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　 ６ 月 ２７ 日現在

機関番号：３７１１２
研究種目：若手研究
研究期間：2020～2023
課題番号：２０Ｋ１４３０１

研究課題名（和文）計算代数手法に基づく正標数の代数曲線に関する研究の深化と暗号応用への展望

研究課題名（英文）Study on algebraic curves in positive characteristic via computational algebraic geometry and its application to cryptography

研究代表者

工藤　桃成（Kudo, Momonari）

福岡工業大学・情報工学部・助教

研究者番号：１０８２４７０８

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：正標数の代数曲線の存在・非存在の決定および数え上げ，関連する計算代数幾何学のアルゴリズム群の整備，さらには同種写像暗号の安全性解析への応用，の研究を行った。特に重要な結果として，超楕円曲線のファイバー積に双有理同値な曲線クラス（一般化Howe曲線と呼ばれる）に着目し，その定義方程式の明示的な記述や，Jacobi多様体間の同種写像の計算アルゴリズムを与えた．さらに，一般化Howe曲線を利用することで，種数3，4，5の各場合において，超特別曲線を高速に探索または全列挙するアルゴリズムを構成した．研究期間全体を通じて，当初の予定以上に多くの研究成果（雑誌論文14件，学会発表27件）が得られた．

研究成果の学術的意義や社会的意義
本研究で開発した計算代数幾何学のアルゴリズムは，代数曲線の研究のみならず他の代数学分野においてもツールとしての利活用が期待されるだけでなく，同種写像暗号や多変数多項式暗号などの量子計算機の解読にも耐性をもつ暗号（耐量子計算機暗号）の安全性解析に応用される．また，本研究で得られた超特別曲線は，同種写像暗号において安全なパラメータとしての利用が期待されるなど，情報セキュリティ分野への貢献にも繋がる．

研究成果の概要（英文）：We studied algebraic curves in positive characteristic, for example, proving the (non-)existence of curves with prescribed invariants such as p-rank and a-number and enumerating such curves over finite field. We also developed related algorithms in algebraic geometry in positive characteristic, and analyzed the hardness of computational problems related to isogenies, which are security base in isogeny-based cryptography. In our study of algebraic curves in positive characteristic, we focused on curves birational to fiber products of hyperelliptic curves (such a curve is called a generalized Howe curve): We wrote down their explicit equations, and constructed algorithms to compute isogenies between their Jacobian varieties. As an application, we presented practical algorithms to find or enumerate superspecial curves, in each case of genus 3, 4, and 5. As a result, we wrote 14 journal papers and gave 27 conference talks in total, throughout the research period supported by this grant.

研究分野：代数幾何学

キーワード：計算代数幾何学　代数曲線　正標数　超特異曲線　超特別曲線　Jacobi多様体　有理点　同種写像暗号

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

代数幾何学と整数論およびその応用分野（暗号理論など）において，代数曲線は古くから研究されてきた重要な研究対象である．特に，正標数の体上では，「付随する Newton 多角形が傾き 1/2 の線分」という不変量を持つ曲線（resp. アーベル多様体）は超特異曲線（resp. 超特異アーベル多様体）と呼ばれ，代数曲線・アーベル多様体の性質を分類する上で中心的な役割を果たす．実際，モジュライ空間上の超特異軌道の構造を調べることで，モジュライ空間全体の構造をより深く調べることができる．それだけでなく，超特異曲線は量子計算機による解読にも耐性を持つ同種写像暗号のパラメータとしての利用も期待されている．ここで標数 $p > 0$ の体上の非特異既約代数曲線（resp. アーベル多様体）が超特異（supersingular）であるとは，そのヤコビ多様体（resp.それ自身）が超特異楕円曲線（無限遠点以外に p 等分点を持たない楕円曲線）の直積に閉体上で同種となるときをいう．さらに同型となるとき，超特別（superspecial）という．

