様式 C-19

科学研究費補助金研究成果報告書

平成２２年　６月　４日現在

研究種目：若手研究（B）
研究期間：2007～2009
課題番号：19700005
研究課題名（和文）代数曲線とそのペアリング計算の暗号への応用について

研究課題名（英文）Computing pairings on curves and their application to cryptography

研究代表者
金山　直樹（ KANAYAMA NAOKI ）
筑波大学・大学院システム情報工学研究科・研究員
研究者番号：70339696

研究成果の概要（和文）：ユーザの ID 情報を公開鍵とする暗号系で用いられるペアリング関数についての研究を行った．ペアリング関数は楕円曲線と呼ばれる曲線の 2 つの点を入力とし，例えば RSA 暗号などの処理の数倍のコストがかかるが，本研究では，数学的アプローチ・実装手法の最適化などを総動員しいくつかの高速ペアリング計算法を得た．また，ペアリング暗号の安全性の根拠の１つであるペアリング逆問題についての考察も行った．

研究成果の概要（英文）：We researched on pairings over (hyper-)elliptic curves. Pairings are used ID-based cryptosystems. However, pairing computation needs large costs comparing to other cryptosystems. In this research, we gave some efficient pairing computation method. Furthermore, we gave a consideration on pairing inversion problem.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	1,100,000	0	1,100,000
2008 年度	900,000	270,000	1,170,000
2009 年度	1,100,000	330,000	1,430,000
年度			
年度			
総　計	3,100,000	600,000	3,700,000

研究分野：情報学基礎
科研費の分科・細目：情報学・情報学基礎
キーワード：(超)楕円曲線，ペアリング関数，ID ベース暗号，Tate ペアリング，ペアリング逆問題，Miller アルゴリズム

１．研究開始当初の背景

楕円曲線上のペアリングはもともと数学の世界（整数論）で用いられていたが，暗号の分野に現れたのは，楕円曲線暗号への攻撃手段として 1990 年代に Menezes らによって提案されたことがきっかけであった．その時には，攻撃アルゴリズムの計算量が楕円曲線の点の個数のビット長についての準指数時間になっているということが衝撃的で，ペアリングの計算時間が実際どれくらいかと言うことは重要視されていなかった．しかし，その後，2000 年になって境らと Boneh らによって独立に，ペアリングを用いた ID ベース暗号方式が提案されたことによりペアリングが再び注目された．ID ベース鍵暗号とはメールアドレスなどのユーザの ID 情報を暗

号通信の鍵に用いるという画期的な暗号系であるが提案時は原理しか与えられておらず，具体的な構成法は知られていなかった．それが，ペアリングの持つ双線形という性質を用いて初めて実現されたのが Boneh らと境らの方式である．これにより，ペアリングをいかに高速に計算するかという問題が実用上大きな意味を持つようになった．実際に日本でも，産学官連携プロジェクトなどで，暗号への応用を目的としたペアリング計算の研究が行われている．本研究は，このような社会的状況を踏まえて，学術面・実用面両方に貢献する成果を目指すものである．

２．研究の目的

目的の説明のため最小限必要な用語の導入をする．楕円曲線Eとは，その定義方程式が$Y^2+a_1XY+a_3Y=X^3+a_2X^2+a_4X+a_6$という形で，更に各点で一本だけ接線が引けるような曲線で，暗号に用いる場合では各係数a_k (k=1,2,3,4,6) はq元体GF(q)の元とする．楕円曲線Eの点全体の集合に無限遠点∞を加えた集合に対して幾何学的な方法で演算を定義できx座標y座標ともにGF(q)の元であるような点(x,y)の全体(と∞)もまた群をなす(単位元は∞である)．この群をE(GF(q))と書くことにする．S∈E(GF(q))に対して上の演算についてのn倍算をnSと書き，nS=∞となる最小のnをSの位数とよぶ．楕円曲線上のペアリングとは，楕円曲線Eの点で位数がrであるようなP,Qを入力とし１のr乗根を出力とする関数で，第1成分と第2成分両方に対して線形性を持つものである．つまり，整数a,bに対して$e(aP,bQ)=e(P,Q)^{ab}$ を満たす関数をさす．e(P,Q)の値は一般に，楕円曲線の係数の属する体GF(q)の拡大体$GF(q^k)$の元となり，拡大次数kは曲線Eに対して定まる．このkを埋込み次数と呼ぶ．

