博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：　超楕円曲線暗号の構成に関する研究
申請者　：　小﨑俊二
審査委員会　：　主査　教授　松尾和人
副査　教授　有田正剛
副査　教授　佐藤直
副査　教授　長尾孝一（関東学院大）

Ⅰ．論文内容の要旨

本論文は、「超楕円曲線暗号の構成に関する研究」と題し、6 章からなっている。

第 1 章「序論」では、本研究の背景と課題および本論文の構成を述べている。まず、公開鍵暗号のデファクトスタンダードである RSA 暗号と比較し楕円曲線暗号がより高い安全性を有することを説明し、楕円曲線暗号の一般化として超楕円曲線暗号が得られること説明している。さらに、超楕円曲線暗号は、楕円曲線暗号と比較してよりコンパクトな基本演算から構成されるため、コンパクトかつ効率的な公開鍵暗号を実現するものとして期待されていることが説明されている。次に、超楕円曲線暗号を実用化するための課題として、「暗号系の安全性」、「安全な暗号系の構成法」、「暗復号処理の高速化」を挙げ、本論文は、超楕円曲線暗号の実用化を目的として、これらの課題のそれぞれについて課題の解決につながるアルゴリズムの提案を行うものであることを述べている。

第 2 章「超楕円曲線とその Jacobian」では、本論文において必要となる数学的知識について準備し、その中で skew-Frobenius 写像を提案している。さらに、この写像の具体的構成を示すとともに、これを効率的に計算可能であることを示している。

第 3 章「離散対数問題とその拡張の解法」では、超楕円曲線暗号の安全性の根拠となる離散対数問題とその拡張問題について説明し、超楕円曲線上の離散対数問題に対して適用可能な解法をまとめた後に、離散対数問題の拡張問題の一つである q-weak Diffie-Hellman 問題の解法に対し、事前計算テーブルを用いることと、計算手順を変更することによってアルゴリズムの漸近計算量を小さくする改良を提案している。さらに、提案アルゴリズムによる攻撃を無効化する方法について論じている。

第 4 章「安全な超楕円曲線暗号の構成」では、安全な超楕円曲線暗号の設計に必要な位数計算アルゴリズムの改良を行っている。まず、種数 2 の超楕円曲線に対する既存の位数計算アルゴリズムと、これに利用されている 2 冪ねじれ計算アルゴリズムについて説明した後に、種数 2 の超楕円曲線の 2 冪ねじれ点の存在する拡大次数に関する補題と 2 ねじれ群の 2 冪ねじれ点への作用に関する補題を示している。そして、これらの補題を利用した 2 冪ねじれ計算アルゴリズムを提案している。また、実装実験により提案アルゴリズムの有効性を確認している。次に、超楕円曲線の Hasse-Witt 行列とその計算アルゴリズムについて説明し、超楕円曲線の位数計算に Hasse-Witt 行列を利用可能であることを説明している。そして、アルゴリズムに現れる p 進整数の必要精度を計算中に段階的に削減可能であり、多項式の reversal を利用することでこの精度を更に削減可能であることを示した後に、これらの性質を利用したアルゴリズムの高速化手法を提案している。また、実装実験により、この高速化法の有効性を確認している。

第 5 章「高速な超楕円曲線暗号の構成」では、超楕円曲線暗号において暗復号処理時間の殆どを占めるスカラー倍算に、第 2 章で提案した skew-Frobenius 写像を利用可能であることを示した後に、skew-Frobenius 写像の性質を利用した、既存のアルゴリズムと比較し事前計算テーブルのサイズが小さいスカラー倍算アルゴリズムを提案している。そして、提案アルゴリズムと既存のスカラー倍算アルゴリズムを 32bit 組込 CPU を搭載したスマートフォン上で実装比較し、提案アルゴリズムの現実的な優位性を確認している。

第 6 章「結論」では、以上の成果をまとめ、第 1 章で挙げた課題に対する本論文の貢献と今後の課題について述べている。

Ⅱ. 論文審査結果の要旨

以上を要するに、本論文は情報セキュリティ要素技術として有用であると期待されている超楕円曲線暗号を実用化するために必要となる複数のアルゴリズムを提案し、その有効性を実装結果によって示したものであって、情報セキュリティ技術延いては情報科学の発展に寄与するところが少なくない。よって、本論文は情報学における博士論文として価値のあるものと認める。

Ⅲ. 審査経過

本審査委員会は、2010 年 1 月 29 日に論文内容とこれに関連する事項について口述試問を行い、申請者が学位取得にふさわしい知見を持つものと判断した。