氏　　名	中島　俊哉
学　位　名	博士（システム情報科学）
学位記番号	第１５号
学位授与年月日	平成２２年３月１９日
学位論文題目	超特異楕円曲線を用いたペアリング暗号の効率的な実装方法
論文審査委員	主査　高木　剛
	副査　高橋　修
	副査　小西　修
	副査　三浦　守
	副査　松尾　和人（情報セキュリティ大学院大学 教授）

論　文　要　旨

審査結果の要旨

本学位論文は超特異楕円曲線を用いたペアリング暗号の効率的な実装方法に関するもので，ペアリング暗号に対する安全な高速アルゴリズムを二つ提案している．上記の研究テーマにおいて，電子情報通信学会英文論文誌１編，情報処理学会論文誌１編，Springer LNCSレベルの国際会議論文１件に採録されている．この他にも国内での学会研究会およびシンポジウムなどで４件の講演発表を行っている．本論文は情報社会を支える多種多様なプロトコルを実現可能なペアリング暗号の高速化を課題とし，その基本演算である有限体上の乗算高速手法を提案し，その効果を実際に示したものであり，情報科学並びに情報社会の発展に貢献するところが大きい．よって本論文は博士（システム情報科学）の学位論文として十分価値のあるものと認め「合」と判定した．