Memoirs of the Faculty of Engineering, Okayama University, Vol.35, Nos.1&2, pp.207-212, March 2001

A Group Signature Scheme with Easy Membership Canceling

Toru NAKANISHI* and Toru FUJIWARA**

(Received December 22, 2000)

In the group signature scheme with a trusted party, a verifier can determine whether or not a signature is made by a member of the group, but cannot identify the member who signed the signature. In case of dispute later on, the signer can be identified by the trusted party. However, for efficient group signature schemes proposed so far, removing a member from the group can be not efficiently performed. In this paper, a group signature scheme with an easy membership canceling is proposed. By sending a request to use a resource together with the group signature on it to the manager of the resource, the manager can control anonymous accesses to the resource. In such an application, the proposed group signature scheme is suitable for canceling of the access privilege.

1. INTRODUCTION

The group signature scheme with a trusted party [1] is the signature scheme satisfying the following conditions:

1. Only members of a group can sign messages.
2. Anyone can determine whether or not a given signature is a valid signature of a member in the group. But anyone except for the trusted party (and the signer) cannot identify the member who signed from the signature, and cannot determine whether or not two signatures are made by the same signer.
3. In case of dispute later on, the signer of a signature can be identified by the trusted party.

As an application of the group signature scheme, this paper deals with the access control for the anonymous accesses to resources. When a user sends a request to use a resource to the manager of the resource,

* Department of Communication Network Engineering

** Department of Informatics and Mathematical Science, Osaka University

the user sends it together with the group signature on it to the manager. Then, the condition 1 enables the manager to check that an access is issued by an approved member. Owing to the condition 2, the accesses are anonymous. The condition 3 enables the manager to identify a member who made an illegal access with the help of the trusted party.

The group signature schemes are first proposed by Chaum et al. in [1], and some improved schemes are proposed in [2, 3], but these schemes have the following drawbacks: The length of the public key of a group depends on the size of group, and the public key must be modified in adding a new member to the group. Recently, an efficient group signature scheme which overcomes the problems is proposed in [4]. The idea of the scheme is that the signature on a message is a non-interactive proof of knowing a membership certificate issued by a trusted party and that the signature depends on the message. Thus, since the public key of the group is only a verification key of the certificate, the public key is invariable even if a new member is added. But, the scheme does not deal with canceling the membership of a member, while the application to the access control requires the rejection of the further access by a user whose access privilege is canceled. A simple solution is changing the public key of the group, but unrelated users have loads.

In this paper, a group signature scheme where canceling the membership of a member is easily performed is proposed. In the scheme, the loads of unrelated users are not required when canceling is performed.

2. PRELIMINARIES

The proposed group signature scheme is an extension of the scheme in [4]. Thus, notations and primitives in [4] are reviewed. The empty string is denoted as $\tilde{0}$. For a set A, $a \in_R A$ means that a is chosen at random from A. For an integer q, let Z_q be the ring of integers modulo q and let Z_q^* be the multiplicative group modulo q. Let $G = \langle g \rangle$ be a cyclic group of order n, where g is a generator of G. For example, as G, a subgroup of order n of $Z_r^* = \{1, \ldots, r-1\}$ with $n|r-1$ can be used. The discrete logarithm of $y \in G$ to the base g is the smallest positive integer x satisfying $g^x = y$. An e-th root of the discrete logarithm of $y \in G$ to the base g is an integer x satisfying $g^{(x^e)} = y$, if such an x exists. Note that if the factorization of n is unknown, computing e-th roots in Z_n^* is assumed to be infeasible as well as noted in [4].

As a primitive to prove the knowledge of secret values without leaking any useful information on the secret, the signature of the knowledge is used. That is a non-interactive proof system and a signature on a message, that is, only one who knows secret values satisfying a statement can compute the signature, a verifier cannot obtain any useful information about the secret values, and an adversary cannot compute an unsigned message by using signatures of messages chosen by the adversary. One of the signatures of the knowledge is the signature on a message m of an entity knowing the discrete logarithm x of y, which is basically a Schnorr signature. The signatures of the knowledge of values satisfying more complex statement can be also constructed as shown in [4]. Three types of signatures of the knowledge are used to construct the proposed group signature scheme. The first one is the signature of the knowledge of representations of $y_1, \ldots, y_w$ to the

