様式 C-19

科学研究費補助金研究成果報告書

平成　23　年　5　月　27　日現在

機関番号：２４４０３
研究種目：基盤研究（Ｃ）
研究期間：2008 ～ 2010
課題番号：２０５０００１８
研究課題名（和文）　楕円、超楕円曲線暗号に適した曲線について

研究課題名（英文）　On the suitable curves for elliptic and hyperelliptic curve cryptography

研究代表者
高橋　哲也（TAKAHASHI TETUSYA）
大阪府立大学・総合教育研究機構・教授
研究者番号：２０２１２０１１

研究成果の概要（和文）：y^2=x^5 +ax, y^2=x^5 +a という形の種数 2 の超楕円曲線、y^2=x^9+ax という形の種数 4 の超楕円曲線について、位数公式を使って、ペアリング暗号に適した曲線を任意の埋め込み次数に対して数多く生成することに成功した。
研究成果の概要（英文）：　We construct many paring-friendly genus 2 hyperelliptic curves of the form y^2=x^5+ ax, y^2=x^5+a and genus 4 hyperelliptic curves of the form y^2=x^9+ax by using the closed point counting formula of the Jacobian of these hyperelliptic curves.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,400,000	420,000	1,820,000
2009 年度	500,000	150,000	650,000
2010 年度	800,000	240,000	1,040,000
年度			
年度			
総　計	2,700,000	810,000	3,510,000

研究分野：代数学
科研費の分科・細目：情報学・情報学基礎
キーワード：楕円曲線暗号、超楕円曲線暗号、ペアリング暗号

１．研究開始当初の背景

公開鍵暗号は、20 世紀には、大きな数の素因数分解が計算量的に困難であることに安全の根拠をおく RSA 暗号や、有限体の乗法群の離散対数問題が計算量的に困難であることに安全の根拠をおく ElGamal 暗号などが使われてきたが、これらの暗号は解読アルゴリズムが準指数関数時間であることより長い鍵長が必要であり、解読アルゴリズムに指数関数時間がかかる有限体上の楕円曲線の有理点のなす群での離散対数問題の困難性に安全性の根拠をもつ楕円曲線暗号が 1990 年代から注目を集め、様々な場所で実際に使われていた。また、楕円曲線暗号は、Weil ペアリング（Tate ペアリング）を用いることによって ID-Based　暗号が実現できることで、その重要性が更に高まっていた。また、ペアリングを用いた ID-based の暗号系に使用する楕円曲線については、その研究はまだ始まったばかりであり、さまざまなプロトコルが考案されはじめている状況であった。それに適した曲線を数多く構成する方法を研究していく必要があったともに、楕円曲線の代わりに超楕円曲線を用いる超楕円曲線暗号は、楕円曲線と加算の速度が変わらないことや、ペアリングを用いて、ID-based 暗号にも使えることなどから、ここ数年、急速に研究が進展しているが、位数計算が困難であるといった問題点も抱えたままであった。

