Front. Electr. Electron. Eng. China 2008, 3(1): 10–19
DOI 10.1007/s11460-008-0012-8

REVIEW ARTICLE

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] proposed 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 channe1. Based on identity-based cryptography, Awasthi and Sunder [19] gave efficient ring signature schemes and proxy ring signatures. Herranz and Sáez [20] presented a

Translated from *Journal on Communications*, 2007, 28(5): 109–117
[译自: 通信学报]

Lingling WANG (✉), Guoyin ZHANG, Chunguang MA
College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China
E-mail: lingling@hrbeu.edu.cn

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 signcryption 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, S_s) is a probabilistic polynomial algorithm that produces a ring signature σ 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_s of the sth member (who is the actual signer).

Ring-verify (m, S_s) is a deterministic algorithm that takes a message m and a signature σ, which includes the public keys of all the possible signers, and outputs either "true" if the ring signature is valid, or "false" otherwise.

In a ring signature, different members can use different independent public key signature schemes, with different keys and signature sizes. We can see that a ring signature scheme satisfies the properties of anonymity (or signer-ambiguity) and spontaneity (namely, no setup procedure). Rivest, et al. [1] formalized "Ring Signature" because their construction of the signature forms a ring structure. Some other works in the literature also call this kind of signature (with the above properties) "Ring Signature" although some of them may not have a ring structure in their construction.

2.2 The security requirements

A secure ring signature scheme must satisfy the following properties:

Correctness: Any verifier with overwhelming probability must accept a ring signature generated in a correct way.

Anonymity: Any verifier should not have a probability greater than $1/n$ to guess the identity of the real signer who has computed a ring signature on behalf of a ring of n members. If the verifier is a member of the ring distinct from the actual signer, then its probability to guess the identity of the real signer should not be greater than $1/(n–1)$.

Unforgeability: Any attacker must not have non-negligible probability of success in forging a valid ring signature for some message m on behalf of a ring that does not contain him, even if he knows valid ring signatures for messages, different from m, which he can adaptively choose.

3 Sorts of ring signature schemes

The ring signature has a wide application area because of its spontaneity, unconditional anonymity, and group property. However, different application requires a certain specific feature to the ring signature, such as the features of threshold property, linkability, anonymity revocation, and deniability. In accordance with different requirements, the ring signature demands different specific features. In the light of different specific features, we classified the schemes of the ring signature into four types and a further explanation is given as follows.

3.1 Threshold and general access ring signature

Threshold mechanism is a great tool to share the power or secret in a company. A (t, n) threshold signature scheme allows t or more group members to generate a signature on behalf of the group. Any group with fewer than t members cannot generate a valid signature, and any set of the group cannot impersonate another set of members to sign any message without holding responsibility. In case of disputes, the threshold signature can be opened, so that the original signers can be traced without revealing the secret keys.

In 2002, Bresson et al. [5] applied the threshold signature to ring signature, and proposed a threshold ring signature. A t threshold ring signature scheme is a scheme where each ring signature is a proof that at least t members of the ring are confirming the message. In a general access ring signature scheme, members of a set can freely choose any family of sets including their own set, and prove that all members of some set in the access structure have cooperated to compute the signature, without revealing any information about which set it is. Bresson et al. gave a provably secure scheme (BSS) by utilizing a combinatorial notion that is called fair partition.

In 2003, Wong et al. [13] presented a new threshold ring signature scheme from the observation of the equivalency between the erasure correction technique of the Reed-Solomon (RS) code and the polynomial interpolation. Later, Liu et al. [46] considered the situation that each ring member used different public key cryptography, and proposed the notion of separability. They combined the separability with threshold signature, and gave a separable threshold ring signature scheme that can use RSA and discrete logarithm (DL).

In 2004, Chow et al. [25] presented the first identity-based (ID-based) threshold ring signature scheme based on secret sharing technique. The scheme was provably secure in the random oracle model and provided trusted authority compatibility. Liu and Wong [26] made fine-grained distinctions on the security models for provably secure ring signature schemes because some schemes may be secure in some of the models but not in the others. They also proposed a threshold ring signature scheme using bilinear maps and showed its security against adaptive adversaries in the strongest model defined. By applying the properties of separability and linkability to threshold ring signature, Tsang et al. [27] proposed the model for separable linkable threshold ring signatures. Herranz and Sáez [28] extended ring signature to distributed ring signature, where a subset of users cooperate to compute a distributed anonymous signature on a message, on behalf of a family of subsets. They proposed two schemes, one for general families of subsets, and another for threshold families of subsets. Wu et al. [29] gave a t-out-of-n ring signature based on a discrete logarithm problem (DLP).

