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　 １ 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：１９Ｋ１１９５６

研究課題名（和文）有限非可換群上の耐量子問題の探究

研究課題名（英文）A Search for Quantum-resistant Problems over Finite Noncommutative Group

研究代表者
静谷　啓樹（SHIZUYA, Hiroki）

東北大学・データ駆動科学・AI教育研究センター・教授

研究者番号：５０１９６３８３

交付決定額（研究期間全体）：（直接経費）　　800,000円

研究成果の概要（和文）：量子計算機時代の暗号という文脈のもと、非可換有限群上の分解問題（以下、DP）の難しさを検討した。DPはBQP程度の容易さを持つとは知られていない。いま、解を持つDPのインスタンス全体を可算無限集合Lとし、実際に解を出力する非決定性多項式時間多価関数をfとする。
このとき、次を示した。LがNPとco-AMの共通部分に属することと、Lがランダム自己帰着性を持つこと。またDPの問題を設定する際、問題を構成する部分群の選び方によっては、fが決定性多項式時間で計算できることも示された。

研究成果の学術的意義や社会的意義
量子計算機で扱えるビット長の伸長は公開鍵系暗号技術の危殆化をもたらすため、すなわち全世界的な情報セキュリティへの脅威となるため、量子チューリング機械モデルでも計算が困難と見られる問題の発掘と、その暗号系への応用が期待されている。すでに格子に関連する問題や、超特異楕円曲線の同種写像に関連する問題などが主流の地位を占め、国際標準も検討されている段階ではあるが、新しい問題が不要となったわけではなく、むしろスペアとして議論を深めておく必要がある。そのための研究活動であり、積み上げた成果でもある。

研究成果の概要（英文）：Under the context of post quantum cryptography, we have investigated the difficulty of the decomposition problem over finite non-commutative groups (DP, for short), which is not known to be as easy BQP. Let L be the countably infinite set of DP instances that have solutions, and let f be the nondeterministic polynomial-time multivalued function that on input an instance, outputs a solution.
We have shown that L is in the intersection of NP and co-AM, and is random self-reducible.Further, we have found a non-trivial NP-complete set which L directly reduces to w.r.t.the many-one reducibility. We have also shown that f can be deterministic polynomial-time computable unless the underlyig subgroup is carefully chosen in the setting of DP.

研究分野：理論計算機科学

キーワード：耐量子問題　有限非可換群　計算量理論

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

現代の情報と情報システムの安全性を支えている暗号技術のうち、特に公開鍵系の技術は電子決済や電子マネー、暗号通貨、電子投票など多くの社会的に重要なシステムにおいて根幹的な技術として機能している。その技術の信頼性は、離散対数問題や素因数分解問題などの数論的な問題を現実的な時間内で解くことがチューリング機械など従来の計算モデル上のアルゴリズムでは難しいという計算量理論的な性質に依拠している。しかしながら、1994 年に Shor [1] によって開発された量子アルゴリズムは、それらの問題が量子チューリング機械のモデル上で容易に解けることを示しただけでなく、長いビット長を処理できる量子計算機が現実世界の機械として開発された場合には、現在の情報システムの安全性を破綻にすら追い込むことも自然な帰結として明らかにするものであった。
このため、量子計算機を駆使しても現実的な時間内には解けない問題に依拠した暗号技術の開発が 21 世紀になって本格化した。本研究代表者も早い段階から、耐量子性が期待されている格子問題を利用した暗号技術の研究 [2]、耐量子性のない問題を耐量子性が備わった問題へ難しさを引き上げる一般的手法（「リフティング」と名付けた）の開発[3] などを通じてこの分野の研究に参画してきた。

２．研究の目的

本研究では、非可換な有限群の上で耐量子性を持つと期待される新たな問題を構成し、その問題の性質（困難さの特徴付け、簡単に解ける場合の特徴付けなど）を解明するとともに、本研究代表者がかつて開発したリフティングの手法をこの問題をもとに改めて構築する。これらの研究活動を通じて耐量子性の理論と技術的選択肢を豊かにすることを目的とする。

３．研究の方法

○全体の概要

本研究で主に対象とする群論的な問題を「（非可換群上の）分解問題」と呼ぶこととする。具体的には次のように定義される。G を非可換な有限群とし、A をその部分群とする。G には属するが A には属さない元（すなわち $G \setminus A$ の元） x,y が入力されたとき、$y=axb$ となる A の元 a, b が存在するなら、それを出力する。

なお、a または b の片方を単位元にとれば他方が容易に求まるように見えるが、それが A の元になるとは限らないため、そこに群の構造と性質が問題の難しさの要因として入り込むことになる。

