This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2008 proceedings.

Anonymous ID-based Group Key Agreement for Wireless Networks

Zhiguo Wan*, Kui Ren†, Wenjing Lou‡ and Bart Preneel*
* K.U.Leuven, ESAT/SCD, Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
Email: {zhiguo.wan,bart.preneel}@esat.kuleuven.be
† Illinois Institute of Technology, Chicago, IL, Email: kren@ece.iit.edu
‡ Worcester Polytechnic Institute, Worcester, MA, Email: wjlou@ece.wpi.edu

***Abstract*—Popularity of group-oriented applications motivates research on security and privacy protection for group communications. A number of group key agreement protocols exploiting ID-based cryptosystem have been proposed for this objective. Though bearing beneficial features like reduced management cost, private key delegation from ID-based cryptosystem, they have not taken into account privacy issues during group communication. In wireless networks, the privacy problem becomes more crucial and urgent for mobile users due to the open nature of radio media. In this paper, we proposed an anonymous ID-based group key agreement protocol for wireless networks. Based on ID-based cryptosystem, our protocol not only benefits from the desirable features of ID-based cryptosystem, but also provides privacy protection for mobile users. More important, in the proposed protocol, the computation cost for each group member is largely reduced to meet the computation capability restriction of mobile devices.**

I. Introduction

As group-oriented applications like collaborative workspaces, teleconferencing, interactive multi-user games etc. are gaining popularity, security and privacy problems in group communication become an increasing concern for users. As the world is going wireless and ubiquitous, these problems become urgent more than ever. A lot of research efforts have been spent on group key management protocols based on different cryptosystems, however, the privacy problem remains relatively untouched until now. In existing protocols, any group member's identity is exposed to everyone, including outside eavesdroppers. This information, though not so important in the wired network, can be exploited by an adversary to trace a mobile user, find out a specific user's movement pattern etc. in the wireless environment. How can a group of mobile users to construct a secure meeting session without others knowing who are in the meeting? How can they make sure the users in the meeting are indeed those expected group members? To achieve these goals, the group key agreement protocol should be able to protect mobile users' identity during the protocol execution.

Group key agreement protocols enable a group of users to agree on a session key to secure their communication. Unlike group key distribution protocols in which the group session key is generated by a centralized server and distributed to all group members, group key agreement protocols construct the session key from shared contributed from every group member. As a result, group key agreement protocols avoid single point of failure, and they can provide perfect forward secrecy to avoid information leakage in case of long-term key compromise.

Recently, a number of group key agreement protocols based on ID-based cryptosystems have been proposed in the literature, and they still exhibit impressive advantages of ID-based cryptosystems. In these protocols, the group member does not have to check any certificate as in traditional public key cryptosystems. And since the public key of a member is just his identity, no large public key database is required any more. Unfortunately, these protocols are designed without consideration of privacy protection, and identities of group members are all disclosed during the protocol execution.

In this paper, we analyze existing ID-based group key agreement protocols, and discuss their weaknesses and design flaws. Then we present an anonymous ID-based group key agreement protocol for wireless networks. Our protocol not only preserves the good features inherited from ID-based cryptosystems, but also keeps group members anonymous to outside eavesdroppers. To our best knowledge, this is the first ID-based group key agreement protocol providing privacy protection. In our protocol, we assume each user registers at a trusted server and obtains his private ID-based key. An initiator can send a request to the expected group members calling for a private meeting session. All the information the initiator has to know are identities of other users he wants to include in the meeting. By a similar session key construction method as the BD protocol [1], [2], but with substantially reduced computation cost, our protocol can establish the group session key with only 3 rounds.

The rest part of the paper is organized as follows. Related work on ID-based group key agreement protocols are discussed in Section II. Then after we present the network model, security requirements and the adversary model in Section III, the anonymous ID-based group key agreement protocol is described in Section IV. We then analyze its security and privacy as well as performance, and we draw the conclusion at the end.

II. Related Work

Existing authenticated group key agreement protocols using the ID-based cryptosystem, pairing, or the ECC cryptosystem, can be classified into three groups according to the structure

used in the group key construction: 1) the protocols based on the TGDH tree structure [3], 2) those based on the Burmester and Desmedt mechanism [1], and 3) those without special internal structure. The TGDH structure used in group key agreement can reduce computation cost from n to $\log n$, but it needs $\log n$-round communication. The BD mechanism can better make user of the broadcast media in wireless networks to construct the group key in constant rounds.