２．研究の目的

本研究の目的は、楕円曲線暗号・超楕円曲線暗号に適した楕円曲線、超楕円曲線について

の条件をチェックし、それらに適した楕円曲線、超楕円曲線を生成することである。以下、具体的な目的について個別テーマにしたがって述べる。

(1) ペアリングを用いた暗号に適した楕円曲線の生成

ペアリングを用いた暗号に適した曲線の構成には、楕円曲線暗号の位数 l 、ペアリングを用いて埋め込む有限体の位数 q^k 、(q が定義体の位数、k を埋め込み次数と呼ぶ)について、l が 160 bit 以 上の素数を含み、qk が 1024 bit 以上となるといった条件があるが、楕円曲線の加算のコストを抑える ためには、$\rho = \log q / \log l$ をできるだけ小さく押える必要もある。現在、このような目的を満たす楕円曲線としては、埋め込み次数が 6 以下の場合は、超特異楕円曲線しかペアリングを用いた暗号には使えないことが分かっており(MNT 法)、楕円曲線暗号自体の安全性についても検証する必要がある。一般の ordinary な楕円曲線については、ρ の値を考慮しなければ Cocks-Pinch 法 が一般的な構成法を与えているが ρ が 2 を超える。この ρ を小さくする研究は、一般の k に対しては、l を円分多項式の形で与える Brezing-Weng 法のアイデアが中心となっている。当時、Freeman が Brezing-Weng 法を拡張して、全ての $k > 12$ に対して、ρ を今までの結果より改良するアルゴリズムを提案した。しかし、この方法にも l を与える多項式の次数が大きいという欠点があり、実際に使える曲線はなかなか構成できなかったのでこれを、改良することを目指す。また、ペアリングを用いた暗号のための楕円曲線を CM 法を用いて計算している現在の方法は、特に、CM 体の判別式が小さい場合は将来的に安全性に不安があるので、CM 法を用いない構成か、CM 法を用いても判別式を大きくしながら ρ の値を保つような曲線を探索する。更に、Eurocrypt 2006 においてCheon が Short Signature など のペアリングを用いた暗号の安全性の根拠に用いられる q-weak (strong) Diffie-Hellman 問題を効率的の解くアルゴリズムが提唱され、Pairing 2007 において松尾らによって、より結果が改良され、計算時間が √q のオーダーで短くなることが分かっている。この攻撃に対しては、円分多項式で l を与える 方法は基本的に弱い構造をしているので、これを改良することと、一般に Cheon's アルゴリズムの既 存の構成法に対する影響を調べるとともに Cheon's algorithm に対しての安全性を満たす曲線を組織的に構成することを目指す。

(2) 超楕円曲線暗号の位数計算と超楕円曲線暗号に適した曲線の生成

超楕円曲線は種数 5 以上のときは、Gaudry Attack により、安全性に問題があることが知られている。 また、近年の Teske らの仕事により、種数 3, 4 も安全性が若干落ちることが知られているが、種数 3, 4 では基礎体の位数を 64 ビット以下に取ることができ、曲線上の点の加算に多倍超の演算が必要でないため、加算が高速化できることも知られている。このような状況を考慮し、本研究では種数が 2,3,4 の超楕円曲線について考える。超楕円曲線暗号について、もっとも問題なのは位数の計算が困難であることであった。現在は、虚数乗法を持つ超楕円曲線について、位数を求めているがこれも一般には出来ていない状況である。本研究では、特定の虚数乗法を持つ超楕円曲線に対して位数を公式の形で求めることによって、超楕円曲線暗号に適した曲線を大量に供給できるようにすることを目指す。

(3) ペアリングを用いた超楕円曲線暗号についての研究

超楕円曲線についてもペアリングを用いてID-based 暗号を実現できるが、現状ではペアリングを用いた暗号に使える超楕円曲線の例が少なく、ペアリングについての計算量も大きいので実際の使用は困難である。一方、実際に構成ができれば、多倍超演算が不要になることから演算の大幅なスピードアップが期待できることから種数 3,4 の超楕円曲線についての研究を進めることは重要である。ここでは、特別な超楕円曲線、特に、種数 3,4 で位数が計算可能な超楕円曲線の中で、ペアリングを用いた暗号に利用できる超楕円曲線を構成することと、楕円曲線同様、ρ の値を押さえることが実用には欠かせないので、ρ の値が小さな超楕円曲線を系統的に構成することを目的とする。

３．研究の方法

本研究は、代数学の楕円曲線、超楕円曲線を含む代数曲線、特に有限体上の代数曲線に関する様々な知見を用いて楕円、超楕円曲線暗号に適した曲線の生成、安全性の検証を目指すものであり、理論上想定される仮説を計算機上の実験を繰り返して得られるデータから検証し、それを数学的に証明していく という、「実験数学」の手法により、帰納と演繹を繰り返すという方法で研究を進めていく。以下、研究目的に示した具体的な項目ごとに、研究方法について記述する。

