| | |
|---|---|
| 氏　　名 | 加藤　英洋 |
| 授与した学位 | 博　士 |
| 専攻分野の名称 | 工　学 |
| 学位授与番号 | 博甲第３９９６号 |
| 学位授与の日付 | 平成２１年　９月３０日 |
| 学位授与の要件 | 自然科学研究科　産業創成工学専攻<br>（学位規則第５条第１項該当） |
| 学位論文の題目 | Efficient Algorithms of Multiplication and Exponentiation in Extension Field for Cryptographic Applications<br>（暗号応用を目的とした，拡大体上の乗算およびべき乗計算の効率的アルゴリズム） |
| 論文審査委員 | 教授　森川　良孝　　教授　舩曳　信生　　准教授　中西　透 |

## 学位論文内容の要旨

近年ID ベース暗号など，ペアリングを用いる暗号応用技術が注目されている．ペアリングは，楕円曲線上の加法群から拡大体上の乗法群への双線形写像として定義される．ペアリング親和曲線では標数$p$，拡大次数$m$に制限が加えられ，その条件のもとで高速にペアリングを実装する必要がある．しかし従来の拡大体構成法（乗算アルゴリズム）はこの制限を満たすものではなかった．

そこで本論文では，type-<$k,m$>ガウス周期正規基底(GNB)，type-<$2k,m$>GNBを用いた拡大体構成法とその乗算アルゴリズムを提案している．前者および後者のGPNBはそれぞれ$8p$が$m(p-1)$を割り切る場合および$4p$が$m(p-1)$を割り切る場合を除いて，任意の$p,m$の組に対して構成可能である．本論文ではこれらの拡大体構成法のもとで，新たに高速な乗算アルゴリズムを提案し，特別な$p,m$だけに適用できる最適効率体(OEF) 構成法に比べて比肩する時間で乗算が実行できることを示している．

一方拡大体の応用分野では主たる演算として拡大体上のべき乗算がよく用いられる．例えばペアリングの計算では，約半分の時間が拡大体上のべき乗算に費やされることも少なくない．本論文では，このような要求からフロベニアス写像と呼ばれる写像を効果的に用いた新たな拡大体上べき乗算アルゴリズムを提案している．

正規基底表現を用いた場合フロベニウス写像(FM)と呼ばれる演算は，要素の入れ替えだけで実行可能である．したがってべき乗数$n$が標数$p$より大きい場合には，FMを用いることによりべき乗算を高速に行うことが可能となる．この事実に注目してFrobenius Abusing(FA)法と呼ばれるアルゴリズムが提案されている．FA法では，1) べき乗算に多くの事前計算を用いるため，被べき数が変化する場合は計算量が増大する，2) FMが高速実装できない拡大体では非効率である．これらを解決するために，本論文では並列バイナリ法を併用したFM-べき乗算アルゴリズムを提案している．FA法と比較すると，乗算回数は平均で20%ほど増加するが，フロベニアス写像は逆に削減できている．すなわち提案べき乗算法は，上記1),2)の問題をもつ拡大体において実用的であることを示している．

## 論文審査結果の要旨

近年ID ベース暗号など，ペアリングを用いる暗号応用技術が注目されている．ペアリングは，楕円曲線上の加法群から拡大体上の乗法群への双線形写像として定義される．ペアリング親和曲線では標数$p$，拡大次数$m$に制限が加えられ，その条件のもとで高速にペアリングを実装する必要がある．しかし従来の拡大体構成法（乗算アルゴリズム）はこの制限を満たすものではなかった．

そこで本論文では，type-<$k,m$>ガウス周期正規基底(GPNB)，type-<$2k,m$>GPNBを用いた拡大体構成法とその乗算アルゴリズムを提案している．前者および後者のGPNBはそれぞれ$8p$が$p(m-1)$を割り切る場合および$4p$が$p(m-1)$を割り切る場合を除いて，任意の$p,m$の組に対して構成可能である．本論文ではこれらの拡大体構成法のもとで，新たに高速な乗算アルゴリズムを提案し，特別な$p,m$だけに適用できる最適効率体(OEF) 構成法に比べて比肩する時間で乗算が実行できることを示している．

一方拡大体の応用分野では主たる演算として拡大体上のべき乗算がよく用いられる．例えばペアリングの計算では，約半分の時間が拡大体上のべき乗算に費やされることも少なくない．本論文では，このような要求からフロベニアス写像と呼ばれる写像を効果的に用いた新たな拡大体上べき乗算アルゴリズムを提案している．

正規基底表現を用いた場合フロベニウス写像(FM)と呼ばれる演算は，要素の入れ替えだけで実行可能である．したがってべき乗数$n$が標数$p$より大きい場合には，FMを用いることによりべき乗算を高速に行うことが可能となる．この事実に注目してFrobenius Abusing(FA)法と呼ばれるアルゴリズムが提案されている．FA法では，1) べき乗算に多くの事前計算を用いるため，被べき数が変化する場合は計算量が増大する，2) FMが高速実装できない拡大体では非効率である．これらを解決するために，本論文では並列バイナリ法を併用したFM-べき乗算アルゴリズムを提案している．FA法と比較すると，乗算回数は平均で20%ほど増加するが，フロベニアス写像は逆に削減できている．すなわち提案べき乗算法は，上記1),2)の問題をもつ拡大体において実用的であることを示している．

以上本論文は，暗号実装上有意な成果を上げており，博士の学位に値すると判定する．