Event-Oriented k-Times Revocable-iff-Linked Group Signatures

Man Ho Au[1], Willy Susilo[1], and Siu-Ming Yiu[2]

[1] Center for Information Security Research
School of Information Technology and Computer Science
University of Wollongong, Wollongong 2522, Australia
{mhaa456, wsusilo}@uow.edu.au
[2] Department of Computer Science
The University of Hong Kong
Pokfulam, Hong Kong
smyiu@cs.hku.hk

Abstract. In this paper, we introduce the notion of event-oriented k-times revocable if and only if linked group signatures (k-EoRiffL group signatures). In k-EoRiffL group signatures, signers can sign on behalf of a group anonymously and unlinkably up to a permitted number of times (k) per *event*. No party, even the group manager, can revoke the anonymity of the signer. On the other hand, everyone can identify the signer if he signs more than k times for a particular *event*. We then show that k-EoRiffL group signatures can be used for k-times anonymous authentication(k-TAA), compact e-cash, e-voting, etc.

We formally define security model for the new notion and propose constant-size construction, that is, size of our construction is *independent* of the size of the group and the number of permitted usage k. Our construction is secure based on the q-strong Diffie-Hellman assumption and the y-DDHI assumption.

Keywords: event-oriented, revocable anonymity, group signature, k-TAA.

1 Introduction

In the age of information technology, number of applications over the Internet continues to grow. These include messaging, voting, payments, commerce, etc. At the same time, people are concerned with their personal privacy and are aware of the protection of privacy.

Anonymity is an important form of privacy protection. This is especially true in case of group-oriented cryptography, where a group of users are involved. In schemes where participation of one or a proper subset of members is required to complete a process, anonymity refers to whether participants are distinguishable from non-participants. Users may prefer perfect anonymity, meaning that it is not possible to distinguish participants from non-participants so as to maintains their privacy in participating the process. In [3], anonymity can be divided

L. Batten and R. Safavi-Naini (Eds.): ACISP 2006, LNCS 4058, pp. 223–234, 2006.

into 4 different levels, namely, *No Anonymity*, *Revocable Anonymity*, *Linkable Anonymity* and *Full Anonymity* accordingly. Extending their ideas, we further refine levels of anonymity for group-oriented cryptography as follow, from highest level to lowest level (no anonymity).

1.1 Levels of Anonymity for Group–Oriented Cryptography

Full Anonymity. It means that identity of the participating user is indistinguishable from the non-participating users by *any* party. A prominent example is ring signature, formalized in [19]. Many ring signatures are then proposed subsequently and the constant-size construction (meaning the size of the signature is independent of the size of the group) first appeared in [10], followed by [16].

Linkable Anonymity. Users can participate in the process anonymously but their participation are linked, that is, everybody can tell if the underlying participant in two separate processes are the same. An example is linkable ring signature[13, 25, 24], where everybody can tell if two signatures are generated from the same signer. However, no one can tell who the actual signer is. A generalized notion is k-times linkable anonymity, meaning that suppose the user participate for k times or less, he enjoys full anonymity while if he participate for more than k times, at least two of his participations are linked.

Revocable-iff-linked Anonymity. Similar to linkable anonymity, users enjoy full anonymity if they only participate once. However, if they participate twice, everybody can reveal their identity. Some e-cash scheme [7, 2], tracing-by-linking (TbL) group signature scheme[26] are examples of this type. In [7, 2], no one (even the bank) could revoke the anonymity of the spender of the e-cash while in case someone spends twice, his identity is revealed. A more general notion is k-times Revocable-iff-Linked anonymity, in which user identity is revealed if he participate for more than k times. Examples include compact e-cash scheme[8], k-times anonymous identification (k-TAA)[21, 17].

Revocable Anonymity. Basically it means anonymity to everybody except an *Open Authority(OA)*. From user's standpoint, it can be regarded as a lower anonymity level than Revocable-iff-Linked anonymity since in the user must trust the OA not to abuse his power in comparison with Revocable-iff-Linked anonymity where users are anonymous unless they break the condition themselves. Group signature[1] is a famous example.

Linkable and Revocable Anonymity. As its name suggest, users enjoy linkable anonymity towards everybody except OA, where OA can always revoke the anonymity of the user. Systems where users are identified by pseudonym[12] with an authority knowing the corresponding identity of the user for each pseudonym belongs to this category. Many e-cash schemes[9, 23] in fact belongs to this category too. Should a user double-spends, everybody can detect it and the OA can then reveal the identity of the cheater.

Revocable-iff-Linked and Revocable Anonymity. Similarly, users enjoy revocable-iff-linked anonymity to everybody except OA. In fact, Linkable (resp.