Anonymous Authentication in Dynamic Groups

2001027, Jongseong Kim

Information and Communications University,
58-4, Hwaam-dong, Yusong-gu, Taejon, 305-732, Korea
jskim224@icu.ac.kr

Abstract. Electronic commerce is widely spread with popular use of Internet. The goal of this work is to make an anonymous authentication protocol for dynamic group in order to apply it to public network such as Internet. Using by concepts of Diffie-Hellman key agreement protocol and hash chain, we construct an efficient and useful anonymous authentication protocol in dynamic group. Especially, our protocol is suitable for an English auction and open bidding system. Temporal group organization in such systems is very important work since auction or bidding is done during specific time period. Our protocol consists of group members, a group manager and a verification center. In our protocol the verification center that acts like TTP does not possess any major information needed to identify group members. Similar to the verification center, the group manager cannot identify the group member without verification center's help. Therefore our protocol, unlike other existing anonymous authentication protocols using TTP, is more secure if either of them is honest.

Keywords: anonymous authentication, dynamic group, English auction, hash chain, forward security

1 Introduction

In the last few years, the number of the user of Internet has rapidly increased, accordingly the EC (electronic commerce) has boomed. Both Internet and the wireless network are public networks and considered to be insecure, where messages can be eavesdropped, captured, modified and inserted by intruders. Intruders may also impersonate as valid parties for illegal gain. The business transactions moving over Internet must be protected safely. Perhaps the most important area of network security is that of authentication and the related topic of digital signature. Nowadays, auctions become popular business areas and they play an important role in EC. In such systems, the group member wants to participate in bidding but she does not want to reveal her identity except when honor is award to her as winning bidder. This is the basic problem of *Anonymous Authentication.* Sometimes managing group membership dynamically becomes critical activity in several environments such as English auction or open bidding system. There are some important activities like organizing groups, managing membership, and selecting special group member as the winner. In wireless network with power-limited devices such as smart cards or mobile phones, the above work is much more difficult to perform within specific time periods efficiently. Especially, all participated members must make decision timely to win against competitors. In order to ensure valid membership for all group members, many approaches have been studied. In this work, we develop a new scheme for anonymous authentication that supports one time registration and allows multiple commitments. We employ the properties of hash function, which are One-wayness and Collision-free. Using these properties, we construct our protocol efficiently. Especially, it is suitable for an English auction in which all bidders can submit bet information to win the race. Also, our protocol can be used for either only one time commitment or multiple commitments.

Section 2 of this paper introduces some requirements for anonymous authentication protocols. Section 3 reviews previous work more detail. In section 4, we briefly introduced Diffie-Hellman key exchange protocol and Lamport's one time password. We use these concepts in section 5 to construct our proposed protocol. In section 6, we present security and efficiency of proposed protocol, compares them to that of [1], and conclude in section 7.

2 Requirements for Anonymous Authentication Protocols

To keep dynamic group membership anonymously, the following five requirements are essential to authenticate membership in dynamic groups.

- *Security* : Only members of group can be authenticated.
- *Anonymity* : Only authenticated member can reveal that she is a member of group.
- *Unlinkability* : Transactions cannot be identified that who makes and sends.
- *Formationability* : Group manager can efficiently build and maintain new groups that will be used specific time period.
- *Maintainability* : Group manager can easily add or remove members of group and change members' authentication key.

Usually group requires validity of group members by logging into the system so they can control and manage their members as clients. In auction or bidding systems, the group bulletins credential level of its group members in order to provide credit information to opposite parties such that buyers and/or sellers. Therefore, the definition of anonymity is acceptable and we can achieve unlinkability since neither the group manager nor the verification center can know some transactions, which are from which group members.

Note that auction or bidding rounds have limited time periods. Whenever auction is finished, the group is needless since the group members participated in current auction usually differ from that of next auction or bidding. Another consideration is that all members of group are not participated in auction. In that case, group formation becomes very important tasks.

To make dynamic group membership, adding or removing members is essential and changing authentication key is frequently required since human being falls into forgetfulness his secret information and to avoid keeping long-term key which has high probability of disclosure.

3 Previous Works

Group signature [2] was first introduced by Chaum and van Heyst. But it has serious problems as follows;

- If a member wants to sign many messages, he must select a new key pair for each message or the signature can be linked. The more signatures are allowed to make, the longer the length of the public key of group is required and
- If a new person wants to be a member, all other members must select a new key-pair or, it is easy to identify the public key of the new member.

