ISSN 2616-5775 Vol. 4, Issue 8: 48-51, DOI: 10.25236/AJCIS.2021.040809

An efficient anonymous revocable ring signature scheme

Jia Wang[1*], Jingyuan Li[2], Ke Zhang[3]

[1]Shaanxi Normal University, Xi'an 710119, China
[2]Shaanxi Normal University, Xi'an 710119, China
[3]Shaanxi Normal University, Xi'an 710119, China
[*]Corresponding Author

Abstract: *Compared with other schemes, the ring signature scheme proposed in this paper has the characteristics of revocable anonymity. When malicious users publish false messages, we can find an effective algorithm to revoke anonymity, calculate the real signer identity in the ring signature members, and ensure the reliability and robustness of the ring signature system. Finally, the scheme is analyzed from the aspects of security and performance, The results show that the ring signature scheme with revocable anonymity in this paper is more secure, more efficient and lower operation cost.*

Keywords: *Ring signature, Anonymity, Revocable, encryption algorithm*

1. Introduction

The concept of ring signature was first proposed by Shamir et al. In cryptography in 1984. The algorithm is a signature system based on authentication. Different from other traditional signatures, the signature is a group signature composed of multiple members. The signature is associated with the public key of all members and the private key of the signer, This feature can make the generated signature anonymous and unforgeable. The receiver cannot obtain the relevant information of any real signer according to the public key and signature information. In cryptography, users' public and private keys need to be managed by a key escrow center, which is a trusted, safe and reliable organization. In order to solve the problem of key management, scholars proposed a certificateless public key system in subsequent research. Users' public keys can be guaranteed without a certificate center, which greatly improves security and reduces system overhead, More researchers' mining is obtained in the follow-up application[1].

The ring signature scheme was proposed by three cryptologists Rivest, Shamir and TauMan in 2001. In short, the significance of the ring signature technology is to realize the privacy of the transaction, that is, other participants in the blockchain system cannot trace the sender of the transaction. The thought of ring signature technology can be traced back to France in the 17th century. It is said that when the French ministers put forward their opinions to the king, in order not to let the king find out who was wearing the head, they adopted this way of ring signature. Everyone's names are arranged in the form of a ring, hiding the order, and the initiator can't find out[2,3]. In application, ring signature is the signature of a mixed group of information senders in the common signature. Only the information sender knows that the signature is sent by himself. Other members can only determine that it is sent from one of the ring signature members, but they can not determine which signer is the specific signer, and only one is the real initiator of the information signature.

As one of the most typical schemes in digital signature, ring signature application scenario is very suitable for fields requiring anonymity, such as voting system, digital currency, blockchain system, etc., and can effectively protect users' personal privacy and other sensitive information. Relevant algorithms involve expertise in bilinear pairs of cryptography, discrete logarithm problem, lattice theory and other related fields, Compared with the asymmetric encryption scheme of traditional PKI system, the computational overhead is low, but the ring signature also has its own defects. For example, with the increase of the number of ring signature members, the efficiency of signature generation and verification will also be affected[4].

2. Preparatory knowledge

2.1 Discrete logarithm problem

If for an integer *b* and a primitive root *a* of prime *p*, a unique exponent *i* can be found, so that: $b=a^i$ (mod *p*) where $i \geq 0$ and $i \leq p-1$ are true, then the exponent *i* is called the discrete logarithm of module *p* based on a of *b*. The discrete logarithm problem is that when a large prime number *p* and its original root *a* are known, if a *b* is given, it is quite difficult to calculate the value of *i*.

Arbitrarily take a, $b \in G1$, $k \in Z_q^*$, and satisfy $B = k * A$. assuming that *P*, $a * P$ and $b * P$ are known, $a * b * P$ can be calculated[6].

2.2 Bilinear mapping

A bilinear mapping is a function of one element in the third vector space generated by two elements in the vector space, and the function is linear for each parameter. Bilinear mapping can be described by quintuples (*p*, *G1*, *G2*, *GT*, *e*). *G1*, *G2* and *GT* are three prime order multiplicative cyclic groups with order *p*. a mapping relationship e defined on these three groups: $G1 \times G2$ —> *GT* meets the following properties. Bilinear mapping has the characteristics of non degeneration, computability and bilinear. The specific requirements are as follows:

(1) Bilinear: for arbitrary selection of a, $b \in Z_p$, arbitrary selection of $R,S \in G1$, there is $e(a*R, b*S)=a*b*e(R, S)$.