In 2005, Isshiki and Tanaka [30] pointed out that BSS [5] is efficient when the number t of signers is small compared with the number n of group members. However, it is inefficient when t is $\omega(\lg n)$. They proposed a new threshold ring signature scheme (ITS) that is efficient when the number of signers is large compared with the number n of ring members, by modifying the trap-door one-way permutations in the ring signature scheme and using the combinatorial notion of fair partition. The fair partitions played different roles in ITS and BSS. Namely, ITS scheme uses the fair partitions for proving correctness and unforgeability, while BSS scheme employs the fair partitions for correctness and anonymity.

Au et al. [31] proposed to construct different schemes according to the different levels of signer anonymity. They presented the first ID-based threshold ring signature scheme that is not based on bilinear pairings, and the first ID-based threshold linkable ring signature scheme. They also showed how to add identity escrow to the two schemes. With identity escrow, some trusted authority can revoke the anonymity of a ring signature if needed.

3.2 Linkable ring signature

The notion of linkable ring signatures (LRS), introduced by Liu et al. [14], allows anyone to determine whether two ring signatures are signed by the same group member. Liu et al. also presented a linkable ring signature scheme (LSAG), which was proved to secure using a new efficient reduction of famous rewind simulation lemma that satisfies the properties of anonymity. Based on it, they also constructed a new efficient one-round e-voting system that does not possess a registration phase. Later, Tsang et al. [15] introduced the security notions of accusatory linkability and non-slanderability to linkable ring signatures. They presented the first separable linkable ring signature scheme, which supports an efficient threshold option. In Ref. [15], compared with "group-oriented" linkability, a new linking criterion called "event-oriented" linkability was also proposed, in which one can tell whether two signatures are linked, if and only if they are signed for the same event, despite the fact that they may be signed on behalf of different groups. They pointed out that event-oriented linkable ring signatures are comparatively more flexible in application.

In 2005, in order to capture new and practical attacking scenarios, Liu and Wong [47] enhanced the security model of Ref. [14] by providing a stronger notion of signer anonymity and redefining linkability. They also proposed two polynomial-structured LRS schemes. Tsang and Wei [33] extended the short ring signature scheme construction of Dodis et al. [16] to the first short LRS scheme construction (SLRS), and reduced its security to a set of assumptions, including a new hardness assumption, the link decisional RSA (LD-RSA) Assumption. They also took advantage of SLRS to construct an e-voting scheme, direct anonymous attestation and an e-cash scheme.

In 2006, Au et al. [45] detected a subtle blemish in the security model for SLRS. They pointed out that their security model glossed over the existence of an empowered central authority. They investigated the literature on the security models proposed for linkable ring signatures and formalized a new one that was the strongest among all. A new short linkable ring signature construction (NSLRS) based on SLRS was also proposed, which is secure under their new security model. In a linkable ring signature, when two ring signatures are produced by the same signer, then anyone can link the signatures. In Ref. [48], Liu et al. introduced a new concept called linkable ring signature with designated linkability, so that ring signatures can only be linked by a designated party whenever necessary. This concept not only guarantees the privacy of the signer, but also protects the receiver from being abused. A specific scheme based on LSAG (RSDL) was also given in Ref. [48].

We will make comparison among the schemes above. LSAG is based on a discrete logarithm problem. The structure is simple, and the follow-up papers on the theory and applications of linkable ring signatures are all based on it. For a ring with n members, the signature size of LSAG is $o(n)$. Likewise, RSDL is also based on LSAG, but the computation for linkable tag is different. Their approach is to encrypt the linkable tag using existing techniques, namely, the ElGamal encryption algorithm and non-interactive zero knowledge proof, in order to guarantee the validity of the signature (including the validity of the linkability) to be publicly verifiable. The signature size of RSDL is also $o(n)$. SLRS is the first LRS scheme, the signature size of which is $o(1)$. However, the security of SLRS is based on a zero knowledge proof system, a new hardness assumption (the link decisional RSA (LD-RSA) assumption), and PK-bijectivity, so that the structure is complicated. NSLRS is an improved SLRS. Denote by QR(N), the group of quadratic residues modulo a safe prime product N. NSLRS is secure if the decisional Diffie-Hellman (DDH), strong RSA and Link Decisional RSA problems are hard in QR(N). NSLRS is the most practical and efficient linkable ring signature scheme among all LRS schemes proposed. It consists of five polynomial-time algorithms (Init, Key-Gen, Sign, Verify, Link), which we will sketch below.