bases $g_1, \ldots, g_v$ on message m, and it is denoted as

$$SKREP[(\alpha_1, \ldots, \alpha_u) : (y_1 = \prod_{j=1}^{l_1} g_{b_{1j}}^{\alpha_{e_{1j}}}) \wedge \cdots \wedge (y_w = \prod_{j=1}^{l_w} g_{b_{wj}}^{\alpha_{e_{wj}}})](m),$$

where constants $l_i \in \{1, \ldots v\}$ indicate the number of bases on representation of y_i, the indices $e_{ij} \in \{1, \ldots, u\}$ refer to the elements $\alpha_1, \ldots, \alpha_u$ and the indices $b_{ij} \in \{1, \ldots, v\}$ refer to the elements $g_1, \ldots, g_v$. For example, $SKREP[(\alpha, \beta) : y = g^\alpha \wedge z = g^\beta h^\alpha](m)$ is the signature on m of an entity knowing the discrete logarithm of y to the base g and a representation of z to the bases g and h, where the h-part of this representation equals the discrete logarithm of y to the base g. The second type is the signature of the knowledge of the e-th root of the discrete logarithm of z to the base g on m, and is denoted as

$$E - SKROOTLOG[\beta : z = g^{\beta^e}](m).$$

The third type is the signature of the knowledge of the e-th root of the g-part of a representation of v to the bases h and g on m, and is denoted as

$$E - SKROOTREP[(\gamma, \delta) : v = h^\gamma g^{\delta^e}](m).$$

For the constructions of these signatures, refer to [4]. Note that $E - SKROOTLOG$ and $E - SKROOTREP$ are efficient if e is small.

3. A GROUP SIGNATURE SCHEME WITH EASY MEMBERSHIP CANCELING

In this section, a group signature scheme where canceling the membership is easily performed is presented. The participants are members in a group, verifiers who verify the signatures of the members, a group manager who manages the membership of members in a group, and a trustee who identifies the signer from a signature and enables canceling of the membership. In [4], the group manager not only manages the membership but identifies the signer. But, in this paper, the power is distributed to the group manager and the trustee. The proposed scheme consists of six parts, system setup, entry into group, signing, verification, identifying signer from signature and canceling of membership. In the system setup, the setups of keys of participants are performed. When a person enters the group, the entry into group is used. In the signing, a member in the group computes his group signature. In case of dispute later on, the trustee identifies the signer in the identifying signer from signature, and the trustee enables canceling the membership of a member in the canceling of membership.

System setup: The group manager computes the followings:

- An RSA modulus n and two public exponent $e_1, e_2 > 1$,
- Two integers $f_1, f_2 > 1$,
- A cyclic group $G = \langle g \rangle$ of order n in which computing discrete logarithm the base g cannot be computed,

- An element $h \in G$ whose discrete logarithm to base g is unknown.

The public key for the group is $\mathcal{Y} = (n, e_1, e_2, f_1, f_2, G, g, h)$, and the secret key is the factorization of n. Note that e_1, e_2, f_1 and f_2 must satisfy that solving the congruence $f_1 x^{e_1} + f_2 \equiv v^{e_2} \pmod{n}$ is hard. The choices for e_1, e_2, f_1 and f_2 are discussed in [4].

For each group, the trustee publishes $y_R = h^\rho$ where $\rho \in_R Z_n$ while ρ is kept secret. Furthermore, the participants publishes the public key of any digital signature scheme and keeps the corresponding secret key. Hereafter, except for signing, the values sent from each participant are signed on the digital signature scheme.

Entry into group:

1. A person U who enters a group chooses $x_1 \in_R Z_n^*$ to compute $y_1 = x_1^{e_1} \bmod n$ and $z_1 = g^{y_1}$. U sends the trustee y_1 and z_1.

