Comparison of Anonymous Authentication Protocols

Jongseong Kim and Kwangjo Kim

International Research center for Information Security(IRIS),

ICU, Korea

Abstract

An anonymous authentication scheme allows a user to identify himself as a member of a group of users in a secure and anonymous way. It seems to be crucial and indispensable components in English auction, electronic voting and open procurement, which are getting very popular business areas in E-commerce. First, we briefly describe the previous anonymous authentication protocols how to work and what cryptographic techniques adopted to increase performance and achieve anonymity. Second, we compare those protocols from the viewpoint of the communication and computation complexity and the specific cryptographic techniques used in their protocols.

I. Introduction

Anonymous authentication for a dynamic group is indispensable component in English auction and open procurement, which are getting very popular business areas in E-commerce. In these systems, group members want to participate in the group activities without revealing her identity except when honor is awarded to herself as a winner. This is the basic problem of anonymous authentication. In the literature, many anonymous authentication schemes were proposed based on witness-indistinguishability or zero-knowledge [6, 7, 8].

Up to now, most of the previous works have been tried to reduce complexities of computation and communication in their protocols. Yet no schemes are practical enough to be used in environments with power-limited devices such as smart cards or mobile devices.

Another important concern is that managing a group dynamically is a crucial task for a group manager while every group is alive and has a variant life cycle.

In wireless network with power-limited devices, managing a group dynamically is much more difficult to perform within specific time periods. Moreover, all participants must make a decision timely to win against competitors. Therefore, an efficient and practical protocol is indeed required. In this paper, we focus on complexity and some characteristics of the existing protocols to support developing new efficient protocols.

The remainder of this paper is organized as follows. Section II describes the security requirements of an anonymous authentication protocol(**AAP**) and its complexity and in Section III we analyze efficiency and complexity of previous works. Section IV compares 2 complexities and examines the cryptographic techniques adopted in their protocol. Finally, we will make concluding remarks in Section V

II. Preliminaries

We present the requirements that **AAP** must meet and define its security. Also, examine cryptographic techniques used to construct **AAP**

1) Security: Only members of group can be authenticated.

2) Anonymity: Only authenticated member can reveal that he is a group member.

3) Unlinkability: Transactions cannot be identified that who makes and sends.

4) Maintainability: Adding or removing group member is easy.

A group manager usually checks the validity of group members by logging into the system so they can control and manage their members as clients. Therefore, the property of security and anonymity can be acceptable. Note that any group has the limited time periods. Whenever the time is expired, the group may be discarded since the group members participating in current group usually differ from those of next groups. So, unlinkability and maintainability become very important task. To dynamically manage group, adding or removing members is crucial.

Another important criterion we must consider is performance. To measure this, we check computation and communication complexity of the given protocols.

In this section, we describe 4 previous works. The first scheme is based on proof of knowledge [1] and the second one makes use of all members' public key set [2], the third one discrete logarithm problem [3] and the last one hardness to find a pair satisfying a specific condition of RSA [4].

1. BM99[1]

Let m be the total number of users to be authenticated. Let $l > m$ be the smallest prime larger than m. This scheme is built on top of any proof of knowledge for the l-th root of a number modulo $N = pq$. In this paper, we only consider their basic scheme.

The issuer generates an k-bit RSA modulus $N = pq$ and picks a random $t \in Z_N$ and sets $T = t^l \bmod N$, $\mu \in Z_N$ to be some l-th root of unity such that $\mu \neq 1 \bmod p$ and $\mu \neq 1 \bmod q$. The values N, T and l are made public while t and μ keeping secret. $\beta_i = t \cdot \mu^i \bmod N$ is given to the user as the secret key.

For proving identity, the two facts must be checked simultaneously : (1) the user knows an l-th root of T, and (2) the blinding factor r^l used during the protocol is an l-th residue modulo N. First, the user picks random $r \in Z_N^*$, computes $u = r^{l^2} \bmod N$, $y = \beta_i \cdot r^l \bmod N$ and sends (u, y) to the verifier. Second, the verifier checks that $y^l = T \cdot u \bmod N$ and accepts if holds. Finally, the user proves that u is an l^2-th residue modulo N in zero knowledge. At the identification step, the agent uses the "baby-step and giant-step" to find out the member's identity.

2. SPH99[2]

This scheme makes use of all members' public key to hide identity of a member based on a deterministic encryption scheme like RSA.

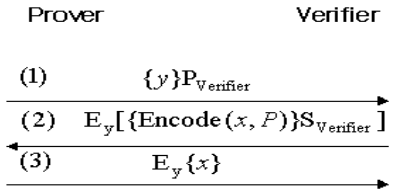

Fig 1: SPH99 Scheme

The prover randomly selects a session key y and then encrypts y with the verifier's public key. In response, the verifier randomly picks x and creates a message containing a verifiably common secret encoding of x, signs it, and then encrypts with the session key y. The prover decrypts and verifies the verifier's signature to reveal a value x from Encode (x, P). Finally, the prover proves her membership by sending x to the verifier. The verifier concludes that the prover is a valid member of a group.

In the scheme, the group manager encrypts a common secret value x under each user's public key and gives it to the user. In order for

a user to authenticate himself, he must send x to the group manager. Also, the member must verify that x has commonality or not by encrypting it with other member's public key and compare this with encrypted value sent by the group manager.

This scheme uses quite simple concept but requires unreasonable computational amount, as the size of the public key set is linear in the number of the group members, while it can remove a member from the group easily.

3. LDZ02[3]

This scheme is based on the discrete logarithm problem where anonymity is achieved by witness hiding technique in zero knowledge. Let p be a large prime and G be a cyclic sub group of z_p^* with order q and g be a generator of G. The public keys of all legal users are denoted by $y_1, \cdots, y_m$.

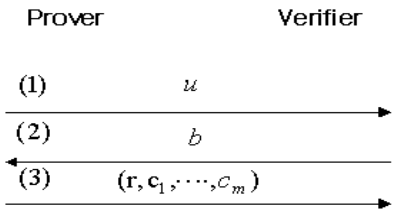

Fig 2: LDZ02 Scheme

In this scheme, $y_i = (g^{x_i} \bmod p)$ is the prover's public key and x_i is his secret key. The prover choose $s, d_1, c_2, \ldots, c_m \in Z_q$ uniformly at random, computes $u = g^s y_1^{d_1} y_2^{c_2} \cdots\cdots y_m^{c_m}$ and sends it to the verifier. The verifier chooses $b \in z_q$ uniformly at random and sends it to the prover. On receiving, the prover computes $c_1 = b \oplus c_2 \cdots \oplus c_m$, $r = s + (d_1 - c_1)x_1$ and sends $(r, c_1, \cdots, c_m)$ to the verifier. Finally, both $u = g^r y_1^{c_1} y_2^{c_2} \cdots\cdots y_m^{c_m}$ and $b = c_1 \oplus \cdots\cdots \oplus c_m$ are satisfied then accept.

4. KP98[4]

The goal of this scheme, variation of the group signature[5], is for a group member to anonymously identify himself as a member rather than being able to sign a message. In the scheme using RSA, the member does not give his identity to the verifier directly, but gives the information to the verifier that would allow the verifier to determine the member's identity. A $Cert(a, b)$ satisfies $a^e - b^e = \delta$ where δ can be either set randomly or to a fixed number and (a, b) is given to the group member. a^e contains the name of the member. For registration, the member choose a_1, b_1 uniformly at random and then sets a_2, b_2 satisfying $a = a_1 a_2$ and $b = b_1 b_2$. Also chooses that x, y are relatively prime to n. The verifier checks that the values committed by the group member are valid or not in zero knowledge.

1) $x, a_1, (a_1)^e, a_1 x, b_1, (b_1)^e$ and $b_1 x$
2) $a_2, (a_2)^e, b_2, (b_2)^e$ and $b_1 x$
3) $x(a_1)^e, (a_2)^e, y$ and $x(a_1 a_2)^e + y$
4) $x(b_1)^e, (a_2)^e, y$ and $x(a_1 a_2)^e + y$
5) $(x(a_1 a_2)^e + y) - (x(b_1 b_2)^e + y) = \delta x$

Above 5 tests hold only if $(a_1 a_2)^e - (b_1 b_2)^e = \delta$. To recover the complete identity, the verifier gives the transcripts of the proof to the escrow agent. Since the commitment on the $(a_1)^e$ and $(a_2)^e$ were encrypted with the agent's public key, the agent can get the value of a_1, a_2 and reveal the identity of the member using the value a. Unlike the previous schemes using agent, the escrow agent has no responsibility in setting up the system. Therefore, the member or verifier can choose the escrow agent independently.

III. Comparison

We compare mentioned 4 schemes from the viewpoints of computation and communication complexity, which is summarized in Tables 1 and 2, respectively. In addition, we state the important cryptographic applications adopted in

their protocols. We denote an exponentiation by E, the number of group members by m and the bit-length by n.

Table 1: Computation Complexity

	BM99	SPH99	LDZ02	KP98
Preparation	(m+1)E	mE	mE	3mE
Registration	1E	1E	(m+1)E	4E
Verification	7E	2E	(m+1)E	2E
Identification	(m/2)E	2E	2E	2E

Table 2: Communication Complexity

	BM99	SPH99	LDZ02	KP98
Registration	n	n	n	2n
Verification	5n	(m+1)n	(m+2)n	3n
Identification	4n	2n	2n	3n

Now, we point out important cryptographic properties adopted in each protocol.

● Hard problem used

BM99 scheme based on proof of knowledge for the l-th root of numbers and SPH99 scheme deterministic encryption scheme like RSA. But LDZ02 scheme based on the discrete logarithm problem and KP98 scheme on hardness to find (a, b) such that $(a^e - b^e) = \delta$ in RSA.

● Linearity of group size

At the identification step of BM99 scheme, the agent uses the "baby-step and giant-step" to find a member's identity where computation amount is linear on the number of the group members. Also, computation amount of SPH99 scheme is linear on the group size, since the group manager encrypts x for m times using a public key set for all group members. Also, LDZ02 scheme is similar to SPH99 scheme. But, KP98 scheme is not strongly dependent to the group size. The manager only generates *Cert* and assign it to all the group members.

● Identity hiding techniques

In BM99 and LDZ02 scheme, the anonymity is achieved by witness hiding technique in zero knowledge. SPH99 scheme hides member's identity using the set of public key of all group members. But, this concept causes critical problem like computation linearity in group size. KP98 scheme hides the member's identity using the partial knowledge of (a, b).

● Agent

Only BM99 and KP98 scheme used an agent to escrow member's identity.

IV. Concluding Remarks

We briefly describe and compare the previous anonymous authentication protocols from the viewpoint of the communication and computation complexity and cryptographic properties. As a result, no schemes surveyed so far are practical enough to be used in power-limited devices. So, we are now designing an efficient and robust **AAP** [9].

References

[1] D. Boneh and M. Franklin, "Anonymous authentication with subset queries", *ACM CCS 1999, ACM Press*, pp. 113-119, 1999.

[2] S. Schechter, T. Parnell, and A. Hartemink, "Anonymous authentication of membership in dynamic groups", *FC'99*, LNCS 1648, pp. 184-195, 1999.

[3] C.H. Lee, X. Deng, and H. Zhu, "Design and security analysis of anonymous group identification protocols", *PKC2002,* LNCS 2274, pp. 188-198, 2002.

[4] J. Kilian and E. Petrank, "Identity Escrow", *Crypto'98,* LNCS 1462, pp. 169-185. 1998.

[5] D. Chaum and E. van Heyst, "Group signatures", *Eurocrypt'91*, LNCS 547, pp. 257-265, 1991.

[6] U. Feige and A. Shamir, "Witness indistinguishability and witness hiding protocols", *Proc. of the 22nd STOC,* pp. 416-426, 1990.

[7] O. Goldreich, S. Goldwasser, and S. Micali, "Interleaved zero-knowledge", *ECCC*, Report No. 24, 1999.

[8] O. Goldreich, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems", *SIAM Journal on Computing*, 18: pp. 186-208, 1989.

[9] J. Kim, M. Kim, and K. Kim, "Anonymous authentication protocol for dynamic groups with power-limited devices using hash chain", submitted.