アーベル多様体の場合，各次元におけるモジュライ空間上の超特異軌道の基本構造（次元，既約成分の個数，各成分の次元など）は完全に決定されており，近年では階層構造などのより精密な構造の研究が進展している．一方で代数曲線の場合，種数 3 以下の場合に限り，超特異曲線（および超特別曲線）の（非）存在性は任意標数 $p > 0$ に対し決定されている（Deuring，井草，伊吹山，桂，Oort らの研究）．これらの結果は，主にアーベル多様体のモジュライ理論に基づく整数論的な手法によって得られた．実際，種数 1 （resp. 2, 3）の場合の手法は，「Mass 値の計算を，ある定値四元数環（resp. 四元数ユニタリ群）の類数計算に帰着させ，Hecke 作用素の跡公式により実現する」というもので，非常に整数論的である．一方で種数 g が 4 以上の場合，一部の標数を除き，超特異軌道の構造を含め，超特異曲線の（非）存在性を決定する理論や計算手法が整備されていない．具体的な原因として，代数曲線のモジュライ空間がより巨大かつ複雑になるだけでなく，種数 3 以下の場合にはない困難性として，種数 g の代数曲線のモジュライの次元が，次元 g の主偏極アーベル多様体のモジュライの次元より低い（よって代数曲線のヤコビ多様体として実現不可能な主偏極アーベル多様体が存在する）ため，種数 3 以下の場合における先行結果を得るための手法が同様には機能しない．そこで報告者らは本研究計画の申請時以前に、主に種数 4,5 の場合に、超特異曲線の中でも強いクラス（閉体上での同型類が有限個しかない）である超特別曲線について，その数え上げを計算問題に帰着させ，グレブナー基底などの計算代数手法により計算問題を効率的に解くアルゴリズムを開発した．アルゴリズムを計算機代数システム Magma 上で実装・実行することで，種数 4 の非超楕円曲線，超楕円曲線，種数 5 の曲線の一部について，小標数の場合に超特別曲線を全て決定した．特に重要な結果として，種数 4，標数 7 では超特別曲線は存在しないという結果を得た．また，特定の合同式を満たす無限個の p に対する超特別曲線の構成的な存在性証明にも成功した．一方で，種数 4,5 における一般的な $p > 0$ に対する結果や，より高い種数に対する結果は依然として得られていなかった．また，超特異曲線についても同様の状況であり，上述の通り超特異軌道の構造はもとより，超特異曲線の（非）存在性でさえ（特殊な p を除き）示されていなかった．

２．研究の目的

代数幾何学と整数論およびその応用分野（暗号理論など）において，代数曲線は重要な研究対象である．特に，正標数の体上では，ある不変量を持つ曲線の（非）存在性が中心的な未解決問題となっている．本研究では，その中でも特に重要な超特異曲線について，高種数・一般標数における（非）存在性を明らかにすることを主目的としており，理論・計算・応用を含む多方面からのアプローチによってその解決を目指している．超特異曲線の中でも強いクラスである超特別曲線については，報告者らによる先行研究において数え上げのアルゴリズムが知られているので，本研究ではその高速化改良によってさらに大きな標数での結果を得ることや，計算機上で得られた結果をもとに理論的な証明を与えることを目指す．また，超特別曲線は a-数（a-number）と呼ばれる不変量の値が種数に等しい曲線であるが，a-数が種数に等しくないが近い値をとるような曲線の（非）存在性についても明らかにする．一方で超特異曲線の存在は，曲線のモジュライ空間上の超特異軌道が空でないことを意味する．そのため，超特異軌道が空でないことがわかった後は，その軌道の構造（次元など）を明らかにする．また本研究では，学術論文の公開に加えて，得られる結果をデータベースとして一般公開するとともに，実装アルゴリズム・ソースコードを公開する．これにより，計算機の専門・非専門に関わらず，本研究に関係する分野の研究者に必要となるデータを簡単に利活用できる環境を整備する．

本研究では，上記の目的を達成する過程で，正標数における代数曲線の計算理論の構築・整備や，関連する計算代数幾何学のアルゴリズム，および計算機整数論のアルゴリズムの開発等も行う．これらの計算理論やアルゴリズムは，代数学の諸分野における計算問題の解決にも有効となり得るだけでなく，公開鍵暗号や電子署名方式の安全性解析においても有用なツールとなり得る．また，本研究で得られる曲線の一部は，量子計算機による解読に耐性を持つ新たな暗号方式のパラメータとしての利用が期待されているため，本研究の完成により，代数学の諸分野のみならず情報セキュリティに対する貢献も可能となる．

３．研究の方法

「１.研究開始当初の背景」に述べた,報告者らによって提案された計算ベースの研究手法は,超特異曲線の中でも強いクラスである超特別曲線の同型類の数え上げに特化している．従って,（超特別とは限らない)超特異曲線の(非)存在性を含む超特異軌道の全容を解明するためには,代数曲線論や代数曲線・アーベル多様体のモジュライ理論に基づく新たなアプローチが必須である．そこで本研究では，そのような新たなアプローチの提案と,これまでの計算ベースの手法の高速化改良・高種数版の開発を行い，これら二つを組み合わせることで本研究目的の達成を目指す.

