Membership Authentication for Hierarchical Multigroups Using the Extended Fiat-Shamir Scheme

Kazuo Ohta *Tatsuaki Okamoto* *Kenji Koyama*[†]

NTT Communications and Information Processing Laboratories
Nippon Telegraph and Telephone Corporation
1-2356, Take, Yokosuka-shi, Kanagawa, 238-03 Japan

[†]NTT Basic Research Laboratories
Nippon Telegraph and Telephone Corporation
3-9-11, Midori-cho, Musashino-shi, Tokyo, 180 Japan

Abstract

We propose two membership authentication schemes that allow an authorized user to construct one master secret key for accessing the set of hierarchically ordered groups defined by the user, without releasing any private user information. The key allows the user to prove his membership of his true groups and all lower groups, without revealing his name or true groups. The user can calculate the secret member information needed to access a group from his master secret key, and can convince a verifier using the extended Fiat-Shamir scheme. Each of two proposed schemes can generate the master secret key. To ensure the user's privacy, one uses the blind signature and pseudonym encryption techniques, and the other uses Euclid's algorithm. Because each user stores only one master secret key, memory usage is very efficient. Moreover, verifiers can check membership validity using public information independent of the number of users in an off-line environment. Therefore, our schemes are suitable for smart card applications.

I.B. Damgard (Ed.): Advances in Cryptology - EUROCRYPT '90, LNCS 473, pp. 446-457, 1991.

1. Introduction

There are many situations in which a user must prove his authority to others. The easiest and most direct way is to prove his identity. From the standpoint of privacy protection, however, the user often prefers to conceal his identity, that is, to prove his authority as an anonymous user [C1]. When a user is granted service privileges based on his membership of a certain group, for example, a special discount rate is available to members of a group, it is more essential to prove his authority rather than to show his identity. We call this type of authentication, *membership authentication* [C2, KMI1]. This authentication convinces verifiers that the user is a valid member of a certain group without revealing his identity, while user authentication proves the validity of a user by displaying his identity.

When these membership authentication schemes are implemented with smart cards, the following problems have to be considered.

- Efficiency: When a user participates in many groups, he must keep one smart card for each group. This is very inefficient. Thus, these cards should be combined into a single card. In other words, if a secret key represents membership in a group, many secret keys must be replaced with a single secret key.
- Group Isolation: When a user participates in many groups, he may want to conceal group membership so that no third party or group can determine the user's membership in other groups.
- Hierarchy: The range of services available or soon to be available to smart card users is extremely rich and varied. It is obvious that financial institutions and credit companies will want to issue cards with different service ratings. High level cards can access a broadrange of services, while low level cards are restricted to just one or two services. The services or groups are arranged hierarchically, and a user, who is a member of a *superior* group, is automatically a member of all affiliated lower groups.

To implement membership authentication or related services, several schemes have been proposed by [C2], [KMI1], [K] and [AT, MTMA]. However, the schemes of [C2, KMI1] do not treat the hierarchical situation, and do not satisfy the group isolation conditions either. The scheme of [K] is an inefficient authentication in which a high position user must keep excessive secret information. The access control scheme proposed by [AT, MTMA] uses cryptographic key assignment, however, it can not be used directly as an authentication scheme.

In this paper, we propose two membership authentication schemes using an extension of the Fiat-Shamir scheme, which solve the above mentioned problems. Each scheme stores only one master secret key in a card in order to prove various memberships, that is, memory usage is very efficient in the proposed schemes. These schemes allow a user, who occupies one position in a hierarchical structure, to authenticate his membership of any lower position without revealing his identity or original position, that is, the hierarchical property is realized and the group isolation is ensured with our schemes. Moreover, each verifier can check membership validity using public information independent of the number of users in an off-line environment. Therefore, they are suitable for smart card applications.

2. Components

Each scheme has the following components.

- Center - an organization established through the cooperation of various groups. It issues multipurpose smart cards. There is secret information known only to the center. The center can not access the secret information of the various groups.
- Group Administrator - an organization that authenticates a member's identification when he registers with the group. The administrator also maintains a member's database, which stores each member's qualification information; address, salary, age etc., which is private information.

- User - a member of one or several groups.
- Verifier - an entity that checks membership validity. Typical examples of verifiers are terminals that can read various smart cards. These terminals are located in shops where various smart cards are used.

3. Requirements

There are seven requirements for membership authentication for hierarchical multigroups [OkOh].

(1) Completeness - a true user is judged valid by any verifier who uses public information.

(2) Soundness - a false user is not judged valid by verifiers.

(3) Anonymity - identity of user is secret to the verifier and any third party.

(4) Group isolation - information as to which groups a user belongs is secret to everyone except the respective group administrators. Hereafter, we assume there is no conspiracy of group administrators.

(5) Efficiency of verifier - verification is implemented in an off-line environment, that is, a verifier does not have to access the center or group administrators for verification. The amount of information used by a verifier does not depend on the number of users.

(6) Efficiency of user - the amount of information used by a user does not depend on the number of groups the user belongs to.

(7) Group hierarchy - when the set of groups is hierarchical, a user, who is a member of a certain set of groups, is a member of all lower affiliated groups. That is, the card can generate secret membership information corresponding to lower groups from the one piece of secret information that corresponds to the highest groups a user belongs to. It is important to ensure that the card can only generate information about the user's groups.

4. The Proposed Schemes

We propose two schemes that satisfy the above mentioned requirements. The first one is center oriented, and the second one is user oriented. In both schemes, the user's card stores the secret hierarchical membership information defined as a form similar to those proposed by Akl et al. in the construction method of hierarchical access key [AT, MTMA] and by Chaum in the denomination scheme [C3]. A user uses one piece of secret hierarchical membership information, we call it his master secret key. We apply both the blind signature technique [C1] and the pseudonym encryption technique [C4] to generate the master secret key in the first scheme, and we use Euclid's algorithm to calculate it from several pieces of secret membership information issued by the group administrators separately in the second scheme. These techniques ensure group isolation and anonymity. The user generates membership information from the master secret key, and proves that he has the membership information by using the extended Fiat-Shamir scheme [GQ, OhOk1] or its symmetric version [O] in both schemes.

4.1 Groups Hierarchical Structure

We assume a set of groups has a structure of partial order (see Fig.1). The notation (○) indicates a group, and a line indicates an order relationship. That is, $G_i \geq G_j$ means that group G_i has a higher position than group G_j. This notation ($\geq$) satisfies the order relationship.

4.2 Center Key Generation and Distribution

The center randomly generates two large prime numbers p and q and keeps them secret. It also generates public information, such as $n(= p \times q)$, $a \in Z_n$, where $Z_n = \{0, 1, \cdots, n-1\}$, and b_i, which corresponds to group G_i ($i = 1, 2, \cdots$) and satisfies both $\gcd(b_i, b_j) = 1$ ($i \neq j$) and

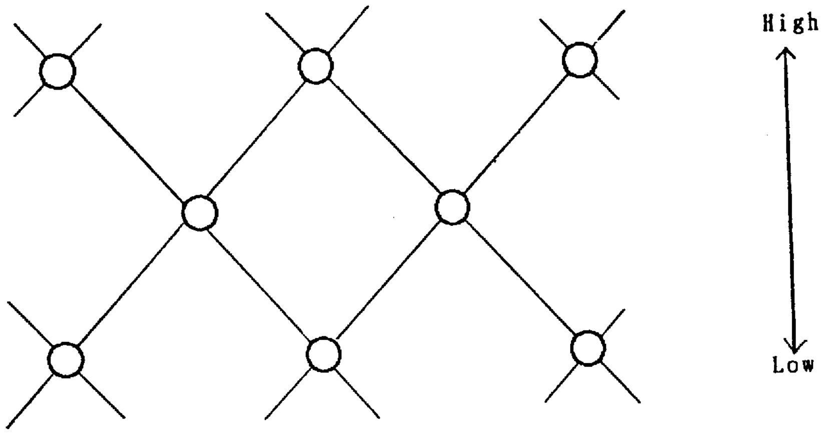

Fig.1 Hierarchical structure of groups

$\gcd(b_i, L) = 1$, where $L = lcm(p-1, q-1)$. It moreover calculates

$$e_i = \prod_{j \in \{j| \; G_i \geq G_j\}} b_j,$$

that is, e_i is the product of $\{b_j\}$ whose index j correponds to that of G_i or groups lower than G_i. Finally, the center distributes public keys to users and verifiers.

Only in the second scheme, the center secretly distributes membership information $w_i = a^{1/e_i} \bmod n$, where $1/e_i$ is the inverse element of e_i in $\bmod L$, to the group administrator of G_i.

4.3 Group Administrators Signature Key Generation and Registration

Each group administrator generates a key for a digital signature scheme, and registers the public key in a public information directory. This procedure is necessary in the first scheme.

