Form 2

Dissertation Abstract

Report no.	(Course-based) No. 1099	Name	MAHARAGE NISANSALA SEVWANDI PERERA
Dissertation title	Dynamic Group Signatures using Verifier-local Revocation (検証者の局所的な登録無効化を用いた動的グループ署名)		

Abstract

※ The abstract should be in keeping with the structure of the dissertation (objective, statement of problem, investigation, conclusion) and should convey the substance of the dissertation.

Group signatures allow members to sign on behalf of the group while hiding their identity. In other hand, it allows the group manager to open the signatures and identify the signer of the signatures. An efficient Member revocation is an important feature in group signatures schemes when applying in the real world.

This thesis discusses the member revocation approaches and use Verifier-local revocation (VLR) as the member revocation method. VLR is the most simple and efficient revocation technique up to now since it requires only to update the verifiers who are in less in number when a member is revoked. VLR schemes use a token system. Thus, when a member is revoked his token is passed to the verifiers. However, the existing VLR group signature schemes rely on a weaker security notion called selfless-anonymity. Thus, this thesis consider how to achieve strong security while providing full dynamicity to the group signature schemes with VLR. Moreover, most of the existing fully dynamic groups are constructed based on number theoretical assumption which will be in danger when the quantum computers become a reality. Lattice-based cryptography is a solution for this problem.

Strong security can be achieved in two different ways for VLR schemes. One is with restricted version of full anonymity and another is involvement of group manager.

As a result first we suggest a new security notion and a revocation token generation method that separately create tokens without depending on the secret signing keys. Moreover, we provide a lattice-based group signature schemes with VLR using the proposed revocation token generation technique and the new security notion.

Next we consider the difficulties of achieving strong security for full dynamic group signature schemes with member registration and member revocation with VLR. As a solution for those problems, we propose another new security notion and we present two types of schemes that satisfies both member registration and member revocation with VLR.

Using the second method we present a new VLR scheme that achieves the full anonymity with the group manager's signature for member revocation messages.

In addition, finally, we discuss and present a technique to improve the efficiency of VLR group signature schemes.

Accordingly, we present seven VLR group signature schemes in our thesis.