アーベル群やハッシュ関数にも厳しい条件が課されており，実際にその条件を満たす群やハッシュ関数は見つかっていない．そこで，以下のアプローチにより上記の問題を解決するような暗号方式の構成を目指した．

(1) 構造が比較的単純な非アーベル群をプラットフォームとした暗号方式を構成する．
(2) AAG 暗号方式のエッセンスを生かしつつ，より単純な暗号方式に改良する．

４．研究成果

(1) 改良 AAG 暗号方式の提案

まず，位数が異なる 2 素数 p と q の積 pq であるような半直積を考え，群の構造を調査した．そしてそれを元に，AAG 暗号方式の安全性の根拠となる問題の難しさや方式を改良するための検討を実施した．その結果，その群上で構成した AAG 暗号方式の安全性を高めるために必要とされる条件を明らかにすることができた．このことは，暗号方式内の鍵生成等に，どのような性質を持った（群の）元を利用するのが適切であるかという問題に対する一つの解を与えている．一方で，元の選び方を適切に行ったとしても，既存の方式が抱えている問題点を解決できない場合があることが判明した．さらに，この問題点と暗号方式の安全性は密接に関わっていることも明らかになった．そのため，プラットフォームとして新たに位数が素数 p と p とは異なる素数 q の 2 乗の積 pq^2 であるような半直積を考え，上と同様の考察を実施した．そ

の結果，改良 AAG 暗号方式を構成し，それが望ましい安全性を有していることを証明した．本成果についてまとめた論文は，2022 年度末に Journal of Mathematical Cryptology に掲載された．
AAG 暗号方式は，数学的に証明可能な安全性を有する暗号方式を任意の非アーベル群上で構成するための一つの一般的手法を与えているが，やや弱い形の安全性しか有していなかった．本研究で構成した改良 AAG 暗号方式は，非アーベル群の中でも半直積という限定された枠組みではあるが，最も強いと考えられる安全性を有する方式を構成するための一つの一般的手法を与えたということを意味している．

(2) 位数が pq および pq^2 の半直積の構造の調査
改良 AAG 暗号方式を構成するため，位数が pq および pq^2 の半直積の構造を調査した．特に，位数が pq^2 の半直積の構造については先に述べた論文中に与えている．半直積自体は代数学の教科書などで数多く紹介されているものの，演算構造などを詳細に調べた結果はこれまでにほとんどない．本調査は，半直積上で新たな暗号方式を構成する際，また暗号方式の安全性の根拠となる問題の難しさを調査する際に役立つと考えている．

(3) 半直積における改良 AAG 暗号方式の安全性の根拠となる問題に関する考察
公開鍵暗号方式の復号アルゴリズムには，通常，暗号文の妥当性をチェックする箇所がある．アーベル群上で構成された暗号方式の多くは，その妥当性のチェックが「可換性」を用いて行われる．一方で，非アーベル群上で構成された AAG 暗号方式では可換性を利用できないため，同様のチェックを実施するためには判定共役問題を解く必要がある．しかしながら，一般にこの問題は難しいと考えられている．そのため，AAG 暗号方式では暗号文の妥当性のチェックを実施することができず，結果として弱い安全性しか証明することができなかった．それに対して改良 AAG 暗号方式では，調査の結果得られた半直積の性質を活用し，かつ暗号方式もそれに合わせて改良することでこの問題を解決することができた．一方で，副産物として位数が pq^2 の半直積では，(一定の制限はあるものの) 判定共役問題が容易に解けることが示された．ただし，この結果は「任意の非アーベル群に対して判定共役問題が容易に解ける」や「半直積に対して判定同時共役問題 (改良 AAG 暗号方式の安全性の根拠となる問題) が容易に解ける」という結論を示すものではない．これらのことは，半直積における共役問題においてある種の「ギャップ」が存在することを示唆している．このような「ギャップ」はアーベル群上の問題においても類似の研究があり，本研究者らも 2021 年に IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences にて一つの成果を公表している．したがって，改良 AAG 暗号方式を構成する際に得られた副産物についても同様の考察ができるのではないかと期待している．

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　2件）

１．著者名 Isobe Shuji、Koizumi Eisuke	４．巻 17
２．論文標題 A construction of encryption protocols over some semidirect products	５．発行年 2023年
３．雑誌名 Journal of Mathematical Cryptology	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） 10.1515/jmc-2022-0018	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 KRAIEM Firas、ISOBE Shuji、KOIZUMI Eisuke、SHIZUYA Hiroki	４．巻 E104.A
２．論文標題 On a Relation between Knowledge-of-Exponent Assumptions and the DLog vs. CDH Question	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 20～24
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020CIP0002	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 KRAIEM Firas、ISOBE Shuji、KOIZUMI Eisuke、SHIZUYA Hiroki	４．巻 25
２．論文標題 On the Classification of Knowledge-of-exponent Assumptions in Cyclic Groups	５．発行年 2019年
３．雑誌名 Interdisciplinary Information Sciences	６．最初と最後の頁 67～74
掲載論文のDOI（デジタルオブジェクト識別子） 10.4036/iis.2019.R.03	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 －

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 Firas KRAIEM, Shuji ISOBE, Eisuke KOIZUMI, Hiroki SHIZUYA
２．発表標題 On a relation between knowledge-of-exponent assumptions and the DLog vs. CDH question
３．学会等名 2020年暗号と情報セキュリティシンポジウム
４．発表年 2020年

〔図書〕　計1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