(2) Non degeneracy: there is $R,S \in G1$, so that $e\ (R, S) \neq 1G2$, where *1G2* is the unit element on *G2* group.

(3) Computability: there is an effective algorithm to calculate the value of $e\ (R, S)$ for any R, $S \in G1$.

2.3 Ring signature

Ring signature is named because a parameter implied in its signature forms a ring according to certain rules. In many later proposed schemes, the signature structure is not required to be ring, as long as the formation of the signature meets the characteristics of spontaneity, anonymity and group, which is also called ring signature. Suppose there are *n* users, and each user has a public key and its corresponding private key. Ring signature is a signature scheme that can realize the unconditional anonymity of the signer. It mainly consists of the following algorithms:

(1) Generate key pair: a probabilistic polynomial time (*PPT*) algorithm, the input is the security parameter K, and the output is the public key and private key. Here, it is assumed that *Gen* generates a public key and private key for each user, and the public and private keys of different users may come from different public key systems, such as *RSA* and *DL*.

(2) Signature generation: a probabilistic polynomial algorithm generates a signature *sign* for message *m* after inputting the public key $L=\{y_1\ , y_2\ ,\cdots, y_n\}$of message *m* and *n* ring members and the private key *sk* of one member, in which a parameter in the *sign* is in a ring according to certain rules.

(3) Signature verification: a deterministic algorithm. After inputting (*m*, *R*), if *R* is the ring signature of *m*, it will output "*true*", otherwise it will be "*false*".

In the ring signature system, the real identity of the signature initiator is hidden, and other participants do not know who is the real sender, which brings inconvenience to prevent the double flower problem. Key mirroring technology, that is, the same public key will produce the same *key image*, and all nodes in the system will maintain a set of *key images* that have been seen, If the *key image* of a transaction appears in the set, it is considered valid. In this way, each transaction is different through the *key image*, and the participants can easily detect and judge whether it is double flower.

3. Efficient anonymous revocable ring signature scheme

(1) Generate global parameters

The addition group $G1$ of prime order q with generator p, $G2$ is a multiplication group of order q, and there is e: $G1\times G1 \longrightarrow G2$ is a bilinear pairing function, and take H1 and H2 as one-way secure hash functions, $H1$: $\{0,1\}^* \longrightarrow G1$, $H2$: $\{0,1\} \longrightarrow Z_q^*$, randomly select the parameter j$\in Z_q^*$, set j as the main key, calculate the public key $Pub=p*s$, and disclose the global parameter $param=\{G1,G2,H1,H2,p,Pub,q\}$

(2) Key generation

The members of the ring signature send their identity ID_i to the global function. The global function calculates $IM_i=s*H1(ID_i)$, encrypts the IM_i with a symmetric encryption algorithm and sends it to the identity ID_i. The ring signature members randomly select $K_i \in Z_q^*$, and calculate $S_i=IM_i*K_i$, $Y_i=(p+H1(ID_i))*K_i$,. The private key is set to (K_i, IM_i), the public key is set to Y_i, and the public key is published for signature purposes.

(3) Generate ring signature

For the set whose ring signature members are $W=\{ID_1,ID_2, \dots ID_n\}$, assuming that the signer is ID_j, according to step (2), $Y_j=(p+H1(ID_j))*K_j$ and the private key is (K_j, IM_j). The signature generation is as follows:

Let the signature *message* be message, randomly select t_i, $m_i \in Z_q^*$, calculate $T_i=t_i*p(i\neq j, i=1,2, \dots ,n)$, $R_i=(p+H1(ID_i))*m_i$, $RK_i=m_i*Y_i$, and calculate $\mathrm{R} = \sum_{i=1}^{n} R_i * K_j$, $h_i=H2(R\|W\|T_i\|message)$.

$t_j \in Z_q^*$ is randomly selected and t is calculated $T_j = t_j * H1(ID_j) - \sum_{u=1}^{n}(T_u + Y_u * h_u)$ and $j\neq i$, then calculate $h_j=H2(R\|W\|T_j\|message)$, $RE=t_j*IM_j+h_j*S_j+ Pub * K_j * h_j$, and finally calculate the ring signature as $Sign=\{message,T_1,T_2,\dots,T_n, RK_1,RK_2,\dots, RK_n, R, RE, W\}$

(4) Verify signature

The ring signature is verified to ensure the validity and reliability of the message. The calculation process is as follows:

$h_i=H2(R||W||T_i||message)$, and $i=1,2,\dots,n$

Verification signature $e(Pub, \sum_{i=1}^{n}(T_i + Y_i * h_i)) = e(p, RE)$

If the equation holds, the signature of the *message* is valid; otherwise, the signature is invalid.

(5) Revocable anonymity

For the member signer ID_u of the ring signature W, if the signer has false behavior and needs to be tracked and revoked, it is necessary to poll the ring signature members and calculate the response to find out the real signer ID_u. The specific calculation process is as follows:

Calculate R_i for poller ID_i, $R_i = RK_i * K_i^{-1}$, then calculate the bilinear function $e(RK_i, p+H1(ID_i))=e(R_i,Y_i)$ to judge whether R_i is reliable. If it is effective and reliable, calculate $\sum_{i=1}^{n} R_i$ again to determine the final real signer, so as to achieve the purpose of anonymity of revocable ring signature.

4. Safety analysis

(1) Unforgeability

In order to prove that the private key of the real signer is safe and reliable, set the attacker to calculate a part of K_i of the user's private key from the ring signed public key Y_i by various methods, which will be a *DLP* discrete logarithm problem. Then, in the process of global parameter calculation, only part of the information of the private key is available, and the user's private key cannot be accurately inferred, so the user's private key cannot be forged to generate a signature.

(2) Revocability of signature

The algorithm proposed in this paper optimizes the use scenario of ring signature. When malicious users publish false information or maliciously destroy the normal use of signature, the revocability of signature is more important. Our scheme collects the R_i values of each signature ring member in turn through polling, It can be seen from section (5) of the scheme that K_i is unforgeable, so R_i can not be forged. When it is necessary to revoke the anonymous signature, collect all R_i and use bilinear calculation to verify the validity. If it is valid, the real signer can be determined to realize the purpose of revoking the anonymous signature.

(3) Traceable authentication: in order to verify the signature identity, the signer can provide his own relevant information to prove that he is a real signer. The signer identity can be verified through the verification formula with traceable and verifiable functions.

5. Performance analysis

Compared with the traditional elliptic curve logarithmic function calculation, the scheme in this paper has lower operation overhead and higher efficiency. Assuming that the logarithm operation and scalar multiplication operation overhead are TP and TC respectively, and the number of ring members is t, the efficiency of the scheme in this paper and the algorithm in reference [7] is analyzed and compared, as shown in Table 1.

Table 1 Performance comparison of revocable ring signature schemes

algorithm	Literature [7]	Paper scheme
Ring signature	*(5t-2)*TC*	*(4t+3)*TC*
Signature verification	*2TP+t*TC*	*2TP+t*TC*
Revoke signature	*4t*TP+2n*TC*	*4t*TP*

It can be seen from the above that the scheme in this paper has obvious advantages in the ring signature stage and the anonymity of revocation signature. There is little difference in the operation cost in the signature verification stage. The smaller the operation cost, the smaller the system overhead, and the more obvious the performance improvement.

6. Conclusion

The ring signature scheme proposed in this paper has the characteristics of anonymity, revocability and correctness. At the same time, it has an anonymous revocable ring signature scheme. When there are malicious users in the ring signature, it can track the source, locate the real signer and improve the reliability of the signature. Finally, it is analyzed and compared with literature [7], It is proved that the scheme in this paper has obvious advantages and efficiency.

References

[1] Ren Y, Guan H, Zhao Q. An efficient lattice-based linkable ring signature scheme with scalability to multiple layer[J]. Journal of Ambient Intelligence and Humanized Computing, 2021:1-10.

[2] Lin T C, Yeh T Y, Hwang M S. Cryptanalysis of an ID-based Deniable Threshold Ring Authentication[J]. International Journal of Network Security, 2019, 21(2):298-302.

[3] GAO, Wen, HU, et al. Efficient Ring Signature Scheme Without Random Oracle from Lattices[J]. Chinese Journal of Electronics, 2019.

[4] Ren Y, Danting X U, Zhang X , et al. Deletable blockchain based on threshold ring signature[J]. Journal on Communications, 2019.

[5] Samra B, FouziSemchedine. A certificateless ring signature scheme with batch verification for applications in VANET[J]. Journal of Information Security and Applications, 2020, 55(December 2020):102669.

[6] Duong D H, Tran H, Susilo W , et al. An efficient multivariate threshold ring signature scheme[J]. Computer Standards & Interfaces, 2020, 74.

[7] Liu F, Wang Q. An Identity-based Batch Verification Scheme for VANETs Based on Ring Signature with Efficient Revocation[J]. 2021.