Group-oriented ring signature

Chunbo Ma and Jun Ao

School of Information and Communication,

Guilin University of Electronic Technology, Guilin, Guangxi, 541004, P. R. China

Abstract. In this paper, we present an improved Rivest's ring signature scheme. In our scheme, the size of the signature is only related to the ring members, and the signer needs no to publish amount of random numbers. On this basis, we propose a group-oriented ring signature. In this scheme, only the person who belongs to the designated group can verify the validity of the ring signature. The security of these two schemes can be proved by using Forking Lemmas.

Key words. Ring signature, Group, Verification.

1. Introduction

The notion of ring signature was introduced in 2001 by Rivest, Shair and Tauman. Ring signature is very different from the group signature scheme and has following characteristics: a message signer is allowed to form a set of possible signers to conceal identity. All the possible signers constitute a distributed structure, and maybe members do not know the fact thatthey have been involved in a ring signature. To the verifier, he can verify the validity of a ring signature, however, he has no the ability to distinguish who produces the signature. What he can determine is that if the signature is valid, then the signer must be in the set of signers listed in the signature.

An example can better describe the application of ring signature. A company's senior managements are preparing to anonymously disclose some information to news media. Then, designing a ring signature is an effective method to complete is mission. A ring signature can be produced by using the set of all the senior managements. After receiving the signature, the news media can verify that whether the signature is generated by the company's senior managements, but the signer's actual identity can't be traced.

After the introduction of ring signature, many scholars have made in-depth research in this field and proposed a great number of related signature schemes. However, most of the current ring signatures and other multi-participants signature schemes, such as group signature, have to face such a defect that the length of the signature grow linearly with increasing in participants. In Rivest's ring signature scheme, the form of the signature is as $(m, P_1, P_2, \cdots P_r; v; x_1, x_2, \cdots x_r)$. Where $P_{1\le i\le r}$ is the ring member, and $x_{1\le i\le r}$ is a random number selected by the signer for $P_{1\le i\le r}$. It is obviously that the length of the signature is related to the amount of the random numbers and the ring members. The size of a ring signature in practice affects the storage of a system, especially for those of resource-limited systems. Therefore, how to shorten the length of the ring signature is very important in practice.

Group signature deals with those situations in which the signing is performed by a group of entities. However, in some instances, the signer maybe wants his signature only be verified by some designated members. Therefore, the signature with limited verification range is needed. Also, the signer of a ring signature has similar needs.

In this paper, we present a scheme to shorten the length of a ring signature. In our scheme, a signer need not to list amount of random numbers in a ring signature. With this method, the length of a ring signature is greatly shortened. On this basis, we propose a group-oriented ring signature. Comparing to Rivest's ring signature, the signer in group-oriented ring signature is allowed to designate several verifiers. In other words, the designated verifiers form a set that only in this set, one can verify the well designed group-oriented ring signature.

2. Related works

The concept of ring signatures was first introduced by Rivest, Shamir and Tauman [2] in 2001. Thereafter, a great number of extended ring signature schemes have been proposed.

In 2003, in order to prove the security of ring sinature schemes, Herranz and Sáez [3] introduced generalized forking lemmas to prove the security of ring signature scheme. In 2004, Awasthi and Sunder [4] presented an efficient identity-based ring signature scheme and a proxy ring signature.

In 2005, Nguyen [5] proposed an ID-based ring signature with constant size. Liu and Wong [6] gave a method to solve the key exposure problem in ring signature, and presented the first forward secure ring signature scheme and the first key-insulated ring signature scheme.

Random oracle model (ROM) has been widely used in proving the security of a ring signature. However, ROM is just suit for established attacks. Nobody knows what artifice the attackers will use. So studying ring signature without ROM is a challenging problem. In 2006, Chow et al. [7] proposed a ring signature scheme which is secure against adaptive chosen message attack without random oracle model.

Kallahalla et al. [8] presented a secure storage scheme, PLUTUS, in 2003. The primary goal of the scheme is to provide file owners with direct control over authorizing access to their files as well as scalable key management. For the user of PLUTUS, when he is allowed access to a certain re-encrypted files using given file-group key, then he can generate previous versions from the given key. The nature of the RSA scheme ensures that the user can't obtain the follow-up version.

