Journal of Electronics and Information Science (2021) 6: 69-74
Clausius Scientific Press, Canada
DOI: 10.23977/jeis.2021.060211
ISSN 2371-9524

Efficient identity based ring signature scheme in prime order group

Jingyuan Li[1,a,*]

[1]*Shaanxi Normal University, Xi'an, China*
[a] *huxianfangyuan@foxmail.com*
**corresponding author*

Keywords: Prime order, identity based signature, ring signature, anonymity

Abstract: Aiming at the problem of long signature generation and verification time caused by low operation efficiency in ring signature algorithm based on composite order group, an asymmetric identity based ring signature scheme based on prime order group is proposed. The model definition and specific identity based ring signature scheme design of the proposed scheme are described, and the correctness and security of the proposed scheme are analyzed. Finally, the efficiency of the core operation part of the algorithm is explained. Compared with the correlation signature algorithm based on composite order group, the optimization has a great improvement in operation overhead and performance, and the designed scheme is unforgeable. The designed signature scheme meets the unconditional anonymity and unforgeability of ring signature.

1. Introduction

With the increasingly serious problem of network information security, hijacking transmission data, tampering and forging sender messages in important transaction scenarios such as e-commerce have greatly reduced people's trust in network information. The reliability and effectiveness of transmission data has become the focus of research. At this time, the emergence of a new technology "digital signature" has solved the pain point of information security, The basis of digital signature technology is mainly cryptography and applied mathematics. The signer has a public key and private key before sending the message, signs the message through the key pair and sends it together with the message. The receiver verifies the signature to confirm whether the data is complete and effective, which solves the risk of hijacking and tampering in previous single data transmission.

In 2001, three cryptologists, Rivest, Shamir and Tauman, first proposed the concept of ring signature. It is a simplified group signature. Any member of the ring can send message signatures in the name of the ring. The receiver verifies the ring signature. The ring signature cannot be determined to be sent by that member, but only knows that the signature comes from a member of the ring [1]. All members of the ring are equal and fair. There is no distinction between managers, nor the establishment and cancellation process of the ring. It has good anonymity. A typical application scenario of ring signature is anonymous reporting. In an organization, informants in the

organization can use the public keys of other members to sign a report together with their own public and private keys. The manager (verifier) will see that such a report is indeed initiated by someone in the organization, but the manager will not know which member initiated the report. In this way, when the authenticity of the report is ensured, the informant is hidden to avoid some adverse consequences to the informant, such as malicious retaliation. Ring signature technology still has many inherent shortcomings. For example, using a general ring signature, the signer successfully hides among a group of people and is difficult to be found. Therefore, relying solely on the ring signature, the signer can make two different remarks on the same problem and then not be found. In this way, it is likely to become the fuse of contradictions. Whether it is used for false disclosure, repeated false voting, or troublesome repeated consumption of the same currency in cryptocurrency, it is an unavoidable problem. Therefore, in order to enhance the privacy of the transaction and ensure its reliability. The privacy and security features of ring signature are widely used in practical applications. For example, the electronic voting system needs security requirements such as transparency, anonymity and public counting. The electronic voting scheme based on ring signature can solve the problems of voters' anonymity, repeated voting and public verification, so as to ensure that no person or institution can obtain the intermediate voting results before the end of voting, improve the fairness requirements of electronic counting.

Ring signature technology hides the address of the transaction initiator by mixing the signature of the transaction initiator with other bait signatures. Because ring signature technology can significantly improve the information security of platform participants, it has attracted extensive attention from people in the field of block chain and information security. Ring signature is a kind of group signature, but its special feature is that there is no uniformly managed trust center, which is anonymous for the verifier of the signature [2]. Since the concept of ring signature was proposed, it has attracted extensive research for different use scenarios. Literature [3] proves and proposes a ring signature scheme based on the standard model. Literature [4] constructs a strong ring signature algorithm, and combines the proof process for security under the standard model. Literature [5] and literature [6] propose a scheme based on complexity assumption (Diffie-Hellman) The ring signature method reduces the number of operations of bilinear pairs, and designs an anti collusion convertible ring signature, which can verify the signer's identity and ensure that other members of the ring do not generate a signature. Document [7] combines ring signature and bilinear mapping, and proves the security. Document [8] proposes a network signature, which can realize pan Chinese ring signature results through combined signature. The methods proposed in document [9] and document [10] involve bilinear pair operation, and the efficiency of bilinear pair operation will be greatly reduced with the increase of the number of members. Document [11] proposes an identity based ring signature method. In the security proof, the encryption technology of composite order bilinear group is used to achieve complete anonymity, which is less efficient than the prime order group algorithm used in this paper. According to reference [12], the 160 bit prime order group with order n and the 1024 bit composite order group can achieve the same security level, but the bilinear pair operation cost of the composite order group is much greater than that of the prime order group. Therefore, the identity based ring signature scheme based on the bilinear pair operation of the prime order group is of great significance.

Combined with the previous research methods, this paper designs an authentication based ring signature scheme of prime order group, which can construct identity based ring signature on prime order group. Compared with the bilinear pairing operation of composite order group, it greatly reduces the operation overhead and improves the efficiency of signature generation and verification. Through security analysis, it is verified that the scheme has the security characteristics of anti identity attack and unconditional anonymity. Firstly, this paper introduces the relevant knowledge needed by the authentication based ring signature scheme. Secondly, the identity based ring

signature model based on prime order group is designed, and the security definition model of the scheme is analyzed. Finally, the scheme description and security analysis and verification are carried out in detail.

2. Basic knowledge

2.1. Asymmetric pairs of prime order groups

Let (G_1, G_2, G_T) be three cyclic groups of order prime p, where $G_1= \{P_1\}$ and $G_2= \{P_2\}$ are additive groups of P_1 and P_2 respectively, and G_T is multiplicative group. Bilinear pair $e: G_1 \times G_2 \rightarrow G_T$ satisfies the characteristics of bilinear, non-degenerate and computability.

(1) Bilinear. For $P_1, Q_1 \in G_1$ and $P_2, Q_2 \in G_2$, there are the following formulas:

$e(P_1,P_2+Q_2)=e(P_1,P_2)*e(P_1,Q_2)$, $e(P_1+Q_1,P_2)=e(P_1,P_2)*e(Q_1, P_2)$

(2) Non-degenerate. $e(P_1, P_2)\neq 1 \in G_T$

(3) computability. For any $P \in G_1$ and $Q \in G_2$, there exists an effective method $e(P, Q)$

When G_1 is not equal to G_2 we call this an asymmetric bilinear mapping. For $S_1 \in G_1$ and $S_2 \in G_2$, $S_1 \sim S_2$ is used to indicate that S_1 and S_2 have the same discrete logarithm, where S_1 is based on P_1 and S_2 is based on P_2.

2.2. Complexity hypothesis

The Diffie-Hellman(DDH) hypothesis of complex judgment assumes that P_1 and P_2 are random generators of G_1 and G_2 respectively, $x_1,x_2,c \in \boldsymbol{Z_p}$, $Y_1 \in G_1$. DDH problem in G_1 is given $(P_1, x_1*P_1,x_2*P_2,P_2,Z_1=(x_1*x_2+c)*P_1)$, determine whether $c=0$ or $c \in \boldsymbol{Z_p}$.

Let β be a PPT algorithm with 0 or 1 output, and define the advantages of β to solve DBDH problems as:

$$Adv_{DBDH}=|Pr[\beta(P_1,x_1*P_1,x_2*P_1,x_3*P_1,P_2,x_1*P_2,x_2*P_2,x_3*P_2,e(P_1,P_2)^{x1*x2*x3})=1]-Pr[\beta(P_1,x_1*P_1,x_2*P_1, x_3*P_1,P_2, x_1*P_2,x_2*P_2, x_3*P_2,Y_T)=1]|$$

If for any challenger β running time is t, the advantage of ADv_{DBDH} problem is $ADv_{DBDH} \leq \varepsilon$, then the DBDH hypothesis of (ε, t) is valid.

