Group Authentication and Group Key Distribution for Ad Hoc Networks

Feng Wang[1], Chin-Chen Chang[2,3] and Yeh-Chieh Chou[2]
(Corresponding author: Chin-Chen Chang)
Department of Mathematics and Physics, Fujian University of Technology[1]
Fuzhou, Fujian, 350118, China
Department of Information Engineering and Computer Science, Feng Chia University[2]
No. 100, Wenhwa Rd., Seatwen, Taichung, Taiwan 40724, R.O.C.
Department of Computer Science and Information Engineering, Asia University[3]
500, Lioufeng Rd., Wufeng, Taichung, Taiwan 41354, R.O.C.
(Email: alan3c@gmail.com)
(Received Oct. 3, 2014; revised and accepted Nov. 15, 2014)

Abstract

Group authentication and group key distribution ensure the security of group communication. Most existing schemes of group authentication and group key distribution need the assistance of a group manager. However, deciding upon a group manager can be difficult work for some practical applications, especially in an Ad Hoc network. Therefore, we proposed a group authentication and group key distribution scheme that does not require a group manager. Our proposed scheme is an identity-based scheme based on bilinear pairing. In our proposed scheme, any user can easily generate a group for communication purposes. All or part of a group can authenticate each other and obtain a group key without foreknowledge or limiting the number of individuals attending the communication session. Any group member can join or quit the group communication securely in the duration of the meeting. Our proposed scheme requires little communication and computation cost and is resistant to common attacks. Furthermore, in order to take full advantage of the properties of computing ability, which can differ within Ad Hoc networks, our proposed scheme can designate the user with the greatest computing ability to distribute the group key.

Keywords: Ad Hoc networks, bilinear pairing, group authentication, group key distribution

1 Introduction

In recent years, Group communication [3, 16] has become more and more popular in many applications. It involves many-to-many communication, in contrast to the one-to-one or one-to-many communication forums in conventional communication. With this kind of communication, several members of a group can exchange messages to each other securely. To achieve this goal, mutual authentication and sharing of a session key among the group members takes place. The properties of group communication are as follows: 1) The communication users in the group must belong to the same group, 2) the session key sharing among group members needs to be the same, and 3) only group members can get the transmitted message from the group communication.

There are two group communication models for different applications. One group communication model, such as the Wireless Sensor Network [10], only requires group members to authenticate each other. Under the conventional authentication scheme, if there are n members in the group, the user needs to perform authentication for the other users that belong to the group $n-1$ times, for which the time complexity is $O(n)$. In 2013, Harn [7] proposed a group authentication scheme based on Shamir's secret sharing method [17], which facilitates authentication for all users in the group with only a one-time interaction, for which the time complexity is $O(1)$. Under Harn's scheme, a group manager (GM) first registers as a user. Then the users can authenticate each other without the assistance of the GM if they know the number of participants to authenticate.

In the other group communication model, users need to share a session key, such as in the case of a group conference. There are two kinds of methods for sharing a session key in group communication [5]. One is the group key agreement protocol [8], and the other is group key distribution protocol [19]. With regard to group key agreement protocol, all members in the group will consult together to determine and distribute the session key, which requires several rounds of interaction. Although there are some one round group key agreement proto-

cols [22, 23], the group keys generated in those protocols are for Asymmetric cryptosystem, which is not suit for a large number of data encryption. Under group key distribution protocol, a group manager decides the session key. Generally, the latter is more efficient than the former, because in the latter case, the group manager does most of the key distribution work.

However, the models we aforementioned are not suitable for the Ad Hoc network [11, 14] environment. This type of environment does not rely on pre-existing network architecture, and each node in the network has the capability to transmit the message to the other node. Predetermining a group manager (GM) is difficult in this scenario. Therefore, foreknowledge of the number of participants in Harn's scheme [7] or distribution of the session key with the help of the GM present inconveniences. Furthermore, a group member may want to join the group communication after the group communication has begun in some practical applications. However, we did not find a group authentication key setup scheme with a join phase in the process of communication in the reviewed literature.

To solve the problems mentioned above, we proposed an identity-based group authentication and key distribution scheme based on bilinear pairing. The main contributions can be summarized below.

1) Our proposed scheme doesn't need the selection of a group manager, and can designate the user with the most advanced computing ability to distribute group key, therefore, it is suitable for Ad Hoc networks.

2) Our proposed scheme separates the authentication phase from the key distribution phase for different applications.

3) A join phase and revocation phase are employed in our proposed scheme to enable group members to join or leave the meeting before or during the process.

4) Our proposed scheme requires little communication and computation cost. It only calls for two rounds of interaction in the authentication phase and one round of interaction in the key distribution phase. And it require less computation cost compared with Zhang et al.'s scheme [23].

5) Our proposed scheme can fulfill several security requirements, such as mutual authentication, consistency of group key, and perfect forward security. Moreover, the scheme can counteract several well-known attacks, such as impersonation attack, man-in-the-middle attack, and replay attack.

