Improvement And Research of Group Signature Scheme Based on Chinese Remainder Theorem

Ai-qin QI[1, a] Yong-jun SHEN[2,b]

[1]School of Mathematics and Computer Science Institute Northwest University For Nationalities Lanzhou, China

[2]School of Information Science&Engineering Lanzhou University Lanzhou, China

[a]qi-133@163.com [b]shenyj@lzu.edu.cn

Keywords: group signature,chinese remainder theorem , not relevance, RSA

Abstract. Based on the analysis of the group signature scheme based on the Chinese remainder theorem, it is found that the existing schemes have shortcomings in anti fake, anti- frame, anti - joint attacks and non - connection. Tthis paper puts forward an improved group signature scheme that apply RSA signature algorithm.The group center participates in the group signature generation, verification and open process. Under the assumption of RSA and discrete logarithm problem, it is proved that the new scheme has good characteristics with anonymity, not relevance, anti-counterfeiting character, trace ability and so on. Compared to other relevant schemes it is more robust and secure.

Introduction

Group signature initially was proposed by Chaum and van Heyst [1] in 1991, any of the group members executes an anonymous signature operation on behalf of the group and the verifier can confirm the digital signature but not determine which member's signature that is . When a dispute occurs, the signer can be identified by the association of a trusted institution or the group members.

In this paper, we propose a signature scheme based on chinese remainder theorem, which meets all the the security requirements of group signature such as anonymity, not relevance, anti-counterfeiting character, trace ability and so on and also has the forward security feature. Compared with other schemes, the proposed scheme is more efficient and more secure.

The rest of the paper is organized as follows: Section 2 discusses related work. Section 3 presents the proposed signature scheme . Section 4 analyzes the security and the performance of the proposed scheme. Section 5 finally concludes the paper.

Related work

Generally speaking, a group signature scheme includes the group, group members, the signature verifier and a trusted authority. Because the group members always increase or withdraw dynamically, the application of group signature in the practical scenario is often dynamic. Therefore, how to design efficient dynamic group signature becomes many scholars' research goals.

Camenish et al. proposed a group signature scheme [2] · which is suitable for large groups. The group signature scheme proposed by Ateniese et al. [3] can resist the attack of the attackers, but can not meet other requiremets of group signature .

In 2003, Shangping Wang et.al[4] studied the revocation and deletion of the group members. Zewen Chen et al.[5] proposed a group signature scheme based on Chinese remainder theorem in 2004, which could safely and efficiently increase or undo the group members without changing the signature key of the other group members . In 2006 , Hu et al. [6] analysised the literature [5] and pointed out that the scheme could not resist the forgery attack and not have the unlinkability and not effectively revoke members etc. In 2007, Feng He Wang et al [7] found that the scheme [5] under the combined attack can forge the group signature of any member and can not resist framing attack and can fake group

members to produce signatures and other security problems.Then they improved the scheme by the Schnorr Signature method, but the scheme does not meet the non connection of group signature. In 2009, Steven et al [8] began to use RSA common modulus attack method to solve relevance and the problems of adding or deleting group members and resistance of forged signatures in the group center.

In 2012, Liwei Tang et al. [9] proposed a group blind scheme based on Chinese remainder theorem .Through the analysis we found that the scheme does not satisfy the group signature in a non connection. In this paper, we propose a signature scheme based on chinese remainder theorem, which meets all the the security requirements of group signature such as anonymity, not relevance, anti-counterfeiting character, trace ability and so on and also has the forward security feature. Compared with other schemes, the proposed scheme is more efficient and more secure.

The proposed scheme

The group signature scheme we propose includes the group center, the group manager, group members and the user. Group center initializes the system ,establishes the signature system and generates the public key for the group members. Group manager plays a role of a trusted body, when the dispute occures it will open the valid group signature to determine the identity of the signer. Group members and the group center sign the message, the user verify the signature. The specific algorithm is described as follows:

Establishment .Step 1: The group center selects two large prime numbers p, q and calculates n = p*q, n is the modulus of the public key and the private key, φ(n)is Euler function andφ(n)=(p-1)(q-1). The group center randomly selects a number of e which meets gcd(e, φ(n))=1 and computes a number of d that meets ed≡1(modφ(n)), (e,n) is the public key,d is the private key. The group center announces a hash function h for the later use.Step 2:Every group member U_i selects two large prime numbers m_i,q_i and calculates $n_i = m_i*q_i$, n_i is the modulus of the group memer 's public key and the private key. The group member randomly selects a number $x_{i,0} \in Zni^*$ and computes $x_{i,0}y_i \equiv 1(\mathrm{mod}\varphi(ni))$, y_i is the public key, $x_{i,0}$ is the private key. The group member U_i selects ID_i as the identity of group member U_i and sends (y_i， n_i， ID_i)to the group center.Step 3:When receiving (y_i， n_i， ID_i),the group center saves the information and selects a number of p_i which meets $n_i > p_i > y_i$ and computes $Z_i = p_i^{y_i} \mathrm{mod}(n_i)$. Then the group center sends Z_i to the group member U_i .The group member U_i uses $x_{i,0}$ to decrypt Z_i and gets p_i.Step 4:Supposing there are k group numbers in the group center ,the group center use chinese remainder theorem to get the answer $c = \sum_{i=1}^{k} y_i M_i k_i \bmod M$ ($M = \prod_{i=1}^{k} p_i$, $M_i = \frac{M}{p_i}, 1 \le i \le k$, $k_i = M_i^{-1} \bmod p_i, 1 \le i \le k$) ,according to the equation $c \equiv y_i (\mathrm{mod}\ p_i)$ (i = 1， …， k， gcd(p_i， p_j) = 1(i ≠ j)). The group center announces the public key (n , e) and saves the privete key d and the answer c.

Increase in members. Supposing there are k group numbers in the group center , the user U_{k+1} wants to join the group. U_{k+1} selects two large prime numbers m_{k+1},q_{k+1} and calculates $n_{k+1} = m_{k+1}q_{k+1.}$, $\varphi(n_{k+1})=p(m_{k+1}-1)*(q_{k+1}-1)$. User U_{k+1} randomly selects a number $x_{k+1,0} \in Zni^*$ and computes $x_{k+1,0}y_{k+1} \equiv 1(\mathrm{mod}\varphi(n_{k+1}))$, y_{k+1} is the public key, $x_{k+1,0}$ is the private key. The user U_{k+1} sends (y_{k+1} ,n_{k+1} , ID_{k+1}) to the group center. Group center saves (y_{k+1} ,n_{k+1} , ID_{k+1}) ,selects a number p_{k+1} which meets $n_{k+1} > p_{k+1} > y_{k+1,}$ ($p_{k+1} \neq p_i$,i =1 , 2 , … , k) and computes $z_{k+1} = (p_{k+1})^{yk+1} \mathrm{mod}(n_{k+1})$. Then the group center sends z_{k+1} to user U_{k+1} .User U_{k+1} uses $x_{k+1,0}$ to decrypt z_{k+1} and gets $p_{k+1.}$ The user U_{k+1} is now a member of the group.

Revocation of members . In order to revoke the group members ,the group center sets y_i as another random number y_i ' and recalculates c ,then replaces the answer c and saves it. In this process the public key (n , e) does not change and this reduces the impact of network traffic.

Refreshment of keys .Supposing the j-th time period ($1 \le j \le T$), the private key of the group members U_i is $x_{i,j}$ and the private key of the j+1 time can be deduced by the equation $x_{i,j+1} = (x_{i,j}2^l) \bmod n_i$, l is the length of the private key. If j = T, the group member output j+1 time of the private key as empty. When the private key is generated in the second j+1 time period, the private key of the first j time period is immediately erased.

Generation of signature .In this scheme, the group signature generation requires the group center to participate. Given the time j, the group member U_i needs to sign the message m ,the specific process is as follows:Step1:The group center selects a random r ,computes $m'=h(m)\, r^{y_{i,j}} \bmod (n_i)$ and sends it to the member U_i ,the member U_i gets $s_i'=(m')^{x_{i,j}} \bmod (n_i)= h(m)^{x_{i,j}} r$ by the private key $x_{i,j}$ and sends (m', s_i', p_i) to the group center.Step2:The group center computes $s_i=s_i' r^{-1} \bmod (n_i) = h(m)^{x_{i,j}}$ and judges if h(m) equals $s_i^{y_i} \pmod{n_i}$ by the equation $y_i = c \pmod{p_i}$. Then it selects a random $\alpha_i \in Z_n^*$ which meets $\alpha_i h(s_i' \| r) < n$, computes $r1 = p_i + \alpha_i h(s_i' \| r) \pmod n$; $r2 = (\alpha_i h(s_i' \| r))^e \pmod n$; $C = (h(s_i' \| s_i \| r1 \| r2))^d \pmod n$. The group center sends $(j, s_i', s_i, C, r1, r2)$ to the user and this is the final group signature .