本研究では具体的に以下のことについて調査をする：

(1)ペアリング計算に適した曲線の探索

ペアリング暗号への応用の観点から見ると，埋込み次数kは大きくないことが望ましい．埋込み次数kが大きくない楕円曲線の代表としてsupersingular楕円曲線があり，それらについてはkは6以下であることが知られている．しかし，それはある意味，supersingular楕円曲線の限界を示しているともいえる．なぜなら，何かの事情である程度大きな（例えば10以上の値の）kを必要とする場合にはsupersingular楕円曲線は適用できないからである．

このような問題に対する対策として，supersingular楕円曲線以外の曲線たちに対しても効率的にペアリングを計算できる方法の確立が有効である．対象となる曲線としては，

・supersingularでない（通常，ordinaryと呼ばれる）楕円曲線

・supersingularな超楕円曲線

がある．ordinary楕円曲線に対しては，埋込み次数kの上限値は無い．そして固定された値kに対してkを埋込み次数として持つ楕円曲線を効率的に生成する方法が宮地ら，Barretoらによって提案されている．supersingularな超楕円曲線の例としては，標数pの有限体上の超楕円曲線$Y^2=X^p-X+d$がpの値に応じて埋込み次数がpまたは2pとなることがDuursma―櫻井によって示されている（この曲線をDS曲線と呼ぶことにする）．これらの曲線は，supersingular楕円曲線に続く「次世代のペアリング用曲線」の有力候補といえる．

しかし，一般には，小さい埋込み次数を持つ楕円曲線の存在比率はかなり小さいことが知られている．そして，supersingular 超楕円曲線についても，有効にペアリング計算ができそうな曲線は今のところ小数しか知られていない．したがって，「ペアリング用曲線」の更なる探索はまだまだ重要な課題である．

(2)ペアリング計算アルゴリズムについての研究

楕円曲線上のペアリングにもいくつか種類があるが，ペアリングを用いた暗号方式が初めて提案された論文で用いていた Weil（ヴェイユ）ペアリングよりも，現在では Tate（テイト）ペアリングを用いるのが主流である．Tate ペアリングの方が，おおむね 2 倍の速さで計算できるからである．その Tate ペアリングの改良として現在知られているのが「η ペアリング」と「Ate ペアリング」である．前者は supersingular な曲線（楕円・超楕円曲線いづれにも適用可能）の，後者は ordinary 楕円曲線の特性を生かして高速化したものである．またその改良として Ate_i ペアリング，R-Ate ペアリング，Optimal ペアリングが提案されている．Ate ペアリングについては，その後，超楕円曲線にまで拡張したものが提案されたが，それ以降のペアリングに対しては Ate ペアリングと同様に構成できると考えられるが，実装例は殆どない．上述の DS 曲線やいくつかの超楕円曲線についてはその特質を生かした高速化が可能と予想されるのでそれを実現することを目標とする．

３．研究の方法

(1)ペアリング計算に適した曲線の探索

上述のように，ペアリングに適した曲線の探索は宮地ら，Barreto らによるもの及びそれらの後続版がいくつか知られているが，本研究ではこれらと視点を変えて，特殊な性質をもつ楕円曲線の探索を試みた．それは，2005 年に Scott の提案した Superoptimal ペ

アリングと呼ばれるペアリングに適した曲線で，曲線上のある準同型写像をもつものである．ある形の楕円曲線については高島による結果があり，本研究では他の形の曲線を対象とする．

