Lingling WANG, Guoyin ZHANG, Chunguang MA

A survey of ring signature

Abstract Ring signature allows specifying a set of possible signers without revealing which member actually produces the signature. This concept was first formalized in 2001 by Rivest, Shamir and Tauman. In this paper, we review the state-of-the-art of ring signature, summarize the study of ring signature schemes in the literature and investigate their relationships with other existing cryptographic schemes. We also describe a large number of extensions, modifications and applications of ring signatures after the original version of this work. Some problems in the study of this field were presented as well. Finally, we discuss a number of interesting open problems and point out the possible future work.

Keywords ring signature, existing cryptographic schemes, modification, application

1 Introduction

The notion of ring signatures was first introduced and implemented in 2001 by Rivest, Shamir and Tauman [1]. A ring signature scheme can be considered as a simplified group signature scheme [2]. In a ring signature scheme, there are neither prearranged groups of users, nor procedures for setting, changing or deleting groups, nor any way to distribute specialized keys. A valid ring signature convinces a verifier that the signature is generated by one of the ring members, without revealing which participant is the actual signer. Ring signature provides an elegant way to leak authoritative secrets in an anonymous way, and to implement designated verifier signature schemes that can authenticate emails without undesired side effects. The property of unconditional anonymity is very useful when it is indispensable for some information to be protected for a long time.

A great number of related ring signature schemes have been proposed since its introduction. In 2002, Abe et al. [3] addressed how to use public-keys of several different signature schemes to generate 1-out-of-\(n\) signatures. Ring signature schemes based on bilinear pairings and identity-based cryptography [4] were proposed by Zhang and Kim. Bresson et al. [5] presented the notion of a threshold ring signature scheme, and applied it to Ad-hoc networks. To protect privacy, Naor [6] proposed the concept of deniable ring authentication.

In 2003, based on the deniable ring authentication proposed in Ref. [6], Susilo and Mu [7] gave a non-interactive scheme that can be used in practice without having to use the anonymous routing channel (e.g., MIX-nets). Considering the situation that the actual signer is willing to prove to the verifier that he actually signs the signature, Lv and Wang [8] introduced a verifiable ring signature. Gao et al. [9] presented an efficient ring signature scheme based on the Nyberg-Rueppel signature scheme. To prove the security of ring signature schemes, Herranz and Sáez [10] generalized forking lemmas to the ring signatures’ scenario. Zhang et al. [11] combined proxy signature with ring signature to obtain proxy ring signatures. Chen et al. [12] utilized ring signatures to construct concurrent signatures. Wong et al. [13] proposed another way to construct ring signatures—Reed-Solomon (RS) code construction—and gave a threshold extension.

In 2004, Liu et al. [14] and Tsang et al. [15] proposed linkable ring signatures that can detect whether two signatures are signed by the same signer. Dodis et al. [16] discussed the problem of anonymous authentication in Ad-hoc groups, and pointed out that the one-way accumulator [17] is a great tool to solve the problem. As for verifiable ring signature, Gan and Chen [18] presented an efficient method to transform Rivest’s scheme into a verifiable ring signature scheme, in which the actual signer can embed identification information in a so-called subliminal channel. Based on identity-based cryptography, Awasthi and Sunder [19] gave efficient ring signature schemes and proxy ring signatures. Herranz and Sáez [20] presented a
new ID-Based scheme. By combining ring signature and authenticated encryption together, Lv et al. [21] introduced a new type of authenticated encryption signature called ring authenticated encryption. In Ref. [22], Cao et al. found some weaknesses in Lv et al.’s scheme, stating that it cannot achieve signer-verifiability and recipient-verifiability properties. Subsequently, they proposed an improved ring authenticated encryption scheme to eliminate these weaknesses. Wang et al. [23] gave a new group signature scheme based on the idea of ring signature. Chan et al. [24] proposed the notion of blind ring signature. Further study on blind ring signature can be found in Refs. [25–29].