The designated verifier signature first proposed by Jakobsson, Sako and Impagliazzo in 1996 [1] and followed by many research results. Jakobsson et al. extended the designated signature to multi-designated verifier signature.

Ma et al. presented the concept of group inside signature [9]. In their scheme, any one in the same group with the signer can verify the signature generated by the signer. Thereafter, Ma et al. [10] designed a group-oriented encryption scheme. In such a scheme, anyone can encrypt a message using the group public key and distribute the ciphertext to the designated group. Any member in the group can independently decrypt the ciphertext via his private key. In this type of signatures, the anonymous of the signer is not considered.

3. Rivest's ring signature scheme

In a ring signature scheme, a message signer forms a ring of any set of possible signer including him/herself. Without loss of generality, assume that there are n members in a ring, and the scheme is defined by the following procedures.

Step1. According to the security parameter k^*, the system manger produces the system parameters and the RSA key pair (e_i, d_i) for each member. Here e_i is a public key and d_i is the

matching private key.

Step2. On input a message m and the public keys $e_1, e_2, \cdots, e_n$ of the n ring members, the signer with his secret key produces a ring signature σ for the message m.

Step3. On input (m, σ), the verifier performs verification algorithm and outputs either "True" or "False".

A fairly-generated ring signature should be accepted as valid with respect to the specified ring with overwhelming probability; and it must be infeasible for any user, except with negligible probability, to generate a valid ring signature with respect to a ring he does not belong to.

In paper [2], Rivest et al. present two ring signature schemes, one is RSA version, and another is Rabin version. To simplify the presentation, we just describe the RSA version.

Assume that the PKI manager produces a sequence of RSA key pairs. Without loss of generality, we suppose that ring member P_i has a public key (n_i, e_i), the matching private key is d_i. Member P_i takes $\{P_0, P_1, \cdots, P_{n\geq i}\} \setminus P_i$ as the non-sign ring members, in other words, the ring members $\{P_0, P_1, \cdots, P_{n\geq i}\} \setminus P_i$ don't sign a message. To produce a ring signature, P_i performs following steps.

Step1. The signer P_i sets a fixed value v and computes the symmetric key s as the hash of the message m to be signed:

$$s = H(m).$$

Here H is a cryptographic one-way function. The signer chooses a random number for each non-sign ring member. We define the selected random number set is $\{x_0, x_1, \cdots, x_{n\geq i}\} \setminus x_i$.

Step2. Solve for x_i. The signer P_i solves the following ring equation for x_i.

$$C_s(x_0^{e_0}, x_1^{e_1}, \cdots, x_i^{e_i}, \cdots x_n^{e_n}) = v$$

Where $C_s(y_1, y_2, \cdots, y_n)$ is a combining function, which takes as input a key s, and arbitrary values $y_1, y_2, \cdots, y_n$.

Step3. The signature on message m is defined as follows.

$$(m, P_0, P_1, \cdots, P_n, v, x_0, x_1, \cdots, x_n)$$

Here we can see that the size of the ring signature grow linearly with the size of the ring member set. One reason is that the signature must list the ring members, and another reason is that the signer should produce a random number for each participant. Listing the ring members in a ring signature is unavoidable, and it is an inherent disadvantage. Therefore, reasonably choosing $(x_0, x_1, \cdots, x_n)$ is a way to shorten the length of the ring signature.

4. Shorten Rivest's ring scheme

In this section, the system parameters are as defined in section3. As we have mentioned above, Rivest's ring signature is as $(m, P_0, P_1, P_2, \cdots, P_n, v, x_0, x_1, x_2, \cdots, x_n)$. To verify the validity of a ring signature, one should verify whether the following equation holds.

$$x_0^{e_0} + x_1^{e_1} + \cdots + x_n^{e_n} = v$$

Where, $e_0, e_1, \cdots e_n$ are the public keys of $P_0, P_1, \cdots, P_n$, respectively. In addition, We define $x_0 = H(m \| c)$. Where c is a random number and "||" denotes concatenation. Before going through, we first introduce a theorem used in our signature scheme.

Theorem[11]: Let $T = \sum_{i=1}^{n} a_i y^{i-1}$, where $0 \le a_i < y$. Then $\left\lfloor \frac{T}{y^{j-1}} \right\rfloor \bmod y = a_j$.

We assume that ring member P_i will perform following ***Generation Algorithm*** to produce a ring signature on message m.

