Efficient Algorithms for Elliptic Curve Cryptosystems using Endomorphisms

伯田, 恵輔

https://doi.org/10.15017/1398315

出版情報：九州大学, 2013, 博士（機能数理学）, 課程博士
バージョン：

氏　　名：伯田 恵輔

論文題目：Efficiency and Security Analysis of Public Key Schemes
via Endomorphisms of Algebraic Varieties
(代数多様体の自己準同型写像を用いた公開鍵暗号の効率性と安全性の解析)

区　　分：甲

論　文　内　容　の　要　旨

公開鍵暗号系は、暗号化、デジタル署名、鍵交換の機能を提供し、なりすまし、盗聴、改ざん、といったセキュリティ脅威を防ぐ基本的な対策技術である。公開鍵暗号系の安全性は素因数分解問題、有限体または楕円曲線上の離散対数問題などの数論問題の計算困難性に依存しており、そのため、公開鍵暗号系では暗号学的数論関数の計算が処理全体の大部分を占める。公開鍵暗号系の一種である楕円曲線暗号は、世の中で標準的に利用されている RSA 暗号と比べ、鍵長が短いこと、高い効率性を兼ね備えていることから、組込み機器での利用で有望視されている。楕円曲線暗号で利用される暗号学的数論関数はスカラー倍算と呼ばれる処理であり、与えられた楕円曲線上の点と正整数から整数倍点を計算する処理である。十分な計算能力を持たない機器で楕円曲線暗号を実用的に用いるためにはスカラー倍算の高速化が望まれる。

一方、代数多様体の自己準同型写像は現代数学において重要な役割を担っている。例えば、楕円曲線の自己準同型写像は、楕円曲線の数論的な側面を研究するために重要であり、多項式同型写像は Jacobian conjecture や tame generators problem などのアフィン代数幾何の問題で重要である。

本論文では代数多様体の自己準同型写像を扱う。暗号では公開鍵暗号系の暗号学的数論関数の計算の高速化だけでなく、公開鍵暗号系の安全性評価においても自己準同型写像が利用されている。有限体上定義された部分体楕円曲線（楕円曲線が有限体 k 上定義されており、暗号利用では k の拡大体の有理点集合に焦点を当てる)では、Frobenius 写像は計算機上で高速に計算できる。そのため、スカラーの Frobenius 展開（整数係数の Frobenius 写像による多項式表現)を利用したスカラー倍算の計算方法が知られている。しかしながら、効率性の改善のためには、非零な係数の個数が少ない Frobenius 展開を構成することが望まれる。加えて、Frobenius 展開の非零である係数の個数を調べることは、スカラー倍算の効率性を解析するだけでなく、無駄な処理がないかどうかを判定することにも繋がるため、重要な課題である。

また Frobenius 展開は、デジタル署名の一括検証（複数のデジタル署名を同時に検証することによる検証処理の高速化技術)において、検証プロセスを第三者から秘匿したり、検証処理を高速化するために利用されるが、従来技術では署名の個数が少ない場合に効率性が落ちるという問題点がある。

以上を鑑みて、数種類の楕円曲線に対し、Frobenius 展開の性質を調べ、以下の結果を得た：

1. 米国立標準技術研究所や標準化団体が利用を推奨する楕円曲線（Koblitz 曲線)における非零な係数の個数が少ない Frobenius 展開を、Koblitz 曲線とは異なる楕円曲線上で構成した。また、上記 Frobenius 展開が暗号学的に望ましい性質をもつことを証明した。
2. 上記で述べた Koblitz 曲線における非零な係数の個数が少ない Frobenius 展開は、ある種の条

件のもとで、零な係数の個数が最小であることが証明されている。この Frobenius 展開は長さ(多項式と見なしたときの次数)もほぼ最小であることを示した。また、上記の最小性の別証明を示した。さらに、上述の Frobenius 展開の長さを最小にする変換方法を得た。

3. 2 種類の楕円曲線に対し、Frobenius 展開の表現の一意性などを証明し、署名の個数が比較的少ない場合における高速かつ安全な一括検証方法を構成した。

これらの結果は、世の中で実用上安全かつ高速に楕円曲線暗号を実現する方法を提供するとともに、(ある種の条件のもとで)実用上利用されている楕円曲線暗号の効率性の理論的な限界を与えている。