Fundamental Security Technologies

Anonymous Authentication: For Privacy and Security

By Kazue SAKO,* Shoko YONEZAWA* and Isamu TERANISHI*

ABSTRACT This paper presents NEC's activities on anonymous authentication. Anonymous authentication is a means of authorizing a user without identification. The technology serves as a breakthrough to enhance the privacy of the user and yet preserve the security of the system. A well-known example of such an authentication scheme is called the 'group signature scheme,' where a user can be authorized as a group member without identifying the name of the member. We propose a new group signature schemes that solve the member revocation problem and the centralized authority problem. We further propose a new notion of k-times anonymous authentication, whereby unlike the group signature scheme; no authority can identify a user who has accessed less than k-times.

KEYWORDS **Group signature, Cryptographic protocol, Zero-knowledge proof, Privacy**

1. INTRODUCTION

In recent years, authentication procedures have been increasing to ensure security of the individual. Simultaneously, users are becoming increasingly worried about infringement of their privacy, as they fear authorities are tracking their whereabouts and activities. However, allowing complete anonymous access for reasons of privacy could result in an alarming amount of crime. It has long been desired to develop technologies that both fulfill security and privacy needs.

The notion of anonymous authentication is considered to achieve this goal, that is, a legitimate user can be authorized yet have a certain amount of anonymity in meeting privacy requirements. In this paper, we present our two approaches in achieving anonymous authentication.

One approach is by enhancing group signature technology, where a vast amount of research is currently being carried out worldwide. This technology enables the verification of whether or not a user can be permitted access, without actually identifying the user. We present new group signature schemes that solve the centralized authority and member revocation problems respectively.

The other approach is based on a novel paradigm of security and privacy thresholds. In this approach, users are granted maximum privacy when they access services up to a limited number of times, but will be identified once they exceed the permitted maximum number of access times. Using our scheme, which is called the k-times anonymous authentication scheme, we can realize secret voting systems, anonymous e-coupons and anonymous Internet trial-browsing services.

We will describe our initial approach in Section 2, and the latter one in Section 3.

2. GROUP SIGNATURE SCHEME

2.1 Overview

A group signature scheme is technology that enables a user to prove that he belongs to a group without identifying himself. Additionally, there is an authority called the Group Manager who can identify the user in case of problems. Situations that would appreciate the privacy and security provided by the group signature scheme are to be found in the cases of rental video shops or libraries. It is often the case that users do not want to be identified when borrowing videos or books since the video titles or book titles can reveal a customer's interests and tastes. However, if the video or book lending procedure were carried on in a totally anonymous manner, the shop or library would have problems in identifying the user when a videotape or book is not returned.

When applying a group signature scheme in say a library system, a user first signs-up with the system and has his secret key stored in his smart card. When borrowing a book, he issues a group signature. This will tell the clerk at the desk that the user is indeed a user who signed up with the library, but will not give

*Internet Systems Research Laboratories

him any information identifying the user, not even a clue as to whether the same user has borrowed some book before. The group signature will be attached to the title of the book that was lent out, with the return due date. If the book is returned before the due date, the event will be recorded and a conveniently anonymous process is completed.

However, if the book is not returned even after the due date, the clerk will consult the head of the library with the group signature on the unreturned book. The head who serves as Group Manager can identify the user from the group signature using the group manager key. The library is now able to request the user to return the book.

2.2 Distribute and Separate Authorities

Although the group signature schemes succeed in hiding a user's identity from a clerk in the library, the scheme does not hide it from the head of the library that performs the role of Group Manager. It is thus desired to distribute the role of Group Manager so that not only a single person but a quorum of multiple users is needed when revealing a user's identity. Another role of the Group Manager is to perform a sign-up procedure with a new user. It is preferable to be able to separate the ability of these two roles, so that the roles can be performed by different individuals (**Fig. 1**).

In order to decentralize the power of Group Manager, we have succeeded in creating an efficient group signature scheme where the role of a Group Manager can be separated into two roles, that in the sign-up phase and that in the tracing phase, and that each role can be efficiently distributed among multiple entities. The details of the proposed scheme are described in **Fig. 2**.

2.3 Member Revocation Model

Another important issue regarding the group signature scheme is how to revoke a member. That is, it is desired to deprive the privileges of the group to a user who is no longer a member. It is easy to identify a revoked user under usual authentication. However, if one is using anonymous authentication, it is hard to distinguish if the user is a revoked user or not, since it is hard to identify the user.

In order to solve this problem, we have introduced a new practical model called OMSP (On-line Membership Status Protocol) Responder model, which has a high affinity with a familiar notion called OCSP (On-line Certificate Status Protocol). The OCSP model is used in the ordinary public-key based authentication system, where a verifier of a digital signature inquires to the OCSP server if the certificate that is attached to a digital signature is still valid. The idea of OCSP is introduced to reduce the burden on verifiers to maintain the list of revoked users. On the other hand, in the OMSP Responder model, a verifier of group signatures inquires to the OMSP server if the group signature has been issued by a valid member.

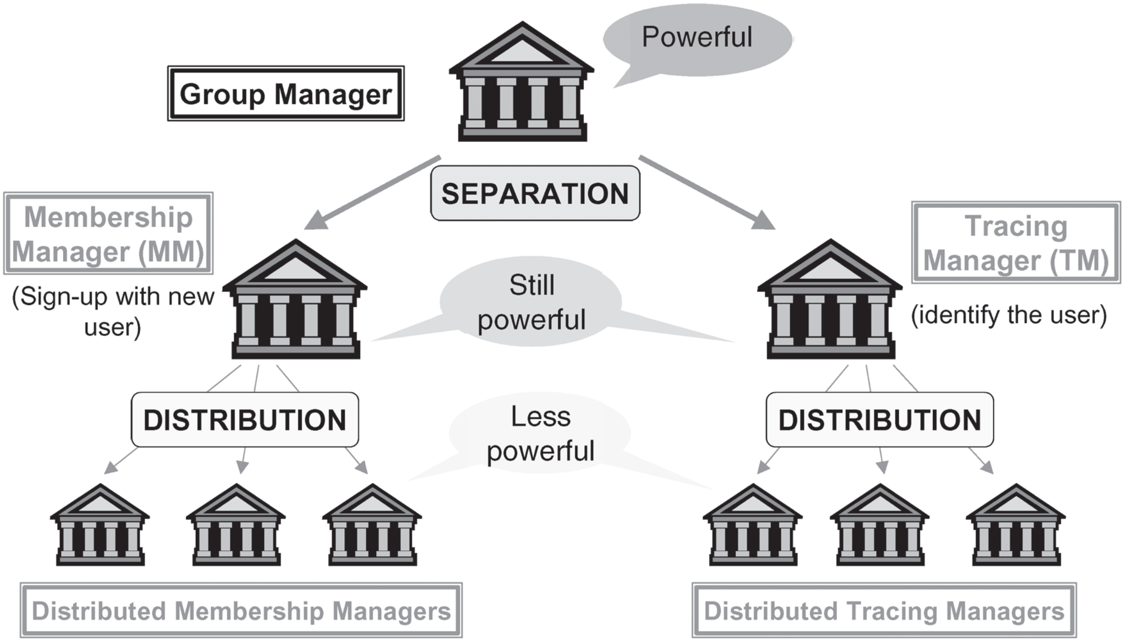

Fig. 1 OMSP Responder model.

The aim is not to reduce the burden on the verifiers, but to compliment what the verifiers cannot do. **Figure 3** illustrates this model.

Since the infrastructure of the OCSP is being used today, it would not be a difficult task to add the OMSP model to it, and thus it would be easy to solve the issue of member revocation if group signatures have been widely deployed.

3. k-TIMES ANONYMOUS AUTHENTICATION

3.1 A New Paradigm Based on Limited Access

We can regard the group signature scheme as a scheme that preserves the privacy of users to entities other than a Group Manager. That is, there is no privacy to a Group Manager because to this entity, a group signature is like an ordinary signature in the sense that a Group Manager can always identify the user. In this section, we present a novel scheme that achieves a new paradigm: users are granted maximum privacy when they access services up to a limited number of times, but will be identified once they exceed the permitted maximum number of access times.

p, q, P : large primes s.t. q | p-1 and p | P-1

g, h, f : generators of order q subgroup of Z_p*

G, H : generators of order q subgroup of Z_P*

$y = h^{\upsilon} \bmod p$: public key for the Membership Manager

$e = g^{\epsilon} \bmod p$: public key for the Tracing Manager

Membership certificate (r_U, ξ_U)

Group signing key σ_U

s.t. $r_U = y^{r_U} g^{\sigma_U} h^{\xi_U} \bmod p$

Signature Generation

1. Compute an ElGamal ciphertext of r_U

$$(g', e') = (g^{\tau}, r_U^{-1} e^{\tau}) \bmod p \quad (\tau \in_U Z_q)$$

2. Compute "proof of knowledge" of (r_U, ξ_U) , σ_U , τ satisfying

$$\begin{cases} (g', e') = (g^{\tau}, r_U^{-1} e^{\tau}) \bmod p \\ r_U = y^{r_U} g^{\sigma_U} h^{\xi_U} \bmod p \end{cases}$$

3. Output $(g', e', h', J,$ "proof of knowledge" $)$

Signer Tracing

1. Compute $\bar{r} := g'^{\epsilon}/e' \bmod p$

2. Find (r_U, ξ_U) s.t. $r_U = \bar{r}$

Fig. 2 Details of the proposed scheme.

This paradigm is already adopted today in many cases. For example, voters should be granted maximum privacy and security on their first vote. However, if the user tries to make a second vote the action should be identified as illegal. Another example is when one is allowed anonymous use of coupon tickets, but detection should occur when there is a breach of use. Also, coins are anonymous but can be used once only.

3.2 Applications

By deploying our new scheme, namely the k-times authentication scheme, one can enjoy secure electronic voting systems, electronic coupon services and digital cash systems with enhanced privacy. It is worth noting that in such voting systems, a user can hide not only for whom a vote is cast, but also whether or not a vote has in fact been cast.

Another interesting application of our scheme is anonymous Internet trial-browsing services. In this service the user may be allowed to browse a maximum of five times without being identified, but will be identified and charged on the sixth count of access etc.

The biggest advantage of our scheme is that the user can apply to multiple services with a variety of thresholds with a single key or 'License' issued at the registration stage (**Fig. 4**). We believe that the scheme can serve to upgrade current key public infrastructures to more privacy-enhanced systems.

3.3 Scheme

The k-times authentication protocol is comprised of three procedures namely sign-up, authentication, and identification. In the sign-up procedure a user obtains a license from the registration center. When a

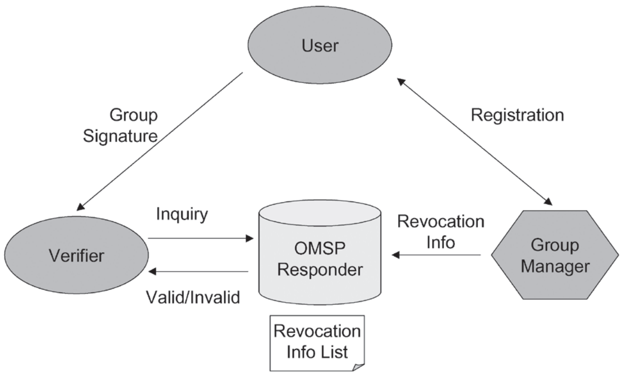

Fig. 3 Decentralizing authorities.

service provider wishes to allow a user to anonymously access up to k times, the provider publishes a set of k numbers, which is called a 'tag base.' When a user wishes to access this provider, he picks one of the unused numbers from the tag base and performs the authentication procedure. If the user has accessed the provider more than k times, he/she should have used some number from the tag base twice. Using this information, anyone, including the service provider can identify whom it was that accessed over the permitted number of times. A more detailed scheme is provided in **Fig. 5**.

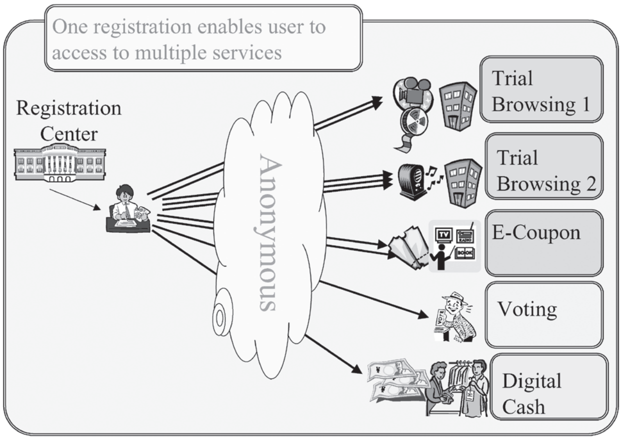

Fig. 4 Registration stage.