NIST（アメリカ国立標準技術研究所）は耐量子性を持つと見られる暗号系を概ね次のように分類している。格子に基づくもの、誤り訂正符号に基づくもの、多変数多項式に基づくもの、ハッシュ関数に基づくもの、およびその他である。実は、この「その他」の分類には超特異楕円曲線の同種写像に基づくものや、非可換群上の共役分解問題に基づくものなどが含まれている。本研究の分解問題は共役分解問題との関係性が深いことから、分類上はその他という雑多なものの一つという位置づけではある。

本研究では次の 2 点を達成することを目標とする。

・分解問題の難しさを多角的に検討して耐量子性の状況証拠を積み重ねること
・かつて本研究代表者が開発したリフティング技術を分解問題の活用により再構築すること

ここにリフティングとは、耐量子性が備わっていると見られる問題を比喩的に言えばゴンドラのように利用し、耐量子性のない問題をゴンドラに入れて耐量子性の領域へ引き上げ、量子計算機による攻撃を回避する計算量理論的な手法のことである。

以下、本研究で解明を目指す主要な個別テーマを述べる。

○計算量的困難さ

まずは分解問題の難しさについて、代表的な計算量のクラスを使って特徴付けを行う。具体的には、解を持つインスタンスの可算無限集合を $L=\{(x,y)\}$ としたとき、問題を定義した非可換群の二項演算が簡単に実行できるなどの仮定のもとで L がクラス NP に属することは自明であるものの、その補集合が属するクラスは必ずしも明らかではない。その特徴付けによって、NP 内部の階層構造の中で集合 L の複雑さが定位される。一方、(x,y) を入力としたときに (a,b) を出力する関数 f と見たとき、f が関数のクラス NPMVg に属することは明らかであるが、群の選び方や部分群の取り方によっては多項式時間計算可能な関数になってしまう可能性があり、その点も解明する。

○ランダム自己帰着性

ランダム自己帰着性は 1980 年代前半には既に認識されていた概念で、1990 年代には理論が精密化された[4][5]。本研究代表者も同年代に有限群から有限集合への写像の逆写像を計算する問

題がランダム自己帰着性を持つための条件を考察している[6]。
本研究で検討する分解問題もランダム自己帰着性を持つと期待される。具体的には、(x,y)というインスタンスに $y=axb$ という解が存在するならば、インスタンス (x,y) をランダムな A の元 r, s, t, u を使って (rxs, tyu) というインスタンスに変換した場合にも解 (α,β) は存在し、もし(α,β) が求まれば $a=t^{-1}\alpha r$，$b=s\beta u^{-1}$ により a,b が求まる。しかしランダムに変換した結果、部分集合、部分群や x の両側 A 軌道の上を一様ランダムに動くかどうかは精査が必要である。ランダム自己帰着性を持つグラフ同型問題は耐量子性も持つと見られていたが、Babai [7]のアルゴリズムによって難しさが著しく低下したため、再吟味が必要とも考えられる。

○リフティング技術
リフティング技術によって持ち上げられる関数と持ち上げる関数の一般的な関係は、本研究代表者の過去の研究[3]により、関数の計算量クラスの言葉（NPMV や NPSV など）を使って概ね解明されている。実際、離散対数を与える関数と同型なグラフの置換を与える関数について、前者を後者で持ち上げる例を示した。本研究では、分解問題の解を与える関数 f を使い、リフティングの条件を精査した上で様々な関数を持ち上げる手法を検討する。

[1] Peter W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” Proc. FOCS’94, pp.124-134 (1994). (ジャーナル版：SIAM J. Comput. Vol.25, pp.1484-1509 (1997))
[2] Shingo Hasegawa, Shuji Isobe, Masahiro Mambo, Hiroki Shizuya, Yuichi Futa, Motoji Ohmori, "A countermeasure for protecting NTRUSign against the transcript attack," Interdisciplinary Information Sciences, vol.13, no.2, pp.181-188 (2007).
[3] Shingo Hasegawa, Hiroyuki Hatanaka, Shuji Isobe, Eisuke Koizumi, Hiroki Shizuya, "Making cryptographic primitives harder," IEICE Trans. Fundamentals, Special Section on Cryptography and Information Security, vol.E91-A, no.1, pp.330-337 (2008).
[4] M. Tompa and H. Woll, “Random self-reducibility and zero knowledge interactive proofs of possession of information,” Proc. FOCS’87, pp.473-482 (1987).
[5] J. Feigenbaum and L. Fortnow, “Random-self-reducibility and complete sets,” SIAM J. Comput., vol 22, no.5, pp.994-1005 (1993).
[6] H. Shizuya and T. Itoh, “A group-theoretic interface to random self-reducibility,” Trans. of the IEICE, Special Issue on Cryptography and Information Security, vol.E-73, no.7, pp.1087–1091 (1990).
[7] L. Babai, “Graph isomorphism in quasipolynomial time (Extended abstract),” Proc. STOC’16, pp.684-697 (2016).