2.3. Ring signature algorithm

With regard to ring signature, people are generally confused about the double flower problem caused by anonymity. For example, under the ring signature platform, I purchased a service from the seller. How can the platform hide my identity and prevent "double flower" and other problems to ensure the safety of the transaction?

As for the double flower problem. The "double flower problem", also known as the "double payment problem", vividly says that anyone who receives electronic money can copy it and send it arbitrarily for many times. The outside world cannot confirm whether there is repeated payment in a transaction.

In the ring signature system, the real identity of the consumer 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.

In addition, it should be pointed out that encryption with ring signature technology will increase the transaction volume and have higher requirements for performance. Ring signature is the origin of the signature of the implicit parameters of ring according to certain rules, and the main purpose of the algorithm is used to ensure that the signer can use a completely anonymous way for signing messages, the scope of the signer can choose to be anonymous or signature object group, group membership and signature receiver didn't know they contained in which members of the ring, It is also uncertain who is the real message signer in the ring members. There is no group establishment process and centralized management organization, and there is no need to join and quit the ring in advance. The formation of the ring is the ring members designated by the signer according to the needs.

Ring signature algorithm definition: in a ring with n members, the ring signature algorithm mainly includes initialization, private key generation, signature generation and signature verification.

Initialization: Run *PKG* key generator, input security parameter γ, output master key *MSK* and system public parameter *Params*.

Private key generation: Each ring member has a unique identity *ID*, and the private key Sk_{ID} is output by entering the master key *MSK*.

Signature generation: input system public parameters *Params*, identity set $\{ID_1, ID_2,\ldots,ID_n\}$, the message m and the user's private key Sk_{ID}, output the final ring signature δ.

Verify signature: input system public parameter *Params*, identity set $\{ID_1, ID_2,\ldots,ID_n\}$, message m, and ring signature result δ are verified, and *success* is output, otherwise *fail* is output.

2.4. Security requirements of ring signature

(1) Unconditional anonymity: for a given identity set $\{ID_1,ID_2,\ldots,ID_n\}$, message m and ring signature δ. Even with powerful computing ability, the challenger cannot find out the real signer with a higher probability than random guessing, that is, the highest probability of the challenger guessing the identity of the real signer is $1/n$.

(2) Unforgeability: if the challenger does not know any private key of the ring member, even if it obtains the ring signature result generated by other members through illegal means, the challenger cannot forge legitimate message signature.

(3) Good features: it can realize the unconditional anonymity of signers to protect privacy, signers can also realize the related functions of group signature, there is no administrator and third party authority in decentralization, signers can also specify their own anonymous range, etc.

3. Identity based efficient ring signature scheme

3.1. Scheme description

(1) Initialization: set the asymmetric bilinear mapping e: $G_1\times G_2\rightarrow G_T$, $G_1 = \{P_1\}$ and $G_2 = \{P_2\}$ are the additive group of P_1 and P_2, G_T is the multiplicative group. Randomly select parameters $a, v, \mu \in \mathbf{Z_p}$, with $V_2=v*P2$, $U=\mu*P2$, $\tau*P_2= V_2+a* U(\tau= v+a*\mu)$, H_0 and H_1 are the Anti-collision hash functions. PKG randomly selects$\alpha \in \mathbf{Z_p}$, $Q_1, W_1, U_1 \in G_1$, $Q_2, W_2, U_2 \in G_2$, $Q_1\sim Q_2$, $W_1\sim W_2$, $U_1\sim U_2$. Master key $MSK=\alpha*P_2$, a public parameters $Params =\{P_1, a*P_1, \tau*P_1, Q_1, W_1, U_1, e(P_1,P_2)^{\alpha}, H_0, H_1\}$.

(2) Private key generation: aiming to unique *ID*, $r \in \mathbf{Z_p}$, $K_{ID} \in \mathbf{Zp}$ is randomly selected, and the calculation process of private key is as follows: $id=H_0(ID)$, $A_{ID}=\alpha*P_2+r*V_2$, $B_{ID}=r*U$,

$C_{ID}=r*(id*Q_2+K_{ID}*W_2+U_2)$, $D_{ID}=r*P_2$. The output private key is $SK_{ID}=(A_{ID}, B_{ID}, C_{ID}, D_{ID})$ and sends the private key and set $\{K_{ID}, P2, V_2, U, Q_2, W_2, U_2\}$ to the user with the *ID*.

(3) Signature generation: set identity $set=\{ID_1, ID_2, \ldots, ID_n\}$, the signer is the π user in the identity set and its identity number is *ID*. The ring signature algorithm for generating message *m* is as follows: Suppose $i \in [n]$, calculate $id_i=H_0(ID_i)$ and $M=H_1(m, set)$.

Randomly selectedλ_i, η_i, $K_i \in \boldsymbol{Z_p}$, $K_\pi=K_{ID}$, make it meet the $\sum_{i=1}^{n}\lambda_i=0$ and $\sum_{i=1}^{n}\eta_i=\theta$.

When $i\neq\pi$, $A_i=\lambda_i*P_2+\eta_{i*}V_2$, $B_i=\eta_{i*}U$, $C_i=\eta_i*(id_i*Q_2+K_i*W_2+U_2)$, $D_i=\eta_i*P_2$

When $i=\pi$, $A_\pi=\alpha*P2+M*P2+\lambda_\pi*P_2+(\eta_\pi+\eta)$, $B_\pi=B_{ID\pi}+\eta_\pi*U=(\eta_\pi+\eta)*U$

$C_\pi=(\eta_\pi+\eta)*(id_\pi*Q_2+K_\pi*W_2+U_2)$, $D_\pi=D_{ID\pi}+\eta_\pi*P_2=(\eta_\pi+\eta)*P_2$

Generate the final message signature$\delta=\{A_i, B_i, C_i, D_i, K_i\}$, $i \in n$.

(4) Signature verification: After receiving the message *m* and ring signatureδ, the signature receiver calculates $id_i=H_0(ID_i)$ and $M=H_1(m, set)$, and randomly selects $s, c_1,\ldots,c_n \in \boldsymbol{Z_p}$ and $c_i\neq k_i$, and then calculate $T_1=s*P_1$, $T_2=a*s*P_1$, $T_3=-s*\tau*P_1+s*W_1$, $T_{4,i}=s*(id_i*Q_1+c_i*W_1+U_1)$. Finally, verify whether equation (1) is true. If it is true, the verification succeeds; otherwise, the verification fails.

$$\prod_{i=1}^{n} e(T_1, A_i) * e(T_2, B_i) * e(T_3, D_i) = e(P_1, P_2)^{\alpha s} * e(P_1, P_2)^{Ms} * \prod_{i=1}^{n}\left(\frac{e(T_{4,i}, D_i)}{e(T_1, C_i)}\right)^{\frac{1}{c_i-k_i}} \quad (1)$$

3.2. Safety analysis

(1) Correctness. The signature generated by the ring signature algorithm needs to be verified by the receiver to ensure the correctness of the generated signature. The verification process is as follows:

$$\prod_{i=1}^{n} e(T_1, A_i) * e(T_2, B_i) * e(T_3, D_i) = e(P_1, P_2)^{\alpha s} * e(P_1, P_2)^{Ms} * e(W_1, P_2)^{s*(\sum_{i=1}^{n}\eta_i+\eta)}$$

$$= e(P_1, P_2)^{\alpha s} * e(P_1, P_2)^{Ms} * \prod_{i=1}^{n}\left(\frac{e(T_{4,i}, D_i)}{e(T_1, C_i)}\right)^{\frac{1}{c_i-k_i}}$$

(2) Unforgeability. In the scheme where the ring signature member is *n*, it is assumed that the Challenger inputs security parameters γ, public parameter *params* is obtained through the initialization algorithm, and then the query key generation algorithm can be initiated in polynomial time. Enter your own unique identity *ID* and public parameters to obtain the returned private key SK_{ID}. Enter the identity set $\{ID_1, ID_2\ldots ID_n\}$ and message *m* to obtain the ring signature result of an identity base δ。 The Challenger finally enters the ring signature δ, $\{ID_1, ID_2\ldots ID_n\}$ and message *m* are verified. Since the identity set and message have not appeared before, according to the complexity assumption in Chapter 1.2, the probability of the Challenger passing the verification is ε, this is negligible.

4. Performance analysis

For the comparison between the prime order group signature scheme proposed in this paper and the ring signature scheme based on composite order group in reference [13], we use Intel i7 processor, 8g memory and Linux operating system, install *PBC* library and *GMP* library, call basic cryptography related operation functions, and write the algorithm implementation part of ring signature in *C* language for testing.

Table 1: Comparison of calculated cost for our proposals and literature [13].

Scheme	Initial (ms)	Generate key (ms)	Signature (ms)	Verification (ms)
Literature[13]	850	386	58321	65235
Our proposals	310	60	3800	1320

When the number of ring members n is set to 100, the calculation cost of the comparison document [13] and the scheme in this paper is shown in Table 1. It can be seen that the calculation cost of prime order group is much less than that of composite order group.

5. Conclusions

In this paper, a ring signature scheme based on bilinear mapping function of prime order group for authentication is proposed. It has unconditional anonymity and signature verifiability to the signer, has advantages in protecting the signer's personal privacy, improves the security of message signature, and solves the problem of large operation consumption based on composite order group, With the linear growth of ring signature members, the advantages are more obvious.

References

[1]RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret[A]. Proc ASIACRYPT'0l[C].Springer-Verlag,2001.552-565.

[2]CHAUMD, HEYST VE. Group sjgnatures[A].nDc CROCRYPrr'9l[C].Springer.Verlag,1991.257-265.

[3]SHACHAMH, WATERS B. Efficient ring signatures with-out random oracles[C].1 0th International Conference on Practice and Theory in Public-Key Cryptography, 2007. 66-1 80.

[4]BENDER A, KATZ J, MORSELLI R. Ring signatures: Stronger definitions, and constructions without random oracles[J].Journal of Cryptology, 2009, 22: 1 1 4-1 38.

[5]SHIM K. An efficient ring signature scheme from pairings[J].Information Sciences, 201 5, 300: 63-69.

[6]YEON H, YOUNG C, SOOK C, et al. Collusion-resistant convertible ring signature schemes[J].Science China Information Sciences, 201 5, 58: 01 21 08-01 21 23.

[7]ZHANG X, LIU Z, WANG X. Ring signature scheme from multi-linear maps in the standard model[C].1 0th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 201 5: 859-864.

[8]BOYEN X. Unconditionally anonymous ring and mesh signatures[J].Journal of Cryptology, 201 6, 29: 729-774.

[9]ZHANG F, KIM K.ID-based blind signature and ring sig-nature from pairings [J].Advances in Cryptology-ASIA-CRYPT.2002, LNCS, 2501 : 533-547.

[10]HERRANZ J, SAEZ G. New identity-based ring signature schemes [C].6th International Conference on Information and Communications Security, 2004, LNCS, 3269: 27-29.

[11]FREEMAN D M. Converting pairing-based cryptosystems from composite-order groups to prime-order groups[C]//Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2010: 44-61.

[12]FREEMAN D M. Converting pairing-based cryptosystems from composite-order groups to prime-order groups[C]//Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2010: 44-61.

[13]AU M H, LIU J K, SUSILO W, et al. Realizing fully secure unrestricted ID-based ring signature in the standard model based on HIBE[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(12): 1909-1922.