Generation Algrithm

Step1. Member P_i chooses a random number k, and produces a RSA key pair (d^*, e^*), and then computes following values.

$$k^{d^*}, k^{d^* d^*}, \cdots, k^{(d^*)^n}$$

Publish $k^{(d^*)^n}$ and e^*. In addition, we define $k^{(d^*)^n} = U$.

Step2. P_i picks random number $x_j < k$ for all the other ring members $1 \le j \le n$, $j \ne i$ and solves the following ring equation for $x_{i \ne 0}$.

$$x_0^{e_0} + x_1^{e_1} + x_2^{e_2} + \cdots + x_i^{e_i} + \cdots + x_n^{e_n} = v$$

Step3. Compute $\Omega = \sum_{i=1}^{n} k^{(d^*)^i} \cdot x_i$, and produce a ring signature $(m, P_0, P_1, P_2, \cdots, P_n, \Omega, v, c, U, e^*)$ on message m.

After receiving above signature, a verifier performs ***Verification Algorithm*** to verify the signature.

Verification Algorithm

Step1. Compute $x_0 = H(m \| c)$.

Step2. Compute

$$k^{(d^*)^{n-1}} = U^{e^*}, k^{(d^*)^{n-2}} = U^{(e^*)^2}, \ldots, k^{(d^*)^{n-n+1}} = U^{(e^*)^{n-1}}, \quad k = U^{(e^*)^n}$$

Step3. Compute $x_{i\geq 1}$ as follows.

$$x_{i\geq 1} = \left\lfloor \frac{\Omega}{k^{(d^*)^i}} \right\rfloor \bmod k$$

Step4. Verify if the following equation holds.

$$x_0^{e_0} + x_1^{e_1} + x_2^{e_2} + \cdots + x_i^{e_i} + \cdots + x_n^{e_n} = v$$

If above equation holds, it shows that the ring signature is valid.

5. Group-oriented ring signature

Designated verifier signature first proposed by Jakobsson, Sako and Impagliazzo in 1996 [1]. It is very useful in controlling the message transmission range. In this kind of signature schemes, nobody besides the designated person can verify the signature. Ma et al. extended the notion, and proposed the group-oriented encryption [13]. In group-oriented signature, nobody besides the designated group can verify the signature. Obviously, in a PKI authentication frame, each person should have his own key pair. So the core issue of group-oriented signature is how to design a scheme in which each group member is allowed to verify the signature independently. As we have mentioned above, a ring signature with limited verification range is necessary in some instances. A signer can perform following steps to produce a group-oriented ring signature.

Step1. The ring signer P_i chooses a random number y and computes value Q. Here $0 \leq v^{d^*} < y$.

$$\sum_{i=0}^{n} v^{d^*} y^{\prod_{j=0}^{n} e'_{j\neq i}} = Q$$

We define the set of verifiers as $(V_1, V_2, \cdots, V_n)$. Here e_i' is the public key of the designated verifier V_1. Without loss of generality, we suppose that V_i will verify the signature produced by P_i.

Step2. Compute and publishe value W.

$$y^{\prod_{i=0}^{n} e_i'} = W$$

Step3. Perform the ***Generation Algorithm*** in Section 4, and output a group-oriented ring signature

$$(m, P_0, P_1, P_2, \cdots, P_n, Q, \Omega, c, W, y, U, e^*)$$

To verify the signature $(m, P_0, P_1, P_2, \cdots, P_n, Q, \Omega, c, W, y, U, e^*)$, the verifier V_i takes following steps.

Step1. Compute $x_0 = H(m \,||\, c)$.

Step2. Compute the value v.

$$\left\lfloor \left(\frac{Q}{W^{d_i^{'}}} \right)^{e^*} \right\rfloor \bmod y \equiv \left\lfloor \left(\frac{\sum_{i=0}^{n} Z^{d^*} y^{\prod_{j=0}^{n} e_{j\neq i}^{'}}}{y^{d_i^{'} \prod_{j=0}^{n} e_{j\neq i}^{'}}} \right)^{e^*} \right\rfloor \bmod y = v$$

Step3. Perform the ***Verification Algorithm*** in section 4 and verify if the following equation holds.

$$x_0^{e_0} + x_1^{e_1} + x_2^{e_2} + \cdots + x_i^{e_i} + \cdots + x_n^{e_n} = v$$

If above equation holds, it shows that the ring signature is valid.

