立教大学学術推進特別重点資金（立教ＳＦＲ）
大学院学生研究
２０２３年度研究成果報告書

研究科名	立教大学大学院　理学研究科　数学専攻			
研究代表者（2024年3月現在のものを記入）	在籍課程・学年 ☐博士前期課程　年 ☑博士後期課程　2年	氏　名 片山　瑛		
指導教員	所属部局・職名 理学部数学科・教授	氏　名 安田雅哉		
自然・人文・社会の別	(自然)・人文・社会		**個人・共同の別**	(個人)・共同　名
研究課題	有限体上のアーベル多様体の理論的及び計算機的の解析・耐量子計算機暗号の安全性評価			
研究組織（研究代表者・共同研究者）※2024年3月現在のものを記入	在籍研究科・専攻・課程・学年 理学研究科・数学専攻・博士後期課程2年	氏　名 片山　瑛		
研究期間	２０２３　年度			
研究経費（1円単位）	（支出金額）　500,000円　／（採択金額）　500,000円			

研究の概要（200～300字で記入、図・グラフ等は使用しないこと。）

(1)**有限体上のアーベル多様体の理論的及び計算機的解析**:有限体上に定義されたアーベル曲面の不変量は数論幾何学・計算機代数幾何の分野において注目されている対象である。特に本研究においては様々な応用のあるブラウアー群に対して、位数・構造計算を行う。

(2)**耐量子計算機暗号の安全性評価**:近年、量子計算機の発展により現在使われている暗号の危殆化が懸念されており、その対策技術として耐量子計算機暗号と呼ばれる新たな暗号方式の研究が盛んである。本研究では、耐量子計算機暗号のうち、格子理論を基にした方式、同種写像問題を基にした方式の安全性評価・安全性強化に向けた新たなアルゴリズム開発を行う。

キーワード（研究内容をよく表しているものを３項目以内で記入。）

〔アーベル多様体の不変量　〕〔ブラウアー群計算　〕〔耐量子計算機暗号　〕

研究成果の概要（図・グラフ等は使用しないこと。）

(1) **有限体上のアーベル多様体の理論的及び計算機的解析**:

(研究動機)

アーベル多様体とは代数幾何学・数論幾何学上非常に良い性質を持っている数学的対象であり、その応用は多岐に及び、近年では数理物理学や暗号理論などでその重要性が盛んに議論されている。特に一次元のアーベル多様体である楕円曲線は数論幾何学やアーベル多様体論における最も基本的な対象であり、保型形式論や岩澤理論など幅広い応用があり 20 世紀以降さまざまな側面から研究が行われていた。

本年度の成果としては有限体上アーベル曲面のブラウアー群の部分群の構造計算・有限体上の同種な楕円曲線間の同種写像のなす群の構造計算について研究を行った。

(a) 有限体上の同種な通常楕円曲線間の同種写像をなす群の構造の決定・基底計算

有限体上の同種な通常楕円曲線 E, E'に対して、その間の同種写像のなす群$\mathrm{Hom}(E, E')$は、$\mathbb{Z}$-加群として階数 2 の自由加群の構造を持つことが知られている。一方、従来の研究ではどのような写像が$\mathrm{Hom}(E, E')$の生成元となるか、2 つ同種写像が基底となるかの判定手法が知られていなかった。本件では、通常楕円曲線の同種写像のなすグラフ構造が持つ isogeny volcano という構造をうまく活用し、さらに自己準同型環 $\mathrm{End}(E), \mathrm{End}(E')$の作用を考えることで同種写像のなす群の生成元を求めるアルゴリズムの開発、さらに出力結果が生成元であることを確かめる判定法の提案・証明に成功した。また、得られた生成元から線型独立なものを抽出し、$\mathbb{Z}$-基底として得られた生成元から 2 つの同種写像を求める方法を提示した。以上の研究成果を 2023 年 8 月に開催されたキューバにて開催された査読付き国際会議「Computer Algebra in Scientific Computing 2023」(CASC2023)においては「Computing a Basis of Isogeny Groups Between Two Isogenous Ordinary Elliptic Curves over a Finite Field」という題目で extend abstract として投稿・発表を行った。一方、本発表で提案したアルゴリズムは計算量が多いものであったため、より精査したアルゴリズムをまとめ、来年度開催される「International Workshop on the Arithmetic of Finite Fields 2024」(WAIFI2024)にカンファレンスペーパーとして投稿済みである。

(b) 有限体上のアーベル曲面のブラウアー群の位数計算・一部の部分群の構造計算

有限体上のアーベル曲面Xに対して、そのブラウアー群 $\mathrm{Br}(X)$ は 2 次エタールコホモロジー群$H^2_{\text{ét}}(X, \mathbb{G}_m)$として定義される。特に、位数に関しては Artin-Tate の公式と呼ばれるものが知られており、一部のアーベル曲面に対して計算可能であった。しかし、アーベル曲面の不変量の一つである Néron-Severi 群の判別式の計算が困難であったため、汎用的に計算はできなかった。本件の前半では二つの楕円曲線 E, E'の積と同型なアーベル曲面 $X \simeq E \times E'$に対して同種写像のなす群の判別式計算を汎用的に可能にし、公式を導くことで、計算機上でブラウアー群の位数計算を可能にした。本件の後半ではブラウアー群の部分群の構造計算を行った。今回扱った手法としては、エタールコホモロジーだけでなくガロアコホモロジーとの比較や作用を考えることにより、具体的な写像と完全列を構成する。本件では部分群 $H^1(G, \bar{X}) \subset \mathrm{Br}(X)$を同種でない楕円曲線の積の場合に限り計算可能にした。以上の研究成果を査読付き雑誌 JJIAM にて「Computing the Brauer group of the product of two elliptic curves over a finite field」という題目で投稿し、採択された。しかし、今回計算可能になったケースは全て部分群が自明なものとなり、その原因を解明することが次の課題となった。

(c) 有限体上の同種な超特異楕円曲線間の同種写像をなす群の構造の基底計算

最後に第一の結果の発展として、同種な超特異楕円曲線間の同種写像のなす群の基底計算のアルゴリズム開発を行った。超特異楕円曲線間の同種写像に関しては、耐量子計算機暗号に対しても幅広く応用が存在し、現在注目の集まっている分野である。背景として、通常楕円曲線の場合と異なり、2 つの超特異楕円曲線間 E, E'の同種写像のなす群$\mathrm{Hom}(E, E')$は、$\mathbb{Z}$-加群として階数 4 の自由加群の構造を持つことが知られている。特に、その加群の判別式の絶対値は標数pの二乗と一致することを(1-b)にて証明した。この性質を用いることで明示的な基底を計算するためには、(1-a)同様に生成元となるような同種写像を探すことが課題となった。解決手法として Meet-in-the-Middle アルゴリズムを用いることで 2-同種パスと 3-同種パスを与えることで、二つの次数の互いに素であるような 2 つの同種写像が得られ、それらを用いて生成元を出力できるアルゴリズムを考案した。さらに、二つの超特異楕円曲線の j-不変量を与えることで具体的な数値例も出力できるような実装例を提示することができた。これらの研究成果は来年度の CASC2024 において投稿予定である。

研究成果の概要（つづき）

(2) **耐量子計算機暗号の安全性評価:**

(研究動機)

現在、幅広く普及している暗号(RSA,楕円曲線暗号)は量子コンピュータを用いて容易に解読できることが示されている。これに対抗する暗号手法として耐量子計算機暗号の研究が近年盛んである。特に、米国標準技術研究所(NIST)では、耐量子計算機暗号の暗号方式の標準化計画を 2016 年から現在まで進めており、格子理論や同種写像問題などを基にした暗号方式が提案され、いくつかの方式が選定された。

(a)FALCON のマスキング実装

FALCON は NIST により選定された暗号方式のなかで格子理論を基にした署名方式の暗号である。近年、耐量子計算機暗号の攻撃技術として近年 Side-Channel 攻撃が盛んに研究されている。この対策技術としてマスキング実装というものが存在する。マスキング実装とは暗号方式における秘匿情報を分割しそれらの分割された情報間の演算の安全性を強化することにより、攻撃手法を対策するものである。NIST により選定された格子理論ベースの暗号方式に対してマスキング実装の報告があるが、FALCON のみマスキング実装の報告がされていない。

本年度、挑戦した課題として FALCON のマスキング実装の考案について以下の 3 つの技術の研究を行った:

1. FFT 変換時のマスキング技術

従来報告されているマスキング実装は代数的な変換と乱数を用いた安全なノイズを加えることで成り立っている。本件では、秘匿情報の分割と FFT 変換の互換性から乱数を用いたノイズの生成のみが必要であれば良いことがわかった。具体的には FFT 空間の基底と有理数の乱数を用いることによりこの課題を解決することができた。

2. サンプルベクトル生成のマスキング技術

FALCON のサンプルベクトル生成は FALCON 木を用いて生成される。本件ではアルゴリズム全体の分割は行うことは叶わなかったが、本来、情報を分散して計算する手法であったため、最終的にサンプルベクトルを用いて出力する FALCON 木をどのように処理するかが問題となっていた。この解決案として FALCON 木自身も分割し、本来の分散で情報が安全になったところで分割状態から直すという手法を使うことにより、分割されたサンプルベクトルの生成に成功した。

3. ノルム計算時のマスキング技術

本技術の課題として分散されたノルム計算が分割前の情報の演算から得られたノルムと一致する技術を開発することが必要であった。これに対して、元情報の異なる 2 つの分割された情報と線形代数学の基本的な性質である内積によるノルム計算を用いることにより、課題解決に繋げることができた。

