論 文 内 容 の 要 旨

博士論文題目

Pairings on Hyperelliptic Curves of Genus 2 at High Security Levels

（高セキュリティレベルにおける種数２の超楕円曲線を用いたペアリング）

氏　　名　石井　将大

（論文内容の要旨）

（１，２００字程度）

Pairings on hyperelliptic curves including elliptic curves have been applied to many cryptographic schemes (e.g., functional encryption and its varieties), and the various optimization methods that increase the speed of pairing computations have been exploited. In contrast to pairings on elliptic curves, hyperelliptic curves are not considered to be more efficient than elliptic curves for constructing general pairings. However, the extent of the difference between pairings on elliptic curves and pairings on genus 2 hyperelliptic curves has not been clarified.

This dissertation is aimed at clarifying this difference by first examining suitable pairing-friendly genus 2 curves for pairing purposes. Other researchers have pro- posed the construction of genus 2 curves, we show that the Kawazoe–Takahashi families of curves are the most efficient for constructing pairing at 192- and 256- bit security levels and also provide the cost estimations of several pairings on the curves.

Furthermore, we exploit a new variant of Weil pairing with an automorphism and propose an effective calculation method. This is the first detailed evaluation of pairings on genus 2 hyperelliptic curves at the high security levels.

氏　名	石井　将大

（論文審査結果の要旨）

本論文は，公開鍵暗号方式において利用されるペアリングについて，特に種数2の超楕円曲線上定義されるものについて包括的に調査したものである．一般的に，種数2以上の超楕円曲線を用いて構成したペアリングは，楕円曲線上のペアリングに比べ非効率的であると言われているが，具体的なペアリングの構成と，計算コストの詳細な比較評価は行われていなかった．更に，種数2以上の超楕円曲線は楕円曲線と比較して，より高次のtwist曲線や，曲線のより大きな自己同型群を持つ等，ペアリングの構成において有効的な性質を持っている．これらの点を考慮して全体的にペアリングの評価を行う必要があった．

本論文の成果は以下の通りに要約される．

1. 種数2のpairing-friendlyな超楕円曲線において高セキュリティレベル，即ち，192-，256-bitセキュリティレベルにおけるペアリングの構成を想定し，最適な選択としてKawazoe-Takahashi曲線がふさわしいことを示した．
2. 各セキュリティレベルにおいて，適切なKawazoe-Takahashi曲線のパラメタを設定し，Tate-typeペアリングにおいてはtwisted Ateペアリングが最適な構成であることを示し，その詳細なコスト評価を与えた．更に，ベンチマークテストにより具体的な実装評価を与え，コスト評価と合わせて，最新の楕円曲線上のペアリングに対する性能評価を与えた．
3. 計算コストの小さな自己同型を用いたWeil-typeペアリングの構成について，楕円曲線で得られていた結果を拡張し，種数2の超楕円曲線を利用した場合もWeilペアリングの変形として新たなペアリングが得られることを示した．更に，Kawazoe-Takahashi曲線を用いて，その自己同型を用いたWeil-typeペアリングを効率的に計算可能なことの明示的な証明を与えた．

これらは種数2の超楕円曲線上のペアリングについて初めての包括的な研究による成果であり，これにより，超楕円曲線上のペアリングと楕円曲線を用いた場合との性能差が明らかになり，実用面において，ペアリング暗号を構成する際の適切な一つの指標を与えるものと期待できる．また，本論文が示したペアリングの高速化手法は，今後の高セキュリティレベルにおけるペアリングの構成においても適用可能であり，特に自己同型を用いたWeil-typeペアリングについてはTate-typeペアリングと比較してより効率的に構成できる可能性がある．

以上から，本論文の成果は学術上のみならず，実社会における貢献度も高いものと評価できる．従って，本論文は博士（工学）の学位としてふさわしいものと認める．