Journal of Computer and Communications, 2014, 2, 39-42
Published Online March 2014 in SciRes. http://www.scirp.org/journal/jcc
http://dx.doi.org/10.4236/jcc.2014.24006

A Novel Scheme for Deleting Group Members

Junping Yao, Xinshe Li, Junchun Ma

Xi'an High-Tech Institute, Xi'an, China
Email: junpingy200225@163.com

Received November 2013

Abstract

Deleting group members safely and efficiently has been a hot research issue in the field of the group signature. Some resolutions have been proposed by cryptography experts, but in some way, problems like loophole and low efficiency have been confusing us in the research. To solve the problem, the writers try to give a new secret key updating algorithm based on improving Wang Shangping's group members deleting scheme, and analyze the safety and efficiency of implementation systematically in the paper.

Keywords

Group Signature; Secret Feature Key; Public Feature Key; Group Manager

1. Introduction

Group signature [1] has drawn much attention in academy of cryptography since it was proposed in 1991; group signature scheme [2] proposed by Camenisch Stadler in 1997 was an important progress in group signature analysis. The scheme used knowledge signature concept (especially SKROOTLOG signature and SKLOGLOG signature). E. Bresson and J. Stern proposed a solution scheme of group members deleting problem in 2001 [3], which was developed from Camenisch Stadler group signature scheme. It must be proved that public key z must not be in the list of deleting public keys with zero-knowledge when signers signed on the message M. The number of evidence in signature grows in a linear way with the growth of number of the deleted objects, so it is not suitable for large groups. Wang Shangping proposed a new solution to group members deleting problem in the Camenisch Stadler group signature scheme [4]. When new members join in the group or the existing members are deleted from the group, group manager calculates a new group feature key U_G and update operator U, then member's secret characteristics key gets updates. The group public key has nothing to do with the number of group members. Literature [5,6] analyzes the mathematical principle of parameters selection in the group signature members deleting scheme [4], and it proves that Wang Shangping's scheme can't delete members in an actual way but proving process is not given.

Inspired by some research results such as group signature [1,7], blind signature [8,9], authentication encryption signature [10,11] and proxy signature, based on Wang Shangping's scheme, by converting secret feature key update operator public into secret when members are registered or deleted, the update process was executed by group manager instead of group members, a new group member's deleting scheme is proposed, in which secret feature key of group members will not change with members' deleting or joining.

How to cite this paper: Yao, J.P., Li, X.S. and Ma, J.C. (2014) A Novel Scheme for Deleting Group Members. *Journal of Computer and Communications*, **2**, 39-42. http://dx.doi.org/10.4236/jcc.2014.24006

2. A Novel Scheme

2.1. Foundation

Group manager is just the same as it in Camenisch-Stadler scheme in system setup phase, the difference is that we add a RSA public parameter e whose module is n, and e must coprime with $\phi(n)$. Group public key is $Y=(n,e,e_1,e_2,f_1,f_2,G,g,h,y_R)$, group manager public key is $y_R:=h^w$, prime factor of $\frac{1}{w}$ and n is group manager's secret key.

The process of getting members certificate is completely the same with member's registering in Camenisch Stadler's scheme. And we can assume group containing $m-1$ members $\{G_1,G_2,\cdots G_{m-1}\}$ in the initial establishment. Group public feature key is $U_G:=z_{G_1}z_{G_2}\cdots z_{G_{m-1}}z'$, the secret feature key of member G_i is $U_{G_i}=(z_{G_1}z_{G_2}\cdots z_{G_{i-1}}z_{G_{i+1}}\cdots z_{G_{m-1}}z')^{\frac{1}{e}}$, where z_{G_i} is the public key of group member $(1\le i\le m-1)$, and $z'\in{}_R G$, $k:=1$.

2.2. Members' Joining In

If Alice wants to join the group, she can establish her member certificate first, just as registering in Camenisch Stadler's scheme [3]. Set Alice is the m-th member G_m. Set group current public feature key $U_G:=z_{G_1}z_{G_2}\cdots z_{G_{m-1}}z'$, which z_{G_i} is public key of the group members $(1\le i\le m-1)$, and $z'\in{}_R G$. The group manager calculates the following value:

1) The new group public feature key and new value of k:

$$U_G:=z_{G_1}z_{G_2}\cdots z_{G_{m-1}}z_{G_m}z'' \quad k:=k+1$$

in which $z''\in{}_R G$.