以上を本年度の成果として SCIS2024 において「FALCON におけるマスキング実装の提案」として発表を行った。

(b)同種写像暗号の求解法とその応用

耐量子計算機暗号のうち同種写像暗号の攻撃手法とは、有限体上の超特異楕円曲線間の同種写像を求める問題と直結している。この問題の帰結として楕円曲線の自己準同型環が計算可能かというものがある。昨年度、標数が 20bit 以下の基礎体とした有限体に対して超特異楕円曲線の自己準同型計算が可能となった。

本年度、取り組んだ課題としては以下の二つがある:

1. より高い bit の標数を持つ基礎体$\mathbb{F}_p$上の超特異楕円曲線の自己準同型環計算

昨年度までアルゴリズムでネックとなっていたサイクル探索のアルゴリズムに対して depth-search というグラフ構造を応用した技術を埋め込むことにより、より高速に計算が可能になり、また標数が 40-bit の素数に関しても約 3 時間半で計算可能となった。2023 年度現在この計算結果は古典計算機上の計算例として最も早い計算記録となった。

2. 基礎体の二次拡大体$\mathbb{F}_{p^2}$上の超特異楕円曲線の自己準同型環計算

昨年度は素体上超特異楕円曲線の自己準同型環計算が可能であったが、この技術の根幹には素体上でのフロベニウス射が自己準同型環を含む四元数代数の基底に埋め込むことが可能であるという事実に依存している。一方、二次拡大体上定義される超特異楕円曲線はこのようなフロベニウス射は存在しなかったため、四元数代数の元に埋め込む際の基準が足りないという課題があった。この解決案としてトレース計算で得られる不定方程式から埋め込みの基準を 3 つ定めることにより、自己準同型環計算が可能になった。本結果は現在資料としてまとめ来年度に投稿予定である。

※この（様式２）に記入の成果の公表を見合わせる必要がある場合は、その理由及び差控え期間等を記入した調書（Ａ４縦型横書き１枚・自由様式）を添付すること。

研究発表（研究によって得られた研究成果を発表した①～④について、該当するものを記入してください。該当するものが多い場合は主要なものを抜粋してください。なお、成果発表を確認できる資料を合わせて研究成果報告書提出フォームより提出してください（紙媒体等、研究成果報告書提出フォームから提出できない場合は、別途リサーチ・イニシアティブセンターへ提出してください）。

①雑誌論文（著者名、論文標題、雑誌名、巻号、発行年、ページ）
②図書（著者名、出版社、書名、発行年、総ページ数）
③シンポジウム・公開講演会等の開催（会名、開催日、開催場所）
④その他（学会発表、研究報告書の印刷等）
※修士論文・博士論文は含みません。

①雑誌論文

- 査読付き論文(2件)
  1. 「Computing the Brauer group of the product of two elliptic curves over a finite field」, (Authors: Akira Katayama, Masaya Yasuda, 2023, Online First, Japan Journal of Industrial and Applied Mathematics (JJIAM))
  2. 「Computing endomorphism rings of supersingular elliptic curves by finding cycles in concatenated supersingular isogeny graphs」(Authors: Yuta Kambe, Akira Katayama, Yusuke Aikawa, Yuki Ishihara, Masaya Yasuda, Kazuhiro Yokoyama , 2024年採択済み, Commentarii mathematici Universitatis Sancti Pauli)

④その他

- 国内学会(4件):
  1. 「FALCONにおけるマスキング実装の提案」(著者: 片山瑛, 中邑聡史, 上野真奈, 安田雅哉, 2024年1月 SCIS)
  2. 「近似最近ベクトル探索と埋め込み法を用いた格子による素因数分解法の実装報告」(著者: 佐藤新, Auzemery Aurelien, 片山瑛, 安田雅哉, 2024年1月 SCIS)
  3. 「同種写像グラフ上のサイクル探索による同種写像求解法の高効率化」(著者: 神戸祐太, 片山瑛, 相川勇輔, 石原侑樹, 安田雅哉, 横山和弘, 2024年1月 SCIS)
  4. 「超特異楕円曲線の自己準同型環計算とその暗号応用」(著者:片山瑛, 2024年2月 CRESTミニワークショップ)
- 査読付き国際学会(2件)
  1. 「Solving the supersingular isogeny problem over Fp via the Deuring correspondence」, (Authors: Yuta Kambe, Akira Katayama, Yusuke Aikawa, Yuki Ishihara, Masaya Yasuda, Kazuhiro Yokoyama, 2023年8月 MathCrypt2023, Santa Barbara, US)
  2. 「Computing a Basis of Isogeny Groups Between Two Isogenous Ordinary Elliptic Curves over a Finite Field」, (Author: Akira Katayama, 2023年8月 CASC2023, Havana, Cuba)