The rest of this paper is given as follows. The preliminaries are provided in Section 2, and we describe our proposed scheme in Section 3. The security analysis is given in Section 4. In Section 5, a comparison with other schemes is given. Lastly, Section 6 gives the conclusion.

2 Preliminaries

In this section, we review some preliminaries including bilinear pairing [15, 20, 21], Diffie-Hellman Assumption [6, 15, 20, 21], and Gentry and Ramzan's identity based multisignature scheme [6].

2.1 Bilinear Pairing

Let G_1 be additive group and G_2 be a multiplicative group with the same prime order q, while P is a generator of G_1 [15, 20, 21]. The map $e : G_1 \times G_1 \longrightarrow G_2$ is called a bilinear map if the following three properties are held:

1) Bilinear: For all $a, b \in Z_q^*$, the equation $e(a \cdot P, b \cdot P) = e(P, P)^{a \cdot b}$ is held.

2) Non-degenerate: $e(P, P) \neq 1$.

3) For any $P_1, P_2 \in G_1$, there is an efficient algorithm to compute $e(P_1, P_2)$.

2.2 Diffie-Hellman Assumption

1) Computational Diffie-Hellman assumption [6].
Given that $a \cdot P, b \cdot P \in G_1$ with $a, b \in Z_q^*$ is unknown, there is no probabilistic polynomial-time algorithm to compute $a \cdot b \cdot P \in G_1$.

2) Bilinear Diffie-Hellman assumption [15, 20, 21].
Given that $P, a \cdot P, b \cdot P, c \cdot P \in G_1$ with $a, b, c \in Z_q^*$ are unknown, there is no probabilistic polynomial-time algorithm to compute $e(P, P)^{a \cdot b \cdot c} \in G_2$ Note that if we know anyone among a, b, c, we can compute $e(P, P)^{a \cdot b \cdot c}$ easily. For example, if we know parameter a, then we can compute $e(P, P)^{a \cdot b \cdot c}$ easily by $e(P, P)^{a \cdot b \cdot c} = e(b \cdot P, c \cdot P)^a$.

2.3 Gentry and Ramzan's Identity-based Multisignature Scheme

A multisignature approach [9] means that there are several signers cooperatively to sign on the same message to generate a single and valid signature, then the verifier can verify the signature using the public key of all of the signers. To combine the multisignature and identity-based cryptosystems [18], Gentry and Ramzan [6] proposed an identity-based multisignature scheme using bilinear pairing in 2006. Their scheme is secure in the random oracle model under the computational Diffie-Hellman assumption. The scheme consists of five phases: setup phase, private key extraction phase, individual signing phase, aggregation phase, and verification phase, which are described in detail as follows.

Setup Phase. The private key generator (PKG) chooses an additive group G_1 and a multiplicative group G_2 with the same prime order q. This also includes an admissible bilinear map $e : G_1 \times G_1 \longrightarrow G_2$, an arbitrary generator P of G_1, and two hash functions

$H_1, H_2 : \{0,1\}^* \longrightarrow G_1$. Then the PKG picks a random number $s \in Z_q^*$ as the master secret key, then computes $P_{pub} = s \cdot P$ and publishes the parameters $(G_1, G_2, q, P, P_{pub}, e, H_1, H_2)$.

Private Key Extraction Phase. Given the user U_i's identity ID_i, the PKG picks its master secret key $s \in Z_q^*$ and computes $SK_i = s \cdot H_1(ID_i)$ as U_i's private key. Then it sends SK_i to U_i via a secure channel.

Individual Signing Phase. Given a message m, the user U_i picks a random number $r_i \in Z_q^*$. Then computes $R_i = r_i \cdot P$ and $\sigma_i = r_i \cdot H_2(m) + SK_i$. Afterward, the couple (R_i, σ_i) is U_i's individual signature of message m.

Aggregation Phase. Anyone who collected n users' individual signatures (R_i, σ_i) of the same message m, for $i = 1, 2, ..., n$, can generate the n users' multisignature (R, σ), where $R = \sum_{i=1}^{n} R_i$, $\sigma = \sum_{i=1}^{n} \sigma_i$.

Verification Phase. Upon receipt of the multisignature (R, σ), the verifier computes $Q = \sum_{i=1}^{n} H_1(ID_i)$ and checks if the equation $e(\sigma, P) = e(R, H_2(m) \cdot e(P_{pub}, Q))$ holds. If so, he/she accepts the multisignature; otherwise, he/she rejects it.

3 The Proposed Scheme

In this section, we propose a group authentication and group key distribution scheme for Ad Hoc networks which are based on bilinear pairing. The scheme can be divided into five phases; i.e., 1) the initialization phase, 2) the group authentication phase, 3) the group key distribution phase, 4) the join phase, and 5) the revocation phase. When the user wants to generate a group to transmit a message, he/she can use the group authentication phase to authenticate the users that belong to the group. Then, the user can use the group distribution phase to distribute the session key to each user. In addition, if there is a new group member who wants to join the communication during the process of the communication, he/she can execute the join phase. Finally, if there is a group member who wants to exit the communication, he/she can execute the revocation phase to release this group member.

3.1 The Initialization Phase

Before communicating with others, a user must perform this phase to obtain his/her private key. The PKG selects the system parameters. The user provides his/her identity to the PKG, and the PKG generates the user's private key and sends it to the user via a secure channel.

Step 1. (Set up) This is identical to the setup phase of Gentry and Ramzan's multisignature in Subsection 2.3, except the PKG chooses a symmetric encryption/decryption algorithm E/D and a group key space GK, and publishes the parameters (E, D, GK) also.

Step 2. (Private key extraction) This is identical to the private key extraction phase of Gentry and Ramzan's multisignature in Subsection 2.3.

3.2 The Group Authentication Phase

Suppose a user U_1 wants to generate a group with n users including him- or herself. He/She broadcasts the request. Let $U = \{U_1, U_2, ..., U_n\}$ denote n users, m denote the purpose, and T denote the current time. There are $t-1$ users who respond to the activity, denoted by $U_2, ..., U_t$ They can perform the following steps for authentication. We give an example for $t = 4$ to explain this phase in Figure 1 too.

Step 1. The initiator user U_1 first picks a random number $r_1 \in Z_q^*$, then computes $R_1 = r_1 \cdot P$, $h = H_2(m||U||T)$, and $\sigma_1 = r_1 \cdot h + SK_1$. After that, (R_1, σ_1, m, U, T) is broadcast to all n users.

Step 2. After the other users receive the message, each user $U_i, (i = 2, 3, ..., t)$ picks a random number $r_i \in Z_q^*$, then computes $R_i = r_i \cdot P$, $h = H_2(m||U||T)$, and $\sigma_i = r_i \cdot h + SK_i$. After that, the message (R_i, σ_i, m, U, T) is broadcast to all t users.

Step 3. For $i = 1, 2, 3, ..., t$, each user U_i computes $R = \sum_{i=1}^{t} R_i$, $\sigma = \sum_{i=1}^{t} \sigma_i$, and $Q = \sum_{i=1}^{t} H_1(ID_i)$. Then he/she checks to determine if the equation $e(\sigma, P) = e(R, h) \cdot e(P_{pub}, Q))$ holds. If so, the t users accept the procedure, and otherwise, terminate the procedure.

3.3 The Group Key Distribution Phase

Note that the users computing abilities are different from each other in Ad Hoc networks. Therefore, after having succeeded in the group authentication phase, the initiator user U_1 to designate one user $U_j, (1 \leq j \leq t)$ who has the greatest computing ability to distribute the group key. Without loss of generality, we assume that user U_1 performs the group key distribution work, and he/she distributes the group key in the following two steps. Furthermore, we give an example for $t = 4$ to explain this phase in Figure 2.

Step 1. The initiator, user U_1, picks a random number $gk \in GK$ as the group key. For $i = 2, 3, ..., t$, User U_1 computes $k_i = e(r_1 \cdot R_i, R_{[(i-1) \bmod (t-1)]+2})$, $gk' = U_1||T||gk$, and $c_i = E_{k_i}(gk')$ and broadcasts c_i to all other $t-1$ users.