４．研究成果

研究期間全体を通じて，正標数の代数曲線の存在・非存在の決定および数え上げ，関連する計算代数幾何学のアルゴリズム群の整備，さらには同種写像暗号の安全性解析への応用，の研究を行い，当初の予定以上に多くの研究成果（雑誌論文 14 件，学会発表 27 件）が得られた．以下に，各成果の概要を述べる.

Ａ．超特異曲線および超特別曲線に関するもの

A-1.本研究開始年度の前年度に，原下秀士氏（横浜国立大学），千田駿人氏（横浜国立大学卒業生）との共同研究で，本研究の予備的結果として「任意標数に対する種数 4 超特異曲線の存在」を証明しておりプレプリントにまとめていたが，その結果のモジュライ理論等を用いた定式化などを本研究開始年度に新たに行った．その後，一連の結果をまとめた論文は学術雑誌 Research in Number Theory への掲載が決定し，出版済みである.

A-2.原下秀士氏，Everett W. Howe 氏との共同研究で，楕円曲線のファイバー積として定義される種数 4 の曲線クラス（Howe 曲線）に着目し，アーベル多様体間の Richelot 同種写像を利用することで超特別 Howe 曲線の同型類を高速に列挙するアルゴリズムを開発した．アルゴリズムを計算機代数システム Magma 上で実行することで,11 以上 200 以下の素数について,超特別 Howe 曲線の同型類を全て決定した．また，11 以上 20000 以下の全ての素数について，超特別 Howe 曲線が存在することを示した．この結果は国内外で高く評価され，2020 年 6〜7 月に開催された査読付き国際会議 ANTS-XIV に採択されるとともに，2020 年 10 月に開催された国際研究集会 supersingular2020（RIMS 共同利用）における招待講演にて発表した.

A-3.原下秀士氏，大橋亮氏（当時・横浜国立大学，現在・東京大学）との共同研究で，種数 3 非超楕円曲線で自己同型群が位数 6 または 9 の巡回群であるようなものについて，とり得る a-数の値を決定するとともに,a-数が最大となるような曲線の同型類個数を決定した.研究手法としては,代数曲線の算術的手法に超幾何級数を組み合わせている.結果をまとめた論文は研究期間終了後の最近になって学術雑誌 Acta Arithmetica に掲載が決定された.

A-4.原下秀士氏，大橋亮氏（当時・横浜国立大学，現在・東京大学）との共同研究において，自己同型群が Klein 四元群を含むような種数 4 超特別超楕円曲線の高速生成アルゴリズムを開発し，計算機上の実行によって従来研究よりも非常に大きな標数（7,000 程度）に対し数え上げの結果を得ることができた．この結果は査読付き国際会議 WAIFI2022 に発表が受理され，結果をまとめた論文は同会議プロシーディングスの一記事として Springer から出版された.

A-5.中川輔氏（当時・東京大学，現在・卒業生），高木剛氏（東京大学）との共同研究で，自己同型群が位数 6 巡回群を含む種数 4 超特別超楕円曲線の高速数え上げアルゴリズムを開発した．この結果は査読付き国際会議 CASC2022 に発表が受理された．その後，結果をまとめた論文は学術雑誌 Mathematics in Computer Science に受理され，出版済みである.

A-6.種数 5 非超楕円 Howe 曲線の平面特異 6 次曲線モデルについて，明示的な定義方程式，特異点の個数・配置を決定した．うち一部は守谷共起氏と共同で研究を行った．また，守谷氏，大橋亮氏と共同で，種数 5 非超楕円 Howe 曲線のうち超特別なものを全て列挙するアルゴリズムを構成し，計算機上の実行により，100 未満の任意の素数に対し全列挙に成功した．特に，7 以上 97 以下かつ 13 以外の全ての素数に対し，種数 5 超特別曲線が存在することが示された．これらの結果について，3 件（単著 1 件，共著 2 件）に分けて論文執筆済みであり，現在雑誌または査読付き国際会議に投稿中である.

B. 代数曲線の算術理論および計算代数幾何学のアルゴリズムに関するもの

B-1. 原下秀士氏との共同研究で，種数 5 の代数曲線に関して二つの結果を得た．一つ目は，種数 5 曲線が超楕円でもトリゴナルでもない場合に，その曲線と双有理同値になるような平面特異 6 次曲線を明示的に構成し，この構成を利用し有理点を多くもつ曲線を全て決定するアルゴリズムを開発した．この結果は国内外で高く評価され，計算代数幾何学の査読付きトップカンファレンスである MEGA2021 に採択されるとともに，日本数学会の 2021 年度秋季総合分科会を含む各種国内学会で発表した．二つ目として，種数 5 曲線が超楕円またはトリゴナルの場合にも同様のアルゴリズムが得られ，その結果を国際会議 ICMC2022 で発表した．これらの結果をまとめた 2 件の論文は，それぞれ学術雑誌 Journal of Symbolic Computation と Commentarii Mathematici Universitatis Sancti Pauli への掲載が決定している．

B-2. 古江弘樹氏（当時・東京大学，現在・NTT）との共同研究で，多変数多項式成分行列を用いた，有限体上の代数方程式系を高速に解くアルゴリズムを開発した．この結果は査読付き国際会議 PQCrypto 2024 に発表が受理さた．また，研究期間終了後の最近になって，結果をまとめた論文は同会議プロシーディングスの一記事として Springer から出版された．

B-3. 原下氏との共同研究で，特異点を持つ平面曲線の特異点解消を求めるアルゴリズム，およびその得られた非特異曲線の正則微分形式のなす空間を計算するアルゴリズムを開発した．この結果はプレプリントにまとめ arXiv に公開済みである．

B-4. 守谷共起氏（当時・東京大学，現在・Birmingham 大学）との共同研究で，アーベル多様体間の分解 Richelot 同種写像を計算するアルゴリズムを開発し，その応用として種数 3 の場合に超特別曲線を高速に列挙するアルゴリズムを構成した．この結果はプレプリントにまとめ arXiv に公開済みであり，現在雑誌投稿中である．

B-5. 代数幾何学の研究において古典的に重要な連接層のコホモロジー群について，本研究開始年度の前年度に，正標数の体上の代数多様体の構造層に対するコホモロジー群へのフロベニウス作用（正確には特定の基底に関して表示する行列：Hasse-Witt 行列）を計算するアルゴリズムを与えており，本研究開始年度に日本数式処理学会の奨励賞を受賞した．本研究期間後半になって，代数多様体がある意味で退化している場合などの特殊な状況で有効となる，より簡略化されたアルゴリズムを新たに与えた．その新規結果をまとめた論文は日本数式処理学会の学会誌「数式処理」に査読付き論文（奨励賞受賞論文）として掲載が受理され，出版済みである．

C. 同種写像暗号への応用に関するもの

C-1. 池松泰彦氏（九州大学）らとの共同研究で，超特異楕円曲線間の同種写像の高速計算法を開発し，暗号分野への応用可能性を示した．結果をまとめた論文は査読付き国際会議 APKC2020 に採択され，プロシーディングスの一記事として電子出版済みである．

C-2. 神戸佑太氏（当時・埼玉大学，現在・三菱電機）らとの共同研究で，構成的 Deuring 対応問題と呼ばれる，超特異楕円曲線に関連する計算問題を解くための主要なツールである Kohel-Lauter-Petit-Tignol アルゴリズムをフリーソフトウェア Sage に実装した．実装結果をまとめた論文は 2021 年 3 月に開催された査読付き国際会議 ICMC2021 に採択され，プロシーディングスの一記事として出版済みである．また，その後の共同研究では，超特異楕円曲線に関する主要な計算問題である構成的 Deuring 対応問題を解く高速計算法を開発し，査読付き国際会議 MathCrypt2021 に発表が受理された．その後，結果をまとめた論文は学術雑誌 Mathematical Cryptology に受理された．

以上の他にも，自己同型群が Klein 四元群より真に大きい種数 4 超特別超楕円曲線の数え上げの結果，外積代数におけるグレブナー基底の高速計算に関する結果，同種写像暗号 B-SIDH の解読に関する結果，などが得られており，それぞれ論文にまとめ国際会議または雑誌投稿中である．

５．主な発表論文等

〔雑誌論文〕　計14件（うち査読付論文　14件／うち国際共著　1件／うちオープンアクセス　11件）

１．著者名 Kudo Momonari、Nakagawa Tasuku、Takagi Tsuyoshi	４．巻 17
２．論文標題 Efficient Search for Superspecial Hyperelliptic Curves of Genus Four with Automorphism Group Containing C6	５．発行年 2023年
３．雑誌名 Mathematics in Computer Science	６．最初と最後の頁 21 pages
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s11786-023-00571-w	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 工藤桃成	４．巻 29
２．論文標題 代数多様体のコホモロジー群へのフロベニウス作用を計算するアルゴリズム	５．発行年 2023年
３．雑誌名 日本数式処理学会論文誌「数式処理」	６．最初と最後の頁 3-30
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 オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Momonari Kudo, Shushi Harashita	４．巻 70
２．論文標題 Algorithmic study of superspecial hyperelliptic curves over finite fields	５．発行年 2022年
３．雑誌名 Commentarii Mathematici Universitatis Sancti Pauli	６．最初と最後の頁 49-64
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 オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Ohashi Ryo、Kudo Momonari、Harashita Shushi	４．巻 13638
２．論文標題 Fast Enumeration of Superspecial Hyperelliptic Curves of Genus 4 with Automorphism Group V_4	５．発行年 2023年
３．雑誌名 S. Mesnager, Z. Zhou (eds), Arithmetic of Finite Fields, WAIFI 2022, Lecture Notes in Computer Science	６．最初と最後の頁 107～124
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-22944-2_6	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 Yuta Kambe, Masaya Yasuda, Masayuki Noro, Kazuhiro Yokoyama, Yusuke Aikawa, Katsuyuki Takashima and Momonari Kudo	4．巻 1(2)
2．論文標題 Solving the constructive Deuring correspondence via the Kohel-Lauter-Petit-Tignol algorithm	5．発行年 2022年
3．雑誌名 Mathematical Cryptology	6．最初と最後の頁 10-24
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 オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Ryoya Fukasaku, Yasuhiko Ikematsu, Momonari Kudo, Masaya Yasuda and Kazuhiro Yokoyama	4．巻 -
2．論文標題 Introduction to algebraic approaches for solving isogeny path-finding problems	5．発行年 2022年
3．雑誌名 RIMS Kokyuroku Bessatsu (Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties)	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） なし	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 Momonari Kudo	4．巻 -
2．論文標題 Counting isomorphism classes of superspecial curves	5．発行年 2022年
3．雑誌名 RIMS Kokyuroku Bessatsu (Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties)	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） 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 －

1．著者名 Momonari Kudo and Shushi Harashita	4．巻 -
2．論文標題 Introduction to Computational Algebraic Geometry	5．発行年 2022年
3．雑誌名 RIMS Kokyuroku Bessatsu (Algebraic Number Theory and Related Topics 2020)	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） なし	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 Kudo Momonari、Harashita Shushi、Senda Hayato	４．巻 6
２．論文標題 The existence of supersingular curves of genus 4 in arbitrary characteristic	５．発行年 2020年
３．雑誌名 Research in Number Theory	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） 10.1007/s40993-020-00217-x	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 Kudo Momonari	４．巻 -
２．論文標題 Computing representation matrices for the action of Frobenius on cohomology groups	５．発行年 2020年
３．雑誌名 Journal of Symbolic Computation	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.jsc.2020.07.015	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 Takahashi Yasushi、Kudo Momonari、Fukasaku Ryoya、Ikematsu Yasuhiko、Yasuda Masaya、Yokoyama Kazuhiro	４．巻 15
２．論文標題 Algebraic approaches for solving isogeny problems of prime power degrees	５．発行年 2020年
３．雑誌名 Journal of Mathematical Cryptology	６．最初と最後の頁 31～44
掲載論文のDOI（デジタルオブジェクト識別子） 10.1515/jmc-2020-0072	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 Ikematsu Yasuhiko、Fukasaku Ryoya、Kudo Momonari、Yasuda Masaya、Takashima Katsuyuki、Yokoyama Kazuhiro	４．巻 -
２．論文標題 Hybrid Meet-in-the-Middle Attacks for the Isogeny Path-Finding Problem	５．発行年 2020年
３．雑誌名 Proceedings of The 7th ACM ASIA Public-Key Cryptography Workshop (APKC 2020)	６．最初と最後の頁 36～44
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3384940.3388956	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 Kudo Momonari、Harashita Shushi、Howe Everett W.	４．巻 4
２．論文標題 Algorithms to enumerate superspecial Howe curves of genus 4	５．発行年 2020年
３．雑誌名 Open Book Series	６．最初と最後の頁 301～316
掲載論文のDOI（デジタルオブジェクト識別子） 10.2140/obs.2020.4.301	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 該当する

