氏　名	高島　克幸

（論文内容の要旨）

近年，楕円曲線及び超楕円曲線ヤコビ多様体上のペアリング演算を用いた暗号系の研究が活発であるが，本論文は，それら代数曲線ヤコビ多様体に関連する計算法の研究と，その成果の新たな暗号系構成法への応用という研究結果をまとめたものであり，６章から構成されている．

第１章は序論であり，本研究の目的とその内容について概観している．

第２章では，ペアリング暗号用の楕円曲線の構成法に関して，新たな提案をしている．ペアリング暗号に用いる楕円曲線では，その安全性を変更する際に，埋め込み次数というパラメータが重要な役割を果たしている．
一方，ペアリング演算の効率を高めることが，実用上重要な課題となっている．本章でそれら２要件を満たす曲線構成法を提案している．安全性変更が容易であると共に，高速演算を実現する今回の楕円曲線構成法は，ペアリング暗号実用化に大きく寄与するものである．最後に，具体的に有効な曲線パラメータの提示も行っている．

第３章では，あるクラスの種数２超楕円曲線ヤコビ多様体上で，実乗法写像と呼ばれる演算を利用した新しい高速スカラー倍算法の提案を行っている．
それらの曲線には，ペアリング暗号に有効な曲線も含まれている．従来は，超楕円曲線の自己同型写像がスカラー倍算高速化に用いられてきたが，本章では，それとは異なるヤコビ多様体上の演算をスカラー倍算高速化に利用している．
これにより，高速演算を有する曲線のクラスが大きく広がっている．また，最後に具体的に有効な曲線パラメータの提示も行っている．

第４章では，ディストーション写像と呼ばれる演算法の数学的特性を明らかにしている．高種数の超楕円曲線ヤコビ多様体上の高次元ベクトル空間構造を暗号に活用するために，超特異曲線ヤコビ多様体上の自己準同型写像であるディストーション写像の完全な決定を行っている．従来，数論アルゴリズム分野で，全ての自己準同型写像を具体的に決定した例は，特殊な曲線に限っても，自明な場合を除いては，ほとんど報告されていないが，本章で，ある特殊な２タイプの曲線に対し，その決定している．
つまり，自己準同型写像全体がなすベクトル空間の基底を，効率的に計算可能な写像として具体的に決定した結果となっている．そこでは，ガウス和作用素という自己準同型写像の数論的性質が重要な役割を果たしている．それ自身，理論的な寄与を有するが，次章での新たな暗号系構成法の基盤を与える結果となっている．

第５章では，ディストーション固有ベクトル空間という高次元ベクトル空間でのベクトル分解問題の計算量的困難性の評価を確立し，それに基づいて，様々な暗号及び署名法構成を行っている．まず，ベクトル分解計算問題の困難性を，一般化された Diffie-Hellman 計算問題の困難性に帰着する結果を示している．
本結果は，ベクトル分解計算問題の困難性を仮定することが妥当であることを示している．暗号応用には判定問題困難性が重要であるので，次に，ベクトル分解判定問題，部分空間判定問題，及び一般化されたDiffie-Hellman 判定問題の困難性を，線型性判定問題の困難性に帰着する結果を示している．
本結果は，上記の各種判定問題困難性を仮定することが妥当であることを示している．それらの困難性結果に基づいて，新たなトラップドア全単射関数を提案している．
最後に，そのトラップドア全単射関数が導く高次元準同型暗号や各種署名方式を示している．通常署名方式の他に，ユーザのプライバシを考慮した機能を提供するブラインド署名方式及び否認不可署名方式を提案している．それらの暗号及び署名方式は全く新しいものである．

第６章は結論で，本論文で得られた成果を要約している．

氏　名	高島　克幸

（論文審査の結果の要旨）

本論文は，楕円曲線及び超楕円曲線ヤコビ多様体に関連する計算法に関する研究と，その新たな暗号系構成法への応用をまとめたものであり，得られた主な成果は次のとおりである．

１．高速処理可能なペアリング暗号用の楕円曲線の構成法に関して，新たな提案を行った．ペアリング暗号に用いる楕円曲線では，その安全性を変更する際に，埋め込み次数というパラメータが重要な役割を果たしている．また，一方，ペアリング演算の効率を高めることが，実用上重要な課題となっている．それら２要件を満たす曲線構成法を提案した．本論文の，安全性変更が容易であると共に，高速演算を実現する曲線構成法は，ペアリング暗号実用化に大きく寄与するものである．

２．実乗法写像と呼ばれる演算を利用して，あるクラスの種数２超楕円曲線ヤコビ多様体上で，新しい高速スカラー倍算法を提案した．それら曲線にはペアリング暗号に有効な曲線も含まれている．従来とは全く異なるヤコビ多様体上の演算をスカラー倍算高速化に利用した．これにより，高速演算を有する曲線のクラスが大きく広がり，また，ペアリング暗号の実用化にも寄与することになった．

３．高種数の超楕円曲線ヤコビ多様体上の高次元ベクトル空間構造を暗号に活用するために，ディストーション写像と呼ばれる演算法の数学的特性を明らかにした．特に，効率的に計算可能なディストーション写像の完全な決定を行った．数論アルゴリズム分野で，このような自己準同型環の決定は一般に困難な問題であるが，本論文は，ある特殊な曲線で，その決定を完全に行った．それ自身，理論的な寄与を有するが，下記の新たな暗号系構成法の基盤を与える結果となっている．

４．高次元ベクトル空間を暗号に応用するために，ディストーション固有ベクトル空間の定式化を行うと共に，その空間上のベクトル分解問題の計算量的困難性の評価を確立し，それに基づいて，様々な暗号及び署名法構成を行った．まず，ベクトル分解問題と，一般化された Diffie- Hellman 問題や線型性判定問題といった既存問題の間の関係を明らかにし，ベクトル分解問題困難性を示した．その困難性に基づいて，新たなトラップドア全単射関数を考案し，最後に，そのトラップドア全単射関数が導く高次元準同型暗号や各種署名方式（通常署名，ブラインド署名，否認不可署名）を提示した．それらの暗号及び署名構成法は全く新規であり，更なる新規機能実現の可能性を示している．

以上，本論文は，楕円曲線及び超楕円曲線ヤコビ多様体に関連する計算法に関する研究と，その成果の新たな暗号系構成法への応用という研究成果をまとめたものであり，学術上，実際上寄与するところが少なくない．

よって，本論文は博士（情報学）の学位論文として価値あるものと認める．

また，平成２１年２月９日実施した論文内容とそれに関連した試問の結果，合格と認めた．