4.4 User's Secret Master Key Generation

Let Γ represent a set of indexes of groups a user belongs to, and this user already has the master secret key w corresponding to Γ, where $w = a^{\frac{1}{A}} \bmod n$ and $A = \prod_{j \in \Gamma} b_j$. Suppose the user becomes a member of a new group G_i (*i.e.*, $i \notin \Gamma$). Note that if Γ is an empty set then $w = a$.

(1) Scheme 1 (Center Oriented)

The master key generation algorithm proposed here combines the blind signature technique [C1] and the pseudonym encryption technique [C4] in order to protect user's privacy.

First, the user calculates $c = r^{e_i} \cdot w \bmod n$, where r is a random number in Z_n satisfying $\gcd(r, n) = 1$, and sends it to the group administrator of G_i. After the group administrator confirms the user's qualifications, the user receives a digital signature s of c from G_i, and sends (c, s) to the center.

The center checks the validity of (c, s) using the public information of the group administrator G_i. When the check is passed, the center calculates $d = c^{1/e_i} \bmod n$, where $1/e_i$ is the inverse element of e_i in mod$L$, and sends it to the user.

Finally, the user calculates a new master secret key w' corresponding to Γ', where $\Gamma' = \Gamma \cup \{j | \; G_i \geq G_j\}$, as follows:

$$B = \prod_{j \in \Gamma \cap \{j | \; G_i \geq G_j\}} b_j,$$

$$w' = (d/r)^B \bmod n.$$

Note that the blind signature technique is used for the communications between users and group administrators to ensure group isolation, and the pseudonym encryption technique is used for communications between users and the center to ensure user anonymity.

(2) Scheme 2 (User Oriented)

Euclid's algorithm is used here in order to generate master secret keys. Since the user calculates his new master secret key by himself, the blind signature and pseudonym encryption techniques are not necessary.

First, the user requests the group administrator G_i to issue secret membership information $w_i = a^{1/e_i} \bmod n$, where $1/e_i$ is the inverse element of e_i in $\bmod L$.

Then, the user calculates a new master secret key w' corresponding to Γ', where $\Gamma' = \Gamma \cup \{j|\ G_i \geq G_j\}$, from w and w_i in the following way:

Step 1: The user calculates $B = \prod_{j \in \Gamma'} b_j$.

Step 2: He calculates $c = B/A$ and $d = B/e_i$.

Step 3: He calculates α and β satisfying

$$\alpha c + \beta d = 1$$

using Euclid's algorithm. Note that $gcd(c, d) = 1$ holds, since $B = lcm(A, e_i)$ holds.

Step 4: He calculates $w^{\alpha} w_i^{\beta} \bmod n$. (If Γ is an empty set then $w = a$ and $A = 1$.)

Note that since $w_i = a^{1/e_i} \bmod n$, $w' = a^{1/B} \bmod n$ and $w = a^{1/A} \bmod n$ imply $w'^{c} \equiv w \pmod n$ and $w'^{d} \equiv w_i \pmod n$, then $w^{\alpha} w_i^{\beta} \equiv (w'^{c})^{\alpha} (w'^{d})^{\beta} = w'^{\alpha c + \beta d} \equiv w' \pmod n$ holds.

4.5 Users Membership Authentication

When the user attempts to prove his membership of group G_k (*i.e.*, $k \in \Gamma'$), he calculates member information w_k corresponding to G_k from the master secret key w' as follows:

$$B' = \prod_{j \in \overline{\{k'|\ G_k \geq G_{k'}\}} \cap \Gamma'} b_j,$$

$$w_k = w'^{B'} \bmod n = a^{1/e_k} \bmod n,$$

where the notation $\overline{S}$ means the complement set of S.

Finally, the user convinces a verifier that he has secret membership information w_k, which satisfies $w_k^{e_k} \equiv a \pmod{n}$, by using the extended Fiat-Shamir scheme or its symmetric version, where e_k is the public information corresponding to group G_k and a is the public information of the system.

5. Discussion

Since each scheme stores only one master secret key in a card, efficiency of user is realized.

During the authentication phase, since the extended Fiat-Shamir scheme [GQ, OhOk1] or its symmetric version [O] are used, completeness, soundness and efficiency of verifier are realized.

Since both the blind signature and pseudonym encryption techniques are applied to generate the master secret key in *Scheme 1*, and Euclid's algorithm is used in *Scheme 2*, group isolation and anonymity properties are ensured.

The group hierarchy property, that the card can *only* generate information $a^{1/e_k} \bmod n$ corresponding to lower groups G_k from the master secret key w', was ensured by the recent result of Everste and van Heyst [EH].

6. Applications

The proposed schemes are applicable to membership authentication *without hierarchy.* Consider the three groups, G_j, G_i and G'_i. G_i and G'_i have the same level, and are subordinated to the higher group G_j where $G_j = G_i \cap G'_i$, $b_j = 1$, and $e_j = e_i \times e'_i$. Our scheme is applicable to this situation providing "$(G_i \cap G'_i)$ *authentication*" [KMI2] without modifying any public information.

With the proposed schemes, if new relationships between the highest group and another group are introduced or a new group is added to the highest position in the hierarchical structure, only the public information corresponding to the new group is influenced. However, if lower group sets are restructured, the public information corresponding to all higher groups is influenced. Therefore, extension of the hierarchical structure of groups should be considered in advance.

Membership signature schemes for hierarchical multigroups can also be realized in a similar way using the extended Fiat-Shamir scheme [GQ, OhOk1] or its symmetric version [O].

Our schemes are also applicable to membership authentications in a company's hierarchical organization or in access control services of computer systems, without revealing any private information such as the person's name or true position.

The schemes can also be used, when the set of groups are constructed hierarchically in *reverse order.*

7. Conclusion

We have proposed two membership authentication schemes that generate master secret keys for hierarchical multigroups. In order to generate a master secret key ensuring the user's privacy, one uses the blind signature and pseudonym encryption techniques and the other uses Euclid's algorithm. The schemes satisfy all requirements for membership authentication in hierarchical multigroups. However, the security of the proposed schemes has not yet been confirmed.

Acknowledgement

The authors would like to thank Professor Matsumoto of Yokohama National University for his valuable suggestions.

References

[AT] S.G.Akl and P.D.Taylor, "Cryptographic Solution to a Problem of Access Control in a Hierarchy," ACM Trans. on Computer Systems, 1, 3, pp.239-248 (1983)

[C1] D.Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete," Comm. of the ACM, 28, 10, pp.1030-1044 (1985)

[C2] D.Chaum, "Showing credentials without identification: Signatures transferred between unconditionally unlinkable pseudonyms," Advances in Cryptology, Eurocrypt'85, Springer-Verlag, 1986, pp.241-244

[C3] D.Chaum, "Online Cash Checks," Eurocrypt'89 (1989)

[C4] D.Chaum, "Untraceable electronic mail, return addresses and digital pseudonyms", Comm. of the ACM, 24, 1981, pp.84-88

[EH] J.H.Everste and E. van Heyst, "Which RSA signatures can be computed from some given RSA signatures?", in these proceedings

[GQ] L.C.Guillou and J.J.Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Tranamission and Memory," Eorocrypt'88 (1988)

[K] K.Koyama, "Demonstrating membership of a group using the Shizuya-Koyama-Itoh (SKI) protocol," The 1989 Symposium on Cryptography and Information Security (CIS'89), Gotenba, Japan (1989)

[KMI1] M.Kurosaki, T.Matsumoto and H.Imai, "Simple Methods for Multipurpose Certification," The 1989 Symposium on Cryptography and Information Security (CIS'89), Gotenba, Japan (1989)

[KMI2] M.Kurosaki, T.Matsumoto and H.Imai, "Proving that you belong to at least one of the specified groups," The 1990 Symposium on Cryptography and Information Security (SCIS'90), Hihondaira, Japan (1990)

[MTMA] S.J.Mackinnon, P.D.Taylor, H.Meijer and S.G.Akl, "An Optimal

Algorithm for Assigning Cryptographic Keys to Control Access in a Hierarchy," IEEE Trans. on Computers, 34, 9, pp.797-802 (1985)

[O] K.Ohta, "Efficient Identification and Signature Scheme," Electro. Lett., 24, 2, pp.115-116 (1988)

[OhOk1] K.Ohta and T.Okamoto, "Modification of the Fiat-Shamir Scheme," Crypto'88 (1988)

[OhOk2] K.Ohta and T.Okamoto, "Membership authentication for Hierarchical Multigroups Using Master Secret Information," The 1990 Symposium on Cryptography and Information Security (SCIS'90), Hihondaira,
Japan (1990)

[OkOh] T.Okamoto and K.Ohta, "Membership authentication for Hierarchical Multigroups Using the Extended Fiat-Shamir Scheme," 1989 Autumn Natinal Convention Record, IEICE, Engineering Science, SA-8-5, (Sept. 1989)