Let N be a safe prime product if $N = pq(2p'+1)(2q'+1)$ for some primes p, q, p', q' such that p' and q' are of the same length.

Init. Input the security parameter λ, generate a collision-resistant one-way accumulator f, together with its description desc. Choose a generator g of QR(N), where N is defined in desc. Output system public parameters param $= (1^{\lambda}$, desc, $g)$.

Key-Gen. Input the system's parameters param, the algorithm outputs the key pair $(sk_i, pk_i) = ((p_i, q_i), y_i)$. Upon obtaining the key pair, the algorithm executes the prove protocol with the certificate authority (CA) to obtain a certificate. The user public key is then augmented with the certificate and the key pair is returned.

Sign. Input public key set $Y = \{pk_1, pk_2, \ldots, pk_n\}$ and the private key $sk_\pi = (p_\pi, q_\pi)$. At first verify the certificates. Then, compute the witness $w_\pi \leftarrow f(u, \{y_i \mid i \neq \pi\})$ of y_π and accumulated value $v \leftarrow f(w_\pi, y_\pi)$. Compute a signature for M:

$$\sigma' = SPK\{(w, y, p. q): w^y = v \bmod N \\ \wedge y = 2pq + 1 \wedge y \in S(2^l, 2^u) \\ \wedge q \in S\left(2^{l/2}, 2^u\right) \wedge y' = g^{p+q} \bmod N\}(M).$$

The signature σ returned by the algorithm is given by $\sigma = (v, y', \sigma')$, where the tag y' is uniquely determined by the private key sk_π.

Verify. Given the public key set and the signature σ, verify the certificates and the statement $v = f(u, \{y_i \mid i \in [1, n]\})$, and then accept if both checks pass or otherwise reject.

Link. Given two valid signatures, extract their respective linkability tags y' and return linked if they are the same or unlinked otherwise.

3.3 Verifiable ring signature

A ring signature scheme enables a signer to produce a signature without revealing its identity. However, in some situations, a mechanism should be available for someone to prove that he or she is the real signer of the ring signature. For example, the government would like to reward the real signer. Naturally everyone in the ring is eager to claim to be the signer of the ring signature.

Fortunately, Lv and Wang [8] formalized the notion of verifiable ring signatures in 2003, which possesses the following additional property: if the actual signer is willing to prove to a recipient that he signed the signature, then the recipient can correctly determine whether it is true or not. Gan and Chen [18] proposed an efficient method to transform Rivest's scheme into a verifiable ring signature scheme, in which the actual signer can embed identification information into a so-called subliminal channel. In 2005, Lee et al. [32] proposed an efficient convertible ring signature scheme, which not only keeps all properties of a ring signature, but also enables the real signer to turn his ring signature into an ordinary signature by releasing some information.

The deniable ring signatures (DRS) proposed by Susilo and Mu [43] also has the property of anonymity revocation. The difference from the ring signatures is that the DRS allows verifier V to interact with the signer or entities to confirm that the signer/entity generates the signature with zero knowledge interactive proof. Compared with the schemes proposed in Refs. [8,18,32], DRS also solved the problem in which the signer can shift the blame to entities. Later, Wang and Liu [44] introduced a signer-admission ring signature scheme (WL06), which combines the idea of the designated confirmer signatures (DCS) and the designated verifier proofs.

In most of the proposed verifiable ring signature schemes, the identity of the signer can be verified publicly. However, the WL06 only allows the designated verifier to identify the actual signer, and the verifier cannot prove to others the identity of the signer. In essence, the WL06 is a zero knowledge proof with a non-transferability property. WL06 differs from DCS in that a conversion proof for the incomplete signature is placed in the signature generation phase. This can prove that uncertain factors a and b are properly constructed. Thus, the actual signer can, by running an interactive protocol, prove to others that he or she knows the discrete logarithm of b to the base a.

Recently, Zhang et al. [49] introduced a new verifiable ring signature scheme based on Nyberg-Rueppel signature. The scheme realizes the ring signature by merely using the hash functioning, which can verify the actual signer besides satisfying the properties of unconditional anonymity and non-forgeability. A traceable ring signature scheme (TRS) was also introduced by Fujisaki and Suzuki [50]. A traceable ring signature can restrict "excessive" anonymity. It has a "tag" that consists of a list of ring members and an issue that refers to, for instance, a social affair or an election. A ring member can make any signed but anonymous opinion regarding the issue, but only once. Fujisaki and Suzuki pointed out that the TRS suited many applications, such as an anonymous voting on a BBS and a dishonest whistle-blower problem.

3.4 Deniable ring authentication

Digital signatures enable authenticating messages in a way that disallows repudiation. While non-repudiation is essential in some applications, it might be undesirable in others. In 2002, Deniable ring authentication, which merges ring signatures and deniable authentication, was first introduced in Ref. [6] by Naor. In a deniable ring authentication, it is possible to convince a verifier that a member of an Ad-hoc subset of participants is authenticating a message m without revealing who has issued the signature, and the verifier cannot convince any third party that the message m is indeed authenticated. It has been found in a number of various applications.

For a scheme to be a Deniable ring authentication, it should: 1) Enable the sender for any message one wishes and for any Ad-hoc collection S of users containing the sender to prove (interactively) that a member of S is the one that confirms the message. 2) Be a good authentication scheme, i.e., not allowing forgeries. Ideally, an adversary should not be able to make a receiver accept any message not sent by a member of S. 3) The authentication is deniable in the zero knowledge sense, i.e., the recipient could have simulated the conversation alone and the result would have been indistinguishable. 4) The authentication should be source hiding or preserve the "anonymity in a crowd of the sender, for any arbitrary subset S of users or any two members of S generate indistinguishable conversations to the recipient. 5) The scheme should not assume that the verifier of the authentication is part of the system and has established a public key.

Naor provided the first construction of a Deniable ring authentication protocol based on the assumption that users have public-keys of some good encryption schemes. We call it MN02. In 2003, Susilo and Mu [7] pointed out the flaw of MN02: the verification is done interactively, and hence, the requirement of having an anonymous routing, such as MIX-nets, is essential. Moreover, the message size is longer compared with a normal ring signature. Then Susilo et al. defined the notion of non-interactive deniable ring authentication, and proposed a generic method for converting a ring signature scheme into a non-interactive deniable ring authentication scheme. They showed that a non-interactive deniable ring authentication scheme can be constructed from a ring signature scheme combined with a chameleon hash. Then they provided a ring signature scheme with a designated verifier. We call it WS03. The size of WS03 is the same as the original ring signature scheme plus a random number. Also, WS03 only requires the designated verifier V to have a published chameleon hash function to be used by the signer, rather than to interact with the authenticator. However, there is a restriction in WS03 that the verifier has to set up a chameleon hash function before a message can be sent to him/her, which is certainly not practical. Later, Susilo and Mu [43] drew on an ID-based chameleon hash function to construct their scheme, in which the only requirement for the verifier is to have his ID published.

4 Other signatures related to ring signature

After Rivest et al.'s first ring signature scheme was announced, many ring signature schemes have been proposed. Ring signatures can be combined with other special signatures to obtain some new types of ring signatures. Some kinds of the combined signatures are listed as follows.

4.1 Proxy ring signature

Proxy ring signature can be viewed as the combination of proxy signature and ring signature, so it satisfies all the requirements of general proxy signature besides the requirements of ring signature. Proxy ring signature has been shown to be useful in various applications, such as electronic polling, electronic payment, etc. Consider the following scenario: an entity delegates his signing capability to some proxy signers. Any proxy signer can perform the signing operation of the original entity. These proxy signers want to sign messages in behalf of the original entity while providing unconditional anonymity. In this situation, proxy signature and group signature are not suitable. Fortunately, the problem can be solved by proxy ring signature. The first proxy ring signature scheme was proposed by Zhang et al. [11] in 2003. Later, Lang et al. [51] proposed an improved identity-based proxy ring scheme from bilinear pairings. Compared with Zhang's scheme, Lang's scheme is a computational efficiency improvement for signature verification because the computational cost of bilinear pairings required is reduced from $o(n)$ to $o(1)$. In 2006, Li et al. [52] presented formally the definition and security model for proxy ring signature. Subsequently, they proposed a short proxy ring signature scheme, with rigorous security proofs, which was argued to be more efficient than the existing proxy ring signature schemes.