2) Group members' secret feature key update factor:

$$U:=(\frac{z_{G_m}z''}{z'})^{\frac{1}{e^k}}$$

3) The secret feature key of the new member G_m (Alice):

$$U_{G_m}:=(z_{G_1}z_{G_2}\cdots z_{G_{m-1}}z'')^{\frac{1}{e^k}}$$

4) The secret feature key of other group members:

$$U_{G_i}:=(U_{G_i})^{\frac{1}{e}}U$$

while the group manager makes a new group public feature key U_G and the new value of k public, keeps update factor U secret, and sends a secret key U_G to G_m (Alice) privately. A new member G_m verifies $(U_{G_m})^{e^k}z_{G_m}=U_G$ to judge whether the secret feature key U_G sent by group manager is correct. Then, group manager calculates the secret feature key of other legal members $G_i(1\le i\le m-1)$ except G_m, and sends the secret feature key to group members confidentially, members verifies $(U_{G_i})^{e^k}z_{G_I}:=U_G$ to judge whether the secret feature key U_G sent by group manager is correct.

2.3. Members' Deleting

Members' deleting is an inverse process of members' joining in. The following will explain how a group manager deletes the member G_j. Group manager deletes its public key z_{G_j} which is in group public feature key U_G, and changes the random number, then releases the new group public feature key U_G and new value of k, and calculates the secret feature key update factor U and secret feature key of other group members, thus, we can generate a valid group signature after deleting G_j.

Set current group public feature key as:

$$U_G:=z_{G_1}z_{G_2}\cdots z_{G_m}z'$$

in which $z' \in_R G$. In order to delete group member G_j, group manager calculates the following value:

1) The new group public feature key and new value of k

$$U_G := U_G \frac{z''}{z_{G_j} z'} = z_{G_1} \cdots z_{G_{j-1}} z_{G_{j+1}} \cdots z_{G_m} z''$$

in which $z'' \in_R G$

$$k := k+1$$

2) The secret feature key update factor of group members

$$U := \left(\frac{z''}{z_{G_j} z'}\right)^{\frac{1}{e^k}}$$

3) The secret feature key of $G_i (i \neq j)$

$$U_{G_i} := (U_{G_i})^{\frac{1}{e}} U$$

Group manager makes a new group public feature key U_G and new value of k public, keeps update factor U secret, and sends secret key privately to $G_i (i \neq j)$. Group member $G_i (i \neq j)$ verifies $(U_{G_i})^{e^k} z_{G_i} := U_G$ to judge whether the secret feature key U_{G_m} sent by group manager is correct.

2.4. Signature Process

We can suppose that group has the legal members $G_1, \cdots, G_m$, group public feature key $U_G = z_{G_1} \cdots z_{G_m} z'', z'' \in_R G$, group member $G_i (1 \le i \le m)$ signs on message M on the behalf of the group. G_i calculates

$$\tilde{z} := h^r z_{G_i} (r \in_R z_n{}^*)$$

$$d := y_R^r$$

$$A = U_{G_i} g^r$$

$$B = h^r g^{re^k}$$

$$V_1 := SKROOTREP[\alpha, \beta : \tilde{z} = h^\alpha g^{\beta^{e_1}}](M)$$

$$V_2 := SKROOTREP[\gamma, \delta : \tilde{z} = h^\gamma g^{\delta^{e_2}}](M)$$

$$V_3 := SKREP[\varepsilon, \xi : d = y_R^\varepsilon \wedge \tilde{z} = h^\varepsilon g^\xi \wedge B = h^\varepsilon g^{\varepsilon e^k}](M)$$

The signature that member G_i signing on message M is $(\tilde{z}, d, A, B, V_1, V_2, V_3)$, where the calculating process of $\tilde{z}, d, V_1$ and V_2 is the same as it is in Camenisch Stadler's scheme. We add A and B, where A contains secret feature key U_{G_i} of member G_i, B is set to verify the correctness of A, proving process for the correctness of B is added in V_3.

