氏名	NASIMA BEGUM
授与した学位	博　士
専攻分野の称	工　学
学位授与番号	博甲第５０４５号
学位授与の付	平成２６年　９月３０日
学位授与の件	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	A Study of Efficient Proofs for Conjunctive Normal Forms on Attributes in Anonymous Authentication Systems （匿名認証システムにおける属性の和積標準形の効率的証明に関する研究）
論文審査委員	教授 舩曳信生　教授 田野 哲　准教授 野上保之　教授 中西 透（広島大学）

学位論文内容の要旨

In this thesis, firstly, we propose an anonymous credential system with the constant-size proofs for CNF formulas and the efficient proof generation using an extended accumulator and the zero-knowledge proof, and show experimental results based on the implementation. Secondly, we propose an extension of the anonymous credential system with the constant-size proofs for CNF formulas to reduce the long public key. Thirdly, we propose an efficiency improvement of the computational overhead based on online/offline precomputation technique to reduce the online computational costs of the proof generation in case of lots of AND relations in the proved CNF formulas.

In Chapter 2, we start this thesis by giving an overview on the mathematical fundamentals for pairing-based group signature schemes in this thesis. This chapter covers the introduction of the mathematics setting such as groups, bilinear maps, and the basic concept of pairings. Then, the complexity assumptions and cryptographic primitives used in this thesis are illustrated.

In Chapter 3, we propose the construction of a pairing-based anonymous authentication system with efficient proofs, such that the combinations of AND and OR relations on attributes can be proved as CNF formulas. The proposed system is constructed using a paring-based extended accumulator. This chapter also illustrates the design of implementation of anonymous authentication system for user attributes.

In Chapter 4, we give the implementation of a pairing-based anonymous authentication system which is proposed in Chapter 3. This chapter covers the algorithm to achieve an efficient proof generation and shows the measurement results of the prover time and the verification time.

In Chapter 5, we describe an extension to reduce the public key size and an evaluation of the efficiency based on an implementation.

In Chapter 6, we explain an offline/online technique for efficiency improvement. This chapter also shows the overhead of processing times and data sizes with the efficiency improvement.

Finally, in Chapter 7, we conclude this thesis together with some future works.

論文審査結果の要旨

In this thesis, she presented the study on efficient proofs for Conjunctive Normal Forms (CNF) formulas on attributes in anonymous authentication systems.

Firstly, she proposed the method of the constant-size proof for CNF formulas and the efficient proof generation method by using the extended accumulator and the zero-knowledge proof for anonymous authentication systems. She implemented the proposals and showed their experimental results.

Secondly, she proposed an extension of this method to reduce the long public key by dividing a CNF formula into multiple ones.

Thirdly, she proposed the efficiency improvement of the computational overhead based on online/offline pre-computation technique, which can reduce the online computational costs of the proof generation in case of lots of AND relations in the proved CNF formulas.

From the overall evaluation of this thesis, the applicant has satisfied the qualification condition for the doctor degree in Engineering from the Graduate School of Natural Science and Technology at Okayama University.