(2)ペアリング計算アルゴリズムについての研究

本研究では主に，ある特性を持った超楕円曲線のペアリング計算の高速化に取り組んでいる．超楕円曲線の場合，一般には，曲線の因子と呼ばれる，「曲線の g 個以下の点の組み合わせ」を入力とする．ここで g とは，曲線の種数と呼ばれる曲線固有の量である（楕円曲線は種数１の曲線である）．従って，supersingular な超楕円曲線の場合でも一般には計算が大変であると予想できるが，入力する因子が特別な場合 —— 具体的には，ただ１個の点からなる因子（ここではこれを特殊因子と呼ぶことにする）の場合——にはかなりの高速化が期待される．ペアリング計算が特に高速化を期待できる場合とは，選んだ曲線の任意の特殊因子に対して「特殊因子の n 倍＝（別の）特殊因子」を満たす整数 n が存在する場合である．標数 2 の有限体上種数 2 の曲線（の一つ）についてはηペアリングの提案者が実際に実例を出している．本研究では種数 4 のある超楕円曲線についての検討を行う．

(3)ペアリング逆問題についての研究

ほとんどのペアリング暗号では，楕円曲線上の離散対数問題・有限体の乗法群上の離散対数問題とともにこのペアリング逆問題の計算量的困難性を仮定する．ある楕円曲線 E とその上でのペアリング関数 e(*,*)を固定して考える．有限体の元 z から z=e(P,Q)であるような点 P(または Q あるいは(P,Q)の組)を求める問題をペアリング逆問題と呼ぶ．Tate ペアリング(および Ate ペアリングなど)は通常，Miller のアルゴリズムを実行してから最終べき乗を行うので，Tate ペアリングの逆問題に対しては，「最終べき乗の逆問題」と「Miller アルゴリズムの逆問題」の 2 段階に分けて考えるという素朴なアプローチを考えることができる．

４．研究成果

(1)ペアリング計算に適した曲線の探索

標数 p（大きなビット長の素数）の有限体上で，superoptimal ペアリングと呼ばれるペアリングの計算に向いた楕円曲線の生成方法について考察した．ペアリング計算に適した楕円曲線の形として，Y^2=X^3+aX 型と Y^2=X^3+b 型とがあり，後者については既に考察がなされており，我々は前者の曲線について調べた．既存研究で用いられた手法を Y^2=X^3+aX 型版にアレンジし曲線生成アルゴリズムを実装して数値実験を行った．その結果として，superoptimal ペアリングに適した Y^2=X^3+aX 型曲線の実例を得た．この型の曲線は曲線の有理点群の部分群の位数 r が特殊な形をしているため，曲線の埋め込み次数を多様にコントロールできる事が予想されたが，実際に生成された曲線でもそうなっており，この曲線を用いた superoptimal ペアリングの実用性が期待できる結果となった．

(2)ペアリング計算アルゴリズムについての研究

①種数 4 の超楕円曲線上のペアリングの構成

我々が選んだ種数 4 の超楕円曲線は，標数 2 の有限体上で定義された種数 4 の超楕円曲線 Y^2+Y=X^9+X^5 である．この曲線の基本性質はこの研究のはじまる前にすでに我々自身が得ており，それは以下の通りである：

・超特異曲線である，
・特徴的な形の distortion map をもつ，
・特殊因子の 32 倍はまた特殊因子である
・埋込み次数は 20 である．

これらを利用した高速ペアリング計算の方法を提案した．その第一ステップとして実装の基礎となる 20 次拡大体の基底のとり方について調べた．この基底の取り方は，特に，ペアリング計算の最終ステップである「最終べき乗」操作の効率に大きな影響を及ぼす．我々は，その最終べき乗について最適と思われる基底の候補を得た．次にこの曲線の因子の 32 倍が簡明に表現できることを利用してペアリング計算で用いる Miller のアルゴリズムで行なわれる処理の反復操作の回数を削減する事が可能となった．例えば標数 2 の有限体の元の形で約 1280 ビットのペアリングを計算しようとする場合，楕円曲線(種数 1 の曲線)を用いればペアリング入力とする曲線上の点の座標を約 320 ビット長とせねばならないが，提案法であれば座標は約 64 ビットで十分で，反復回数が約 1/5 に短縮できることがわかった．そして，最初に考えた 20 次拡大体の基底の取り方の下で，ペアリング計算の最終ステップである「最終べき乗」の計算量を評価した．

②DS 曲線上のペアリングの構成

『研究の目的』でも触れた DS 曲線(Duursma – 桜井の曲線)とは標数 p の有限体上で定義された Y^2 = X^p-X+d 型の超楕円曲線で，以下の性質を持っている：

・超特異曲線である，
・特徴的な形の distortion map をもつ，
・被約因子の p 倍公式が非常に扱いやすい形で表現される．

これらはペアリング計算に適した性質で，これらを用いて，DS 曲線上での Tate ペアリングの実装も幾つか成されている．本研究では，2007 年に提案された Optimal ペアリングと呼ばれるペアリングが Duursma-桜井曲線に適

用可能か考察し，適用可能でかつ，この曲線上での他のペアリング計算と比較して，Miller アルゴリズムの反復回数を既存の DS 曲線ペアリングに比べ短縮できることを示した．また，この Optimal ペアリングの計算アルゴリズムも記述し，p を用いて演算回数を評価した．

(3)ペアリング逆問題についての研究

本研究では，Ate ペアリングの改良版である Ate_i ペアリングの逆問題がある仮定の上では効率的に解かれ得ることを示した．Ate_i ペアリングは(k-1)個(k は曲線の埋込み次数)考えられるが，その内の幾つかの間には，整数論でよく知られている円分多項式を基にした関係式を持っていることが示されるので，ある一個の Ate_i ペアリングを持って更にある仮定が満たされれば他の Ate_i ペアリングも計算され，それを用いてペアリング逆問題が解かれるというものである．この仮定がかなり強いので，本結果がペアリング暗号の安全性に大きく影響することは今のところ少ないと思われるが，本結果の大きな特徴は，『研究の方法』で述べたアプローチのうちの「Miller アルゴリズムの逆問題」を解く必要がないことである．

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）

〔学会発表〕（計 6 件）

① 張一凡，金山直樹，岡本栄司，“Optimal pairings on Duursma-Sakurai curves,” 2010 年暗号と情報セキュリティシンポジウム(SCIS2010)，2010 年 1 月 20 日，かがわ国際会議場

② 坂下泰紀，金山直樹，岡本栄司，“入力の１つの点が共通な複数ペアリングの同時計算法,” 2010 年暗号と情報セキュリティシンポジウム(SCIS2010)，2010 年 1 月 20 日，かがわ国際会議場

③ 田村洸太，金山直樹ほか 4 名，“検証機能を有する楕円曲線上のスカラ倍算の委託計算,” 電子情報通信学会 ISEC 研究会，2009 年 9 月 25 日，機会振興会館

④ 金山直樹，岡本栄司，“ペアリング逆問題についての一考察,” 電子情報通信学会 ISEC 研究会，2009 年 9 月 25 日，機会振興会館

⑤ 照屋唯紀，金山直樹，岡本栄司，“ペアリング高速計算に適した準同型写像を持つ楕円曲線の生成,” 2009 年暗号と情報セキュリティシンポジウム(SCIS2009)，2009 年 1 月 22 日，大津プリンスホテル

⑥ 山口武洋，金山直樹，岡本栄司，“ある超楕円曲線の η_T ペアリングについて,” 2009 年暗号と情報セキュリティシンポジウム(SCIS2009)，2009 年 1 月 22 日，大津プリンスホテル

６．研究組織

(1)研究代表者

金山　直樹（ KANAYAMA NAOKI ）
筑波大学・大学院システム情報工学研究科・研究員
研究者番号：70339696

(2)研究分担者

なし

(3)連携研究者

なし