(1) ペアリングを用いた暗号に適した楕円曲線の生成

Cheon's algorithm の与える影響について、

計算機でデータを集めて分析し、必要 な対策を考えることにあてる。ペアリングを用いた暗号に用いる楕円曲線の生成のために、もっとも 重要なのは「埋め込み次数」であるが、その他にも実際の暗号の使用にあたっては、 楕円曲線の位数 l と定義体の有限体の位数 q の比 ρ 、l を多項式で与える場合には、その多項式の次数 r が重要である。これまでは、ρ の値のみが注目され r の値はそれほど問題にされてこなかった。しかし、簡単な計算機実験で、r が大きいと、Cheon’s algorithm に対する安全性を考慮すると、実際に暗号に使える曲線はほとんど出てこないことが分かってきた。このような状況を改善するために ρ の値を保ったまな、r を小さくする方法について考える。これまでのところ、埋め込み次数 k=2n に 対して n が素数で 4 を法として 1 という制限をつければ、r をこれまで知られている Freeman の結果より、小さくできることが分かっているが、これを、一般の n に対して、虚2次体の取り方を変えることで実現できるかを検討する。上記の方法で、うまくいかない場合にはまた、Cheon’s algorithm を Cocks-Pinch タイプを除く、これまでの全ての Paring を用いた楕円曲線暗号について適用し、Short signature のような、Cheon’s algorithm が適用可能なタイプの暗号の安全性を計算機によりチェックし、虚 2 次体、l を与える多項式の両方を変更して、適切な曲線を見つけ、その特徴を一般化するという方法をとる。また、Cocks-Pinch 法は、Cheon’s algorithm に影響されない曲線を与え得る唯一の一般的な方法であるが、ρ は常に 2 より大きくなってしまうという欠点も抱えているので、ρ が多少大きくても、Cheon’s algorithm に影響を受けにくい Brezing-Weng タイプのアルゴリズムを多項式の形を円分多項式以外をとること、あるいは、円分多項式でも拡大次数を最適化しない方法で取ることも検討する。

(2) 超楕円曲線暗号の位数計算と超楕円曲線暗号に適した曲線の生成

位数計算については、一般の超楕円曲線の位数を計算することを目指すのではなく、特定の形、例えば y^2 = x^(2g) + ax + b のような超楕円曲線の位数を計算する。この場合、ある程度具体的な公式が立てられる可能性があるので、まず有限体の位数 p が比較的小さなところで計算機での実験を行う。実際には、Hasse-Witt 行列と 2 項係数の計算でほとんどできると予想される。特に、種数 3,4 について、 パラメータ付きの曲線群の位数を計算できると超楕円曲線暗号に適した曲線を生成できる可能性がある。

(3) ペアリングを用いた超楕円曲線暗号についての研究

ペアリングを用いた種数 2 以上の超楕円曲線暗号の研究は始まったばかりであり、Freeman が実際に使える曲線をいくつか生成しているぐらいであった。パラメータが増えるとそのままでは扱いが難しいので、y^2 = x^(2g)+1 + a x^i + b のような項数が少ない曲線について、埋め込み次数が小さくなる族を探すことから着手した。

以上の全ての研究において、計算機によるシミュレーションが必須であり、1 台は高速なコンピュー タが必要である。また、数式処理ソフトとして Magma がさまざまな数論、代数幾何アルゴリズムが 高速に実装されており、代数曲線暗号の研究には欠かせないものとなってきているので、これを利用した。

４．研究成果

本研究の最大の成果は、y^2=x^5 +ax, y^2=x^5 +a という形の種数 2 の超楕円曲線、y^2=x^9+ax という形の種数 4 の超楕円曲線について、位数公式を使って、ペアリング暗号に適した曲線を任意の埋め込み次数に対して数多く生成することに成功したことである。

目的の個別テーマごとに以下詳述する。

(1) ペアリングを用いた暗号に適した楕円曲線の生成

本テーマについては、計画にしたがって、研究を進めた結果、科研費の補助を受ける以前に、Cheon’s Algorithm に対して、耐性を持った曲線の構成に成功し、補助期間開始前に発表したため、ここでは述べない。

(2) 超楕円曲線暗号の位数計算と超楕円曲線暗号に適した曲線の生成

本テーマについては、y^2=x^5 +a という形の種数 2 の超楕円曲線、y^2=x^9+ax という種数 4 の超楕円曲線に関する位数公式を得て、それを活用して、具体的な曲線の生成を行ったが、これだけでは実用上の価値が乏しく、ペアリング暗号への応用まで含めて、発表に至ったので (3) の部分で合わせて述べる。

(3) ペアリングを用いた超楕円曲線暗号についての研究

研究開始時には、超楕円曲線暗号自体の研究がようやく具体的な曲線について始まったばかりであったが、補助期間中に具体的な成

果となったのは、ペアリング暗号についての応用まで含んだ本テーマであった。以下、具体的な成果について、詳しく述べる。

① ordinary Jacobian を持つ y^2=x^5 + ax の形のペアリングに適した超楕円曲線でρが４以下（k=24 のときは ρが３程度）のものを構成したこと。([1])