4.2 Blind ring signature

Blind ring signature, which can be regarded as the combination of blind signature and ring signature, was first proposed by Chan et al. [24] in 2005. Chan et al. gave a general construction of blind spontaneous anonymous group (SAG) 1-out-of-n and t-out-of-n signature schemes from essentially any major blind signature. However, Chan's scheme was obscure and it was unclear who actually engaged in the different protocols. Later, Wu et al. [35] pointed out that the blindness of the existing blind ring signature schemes was easy to break by a malicious anonymous signer of dynamic groups. They proposed to integrate the blindness of the message into ring signatures for static groups, and gave a static blind ring signature scheme, which is provable under the extended ROS assumptions in the random oracle model and the generic group model. Here, ROS refers to finding an overdetermined, solvable system of linear equations modulo q with random inhomogeneities (right sides). In addition, after the group public key was generated, the space, time and communication complexities of the relevant parameters and operations were constant. In 2006, after discussing the disadvantages of the proposed blind ring signature schemes, Herranz and Laguillaumie [53] presented a simple blind ring signature scheme based on pairings on algebraic curves. The security of their scheme is proved in the random oracle model, under the chosen-target-CDH assumption.

4.3 Ring authenticated encryption

An authenticated encryption scheme allows the verifier to recover and verify the message simultaneously. In 2004, Lv et al. [21] introduced a new type of authenticated encryption called ring authenticated encryption, which is an authenticated encryption scheme where the verifiability property holds with respect to a ring signature scheme. In Ref. [22], Cao et al. found some weaknesses in Lv et al.'s scheme, stating that the scheme cannot achieve signer-verifiability and recipient verifiability properties. Cao et al. also proposed an improved ring authenticated encryption scheme to eliminate these weaknesses. Later, Cao et al. [54] designed an ID-based ring authenticated encryption scheme based on Boneh and Frankliny's ID-based encryption scheme and Zhang and Kim's ID-based ring signature scheme. In 2006, Huang et al. [42] combined the ring signature with the signcryption scheme, and proposed an ID-based ring signcryption scheme based on Weil pairings. Compared with the ring authenticated encryption, ring signcryption is easier to accomplish, possessing more properties.

5 Applications

Ring signatures have been shown as a powerful tool for applications in the field of management, military affairs, politics, economics and the like. It plays a very important role in keeping the confidential information, voting for the crucial leaders, carrying out the e-business, press releasing and so on. We will mainly introduce four of its applications briefly as follows.

5.1 Leaking secrets

Leaking a secret anonymously is the motivation for Rivest et al. to propose ring signatures. For example, suppose that Bob is an employee in a company, and that Bob wishes to leak a corrupt fact about the manager to a journalist, in such a way that Bob remains anonymous, while the journalist is convinced that the leak comes indeed from the company. Bob cannot send to the journalist a standard digitally signed message. Although such a message can convince the journalist that it comes from the company, it also directly reveals Bob's identity. It also doesn't work for Bob to send the journalist a message through a standard anonymous letter, since it strips off all source identification and authentication. The journalist would have no reason to believe that the message really comes from the company at all. A standard group signature scheme does not solve the problem, since it requires the prior cooperation of the other group members who may be controlled by the manager to set up, and leaves Bob vulnerable to later identification by the group manager. Nonetheless, the ring signature can solve the entire problems above.

5.2 E-voting or e-cash system

It is efficient and more secure to apply ring signature to e-cash and e-voting systems. For example, we can adopt linkable ring signature to solve the problem of tracing the double spenders/voters directly. In Ref. [33], a short linkable ring signature scheme (SLRS) is designed for e-voting and e-cash systems, especially when the ring size is large. However, SLRS can only be used to detect the double spenders, and it does not work well in tracing the identity of the spender. Accordingly, it becomes necessary to draw on new techniques to improve the existing ring signature schemes or design new schemes.

5.3 Protecting intellectual property

Protecting intellectual property in digital goods has been a subject of research for many years and has led to the development of various techniques. Among them, fingerprinting schemes are important techniques for the protection of intellectual property. In Ref. [36], Lei et al. presented an anonymous fingerprinting scheme using a modification of the Schnorr ring signature. When a buyer wants to buy digital goods, he or she can sign the text m that describes the deal on behalf of the ring, which can bring full anonymity and unlinkability. Once fingerprinted copies are redistributed, a merchant still could trace the buyer with a slightly different version.

5.4 Ad-hoc networks and wireless sensor networks

The steadily growing importance of portable devices and mobile applications has spawned new types of groups of interacting parties—Ad-hoc groups. The highly dynamic nature of such groups raises new challenges for networking. Ad-hoc networks may be described as networks with minimal infrastructure, lacking fixed routers or stable links. Such Ad-hoc networks inherently deal with spontaneous Ad-hoc groups; other instances of Ad-hoc groups are not dependent on the particular network infrastructure. For instance, a group of users who spontaneously decide to communicate sensitive data need a suite of protocols that do not involve any trusted third party or certification of any new public keys. Security goals have to be considered in the new context. Ring signatures are perfectly suited to such a setting, since no setup protocol is required to use them. In addition, since the wireless sensor network is similar to Ad-hoc networks, we can also apply ring signature to it. That will solve many problems in wireless sensor networks, such as anonymous authentication among nodes.