４．研究成果
研究の方法で述べた各項目について成果の概要を述べる。なお分解問題を、その解が存在するかどうかの「判定問題」と、実際に分解問題の解を与える「計算問題」に分けて記述している。

【全般的仮定】
分解問題を考えている有限非可換群 G の一般的な性質としては、G の二項演算が容易に実行できるという自然な仮定のほか、暗号への応用を考慮して、いくつか計算量的な仮定を追加している。具体的には、G 上で逆元の計算が容易なこと、G の元かどうかの識別が容易なこと、G の元 u, v が与えられたとき、$u=v$ かどうかを容易に判定できること、G から一様ランダムに元を選ぶことが容易であること、さらに G の部分群 A について、G の勝手な元が部分群 A に属するかどうかを容易に判定できること、である。ここに「容易に」とは、基本的に多項式時間を想定している。

【判定問題】
「(非可換群上の）分解問題」の判定問題とは、G を非可換な有限群、A をその部分群としたとき、G には属するが A には属さない元（すなわち $G\setminus A$ の元） x, y が入力されたとき、$y=axb$ となる A の元 a, b が存在するような$\{(x,y)\}$の集合(すなわち、解が存在するインスタンスだけを元とする集合） L を考え、勝手な文字列(x,y)に対してそれが L に属するかどうかを判定する問題である。なお、個々の G は有限群であるが、あらゆる大きさの G を包括して議論するため、Lは可算無限集合となる。

(1)難しさの特徴付け
L は自然に NP 集合だが、より精密にはクラス NP 内部の階層構造における低階層のレベル 2 に入ることが判明した。具体的には、A の補集合が Arthur-Merlin ゲーム（定数ラウンドの対話証明）を持つことを示せたので、$L\in$NP$\cap$co-AM から自動的に低階層のレベル 2 に入った。この場合、解が存在するインスタンスかどうかのみを判定する問題を考えるのであって、具体的な解の計算を求める分解問題はその判定問題と多項式時間チューリング帰着の意味で同等か難しい（同等であるなら、この集合は自己計算可能解（後述）を持つという重要な性質を満たすが、それはまだわかっていない)。なお、この結果の自明な系として、分解問題に基づくその集合 L が NP 完全ならば、多項式時間階層（PH）は第 2 レベルまでつぶれることになる。

この結果は、例えば素因数分解問題で素因数を具体的に計算する問題や、有限体上の乗法群や楕円曲線の群で定義された離散対数問題で対数を具体的に計算する問題が低階層のレベル 1 の集合で特徴づけられることと対比すれば、分解問題の暗号学的な位置づけを計算量理論の観点から示唆するものとなる。もちろん、レベル 2 にあるからといってレベル 1 に落ちない保証はない上に、レベル 1 やレベル 2 と量子多項式時間計算可能なクラスの関係も未解明であるから、単なる定性的な傾向を見ているに過ぎない。

(2)明示的に帰着する NP 完全集合

前項のとおり解を持つインスタンスの可算無限集合 L について、$L \in \mathrm{NP} \cap \mathrm{co\text{-}AM}$ であり、したがって L が NP 完全ならば $\mathrm{PH} \subseteq \Pi_2$ と潰れる。一方で、L から明示的に帰着する NP 完全集合を知ることは、問題の難しさの位置づけを多角的に知るための情報を含んでいるため、この点を検討した。ここで言う「明示的」とは、各 NP 集合から SAT へのジェネリックな帰着のことではなく、また、SAT と L のマーク付き和集合への帰着のような、関係性の本質的な情報を含まない帰着でもない。求めているのは、ちょうど、グラフ同型性判定問題(NP∩co-AM)と部分グラフ同型性判定問題(NP 完全)の関係と並行的な姿になるような NP 完全集合のことである。

本研究では、ブール式を充足させる割り当てのパターンに合致する分解問題のインスタンスを対応させる形で集合 D を構成し、D が NP 集合であること、L から直接的に D に多項式時間多対一帰着すること、SAT からも D に多項式時間多対一帰着することの 3 点を証明することで、集合 D が NP 完全であることを示した。

なお、SAT は自己計算可能解（インスタンスの充足割り当てを、SAT 自身をオラクルにして多項式時間で計算可能な性質）を持つことが知られているが、D については現時点で不明である。

(3)ランダム自己帰着性

直観的に言えば、集合 S のインスタンス x を乱数によって y に変換し、$y \in S$ ならば $x \in S$ であり、また逆も成り立つような関係が成り立つとき、ランダム自己帰着性を持つと言う。本研究では、前項までと同じ L について、ランダム自己帰着性が成立することを確認した。これにより、L は完全ゼロ知識証明を持つことになるが、このことは(1)の $L \in \mathrm{NP} \cap \mathrm{co\text{-}AM}$ と矛盾しない。

また、ランダム自己帰着性より広い概念として自己帰着性(self- ではなく auto-reducibility)があるが、自然にこれも満たしている。この帰着は、厳密には多項式時間チューリング自己帰着性である。

【計算問題】

「(非可換群上の）分解問題」の計算問題とは、G を非可換な有限群、A をその部分群としたとき、G には属するが A には属さない元（すなわち $G \setminus A$ の元） x, y が入力されたとき、$y = axb$ となる A の元 a, b が存在するなら、それを出力する問題である。

(1)ランダム自己帰着性

判定問題で使った方法をそのまま使って、計算問題としてもランダム自己帰着性を示せる。

また、分解問題を解く関数を f としたとき、f は明らかに非決定性多項式時間多価(NPMV)関数のクラスに属するが、その単価洗練関数(refinement)が存在すればという仮定のもとで、f は自己帰着性(auto-reducibility)を持つことがわかる。

(2)弱い部分群の発見

分解問題を定義する非可換有限群 G やその部分群 A が特定の性質を持つものとして条件を設定すると、問題自体が簡単になる可能性がある。そこで、まずは部分群の性質を変えて検討を行った。実際に簡単になってしまうとき、これを「弱い部分群」と呼ぶことにする。このような特別な条件を具体的に探索することは、インスタンスの平均的な計算量を見積もる上でも重要な作業になる。

検討の結果、A が正規部分群であれば弱い部分群になることが明らかになった。具体的には、A が正規部分群であれば、決定性多項式時間で解を求めることができることを証明した。具体例で言えば、体 K 上の n 次一般線形群を G とし、同じ体上の n 次特殊線形群を A と設定した分解問題は、決定性多項式時間で解けることになる。

この弱い部分群については、本研究で対象としている分解問題の難しさに関する現時点でほとんど唯一の構造定理と思われ、分解問題の暗号系への運用の重要なガイドラインを与えるものである。

【その他】

リフティングについてはうまくリフトする仕組みを構築できなかった。本研究代表者がこれまでリフティングに使った道具がグラフ同型問題であり、基本的に n 次対称群という非可換群がベースの仕組みであったことから本研究の分解問題と親和性・互換性が高いであろうとの当初の見通しであったが、実際はそうではなかった。判定問題の(2)で使ったテクニックの応用を含めて、今後の検討課題としたい。

５．主な発表論文等

〔雑誌論文〕　計5件（うち査読付論文　5件／うち国際共著　1件／うちオープンアクセス　3件）

１．著者名 Shingo Hasegawa, Masashi Hisai, Hiroki Shizuya	４．巻 11
２．論文標題 Public-key Projective Arithmetic Functional Encryption	５．発行年 2021年
３．雑誌名 International Journal of Networking and Computing	６．最初と最後の頁 299-318
掲載論文のDOI（デジタルオブジェクト識別子） 10.15803/ijnc.11.2_299	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 Anaelle Le Devehat, Hiroki Shizuya, Shingo Hasegawa	４．巻 13099
２．論文標題 On the Higher-bit Version of Approximate Inhomogeneous Short Integer Solution Problem	５．発行年 2021年
３．雑誌名 Lecture Notes in Computer Science	６．最初と最後の頁 253-272
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-92548-2_14	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 Firas Kraiem, Shuji Isobe, Eisuke Koizumi, Hiroki Shizuya	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 Trans. Fundamentals, Special Section on Cryptography and Information Security	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 オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Firas KRAIEM, Shuji ISOBE, Eisuke KOIZUMI, Hiroki SHIZUYA	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 －

1．著者名 Anaelle Le Devehat, Shingo Hasegawa, Hiroki Shizuya	4．巻 13849
2．論文標題 Preimage Sampling in the Higher-bit Approximate Setting With a Non-spherical Gaussian Sample	5．発行年 2023年
3．雑誌名 Lecture Notes in Computer Science	6．最初と最後の頁 472-490
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-29371-9_23	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

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　2件）

1．発表者名 Shingo Hasegawa, Masashi Hisai, Hiroki Shizuya
2．発表標題 Public-key Projective Arithmetic Functional Encryption
3．学会等名 2020 Eighth International Symposium on Computing and Networking (CANDAR)（国際学会）
4．発表年 2020年

1．発表者名 Takahiro Saito, Daiki Miyahara, Yuta Abe, Takaaki Mizuki, Hiroki Shizuya
2．発表標題 How to Implement a Non-uniform or Non-closed Shuffle
3．学会等名 9th International Conference on the Theory and Practice of Natural Computing (TPNC 2020), LNCS 12494, pp.107-118（国際学会）
4．発表年 2020年

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 Symposium on Cryptography and Information Security
4．発表年 2020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