１．著者名 Kambe Yuta、Aikawa Yusuke、Kudo Momonari、Yasuda Masaya、Takashima Katsuyuki、Yokoyama Kazuhiro	４．巻 -
２．論文標題 Implementation report of the Kohel-Lauter-Petit-Tignol algorithm for the constructive Deuring correspondence	５．発行年 2021年
３．雑誌名 Proceedings of 7th International Conference on Mathematics and Computing (ICMC2021)	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） 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27件（うち招待講演　13件／うち国際学会　8件）

１．発表者名 Hiroki Furue, Momonari Kudo
２．発表標題 On the computational enumeration of superspecial curves
３．学会等名 Computer Algebra in Scientific Computing (CASC 2022)（国際学会）
４．発表年 2022年

１．発表者名 Tasuku Nakagawa, Momonari Kudo, Tsuyoshi Takagi
２．発表標題 Efficient search for superspecial hyperelliptic curves in large characteristic
３．学会等名 Computer Algebra in Scientific Computing (CASC 2022)（国際学会）
４．発表年 2022年

１．発表者名
Kosuke Sakata, Momonari Kudo, Taku Kato, Kazuhiro Yokoyama

２．発表標題
Implementation report on computing Groebner bases over exterior algebras

３．学会等名
Computer Algebra in Scientific Computing (CASC 2022)（国際学会）

４．発表年
2022年

１．発表者名
Ryo Ohashi, Momonari Kudo, Shushi Harashita

２．発表標題
Fast enumeration of superspecial hyperelliptic curves of genus 4 with automorphism group V4

３．学会等名
International Workshop on the Arithmetic of Finite Fields (WAIFI 2022)（国際学会）

４．発表年
2022年

１．発表者名
工藤桃成

２．発表標題
Computational search and enumeration of superspecial curves with extra automorphisms

３．学会等名
九州代数的整数論2023 (KANT2023)（招待講演）

４．発表年
2022年

１．発表者名
工藤桃成

２．発表標題
計算代数幾何アルゴリズムを用いた超特別曲線の存在性と数え上げの進展状況

３．学会等名
早稲田整数論セミナー（招待講演）

４．発表年
2022年

１．発表者名
工藤桃成，大橋亮，原下秀士

２．発表標題
Fast enumeration of superspecial hyperelliptic curves of genus four

３．学会等名
日本応用数理学会2022年年会「数論アルゴリズムとその応用」(JANT) セッション

４．発表年
2022年

１．発表者名
工藤桃成

２．発表標題
グレブナー基底の計算量を評価するための様々な特徴量・不変量の関係

３．学会等名
研究集会「グレブナー基底を中心とした計算代数の基礎理論と暗号への応用」（招待講演）

４．発表年
2022年

１．発表者名
工藤桃成，大橋亮，原下秀士

２．発表標題
種数4の superspecial 超楕円曲線を多項式時間で探索するアルゴリズム

３．学会等名
日本数式処理学会第31回大会

４．発表年
2022年

１．発表者名
Momonari Kudo and Shushi Harashita

２．発表標題
Parametrizing generic curves of genus five and its application to finding curves with many rational points

３．学会等名
MEGA 2021: Effective Methods in Algebraic Geometry（国際学会）

４．発表年
2021年

１．発表者名
大橋亮，工藤桃成，原下秀士

２．発表標題
The a-numbers of non-hyperelliptic curves of genus three with large cyclic automorphism group

３．学会等名
日本数学会2022年度年会

４．発表年
2022年

１．発表者名
工藤桃成，原下秀士

２．発表標題
種数5の非超楕円曲線を定義する方程式の明示的構成とその応用

３．学会等名
日本応用数理学会2021年年会 「数論アルゴリズムとその応用」(JANT) セッション

４．発表年
2021年

１．発表者名
工藤桃成

２．発表標題
Parametrizing generic curves of genus five and its application to finding curves with many rational points

３．学会等名
九州代数的整数論2021夏

４．発表年
2021年

１．発表者名
工藤桃成，原下秀士

２．発表標題
Parametrizing generic curves of genus five and its application to finding curves with many rational points

３．学会等名
日本数学会2021年度秋季総合分科会

４．発表年
2021年

１．発表者名
Momonari Kudo and Shushi Harashita

２．発表標題
Genus-five hyperelliptic or trigonal curves with many rational points in characteristic three

