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　１３　日現在

機関番号：　２２６０４
研究種目：　基盤研究(C)（一般）
研究期間：　2012～2015
課題番号：　２４５４０１３５

研究課題名（和文）代数的アルゴリズムの計算量解析とその公開鍵暗号への応用

研究課題名（英文）Analysis of algebraic algorithms and its applications to public-key cryptography

研究代表者
内山　成憲（Uchiyama, Shigenori）

首都大学東京・理工学研究科・教授

研究者番号：４０４３３１７２

交付決定額（研究期間全体）：（直接経費）　　3,900,000円

研究成果の概要（和文）：本研究では代数的アルゴリズムの計算量的解析を行い公開鍵暗号、特にペアリング暗号への応用について考察を行った。具体的には主に次の結果を得た：Elliptic Netに基づくペアリング計算の高速化やそのアルゴリズムの種数２の超楕円曲線への一般化。有限体上の Elliptic Divisibility Sequenceを用いたDH問題と計算量的に等価な問題の提案。Edward curveと呼ばれる楕円曲線の標準形に対するスカラー倍算アルゴリズムの高速化手法の提案。

研究成果の概要（英文）：In this research, we consider that analysis of algebraic algorithms from computational complexity and its applications to public-key cryptography, especially pairing based cryptography. We mainly gave the following results: A proposal of improving a pairing computation algorithm based on elliptic nets and hyperelliptic nets. A proposal of some computational hard problem based on elliptic divisibility sequences, which is equivalent to DH problem. A proposal of some improvement of scalar multiplication on Edward curves.

研究分野：　暗号理論

キーワード：　暗号　アルゴリズム

１．研究開始当初の背景
これまで多数の公開鍵暗号方式が提案され、それらはICT社会とも呼ばれる現代社会では欠かすことのできない重要な技術となっている。一方、その安全性を支える数学的問題である素因数分解問題や離散対数問題は量子計算機と呼ばれる計算機が実現すると効率的に解かれてしまうことが知られている。RSA 暗号の安全性は素因数分解問題に、ElGamal 暗号の安全性は有限体（又は、有限体上の楕円曲線）上の離散対数問題の計算量的困難さにそれぞれ基づいている。これらの数論的問題は、現在のところ十分大きなサイズであれば、既存の計算機の性能をもってしても現実的な時間では解くことは非常に困難だと考えられている。これまでの計算機の研究の歴史や、上述の数論的問題に基づく公開鍵暗号が現在の社会の基盤を支える技術の一つとなっている事を考えると、将来、量子計算機が実現された際に、社会に与える影響の大きさを少しでも軽減するためにも、今からその対策を進めておくことは重要であると考えられる。
２．研究の目的
本研究では、様々な代数的アルゴリズム、特に代数曲線に関連したアルゴリズムを中心に解析を行い、量子計算機を用いた攻撃に対して耐性を持つ公開鍵暗号の提案を目標とし、既存の方式やそれらが基づく数学的問題の計算量的な解析を行うものである。
３．研究の方法
大きく分けて次の２段階で研究を行った。
（１）代数的なアルゴリズムの解析及び改良：代数曲線に関連する問題や組み合わせ論に関する問題等に対して解析や改良を行う。
（２）上記の問題に基づく暗号への応用：実用的な公開鍵暗号のしかけとなる一方向性関数の候補としては上記の数論的な問題しかないと言っても過言ではなく他の代数学的なアルゴリズムの解析に基づき、新しい一方向性関数の構成を試みる。
４．研究成果
主な結果を以下に述べる。代数曲線特に楕円曲線に関連するアルゴリズムについて考察することは暗号への応用の観点からは重要であるが、一般に楕円曲線上のペアリングの高速計算には Miller によるアルゴリズムが知られており、その改良研究なども多数ある。一方、効率的なペアリングの計算アルゴリズムについては本質的に Miller によるものしか知られていなかったが、2007 年に Stange によって楕円曲線の新しい数論モデルが提案され、それを用いるとペアリング写像が効率よく計算できることも示された。この写像は Elliptic Net と呼ばれるが、これに基づくペアリング計算に関して高速化は出来ないか考察を行った。特に、BN 曲線と呼ばれる最も一般的に利用されるペアリング暗号用の楕円曲線上で Optimal Ate Pairing と呼ばれるペアリングについて考察した。単純に考えると、Miller によるものが効率よく見えるため、ブロックごとの計算などを考慮し、並列計算を試みた。結果として、6 次の twist 上の Elliptic Net を用いて効率よく計算するための並列手法を提案した。今回提案したアルゴリズムはブロックと呼ばれる複数の組からなる数列の計算の高速化として、そのブロックを拡張するなどによるもので、10 並列の場合が最適であることが分かった。また、超楕円曲線上に Elliptic Net を一般化し、それを用いてペアリング計算の新しいアルゴリズムを提案した。また、Fixed Argument pairing と呼ばれるものにも適用しその効果を確かめた。一方、Elliptic Net のいわば特殊な形とも言える Elliptic Divisibility Sequence と呼ばれる楕円曲線の等分多項式と同様の関係式を満たす数列があるが、これを用いて楕円離散対数問題と計算量的に等価な新しい数論的な問題が Stange 等によって提案され、等価性の証明が与えられた。そこで、楕円 DH 問題と計算量的に等価な計算困難は定義できないかと考え、実際に計算量的に等価な問題を定義し、その等価性を示すことが出来た。素数判定法についても考察した。N=h2^{n}-1 の型をした自然数に対する素数判定法が Riesel によって 1960 年代に考察されている。これは、実二次体における Fermat の小定理や単数群の性質に基づくものである。一方で具体的にアルゴリズムとして書き下したものがなく、実装についてはもう少し解析が必要であった。そこで、そのアルゴリズムを具体的に書き下すとともに、特に h=n となる場合、Woodal 数と呼ばれる数に対する高速化について考察した。これは、特殊な場合ではあるが高速実装も行い、素朴な実装と比較すると、入力サイズ k に対して k^{0.415}倍の高速化を与えることがわかった。2007 年に Edwards によって提案された新しい楕円曲線の標準形に基づく楕円スカラー倍の解析を行った。この標準形は Edwards curve と呼ばれる。Edwards によって与えられた標準形を用いたスカラー倍算で、その加法鎖の構成の中でも extended Double-Base Number System と呼ばれる方式に注目し、それらを Edwards curve の様々な座標系の中で拡張座標系と呼ばれる新たな座標系を用いて解析を行った。特に、twisted Edwards curve と呼ばれる曲線に対して適用した。具体的には、3 倍算を明示的に書き下し、スカラー倍の計算量を評価するとともにその最適化を与えた。また、Fibonacci 数列を用いた加法鎖の新しい構成法を示し、数理実験によってその効果を確かめた。Dickson 多項式と呼ばれる有限体上の置換を与える多項式写像の研究から導入された多項式を用いた暗号方式で、素因数分解問題の困難さに安全性の根拠をおいているものに対して安全性解析を行った。中でも、RSA 暗号に対する代表的な攻撃法の一つで秘密鍵のサイズが十文小さい場合に、格子の十