2. The trustee returns U the digital signature, v_T, of the trustee on z_1. v_T assures that the trustee keeps z_1.

3. U chooses $x_2 \in_R Z_n^*$ to compute $y_2 = x_2^{e_1} \bmod n$ and $z_2 = g^{y_2}$. And U chooses $r_1, r_2 \in_R Z_n^*$ to compute $\tilde{y_1} = r_1^{e_2}(f_1 y_1 + f_2) \bmod n$ and $\tilde{y_2} = r_2^{e_2}(f_1 y_2 + f_2) \bmod n$. U sends the group manager $\tilde{y_1}, \tilde{y_2}, z_1, z_2$ and v_T. Furthermore, U proves that they is formed correctly by sending

$$V_1 = E\text{-}SKROOTLOG[\alpha : z_1 = g^{\alpha^{e_1}}](\tilde{0}),$$
$$V_2 = E\text{-}SKROOTLOG[\beta : g^{\tilde{y_1}} = (z_1^{f_1} g^{f_2})^{\beta^{e_2}}](\tilde{0}),$$
$$V_3 = E\text{-}SKROOTLOG[\gamma : z_2 = g^{\gamma^{e_1}}](\tilde{0}),$$
$$V_4 = E\text{-}SKROOTLOG[\delta : g^{\tilde{y_2}} = (z_2^{f_1} g^{f_2})^{\delta^{e_2}}](\tilde{0}).$$

   V_1 proves that z_1 is the form of $g^{\alpha^{e_1}}$ for α which U knows. V_2 proves that $\tilde{y_1} \equiv \beta^{e_2}(f_1 \alpha^{e_1} + f_2) \pmod{n}$ for β which U knows. Thus, the correctness of $\tilde{y_1}$ and z_1 is assured. V_3 and V_4 are like V_1 and V_2.

4. If V_1, V_2, V_3, V_4 and v_T are correct, the group manager sends U $\tilde{v_1} = \tilde{y_1}^{1/e_2} \bmod n$ and $\tilde{v_2} = \tilde{y_2}^{1/e_2} \bmod n$.

5. U gets the certificates $v_1 = \tilde{v_1}/r_1 = (f_1 y_1 + f_2)^{1/e_2} \bmod n$ and $v_2 = \tilde{v_2}/r_2 = (f_1 y_2 + f_2)^{1/e_2} \bmod n$.

Signing: When a member U signs a massage m, U computes $\tilde{g} = g^{r_1}$, $\tilde{z_1} = \tilde{g}^{y_1}$, $\tilde{z_2} = h^{r_2} g^{y_2}$ and $d = y_R^{r_2}$, where $r_1, r_2 \in_R Z_n^*$. Furthermore, U computes the following signature of knowledge:

$$\tilde{V_1} = E - SKROOTLOG[\alpha : \tilde{z_1} = \tilde{g}^{\alpha^{e_1}}](m),$$
$$\tilde{V_2} = E - SKROOTLOG[\beta : \tilde{z_1}^{f_1} \tilde{g}^{f_2} = \tilde{g}^{\beta^{e_2}}](m),$$
$$\tilde{V_3} = E - SKROOTREP[(\gamma, \delta) : \tilde{z_2} = h^{\gamma} g^{\delta^{e_1}}](m),$$
$$\tilde{V_4} = E - SKROOTREP[(\epsilon, \zeta) : \tilde{z_2}^{f_1} g^{f_2} = h^{\epsilon} g^{\zeta^{e_2}}](m),$$

$$\tilde{V_5} = SKREP[(\eta, \theta) : d = y_R^{\eta} \wedge \tilde{z_2} = h^{\eta} g^{\theta}](m).$$

$\tilde{V_1}$ proves that $\tilde{z_1}$ is the form of $\tilde{g}^{\alpha^{e_1}}$ for α which U knows. $\tilde{V_2}$ proves that $f_1\alpha^{e_1} + f_2 \equiv \beta^{e_2} \pmod{n}$ for β which U knows. $\tilde{V_3}$ proves that $\tilde{z_2}$ is the form of $h^{\gamma} g^{\delta^{e_1}}$ for γ and δ which U knows. $\tilde{V_4}$ proves that $f_1\gamma \equiv \epsilon \pmod{n}$ and $f_1\delta^{e_1} + f_2 \equiv \zeta^{e_2} \pmod{n}$ for ϵ and ζ which U knows. $\tilde{V_5}$ proves that $(\tilde{z_2}, d)$ is an ElGamal encryption on $g^{\delta^{e_1}}$. The signature on m is $(\tilde{g}, \tilde{z_1}, \tilde{z_2}, d, \tilde{V_1}, \tilde{V_2}, \tilde{V_3}, \tilde{V_4}, \tilde{V_5})$.

