Foundations of Group Signatures: The Case of Dynamic Groups

Mihir Bellare, Haixia Shi, and Chong Zhang

Dept. of Computer Science & Engineering, University of California, San Diego,
9500 Gilman Drive, La Jolla, CA 92093, USA
{mihir,hashi,c2zhang}@cs.ucsd.edu
http://www-cse.ucsd.edu/users/{mihir,hashi,c2zhang}

Abstract. Recently, a first step toward establishing foundations for group signatures was taken [5], with a treatment of the case where the group is static. However the bulk of existing practical schemes and applications are for dynamic groups, and these involve important new elements and security issues. This paper treats this case, providing foundations for dynamic group signatures, in the form of a model, strong formal definitions of security, and a construction proven secure under general assumptions. We believe this is an important and useful step because it helps bridge the gap between [5] and the previous practical work, and delivers a basis on which existing practical schemes may in future be evaluated or proven secure.

1 Introduction

The purpose of foundational work is to provide strong, formal definitions of security for cryptographic primitives, thereby enabling one to unambiguously assess and prove the security of constructs and their use in applications, and then prove the existence of schemes meeting the given definitions. As evidenced by the development of the foundations of encryption [20, 24, 19, 25, 27, 17], however, this program can require several steps and considerable effort.

This paper takes the next step in the foundational effort in group signatures begun by [5]. Below we provide some background and then discuss our contributions.

1.1 Background and Motivation

Group signatures. The setting, introduced by Chaum and Van Heyst [15], is of a group of entities, each having its own private signing key, using which it can produce signatures on behalf of the group, meaning verifiable under a single public verification key associated to the group as a whole. The basic security requirements are that the identity of the group member producing a particular signature not be discernible from this signature (anonymity), except to an authority possessing a special "opening" key (traceability).

A.J. Menezes (Ed.): CT-RSA 2005, LNCS 3376, pp. 136–153, 2005.

With time, more security requirements were added, including unlinkability, unforgeability, collusion resistance [4], exculpability [4], and framing resistance [16]. Many practical schemes were presented, some with claims of proven security in the random oracle model [1]. However, it is often unclear what the schemes or claimed proofs in these works actually deliver in terms of security guarantees, due largely to the fact that the requirements are informal and sometimes ambiguous, not precisely specifying adversary capabilities and goals. It would be beneficial in this context to have proper foundations, meaning strong formal definitions and rigorously proven-secure schemes.

Foundations for static groups. The first step toward this end was taken by [5], who consider the case where the group is *static*. In their setting, the number of group members and their identities are fixed and frozen in the setup phase, where a trusted entity chooses not only the group public key and an opening key for the opening authority, but also, for each group member, chooses a signing key and hands it to the member in question. Within this framework, they formalize two (strong) security requirements that they call full-anonymity and full-traceability, and show that these imply all the informal existing requirements in the previous literature. They then present a static group signature scheme shown to meet these requirements, assuming the existence of trapdoor permutations.

Dynamic groups. However, static groups limit applications of group signatures, since they do not allow one to add members to the group with time. They also require an uncomfortably high degree of trust in the party performing setup, since the latter knows the signing keys of all members and can thus frame any group member. These limitations were in fact recognized early in the development of the area, and the practical literature has from the start focused on the case where the group is *dynamic*. In this setting, neither the number nor the identities of group members are fixed or known in the setup phase, which now consists of the trusted entity choosing only a group public key and a key for the authority. An entity can join the group, and obtain a private signing key at any time, by engaging in an appropriate join protocol with the authority.

Closing the gap. We thus have the following gap: foundations have been provided for the static case [5], but the bulk of applications and existing practical schemes are for the dynamic case [15, 16, 11, 14, 26, 13, 4, 3, 1]. Since the ultimate goal is clearly to have proven secure schemes in settings suitable for applications, it is important to bridge the above-mentioned gap by providing foundations for dynamic group signatures.

However, an extension of the existing treatment of static groups [5] to the dynamic case does not seem to be immediate. Dynamic groups are more complex, bringing in new elements, security requirements and issues. A dedicated and detailed treatment is required to resolve the numerous existing issues and ambiguities. This paper provides such a treatment.