様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 25 年 5 月 24 日現在

機関番号：１２１０２
研究種目：基盤研究（B）
研究期間：2010～2012
課題番号：２２３０００００２
研究課題名（和文）　新しいペアリング暗号に適した楕円曲線の研究

研究課題名（英文）　Generating elliptic curves suitable for new type of pairing-based cryptography

研究代表者
岡本　栄司（OKAMOTO　EIJI）
筑波大学・システム情報系・教授
研究者番号：60242567

研究成果の概要（和文）：ペアリング暗号は楕円曲線上のペアリングという双線型性を持つ写像を用いた暗号系の総称で、例えば ID ベース暗号の実現で有名になった。その後、クラウドコンピューティング技術の発達などの情勢変化により、更に多様な機能を持つペアリング暗号が望まれるようになり、そしてそれに応え新方式が続々と提案されている。本研究では、そのような次世代ペアリング暗号に適した楕円曲線の生成方法についての研究を行った。

研究成果の概要（英文）：Pairing-based cryptography is a type of public-key cryptography which uses pairings over elliptic curves. Pairings over elliptic curves have bilinearity and we can realize ID-based cryptography by using this property. Recently, ``new type" pairing-based cryptosystems have been proposed based on many interesting mathematical problems. In this research, we worked about generation of elliptic curves suitable for such cryptosystems.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	5,100,000	1,530,000	6,630,000
2011 年度	4,400,000	1,320,000	5,720,000
2012 年度	4,500,000	1,350,000	5,850,000
年度			
年度			
総　計	14,000,000	4,200,000	18,200,000

研究分野：情報学
科研費の分科・細目：情報学基礎
キーワード：ID ベース暗号、楕円曲線、ペアリング、合成数位数、曲線生成

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整数論で用いられていたが、暗号の分野に現れたのは、ECDSA 署名法などいわゆる楕円曲線暗号への攻撃手段として 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入力サイズについての準指数時間で可能であるということが衝撃的でペアリングの計算の実時間が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、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彼らの結果である。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。

２．研究の目的

このように、標準化に向けての具体的な動きも始まったペアリング暗号であるが、クラウドコンピューティングなどの発達により更に多様な機能を持つ「新たなペアリング暗号」に対するニーズも生じ、そして研究も始まっている。そのようなペアリング暗号では、前述の ID ベース暗号などの既存方式とは異なる別の問題の計算量的困難性を仮定するものが多い。そのような仮定を満たすため必要なパラメータ（楕円曲線など）は既存のパラメータ生成法で構成できるか自明では無い。その代表的なものとして、「合成数型の位数の群を持つ楕円曲線」がある。

これまでに提案されていた楕円曲線暗号に適した楕円曲線とは、#E(GF(q))=h・r（r は十分大きな素数、h は小さな整数）と表されるものである。これは、楕円曲線上の離散対数問題に対する攻撃法を避けるために要請されたもので、現在は r のビット長として最低で 160 ビット、推奨値が 256 ビットと言われている。これに対し、合成数位数の楕円曲線とは# E(GF(q))=h・r1・r2（r1、r2：同程度のビット長の十分大きな素数、h$：小さな整数）となる楕円曲線を指す。この曲線を用いたプロトコルは Boneh らによって初めて提案され、そこでは r1 と r2 に最低 512 ビットを要請している。それは、その提案プロトコルの安全性の根拠となる「部分群判定問題」の計算量的困難性を保証するための仮定『n:=# E(GF(q))は公開するが n の素因子は秘密とする』がある、つまり n の素因数分解が難しくなければならないためである。

ペアリング関数の出力値は GF_{q^k}(k は r|q^d－1 を満たす正整数 d の最小のもので、この k を埋込み次数と呼ぶ)であって、効率的なペアリング計算を行うためには、この k が大きくない(例えば k＜100)ような楕円曲線を選ぶ必要がある。しかし、GF(q)上の楕円曲線を任意に選んだ場合にその曲線の埋込み次数が小さい確率はとても小さいことが既に知られている。そこで、埋込み次数の小さい楕円曲線をシステマティックに生成する方法が必要となる。埋込み次数の小さい楕円曲線の「族」に関する初めての成果は宮地らによるものであり、これをより一般化したものが続々と提案された。しかし、これらの結果のほとんどが、上述の# E(GF(q))=h・r（r：十分大きな素数、h：小さな整数）型に限定されたものである。従って、合成数型の位数の群を必要とするプロトコルへの応用は不可能である。このような状況の中 2009 年に Boneh らが合成数位数の楕円曲線を生成する方法を提案した。これにより部分群判定問題の困難性に基づく新たなペアリング暗号の構成が可能となった。本研究では、このような「新しいペアリング暗号」に適した楕円曲線の生成方法に関する研究を目的とする。

３．研究の方法

生成される曲線は、当然ながら脆弱性を持つものでは意味が無い。そこで、生成方法の検討とともに、対象とする問題（例えば上記の部分群判定問題）の困難性に関する検討も研究の大きな柱とする。部分群判定問題に関しては、曲線の生成に関しては前述の Boneh らの方法が十分効率的と判断したので、曲線生成よりも部分群判定問題の困難性に関する検討をメインとする。

また、本研究の採択の直後に、岡本・高島による「関数型暗号」という画期的な暗号が提案された。この暗号は、その処理において、楕円曲線上のスカラー倍計算の回数がペアリングの回数より非常に多いと言う特徴を持っている。これは「第一世代」ペアリング暗号にはあまり見られない特徴で、楕円曲線上のスカラー倍計算の高速化が暗号全体の処理速度向上に大きく貢献する。そこで、この暗号への応用を目指して、スカラー倍計算の高速化を期待できる楕円曲線の生成方法を検討する。

４．研究成果

(1)楕円曲線スカラー倍計算の高速化について

ペアリング暗号における最も主要な処理はペアリング計算と楕円曲線のスカラー倍演算である。幾つかのペアリング高速計算法と高速スカラー倍演算法との関係を調べていくうちに、ペアリング高速計算のためのテクニックをスカラー倍演算の高速化に適用できるのではと考え、その結果として Optimal ペアリングなど幾つかのペアリング関数が高速計算可能な楕円曲線に対して適用可能な高速スカラー倍演算計算法を提案した。

(2)点代入型ペアリング計算における正規化について

Tate ペアリング t(P,Q)は、点 P から導かれる有理関数に Q から導かれる因子を代入することで定義されるが、その後、Ate ペアリング等の、因子ではなく Q そのものを代入する「点代入型ペアリング」が定義された。この種のペアリングを考える場合、点 P から導かれる有理関数が持っている定数倍のずれを処理しなければならないが、関数の正規化を考えることで対処できる。ペアリングを計算するポピュラーなアルゴリズムである Miller のアルゴリズムにこの正規化を組み込むには Miller アルゴリズムの中で用いられる直線関数の正規化を考える(ax+y+c 型の直線を用いる)ことになるが、アルゴリズムの高速化のために a'x+b'y+c'型の直線を用いたい場合が多く、この場合は一般には正規化に対応しない。しかし、ある条件を満たす楕円曲線に対しては、どちらの形の直線を用いても同じ値の Ate ペアリングを計算することが示される。つまり、この場合は正規化の必要がないことを示した。

(3)非常に大きな有限体上での Weli ペアリングと Tate ペアリングの計算効率に関する考察

暗号に用いられているペアリングには Weil ペアリングと Tate ペアリングの 2 つがあるが、現在は Tate ペアリングが主流である。Weil ペアリング、Tate ペアリングはそれぞれ、e_weil(P,Q)=f_P(D_Q)/f_Q(D_P)、e_tate(P,Q)=f_P(D_Q)d ただし d=(q^k-1)/r で表されるのだが、Weil ペアリングの計算では Miller のアルゴリズムと呼ばれる「関数計算」を 2 回要するのに対し Tate ペアリングではそれが 1 回で済むため、Tate ペアリングでは最後に d 乗をする操作（最終べき乗と呼ばれる）が必要なものの、それを考えても Tate ペアリングが高速とされている。

しかし、楕円曲線の係数体 GF(q)のサイズと、埋込み次数と呼ばれるパラメータ k が大きくなると、べき乗指数の d はそれに従い大きくなる。例えば、従来のペアリング暗号では q は 160 ビットから 256 ビットの数、k は 6 から 12 程度の数で盛んに実装されているが、我々の研究対象である「合成数位数の楕円曲線」上でのペアリング計算においては、q は最低でも 1024 ビット（現在では 2048 ビットが推奨されている）であるので、d が飛躍的に大きくなることが予想される。そうなると、d 乗にかかるコストと「関数計算」1 回のコストのバランス次第では Weil ペアリングと Tate ペアリングの優劣が逆転する可能性もあり得る。逆転する場合は、その境界点にあたる q のビット長さや k の値がどの程度になるか把握しておくことが重要である。

そこで、本研究では、q のビット長と k をいくつか固定して合成数位数の楕円曲線を生成し、その曲線上での Tate ペアリングの実装を行ない、関数計算と d 乗の計算時間を実測した。その結果、d 乗の計算は関数計算に比べ非常に少なく、実用レベルでは Tate ペアリングが十分有効であることを検証できた。