4. CONCLUSION

In this paper we have presented our activities with regard to current research into anonymous authentication technology. We believe that a ubiquitous society that fulfills both privacy and security needs is a must, and we will continue our efforts to achieve this goal.

REFERENCES

[1] G. Ateniese, J. Camenisch, et al., "A Practical and Provable Secure Coalition-Resistant Group Signature Scheme," In Advances in Cryptology - CRYPTO 2000, LNCS 1880, pp.255-270, Springer-Verlag, 2000.

[2] D. Chaum and E. van Heyst, "Group Signatures," In Advances in Cryptology - EUROCRYPT '91, LNCS 547, pp.257-265, Springer-Verlag, 1991.

[3] J. Kilian and E. Petrank, "Identity Escrow," In Advances in Cryptology - CRYPTO '98, LNCS 1462, pp.169-185, Springer-Verlag, 1998.

[4] I. Teranishi, J. Furukawa and K. Sako, "k-times Anonymous Authentication," In Advances in Cryptology-ASIACRYPT 2004, LNCS 3329, pp.308-322, Springer-Verlag, 2004.

Sign-up

1) Group Manager generates a user's license $(\mathbf{x}, \mathbf{A}, \mathbf{e})$ s.t. $\mathbf{a}^{\mathbf{x}}\mathbf{a}_0 = \mathbf{A}^{\mathbf{e}} \bmod \mathbf{n}$.

Here $(\mathbf{n},\mathbf{a},\mathbf{a}_0,\mathbf{b})$ is common public data.

2) Public information for the user is $\mathbf{b}^{\mathbf{x}}$.

Authentication

1) Tag Base$\{(\mathbf{s}_i, \mathbf{t}_i)\}_{i=1,\dots,k}$ is published for Service Provider.
2) The user picks $\mathbf{s}_i$ which he has not used before, and computes $\mathbf{s}_i^{\mathbf{x}}$.
3) Service Provider sends random l to the user.
4) The user computes $(\mathbf{b}^{l}\mathbf{t}_i)^{\mathbf{x}}$.
5) The user computes a validity proof of $(\mathbf{s}_i^{\mathbf{x}}, (\mathbf{b}^{l}\mathbf{t}_i)^{\mathbf{x}}, \mathbf{l})$.
6) The user outputs $(\mathbf{s}_i^{\mathbf{x}}, (\mathbf{b}^{l}\mathbf{t}_i)^{\mathbf{x}}, \mathbf{l},$ Proof).

Identification

1) the first component of the output data if the same $\mathbf{s}_i$ is used or not.

$(\mathbf{s}_i^{\mathbf{x}}, (\mathbf{b}^{l_1}\mathbf{t}_i)^{\mathbf{x}}, l_1,$ Proofs)

$\parallel$

$(\mathbf{s}_i^{\mathbf{x}}, (\mathbf{b}^{l_2}\mathbf{t}_i)^{\mathbf{x}}, l_2,$ Proofs)

2) If used twice, the user can be identified.

$$\begin{tikzcd}
\frac{(\mathbf{b}^{l_1}\mathbf{t}_i)^{\mathbf{x}}}{(\mathbf{b}^{l_2}\mathbf{t}_i)^{\mathbf{x}}} = \mathbf{b}^{(l_1-l_2)\mathbf{x}} \arrow[r] & \mathbf{b}^{\mathbf{x}} \arrow[dr] & \\
& & \text{identify the user.} \\
& \text{User's public info } \mathbf{b}^{\mathbf{x}} \arrow[ur] &
\end{tikzcd}$$

Fig. 5 Detailed scheme.

[5] J. Furukawa and S. Yonezawa, "Group Signatures with Separate and Distributed Authorities," Preproceedings of SCN 04, Amalfi Italy. To appear in LNCS Springer-Verlag.

[6] S. Yonezawa and K. Sako, "OMSP Responder: How to Deal with Revoked Members in Group Signatures," In CSS2004 (In Japanese).

Received January 6, 2005

* * * * * * * * * * * * * * *

Kazue SAKO joined NEC Corporation in 1986, and has been engaged in the research of cryptography and its applications. She has worked on the development of secure voting systems, auction systems and fair lottery systems.

Shoko YONEZAWA joined NEC Corporation in 2003, and is engaged in the research of group signatures.

Isamu TERANISHI joined NEC Corporation in 2002, and since then he has been engaged in research into cryptographic protocols, such as k-times authentication protocols and secure multi-party computation protocols.

* * * * * * * * * * * * * * *