6. Security

The security of the presented ring signatures is based on the security of the cryptographic one-way hashing function $H(\cdot)$. To prove the security of the ring signatures, we can use Forking Lemmas. Pointcheval and Stern [12] first introduced the Forking Lemmas method in 2000 to prove the security of a class of signature schemes. The Forking Lemmas presented in paper [12] are based on a reduction technique that they called oracle replay attack. The basic idea of the Forking Lemmas can be described as follows. Assume that an attacker can forge a generic ring signature. Another attacker could obtain, by running the first attacker as a subroutine and replaying enough times the first attacker with randomly chosen hash functions, two forged ring signatures of the same message and with the same randomness. Then, using these two forged signatures, one can solve some intractable problem.

Comparing to proof procedure of paper [12], the proof using Forking Lemmas for ring signature must deal with a set of ring members instead of a unique one. With respect to above main difference, Herranz and Sáez [3] extended to the ring signatures's scenario the Forking Lemmas introduced in [12] to prove the security of the Schnorr signature scheme. The extended Forking Lemmas can also be used in proving our ring signatures.

In addition, given $k^d, k^{d^2}, \cdots, k^{(d)^{n-1}}$, an attacker can't obtain any information on k^{d^n}. This property is achieved by the intractability of decomposition of large numbers.

7. Conclusions

Consider the disadvantage that the size of the ring signature grow linearly with the size of the ring member set. We present a method to shorten the size of the ring signature in this paper. Furthermore, we propose a group-oriented ring signature scheme. In this scheme, nobody besides the designated members can verify the validity of the ring signature. The security of our ring signatures can be proved by using improved Forking Lemmas proposed by Herranz and Sáez.

References

[1] M. Jakobsson, K. Sako, R. Impagliazzo. Designated Verifier Proofs and their Applications.

Proc. of Eurocrypt'96, Springer LNCS Vol. 1070, 142-154 (1996).

[2] R. L. Rivest, A. Shamir and Y. Tauman. How to leak a secret. C. Boyd, ed. In: Proceedings of ASIACRYPT'01. Lecture Notes in Computer Science.

[3] J. Herranz, G. Sáez. Forking lemmas for ring signature scheme. T. Johansson, S. Maitra, eds. In: Proceedings of INDOCRYPT'03. Lecture Notes in Computer Science, Berlin: Springer-verlag, 2003, 2904: 266-279.

[4] A. K. Awasthi, L. Sunder. ID-based ring signature and proxy ring signature schemes from bilinear pairings.International Journal of Network security, 2007, 4(2):187-192.

[5] L. Nguyen. Accumulator from bilinear pairings and application to ID-based ring signatures and group membership revocation. A. Menezes, ed. In: Proceedings of CT-RSA 2005, Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2005, 3376: 275-292.

[6] J. K. Liu, D. S. Wong. Solutions to key exposure problem in ring signature. International Journal of Network security, 2008, 6(2):170-180.

[7] S. S. M. Chow, J. K. Liu, V. K. Wei, et al.. Ring signature without random oracles.In Proceedings of the 2006 ACM symposium on Information, Computer and Communications security, 297-302.

[8] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu. PLUTUS: SCALAble secure file sharing on untrusted storage. In Conference on File and Storage Technology (FAST'03) pp. 29-42.

[9] C. Ma, F. Ao, D. He. Certificateless Group inside Signature. Proceedings of ISADS'05 (7th International Symposium on Autonomous Decentralized Systems, Chengdu. P. R. China), pagers: 194~200.

[10] C. Ma, J. Ao. Group-oriented encryption secure against collude attack. Journal of Convergence Information Technology. 2008, 3(4): 47-53. ISSN: 1975-9320..

[11] T. –C. Wu and T. –S. Wu. Cheating detection and cheater identification in secret sharing schemes. IEE Proc. –Comput. Digit. Tech., 1995, 142(5): 367-369.

[12] D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. Journal of Cryptology, 2000, Vol. 13(3), PP. 361-396.

[13] C. Ma, J. Ao, and J. Li. Broadcast Group-oriented Encryption Secure against Chosen Ciphertext attack. Journal of Systems Engineering and Electronics, 2007, 18(4): 811-817.