氏　　名	LE HOANG ANH
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　　７１３５　　号
学位授与の日付	２０２４年　９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４条第１項該当）
学位論文の題目	ELiPS-based Ciphertext-Policy Attribute-Based Encryption （ELiPS ベースの暗号文ポリシー属性ベース暗号）
論文審査委員	教授　野上　保之　　教授　豊田　啓孝　　准教授　福島　行信

学位論文内容の要旨

This thesis is organized as follows:

Chapter 1: We introduce overall cryptography and Ciphertext-Policy Attribute-Based Encryption (CP-ABE). Then we outline the problems of the original CP-ABE and our motivation for addressing them. The major contributions of this thesis are also presented in this chapter.

Chapter 2: We briefly discuss the mathematical concepts necessary for understanding this thesis. We define modular arithmetic, group, ring, field, frobenius map, elliptic curve, sextic twist, hash function, pairing, types of pairing, and the discrete logarithm problem, including the elliptic curve discrete logarithm problem.

Chapter 3: We introduce an overview of prominent pairing-based cryptography libraries, such as PBC, RELIC, MCL, and ELiPS. We then show a comparison between these prominent libraries in terms that are mainly utilized in the CP-ABE algorithm. Additionally, we present an overview of an access tree, which plays a crucial role in determining who can access encrypted data. Finally, we provide an overview of the CP-ABE scheme.

Chapter 4: We present the implementation of ELiPS-based CP-ABE, including generating a generator g, transforming asymmetric pairing to symmetric pairing, and modifying CP-ABE for integration with the ELiPS framework. We also discuss the experimental evaluation and results.

Chapter 5: We propose two methods to improve the decryption process time in ELiPS-based CP-ABE by minimizing the number of final exponentiations and inversions. We then evaluate our proposal and discuss the results.

Chapter 6: We perform a further performance analysis of ELiPS-based CP-ABE with optimized decryption functions. We describe the evaluation setup and assess the performance of ELiPS-based CP-ABE with these optimizations in terms of decryption time and total execution time.

Chapter 7: We conclude the thesis and outline future works.

論文審査結果の要旨

楕円ペアリング暗号を応用した属性署名技術の効率実装に関する研究を進めており、とくにその成果はELiPS（Efficient Library for Pairing Security）ライブラリと呼ばれる計算ライブラリをベースに改良しながら用いることで、その多くの機能処理について世界最高速での効率化実装を達成したものである。そこに至るまでの理論的な数式およびアルゴリズムの探究、それをプログラミング実装した上での評価および考察、さらにはその成果を他の研究成果やライブラリと理論および実装比較しながらアップデートしてきている。

具体的には、Ciphertext Policy Attribute-Based Encryption（暗号文ポリシー属性ベース暗号：以下、CP-ABE）を考える。これは、様々な条件分け・ヒエラルキーを木構造として記述し、その分岐・条件判定を暗号文ベースで処理するような、属性ベース暗号である。そのヒエラルキーに対して属性を割り当て（例えば教育機関であれば教員・学生の別など）、その判定を暗号文によって秘密裏に処理できるものである。これは広く、PBCライブラリと呼ばれる楕円ペアリング暗号ライブラリを中心に実装されてきた。ここに大きく2つの問題がある。1つは、その暗号強度を80ビットから128ビットセキュリティのレベルに引き上げなければならないこと、もう1つはこれをIoTデバイスなどでも処理できるように効率化する必要がある点である。これらの課題に対して3つのアプローチで本研究は解決を試みている。そのアプローチの1つ目は、セキュリティレベルを大きく上げるためには計算の効率化が必要であり、PBCライブラリが用いている技術が対称型（symmetric）のに対して本研究では非対称型（asymmetric）を用いている点である。これらを巧みに型変換しながら、計算効率化に向けた基礎を構築している。そして2つ目のアプローチとして、ペアリング暗号がMillerループおよび最終べきと呼ばれる2つの計算処理から構成されていることに着目し、それらを分けて考えることによって大幅な計算処理の効率化を実現したのみならず、とくに計算処理時間のかかる逆数計算についてもその必要回数を大幅に少なくしている。そして3つ目として、具体的なアプリケーションを想定して他のライブラリとも実装評価を行いながら、本研究成果（ELiPSライブラリベース）がもっとも効率的にCP-ABEを実現できることを実証している。

それらアプローチと研究の成果をまとめ、国際会議・ジャーナル論文にて発表してきており、十分な研究成果を上げていると考えられるため「合」と判定する。