3. Analysis of the Scheme

3.1. Verificating and Opening the Signature

When we verify the correctness of the signature, we just need to add verifying the establishment of $\frac{U_G}{A^{e^k}} B = \tilde{z}$ in proving process, because the establishment of $\frac{U_G}{A^{e^k}} B = \tilde{z}$ ensures the legality of signer's secret feature key U_{G_i} .The opening process is the same as it is in Camenisch Stadler's scheme.

3.2. Security and Efficiency Analysis of the Scheme

1) The calculation method of group public feature key is the same as it is in Wang Shangping's scheme, but

the legal members' secret feature key is calculated by group manager, and then sent to members confidentially.

2) The deleted members cannot obtain the formula to update his secret feature key, even if conspiring with other members, it is impossible to forge signature that can be admitted.

3) It inherits the fine features of the Camenisch Stadler's scheme; furthermore, it can delete group members effectively.

4) It needs to calculate the new value of k when deleting or adding member, especially when we determine the formula of new member's secret feature key according to the current value of k when adding a new member. These lower the signature and verification efficiency, but the zero-knowledge proof process is eliminated compared to Bresson-Stern scheme [3]. In other words, the improvement scheme is safe, reliable, and high efficient.

4. Conclusion

The scheme of deleting members proposed by Wang Shangping is proved that it cannot actually delete members. And for solving this problem, this paper changes secret feature key update factor into confidential in the member register and deleting process, and the update work for group members' secret feature key is executed by group manager instead of members, in this way, an improvement of secret feature key update algorithm is proposed, and group members' secret feature key does not change with deleting or adding members.

References

[1] Chaum, D. and Van Heyst, E. (1991) Group Signatures. In: *Advances in Cryptology EUROCRYPT*'91. *LNCS* 547, Springer-Verlag, Berlin, 257-265.

[2] Camenisch, J. and Stadler, M. (1997) Effient Group Signature Schemes for Large Groups. *Proceedings of CRYPT*'97, *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, 410-424.

[3] Bresson, E. and Stern, J. (1999) Efficient Revocation in Group Signature. In: Kim, K., Ed., *PKC*2001, *LNCS*1992, Springer-Verlag, Berlin, 190-206.

[4] Wang, S.P., Wang, Y.M. and Wang, X. (2003) A New Solution Scheme for the Member Deletion Problem in Group Signature by Use of Renew Operator. *Journal of Software*, **14**, 1911-1917.

[5] Li, X.S. and Hu, Y.P. (2008) Analysis and Improvement for a Group Signature Member Deletion Scheme. *Journal of Xidian University*, **35**, 478-482.

[6] Huang, Z.J. and Lin, X.Z. (2005) A Group Member Deletion Scheme Cryptanalysis. *Journal of Software*, **16**.

[7] Ateniese, G. and Medeiros, B.D. (2003) Efficient Group Signatures without Trapdoors. In: *Advances of ASIACRYPT*'03. *LNCS*2894, Springer-Verlag, Berlin, 246-268.

[8] Chow, S.S.M. (2009) Blind Signature and Ring Signature Schemes: Rehabilitation and Attack. *Computer Standards & Interfaces*, **31**, 707-712.

[9] Zhang, J.H., Chen, H. and Qin, G. (2009) Cryptoanalysis of Certificateless Partially Blind Signature and Proxy Blind Signature Scheme. *Proceedings of the* 2009 2*nd International Congress on Image and Signal Processing* (*CISP*), 5.

[10] Zhao, W., Lin, C. and Ye, D.F. (2009) Provably Secure Convertible Nominative Signature Scheme. *Information Security and Cryptology* 4*th International Conference*, Revised Selected Papers, 23-40.

[11] Zhang, J.H. and Qin, G. (2008) On the Security of Group Signature Scheme and Designated Verifier Signature Scheme. 2008 *International Conference on Networking*, *Architecture*, *and Storage* (NAS), June 2008, 351-358.