氏　　名	酒見 由美
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4391号
学位授与の日付	平成２３年　３月２５日
学位授与の要件	自然科学研究科　産業創成工学専攻 （学位規則第５条第１項該当）
学位論文の題目	Efficient Pairings and Scalar Multiplications for Next Generation Public Key Cryptography （次世代公開鍵暗号のための効率的なペアリング計算およびスカラ倍算）
論文審査委員	教授　森川　良孝　　准教授　野上　保之　　准教授　中西　透

学位論文内容の要旨

Recently, pairing-based cryptographies such as ID-based cryptographies, group signature authentications have received much attentions.

This thesis accelerates scalar multiplications in G1 and G2 that are frequently carried out, and proposes efficient pairings. However, they have a problem with processing time because a fairly complex calculation is required for their processing. Due to this problem, these sophisticated cryptographies have not yet led to practical use. In this thesis, we propose efficient methods to calculate operations required for pairing-based cryptographies.

In Chapter 2, we briefly review the mathematical fact to define the pairing, and describe about the conventional pairing such as Tate, Ate, it twisted Ate pairings. In addition, a target class of elliptic curves are shown. Ate and twisted Ate pairings improves Tate pairing by setting certain groups that have a special properties to G1 and G2.In this thesis, we target Ate and twisted Ate pairings, and accelerates scalar multiplications in their G1 and G2. Then, new pairings respectively based on Ate and twisted Ate pairings are proposed in later chapters.

Chapter 3 proposes an efficient scalar multiplication in G2 that is used by Ate and twisted Ate pairings. To accelerate a scalar multiplication, it is important that a certain scalar multiplication is calculated by efficiently computable endomorphisms. A target G2 has a property that a certain scalar multiplication is calculated by Frobenius endomorphism that is efficiently computable. Focusing on this property, we derive a key relation available for a scalar multiplication in G2 from the structural properties of target elliptic curves.Then, using the relation, an efficient scalar multiplication is proposed. From experimental results, we show that the proposed scalar multiplication is about 40% faster than the conventional method.

Chapter 4 proposes an efficient scalar multiplication in G1 that is used by Ate and twisted Ate pairings. A target G1 does not have the property similar to G2 such endomorphism is available for a scalar multiplication. Therefore, we can not use the method proposed in chapter 3 to a scalar multiplication in G1.In order to solve this problem, we propose a new endomorphism available for a scalar multiplication in G1.Using the endomorphism, a key relation is derived in the same manner as G2.Then, using the key relation, an efficient scalar multiplication is proposed. From experimental results, this chapter shows that the proposed method is about 30% faster than the conventional method.

In Chapter 5, the rule of addition and multiplication for pairing calculation are described, and it is shown that the approach for accelerating scalar multiplications is also applicable to pairing calculations. Then, we proposes a new pairing based on Ate pairing using the key relation of chapter 3.This is because the property of G2 is closely related to Ate pairing.From experimental results, we show that the proposed pairing is about two times faster than Ate pairings.

On the other hand, the key relation proposed in chapter 6 is closely related to twisted Ate pairing.Focusing on this property, chapter 6 proposes an efficient pairing based on twisted Ate pairing using the key relation.

論文審査結果の要旨

現代情報通信サービスでは，認証や安全性保障，否認防止等を実現する公開鍵暗号が重要なもののであり，中でも属性ベース暗号やグループ署名など，従来暗号より利便性が向上した公開鍵暗号応用技術が注目されている．これらの暗号応用は，数学的に複雑な**ペアリング**と呼ばれる演算が必須であり処理に時間が掛ることから，未だ実用化に至っていない．本論文はペアリング暗号における２つの主要演算を高速化し，ペアリング応用の道を開くことを目的とした．

ペアリングは，２つの楕円加法群$\mathbb{G}_1, \mathbb{G}_2$から乗法群$\mathbb{G}_3$への双線形写像として定義されるが，これらの群を“拡大体”の部分群として埋め込むため計算量が大きくなる．また上述の応用では暗号化・復号時にペアリングに加えて$\mathbb{G}_1, \mathbb{G}_2$上のスカラ倍算と$\mathbb{G}_3$上のベキ乗算を頻用するため，これらにも相当の計算量が必要となる．上の２つの主要演算とはスカラ倍算とペアリング演算のことである．

まずAteペアリング（twist版も含む）で用いる群$\mathbb{G}_2$上のスカラ倍算を高速化した．$\mathbb{G}_2$には計算を全く必要としないFrobenius写像と呼ばれる有理点写像が存在する．提案法では，この写像を組み合わせることで，位数の四乗根程度のスカラ倍に等価である写像を導出し，高速化を行う．そして従来法の60％で計算できることを実験で確認した．一方$\mathbb{G}_1$は素体上の群であるため，Frobenius写像は恒等写像となり$\mathbb{G}_2$と同じ策が奏功しない．そこで，形式的に$\mathbb{G}_1$を高次拡大体に写像し，そこでのFrobenius写像と等価な操作を$\mathbb{G}_1$で考えることにより，新たな関係式を導出し高速化に利用した．その結果従来法の70％で計算できることを実験で確認した．

次に，上述のスカラ倍算の高速化アプローチをペアリング計算にも適用できることを指摘し，上述の$\mathbb{G}_2$の手法をAteペアリングに適用した．また$\mathbb{G}_1$の手法も同様に適用可能であるが，とくにこの場合は並列化が可能であることを始めて指摘した．従来のAteペアリングに比べ$\mathbb{G}_2$手法で約２倍，$\mathbb{G}_1$並列化手法で約３倍の高速化を確認した．

以上のように本論文はペアリング応用に道を開く新たな解決法を提案した点で斬新性・有効性が認められ，博士の学位に値すると認める．