A Separable Threshold Ring Signature Scheme

Joseph K. Liu[1], Victor K. Wei[1], and Duncan S. Wong[2⋆]

[1] Department of Information Engineering
The Chinese University of Hong Kong
Shatin, Hong Kong
{ksliu9,kwwei}@ie.cuhk.edu.hk
[2] Department of Computer Science
City University of Hong Kong
Kowloon, Hong Kong
duncan@cityu.edu.hk

Abstract. We present a threshold ring signature scheme (spontaneous anonymous threshold signature scheme) that allows the use of both RSA-based and DL-based public keys at the same time. More generally, the scheme supports the mixture of public keys for any trapdoor-one-way type as well as three-move type signature schemes. This kind of 'separability' has useful applications in practice as a threshold ring signature is no longer limited to support only one particular type of public keys, as required by all the previous schemes. In the paper, we also show that the signature maintains the anonymity of participating signers unconditionally and is existential unforgeable against chosen message attacks in the random oracle model.

1 Introduction

Let us consider the following scenario. Suppose there are n users in a public-key system in which each of them has a public key pair for digital signature. Their public keys are generated independently without any coordination with others and therefore their keys may correspond to different security parameters. In addition, it is very likely that the keys are for entirely different signature schemes. For example, user 1 may have a key pair for 2048-bit RSA signature scheme [17], user 2 may have one for 1024-bit Digital Signature Algorithm [12], user 3 may have one for 163-bit ECDSA (Elliptic Curve Digital Signature Algorithm) [9], while user 4 may prefer to use one for 1024-bit Schnorr signature scheme [18]. Other users may pick key pairs for their favorable signature schemes other than the previous ones. Under this system setup, t users spontaneously form a group of n possible signers by arbitrarily choose n users including themselves, where $n > t$, and generate a signature for some message such that (1) any public verifier (who has all the n public keys) can tell if the signature is valid (*public verifiability*); (2) can identify who the t actual signers are even when all the

⋆ A part of this work was supported by a grant from CityU(Project No. 7200005).

J.I. Lim and D.H. Lee (Eds.): ICISC 2003, LNCS 2971, pp. 12–26, 2004.

private keys of the n possible signers in the group are known (*anonymity, signer-ambiguity*); and (3) knowing only $t-1$ private keys of the signing group is not enough for forging such a signature (*unforgeability, robustness*). In this paper, we focus on solving the problem and we call the scheme a *separable threshold ring signature scheme* or *spontaneous anonymous threshold signature scheme*.

The notion of ring signature was first formalized by Rivest et al. in [16]. A ring signature scheme allows a signer to *spontaneously* form a group of signers including himself and generate a signature such that any public verifier can tell if the signature is valid while cannot determine the actual authorship of the signature. In addition, the formation of a signing group does not require any coordination of group membership or any TTP (Trusted Third Party), and therefore can be formed by the actual signer without getting any consent from other diversion group members — *spontaneity*. The concept of spontaneity was absent from most previous results on threshold cryptography and threshold signature schemes [7]. The signing group is formed with the intervention of the group manager and may also require coordination among group members. Also the group manager who always knows who the the actual signer is. In the ring signature, the absence of a group manager provides anonymity to the actual signer both inside and outside the signing group.

A (t, n)-threshold ring signature [3] has the similar notion to the ring signature. First, a (t, n)-threshold ring signature scheme requires at least t signers to work jointly for generating a signature. Second, the anonymity of signers is preserved both inside and outside the signing group. Third, those t participating signers can choose any set of n entities including themselves without getting any consent from those diversion group members.

(Separability) An application is said to be separable if all participants can choose their keys independently with different parameter domains and for different types of signature schemes. The term separability was originated from [10] and was diversified in [5]. There exists weaker forms of separability. Partial separability allows only a subset of the participants to choose their keys independently and weak separability requires all participants to use common system parameters. [**?**] provides perfect separability, [10] provides partial separability and [5] provides weak separability. However, all of these schemes are group signature schemes and there is no corresponding variant of threshold ring signature schemes.

There is another scenario: when all participants in an application choose their keys independently but requiring that all the keys are for one single type of signature schemes. For example, all keys have to be for a RSA-based signature scheme but they may have different key sizes. We say that the application has *type-restricted* separability.

1.1 Our Contributions

We present a (t, n)-threshold ring signature scheme (spontaneous threshold signature scheme) that enjoys separability. In each signature, the public keys indicated can be for any trapdoor-one-way type and any three-move type signature