氏　名	MD. AL-AMIN KHANDAKER
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　５９７０　号
学位授与の日付	平成３１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 Pairing Computation Algorithm Using KSS Curves （KSS 曲線を用いた効率的なペアリング計算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　船曳　信生　教授　田野　哲

学位論文内容の要旨

Pairing-based cryptography over the elliptic curves is a relatively new paradigm in public key cryptography. It originates many novel cryptographic protocols that were not possible without pairing. Among these protocols, ID-Based encryption can be interesting for IoT security since it can support a device's ID as a public key. On the other hand, homomorphic encryption can realize strong security and more concrete privacy of patient's information while working with encrypted medical data stored in a cloud data-server. This thesis proposes improvements of some fundamental operations on a particular type of pairing-friendly curve called Kachisa-Schaefer-Scott (KSS) curve of embedding degree 16 and 18. The thesis consists of 9 chapters.

Chapter 1 introduces the basic concepts of cryptography and the overall motivation and the contribution of the thesis.

In Chapter 2, we briefly discuss the mathematical concepts that are related to understanding the concepts of the thesis. We also define the pairing in general, and the target class pairing-friendly elliptic curves.

Chapter 3 proposes an efficient Optimal-Ate pairing for KSS-18 curve. We improve the Miller's algorithm of Optimal-Ate pairing by proposing pseudo-12-sparse multiplication. In order to evaluate our theoretic proposal, we also include some experimental results with recommended parameter settings.

Chapter 4 proposes a technique that will accelerate scalar multiplication in G_2 over KSS-18 curve. It is crucial to derive efficiently computable endomorphisms for accelerating scalar multiplication. The target G_2 group has a property that specific scalar multiplication can utilize Frobenius endomorphism that is efficiently computable. Focusing on this property, we derive an essential relation available for scalar multiplication in G_2 from the structural properties of target elliptic curve. Then, using the relation, we propose efficient scalar multiplication together with multi-scalar multiplication. Besides, from the experimental results, we show that the proposed scalar multiplication is about 60 times faster than the conventional method.

In Chapter 5, we derive twist property for target elliptic curves for the 192-bit security level and compare their performances concerning scalar multiplication. This thesis shows that the sextic twist over KSS-18 curve has an advantage over the quartic twist in KSS-16 curve.

Chapter 6 shows the state-of-the-art improvement of Optimal-Ate pairing over KSS-16 curve at the 128-bit security level. We adopt the most recent parameter and theoretically derive the most efficient pairing calculation. Besides, we also show experimental implementation and compare our result with other pairing-friendly curves.

In Chapter 7, we opt for further acceleration of the result obtained in Chapter 6 by improving the finite field arithmetic. We apply the cyclic vector multiplication algorithm for the acceleration. We show comparative results between Chapter 6's proposal and this. We also show memory optimization for existing final exponentiation algorithm.

Chapter 8 shows the G_2 scalar multiplication by applying different dimension of GLV decomposition. We show theoretical and experimental result and find that 4-dimension is optimal for efficient scalar multiplication in G_2 in KSS-16 curve.

Finally, Chapter 9 concludes this thesis.

論文審査結果の要旨

本論文では，近年とくに高機能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の効率化に関する理論的およびアルゴリズム的な研究の成果と，その実装実験報告を行っている。とくにセキュリティパラメータとして最適と考えられるKSSと呼ばれるクラスの楕円ペアリング曲線にいち早く着目し，その中の埋め込み次数16および18というパラメータでの効率化を達成している。より具体的には，楕円ペアリング暗号に必要となるペアリング写像計算や楕円スカラー倍算などについて，世界トップクラスの計算効率・処理速度を実現しており，そのいずれについても理論的なアプローチを伴ったしっかりとした提案である。また，実装した計算アルゴリズム・関数群については，計算ライブラリとしてgitHubを通じて広く活用できるように公開されている。

とくにその中でも，KSS-18曲線を用いた楕円ペアリング暗号に関しては，拡大体と呼ばれる代数系の上での計算効率化に関して，6次ツイストという同型写像を活用し，18次元のベクトル空間から，その1/6となる3次元のベクトル空間上で計算を活用できるよう効率化したことである。さらに，その18次元のベクトル空間における乗算が必要となる場合においても，そのベクトル中にゼロ係数が多く存在することを利用し，ベクトル乗算の効率を大幅にアップさせている。このような複数の効率化の総和として，楕円ペアリング暗号に係る計算コスト・処理時間を10倍以上効率化している。

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2本，国際会議論文8本にまとめられており，さらに申請者を共著者とする論文や国際会議発表は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。そのことを裏付けるものとして，IACRという情報セキュリティ研究に関する国際団体がサポートする国際会議にも複数採択されている点は特筆すべきものである。

本博士論文は，そのような複数の研究成果が実証実験も交えて詳述されており，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。