超特異(supersingular)でない超楕円曲線(ordinary と呼ばれる)に対してペアリングに適した超楕円曲線の構成は、これ以前に Freeman によってその一般論といくつかの例が得られていたが、本研究では、y^2=x^5+ax の形の超楕円曲線に対して明示的な位数公式を用いて、ρが４以下の超楕円曲線を構成した。これは、一般論でρが８程度であったことからは、画期的な結果であった。
ρが低い具体例
t =1049085
l=14671868289271289365145401996341720272081046900001
p=444292483637841082598410015665493978083277385484222711267571600830352907
a =2
ρ=2.975.

（これ以降、この分野の研究が進み、上記の形の超楕円曲線についても、Kachisa による更なる改良が得られている）

②拡大体で分解しない y^2=x^5+a の形のペアリングに適した超楕円曲線の構成([4])

① の y^2=x^5 +ax は 拡大体で楕円曲線の直積に分解するという点で安全性に関する懸念があった。そのため、拡大体で楕円曲線の直積に分解しない y^2=x^5 +a の形の種数２の超楕円曲線についてペアリング暗号に適した曲線を生成することを検討し、ここでも位数公式を用いることにより成功した。この場合、 ρ が８程度となり、Freeman らによって従来からも知られている結果があったが、Freeman らの結果では、アルゴリズムのループに指数関数回かかる可能性がある部分があり、実際には曲線が見つからないこともあった。位数公式を用いる我々のアルゴリズムは曲線発見のための計算時間が短くなっており、短時間で数多くのペアリングに適した曲線を見つけることに成功している。また、種数 4 の超楕円曲線 y^2=x^9+ax に対しても同様の手法を用いてペアリング暗号に適した曲線の生成することに成功した。

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 4 件）
[1] ”Pairing-friendly hyperelliptic curves with ordinary Jacobians of type y^2 = x^5 +ax”, M.Kawazoe and T. Takahashi, Springer Lecture Notes in Computer Science 5209 ”Pairing 2008”(2008),pp.164-177, 査読あり
[2]”Pairing-friendly Hyperelliptic Curves of Type y^2 = x^5 + c”, A.Comuta, M.Kawazoe and T. Takahashi, Proceedings of the 2009 Symposium on Cryptography and Information Security, 3C4-3, (2009), 査読なし
[3]”Pairing-friendly Hyperelliptic Curves of Type y^2 = x^9 + cx”, A.Comuta, M.Kawazoe, T. Takahashi and I.Yoshizawa, Proceedings of the 2009 Symposium on Cryptography and Information Security, 3C4-4, (2009), 査読なし
[4]”Construction of Pairing-Friendly Hyperelliptic Curves Based on the Closed Formulae of the Order of the Jacobian Group”,A.Comuta, M.Kawazoe, T. Takahashi and I.Yoshizawa, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E93.A (2010), No. 6, pp. 1132-1139, 査読あり

〔学会発表〕（計 4 件）
[1] M,Kawazoe and T.Takahashi, ″Pairing-friendly hyperelliptic curves with ordinary Jacobians of type $y^2=x^5+ax$″, Pairing 2008, 2008.9.2, Royal Holloway, University of London, Egham, UK.
[2] A.Comuta, M.Kawazoe and T. Takahashi “Pairing-friendly Hyperelliptic Curves of Type y^2 = x^5 + c”,Symposium on Cryptography and Information Security 2009,
[3] A.Comuta, M.Kawazoe, T. Takahashi and I.Yoshizawa, ”Pairing-friendly Hyperelliptic Curves of Type y^2 = x^9 + cx”,Symposium on Cryptography and Information Security 2009.

〔その他〕

６．研究組織
(1)研究代表者
高橋 哲也（TAKAHASHI TETSUYA）
大阪府立大学・総合教育研究機構・教授
研究者番号：20212011

(2)研究分担者

川添 充 (KAWAZOE MITSURU)
大阪府立大学・総合教育研究機構・准教授
研究者番号：10295735

(3)連携研究者
(　　)

研究者番号：