氏　　名	南條　由紀
授与した学位	博　士
専攻分野の名称	工　学
学位授与番号	博甲第　　６６３２　　号
学位授与の日付	２０２２年　３月　２５日
学位授与の要件	自然科学研究科　　産業創成工学専攻 （学位規則第４条第１項該当）
学位論文の題目	A Study of Efficient Algorithms for Computing Cryptosystems Using Elliptic Curve （楕円曲線を用いた暗号システムのための効率的なアルゴリズムに関する研究）
論文審査委員	教授　　野上　保之　　教授　　豊田　啓孝　　准教授　栗林　稔

学位論文内容の要旨

Cryptography is an indispensable technique for the secure use of services on the Internet. Currently, cryptography based on an *elliptic curve*, which is called elliptic curve cryptography, is widely used as public-key cryptography. In addition to this, the elliptic curve is one of the important tools that enable various cryptography for the next generation. A map defined over the elliptic curve, which is called a *pairing*, can realize cryptography with various functions. Such cryptography is so-called pairing-based cryptography (PBC). Recently, it is expected to apply PBC for secure database services in cloud technology. It is considered that maps between elliptic curves, which are called *isogenies*, enable post-quantum cryptography that cannot be broken even though a quantum computer is developed. Such cryptography is called isogeny-based cryptography. Particularly, SIDH is one of the isogeny-based cryptosystems and is attracting attention as an alternative protocol such as DH/ECDH based on finite field/elliptic curve cryptosystems, which are adopted for the current key exchange protocols.

Firstly, to put PBC into practical use and spread it, it is necessary to improve the efficiency of the pairing on the elliptic curve. The pairing on elliptic curve is typically computed by two steps, i.e., the Miller loop and final exponentiation. Since the efficiency of the pairing strongly depends on the efficiency of these steps, this thesis especially proposes efficient algorithms for computing the final exponentiation. Besides, the efficiency of the pairing also depends on the constructions of the elliptic curve and finite field in which pairing is defined. Therefore, this thesis also proposes a method for finding attractive parameters such that the optimum constructions for pairing can be adopted. This makes it possible to easily construct of highly efficient pairing.

Secondly, to execute SIDH practically, it is necessary to improve the efficiency of the key generation phases of SIDH. The efficiency of these phases depends on the efficiency of algorithms based on Vélu's formula together with the construction of the finite field in which curves are defined. Although the previous works only considered the specific construction of the finite field, this thesis examines several possibilities of the constructions and determines the recommended constructions for efficient SIDH by an implementation. A new candidate of finite field construction contributes to expanding the elliptic curves that can be used for SIDH.

論文審査結果の要旨

本論文では，近年とくに高機能かつ堅牢な情報セキュリティを実現するとして注目をされる楕円ペアリング暗号および同種写像暗号の研究成果を報告している。楕円ペアリング暗号については，組織的に楕円ペアリング写像を構成できる曲線群に対して，その暗号計算の効率化およびその効率的な実装を可能とする曲線パラメータの設定を汎用化かつ最適化できる方法論とその理論的な裏付けを行っている。加えてそれらを実際にプログラム実装し，世界で初めて発見されるパラメータや効率的な暗号計算アルゴリズムを開発・実装した。これらの成果は，楕円ペアリング暗号に関する研究者にも広く注目されているものである。

一方で，同種写像に関しては量子計算機の台頭に対して，これを用いた解読攻撃にも耐えうる高いセキュリティを実現するための暗号（耐量子暗号）として同種写像を用いた暗号方式が期待されており，NISTの標準化プロセスにおいてもその幾つかの手法がファイナリストとして残っている。しかしながら，同種写像には複雑かつ重たい計算処理が必要になるため，これを現実的なものにするためには効率化実装を欠かすことはできない。そのような最先端の暗号技術に対して本論文では，現実にも供する効率計算アルゴリズムを提案しており，またそのためのパラメータ設定に関しても広く汎用的なアプローチから良い候補を選択できる手法を提案している。同種写像に関するこれらの研究成果は世界的にもあまり知られておらず，極めて先駆的な成果ということができる。

以上のような成果は，申請者を筆頭著者とするジャーナル論文5本，国際会議論文7本にまとめられている。その内の一つの国際会議論文はOutstanding Paper Awardを受賞している。申請者を共著者とする国内外の研究発表も10本以上を数え，広く当該分野の研究者に認められているものである。

本博士論文は，そのような複数の最先端の研究成果を網羅しつつも，その基礎的な数学的準備から詳述されており，博士（工学）の称号を与えるに相応しいものであると判断する。