Tracing-by-Linking Group Signatures

Victor K. Wei

Dept. of Information Engrg., Chinese Univ. of Hong Kong, Hong Kong
kwwei@ie.cuhk.edu.hk

Abstract. In a group signature [19], any group member can sign on behalf of the group while remaining anonymous, but its identity can be traced in an future dispute investigation. Essentially all state-of-the-art group signatures implement the tracing mechnism by requiring the signer to escrow its identity to an Open Authority (OA) [2, 13, 4, 25, 5, 7, 24]. We call them *Tracing-by-Escrowing (TbE)* group signatures. One drawback is that the OA also has the unnecessary power to trace without proper cause. In this paper we introduce *Tracing-by-Linking (TbL)* group signatures. The signer's anonymity is irrevocable by any authority if the group member signs only once (per event). But if a member signs twice, its identity can be traced by a public algorithm without needing any trapdoor. We initiate the formal study of TbL group signatures by introducing its security model, constructing the first examples, and give several applications. Our core construction technique is the successful transplant of the TbL technique from single-term offline e-cash from the blind signature framework [9, 22, 21] to the group signature framework. Our signatures have size $O(1)$.

1 Introduction

In a group signature [19], any group member can sign on behalf of the group while remaining anonymous. However, to investigate a dispute, the signer's identity can be *traced*. Essentially all contemporary state-of-the-art group signatures implement the tracing mechanism by requiring the signer to escrow its identity to an Open Authority (OA) [2, 13, 4, 25, 5, 7]. We call them *Tracing-by-Escrowing (TbE)* group signatures. One drawback is that the OA's trapdoor has the unnecessary power to trace any signature without proper cause. For example, a change in government or administration can mandate the OA to trace some past signatures controversially.

In this paper, we initiate the formal study of *Tracing-by-Linking (TbL) group signatures*. In a TbL group signature, the signer's anonymity cannot be revoked by any combination of authorities. However, if a group member signs twice (per event), then its identity can be traced by any member of the public without needing any trapdoor.

Our main **contributions** are

- We initiate the formal study of tracing-by-linking (TbL) group signatures. We introduce its security model, and construct the first several TbL group

J. Zhou et al. (Eds.): ISC 2005, LNCS 3650, pp. 149–163, 2005.

signatures, and reduce their securities to standard intractability assumptions.
- We extending our constructions from *sign twice and anonymity revoked* to *sign k times and anonymity revoked*.
- We apply TbL group signatures to several applications, including Direct Anonymous Attestation (DAA), anonymous credentials, offline anonymous e-cash, and e-voting.

The paper is **organized** as follows: Section 2 contains the security model. Section 3 contains preliminaries. Section 4 contains constructions and security theorems. Section 5 contains discussions and applications.

Related Results: Essentially all state-of-the-art group signatures are TbE group signatures. The signer anonymity can be revoked by the OA's trapdoor even without cause. Partial key escrows and time-delayed key escrows [35, 30, 3] have been introduced to counteract abuses by the over-powered. The TbL group signature's anonymity is irrevocable by any combination of managers and authorities. There is no OA. In a ring signature [20, 34, 1] the signer anonymity is also irrevocable. But signing any number of times does not result in anonymity revocation. In a linkable group (resp ring) signature scheme [32, 33, 14, 23, 11], signatures from the same signer can be linked, but its anonymity remains. These *link-but-not-trace* group (resp. ring) signatures typically *tag* the double signer in a way such that future signatures from the same signer can be linked more conveniently.

Our intuitions: The core of our construction technique is the successful transplant of the TbL technique from single-term offline e-cash scheme from the blind signature framework [8, 9, 10, 21, 22] to the group signature framework. Our TbL group signature has size $O(1)$. The essence of our TbL technique is to commit some randomness during group membership certification and then require the signer to use these randomness during a 3-move non-interactive zero-knowledge proof. Double spending implies answering challenges twice with the same *certified commitments* and it results in the extraction of the double signer's secret identity.

2 Security Model

We present a security model for the tracing-by-linking (TbL) group signature. In a nutshell, we replace the triplet of security notions, *anonymity*, *full traceability* and *non-frameability*, of TbE group signatures [4, 5] by a new triplet for TbL group signatures: *irrevocable anonymity*, *full linkability* and *non-slanderability*. Motivated by the DAA (Direct Anonymous Attestation) [11] application, our system consists of three types of entities in multitudes:

- Managers of Groups, or, equivalently, Certificate Authorities (CA's), with serial number cnt which stands for *counter value*.
- Users, or, equivalently, TPM (Trusted Platform Module), whose serial number is id.
- Verifiers with serial number bsn which stands for *basename*.