様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　６　月　１６　日現在

機関番号：　２３５０１
研究種目：　若手研究(B)
研究期間：　2014～2015
課題番号：　２６８７０４８６

研究課題名（和文）ペアリングに基づいた暗号系に適した楕円曲線および超楕円曲線の構成研究

研究課題名（英文）Study of construction of pairing-friendly elliptic curves and hyper elliptic curves

研究代表者
岡野　恵司（Okano, Keiji）

都留文科大学・文学部・講師

研究者番号：７０４５４０２２

交付決定額（研究期間全体）：（直接経費）　　1,100,000円

研究成果の概要（和文）：楕円曲線のペアリングを用いた公開鍵暗号系では，ペアリング暗号に適した特別な楕円曲線または超楕円曲線が必要となる．ペアリング暗号に適した楕円曲線の完全族について，「理想的な族」となるための条件に関する結果として，以下の結果を得た．
(1) 埋め込み次数が 3，4，6 の場合には理想的な楕円曲線の完全族は存在しない．
(2) 埋め込み次数が 8 または 12 のとき，非円分的な場合を含めた多くの場合について，理想的な楕円曲線の完全族は存在しない．

研究成果の概要（英文）：Pairing-based cryptographic schemes require elliptic or hyperelliptic curves with special properties. In this research, we study the condition that complete families of such curves are ideal, and we give the followings:
(1) There are no ideal complete families of pairing-friendly elliptic curves with embedding degree 3, 4, or 6.
(2) Many complete families, including non-cyclotomic case, of pairing-friendly elliptic curves the embedding degree 8 or 12 are non-ideal.

研究分野：　代数学

キーワード：　ペアリングを用いた公開鍵暗号系　楕円曲線　埋め込み次数

１．研究開始当初の背景

公開鍵暗号の一つである，有限体上の楕円曲線のペアリングを用いた公開鍵暗号系は，個人情報を暗号鍵として用いる ID-based 暗号などの方式に広く応用されており，従来の RSA 暗号などの暗号系に比べて利便性が高いと考えられている．この暗号方式の特徴の一つとして，任意の曲線が利用可能な楕円 ElGamal 暗号とは異なり，暗号に適した曲線（pairing-friendly 楕円曲線）を用意する必要があるということが挙げられる．その適切条件の一つである，ペアリングの像を含む最小の拡大体と楕円曲線の基礎体との間の拡大次数は，埋め込み次数とよばれ，ペアリング計算が効率的に実行できるかどうかを反映する重要な値となる．十分小さい各埋め込み次数について，より適した楕円曲線を構成することが，この分野の研究課題である．現在では，一度により多くの楕円曲線を構成するために，CM-法によって構成するのに必要なすべての値をパラメータ x の多項式で表現した,「pairing-friendly 楕円曲線の完全族(complete family)」とよばれる族を構成する方法がいくつか提案されている．各 pairing-friendly 楕円曲線対して，どの程度暗号に適しているかを表す値 ρ が定義される．この値が 1 に近いほど暗号として良いとされ，特に $\rho=1$ である場合は，楕円曲線の有理点と暗号に用いる部分群がほぼ一致することを意味し，理想的であるとされる．しかし，現在のところ $\rho=1$ となる pairing-friendly 楕円曲線の完全族は，Barreto-Naehrig による族のただ一つの例しか知られていない．

また最近では，超楕円曲線のペアリングに基づいた暗号研究が盛んに行なわれており，この場合でも ρ が同様に定義される．しかし，その研究は楕円曲線の場合に比べて十分とは言いがたいものであった．

２．研究の目的

現在まで，理想的条件 $\rho=1$ を満たす pairing-friendly 楕円曲線の完全族は唯一つの例しか知られていない．効率的，理論的に 1 に近い ρ を求める方法も，十分確立しているとはいえない．これは，暗号に用いるという実用的観点からみても，また素数位数をもつ楕円曲線の構成という数学的興味の対象としても，着手すべき大きな問題の一つだと思われる．また楕円曲線に対して $\rho=1$ となる族を探す手法を，超楕円曲線に対しても応用することができれば，この方面に関する研究が進展する可能性がある．そこで本研究では，以下のような問題に取り組む．

(1) 埋め込み次数が小さい場合について，ρ が 1 となる条件を完全に決定する．
(2) 一般に $\rho=1$ となることは非常に起こりにくいが，それに近い値をとるものを大量に作ることを目指す．
(3) 超楕円曲線の完全族に対しては，$\rho=2$ の例の存在・非存在について，楕円曲線のときに用いた手法を使って探る．

これらは暗号とは切り離して，純粋な数学の問題として定式化される．

３．研究の方法

既存の研究―構成アルゴリズムを提案して計算機を走らせることによって ρ が小さい値をもつ族を探す手法―とは異なり，数学的理論から $\rho=1$ となる可能性を探るのが本研究の特徴である．本研究は以下の 4 つを中心に行う：

(1) 最も基本的な例である，埋め込み次数が 3,4,6 の場合の完全族を扱い，この場合の ρ が 1 となる条件を完全に決定する．

この考察は，既に得られていた円分的(cyclotomic)完全族（部分群を生成する多項式として円分多項式を用いる，最も標準的な構成方法）に対する結果の一般化である．

(2) 埋め込み次数が比較的小さい場合について，同様に ρ が 1 となる条件を決定する．

Barreto-Naehrig(2006) により構成された BN-曲線族と呼ばれる完全族は，$\rho=1$ を満たす唯一の完全族であるが，これは非円分的(sporadic)完全族（部分群を生成する多項式として一般の既約多項式を用いる)ものである．非円分的完全族における理論的研究は，計算機を用いた実験的研究に比べるとほとんどない．小さい埋め込み次数を考察することで，BN-曲線の特徴づけや，その特徴を手掛かりに $\rho=1$ の完全族の存在性を探る．

(3) 様々な埋め込み次数に対して，ρ が十分 1 に近い値をとるようなペアリングに適した楕円曲線の完全族を，理論的に構成する方法を探る．

例えば円分多項式や，冪基底を根にもつ多項式を用いた場合に，Galois 群の作用や代数体の定義多項式を取り換えることによって，暗号に適する楕円曲線族を測るパラメータ ρ がどのように変化するかを探る．この研究に対しては，例えば CM 法に必要な方程式の解は Gauss 和で表示可能であるという事実からも推察できるように，整数論の知識が大いに活用できると期待できる．理論の検証と実例を得るため，計算機による実験も行っていく．

(4) 超楕円曲線に対し，現在得られている ρ の最良値がベストなものか調べる

非完全族(sparse family)の場合には $\rho=2$ となる例が，完全族に対しては $\rho \geq 2$ の例が見つかっている．楕円曲線の非完全族に対しては，$\rho=1$ となる例が存在し，Karabina-Teske によるこれらの楕円曲線の分類結果が知られている．$\rho=2$ となる非完全族な超楕円曲線族の例に対して，この類似を行う．一方，完全族においては，現在まで $\rho=2$ の例が見つかっていないことから，$\rho \leqq 2$ となる超楕円曲線の完全族は存在する

かという問題に取り組む.

４．研究成果

様々な埋め込み次数に対して構成されるペアリングに適した楕円曲線の完全族について, 理想的条件である $\rho=1$ となるものがあるか否かについて研究した.

2014 年度では，埋め込み次数が 3,4,6 の場合の完全族を扱い，もっとも一般的な状況の下で「$\rho=1$ となる完全族は存在しない」ということを証明した．埋め込み次数が 1,2 の場合は同様の結果が知られているので，これでオイラーの φ 関数が 2 以下となる場合には理想的完全族が存在しないことがいえたことになる．非完全族の場合には埋め込み次数が 3,4,6 の場合に，$\rho=1$ となる宮地-中林-高野の例が知られているので，この結果は完全・非完全の比較対象例としても興味ある結果となった.

次に埋め込み次数 8,12 に関する考察を行った．先行研究により，この埋め込み次数については円分的完全族のほとんどの場合において $\rho\neq1$ であることが分かっている．一方で $\rho=1$ を満たす完全族である BN-曲線族は埋め込み次数 12 をもつから，この埋め込み次数に関する考察は非常に興味深いものであるといえる．この埋め込み次数に関して，円分的・非円分的に関わらず CM-判別式が特別な場合に，ある仮定の下では「$\rho=1$ となる完全族は存在しない」ということを証明した．BN-曲線族は非円分的であって CM-判別式が特別な場合である．しかし最後の“ある仮定”が満たされていないので，この結果から，BN-曲線族以外の曲線族は ρ が 1 にはなり得ないのではないか，という予想が考えられ，その最初の根拠となった.

