Short Linkable Ring Signatures for E-Voting, E-Cash and Attestation

Patrick P. Tsang and Victor K. Wei

Department of Information Engineering,
The Chinese University of Hong Kong,
Shatin, Hong Kong
{pktsang3, kwwei}@ie.cuhk.edu.hk

Abstract. A ring signature scheme can be viewed as a group signature scheme with no anonymity revocation and with simple group setup. A *linkable* ring signature (LRS) scheme additionally allows anyone to determine if two ring signatures have been signed by the same group member. Recently, Dodis et al. [18] gave a short (constant-sized) ring signature scheme. We extend it to the first short LRS scheme, and reduce its security to a new hardness assumption, the Link Decisional RSA (LD-RSA) Assumption. We also extend [18]'s other schemes to a generic LRS scheme and a generic linkable group signature scheme. We discuss three applications of our schemes. Kiayias and Yung [22] constructed the first e-voting scheme which simultaneously achieves efficient tallying, public verifiability, and write-in capability for a typical voter distribution under which only a small portion writes in. We construct an e-voting scheme based on our short LRS scheme which achieves the same even for all worst-case voter distribution. Direct Anonymous Attestation (DAA) [6] is essentially a ring signature scheme with certain linking properties that can be naturally implemented using LRS schemes. The construction of an offline anonymous e-cash scheme using LRS schemes is also discussed.

1 Introduction

A *group signature* scheme [15] allows a member to sign messages anonymously on behalf of his group. The group manager is responsible to form the group and assign to the members the ability to sign. However, in the case of a dispute, the identity of a signature's originator can be revealed (only) by a designated entity.

A *ring signature* scheme [29] can be viewed as a group signature scheme with no anonymity revocation and with simple group setup. Formation of a group is *spontaneous*: diversion group members can be totally unaware of being conscripted to the group. Applications include leaking secrets [29] and anonymous identification/authentication for ad hoc groups [5, 18].

Linkable ring signatures [23] are ring signatures, but with added linkability: such signatures allow anyone to determine if they are signed by the same group member (i.e. they are *linked*). If a user signs only once on behalf of a group, he still enjoys anonymity similar to that in conventional ring signature schemes. If

Robert H. Deng et al. (Eds.): ISPEC 2005, LNCS 3439, pp. 48–60, 2005.
© Springer-Verlag Berlin Heidelberg 2005

the user signs multiple times, anyone can tell that these signatures have been generated by the same group member. Applications include leaking sequences of secrets and e-voting [23]. Concepts similar to linkability also appeared in one-show credentials [7], linkable group signatures [26, 27], and DAA [6].

Early constructions of (linkable) ring/group signature schemes have large signature sizes, which are usually $O(n)$ where n is the group size. Subsequent results incorporating various techniques reduced the sizes of state-of-the-art group signatures to a constant independent of group size. Consult [11, 1, 8, 3, 9, 28] for details. Essentially all ring signatures have sizes $O(n)$. Recently, Dodis, et al. [18] gave a short ring signature scheme construction. In this paper, we extend their technique to construct a short LRS scheme. We also extend [18]'s generic ring (resp. group) signature scheme constructions to their linkable version.

Tracing-by-linking versus tracing-by-escrowing in group signatures. The following two papers came to our attention after the completion of this research: Teranishi, et al. [30] and Wei [34]. They achieve *tracing-by-linking*, i.e. tracing the double signer's public key without identity escrowing to an Open Authority (OA). In comparison, traditional group signatures use the *tracing-by-escrowing* technique, and give the Open Authority the unnecessary power to open an honest signer's identity even when there is no dispute to investigate. Comparing the two tracing-by-linking group signatures: [30]'s has smaller size. [34]'s has larger, but still $O(1)$, size, but it is more flexible and supports features such as tracing the double signer's secret key, tracing the double signer's identity without going through the public key, etc. Another paper containing tracing-by-linking ring signature is due to Tsang, et al. [33].

Constant-sized LRS schemes have many applications. We describe three of them briefly in the following.

E-Voting. There are three basic paradigms for cryptographically secure ballot elections. Under the *blind signature* [13] paradigm, the voters obtain ballots from the authorities, certified but privacy-preserved. This enables them to embed any form of ballot (including write-ins). This approach requires the employment of an anonymous channel between the voter and the tallying authorities to hide the identity of the user at the "ballot casting stage." Note that universal verifiability is missing and robustness is usually achieved by thresholding the authority.

Under the *homomorphic encryption* [16] paradigm, the ballots are encrypted and then "compressed" via a homomorphic encryption scheme into a tally. This compression property allows fast tallying, and is what makes this approach attractive. However the drawback is that pure "compressible" homomorphic encryption is not suitable to deal with write-in ballots.

Under the *mix-net* [12] paradigm, the tallying officials move the ballots between them and permute them in the process while changing their representation (e.g., partially decrypting them). Practical implementations of this approach in its fully robust form is still considered a slow tallying process.

Offline Anonymous Electronic Cash (E-cash). Most of the e-cash systems found in the literature makes use of *blind signatures*. In such systems, the users withdraw electronic coins, which consist of numbers generated by users and