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 １０ 日現在

機関番号：１２６０８
研究種目：若手研究
研究期間：2021～2023
課題番号：２１Ｋ１７７４０

研究課題名（和文）実用的なペアリング暗号の開発

研究課題名（英文）A Practical Pairing-Based Cryptography

研究代表者
石井　将大（Ishii, Masahiro）

東京工業大学・学術国際情報センター・助教

研究者番号：１０７９４３９９

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：ブロックチェーン技術などへの応用を持つペアリング暗号について，その効率的な構成法を具体的に与えた．特に，ペアリング暗号において扱われる数の正当性を担保するための技術の一つである，楕円曲線の有理点群における群所属判定に関し，ペアリングを構成するパラメータ空間において，群所属判定がいつ・どのように行えるかを簡潔かつ完全に記述した．
結果として，より効率的・実用的なペアリング暗号の構成法が明らかになった．

研究成果の学術的意義や社会的意義
本研究対象のペアリング暗号は，ブロックチェーンや，トラステッド・コンピューティングなど現代・次世代のサイバーセキュリティインフラを支える技術の重要な一構成要素であり，実用化されている．
本研究成果により，効率的かつ安全なペアリング暗号の具体的な構成法が与えられ，特にペアリングが関係する暗号アプリケーションの設計者・実装者が，迷わずより適した暗号のパラメータと構成の選択が可能となった．
さらに，楕円曲線の暗号に適した新たな性質を解明し，学術的な貢献も果たした．

研究成果の概要（英文）：We presented a concrete and efficient method for constructing pairing-based cryptography, which can be applied to technologies such as blockchain. In particular, we concisely and comprehensively described when and how group membership verification in the group of rational points on an elliptic curve, a technique to ensure the validity of numbers handled in pairing-based cryptography, can be performed within the parameter space for constructing pairings.
As a result, a more efficient and practical method for constructing pairing-based cryptography has been elucidated.

研究分野：情報セキュリティ

キーワード：ペアリング暗号　ペアリングフレンドリ楕円曲線族　群所属判定問題　余因子消去　同種写像　分散処理基盤

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

ペアリングを利用した暗号アプリケーションの実用化が進み，主要な構成要素であるペアリングに適した楕円曲線についても盛んな標準化活動が見られる．ただし，最適なペアリングを構成するために，楕円曲線や安全性パラメータ，計算アルゴリズムなど多岐に渡る構成要素に対して最適解を見つけることは非常に困難である．

また，近年の離散対数問題を解くアルゴリズムの進化による安全性の見直しにより，現在では利用すべき楕円曲線やペアリングの構成法の新たな候補が乱立し，ペアリングの安全性や効率化手法の詳細な整理がなされていない状態である．この様な状況では，ペアリング暗号の設計において利用者・実装者がペアリングの構成法や，安全性パラメータ，暗号ライブラリを適切に選定することは不可能である．

２．研究の目的

本研究の目的は，効率的なペアリングベース暗号に寄与するペアリングとその構成法の提案と，適切な暗号パラメータ探索を行い，その成果をペアリング暗号の利用者・実装者に提供することである．具体的には以下の研究課題（1)～(3）の解決を試みた．

1)　詳細な安全性解析と効率的な曲線族，楕円曲線モデル，ペアリング構成法の提案，
2)　ペアリングベース暗号の安全性，効率性を向上させるペアリングパラメータの探索，
3)　実用的なペアリングの実証と，その結果や構成要素の詳細を提供する基盤の構築．

３．研究の方法

研究課題（1),(2）について，本研究では特に楕円曲線の自己準同型環など背景にある数学的理論を整理・分析し，ペアリング暗号に適した様々な曲線族に対する安全かつ効率的なパラメータとその探索法を示す．

研究課題（3）については，課題（1),(2）において明らかにした効率的なペアリングと暗号アプリケーションの実証を行うための基盤を，Docker，Kubernetes によるコンテナ運用管理技術を用いて構築を進めている．これにより，パラメータや構成法，計算アルゴリズムの詳細，有限体上のオペレーションカウント，GMP 等のスタンダードな公開ライブラリによる実際の実行環境における計算コスト，ベンチマーク結果等のデータベース化し，提供することを予定している．

４．研究成果

研究課題（2）の解決のために，特にペアリング暗号において扱われる数の正当性を担保するための技術の一つである，楕円曲線の有理点群における群所属判定の効率化に取り組んだ．効率的なペアリングを構成する際によく利用される楕円曲線族をより包括的に扱い，各曲線族における群所属判定手法と，背景にある数学的理論を整理し，群所属判定が曲線族の性質を用いてどのように記述されるかを明らかにした．

具体的には，群所属判定を行うための条件を理論的に厳密に決定し，楕円曲線の自己準同型環とあるイデアルの性質を利用して表現した．これにより，あるペアリングフレンドリ曲線族に対し，ペアリングを構成するパラメータ空間において，群所属判定がいつ・どのように行えるかを簡潔かつ完全に記述できるようになった．

さらに，いくつかの曲線族に対して先行研究と比較してより効率的な群所属判定法を示し，また，先行研究の手法ではあらゆるパラメータには対応できない不十分な判定法の記述を修正することができた．