３．学会等名
8th International Conference on Mathematics and Computing (ICMC 2022)

４．発表年
2022年

１．発表者名
工藤桃成

２．発表標題
計算代数幾何入門 - 暗号解読および代数曲線論への応用事例とともに

３．学会等名
2021年度第8回九州大学マス・フォア・イノベーション・セミナー（招待講演）

４．発表年
2022年

１．発表者名
Momonari Kudo, Shushi Harashita, Everett Howe

２．発表標題
Algorithms to enumerate superspecial Howe curves of genus four

３．学会等名
Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV)（国際学会）

４．発表年
2020年

１．発表者名
工藤桃成

２．発表標題
Recent developments in the study on supersingular curves of low genera

３．学会等名
九州代数的整数論2020夏 on Zoom（招待講演）

４．発表年
2020年

１．発表者名
Momonari Kudo, Shushi Harashita, Everett Howe

２．発表標題
Efficient algorithms for finding and enumerating superspecial Howe curves in much larger characteristic

３．学会等名
日本応用数理学会2020年年会 「数論アルゴリズムとその応用」(JANT) セッション

４．発表年
2020年

１．発表者名
Momonari Kudo

２．発表標題
Counting the isomorphism classes of superspecial curves

３．学会等名
Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties（招待講演）（国際学会）

４．発表年
2020年

１．発表者名
工藤 桃成

２．発表標題
超特異曲線・超特別曲線の明示的構成と関連する計算問題について

３．学会等名
津田塾大学整数論ワークショップ2020（招待講演）

４．発表年
2020年

１．発表者名
工藤桃成, 原下秀士

２．発表標題
計算代数幾何学入門 - 有理点を多くもつ有限体上の代数曲線の構成を通じて

３．学会等名
RIMS共同研究（公開型）「代数的整数論とその周辺」2020（招待講演）

４．発表年
2020年

１．発表者名
工藤桃成

２．発表標題
暗号応用に向けた代数曲線の明示的構成と関連する算術

３．学会等名
第12回 暗号及び情報セキュリティと数学の相関ワークショップ（CRISMATH 2020）（招待講演）

４．発表年
2020年

１．発表者名
工藤桃成

２．発表標題
超特異曲線および超特別曲線に関する最近の話題

３．学会等名
電子情報通信学会九州支部 FIT Student Branch 講演会（招待講演）

４．発表年
2023年

１．発表者名
Momonari Kudo

２．発表標題
Construction of superspecial curves of genus four with extra automorphisms

３．学会等名
10th International Congress on Industrial and Applied Mathematics（ICIAM2023 Tokyo）（招待講演）（国際学会）

４．発表年
2023年

１．発表者名
工藤桃成

２．発表標題
超特別曲線の存在性と数え上げについて

３．学会等名
金沢代数セミナー（招待講演）

４．発表年
2024年

１．発表者名 工藤桃成
２．発表標題 超特別曲線の存在性と数え上げについて
３．学会等名 福工大土曜談話会（招待講演）
４．発表年 2024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
研究協力者	原下　秀士 (Harashita Shushi)		
研究協力者	高島　克幸 (Takashima Katsuyuki)		
研究協力者	安田　雅哉 (Yasuda Masaya)		
研究協力者	横山　和弘 (Yokoyama Kazuhiro)		
研究協力者	高木　剛 (Takagi Tsuyoshi)		

6．研究組織（つづき）

	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
研究協力者	守谷　共起 (Moriya Tomoki)		
研究協力者	大橋　亮 (Ohashi Ryo)		
研究協力者	池松　泰彦 (Ikematsu Yasuhiko)		
研究協力者	古江　弘樹 (Furue Hiroki)		
研究協力者	相川　勇輔 (Aikawa Yusuke)		
研究協力者	深作　亮也 (Fukasaku Ryoya)		
研究協力者	野呂　正行 (Noro Masayuki)		
研究協力者	ハウ　エバレット (Howe Everett)		

6．研究組織（つづき）

	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
研究協力者	神戸　祐太 (Kambe Yuta)		
研究協力者	坂田　康亮 (Sakata Kosuke)		
研究協力者	加藤　拓 (Kato Taku)		
研究協力者	中川　輔 (Nakagawa Tasuku)		
研究協力者	高橋　康 (Takahashi Yasushi)		

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			