Signature verification .Supposing a user A wants to verify the signature $(j, s_i', s_i, C, r1, r2)$, he gets the public key (n , e) and judges if C^e equals $h(s_i' \| s_i \| r1 \| r2) \pmod n$. If the equation holds the signature is correct, otherwise the signature is wrong.

Signature open .The group center verifies the signature $(j, s_i', s_i, C, r1, r2)$ and computes $p_i = r1 - r2^d \pmod n$, $y_i = c \pmod{p_i}$. The group center can find the member U_i by y_i. If the member denies , the group center can judge if h(m) equals $s_i^{y_i} \pmod{n_i}$ to identify members.

Security and performance analysis

Our scheme has the nature of anonymity because only group center know the membership information, and we can not get any member information from the signature (j, si', S_i, C, R1, R2) ,the security is based on the large integer factorization problem and RSA problem.

Elements si', S_i , R1 , R2 and C values will change each time from the siganture (j, si', S_i, C, R1, R2), so the two different signatures of the same member do not leak any member information, this meets not relevance. The group center can use its own private key to open the signature to get the identity information of the group members, which can satisfy the trace ability.

In our scheme, the group members and the group center need unite to generate the group signature . At the same time, because only the group members know their private key information, other people cannot forged the signature of the group members, unless they can solve the large integer factorization problem. So the scheme can resist the forgery attack.

If the attacker has access to the private key $x_{i,j}$ of the group member U_i in the jth stage, he wants to find the private key before $x_{i,j}$, $(1 \le j \le T)$ and forges the signature before j stage. But according to the private key update algorithm, the calculation is not feasible if we do not know the case of n_i decomposition . Therefore even if the signature key is leaked, the time period of the signature is still valid, which ensures the forward security of the proposed scheme.

Based on the above analysis , our scheme has good characteristics with anonymity, not relevance, anti-counterfeiting character, trace ability and so on. It also has the nature of blind signature. Our scheme is more secure .

Compared with the previous scheme, in the signature generation process our scheme only needs hash operations and multiplication, but these costs enable the scheme to satisfy the not relevance, shorten the length of group public key which does not change during adding or deleting group members. At the stage of verifying signature, the scheme only uses one hash and one exponentiation, which

simplies the operation. And the new scheme has the nature of forward security and blind signature, and these properties in other schemes are not available.

Conclusions

In this paper, We propose an improved group signature scheme and analyze the safety and efficiency. The results show that the scheme meet the anonymity, not relevance, anti-counterfeiting character, trace ability and so on. At the same time, the key updating algarithm is added, and the forward security is introduced into the new group signature scheme, which increases the security of the new scheme.

AcknowledgEment

The work is supported by Scientific and technological projects for Central colleges and universities(31920150079).

References

[1] Chaum D, Hey stVE.Group signatures[C] ∥Procof EUROCRYPT′91.Brighto n:Spring erVerlag ,1991 :257-265.

[2] Camenish J, Stadle r M .Efficient group signatures for large groups[C] ∥Procof the CRYPTO′97. Heidelberg :Springe r-Ve rlag , 1997:410-424 .

[3] Ateniese G , Camenisch J , Joy e M , et al .A practical and provably secure coalition-resistant group signature scheme [C] ∥ Adv ances in Cry pto-CRYPTO 2000 .H erdelberg :S pringer-Ver lag , 2000 :2 550-2 700 .

[4] Shangping Wang, Yuming Wang, "A New Solution Scheme for the Member Deletion Problem in Group Signature," Journal of software, 14(11):1911-1917,2003

[5] Zewen Chen, Longyun Zhang, "A group signature scheme based on Chinese remainder theorem," Journal of Electronics.vol. 7, no. 32, pp.1062-1065, 2004.

[6] Bin Hu, Ronghua Shi and Yue Lou, "An improved group signature scheme based on Chinese remainder theorem." Computer engineering and Applications., vol.24, pp.115–116, 2006..

[7 Fenghe Wang, Yupu Hu, and Chunxiao Wang, "Attack and improvement of a group signature scheme based on Chinese remainder theorem," Journal of electronics and information, vol. 29, no. 1, pp.182-184, 2007.

[8] Guohua Cui, Yongjune Geng and et.al, "An improved signature scheme based on Chinese remainder theorem group" Journal of Huazhong University of Science and Technology. vol. 37, no. 6, pp.1-3, 2009.

[9] Liwei Tang, Weizhang Du, "Forward secure group blind signature scheme based on Chinese remainde rtheorem," Journal of computer applications, no. 32, pp.53-55, 2012.