2016 年度は，上記の結果について CM-判別式の仮定を外した場合や，オイラーの φ 関数が同じ 4 となる埋め込み次数である 5,10 の場合について考察を行った．しかし，この場合はまだ解決に至っていない．その原因として，CM-判別式を変えるごとに考察すべき代数体が変わってしまい，その定義多項式も統一的に扱うことが難しいことが挙げられる．そこで後半はここまでの研究成果をまとめ，2015 年 12 月に第 11 回「代数学と計算」研究集会 (AC2015)，2016 年 3 月に日本応用数理学会・研究部会連合発表会で講演を行った．現在，その結果をまとめた論文を査読付き雑誌に投稿中である．すでに Web 上の arXiv に投稿済みであり，国内外の応用数学者のみならず純粋数学の分野からも多数の意見を受けており，一連の研究結果は十分なインパクトをもっていると考えられる.

次の研究として，「様々な埋め込み次数に対して，ρ が十分 1 に近い値をとるペアリングに適した楕円曲線の完全族の構成」の研究に取り組んだ．現在までに，既に知られている完全族から同様の完全族を構成する(例えば BN-曲線族から似たような曲線族を構成する)方法の理論的手掛かりが得られている．実際に計算機を用いて，一つの楕円曲線族から同様の性質をもつ楕円曲線族を構成する方法を得た．しかし，現時点では，十分な応用方面への見込みと満足のできる一般的拡張が得られておらず，今後は応用方面と計算機学に詳しい研究者と共に，アルゴリズムの計算量，暗号の安全性等の研究を進めていく予定である.

研究開始のもう一つの目標であった超楕円曲線に関する類似性を調べる研究は，期間中に十分な成果を得ることができなかった．超楕円曲線の完全族に対しては，今までの研究手法を応用する手法が見いだせず，未だ十分な結果が得られていない．この方面の研究に関しては，他の研究者と協力して新たな研究手法の糸口を見つける方針である.

一連の研究により，一つの予想として「BN-曲線族以外の完全族は ρ が 1 にはなり得ないのではないか」という問題が新たに持ち上がった．今後の研究課題としては，まず以前の円分的完全族に関する論文において，技巧的理由により付けざるを得なかった仮定を外すことがある．これができれば，少なくとも円分多項式を用いた構成に関してこの予想が広い範囲で成り立つことが実証され，予想の大きな根拠になり得る．さらに，埋め込み次数のオイラーの φ 関数が 4 となる 5,10 を含め，今回の埋め込み次数 8,12 の結果を，より拡張することを目指す．また上記でも挙げた現在進行中の，既に知られている完全族から同様の完全族を構成する手法をより洗練していく．さらに超楕円曲線に関する研究は，期間中には十分に行われなかった．研究方法の欄で述べたような研究を今後も進めていく予定である.

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 1 件）

① 岡野 恵司,「ペアリング暗号に適した楕円曲線族が理想的条件をもつ可能性について」, Proceedings of Algebra and Computation 2015, 査読無, 1 巻, 2016, 162--173.

〔学会発表〕（計 2 件）

① 岡野 恵司,「小さい埋め込み次数をもつ理想的なペアリングフレンドリー完全楕円曲線族の存在性について」, 日本応用数理学会 2016 年研究部会連合発表会, 2016 年 3 月 5 日, 神戸学院大学 (兵庫県).

② 岡野 恵司,「ペアリング暗号に適した楕円曲線族が理想的条件をもつ可能性について」, 第 11 回「代数学と計算」研究集会 (AC2015), 2015 年 12 月 16 日, 首都大学東京 (東京都).

〔図書〕（計　0　件）

〔産業財産権〕
○出願状況（計　0　件）

○取得状況（計　0　件）

〔その他〕
ホームページ等
なし

６．研究組織
(1) 研究代表者
岡野 恵司（OKANO, Keiji）
都留文科大学・文学部・講師
研究者番号：70454022

(2) 研究分担者
なし

(3) 連携研究者
なし