SCIS 2009 The 2009 Symposium on Cryptography and Information Security
Otsu, Japan, Jan. 20-23, 2009
The Institute of Electronics, Information and Communication Engineers

A Group Signature Scheme with Efficient Verifier-Local Revocation Check

Toru Nakanishi* Amang Sudarsono* Yumi Sakemi* Yasuyuki Nogami*
Nobuo Funabiki*

Abstract— To achieve a user revocation in group signature schemes suitable for mobile signers, verifier-local revocations have been previously proposed. However, the revocation checks in the verification are inefficient, since these need R separated pairings, where R is the number of revoked members. This paper uses the observation that the product of the pairings can be computed faster than the separated pairings to propose a group signature scheme with more efficient revocation checks.

Keywords: privacy enhancement, group signatures, user revocations, pairings

1 Introduction

A *group signature scheme* [2, 3, 6, 7] allows a group member to anonymously sign a message on behalf of a group, where a group manager (GM) controls the membership of every member. An important topic in the group signatures is the user revocation [2, 3, 6, 7].

Compared to other types of revocations, the verifier-local revocation (VLR) [3, 6, 7] is a suitable revocation mechanism for mobile situations, since the signer of the mobile terminal is not involved to the revocation mechanism (i.e, the signer does not need to fetch the revocation list and the cost of signing is independent of the number of revoked members). The efficient VLR scheme from pairings is obtained in [3]. In [6], the important property "backward unlinkability" is added to the pairing-based scheme. The property means that that even after a member is revoked, signatures produced by the member before the revocation remain anonymous. In [7], using a different assumption called DLIN (Decision Linear) assumption, the scheme with shorter signatures is obtained.

The previous VLR schemes have a disadvantage that the computation of the verification depends on R, where R is the number of revoked members. This means that, as R grows (i.e., for large or dynamic member groups), the verification requires lots of processing time. This heavy computational cost is derived from a pairing-based revocation check. In the revocation check, the verifier checks a pairing-based relation between a check data included in the signature and a revocation token for every revoked member (these token are issued from GM). The dominant costs are R pairing computations.

This paper proposes a VLR scheme with more efficient revocation checks. The better efficiency is obtained from the observation that a product of pairings can be computed faster than separated pairings. Some techniques to compute it faster (we call them multi-pairing techniques) are described in [5]. In our scheme, at the sacrifice of the $O(L)$ slight overhead cost in signing, the revocation checks for L revoked members are executed by the product of 2 $(L+1)$ pairings. As shown later, since we can utilize a fast pairing library [1] where the product of $2(L+1)$ pairings is computed faster than L pairings for $L \geq 4$ with the multi-pairing techniques, we can expect more efficient revocation checks.

* Dept. of Communication Network Engineering, Okayama University

2 Model and Security Definitions

The VLR group signature scheme consists of the following algorithms:

Setup: This probabilistic initial setup algorithm, on inputs ℓ that is an efficiency parameter (see Section 4) and T that is the total number of time intervals, outputs public parameters $param$.

KeyGen: This probabilistic key generation algorithm for GM, on input $param$, outputs the group public key gpk and GM's secret key msk.

Join: This is an interactive protocol between a probabilistic algorithm **Join-U** for the i-th user and a probabilistic algorithm **Join-GM** for GM, where the user joins the group controlled by GM w.r.t. gpk. **Join-U**, on input gpk, outputs $\boldsymbol{usk}[i]$ that is the user's secret key. On the other hand, **Join-GM**, on inputs gpk, msk, outputs $\boldsymbol{reg}[i]$.

Revoke: This probabilistic algorithm, on inputs gpk, a time interval t, $\boldsymbol{reg}[i]$ and RU that is a set of revoked members' IDs, outputs revocation list $\boldsymbol{RL}[t]$.

Sign: This probabilistic algorithm, on inputs gpk, $\boldsymbol{usk}[i]$, t, and signed message M, outputs the signature σ.