Moreover, a ring signature can also be employed to solve the problem of multi-party computation (MPC).

6 Overall conclusions and future work

Up to now, the following flaws separately exist in most ring signature schemes:

1) The size of public keys is dependent on the ring size due to the application of public keys in the signature algorithm.

2) The signature size of the scheme depends on the size of the ring because of the description of the ring members in the signature.

3) Owing to the unconditional anonymity of the ring signature, vicious signers can slander other possible signers in the ring.

4) The schemes (especially blind ring signature schemes) are subject to the chosen group-public-key attack if they are implemented for dynamic groups.

Considering the flaws and the problems existing in ring signatures, we summarize the future work on the theory and its applications.

1) Construct efficient ring signature schemes. In the proposed ring signature schemes, the signature size is dependent on the ring size. This is inefficient especially when the group size is large. Hence, how to construct a ring signature with constant-size signature is an open question, which is also the future work of our research. One solution is to use a one-way accumulator to design a short ring signature scheme.

2) Study the security proof for the scheme. Propose new techniques to prove the security of the scheme, not only in random oracle model but also in standard model. Analyze the existing security model, and consider the attack capability of the adversary roundly.

3) Discuss and improve the proposed schemes. There are some flaws in the proposed schemes, so it is necessary to discuss these schemes, study the security and improve it.

4) Propose new schemes based on new cryptography or new assumption. The hard problems in mathematics are the theory background for secure ring signature schemes. It will be interesting to take advantage of other hard problems to construct new schemes. Moreover, it becomes necessary to draw on new cryptography, such as certificateless cryptography, to design more new efficient and secure schemes.

5) Study the related problem about ring signatures. The problems related to ring signatures are as follows: the linkability, the deniability, anonymity revocation, etc. It is important to propose efficient related schemes, which can be used to solve practical problems.

6) Study the applications of ring signatures. In the proposed ring signature schemes, the study of the application of ring signatures is limited. Hence, it is our task to apply ring signatures to many applications, such as the e-cash system [55], e-voting system [56], and multi-party computation.

7) Study the signatures related to ring signature and their application. Recently, signatures related to ring signature have been proposed more and more. They are proxy ring signature, blind ring signature, and ring authenticated signature, etc. All of these play a great role in the corresponding situation. However, research on this aspect is just in the first stage.

8) Compare ring signature with group signature. Group signature is similar to ring signature, which can be viewed as a simplified group signature. It was proposed earlier than ring signature, and many problems about it have been solved. Therefore, we can draw on the accomplishment of group signature, apply it to ring signature and combine ring signature with group signature to solve some practical problems.

Acknowledgements This work was supported by the Natural Science Foundation of Heilongjiang Province (No. F2004–06) and Basic Research Foundation of Harbin Engineering University (No. HEUFT567).

References

1. Rivest R L, Shamir A, Tauman Y. How to leak a secret. Boyd C, ed. In: Proceedings of ASIACRYPT'01. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2001, 2248: 552–565
2. Chaum D, Heyst V E. Group signatures. Davies D W, ed. In: Proceedings of EUROCRYPT'91. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 1991, 547: 257–265
3. Abe M, Ohkubo M, Suzuki K. 1-out-of-n signatures from a variety of keys. Zheng Y L, ed. In: Proceedings of ASIACRYPT'02. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2002, 2501: 415–432
4. Zhang F G, Kim K. ID-based blind signature and ring signature from pairings. Zheng Y L, ed. In: Proceedings of ASIACRYPT'02. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2002, 2501: 533–547
5. Bresson E, Stern J, Szydlo M. Threshold ring signatures and applications to ad-hoc groups. Yung M, ed. In: Proceedings of CRYPTO'02. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2002, 2442: 465–480
6. Naor M. Deniable ring authentication. Yung M, ed. In: Proceedings of CRYPTO'02. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2002, 2442: 481–498
7. Susilo W, Mu Y. Non-interactive deniable ring authentication. Lim J I, Lee D H, eds. ICISC2003. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2004, 2971: 386–401
8. Lv J Q, Wang X M. Verifiable ring signature. In: DMS Proceedings of CANS'03, 2003, 663–665
9. Gao C Z, Yao Z A, Li L. A ring signature scheme based on the Nyberg-Rueppel signature scheme. Zhou J, Yung M, Han Y, eds. In: ACNS 2003. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2003, 2846: 169–175
10. Herranz J, Sáez G. Forking lemmas for ring signature schemes. Johansson T, Maitra S, eds. In: Proceedings of