Step 2. After receiving the message, for $i = 2, 3, ..., t$,

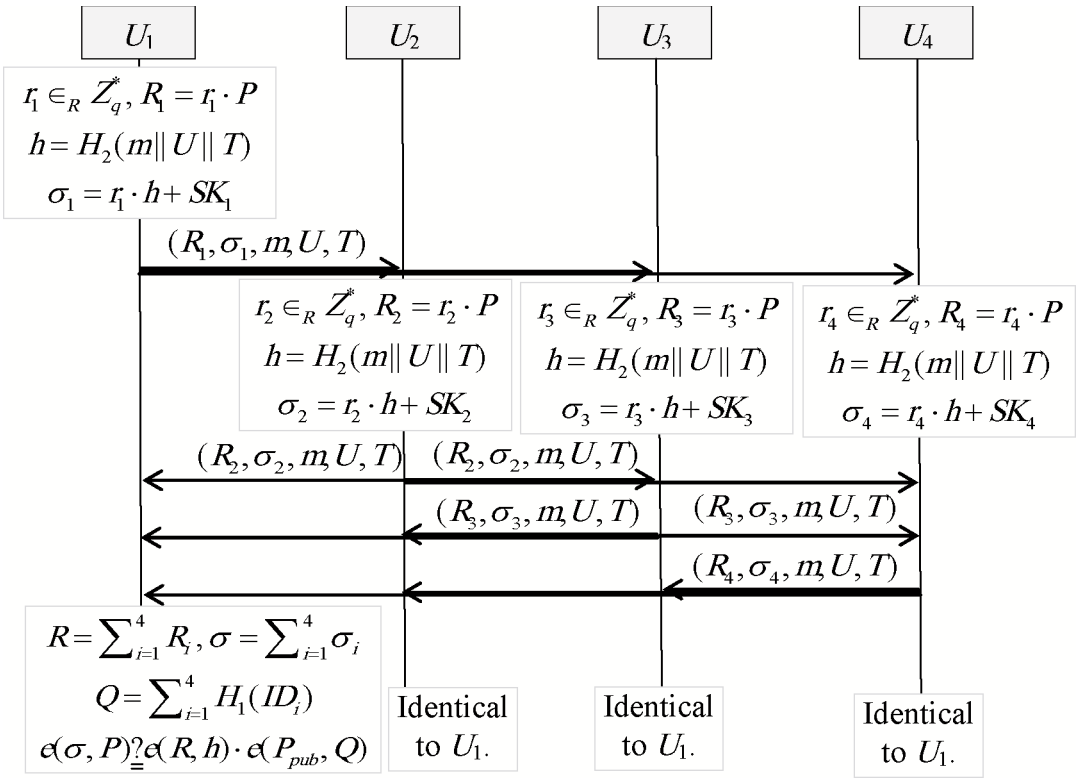

Figure 1: The proposed scheme

each user U_i computes

$$\begin{aligned} k_i' &= e(r_i \cdot R_1, R_{[(i-1) \bmod (t-1)]+2}), \\ gk_i' &= D_{k_i'}(c_i), \\ k_i'' &= e(r_i \cdot R_1, R_{[(i-3) \bmod (t-1)]+2}), \\ gk_i'' &= D_{k_i''}(c_{[(i-3) \bmod (t-1)]+2}). \end{aligned}$$

Then each user U_i checks to see if the equation $gk_i' = gk_i''$ holds and U_1, T are correct. If so, he/she can share the group key gk, and otherwise terminate the procedure. Note that gk, U_1, T satisfies $gk_i' = U_1||T||gk$ or $gk_i'' = U_1||T||gk$.

3.4 The Join Phase

Suppose that there is a user $U_j \in U$ who doesn't attend the group communication at the beginning of the communication for some reason, and he/she wants to join the communication of $\{U_1, U_2, ..., U_t\}$ during the process of the communication. The user U_j can execute the join phase and attend the communication without knowing the content of the previous communication. We describe this phase below and provide an example for U_5 attending the group communication of $\{U_1, U_2, U_3, U_4\}$ to explain this phase in Figure 3.

Step 1. User U_j picks a random number $r_j \in Z_q^*$ and then computes $R_j = r_j \cdot P$, $h_j = H_2(m||U||T||T_j)$, and $\sigma_j = r_j \cdot h_j + SK_j$. After that, this user broadcasts the message $(R_j, \sigma_j, m, U, T, T_j)$ to users $U_1, U_2, ..., U_t$, who have begun the communication, where T_j is the current time.

Step 2. For $i = 1, 2, ..., t$, each user U_i computes $h_j = H_2(m||U||T||T_j)$ and checks if the timestamp T_j is fresh and the equation $e(\sigma_j, P) = e(R_j, h_j) \cdot e(P_{pub}, H_1(ID_j))$ holds. If so, he/she accepts and performs Step 3; otherwise, he/she terminates the procedure.

Step 3. After that, user U_1 picks a new random number $gk_{new} \in GK$ as a group key. Then he/she computes $c = E_{gk}(U_1||T_j||gk_{new})$, $k_{2,j} = e(r_1 \cdot R_j, R_2)$, $c_{2,j} = E_{k_{2,j}}(U_1||T_j||gk_{new})$, $k_{t,j} = e(r_1 \cdot R_j, R_t)$, and $c_{t,j} = E_{k_{t,j}}(U_1||T_j||gk_{new})$ and broadcasts $c, c_{2,j}, c_{t,j}$ to all $t+1$ users.

Step 4. For $i = 2, 3, ..., t$, each user U_i computes $D_{gk}(c)$. Then user U_2 computes $k_{2,j}' = e(r_2 \cdot R_j, R_1)$ and checks whether the equation $D_{gk}(c) = D_{k_{2,j}'}(c_{2,j})$ holds. User U_t computes $k_{t,j}' = e(r_t \cdot R_j, R_1)$ and checks whether the equation $D_{gk}(c) = D_{k_{t,j}'}(c_{t,j})$ holds. User U_j computes $k_{t,j}'' = e(r_j \cdot R_t, R_1)$ and $k_{2,j}'' = e(r_j \cdot R_2, R_1)$ and checks to determine whether the equation $D_{k_{2,j}''}(c_{2,j}) = D_{k_{t,j}''}(c_{t,j})$ holds. If all of the equation holds and U_1, T is correct, the $t+1$ users can share the group key gk_{new}, and otherwise, terminate the procedure.

The Revocation Phase. If a user U_k who wants to leave the group communication, the remaining users

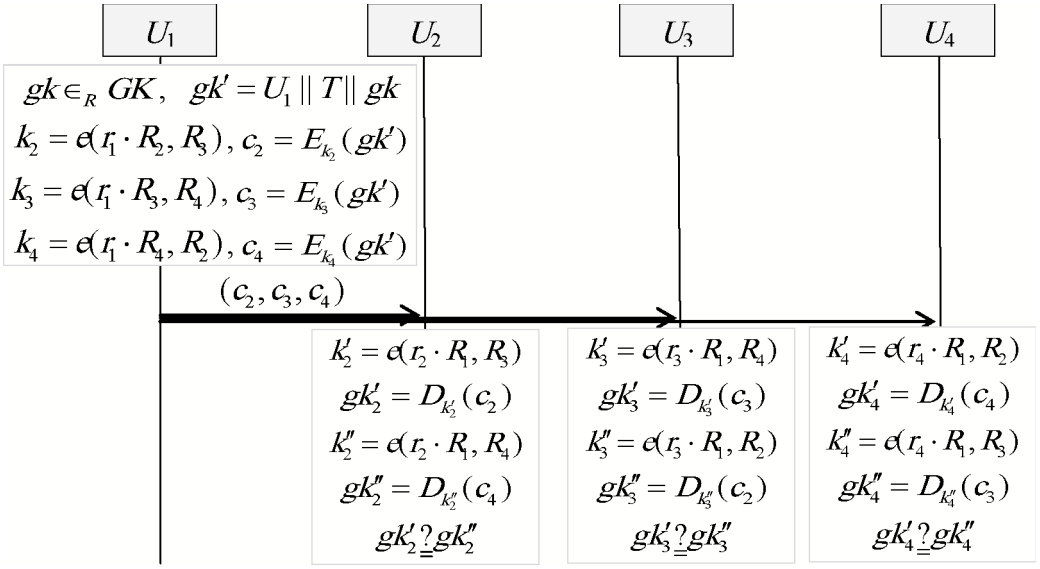

Figure 2: The example of group key distribution phase

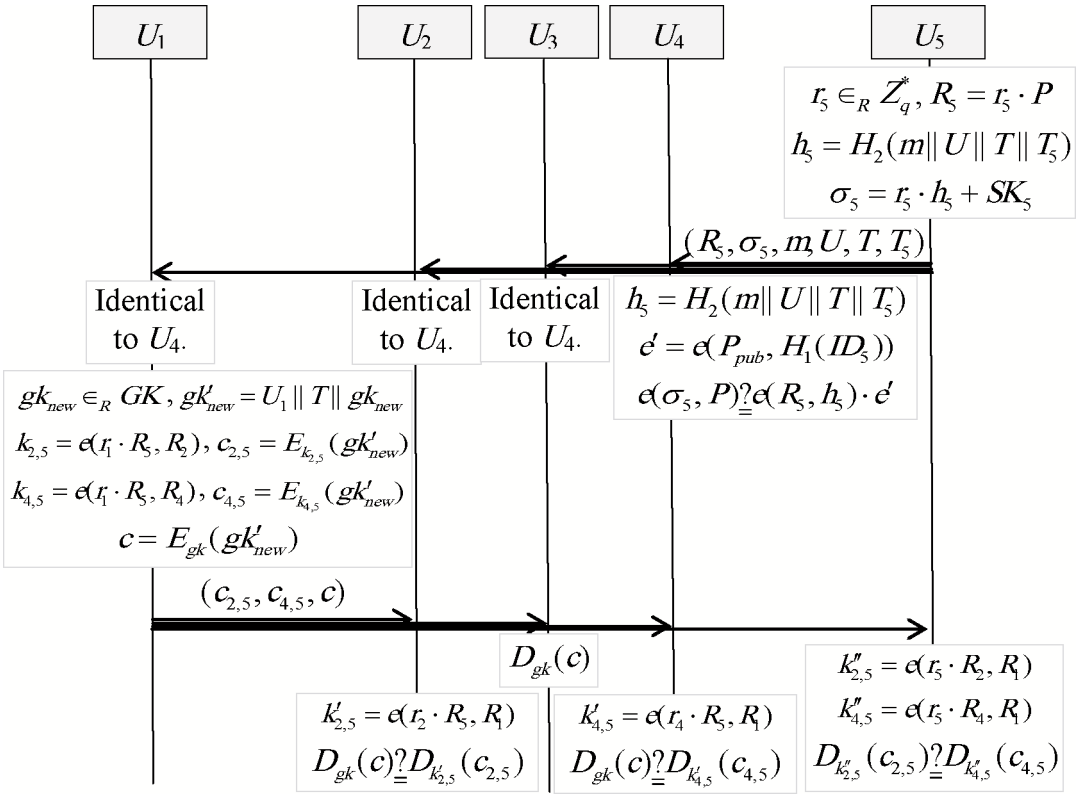

Figure 3: The example of join phase

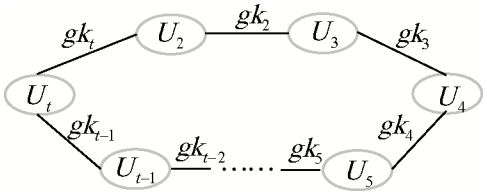

Figure 4: Ring generated by the authenticated group members

perform the group key distribution phase to reinstitute a new group key. Thus, user U_k cannot know the content of the remaining users' communication.

4 Security Analysis

In this section, we analyze several secure requirements that our proposed scheme possesses; i.e., mutual authentication, consistency of the group key, perfect forward security, withstanding the impersonation attack, withstanding the man-in-the-middle attack, and withstanding the replay attack.

4.1 Mutual Authentication

Mutual authentication means that each group member who attends the group authentication must authenticate the validity of all of the other users. The (R, σ) is actually $m||U||T$'s multisignature signed by users $U' = \{U_1, U_2, ..., U_t\}$ during Step 3 of the group authentication phase in our proposed scheme according to [6]. Each user U_i checks the validity of all the other users U' by verifying the multisignature. Any adversary cannot forge the multisignature (R, σ), according to Theorem 1 in [6]. Therefore, the scheme achieves mutual authentication.

4.2 Consistency of the Group Key

The consistency of the group key means that the group key obtained by each group member is identical. All of the authenticated group members (except the distributer) generate a ring described in Figure 4 in the group key distribution phase of our scheme. In Step 2 of the group key distribute phase, each member U_i can obtain two group keys, gk_i and $gk_{[(i-3) \bmod (t-1)]+2}$, which are equal to the value of one of the adjacent members in Figure 4. Therefore, our scheme can ensure the consistency of the group key by each member U_i checking the equality of gk_i and $gk_{[(i-3) \bmod (t-1)]+2}$. Furthermore, the group members can detect that the distributer allocates a different group key even if she/he colludes with one member U_k.

4.3 Perfect Forward Security

Perfect forward security refers to the inability of the adversary to obtain any previous group key, even if she/he knows all the participants private keys [2, 24]. For $i = 1, 2, ..., t$, if an adversary knows user U_i's private key SK_i and the interaction record including R_i and c_i, she/he cannot obtain the group key gk. The R_i is generated by $R_i = r_i \cdot P$, where r_i is selected randomly and kept secret by U_i; Therefore, the adversary cannot compute $k' = e(r_i \cdot R_1, R_{[(i-1) \bmod (t-1)]+2})$ and $k'' = e(r_i \cdot R_1, R_{[(i-3) \bmod (t-1)]+2})$, without knowing r_i, and hence cannot obtain group key gk by computing $D_{k'_i}(c_i)$ or $D_{k''_i}(c_{[(i-3) \bmod (t-1)]+2})$. Therefore, our scheme maintains perfect forward security.

4.4 Withstanding the Impersonation Attack

In Harn's group authentication scheme [7], there are two types of adversaries, including outside attackers and inside attackers. The group management generates a group with n members. The outside attacker tries to impersonate a valid group member to bypass the group authentication. The inside attacker is actually a group member who tries to obtain the secret information of the group.

In our scheme, there is no secret information of the group except each member's private key, so we consider the outside attacker only. However, without knowing user U_i's private key, anyone cannot forge the user U_i's signature. Therefore, it is impossible for anyone to impersonate a valid group member and pass the group authentication.

4.5 Withstanding the Man-in-the-Middle Attack

In the man-in-middle attack, attacker Eve interrupts, eavesdrops, and modifies the message between users Alice and Bob and builds a channel with each one. After that, Alice and Bob still believe that they are in direct communication with each other and in a private channel.

Fortunately, even attacker Eve can change the message R_i to R'_i, She still cannot achieve the purpose because the R'_i cannot pass the multisignature verification. Therefore, our scheme can resist the man-in-the-middle attack.

4.6 Withstanding the Replay Attack

Replay attack refers to the attempt by an adversary to imitate a group member in order to pass the group authentication by replaying the eavesdropped foregone message in group communication. In our scheme, a timestamp is added as a part of signed message in the group authentication phase. The user can resist the replay attack by checking whether the timestamp is fresh. This is the same as in the group key distribute phase. For this reason, our scheme can resist the replay attack.

5 Comparison

In this section, we give the comparison with Harn's group authentication scheme [7], Zhang et al.'s group key agree-

Table 1: Features comparison with the other schemes

Scheme	F1	F2	F3	F4	F5	F6	F7	F8
Harn's [7]	Y	N	Y	Y	-	Difficult	N	Shamir's secret sharing [17]
Zhang et al.'s [23]	N	N	N	N	N	Difficult	Y	CDH and k-BDHE [4]
Liu et al.'s [12]	Y	Y	N	Y	N	Difficult	N	Asmuth and Bloom's secret sharing [1]
Our	N	N	N	N	N	Easy	Y	Gentry and Ramzan's multisignature [6]

F1: Whether needs a group manager to setup the group.
F2: Whether needs a group manager to attend in the group authentication phase or the group key distribution phase.
F3: Whether needs to foreknow the number of members.
F4: Whether needs to limit the least number.
F5: Whether allows to be added or reduced the members in the process of group communication.
F6: Adding or revoking member from the group.
F7: Whether the scheme is an identity based scheme.
F8: What cryptography tool is based on.

Table 2: Efficiency comparison of group key generated with the other scheme

Scheme	Communication rounds	Computation efficiency	Type of generated group key
Zhang et al.'s [23]	1	8 pairing operations	Asymmetric cryptosystem
Liu et al.'s [12]	5	-	Symmetric cryptosystem
Our	1	2 pairing operations	Symmetric cryptosystem

ment protocol [23], and Liu et al.'s group key distribution scheme [12]. The features of those schemes are compared in Table 1. Our proposed scheme does not need a group manager to set up the group or attend the group authentication phase or group key distribution phase. In addition, it is not necessary to foreknow or limit the number of members who attend the group authentication or group key distribution in our proposed scheme. In our proposed scheme, anyone can initiate a group for communication easily. If a member of the group delays attendance of the group communication, he/she can join the group communication late without knowing the previous communication content. If there is a member who wants to quit the meeting, he/she can exit without knowing the later content. Furthermore, our proposed scheme is an identity-based scheme. Therefore, our proposed scheme is more flexible for practical application, especially in the Ad Hoc networks.

As for the efficiency of the group key generated in our scheme, we compare it in Table 2. Note that Harn's group authentication scheme does not give the algorithm for generating the group key, therefore we compare our scheme with Zhang et al.'s group key agreement protocol [23] and Liu et al.'s group key distribution scheme [12] only. Usually, a step of communication is more costly than a step of local computation [13]. Our scheme and Zhang et al.'s group key agreement protocol need 1 communication round compared with 5 communication rounds in Liu et al.'s group key distribution scheme, and therefore are more efficient. So we don't give the computation cost of Liu et al.'s group key distribution scheme. Each user in our scheme needs 2 pairing operations compared with 8 pairing operations in Zhang et al.'s protocol. Although the group key dealer needs $t-1$ pairing operations in our scheme, those operations can be pre-computed. Furthermore, the generated group key in our scheme is for symmetric cryptosystem, which is suit for a large number of data encryption than asymmetric cryptosystem generated in Zhang et al.'s protocol. Therefore, our scheme is more efficient than the other two schemes.

6 Conclusions

In this paper, we proposed a group authentication and key distribution scheme for Ad Hoc networks which is based on bilinear pairing. In our proposed scheme, any user can easily generate a group for communication without a group manager. All or part of the group members can complete the authentication and group key distribution without foreknowledge or limit to the number of members who attend the communication. Any group member can join or quit the group communication easily in the process of the communication without leaking the content of the communication. Our proposed scheme is an identity-based scheme, with little communication and computation cost, properties of mutual authentication, consistency of the group key and perfect forward security, and resistance to impersonation attack, man-in-the-middle attack, and replay attack. Furthermore, our scheme can designate the user with the greatest comput-

ing ability to distribute the group key, which is suitable for the property of computing power asymmetry in the Ad Hoc network environment.

References

[1] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. IT-29, no. 2, pp. 208-210, 1983.

[2] A. K. Awasthi and S. Lal, "A remote user authentication scheme using smart cards with forward secrecy," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1246-1248, Nov. 2003.

[3] B. Bruhadeshwar and S. S. Kulkarni, "Balancing revocation and storage trade-offs in secure group communication," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 1, pp. 58-73, Feb. 2011.

[4] D. Boneh, X. Boyen, E. J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Proceedings of EUROCRYPT 2005*, Aarhus, Denmark, pp. 440-456, May, 2005.

[5] C. Boyd, "On key agreement and conference key agreement," in *Proceedings of Second Australasian Conference on Information Security and Privacy*, Sydney, Australia, pp. 294-302, July 1997.

[6] C. Gentry and Z. Ramzan, "Identity-based aggregate signatures," in *Proceedings on 9th International Conference on Theory and Practice in Public-Key Cryptography (PKC'2006)*, New York, USA, vol. 3958, pp. 257-273, Apr. 2006.

[7] L. Harn, "Group authentication," *IEEE Transactions on Computers*, vol. 62, no. 9, pp. 1893-1898, 2013.

[8] D. He, J. Chen and J. Hu, "A pairing-free certificateless authenticated key agreement protocol," *International Journal of Communication Systems*, vol. 25, no. 2, pp. 221-230, 2012.

[9] S. K. H. Islam and G. P. Biswas, "Certificateless short sequential and broadcast multisignature schemes using elliptic curve bilinear pairings," *Journal of King Saud University - Computer and Information Sciences*, vol. 26, no. 1, pp. 89-97, Jan. 2014.

[10] C. T. Li, M. S. Hwang and Y. P. Chu, "An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks", *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 8, pp. 2107-2124, Aug. 2009.

[11] C. T. Li, M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless Ad hoc networks", *Information Sciences*, vol. 181, no. 23, pp. 5333V5347, Dec. 2011.

[12] Y. J. Liu, L. Harn and C. C. Chang, "An authenticated group key distribution mechanism using theory of numbers," *International Journal of Communication Systems*, vol. 27, no. 11, pp. 3502-3512, Nov. 2014.

[13] W. Mao, Modern Cryptography: Theory and Practice, Publishing House of Electronic Industry, Beijing, China, 2004.

[14] S. A. E. Mohamed, "Secure position verification approach for wireless Ad-hoc networks," *International Journal of Network Security*, vol. 15, no. 4, pp. 248-255, July 2013.

[15] J. Nam, Y. Lee, S. Kim and D. Won, "Security weakness in a three-party pairing-based protocol for password authenticated key exchange," *Information Sciences*, vol. 177, no. 6, pp. 1364-1375, Mar. 2007.

[16] P. Sakarindr and N. Ansari, "Survey of security services on group communications," *IET Information Security*, vol. 4, no. 4, pp. 258-272, Dec. 2010.

[17] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, Nov. 1979.

[18] A. Shamir, "Identity based cryptosystems and signature schemes," in *Proceedings of CRYPTO'84 on Advances in Cryptology*, Santa Barbara, California, U.S.A., vol. 196, pp. 47-53, Aug. 1984.

[19] A. T. Sherman and D. A. McGrew, "Key establishment in large dynamic groups using one-way function trees," *IEEE Transactions on Software Engineering*, vol. 29, no. 5, pp. 444-458, 2003.

[20] Y. L. Tian, C. G. Peng, and J. F. Ma, "Publicly verifiable secret sharing schemes using bilinear pairings," *International Journal of Network Security*, vol. 14, no. 3, pp. 142-148, May 2012.

[21] L. H. Wang, J. Shao, Z. F. Cao, M. Mambo, A. Yamamura, and L. C. Wang, "Certificate-based proxy decryption systems with revocability in the standard model," *Information Sciences*, vol. 247, pp. 188-201, Oct. 2013.

[22] Q. Wu, Y. Mu, W. Susilo, B. Qin and J. Domingo-Ferrer, "Asymmetric group key agreement," in *Proceedings of EUROCRYPT 2009*, Cologne, Germany, pp. 153-170, Apr. 2009.

[23] L. Zhang, Q. Wu, B. Qin and J. Domingo-Ferrer, "Provably secure one-round identity-based authenticated asymmetric group key agreement protocol," *Information Sciences*, vol. 181, no. 19, pp. 4318-4329, 2011.

[24] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and ú. González-Nicolás, "Asymmetric group key agreement protocol for open networks and its application to broadcast encryption," *Computer Networks*, vol. 55, pp. 3246-3255, 2011.

Feng Wang was born in Shandong province, China, in 1978. He received his B.S. degree in Mathematics from Yantai Normal University (now named Ludong University), Yantai, in 2000 and the M.S. degree in Applied Mathematics from the Guangzhou University, Guangzhou, in 2006. Currently, he is a Lecturer in the Department of Mathematics and Physics at Fujian University of Technology and a visiting scholar in Department of Information Engineering and Computer Science at Feng Chia University. His research interests

include computer cryptography and information security.

Chin-Chen Chang received his Ph.D. degree in computer engineering from National Chiao Tung University. His first degree is Bachelor of Science in Applied Mathematics and master degree is Master of Science in computer and decision sciences. Both were awarded in National Tsing Hua University. Dr. Chang served in National Chung Cheng University from 1989 to 2005. His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005. Prior to joining Feng Chia University, Professor Chang was an associate professor in Chiao Tung University, professor in National Chung Hsing University, chair professor in National Chung Cheng University. He had also been Visiting Researcher and Visiting Scientist to Tokyo University and Kyoto University, Japan. During his service in Chung Cheng, Professor Chang served as Chairman of the Institute of Computer Science and Information Engineering, Dean of College of Engineering, Provost and then Acting President of Chung Cheng University and Director of Advisory Office in Ministry of Education, Taiwan. Professor Chang has won many research awards and honorary positions by and in prestigious organizations both nationally and internationally. He is currently a Fellow of IEEE and a Fellow of IEE, UK. On numerous occasions, he was invited to serve as Visiting Professor, Chair Professor, Honorary Professor, Honorary Director, Honorary Chairman, Distinguished Alumnus, Distinguished Researcher, Research Fellow by universities and research institutes. His current research interests include database design, computer cryptography, image compression and data structures.

Yeh-Chieh Chou was born in Taichung, Taiwan, in 1990. He received his Bachelor's Degree in Information Engineering form Chang Jung Christian University, Tainan. Currently, he is the second grade student for master's program of Department of Information Engineering in Feng Chia University. His research interests include computer cryptography and information security.