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（C）
研究期間：2010～2012
課題番号：２２５００００５
研究課題名（和文）　小型デバイスに適した公開鍵暗号技術についての研究

研究課題名（英文）　Public-key cryptography suitable for implementation on small device

研究代表者
金山　直樹（KANAYAMA　NAOKI）
筑波大学・システム情報系・研究員
研究者番号：70339696

研究成果の概要（和文）：ペアリング暗号を IC カードなど限られた計算機資源でも効率的に処理できるように、ペアリング暗号の主要かつコストの大きい処理である「ペアリング計算」と「楕円曲線の点のスカラー倍」の高速計算アルゴリズムについて研究した。その成果として、elliptic net と呼ばれる関数を用いたペアリング・楕円曲線スカラー倍計算の方法を小標数の有限体上の楕円曲線上で行うアルゴリズムを明確に与えるなどの成果を残した。

研究成果の概要（英文）：We worked for developing algorithms for computing pairings and scalar multiplication over elliptic curves in order to implement pairing-based cryptography on IC cards efficiently. We obtained results, for example, about efficient algorithms on computing pairings and scalar multiplication over elliptic curves over finite fields of small characteristic using elliptic nets.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	1,200,000	360,000	1,560,000
2011 年度	1,100,000	330,000	1,430,000
2012 年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,300,000	990,000	4,290,000

研究分野：暗号理論
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

ID ベース暗号とは名前の通り、メールアドレスなどのユーザの ID 情報を公開鍵に用いるという暗号系で、鍵の正当性(「A 氏の鍵」とされているその鍵が本当に A 氏のものか)の保証を鍵認証局なしで可能とする画期的な暗号系であるが、Shamir による 1988 年の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境らと Boneh らの 2000 年での結果である。

２．研究の目的

ID ベース暗号ではユーザ ID をもとにそのユーザの秘密鍵を生成する鍵生成局を要するため、ID ベース暗号は、例えば中・小規模

のネットワークにおける公開鍵暗号に特に有効であると考えられる。この ID ベース暗号を、自治体の医療システム管理に利用することも期待できよう。幾つかの医療機関において、患者のカルテなど重要な機密情報を安全に管理するために、公的 PKI（公開鍵基盤）による IC カード認証の実装実験が行われている。PKI の整備は自治体レベルでもコストが大きいと言われているので、これを本格的に導入する場合は大きな負担がかかる。そこで代わりに ID ベース暗号を導入することが有力と思われる。しかし、ペアリング暗号にも大きな課題があり、ほとんどの方式において必要とされる 2 つの処理「ペアリング計算」と「楕円曲線の点のスカラー倍」は、いずれも決して小さいコストでは無く、現在の IC カードの計算力では実用的な時間での計算はとても望めない。そこで、IC カードなど限られた計算機資源でも効率的に処理できるペアリング暗号の設計を本研究の主目的とする。

３．研究の方法

ペアリング計算・楕円曲線スカラー倍の計算効率は、選択する楕円曲線の性質次第で大きく変動する。本研究で主に取り扱った楕円曲線の係数体は、ハードウェア実装に適していると言われている小標数の有限体である。そして、多くの研究では、supersingular（超特異）と呼ばれる性質を持った楕円曲線を対象とした。また、計算アルゴリズムについては、それまでの定番ともいえる Miller のアルゴリズム（ペアリング計算）や 2 進展開法あるいはその改良版（楕円曲線スカラー倍）だけでなく、2007 年に Stange が導入した elliptic net と呼ばれる関数を用いた方法についても着目した。実際、Stange の紹介した方法は大きな標数の有限体の場合であったので、それを小標数特に 2 と 3 の場合のアルゴリズムを明確に与えることを試みた。

４．研究成果

(1)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。

(2)Duursma-櫻井曲線上でのペアリング計算における正規化の必要性について

これは上述(1)の超楕円曲線版に相当する。既に述べたように、ペアリング関数のハードウェア実装に適した楕円曲線として知られているものに、標数が 2 または 3 の有限体上の supersingular 楕円曲線がある。supersingular な曲線であるので distorsion 写像を有しており、また標数が小さいので有限体演算をハードウェア実装しやすいなどのメリットがある。しかし、これらの曲線はペアリング実装に適した群位数をあまり豊富に提供できないというデメリットがある。例えば標数 3 の有限体の場合で言うと、GF(3^m)に座標を持つ有理点群が暗号に適した大きなビット数の群位数を持つような m として m=97(群位数は約 160 ビット)があるが、その次の m の値は急激に大きくなり、実装が困難になる。したがって、これらの楕円曲線以外にも、ペアリング実装のハードウェア実装に適した曲線を保持しておくことが望ましい。

そのような曲線として有望と思われるのが、Duursma-櫻井によって研究された、標数 p の有限体上で定義される Y^2=X^(p-1)/2-X+d 型の超楕円曲線（これを DS 曲線と呼ぶことにする）である。DS 曲線も supersingular であり、ペアリング計算に大変有用な幾つかの性質を持つことが Duursma らによって示されている。小さい p（5 や 7 など）の場合はハードウェア実装も（2 や 3 の場合に比べ複雑になっても）大標数の体上の楕円曲線にくらべペアリング実装はしやすいと期待される。

本研究では、小さい標数の DS 曲線において Optimal Ate ペアリングを計算する場合に必要とされる「関数の正規化」の必要性について調べた。ある型のペアリング計算においては、「関数の正規化」が必要とされるが、ある条件を満たす楕円曲線の場合はその操作の必要のないことが小椋らによって証明された。本研究はその類似にあたるもので、p=7 の DS 曲線においては関数の正規化が必要ないことを示すことが出来た。

(3)小標数の有限体上の楕円曲線についてのelliptic netによるペアリングの計算について

（概要)2007年にStangeは elliptic net と呼ばれる写像を定義し，これを用いて Tateペアリングを計算する新しい方法を提案した．その後，小椋らによってAteペアリングなどの計算方法が示された．しかし，以上の結果は全て楕円曲線の定義体の標数が5以上の場合である．そこで本研究では Stange の提案した elliptic net の計算アルゴリズムを小標数の有限体上で定義された楕円曲線についても用いられるかを検討した．
（重要性・意義など）本結果によって，ハードウェア実装に相性の良い小標数のペアリング関数を elliptic net で実装できるようになった．

(4)等分多項式を用いた楕円曲線スカラー倍計算法について

（概要）楕円曲線暗号やペアリング暗号における主要処理の一つは楕円曲線上のスカラー倍計算，つまり，楕円曲線の点Pと整数sに対する[s]Pの計算である．楕円曲線上のスカラー倍計算（以後 ECSM と書く）のポピュラーな計算法は楕円曲線上の加算と二倍算の繰り返しによるものであるが，もう一つの方法に，等分多項式を用いた楕円曲線の乗法公式がある．これは楕円曲線論の有名な結果で，暗号への応用は Miller によって既に考察されているが，具体的なアルゴリズムが示されていない．本研究では，上述の Stangeの結果を応用して等分多項式による乗法公式を用いた ECSM 法の実装を行った．その結果，アフィン座標系での二進展開・NAF 法よりも提案手法の方が高速であることがわかった．
（重要性・意義など）等分多項式を用いたECSMの計算が，現時点では最速ではないものの実用的な速度で処理されることを実証した．Elliptic net 計算が高速化されればこの方法に対する期待は更に高まる．

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

(6) Naoki 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.

(7)Naoki 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
金山　直樹（KANAYAMA　NAOKI）
筑波大学・システム情報系・研究員
研究者番号：70339696

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