INDOCRYPT'03. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2003, 2904: 266–279

11. Zhang F G, Reihaneh S N, Lin C Y. New proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairings. http://eprint.iacr.org/2003/104
12. Chen L Q, Kudla C, Paterson K G. Concurrent signatures. Cachin C, Camenisch J, eds. In: Proceedings of EUROCRYPT'04. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2004, 3027: 287–305
13. Wong D S, Fung K, Liu J K, et al. On the RS-code construction of ring signature schemes and a threshold setting of RST. Qing S H, Gollmann D, Zhou J Y, eds. In: Proceedings of ICICS 2003. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2003, 2836: 34–46
14. Liu J K, Wei V K, Wong D S. Linkable spontaneous anonymous group signature for Ad-hoc groups. Wang H X, ed. In: Proceedings of ACISP'04. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2004, 3108: 325–335
15. Tsang P P, Wei V K, Chan T K, et al. Separable linkable threshold ring signatures. Canteaut A, Viswanathan K, eds. In: Proceedings of INDOCRYPT'04. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2004, 3348: 384–398
16. Dodis Y, Kiayias A, Nicolosi A, et al. Anonymous identification in Ad-hoc groups. Cachin C, Camenisch J, eds. In: Proceedings of EUROCRYPT'04. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2004, 3027: 609–626
17. Benaloh J, Mare M D. One-way accumulators: a decentralized alternative to digital signatures. Helleseth T, ed. In: Advances in Cryptology- EUROCRYPT'93. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 1993, 765: 274–285
18. Gan Z, Chen K F. A new verifiable ring signature scheme. Acta Scientlarum Naturalium Universitatis Sunyatseni, 2004, 43(Supp 2): 132–134(in Chinese)
19. Awasthi A K, Sunder L. ID-based ring signature and proxy ring signature schemes from bilinear pairings. http://eprint.iacr.org/2004/184
20. Herranz J, Sáez G. New identity-based ring signature schemes. Lopez J, Qing S H, Okamoto E, eds. In: Proceedings of ICICS 2004. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2004, 3269: 27–39
21. Lv J Q, Ren K, Chen X, et al. Ring authenticated encryption: a new type of authenticated encryption. In: Proceedings of SCIS 2004. Sendi: IEICE Press, 2004, 1179–1184
22. Cao T, Lin D, Xue R. Improved ring authenticated encryption scheme. In: Proceedings of JICC 2004. International Academic Publishers World Publishing Corporation, 2004, 341–346
23. Wang J L, Zhang J H, Wang Y M. A group signature scheme based on ring signature idea. ACTA Electronic Sinica, 2004, 32(3): 408–410(in Chinese)
24. Chan T K, Fung K, Liu J K, et al. Blind spontaneous anonymous group signatures for Ad-hoc groups. Castelluccia C, et al. eds. In: Proceedings of ESAS 2004. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2005, 3313: 82–94
25. Chow S S M, Hui L C K, Yiu S M. Identity based threshold ring signature. Park C, Chee S, eds. In: ICISC 2004. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2005, 3506: 218–232
26. Liu J K, Wong D S. On the security models of (threshold) ring signature schemes. Park C, Chee S, eds. In: Proceedings of ICISC 2004. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2005, 3506: 204–217
27. Tsang P P, Wei V K, Chan T K, et al. Separable linkable threshold ring signatures. Canteaut A, Viswanathan K, eds. In: Proceedings of INDOCRYPT'04. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2004, 3348: 384–398
28. Herranz J, Sáez G. Distributed ring signatures for Identity-Based scenarios. http://eprint.iacr.org/2004/190/
29. Wu Q H, Wang J L, Wang Y M. A t-out-of-n ring signature based on DLP. Advance in ChinaCrypt'04. Beijing: Science Press, 2004, 209–214
30. Isshiki T, Tanaka K. An (n-t)-out-of-n threshold ring signature scheme. Boyd C, Manuel J, Nieto G, eds. In: Proceedings of ACISP 2005. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2005, 3574: 406–416
31. Au M H, Liu J K, Tsang P P, et al. A suite of ID-based threshold ring signature schemes with different levels of anonymity. http://eprint.iacr.org/2005/326/
32. Lee K C, Wei H, Hwang T. Convertible ring signature. IEE Proceedings of Communications, 2005, 152(4): 411–414
33. Tsang P P, Wei V K. Short linkable ring signatures for E-voting, E-cash and attestation. Deng R H, et al, eds. In: Proceedings of ISPEC 2005. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2005, 3439: 48–60
34. Nguyen L. Accumulator from bilinear pairings and application to ID-based ring signatures and group membership revocation. Menezes A, ed. In: Proceedings of CT-RSA 2005. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2005, 3376: 275–292
35. Wu Q H, Zhang F G, Susilo W, et al. An efficient static blind ring signature scheme. Won D, Kim S, eds. In: Proceedings of ICISC 2005. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2006, 3935: 410–423
36. Lei Q, Jiang Z T, Wang Y M. Ring-based anonymous fingerprinting scheme. Hao Y, Liu J, Wang Y, et al, eds. In: Proceedings of CIS 2005. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2005, 3802: 1080–1085
37. Liu J K, Wong D S. Solutions to Key Exposure problem in ring signature. http://eprint.iacr.org/2005/427/
38. Zhang F G, Chen X F. Cryptanalysis and improvement of an ID-based Ad-hoc anonymous identification scheme at CT-RSA 05. http://eprint.iacr.org/2005/103/
39. Chen Y Q, Susilo W, Mu Y. Identity-based anonymous designated ring signatures. Guizani M, Chen H, eds. In: Proceedings of IWCMC'06. USA: ACM Press, 2006, 189–194
40. Chow S S M, Liu J K, Wei V K, et al. Ring signature without random oracles. http://eprint.iacr.org/2005/317/
41. Bender A, Katz J, Morselli R. Ring signatures: stronger definitions, and constructions without random oracles. Halevi S, Rabin T, eds. In: Proceedings of TCC 2006. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2006, 3876: 60–79
42. Huang X Y, Zhang F T, Wu W. An identity-based ring signcryption scheme. ACTA Electronic Sinica, 2006, 34(2), 263–266(in Chinese)
43. Susilo W, Mu Y. Deniable ring authentication revisited. Jakobsson M, Yung M, Zhou J, eds. In: Proceedings of ACNS 2004. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2004, 3089: 149–163
44. Wang C H, Liu C Y. A new ring signature scheme with signer-admission property. Information Sciences, 2007, 177(3): 747–754
45. Au M H, Chow S S M, Susilo W, et al. Short linkable ring signatures revisited. Atzeni A S, Lioy A, eds. In: Proceedings of EuroPKI 2006. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2006, 4043: 101–115
46. Liu J K, Wei V K, Wong D S. A separable threshold ring signature scheme. Lim J I, Lee D H, eds. In: Proceedings of ICISC 2003. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2004, 2971: 12–26

