Accumulators from Bilinear Pairings and Applications

Lan Nguyen

Centre for Information Security,
University of Wollongong, Wollongong 2522, Australia
ldn01@uow.edu.au

Abstract. We propose a dynamic accumulator scheme from bilinear pairings and use it to construct an identity-based (ID-based) ring signature scheme with constant-size signatures and to provide membership revocation to group signature schemes, identity escrow schemes and anonymous credential systems. The ID-based ring signature scheme and the group signature scheme have very short signature sizes. The size of our group signatures with membership revocation is only half the size of those in the well-known ACJT00 scheme, which does not provide membership revocation. The schemes do not require trapdoor, so system parameters can be shared by multiple groups belonging to different organizations. All schemes are provably secure in formal models. We generalize the definition of accumulators and provide formal models for ID-based ad-hoc anonymous identification schemes and identity escrow schemes with membership revocation.

Keywords: Dynamic accumulators, ID-based, ring signatures, group signatures, identity escrow, membership revocation, privacy, anonymity.

1 Introduction

An *accumulator* scheme, introduced by Benaloh and de Mare [5] and further developed by Baric and Pfitzmann [3], allows aggregation of a large set of inputs into one constant-size value. For a given element, there is a *witness* that the element was included into the accumulated value whereas it is not possible to compute a witness for an element that is not accumulated. Camenisch and Lysyanskaya [11] extended the concept to *dynamic* accumulators, that means the costs of adding or deleting elements and updating individual witnesses do not depend on the number of elements aggregated. Accumulators have been found in a number of privacy-enhancing applications, including *ad-hoc anonymous identification*, *ring signatures* [13], *identity escrow* and *group signature* schemes with *membership revocation* [11].

Ring signature schemes, introduced by Rivest et al. [19] and further studied in [9], allows a user to form an ad-hoc group without a central authority and sign messages on behalf of the group. A user might not even know that he has been included in a group and even a party with unlimited computing resources can not identify the signer. Zhang and Kim [23] extended the concept to *ID-based* ring

A.J. Menezes (Ed.): CT-RSA 2005, LNCS 3376, pp. 275–292, 2005.
© Springer-Verlag Berlin Heidelberg 2005

signature schemes, where the group is formed by using members' identities rather than their public keys. ID-base cryptography was introduced by Shamir [20] to simplify key management in public key primitives. In any ID-based system, there is a central authority, called *Private Key Generator* (PKG), to extract private keys from identities. In ID-based ring signature schemes, to comply with the ad-hoc property, the involvement of a central authority is limited to only setting up initial public parameters and generating private keys from identities, and not for forming groups.

While having simple group formation set up as an advantage, the size of ring signatures linearly depends on the group size, as the verifier needs to know at least the group description. However, as pointed out in [13], in many scenarios, the group does not change for a long time or has a short description. So an appropriate measurement of ring signature sizes does not need to include the group description and it is a good direction to find constant-size ring signatures without the group description part. A ring signature scheme (DKNS04) with such a property has been proposed by Dodis et al. [13]. They provide an ad-hoc anonymous identification scheme, where a user can form ad-hoc groups and anonymously prove membership in such groups, and use the Fiat-Shamir heuristics [14] to convert it into the ring signature scheme. The DKNS04 scheme requires user public keys to be primes, that does not seem to allow an ID-based extension. This paper provides the first ID-based ring signature scheme with constant-size signatures (without counting the list of identities to be included in the ring).

The notion of ring signatures is originated from the notion of group signatures, which was introduced by Chaum and Van Heyst [12]. A group signature scheme allows a group member to sign a message on behalf of the group without revealing his identity, and without allowing the message to be linkable to other signed messages that are verifiable under the same public key. The main difference with ring signature schemes lies in the role of a *group manager*. The group manager registers new users by issuing membership certificates that contains registration details, and in case of dispute revokes anonymity of a signed message by 'opening' the signature. In some schemes the functions of the group manager can be split between two managers: an *issuer* and an *opener*. An identity escrow system [15] can be converted into a group signature scheme using the Fiat-Shamir heuristic [14], and group signatures have been used as building blocks for *anonymous credential* systems [2]. A formal model (BSZ04) of group signature schemes was proposed by Bellare et al. [4] with four security requirements (correctness, anonymity, traceability and non-frameability). In Crypto 2000, Ateniese et al. (ACJT00) [1] proposed an efficient group signature scheme with very short length and low computation cost. Ateniese and de Medeiros later proposed an efficient group signature scheme (AdM03) [2] that is 'without trapdoor' in the sense that none of the parties in the system, including the group manager, need to know the trapdoor for generating system parameters. They also outline the importance of this property in real-world applications.