Efficient Secure Group Signatures with Dynamic Joins and Keeping Anonymity Against Group Managers

Aggelos Kiayias[1,⋆] and Moti Yung[2]

[1] Computer Science and Engineering,
University of Connecticut Storrs, CT, USA
aggelos@cse.uconn.edu
[2] RSA Laboratories, Bedford, MA, and Computer Science,
Columbia University New York, NY, USA
moti@cs.columbia.edu

Abstract. The demonstration of an efficient construction proven secure in a formal model that captures all intuitive security properties of a certain primitive is an ultimate goal in cryptographic design. This work offers the above for the case of a group signature scheme (with the traditional notion of dynamically joining users and untrusted join manager). To this end we adapt a formal model for group signatures capturing the state-of-the-art requirements in the area and we construct an efficient scheme and prove its security. Our construction is based on the scheme of Ateniese et al., which is modified appropriately so that it becomes provably secure. This task required designing novel cryptographic constructs as well as investigating some basic number-theoretic techniques for arguing security over the group of quadratic residues modulo a composite when its factorization is known. Along the way, we discover that in the basic construction, anonymity does not depend on factoring-based assumptions, which, in turn, allows the natural separation of user join management and anonymity revocation authorities. Anonymity can, in turn, be shown even against an adversary controlling the join manager.

1 Introduction

The notion of *group signature* is a useful anonymous non-repudiable credential primitive that was introduced by Chaum and Van Heyst [13]. This primitive involves a group of users, each holding a membership certificate that allows a user to issue a publicly verifiable signature which hides the identity of the signer within the group. The public-verification procedure employs only the public-key of the group. Furthermore, in a case of any dispute or abuse, it is possible for the group manager (GM) to "open" an individual signature and reveal the identity of its originator. Constructing an efficient and scalable group signature has been a research target for many years since its introduction with quite a slow

⋆ Research partly supported by NSF Career Award CNS-0447808.

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 151–170, 2005.

progress, see e.g., [14,12,10,11,8,26,2,3,9,24,6]. The first construction in the literature that appeared to provide sufficient security as a general efficient scheme where user joins are performed by a manager that is not trusted to know their keys was the scalable scheme of Ateniese, Camenisch, Joye and Tsudik [3]. It provided constant signature size and resistance to attacks by coalitions of users. This scheme was based on a novel use of the DDH assumption combined with the Strong-RSA assumption over groups of intractable order. Recently, Bellare, Micciancio and Warinschi [4], noticing that [3] only prove a collection of individual intuitive security properties, advocated the need for a formal model for arguing the security of group signature. This basic observation is in line with the development of solid security notions in modern cryptography. They also offered a model of a relaxed group signature primitive and a generic construction in that model. Generic constructions are inefficient and many times are simpler than efficient constructions (that are based on specific number theoretic problems). This is due to the fact that generic constructions can employ (as a black box) the available heavy and powerful machinery of general zero-knowledge protocols and general secure multi-party computations. Thus, generic constructions typically serve only as plausibility results for the existence of a cryptographic primitive [20]. The relaxation in the model of [4] amounts to replacing dynamic adversarial join protocols where users get individual keys (as is the case in [3]) with a trusted party that generates and distributes keys securely.

The above state of affairs [3,4] indicates that there exists a gap in the long progression of research efforts regarding the group signature primitive. This gap is typical in cryptography and is formed by a difference between prohibitively expensive constructions secure in a formal sense and efficient more ad-hoc constructions. In many cases, as indicated above, it is easier to come up with provably secure generic inefficient constructions or to design efficient ad-hoc constructions. It is often much harder to construct an efficient implementation that is proven secure within a formal model (that convincingly captures all desired intuitive security properties). To summarize the above, it is apparent that the following question remained open:

> Design an **efficient** group signature with dynamic joins (and no trusted parties) which is **provably secure** within a formal model.

One of our contributions is solving the above open question by, both, adapting a new model for group signatures (based on the model of traceable signatures [23]), which follows the paradigm of [22] for the security of signature schemes, as well as providing an efficient provably secure construction (in the sense of the scheme of [3]).

This contribution reveals subtleties regarding what intractability assumptions are actually necessary for achieving the security properties. For example, the anonymity property in our treatment is totally disassociated from any factoring related assumption. (In order to reveal such issues a complete proof is needed following a concrete model, and this has not been done in the realm of (efficient) group signatures).