47. Liu J K, Wong D S. Linkable ring signatures security models and new schemes. Gervasi O, Gavrilova M L, Kumar V, et al. eds. In: Proceedings of ICCSA 2005. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2005, 3481: 614–623
48. Liu J K, Susilo W, Wong D S. Ring signatures with designated linkability. Yoshiura H, Sakurai K, Rannenberg K, et al, eds. In: Proceedings of IWSEC 2006. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2006, 4266: 104–119
49. Zhang C L, Liu Y, He D Q. A new verifiable ring signature scheme based on Nyberg-Rueppel scheme. In: Proceedings of ICSP2006. USA: IEEE Press, 2006
50. Fujisaki E, Suzuki K. Traceable ring signature. http://eprint.iacr.org/2006/389
51. Lang W M, Yang Z K, Cheng W Q, et al. An improved identity-based proxy ring signature scheme. High Technology Letters, 2005, 11(1): 17–19
52. Li J, Chen X F, Yuen T H, et al. Proxy ring signature: formal definitions, efficient construction and new variant. In: Proceedings of CIS 2006. USA: IEEE Press, 2006, 1259–1264
53. Herranz J, Laguillaumie F. Blind ring signatures secure under the Chosen-Target-CDH assumption. Katsikas S K, et al, eds. In: Proceedings of ISC 2006. Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2006, 4176: 117–130
54. Cao T J, Lin D D, Xue R. ID-based ring authenticated encryption. In: Proceedings of AINA'05. USA: IEEE Press, 2005, 591–596
55. Ma C G, Yang Y X. Transferable off-line electronic cash. Chinese Journal of Computers, 2005, 28(3): 301–308 (in Chinese)
56. Ma C G, Yang Y X, Hu Z M, et al. A fair electronic check systems with reusable refund. ACTA Electronic Sinica, 2005, 33(9): 1562–1566 (in Chinese)