Verification: The verification of the group signature $(\tilde{g}, \tilde{z_1}, \tilde{z_2}, d, \tilde{V_1}, \tilde{V_2}, \tilde{V_3}, \tilde{V_4}, \tilde{V_5})$ is the verification of $\tilde{V_1}, \tilde{V_2}, \tilde{V_3}, \tilde{V_4}$ and $\tilde{V_5}$.

Identifying signer from signature: When it is ordered to identify the signer from a signature $(\tilde{g}, \tilde{z_1}, \tilde{z_2}, d, \tilde{V_1}, \tilde{V_2}, \tilde{V_3}, \tilde{V_4}, \tilde{V_5})$, the trustee computes $\hat{z_2} = \tilde{z_2}/d^{1/\rho}$ to present $\hat{z_2}$ together with

$$SKREP[\alpha : \tilde{z_2} = \hat{z_2} d^{\alpha} \wedge h = y_R^{\alpha}](\tilde{0}).$$

This $SKREP$ proves that $\tilde{z_2}$ is decrypted into $\hat{z_2}$. The group manager searches z_2 identical with $\hat{z_2}$ to present member's signature on z_2, which indicates the signer.

Canceling of membership: When it is ordered to cancel the membership of a member in the group, the trustee sends verifiers y_1, z_1 and v_T of the member. Then, for each signature $(\tilde{g}, \tilde{z_1}, \tilde{z_2}, d, \tilde{V_1}, \tilde{V_2}, \tilde{V_3}, \tilde{V_4}, \tilde{V_5})$, any verifier can check $\tilde{z_1} = \tilde{g}^{y_1}$. If it holds, the signature is made by the member.

4. DISCUSSION

The differences between the proposed scheme and that in [4] are as follows: While the certificate for y_2 is only issued in the original scheme, the certificate for y_1 is also issued and y_1 is registered in the trustee in this scheme. Next, $\tilde{g}, \tilde{z_1}, \tilde{V_1}$ and $\tilde{V_2}$ are added to the signature. Finally, the canceling of membership is added. The newly added part contributes the canceling of the membership as follows. y_1 enables verifiers to distinguish $(\tilde{g}, \tilde{z_1})$ of a signer whose membership is canceled from others, while $(\tilde{g}, \tilde{z_1})$ is anonymous if y_1 is in secret. The certificate for y_1, $\tilde{V_1}$ and $\tilde{V_2}$ assures that $\tilde{z_1}$ is computed from y_1 which is kept by the trustee. Now, the security of the newly added part is discussed. The unforgeability of the certificates depends on that in the original because of the sameness of the structures. The anonymity of $(\tilde{g}, \tilde{z_1})$ holds owing to the following assumption: For $g, z = g^s, \tilde{g} = g^r$ and $\tilde{z} = \tilde{g}^s$ where $r, s \in_R G$, if r and s are unknown, it is infeasible to determine whether or not the logarithm of z to the base g is the same as the logarithm of $\tilde{z}$ to base $\tilde{g}$. The assumption is based on, for example, the undeniable signature in [5]. The security of the signatures of the knowledge is based on those in the original. The group manager and trustee cannot impersonate a valid member since they cannot know y_2 registered by the member.

By sending a request to use a resource together with the proposed group signature on it to the manager of the resource, the manager can check that an anonymous access is issued by a user having the access privilege. And, the manager can check that an anonymous access is issued by a user whose access privilege is canceled while the anonymity of the other users is not disrupted.

5. CONCLUSION

In this paper, a group signature scheme where canceling the membership is easily performed has been proposed, which is suitable for the anonymous access control since the further access by a user whose access privilege is canceled can be rejected.

REFERENCES

[1] D. Chaum and E. van Heijst : Advances in Cryptology — EUROCRYPT '91, (1991), 241.

[2] L. Chen and T. P. Pedersen : Advances in Cryptology — EUROCRYPT '94, (1995), 171.

[3] J. Camenisch : Advances in Cryptology — EUROCRYPT '97, (1997), 465.

[4] J. Camenisch and M. Stadler : Advances in Cryptology — CRYPTO '97, (1997), 410.

[5] D. Chaum : Advances in Cryptology — EUROCRYPT '90, (1991), 458.