(4)合成数位数の楕円曲線を用いたペアリング暗号の安全性についての考察：

（概要）ペアリング暗号の中には離散対数問題などの他に「部分群判定問題」の困難性を安全性の根拠とする方式がいくつかある。部分群判定問題とは、粗く言うと、有限群 G の元 x が G の非自明な部分群に属しているか判定する問題である。楕円曲線の群の上で考えた場合、RSA 合成数のような素因数分解が困難な合成数を位数として持つ楕円曲線を生成しなければならない。そのような曲線の上での部分群判定問題の困難性について考察した結果、この場合の部分群判定問題がペアリング逆問題に帰着されることがわかった。
（重要性・意義など）本成果は部分群判定問題と他の問題との帰着性関係という非常に新しい内容を持っており、本研究の成果の中でも最も大きなものと考えている。

(5)ペアリング・楕円曲線スカラー倍計算に適した準同型写像を持つ楕円曲線の効率的生成法について：

（概要）2001 年に Gallant らが提案した「特殊な準同型写像を持つ楕円曲線上での高速スカラー倍計算」は非常に有効な手法で、特殊な準同型写像を持つ楕円曲線の効率的な生成法があることが望ましい。これに関する先行研究には高島によるものが知られているが、この方法による楕円曲線はρ値と呼ばれるパラメータが約 2 と大きく、1 に近い値を持つものが望まれる。高島の方法では Cocks-Pinch 法と呼ばれる楕円曲線生成法を用いており、それがρ値を大きくしている。そこで我々は、pairing-friendly 楕円曲線族の生成法を応用して、埋込み次数が 2 と 3 のみを素因子に持つ場合に小さいρ値をもつ曲線を生成できることを示した。
（重要性・意義など）2010 年に岡本・高島によって提案されたインテリジェント暗号など楕円曲線上のスカラー倍計算をペアリング計算よりも多く行う暗号方式が最近多く提案されている。本成果の手法で生成された楕円曲線は、上記暗号方式などの実装に非常に適している。

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８件）
①金山直樹，岡本栄司，齋藤和孝；
ペアリング計算や楕円スカラー倍計算に適した準同型写像を持つ楕円曲線の生成について，査読無し，電子情報通信学会，信学技報第 112 巻第 342 号，pp.23-28,2012

②金山直樹，内山成憲，岡本栄司；
部分群判定問題とペアリング逆問題についての注意，査読無し，電子情報通信学会，信学技報第 112 巻第 305 号，pp.89-92,2012

③金山直樹，劉陽，岡本栄司，齋藤和孝，照屋唯紀，内山成憲；
小標数の有限体上の elliptic net を用いたペアリングと楕円スカラー倍の計算，査読無し，電子情報通信学会，信学技報第 112 巻第 211 号，pp.7-13,2012

④金山直樹，劉陽，岡本栄司，齋藤和孝，照屋唯紀，内山成憲；
Elliptic net を用いた楕円曲線スカラー倍計算について，査読無し，電子情報通信学会，信学技報第 112 巻第 126 号，pp.201-206,2012

⑤照屋唯紀，金山直樹，岡本栄司；
Barreto-Naehrig 曲線上の楕円スカラー倍の高速なソフトウェア実装に関する一考察，査読無し，電子情報通信学会，信学技報第 112 巻第 39 号，pp.11-18,2012

⑥Naoki Ogura, Shigenori Uchiyama, Naoki Kanayama and Eiji Okamoto；
A note on the pairing computation using normalized Miller functions，査読あり，IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E95-A,No.1, pp.196--203, 2012.

⑦Naoki Kanayama, Tadanori Teruya and Eiji Okamoto；
Scalar Multiplication on Pairing Friendly Elliptic Curves，査読あり，IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences,Vol.E94-A, No.6, pp.1285--1292, 2011.

⑧小椋直樹，金山直樹，内山成憲，岡本栄司；
Elliptic Net を用いた Ate ペアリングとその変形，査読無し，電子情報通信学会，信学技報第 110 巻第 200 号，pp.13-19,2010

〔学会発表〕（計２件）

①小椋直樹，内山成憲，金山直樹，岡本栄司；
正規化された Miller 関数を用いたペアリングの計算についての注意，
2011 年暗号と情報セキュリティ・シンポジウム(2011 年 1 月 26 日,於リーガロイヤルホテル小倉)

②小椋直樹，金山直樹，内山成憲，岡本栄司；
Elliptic Net を用いた Ate ペアリングとその変形，2011 年暗号と情報セキュリティ・シンポジウム(2011 年 1 月 26 日,於リーガロイヤルホテル小倉)

６．研究組織
(1)研究代表者
岡本　栄司（OKAMOTO　EIJI）
筑波大学・システム情報系・教授
研究者番号：60242567

(2)研究分担者
満保　雅浩（MAMBO　MASAHIRO）
金沢大学・電子情報学系・教授
研究者番号：60251972
金岡　晃（KANAOKA　AKIRA）
筑波大学・システム情報系・助教
研究者番号：00455924