Constant-Size ID-Based Linkable and Revocable-iff-Linked Ring Signature

Man Ho Au[1], Joseph K. Liu[2], Willy Susilo[1], and Tsz Hon Yuen[3]

[1] Centre 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
University of Bristol
Bristol, BS8 1UB, UK
liu@cs.bris.ac.uk
[3] Department of Information Engineering
The Chinese University of Hong Kong
Shatin, N.T., Hong Kong
thyuen4@ie.cuhk.edu.hk

Abstract. In this paper, we propose a new notion called *Revocable-iff-Linked Ring Signature* (R-iff-L Ring Signature). In R-iff-L ring signatures, a signer can sign on behalf of the whole group, just like ordinary ring signatures. However, if he signs twice or more, he can be linked and his identity can be revoked by everyone. We formally define a new security model for the new notion in identity-based (ID-based) setting and propose a constant-size ID-based construction, that is, the size of the signature is *independent* of the size of the group. In addition, we enhance the security model of ID-based linkable ring signature scheme and provide an implementation with constant size setting. Both schemes are provably secure in our new model.

Keywords: Anonymity, Linkable, Revocable, Ring Signature.

1 Introduction

Group-oriented cryptography refers to cryptographic systems in which 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. According to [2], anonymity for group-oriented cryptography can be divided into 7 different levels, namely, *Full Anonymity*, *Linkable Anonymity*, *Revocable-iff-Linked Anonymity*, *Revocable Anonymity*, *Linkable and Revocable Anonymity*, *Revocable-iff-Linked and Revocable Anonymity* and *No Anonymity*. Examples of group-oriented cryptographic schemes with different levels of anonymity are shown in the following table while interested readers can refer to [2] for a more detailed discussion.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 364–378, 2006.

Anonymity Level	Examples	Size	Event-Oriented	Ad-hoc
Full	Ring Sign[18]	O(n)	N/A	✓
	Anon Ident[11,16]	O(1)	N/A	✓
Linkable	Linkable Ring[13]	O(n)	×	✓
	Eo-Linkable Ring[24]	O(n)	✓	✓
Revocable-iff-Linked				
2-times	E-Cash[6,1],TbL[25]	O(1)	×	×
	this paper	O(1)	✓	✓
k-times	Compact E-Cash[7]	O(1)	×	×
	k-TAA[20]	O(k)	✓	×
	dynamic k-TAA[17]	O(k)	✓	✓
	constant-size K-TAA[21]	O(1)	✓	×
	k-Times Group Signature [2]	O(1)	✓	×
Full+OA	Group Signatures	O(1)	×	×
Link+OA	Fair E-Cash[8,22]	O(1)	×	×

Fig. 1. Examples of group-oriented cryptographic schemes with different levels of anonymity

Ring Signature. Ring signature allows a user to sign on behalf of the whole group, yet no one knows who the actual signer is. The idea was first proposed in by Cramer et al [10] and the notion was formalized by Rivest et al [18]. Variants include threshold setting [26,12,15] and enhanced security [4,9] have been proposed later.

Identity-based Cryptography. In 1984, Shamir [19] introduced the notion of Identity-based (ID-based) cryptography to simplify certificate management. The unique feature of ID-based cryptography is that a user's public key can be any arbitrary string. Since then, many other ID-based signature schemes have been proposed.

In the case of ID-based ring signature, we have to take extra care for the design of schemes. While some of the existing schemes provide anonymity *unconditionally*, others are computational only. The Private Key Generator (PKG) itself may have extra advantage in breaking the anonymity since it is in possession of all the private keys. This problem does not sound serious in normal ID-based ring signature scheme because almost all existing schemes is unconditionally anonymous. However, in the case of linkable ring signatures [13,24,14,23,3] where the verifier is able to determine whether two signatures are signed by the same signer, it is still an open problem to construct one with unconditional anonymity. Within the constraint of computational anonymity, it is a great challenge of providing privacy in an ID-based setting (to the PKG). We require special attention in the design of the scheme.

Contribution. In this paper, we propose a new notion called *Revocable-iff-Linked Ring Signature* which belongs to the Revocable-iff-Linked Anonymity category. In addition, we have the following contributions: