審査の結果の要旨

論文提出者氏名　　小林　鉄太郎

本論文は「Fast Computation Algorithms for Elliptic Curve Cryptosystem （楕円曲線暗号系の高速演算法に関する研究）」と題し，主に楕円曲線暗号を実現する場合に中核となる，楕円スカラー倍演算に関する演算法を整理し，楕円曲線暗号を構成する有限体を素体， 2の拡大体， 最適拡大体（OEF）の3つの場合において，それぞれ①楕円曲線演算の回数の低減，②楕円曲線演算の高速化，③有限体上の演算の高速化の三つの部分に関して，高速なアルゴリズムを提案し，その演算効率を理論的および実験的に明らかにするとともに,C言語による実装によってその有効性の検証を行ったものである.これにより，楕円DSA署名や楕円ElGamal暗号に代表される 楕円曲線暗号の世界最高速実装の実現を可能としている.また，IDベース暗号や秘密鍵共有，ブロードキャスト暗号などを実現するのに用いられる楕円ペアリング演算においても，楕円スカラー倍演算と同様に，三つの部分それぞれに対して演算コストの分析を行い，最適なアルゴリズムを提案している．論文の構成は,「Introduction」を含めて７章からなる.

第１章は「Introduction（序論）」で，本研究の背景を明らかにした上で，研究の動機と目的について言及し，研究の位置付けについて整理している.

第２章は「Base-φ Method（φ進展開法）」と題し，楕円曲線演算の回数を最小化する方法であるφ進演算法を OEF 上の楕円曲線に適用する方法を提案している．単純に OEF に適用しただけでは効果が無いが，事前演算による高速化手法と組み合わせることにより，OEF 上の楕円曲線でもφ進演算法の高速化効果を得ることに成功している．これにより，従来特殊な曲線である Koblitz 曲線でのみ使われていたφ進演算を，初めて OEF などの別の体へ適用することを可能にした.

第３章は「Cyclic Window Method（巡回窓演算法）」と題し，第２章で提案したφ進演算法の最適化を論じている．スカラー倍演算では，「窓法」と呼ばれる演算法がよく使われる．これとφ進演算法を組み合わせる際に，楕円曲線のフロベニウス写像の特有の性質を用いることにより，φ進展開のみに使える「巡回窓法」を用いることができることを示し，その理論上の効率を示している．また，C 言語実装による実測値による検証を行い，従来の方式との比較からその有用性を述べている.

第４章は「Parallel Elliptic Curve Arithmetic（並列度を考慮した楕円演算）」と題し，楕円曲線暗号における基本演算である「楕円加算演算」「楕円２倍演算」の新しい演算法の提案を行っている．従来の楕円加算演算法は，座標系の工夫によって楕円加算演算・楕円 2 倍演算の演算公式が変化することに着目し，各座標系において，有限体上の乗算回数が最小化されることを目標としていた．本章では CPU アーキテクチャの進歩とともに，複数の乗算器をもつアーキテクチャが基本となっていることを考慮して，乗算回数ではなく乗算ステップ数を最適化することを目標とした座標系および演算法の提案を初めて行っている.

第５章は，「Finite Field Inversion（素体上の逆元演算法）」と題し，素体上の逆元演算のコストおよび効率化について論じている．素体上の逆元演算はユークリッドの互除法または，その改良アルゴリズムによって実現されるが,従来は素体上の逆元演算は素体上の乗算演算の 10 倍以上遅いとされていた.このため，楕円曲線暗号を実現する場合，アフィン座標を用いると楕円加算演算・楕円 2 倍演算ともに

逆元演算を行う必要があり，乗算回数が多い代わりに逆元を必要としない Jacobi 座標等のほうが実用上は優れていた．この章では大きなビット長の逆元演算を，短いビット長の演算でエミュレートすることによって高速化する方法を提案している．この結果，提案逆元法を用いることでアフィン座標を用いたほうが高速になるという逆転が生じることが示される．

第 6 章は，「Fast Computation Algorithm for Pairing（高速ペアリング演算法）」と題し，楕円ペアリング演算の大部分を占める Miller のアルゴリズムを高速化する手法について述べている．ペアリング演算の高速化において，最もよく用いられる Tate ペアリングに特化した最適化を行うことで「擬似演算」および「多項式展開」の演算法を導入し，その演算コストについて理論的および C 言語による実装評価を行っている．

最後に第７章は「Conclusion（結論）」で，本研究の総括を行い，併せて将来展望について述べている．

以上これを要するに，本論文は，楕円曲線暗号系の高速演算法をまとめるとともに，すべての部分に関して高速化･最適化のアルゴリズムを提案し，実用上の有効性を明示したものであり，これらの楕円曲線暗号系の高速演算法に関する研究は，電子情報学，特に情報セキュリティ工学上貢献するところ少なくない．

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる．