# SECURE KEY EXCHANGE IN NEW MULTI-PARTY IDENTITY-BASED AUTHENTICATED KEY AGREEMENT PROTOCOL

[1]P.R.VIJAYALAKSHMI ,[2]K. BOMMANNA RAJA

[1] Professor, Department of CSE , K.L.N. College of Engineering Sivagangai , India

[2]Professor and Head, Department of BME, PSNA College of Engineering and Technology, Dindigul, India

E-mail: [1]arsuji2013.putta@gmail.com , [2]dr.k.bommannaraja@gmail.com

## ABSTRACT

Today's computing environments such as internet conferencing, distributed simulation, multi-user games, and many more applications involve dynamic peer groups. Communication among dynamic peer groups must be secure and, at the same time, fast and cost effective. In an internet conference, all participants together establish a common conference key to enable multi-party and secure exchange of messages. The proposed protocol is executed by considering the basic login issues, session validation and formulated key generation with balanced multiple tables. The secret information of a user cannot be determined from the corresponding public information, therefore ensures privacy. Also, computing using bilinear mapping imposes a greater computational cost on a protocol, to improve the efficiency the bilinear mapping is utilized only during the session key computation.

**Keywords:** *Conference Key, Dynamic Peer Groups, Secure Communication, Bilinear Mapping*

## 1. INTRODUCTION

This paper is concerned with security services in the context of dynamic peer groups (DPGs). Such group communication among peers is common in many layers of the network protocol stack and many application areas of modern computing. DPG's typically assume a many-to-many communication pattern rather than one-to-many commonly found in larger, hierarchical groups.

The specific security requirements and needs of dynamic peer groups-in particular, key management are still considered as open research challenges [1]. Recently, several key agreement protocols geared for DPG's were proposed in[3].

Key agreement protocols are used to establish a common session key for encrypting communications between two or multiple parties. In 1976, Diffie-Hellman (1976) proposed the first key agreement protocol which enabled two parties to establish a session key [2]. However, it did not offer member authentication and was susceptible to the man-in-the-middle attack. Since then, different approaches and protocols have been developed to solve the problem, improve security and efficient of protocols (Dutta and Barua, 2005; Menezes et al., 1997).

A research direction in key agreement protocol aims to generalize two-party key agreement sets to multi-party key agreement sets. A special case of multi-party key agreement protocols are three-party (or tripartite) protocols. The pioneer work in the field was conducted by Joux (2000), who showed how to implement a three-party key agreement protocol using pairings. Since in his protocol only one broadcast is required, Joux's protocol is suitable for practical implementation. However, just like the Diffie-Hellman protocol, Joux's protocol does not provide authentication and thus is vulnerable to the man-in-the-middle attack. To solve the problem Al-Riyami and Paterson (2002) presented several protocols some of which use pairing. Their protocols assure authenticity through the use of certificates issued by a Certificate Authority (CA).The signature of CA assures that only the entities which are in possession of the static keys are able to communicate the session keys. Still, in a certificate system the participants must first verify the certificates before using the public key of a user, which requires a large amount of computing time and storage. Hence, an infrastructure is needed to establish and manage the key pairs and certificates, often referred to as certificate-based Public Key Infrastructure (PKI) [5].

As an alternative to certificate-based PKIs, Shamir introduced the concept of identity-based cryptosystems [4] in 1984 in which the user's public key is an easily calculated function of his / her identity (e.g. social security number, etc.), while the user's private key can be calculated for him / her by a trusted authority. An application of identity-based cryptosystems is identity-based authenticated key agreement protocols. In general such protocol includes a number of entities (the usual settings include 2, 3 or n entities) and a trusted authority referred to as Key Generation Center (KGC).

The first two-party identity-based authenticated key agreement protocol which is based on the RSA algorithm [5] was proposed by Okamoto in 1988 [6], whereas the first two-party identity-based authenticated key agreement protocol based on the difficulty of computing a discrete logarithm problem [7]. Later, it was developed into International Standards, for example. PKCS #3 [8] and ANSI X9.42 [9].

Considering an example of internet conference based on key agreement protocol, before the start of the conference, the members must establish a shared key to encrypt the details of the conference; this key is called conference key or session key. The conference is established jointly by all members of the conference, and not by any single member. this method is known as the conference key agreement protocols [3,10-17]. Thus, a situation where one member might have greater rights than other members can be avoided.

In order to let all internet conference participants to exchange information via secret communication, there must be a key agreement protocol to allow members to jointly construct a conference key. This protocol must have a process for detection and elimination of malicious participants so as to prevent legitimate members from obtaining an erroneous conference key [19].

According to technical categories of authentication approach, key exchange protocols may be classified into a number of categories: public-key-based key exchange protocols. A public-key based key exchange protocol adopts public-key cryptographic techniques to achieve the purposes of user authentication and key exchange. On the way of key management, although the public-key-based key exchange protocol is better than password-based key exchange protocol, on-line access to get and verify public keys from a public key system in a network system is time-consuming. Moreover, it needs to require extra efforts to maintain public-keys in a public key system. On the other hand, an identity-based key exchange protocol can be regard as a variation of the public-key based key exchange protocol. An identity-based key exchange protocol is a protocol that uses users' identity or some other information combined with their identity as ones public key to achieve user authentication and key exchange. Thus, a verifier does not verify the certificates of the public keys. Meanwhile, no on-line system authority is required.

This paper proposes a more efficient conference key agreement protocol that provides an explicit key authentication as well as the desired security properties of an authenticated key agreement protocol.

The remainder of the paper is organized as follows. We first discuss the computing environment and the various phases in the proposed protocol in Section 2 and 3. Section 4 carries out security and performance analysis. The conclusion is drawn in Section 5.

## 2. THE COMPUTING ENVIRONMENT

This paper considers the Internet Conferencing application as the computing environment which includes communication in dynamic peer groups. During communication, the user may leave or the new users may join. Whenever the user joins the group for communication, the user must be authenticated by transmitting the user's identity (e.g. user's security name, security code, etc.) to the trusted server.

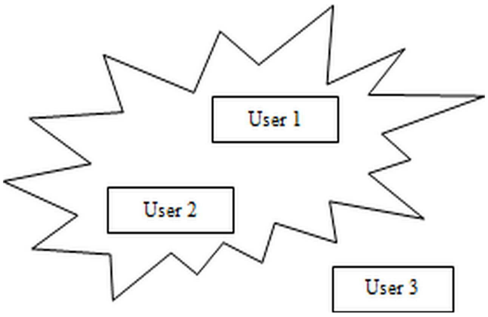

*Figure 1. User Inside And Outside DPG*

Figure. 1 shows that User 1 and User 2 are inside the communicating group and also they are authenticated users. If User 3 needs to join in the group, he / she must be authenticated.

## 3. PROPOSED PROTOCOL

The general objective of the proposed conference key agreement protocol is to allow a group of authenticated people to convene a conference on the Internet.

The proposed method has four phases, including parameter generation phase, secret distribution and commitment phase, sub key computation and conference key computation phase.

### 3.1 Parameter Generation Phase

The system authority selects the following parameters and functions, declares them publicly:

(1) p: a large prime number comprised of 2q + 1, where q is also a large prime;

(2) g: a q-order generator over GF(p);

Each user $U_i$ is provided with the following pair of two corresponding keys:

(1) Private Key denoted as $x_i € Zq*$ ;

(2) Public key denoted as $y_i = g^{x_i} \bmod p$

The protocol starts up the initiator who calls for a conference by initializing a set of participants U. First, let U = $\{U_1 ,U_2 ,\ldots, U_n\}$ be the initial participant set. Each participant $U_i (1\leq i\leq n)$ is a part of U.

### 3.2. Secret Distribution and Commitment Phase

All participants $U_i$ of set U execute the following steps to distribute his subkey to other participants:

**Step 1:** Randomly select an integer $a_i € Zq*$ , and calculate the common session key $k_{ij}$ shared with all other participants $U_j$ using the public key $y_j$ of $U_j$:

$$k_{ij} = y_j^{a_i} \bmod p \bmod q \quad 1\leq j \leq n \tag{1}$$

**Step 2:** Randomly select a line L(x):

$$L(x) = (c_i \bmod q) + CK_i \tag{2}$$

where $c_i = g_i^{a} \bmod p$ and $CK_i$ is the subkey that $U_i$ offers to share with the other participants

$$CK_i = (ID_i) \oplus (random\_int) \tag{3}$$

**Step 3:** Calculate the values $d_{ij}$ and $d_{ij}'$ using the session key $k_{ij}$ and the polynomial L(x):

$$d_{ij} = L(k_{ij})^{*} y_i ,\ 1<=j<=n \tag{4}$$

$$d_{ij}' = k_{ij} \oplus d_{ij} ,\ 1<=j<=n \tag{5}$$

### 3.3 Subkey Computation Phase

Each participant $U_i \in U$ recovers the subkey $CK_j$ using the received message Mj = $\{T, c_j, d_{j1}', d_{j2}', \ldots, d_{jn}'\}$ according to the following steps:

**Step 1:** Check the time stamp T in advance, if it is invalid, terminate the subkey computation and verification phase;

**Step 2:** Calculate the common session key $k_{ji}$ shared with all other participants $U_j$ using the individual private key $x_i$ and the value $c_j$

$$k_{ij} = c_j^{x_i} \bmod p \bmod q ,\ 1<=j<=n \tag{6}$$

**Step 3:** Calculate the subkey CKj using the session key kji , the values dji′ and cj:

$$d_{ji} = d_{ji}' \oplus k_{ji} ,\ 1<=j<=n \tag{7}$$

$$CK_j = (d_{ji} / y) - c_j \bmod q\ k_{ji} \tag{8}$$

### 3.4 Secret Key Computation Phase

$$\text{Secret key } SK = e(CK_1, CK_2, \ldots\ldots, CK_n) \tag{9}$$

where, e is a linear mapping function.

## 4. SECURITY AND PERFORMANCE ANALYSIS

This section analyzes possible attacks on the conference key agreement protocol. The analysis proves that the protocol to be secure against various attacks such as denial-of-service, man-in-the-middle and replay attacks. Furthermore, a good conference key agreement protocol should be efficient in performance, so costs for computation and transmission have to be taken into consideration in demonstrating efficiency.

### 4.1 Parameter Generation Phase

Key agreement protocols are the common way for two principals to achieve secure communication by establishing a session key to encrypt the data that is being sent between them. These kinds of protocols have a long history; the first known protocol was Diffie-Hellman in 1976. Since, many key agreement protocols have been proposed. These kinds of protocols are one of the hardest to develop. Because key agreement protocols are interactive protocols between two or more parties and that there are many different ways to attack the protocols. Designers are still trying to improve the security of the protocols, but despite of the designers' best effort and intentions some protocols still contain flaws. The development of key agreement protocols is based on try-and-fail. A new protocol is developed which provides good security. Then a weakness is found in the protocol, or a new kind of attack is discovered, and the protocol is not longer safe. The security attributes are updated based on the new knowledge, and the whole process starts again. There is so far no formalized way to develop protocols.

The security of the conference key protocol discussed based on the following assumed problem:

[Discrete logarithm problem assumption]

Let p be a large prime number and q is a large prime factor of p−1, g is a q-order generator over GF (p). Given an integer y that satisfies $y=g^x$ mod p. It is computationally secure to obtain the unknown x from the disclosed y.

Also, the authentication is carried out in two levels such as password-based and identity-based. The password-based authentication is done using one-time verification code and followed with the identity-based authentication. Such authentication schemes provide security against denial-of-service attacks and man-in-the-middle attacks.

The generation of new session keys not only during the member join or leave from the conference as well as between a small interval of time ensures perfect forward secrecy. It means that there is no compromising of long term keys.

Also, since the existing users are invalidated if they did not properly logged out , there is the possibility of eliminating the malicious participants at the beginning of the conference itself.

In addition, the formulated key generation with multiple tables secures the user's information as well.

### 4.2 Performance Analysis

The analysis of performance is divided into analyses of computation costs and transmission costs.

Computation costs include cost of calculating the conference key message. Transmission costs include transmission load of messages broadcasted by each participant. Modular addition, modular subtraction and exclusive OR operations have lower computation costs in opposed to modular multiplication or modular exponential operations; hence their computation costs are ignored to make efficiency estimation easier.

Also, the bilinear mapping imposes a greater computational cost, the mapping is used only in the secret key computation phase.

The secret key computation time taken for various key lengths has been analyzed in Pentium system and given in Table 1.

*Table 1: Key Computation Time*

| Key length (bits) | Computation time (ms) (more frequent at lower bound) |
|---|---|
| 512 | Between 120 & 650 |
| 256 | Between 40 & 150 |
| 128 | < 50 (30 ms. – frequent) |

The secret key computation time will be very negligible in the real time computing environment. The key can be refreshed between smaller time intervals will not affect the system performance. By setting very small time limit improves the perfect forward secrecy.

## 5. CONCLUSION

The proposed method enabled quick generation of conference key which ensures all participants to obtain the same and true conference key. The proposed protocol provides the facility in which the generated secret key is changed based on time period which compromise long term keys.

The proposed protocol ensures that the secret information of users cannot be derived from its corresponding public information and hence it is confidential. Also, the proposed protocol efficiently reduces computation load without compromising on security. Hence the conference key agreement protocol works efficiently in a distributed Internet environment.

## REFRENCES:

[1] J. E. Smith and F. W. Weingarten, Eds., "Research Challenges for the Next Generation Internet", *Computing Research Association, Report from the Workshop on Research Directions for the Next Generation Internet*, May 1997.

[2] W.Diffie and M.Hellman, "New Directions in Cryptography," *IEEE Trans. Information Theory*, vol.22, no. 6, Nov.1976, pp.644-654.

[3] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik, "New multiparty Authentication services and Key agreement protocols" , *IEEE journal on selected areas in communications*,vol. 18, No.4, April 2000.

[4] Marko Holbl, Tatjnana Welzer, and Bostjan Brumen, " Two proposed identity-based three-party authenticated key agreement protocols from pairings", *Computers and Security, ScienceDirect*, 2010.

[5] L.Rivest, A.Shamir, and L.Adleman, "Method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM 21* (1978), 120-126.

[6] E.Okamoto, "Key distribution systems based on identification information, Theory and Applications of Cryptographic Techniques" on *Advances in Cryptology, Lecture Notes in Computer Science*, vol.293, Springer, USA,1988, pp.194-202.

[7] T.Elgamal, "A public key cryptosystem and a signature protocol based on discrete logarithms", *IEEE Trans. on Information Theory* 31 (1985) , 469-472.

[8] PKCS #3, *Diffie-Hellman Key-agreement Standard*, RSA Laboratories, Redwood city, California, November 1993.

[9] American National Standards Institute, Accredited Standards Committee X9 Working Draft, Ansi X9,42-1993, "Public key Cryptography for the Financial Services Industry: Management of Symmetric Algorithm Keys Using Diffie-Hellman", *American Bankers Association*, 1994.

[10] C.Boyd, J.M.G.Nieto, "Round-Optimal Contributory Conference Key Agreement", *Proceedings of the 2003 International Workshop on Practice and Theory in Public-Key Cryptography*, 2003, pp.161-174.

[11] C.Popescu, "A Secure Authenticated Key Agreement Protocol", *Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference*, vol. 2, 2004, pp. 783-786.

[12] Y.Kim, A.Perrig, G.Tsudik, "Simple and Fault-tolerant Key Agreement for Dynamic Collaborative Groups", *Proceedings of the Seventh ACM Conference Computer and Communication Security*, 2000, pp.235-244.

[13] B.E.Jung, "An efficient group key agreement protocol", *IEEE Communication Letters* 10 (2) (2006) 106-107.

[14] P.P.C.Lee, J.C.S.Lui, D.K.Y.Yau, "Distributed collaborative key agreement and authentication protocols for dynamic peer groups", *IEEE / ACM Transactions on Networking* 14 (2) (2006) 263-276.

[15] W.H.Kim, E.K.Ryu, J.Y.Im, K.Y.Yoo, "New conference key agreement protocol with user anonymity", *Computer Standards & Interfaces* 27 (2005) 185-190.

[16] Y.Kim, A.Perrig, G.Tsudik, "Group key agreement efficient in communication", *IEEE Transactions on Computers* 53 (7) (2004) 905-921.

[17] M.Steiner, G.Tsudik, M.Waidner, "Key agreement in dynamic peer groups", *IEEE Transactions on Parallel and Distributed Systems* 11 (8) (2000) 769-780.

[18] Chen L, Cheng Z, Smart NP, "Identity-based key agreement protocols from pairings", *Int J Info Secur* 2007, 6(4), 213-41.

[19] Huang H, Cao Z, "An ID-based authenticated key exchange protocol based on bilinear Diffie-Hellman problem", In: *Proceedings of the ACM ASIACCS 2009, ACM*, 2009, p.333-42.

[20] Augustin P.Sarr, Philippe Elbaz-Vincent, and Jean-Claude Bajard, "A new security model for authenticated key agreement", In *SCN* , 2010, pages 219-234.

[21] Augustin P.Sarr, Philippe Elbaz-Vincent, and Jean-Claude Bajard, "A secure and efficient authenticated diffie-hellman protocol", In *Proceedings of the 6th European conference on Public key infrastructures, services and applications, EuroPKI '09*, Berlin, Heidelberg, Springer-Verlag, 2010, pages 83-98.

[22] D C Lou, H F Huang, "Efficient Three-party Password based Key Exchange Scheme", *International Journal of Communication Systems*, 24(4), 2011, pp.504-512.

[23] T Y Chang, M S Hwang, W P Yang, "A Communication-efficient Three-party Password Authenticated Key Exchange Protocol", *Information Science*, 181(1), 2011, pp.217-226.

[24] Monowar H Bhuyan, D K Bhattacharya, and J K Kalita, "CA-KEP : A Secure CA Based 2-Party Key Exchange Protocol", *Journal of Information Assurance and Security*, ISSN 1554-1010, Volume 7 (2012), pp.193-206.

[25] Mohammad Sabzinejad Farash, Mahmoud Ahmadian Attari, Reza Ebrahimi Atani, and Mohamadreza Jami, "A new efficient authenticated multiple-key exchange protocol from bilinear pairings", *Computers and Electrical Engineering* 39, Elsevier, 2013, pp.530-541.