公開鍵暗号系での利用を目的とした汎用拡大体の構成に関する研究開発
(042108003)

Widely applicable extension field as the definition fields
of various public-key cryptographies

研究代表者
野上保之　　岡山大学大学院自然科学研究科
Yasuyuki Nogami, Okayama University Graduate School of Natural Science and Technology,

研究期間　平成 16 年度～平成 18 年度

本研究開発の概要

近年、様々な暗号方式およびその応用技術が提案されている。とりわけ、電子認証技術を実現できる公開鍵暗号方式は、現代情報化社会における重要な要素技術となりつつある。その多くの公開鍵暗号を定義するための代数系として有限体が用いられる。すなわち、そのような公開鍵暗号方式やその応用技術を効率よく実現するために、有限体における基本的な演算（乗算など）を効率よく実装する必要がある。しかし、近年の暗号応用技術では、有限体（とりわけ拡大体）を定義する上で必要となる標数（素数）や拡大次数（ベクトル空間の次元数）に制限を加えることも少なくなく、従来から提案されている効率の良い実装手法が必ずしも適用できるとは限らない。そのような問題に対して、本研究開発では極めて汎用的であり、かつ効率の良い演算をもつような拡大体の実装法（とりわけ乗算の実装法）を開発するものである。

Abstract

Recently, a lot of cryptographic applications have been proposed. Especially, public-key cryptography and its applications have received much attention. Most of them need arithmetic operations in a certain extension field. Thus, it is quite important to efficiently implement the fundamental arithmetic operations such as a multiplication in the extension field. In addition, the implementation needs to be applicable for various parameter settings such as the characteristic and extension degree. The previous works could not be applied for every case. In this research, an efficient multiplication algorithm that can be applied for an arbitrary pair of the characteristic and extension degree is developed.

１．まえがき

公開鍵暗号およびその応用技術の分野において、有限体、とりわけ拡大体を用いる場面が増えてきている。例えば、楕円曲線暗号や楕円曲線上のペアリングと呼ばれる双線形写像を用いた暗号応用技術などである。これら公開鍵暗号方式およびその応用技術を効率よく実装する上で、そのベースとなる拡大体における種々の基本的な演算（乗算などの四則演算）を効率的に実装する必要がある。

本研究開発では、拡大体をベースとするような様々な公開鍵暗号方式およびその暗号応用技術に対して汎用的に用いることができる拡大体、とりわけ拡大体における乗算の実装手法について研究開発を行うものである。

２．研究内容及び成果

2.1　本研究のターゲットとなる課題

拡大体を定義する上で重要となるパラメータとして、標数と呼ばれる素数、拡大次数と呼ばれるベクトルの次元数を表す正整数などがある。例えばペアリングというアプリケーションを考えた場合、これらのパラメータは、ある一定の条件を満たす必要がある。その一方で、従来に用いられてきた拡大体における計算の高速な実装手法についても同様に、ある一定の条件を満たさなければならないものがほとんどである。

これまで広く用いられてきている（高速な演算をもつ）拡大体として optimal extension field （OEF）がある。OEF が準備できるための条件は、拡大次数のすべての素因数が、標数から 1 を引いた正整数を割り切れなければならないというものである。この条件による制約のため、OEF を準備できるパラメータ自身も限定される。

このように、ペアリングのような応用技術に起因するパラメータの制約と、拡大体の実装手法に起因する制約とを共に満たせた場合に、もっとも効率的にその暗号応用技術が実装できると言える。例えばペアリング実装において、標数として 160 ビット程度の素数を用い、拡大次数には 12 という比較的に小さい正整数を用いることがあるが、このようなパラメータに対して OEF を準備できる割合は 3 割程度であることが実験的に分かっている。

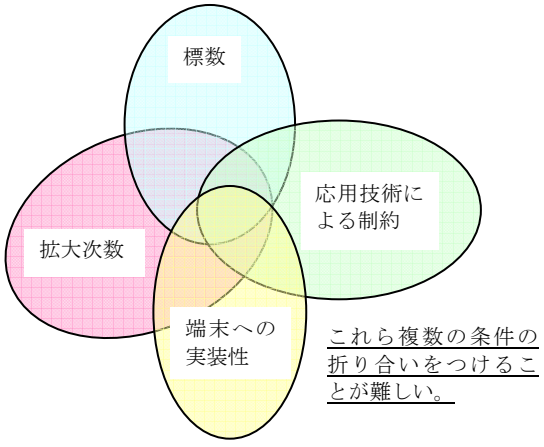

図 1　ターゲットとする課題のイメージ

これまでの研究成果として、標数および拡大次数に対して、(OEF などの従来手法と比べて) 汎用的な拡大体における乗算アルゴリズムである cyclic vector multiplication algorithm (CVMA)を開発してきている。しかしながら、

それでもなお、先に示したようなペアリングのためのパラメータの条件に対しては完全にサポートできていない。OEF を組み合わせて用いることを考えても 7 割程度のサポートにしかならないことが実験的に分かっている。

2.2 本研究成果の概要

拡大体を定義する上で重要となるパラメータである標数および拡大次数に対して汎用的であり、かつ効率よく拡大体上での演算（とりわけ乗算）を行う手法、アルゴリズムの開発を目指した。これまでの研究成果である乗算アルゴリズム CVMA は、ある一定の条件を満たす標数および拡大次数に対してしか用いることができなかった（図 2）。

（条件1） 拡大次数を m として、m+1が素数である
（条件2） 標数を（素数）pとして、pをべき乗してm+1で割って余りをとるという計算を繰り返して、再びpになる周期がm+1である

図 2　標数および拡大次数に対する CVMA の一条件

これに対して本研究では、新たなパラメータを加えて条件を緩和し、任意の標数および拡大次数に対して対応できるよう改良した CVMA を開発した（以下、改良 CVMA）。より具体的には、任意の標数および拡大次数に対して一つのプログラムで対応できる乗算アルゴリズムを開発した。図 3 に、拡大次数が 3 の場合の CVMA の計算式を示す。このアルゴリズムは、拡大体をベースにするような楕円曲線暗号や楕円曲線上のペアリングを用いた暗号応用技術などに対して汎用的に用いることができる。具体的な実装データを紹介すると、標数が 160 ビット程度の素数であり埋め込み次数が 12 のペアリング（ここでは Tate ペアリングと呼ばれるペアリング計算を用いている）に対して組み合わせた実装で、ペアリング計算 1 回に数十ミリ秒程度で処理を行えている。

$$(x_1, x_2, x_3) \times (y_1, y_2, y_3) = (z_1, z_2, z_3)$$

$$z_1 = -(x_2 - x_4)(y_2 - y_4) - x_1 y_1$$
$$z_2 = -(x_3 - x_4)(y_3 - y_4) - x_2 y_2$$
$$z_3 = -(x_1 - x_2)(y_1 - y_2) - x_3 y_3$$

図 3　拡大次数が 3 の場合の CVMA の計算式

2.3 付随するその他の研究成果

本研究の成果に付随して、幾つかの関連する成果が得られた。ここでは、その中の一つとして、同型な拡大体間における基底変換に関する研究成果を説明する。

標数および拡大次数が等しい拡大体は、どのような実装手法を用いても同型となる。しかしながら、その実装手法（用いる基底の選び方など）によって、演算の性能が異なってくる。拡大体における乗算を高速に行えるように実装することもできるし、何らかの写像のような特殊な計算に特化して効果的に実装することもできる。二つの異なる基底を用いた場合、例えばそのターゲットが同じ楕円曲線暗号というアプリケーションであったとしても、相互でのデータの互換性をもたせることが困難となる。このような同型な拡大体に対して、本研究の成果を仲介することによってデータを相互に変換すること（基底変換）ができた。これによって、例えば複数のメーカーなどが、ある公開鍵暗号やその応用製品を、同じ標数および拡大次数、かつ異なる基底を用いて開発した場合に、これら製品間でのデータの互換性を与えることができるようになる。

３．むすび

本研究開発では、拡大体をベースとするような様々な公開鍵暗号方式およびその暗号応用技術に対して汎用的に用いることができる拡大体、とりわけ拡大体における乗算の実装手法について研究開発を行った。本研究の成果は、近年とくに注目を浴びている楕円曲線上のペアリングを用いた暗号応用技術にも有効に用いることができるため、広く利用されることが期待される。

【誌上発表リスト】

[1] Y.Nogami, S.Shinonaga, Y.Morikawa, "Fast Implementation of Extension Fields with TypeII ONB and Cyclic Vector Multiplication Algorithm", IEICE Trans. Fundamentals., Vol. E88-A, No. 5, pp.1200-1208, 2005.5

[2] W.Feng, Y.Nogami, Y.Morikawa, "An Efficient Square Root Computation in Finite Fields GF(p^{2d})", IEICE Trans. Fundamentals of Electronics Communications and Computer Science, vol.E88-A, no.10, pp.2792-2799, 2005.10

[3] H.Katou, W.Feng, Y.Nogami, and Y.Morikawa, "A High-Speed Square Root Algorithm in Extension Fields", The 9th International Conference on Information Security and Cryptology (ICISC2006) LNCS4296, pp.94-106, 2006.11.30

【申請特許リスト】

[1] 野上保之、森川良孝、拡大体の乗算プログラム及び拡大体の乗算装置、日本、2006 年 7 月 24 日

【受賞リスト】

[1] 野上保之、森川良孝、第 6 回 LSI IP デザインアワード（研究助成賞）、“Cyclic Vector Multiplication Algorithm による拡大体上乗算回路”、平成 16 年 5 月 20 日（東京都品川カンファレンスセンター）

[2] 那須弘明、野上保之、難波諒、森川良孝、第 57 回中国支部連合大会電気学会優秀論文発表賞、“Type-II AOPF を用いた高速な既約多項式生成法”、平成 18 年 10 月 21 日

【報道発表リスト】

[1] “楕円曲線暗号およびその応用技術のための高速計算装置”、イノベーションジャパン 2006、平成 18 年 9 月 13－15 日

【本研究開発課題を掲載したホームページ】

http://www.trans.cne.okayama-u.ac.jp/~nogami
（論文、学会発表等の情報を掲載）