【学位論文審査の要旨】

ICT 社会とも呼ばれる今日では、インターネットに代表されるオープンネットワークを安心かつ安全に利用するために暗号技術が広く利用されており、必要不可欠なものとなっている。本論文の中心テーマは計算整数論の公開鍵暗号への応用、特に ID ベース暗号などで利用されている楕円曲線上定義されたペアリング写像の計算の高速化に関するものである。ID ベース暗号は公開鍵暗号の一種であり、利用者の公開鍵として利用者を識別する情報であるメールアドレスや物理的な IP アドレス等を公開鍵として用いることが出来るものである。1980 年代に Shamir によって提案された概念であり、実用的かつ安全性が高いと考えられるものは 2000 年頃に Boneh と Franklin、笠原と境により独立に楕円曲線上のペアリング写像を用いたものが提案され、それ以降、様々な種類のペアリング写像の計算アルゴリズムやそれらの高速化の研究が盛んにおこなわれてきた。ペアリング写像の計算には従来 Miller による因子に基づく表現を用いたものが知られておりそれに関する高速化の研究が多数知られている。一方、2007 年に Stange により elliptic net と呼ばれる写像が定義された。楕円曲線に付随した等分多項式と呼ばれる楕円曲線上の点のスカラー倍を求めるための多項式が満たす関数等式と同様の関係式を満たす数列で elliptic divisibility sequence と呼ばれるものがあるが、この数列の一般化とみなせる写像であり楕円曲線の情報をすべて保持した、言わば楕円曲線の新しい数論的モデルともいえる写像である。その際、一つの応用として Stage により、Tate ペアリングと呼ばれる楕円曲線上のペアリング写像が効率よく計算できることが示され、Miller によるアルゴリズムとは別の計算方法として注目されるようになった。Miller によるアルゴリズムの高速化の研究の中に Aranha 等による並列化や twist 曲線を用いたものがあるが、elliptic net についてはこれまで考察されていない。本論文の目的は、elliptic net を用いた楕円曲線上のペアリング写像の計算について、並列化や twist 曲線などを用いた高速化の提案である。

２　研究の方法と結果

本研究では、ペアリングを用いた暗号系で用いられる代表的な曲線である Barreto-Neahrig（BN）曲線上の optimal ate ペアリングの計算について考察し、twist を用いた高速化及び並列計算アルゴリズムの構築を行った。また、これらの手法が BN 曲線を含むさらに広いクラスの楕円曲線に適用できることを示し、並列計算アルゴリズムにおける効果による曲線の分類なども行った。elliptic net の計算は Stange によるブロックに基づくアルゴリズムが知られている。ペアリング計算の場合は二つの点を入力とするため、２つの整数成分からなる組（i, j）ごとに値 W(i, j)を決め、それらの 11 個の組が一つのブロックとなる。ブロックは W(i-1, 1)から W(i+1, 1)及び W(i-3, 0)から W(i+4, 0)の 11 個からなる。このブロックを用いて、elliptic net の満たす関数等式及び Double and Add method と呼ばれる計算法に基づき効率よく計算可能となる。このとき、W(i, j)は楕円曲線を定義する基礎体の拡大体

の要素となるが、頻繁に計算に用いる W(i, j)が基礎体上の小さな拡大次数を持つ拡大体に属す場合が効率的となる。まず、楕円曲線の twist を用いることで elliptic net が効率よく計算できることが示されている。これは、有限体の適切な元のべき乗を取り、基となる elliptic net に乗じることで得られることが定理として示されている。次に、twist の場合のブロックの成分が基になる elliptic net のブロック成分の間でどう変換されるかを明示的に定理として示している。この際、optimal ate ペアリングを elliptic net を用いて計算するアルゴルズムと twist による elliptic net を用いて計算するアルゴルズムが重要となるが、このアルゴリズムも明示的に示し定理として与えている。次に並列計算であるが、elliptic net のブロックを拡張することで並列計算が高速化できることを示している。これは、ブロックの各要素を並列に計算することで実現できるが、一般論としては並列数を十分大きくできる場合に効果的であるが、計算コストは最も長い直列計算部分のコストとなり、twist の elliptic net では W(・, 1)の部分のコストが支配的となる。

楕円曲線の定義体の標数が 2 でも 3 でもないと仮定しているため自明なものを除けば twist から決まる次数は 2,3,4,6 のいずれかとなる。この次数ごとに並列アルゴリズムを構築している。さらに、構築したアルゴリズムの効率を高めるため、ブロックの拡張という手法を提案している。これは、elliptic net のブロックに 2 つの要素 W(i+2, 1)と W(i+3, 1)を付け加えてブロックのサイズを大きくするものである。この拡張により全体としての計算コストは当然増加するが、並列数が十分大きな場合は、並列計算としてのコストを削減させることが可能となることが示されている。以上に基づき、体の乗算以外のコストは無視して乗算コストの評価に基づく Aranha 等による手法を用いて計算量の評価を行った。その結果、埋め込み次数 3 の超特異楕円曲線を用いた場合に、並列がない場合と拡張ブロックを用いた場合の 8 並列で比較をすると 3 倍弱の高速化が実現できることが実装により示された。他の曲線についても同様な効果が得られている。

３　審査の結果

以上のように､本論文は楕円曲線上のペアリング写像について elliptic net を用いた計算の高速化について進展をもたらしたものである。単に計算整数論の分野における一つの成果というだけでなく、ID ベース暗号という形で、暗号や署名方式への応用を見据えた結果でもあり、本研究は実用的な観点から見ても重要な成果であると考えられる。これらの結果の一部は査読付きの国際研究集会で発表され、査読付き学術論文としても出版されており、国際的にも注目されている。

これらはすべて高く評価が出来ると考えられ、審査員全員一意で本論文は十分に博士（理学）の学位に値するものとして認める結論に至った。

４　最終試験の結果

本学の学位規定に従い、最終試験を行った。公開の席上で論文発表を行い、数理情報科学専攻の大学院担当教員及び外部審査委員による質疑応答を行った。その結果、問題なく承認され合格と判定した。