これらの成果を国内会議 SCIS2022 [引用文献⑤] で速報的に報告した．現在研究対象を更に拡張した結果と，余因子消去についても理論的な成果をまとめ，国際誌への論文投稿準備を行っている．

また，楕円曲線間の同種写像に着目し，ペアリングフレンドリ曲線のみならず，同種写像によって移り合うより広範の楕円曲線を対象とし，安全かつ効率的なペアリングの構成に寄与する曲線やパラメータ探索を行うため，同種写像の性質についても分析を行った．

近年耐量子計算機暗号の一つの候補として注目を浴びている，楕円曲線，あるいはそれらを組み合わせた多様体を含む，より高次のアーベル多様体に対して定義される同種写像を利用した同種写像暗号の研究を進めた．具体的な成果として，アーベル多様体間の同種写像を計算するための explicit formulae の効率化と，楕円曲線を含む超楕円曲線間の同型写像について，具体的なその変換を求めるための手法について分析し，得られた部分的な成果を報告した [引用文献①,③,④]．

楕円曲線上のペアリング暗号においても，曲線の異なる定義式のタイプやモデルについて分析し，ペアリング暗号の効率化を図る必要があり，曲線間の同型 変換の詳細な性質を明らかにすることには意味があり，研究課題（1）の部分的な解決につながる．

本研究で扱うペアリングフレンドリ楕円曲線族は，ブロックチェーン技術など実社会で応用されるものも対象とし，最近提案された曲線に対する分析も追加で行った．安全かつ効率的なペ

アリングの構成に寄与する曲線について，その具体的な定義式やパラメータの探索を効率的に行うため，数式処理システム・暗号計算ライブ ラリを活用した並列分散処理基盤の構築を行っている．具体的にプロトタイプとして，コンテナ技術として Docker，コンテナオーケストレーションシステムとして Kubernetes を活用し，特に多数の複雑な代数演算の分散処理を行うフレームワークの構築を進めている．

このようなコンテナクラスタによる計算基盤構築を [引用文献②] においても進めており，本成果で得られた基本設計とデプロイ・運用技術を活用し，暗号の開発・計算環境に必要な機能の追加を行っている．暗号パラメータの探索支援や，より効率的な安全性解析のための基盤構築として，コンテナオーケストレーション技術を活用した，さらなるタスク処理・ 計算リソース配分の最適化が直近の課題となる．

上記の課題を解決し，特に研究課題（2）への取り組みで得られた部分群所属判定と余因子消去の手法による具体的なパラメータ決定法を用いて，効率的なペアリングの構成を示し，速やかに研究課題（3）を解決する予定である．

＜引用文献＞

① M. Ishii and D. Hayashida: An Optimization for Efficient Computation of Multi-radical (3,3)-isogenies on Jacobians, Mathematical Foundations for Post-Quantum Cryptography: Crypto-Math CREST, 2024 年 7 月出版予定
② 渋谷聡志，石井将大，田中圭介：暗号化通信におけるマイニング検知，2024 年暗号と情報セキュリティシンポジウム（SCIS2024），2024 年 1 月
③ 林田大輝，石井将大：同種写像暗号における超楕円曲線間の同型写像計算コストについて，信学技報，vol．122，no．428，ISEC2022-56，pp．61-67，2023 年 3 月
④ 林田大輝，石井将大：アーベル曲面上の同種写像計算の explicit formulae に関する一考察，信学技報，vol．121，no．429，ISEC2021-69，pp．122-129，2022 年 3 月
⑤ 安田貴徳，石井将大，照屋唯紀：ペアリング高速計算に適した楕円曲線における群所属判定，2022 年暗号と情報セキュリティシンポジウム（SCIS2022），2022 年 1 月

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計4件（うち招待講演　0件／うち国際学会　0件）

１．発表者名
林田 大輝，石井 将大

２．発表標題
同種写像暗号における超楕円曲線間の同型写像計算コストについて

３．学会等名
ISEC・IT・RCC・WBS合同研究会（2023年3月）

４．発表年
2023年

１．発表者名
林田 大輝，石井 将大

２．発表標題
アーベル曲面上の同種写像計算のexplicit formulaeに関する一考察

３．学会等名
ISEC・IT・RCC・WBS合同研究会（2022年3月）

４．発表年
2022年

１．発表者名
安田 貴徳，石井 将大，照屋 唯紀

２．発表標題
ペアリング高速計算に適した楕円曲線における群所属判定

３．学会等名
2022年暗号と情報セキュリティシンポジウム（SCIS2022）

４．発表年
2022年

１．発表者名
渋谷聡志，石井将大，田中圭介

２．発表標題
暗号化通信におけるマイニング検知

３．学会等名
2024年暗号と情報セキュリティシンポジウム（SCIS2024）

４．発表年
2024年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

[書籍掲載論文] M. Ishii and D. Hayashida: An Optimization for Efficient Computation of Multi-radical (3,3)-isogenies on Jacobians, Mathematical Foundations for Post-Quantum Cryptography: Crypto-Math CREST, Mathematics for Industry, Springer Singapore, 2024年7月出版予定

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