分短い長さを求める問題に帰着させ、LLL アルゴリズムを用いて解析を行い、安全性に関しては RSA と同様であることを得た。具体的には、Dickson 多項式を用いた素因数分解問題に基づく公開鍵暗号方式（以下 Dickson 暗号）は、RSA 暗号のある意味での一般化とみなされるため、RSA 暗号に対する攻撃法が適用可能かどうかを調べることには重要である。ここでは、公開鍵 n、秘密鍵 d として、d が n に比べて十分小さい場合に有効となる攻撃法について考察した。1990 年に Wiener により公開鍵 n と e の比で表される有理数を連分数展開する方法で、d のオーダが n^{0.25} よりも小さい場合に n が効率よく素因数分解されることが示されている。また、1997 年に Boneh と Durfee により、LLL アルゴリズムを用いることにより、このバウンドが n^{0.292}まで改良されることが示されている。素因子の一部を既知としたアルゴリズムが橋本等によって提案されてもおり、現在でも活発に研究がされている。Dickson 暗号の場合は、単純に Boneh-Durfee によるアルゴリズムを用いた場合 n^{0.569}となることが示される。但し、e や d のサイズが RSA と比べると 2 倍になっているため、この評価は RSA 暗号の場合とほぼ同等の結果が得られたことがわかる。

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 9 件）

① Hiroshi Onuki, Tadanori Teruya, Naoki Kanayama, Shigenori Uchiyama, The optimal pairing over the Barreto-Naehrig curve via parallelizing elliptic nets, JSIAM Letters, 査読有, Vol.8, 2016, 9-12
https://www.jstage.jst.go.jp/browse/jsiaml/

② Akihiko Onishi, Shigenori Uchiyama, A small secret exponent attck on cryptosystems using Dickson polynomials, JSIAM Letters, 査読有, Vol.7, 2015, 33-35
https://www.jstage.jst.go.jp/browse/jsiaml/7/0/_contents

③ Yasunori Mineo, Shigenori Uchiyama, Scalar multiplication for twisted Edwards curves using extended double-base number system, JSIAM Letters, 査読有, Vol.6, 2014, 37-39
https://www.jstage.jst.go.jp/browse/jsiaml/6/0/_contents

④ Yang Liu, Naoki Kanayama, Tadanori Teruya, Shigenori Uchiyama, Eiji Okamoto, Computing fixed pairings with the elliptic net algorithm, JSIAM Letters, 査読有, Vol.6, 2014, 69-72
https://www.jstage.jst.go.jp/browse/jsiaml/6/0/_contents

⑤ Kazuki Azami, Shigenori Uchiyama, Primality testing of Woodal numbers, JSIAM Letters, 査読有, Vol.6, 2014, 1-4
https://www.jstage.jst.go.jp/browse/jsiaml/6/0/_contents

⑥ Junichi Yarimizu, Shigenori Uchiyama, The elliptic curve Diffie-Hellman problem and an equivalent hard problem for elliptic divisibility sequences, JSIAM Letters, 査読有, Vol.6, 2014, 5-7
https://www.jstage.jst.go.jp/browse/jsiaml/6/0/_contents

⑦ Naoki Kanayama, Yang Liu, Eiji Okamoto, Kazutaka Saito, Tadanori Teruya, Shigenori Uchiyama, Implementation of an Elliptic Scalar Multiplication Method Using Division Polynomials, IEICE Trans. Fundamentals, 査読有, Vol.E97-A,No.1, 2014, 300-302

⑧ Yukihiro Uchida, Shigenori Uchiyama, The Tate-Lichtenbaum Pairing on a Hyperelliptic Curve vis Hyperelliptic Nets, Proc. of Pairing2012, 査読有, LNCS7708, 2013, 218-233

⑨ Naotoshi Sakurada, Junichi Yarimizu, Shigenori Uchiyama, An integer factoring algorithm based on Elliptic Divisibility Sequences, JSIAM Letters, 査読有, Vol.4, 2012, 21-23
https://www.jstage.jst.go.jp/browse/jsiaml/4/0/_contents

〔学会発表〕（計 7 件）

① 小貫啓史,照屋唯紀,金山直樹,内山成憲, Optimal ate pairing の elliptic net による並列計算, 2016 年暗号と情報セキュリティシンポジウム, 2016 年 1 月 19 日, ANA クラウンプラザホテル熊本ニュースカイ（熊本県・熊本市）

② 小貫啓史,照屋唯紀,金山直樹,内山成憲, Elliptic net の並列化による optimal ate pairing の計算, 日本応用数理学会 2015 年度年会, 2015 年 9 月 10 日, 金沢大学（石川県・金沢市）

③ 尾西昭彦,内田寛幸,内山成憲, Dickson 多項式を用いた暗号方式に対する秘密鍵が地裁場合の攻撃法, 日本応用数理学会 2014 年度年会、2014 年 9 月 3 日, 政策研究大学院大学（東京都・港区）

④ 峯尾康則,内山成憲,Twisted Edwards curve を用いたスカラー倍算について, 日本応用数理学会 2013 年度年会,2013 年 9 月 9 日, アクロス福岡（福岡県・福岡市）

⑤ 劉陽,金山直樹,齋藤和孝,照屋唯紀, 内山成憲, 岡本栄司, Elliptic Net による fixed argument pairing の計算について, 日本応用数理学会 2013 年度年会, 2013 年 9 月 9 日, アクロス福岡（福岡県・福岡市）

⑥ 内田幸寛, 内山成憲,Hyperelliptic net による超楕円曲線上の Tate-Lichtenbaum ペアリング, 2013 年暗号と情報セキュリティシンポジウム, 2013 年 1 月 22 日,ウエスティン都ホテル京都（京都府・京都市）

⑦ Yukihiro Uchida, Shigenori Uchiyama, The Tate-Lichtenbaum Pairing on a Hyperelliptic Curve via Hyperelliptic Nets, 5th International Conference on Pairing-based Cryptography(Pairing2012), 2012 年 5 月 16 日, Clogne（Germany）

〔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

６．研究組織
(1)研究代表者
内山　成憲（UCHIYAMA SHIGENORI）
首都大学東京・大学院理工学研究科・教授
研究者番号：40433172

(2)研究分担者
なし

(3)連携研究者
なし