In 2005, for threshold ring signature, further study can be found in Refs. [30,31]. Lee et al. [32] proposed a convertible ring signature that can withdraw the anonymity. Tsang and Wei [33] constructed the first short linkable ring signature for e-voting and e-cash systems. Nguyen [34] gave a dynamic accumulator based on bilinear pairings, and presented an ID-based Ad-hoc anonymous identification scheme. He pointed out that applying the Fiat-Shamir heuristics to the ID-based Ad-hoc anonymous identification scheme results in an ID-based ring signature scheme with constant-size signatures. Wu et al. [35] gave an efficient blind ring signature scheme. To overcome the disadvantages of existing fingerprinting schemes, an anonymous fingerprinting scheme using a modification of Schnorr ring signature was presented in Ref. [36]. Liu and Wong [37] suggested solutions to the key exposure problem in ring signature. They proposed the first forward secure ring signature scheme and the first key-insulated ring signature scheme.

In 2006, Zhang and Chen [38] discussed the authentication scheme in Ref. [34], and improved it. Chen et al. [39] extended the existing notion of ring signatures, and proposed the concept of identity-based anonymous designated ring signature which can be used in a Peer-to-Peer (P2P) network. Almost all of the proposed ring signature schemes relied on the random oracle model (ROM) for security proof. However, ROM does not take into account certain realistic attacks, and previous definitions of security for ring signature schemes are too weak. In Ref. [40], based on bilinear pairings, Chow et al. proposed a ring signature scheme which is verified to be secure against adaptive chosen message attack without using the random oracle model. Bender et al. [41] proposed new definitions of anonymity and unforgeability, which addressed most realistic threats, and proved that their new notions were strictly stronger than previous ones. They also showed two constructions of ring signature schemes in the standard model. In Ref. [42], Huang et al. proposed an ID-Based ring sign- cryption scheme. In addition, new further studies on anonymity revocation of ring signature can be found in Refs. [43,44]. Au et al. [45] observed a subtle and yet imperative blemish glossed over by the security model definition in Ref. [33]. Then they proposed a new short linkable ring signature scheme that was improved upon the existing scheme.

From the development procedure of ring signature, we can divide it into three stages as follows.

2001–2002: Marked by Rivest’s view of ring-signature, the work of this stage mainly took Rivest’s view as the reference and further proposed the detailed signature scheme.

2003–2004: Some researchers in the field of cryptology focused on the research work on ring signature two years after the ring signature was proposed. This is such an important stage for the development of ring signature that many new ideas, new concepts, new models and new schemes sprang up.

2005–the present: The research work on the security, efficiency and practicability of the ring signature was emphasized in this stage. For instance, there are studies on the secure and efficient scheme of ring signature, the mutual transformation of ring signature and common digital signatures and the popularization of ring signature.

In this paper, we tried to survey different ring signature schemes to the best of our knowledge. The definitions of ring signature are described in Sect. 2. Then, we classify the proposed ring signature schemes into four kinds, namely threshold ring signature, linkable ring signature, verifiable ring signature, and deniable ring signature. In Sect. 4, ring signature schemes combined with other signatures are summarized, namely proxy ring signature, blind ring signature, and ring signcryption. The last section concludes this paper and discusses future work.

2 Definitions

2.1 Ring signatures

We call a set of possible signers a “ring”, the ring member who produces the actual signature the “signer” and each of the other ring members a “non-signer”. Assume there are \( n \) members in a ring. A ring signature scheme is defined by the following procedures:

- **Key-Gen** \( (k) \) is a probabilistic polynomial algorithm that accepts security parameter \( k \), and returns system parameters and key pairs (public key \( P_i \) and the corresponding secret key \( S_i \)).

- **Ring-sign** \( (m, P_1, P_2, ..., P_r, S_i) \) is a probabilistic polynomial algorithm that produces a ring signature \( \sigma \) for the message \( m \), given the public keys \( P_1, P_2, ..., P_r \) of the \( r \) ring members, together with the secret key \( S_i \) of the \( i \)th member (who is the actual signer).

- **Ring-verify** \( (m, S_i) \) is a deterministic algorithm that takes a message \( m \) and a signature \( \sigma \), which includes the public keys of all the possible signers, and outputs either “true” if the ring signature is valid, or “false” otherwise.