Another work [3] was proposed by Camenisch and Stadler which is much more efficient than [2]. But it is still unsuitable for allowing multiple commitments such as English auction in which any group member can bid multiple times for winning the race against competitors. [4] based on any proof of knowledge for the $l'th$ root of modulo N and RSA scheme, but the user proves that he knows the some information that is an l^2'th residue modulo N. Until now, this kind of work require more computing time.

In [1] anonymous authentication protocol based on public authentication keys of all group members was introduced. As denoted by the authors VCS(Verifiably Common Secret) space grows linearly with the number of member of group, as does the time required to generate, transmit, and verify the entries. Also the protocol uses public-key cryptosystem to encrypt secret value x with all members' public authentication key, where x is the ticket value. It must be time consuming work. To reduce this work, they introduced the concept of subsets. In this case, a prover must select a subset of public authentication keys of all group members and include himself to the subsets. Therefore, any prover finds out group member's public authentication key set and keeps its ordered list. If prover loses his index, he cannot obtain the ticket value x.

4 Background

Our protocol based on Diffie-Hellman key exchange technique[5] and one time password which was developed firstly by Lamport[6].

4.1 Diffie-Hellman Key Exchange Technique

The first published public-key algorithm appeared in 1976 by Diffie-Hellman that defined public-key cryptography and is generally referred to as Diffie-Hellman key exchange. Today, a number of commercial products employ this key exchange technique. The purpose of this algorithm is to enable two parties to exchange a key securely and then it is used for subsequent encryption of messages. The Diffie-Hellman algorithm depends on the difficulty of computing discrete logarithms. Briefly, we describe the Diffie-Hellman key exchange in the following way.

There are two publicly known numbers: a prime number q and an integer α that is a primitive root of q. User A selects $X_A < q$ and computes $Y_A = \alpha^{X_A}$ mod q. Similarly, user B selects a random integer $X_B < q$ and computes $Y_B = \alpha^{X_B}$ mod q. They exchange Y value each other and keep X value as an own secret. Thus, user A computes the key as $K = (Y_B)^{X_A}$ mod q and user B computes the key as $K = (Y_A)^{X_B}$ mod q. Finally, the two parties share a common key, K.

The algorithm has two attractive features [7]:

1. Using Secret keys are created only when needed. There is no need to store secret keys for a long period of time.
2. The exchange requires no preexisting infrastructure other than an agreement on the global parameters.

But Diffie-Hellman key exchange is malleable against meet-in-middle attack [8]. To prevent this attack, we employ sender's digital signature for exchange data.

4.2 One Time Password

In Lamport's scheme, a password is used only once. If a password is used, the same password never used again. Therefore, the scheme eliminates any attempt of eavesdropping. In this scheme, any user must use a sequence of passwords $s_1, s_2, ..., s_n$ where s_i is the password by which the user identifies himself for the ith time. Each user selects an integer s as a seed and prepares a one-way hash function H to calculate the password chain $s, H(s), H(H(s)), ..., H^n(s)$ where n is a fixed constant defining the number of identification to be allowed. A user gives initial password $s^0 = H^n(s)$ to the verifier. For any login time $i, 1 \leq i \leq n$, the user sends the i-th value $s^i = H^{n-i}(s)$. The protocol works as follows:

- Initiation : A $\rightarrow$ B : $s^0 = H^n(s)$
- i-th login : A $\rightarrow$ B : $i, s^i = H^{n-i}(s)$

The Verifier needs a secure database for each user to maintain {user-id, i, s^i}. It is impossible to compute next password $H^{n-1}(s)$ from $H^n(s)$ since H is a one-way hash function. Thus, the scheme has some security advantages that even if the current password is revealed, the system is protected from attackers.

5 Proposed Anonymous Authentication Protocol

In this Section, we describe the proposed anonymous authentication protocol that allows multiple commitments in a specific session round and assures forward security.

Assumption: The hash function and random number generator are collision free.

5.1 Notation

- q : Large prime
- α: Primitive root of q
- H : Universal hash function
- U_i: Group member$_i$
- $\{R\} = \{R_i \mid i = 1, j\}; j \geq m$: Set of random number
- m : The number of the group members
- R_i : Assigned random number to $U_i, i \geq m$
- K_{GV} : Shared session key between GM and VC
- S_i : Seed value of U_i
- $E_k(\bullet), E(\bullet)_k, S_k(\bullet)$: Asymmetric, symmetric, digital signature respectively
- T : Secret session key per each session
- t : Decreased interval of n
- n : Maximum hashing counts on seed

5.2 System Set-up

The entities of our protocol consist of the group manager(GM),the verification center(VC), and m group members U_i $(i = 1, ..., m)$. The role of each entity is as follows:

GM
- He has responsibilities to manage a group and determines large prime q, primitive root a of q, and a universal hash function H.
- He generates a shared session key K_{GT} collaborating with VC and it is kept secret both GM and VC.
- He generates random numbers R_i $(i = 1, ..., n, n \geq m)$, which will be assigned randomly by GM to the group member participated in the current session.
- He generates a secret key T that is assigned to only this session.
- He maintains a secret database for keeping member's id U_i and its assigned random number R_i.
- If he wants to reduce time of verification delegated to VC, after initial verification done by VC, he may keep firstly submitted hash value $H^{n-t}(S_i)$ of each member like VC to verify validity of the group members by himself.

VC
- She has responsibilities to verify the member participating a current session is valid or not.
- She generates a shared session key K_{GT} collaborating with GM.
- She maintains a secret database for keeping each member's last hash value $H^n(S_i)$.

Member (U_i where $i = 1, ..., m$)
- Any member has to register to GM to participate in the current group.
- He can commit himself many times using his chained hash values $H^{n-t}(S_i)$.

In general, TTP seems to be, must be trust and assumed as an honest entity and it usually knows the key information about related entities. But in our protocol, VC has much less meaningful information needed to identify a group member. Without collaborating GM with VC, neither can know member's identity.

5.3 Anonymous Authentication protocol

The proposed protocol consists of the following four steps. Whenever GM wants to make a group for special purpose, he can execute preparation step since a group can be made temporarily. Registration of group member is only one-time in the protocol, but commitment step is executed whenever U_i wants to commit and this step has an ability to verify validity of U_i if the commitment of U_i is not the first time. Finally, the step four is executed.

Step 1. Preparation :

1. GM chooses a large prime q and a primitive root a of q and makes them public and prepares a universal hash function H.
2. GM selects a random integer X_G as secret, computes $Y_G = a^{X_G} \bmod q$ and encrypts Y_G using VC's public key and sends VC it.
3. VC selects a random integer X_V as secret, computes $Y_V = a^{X_V} \bmod q$ and computes a secret key $K_{GV} = Y_G^{X_V} \bmod q$.
4. VC encrypts Y_V using K_{GV}, encrypts both it and Y_V using GM's public key and sends it to GM.
5. GM decrypts Y_V using his secret key, computes a secret key $K_{GV} = Y_V^{X_G} \bmod q$ and verify $Y_T \stackrel{?}{=} D(Y_T)_{K_{GV}}$
6. If valid then GM generates random numbers $(R1, R_2, ..., R_n, n \geq m)$ and a random number T only for this session and encrypts them using K_{GV} and sends it to VC.
7. VC decrypts it using K_{GV} and stores all them to the secure database in order.

Step 2. Member Registration:
A group member U_i who wants to commit must register to GM only once:

1. U_i encrypts his user-id using GM's public key and sends it to GM.
2. GM chooses a random number R_i randomly and encrypts it together T using K_{GV} and encrypts again it using U_i's public key $(E_{U_{i_{pub}}}[E(R_i, T)_{K_{GV}}])$.
3. U_i decrypts it using his private key to find out $E(R_i, T)_{K_{GV}}$, chooses a seed S_i and hashes it n times($H^n(S_i)$), encrypts them using VC's public key and sends it to VC.
4. VC decrypts it and verifies $R_i \stackrel{?}{\in} (R_1, R_2, ..., R_n)$ and T, if valid, sends message "*Accept*" to the member U_i and stores $\{R_i, H^n(S_i)\}$ to the secure database.

Step 3. Commitments:

A group member U_i can commit whenever he wants:

1. U_i determines t, computes hash chain value $H^{n-t}(S_i)$, encrypts them with some $INFO_i$ using GM's public key and sends $E_{G_{pub}}[H^{n-t}(S_i), t, INFO_i]$ to GM. The $INFO_i$ can be any information (such as bidding price).
2. When the member U_i commits firstly, GM requests the validity of the member U_i to VC sending by $E_{VC_{pub}}[S_{GM}\{H^{n-t}(S_i), t\}]$, otherwise GM can verifies the validity of the member by himself.
3. VC decrypts it and verifies $H^t\{H^{n-t}(S_i)\} \stackrel{?}{=} H^n(S_i)$. If valid, then sends the message "OK" to GM.

Stage 4. Finding Member's Identity :

When expiration date is over, GM and VC can find out the qualified group member easily.

1. GM sends $E_{VC_{pub}}[S_{GM}\{H^{n-t}(S_i), t\}]$, which is the winning member's commitment, to VC.
2. VC decrypts it and verifies $H^t[H^{n-t}(S_i)] \stackrel{?}{=} H^n(S_i)$.
3. If valid, then VC sends R_i related in $H^n(S_i)$ to GM.
4. GM declares U_i who has the random number R_i is just the winning member and writes U_i on the bulletin board.

6 Security and Efficiency Analysis

We show that the proposed protocol is sound, reveals no information about the group member's secret, and reveals no information about the group member's identity within specific time periods and our protocol satisfies following five requirements.

1. **Security:** In our protocol, the common session key K_{GV} is created by GM with VC and which lifetime is limited during specific session period. The value of K_{GV} varies from that of previous or next session. This decreases the probability of reveal the value of the common session key K_{GV}. When the session key is exchanging, to prevent meet-in-the-middle attack, we adopt digital signature.
   Only legitimated user can obtain the random number R_i from GM. An unqualified user cannot obtain R_i, so she does not pass the verification of VC. U_i only do deliver the value R_i to VC since she does not know the common session key K_{GV}. This prevents conspiracy with other group members, since no group member can know assigned random number R_i.

2. **Anonymity:** At registration step, GM assigns the random number R_i to the group member U_i. At that time, GM knows the identity of U_i. But at the commitment step, GM cannot know the identity of U_i since U_i submits only this information $\{H^{n-t}(S_i), t, INFO_i\}$. GM has no information about

a seed S_i. Similarly, VC cannot know the identity of U_i because U_i sends $H^n(S_i)$ to VC, therefore VC also cannot know which random number R is assigned to the group member U_i.

3. **Unlinkability:** To achieve anonymity against GM,VC, and any other group members, U_i must chooses a new seed S_i per each session. Although GM and VC can know previous information using current information but they still do not know the owner of the information.

4. **Formationability:** In our protocol, the group formation is quite simple. At this step, only legitimated users and who want to participate the group can be picked out, therefore GM can make the group without redundancy. Whenever needs to construct a new group, GM does following simple works;
   (a) Using Diffie-Hellman key exchange technique, GM makes K_{GM} with VC and,
   (b) Without considering weather group members' public keys are changed or not, GM can generates a set of random number.

5. **Maintainability:** If a new user wants to be a group member during specific time period, GM only assigns a random number U_i to new user. If there is any malicious member, GM requests VC to delete S_i from secure database. After that, the malicious member cannot do anything. If a valid group member cannot pass verification of VC or GM, even though obeys the procedures of our protocol, he can claim immediately that he is a valid group member. All entities are under observation.

We compare the features of proposed protocol with [1] in Table 1.

Table 1. Comparison of proposed scheme with [1]

Features	[1]	Proposed
Security	O	O
Anonymity	O	O
Unlinkability	O	O
Group Formation	Not easy n times asymmetric encryption	Easy 1 time symmetric encryption
Maintainability	Easy	Easy
One-time password	x	O
Easy revocation	O	O
Using TTP	O	O

n = the number of group members

7 Conclusion

These days, electronic commerce activities become a part of our life and anonymous authentication,in many cases, is essential. Especially, managing dynamic group membership is critical since time based system such as auction or bidding in which everyone treats time as success factor to compete with each other for the win. There are many researches on an anonymous authentication using zero-knowledge interactive proof, information theory and etc. But until now anonymous authentication areas are on their way to succeed in overcoming several difficulties. In this paper we have shown securities and efficiency of our protocol. We employ Diffie-Hellman key exchange technique to make a session key efficiently and Lamport's one time password to allow multiple commitments using hash chain. Our protocol can be used for either only one time commitment or multiple commitments.

References

[1] S. Schechter, T. Parnell and A.Hartemink,"Anonymous Authentication of Membership in Dynamic Groups", In *Financial Cryptography '99* LNCS 1648, pp 184-195, 1999

[2] D. Chaum and E. van Heyst, "Group Signatures", In proc. *Eurocrypto'91*, pp 257-265, 1991.

[3] J. Camenisch and M. Stadler, "Efficient group signature systems for large groups", In proc. *Crypto'97*, pp 410-424, 1997.

[4] D.Boneh, M. Franklin, "Anonymous Authentication with subset queries", In *CCS '99, 6th ACM Conference on Computer and Communications Security*, ACM Press, November 1999

[5] Diffie. W., and Hellman. M, "New directions in cryptography", In *IEEE Transactions of on Information Theory IT-22*, pp 644-654, 1976.

[6] L. Lamport, "Password authentication with insecure communication", *Communication of the ACM*, 24(11), pp 770-771, 1981

[7] W. Stallings, "Cryptography and Network Security", Upper Saddle River, NJ: Prentice Hall, 1999.

[8] C. Huitema, "IPv6: The New Internet Protocol", Upper Saddle River, NJ: Prentice Hall, 1998