氏名	AMANG SUDARSONO
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4260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	A Study of Pairing-Based Anonymous Authentication Systems and Their Applications （ペアリングを用いた匿名認証システムとその応用に関する研究）
論文審査委員	教授　船曳　信生　　教授　杉山　裕二　　准教授　中西　透

学位論文内容の要旨

In this thesis, firstly, we propose a pairing-based anonymous IEEE802.1X authentication system using a pairing-based group signature scheme for wireless local area networks. Secondly, we propose a pairing-based group signature scheme with an efficient revocation check. Thirdly, we propose a pairing-based anonymous attribute authentication system suitable for electronic identification.

In the Chapter 2, we start this thesis by giving an overview on the mathematics 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 proofs of knowledge on representations used in this thesis are illustrated.

Chapter 3 explains the construction of a pairing-based anonymous IEEE802.1X authentication system. The model of the VLR group signature scheme and the modified VLR group signature scheme for the anonymous authentication are exposed. This chapter also illustrates the proposed system and the implementation of anonymous IEEE802.1X authentication for wireless networks.

Chapter 4 gives the construction of a pairing-based VLR group signature scheme with efficient revocation check. This chapter covers the algorithm to achieve an efficient revocation check and shows the measurement results of the signing time and the verification time.

Chapter 5 describes the construction of the anonymous authentication system with efficient proofs of attributes using a pairing-based accumulator. In particular, this chapter shows the construction system in the application to an electronic identity card (eID).

Finally, Chapter 6 concludes this thesis together with some future works.

論文審査結果の要旨

The applicant proposed two anonymous authentication systems with their applications, and an improved scheme for the verifier-local revocation (VLR) group signature.

Firstly, he proposed a pairing-based anonymous IEEE802.1X authentication system for wireless local area networks. He defined the model of the VLR group signature scheme, and modified VLR group signature scheme for the anonymous authentication system. Then, he designed the protocol of this system, and applied it for the wireless network authentication system. Finally, he showed the practicality of the system with up to 1,000 revoked users.

Secondly, he improved the VLR group signature scheme with the revocation check by reducing the computation cost at the authentication server to verify the user. This improvement is derived from the observation that the product of pairings can be computed faster than the separated pairings by using a technique called multi-pairing. He implemented this improved scheme, and showed that the scheme reduced the verification time by 10% from the original VLR scheme.

Thirdly, he constructed a pairing-based anonymous attribute authentication system suitable for the electronic identification. This system provided efficient proofs of attributes using a pairing-based accumulator. He implemented the proposed system for the electronic identity (eID) application, and showed the practicality of the system with the total processing time within a second.

From the overall evaluation of the 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.