審 査 の 結 果 の 要 旨

氏　　名　　スッパキットパイサーン　ウォラポン

本論文は、楕円曲線暗号の計算上ボトルネックとなっているスカラー乗法を、スカラー表現を乗法の計算をより高速に行うことが可能なように表現することによって、高速化するアルゴリズムを提案したものである。

本論文は六章からなり、第一章では、まず、本論文のようなスカラー乗法計算の高速化が求められる背景として現在最も用いられている暗号技術のひとつである楕円曲線暗号における問題を挙げ、研究の必要性および動機づけを明らかにしている。さらに、これまでのスカラー乗法計算を効率化するための手法の基本的な考え方の概略を述べるとともに、本論文がそれらに対してどのような貢献を行ったかを概観している。さらに第二章においては、本論文の背景知識として、楕円曲線暗号、その中で用いられるスカラー乗法、そのスカラー乗法を高速化するための既知のスカラー表現方法の概略を紹介している。

スカラー乗法の効率化は、積をとる２つのスカラーのそれぞれの表現間で定義されるハミング距離が小さいような２つのスカラーの表現を見つけることができれば、達成されるが、第三章では、本論文の中核となる、ハミング距離を理論的に最小化する手法を提案している。さらに、第四章では、その理論的な性能をマルコフ連鎖解析の手法を用いて解析し、一部のスカラー表現においては、提案手法が最適であることを示すなど、永年の未解決問題を解決している。さらに、第五章においては、第四章までのスカラー表現をさらに複数の底に対応した場合のスカラー乗法を効率化するスカラー表現を最適化する手法について提案を行っている。第六章では、本論文で提案した手法と有効性を総括し、さらに今後考察すべき課題についての展望が示されている。以上のように、本論文は、スカラー乗算という基本的演算を効率化するアルゴリズムを提案することによって、楕円曲線暗号演算の効率化を図ることに成功したものである。

なお、本論文の第三章、第四章、第五章は、枝廣正人氏、今井浩氏との共同研究であるが、論文提出者が主体となって立案、分析、検証を行ったもので、論文提出者の寄与が十分であると判断する。

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる。