論文 / 著書情報
Article / Book Information

題目(和文)	グループ署名に関する種々の研究
Title(English)	Studies on Group Signature
著者(和文)	石田愛
Author(English)	Ai Ishida
出典(和文)	学位:博士(理学), 学位授与機関:東京工業大学, 報告番号:甲第10755号, 授与年月日:2018年3月26日, 学位の種別:課程博士, 審査員:田中 圭介,渡辺 治,鹿島 亮,伊東 利哉,尾形 わかは
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第10755号, Conferred date:2018/3/26, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	論文要旨
Type(English)	Summary

（博士課程）
Doctoral Program

論 文 要 旨

THESIS SUMMARY

専攻： Department of	数理・計算科学　専攻	申請学位（専攻分野）： Academic Degree Requested	博士　（　理学　） Doctor of
学生氏名： Student's Name	石田　愛	指導教員（主）： Academic Supervisor(main)	田中　圭介
		指導教員（副）： Academic Supervisor(sub)	

要旨（英文 800 語程度）
Thesis Summary（approx.800 English Words ）

This thesis has four contributions in the field of group signature. We outline each contribution in the following.

Firstly, we discuss about the minimum assumptions for the existence of group signature. Specifically, we point out that these minimal assumptions are depends on whether the target group signature is fully anonymous or selfless anonymous. The previous works showed that a public key encryption (PKE) scheme can be constructed from a group signature scheme that satisfies full anonymity. Therefore, it is unlikely to construct a fully anonymous group signature scheme only from a one-way function (OWF). This is because, if a fully anonymous group signature scheme can be constructed from a OWF, this fact contradicts to the impossibility result by Impagliazzo and Rudich. On the other hand, there still remains a possibility that a group signature scheme which satisfies selfless anonymity can be constructed without a PKE scheme since a conversion from a selfless anonymous group signature scheme to a PKE scheme is not known. In this thesis, we give a construction of a selfless anonymous group signature scheme without any PKE scheme. Concretely, we construct a selfless anonymous group signature scheme from a symmetric key encryption scheme, a commitment scheme, a digital signature scheme, and a non-interactive zero-knowledge (NIZK) proof system. This result indicates that a selfless anonymous group signature scheme can be constructed from a OWF and a NIZK proof system. Moreover, from the result, we discuss the gap between fully anonymous group signature and selfless anonymous group signature from the practical and theoretical aspects.

Secondly, we propose the first VLR-GS scheme that satisfies full anonymity, which is considered to be the de-facto standard security notion. As mentioned, VLR-GS is a special type of revocable group signature which enables a user to sign massages without referring information regarding revoked users. After the first scheme was given by Boneh and Shacham in 2004, there have been several proposals of VLR-GS schemes. However, all of these schemes only achieve a weak security notion, selfless anonymity. This security notion is strictly weaker than the de-facto standard security notion, full anonymity. Therefore, for more than a decade, it has been an open problem whether a fully anonymous

VLR-GS scheme can be achieved since it is known that there is a big theoretical gap between selfless anonymous group signature and fully anonymous group signature. In this thesis, we give an affirmative answer to this problem. Concretely, we show a construction of a fully anonymous VLR-GS scheme from a digital signature scheme, a PKE scheme, and a non-interactive zero-knowledge proof system. Although the building blocks are essentially the same as those of a standard group signature scheme, we additionally require the underlying PKE scheme to satisfy key privacy which is essential to ensure that the VLR-GS scheme is fully anonymous. Moreover, we give VLR-GS schemes with backward unlinkability, which ensures that even after a user is revoked, signatures produced by the user before the revocation remain anonymous.

Thirdly, we propose new functionality of group signature, deniability. This functionality allows the opener to generate a proof showing that the specified user is not the signer without revealing the actual signer.

By using a group signature scheme, a user can sign a message on behalf of a specific group without revealing his identity, but in the case of a dispute, the opener can expose the identity of the signer. Although such functionality seems to be quite useful for protecting users' anonymity and tracing a malicious user simultaneously, this is insufficient for some situations in which a user wants to only show that he is not the signer of a signature. In this thesis, we introduce the notion of deniable group signature, which allows an authority to prove that the specified user is not the signer. More precisely, in addition to all the functionalities of standard group signature, deniable group signature provides another functionality that the opener can generate a denial proof that proves non-ownership of a signature for a user. Moreover, we propose a method for designing a deniable group signature scheme and a concrete instantiation.

Finally, we give a cryptanalysis of the scheme denoted as Mechanism 6 in the ISO/IEC 20008-2 standard. Mechanism 6 is the only standardized group signature scheme that does not aim at pro- viding additional functionalities. In this thesis, we firstly break the anonymity of Mechanism 6 in the standard security model, i.e., the Bellare-Shi-Zhang model. We then discuss possible countermeasures against our attack. Consequently, we provide a detailed analysis of the security properties offered by Mechanism 6 and characterize the conditions under which its anonymity is preserved. From this analysis, we also derive a simple patch for Mechanism 6.