The first group of ID-based authenticated group key agreement protocols includes [4], [5], [6], [7], [8], [9]. The scheme in [4] is the first ID-based authenticated group key agreement protocol. It makes use of a binary key tree structure, and has similar computation complexity as the TGDH protocol. On the other hand, the protocol [4] achieves authentication with the ID-based cryptosystem, hence avoids management of certificates. But during the protocol, identities of group members are transmitted in clear, and no privacy protection is available.

The protocol proposed in [5] is also a TGDH-based protocol, but it is extended from the tripartite protocol proposed by Joux [10]. Hence it uses a trinary key tree structure different from the binary key tree used in TGDH. It is worth to note the protocol does not provide authentication, just like Joux's protocol.

The protocol in [6] is an authenticated extension of the Joux protocol, and its security has been formally proved in the paper. The authentication is achieved by combining signatures with the key tree structure. An extension in dynamic scenarios of this protocol is proposed by the same authors in [7], also with a formal proof. But the privacy protection is not considered in either protocol.

Also based the TGDH tree structure, Wu et al. [8] proposed an ID-based authenticated group key agreement protocol, but the protocol is later shown to be vulnerable to the impersonation attack [11]. The attack can cause the group members to not able to agree on a common session key. The protocol also adopts the TGDH structure, but it is based on a certificateless cryptosystem, which is a variant of ID-based cryptosystems. It has better computation and communication efficiency.

Schemes proposed in [12], [13], [14], [15] fall in the second type of protocols. Two ID-based authenticated group key agreement protocols [12], [13] are designed based on the BD mechanism [1]. More or less similar to each other, these two schemes are shown to fail to achieve authentication by Zhang and Chen [16], [17]. In the attack presented in [16], two colluding adversaries can impersonate as a valid member in a new protocol execution if they have previous execution transcripts of that valid member. To resist this collusion attack, a method using a synchronized counter has been proposed in [14], but the cost of this solution is the additional synchronization mechanism. A similar scheme [15] is also based on the BD mechanism, but it requires ECC certificates for authentication.

The remaining protocols have no special structure, and they belong to the third category, including [18]. The group key agreement protocol proposed in [18] is based on a variant of ID-based cryptosystems. The group key can be constructed within only one round, and computation cost is also less than other protocols. This is achieved by using a slightly different ID-based key setting, in which two master secrets are used instead of only one in normal ID-based cryptosystems. Unfortunately, the protocol is deprived of all advantages of ID-based encryption by the special setting. One's public key is no longer the identity, and it must be computed and published like traditional PKC systems. Moreover, the drawback of this one-round protocol is lack of authentication on the messages, though the protocol is claimed to be an authenticated protocol. An adversary can impersonate as a group member to send out a message without being detected, and this would make the group not able to construct a group key.

III. Network Model, Security Requirements and Adversary Model

A. Network Model

The network model assumed in this protocol is a wireless network in which a broadcast channel is shared in the network. Due to the broadcast nature of the radio media, a message can be broadcast in the network with only one transmission. Hence, the proposed protocol should take advantage of this feature of the wireless network for better performance. The wireless network can be a multihop ad hoc network, or a WLAN, as long as broadcast messages can be efficiently delivered. If it is a multihop ad hoc network, then we assume that the anonymous routing mechanism is already in place in the network. The source can find a route to an expected destination with such an anonymous routing mechanism, like [19].

B. Security Requirements

We first analyze security requirements in order to provide a better solution for the problem. The basic security requirements for the group key agreement protocol—authentication,confidentiality,integrity—should be fulfilled in the first place. In the case of group communications, the security problem becomes much more complex than two-party communication. When dynamic group membership events happen, a previous group member should not be able to access the group communication any more, while a later group member cannot access group communication content before he joins the group. Hence, the security solution should provide group *forward secrecy*, *backward secrecy*.

As privacy is becoming an increasing concern nowadays, a good group key agreement protocol should be designed with privacy protection in mind. A group member's identity should be protected from the eavesdropper, so that he is unable to trace or monitor activities of a specific user. Moreover, an outside adversary should not be able to link the same user in two group communication sessions.

In summary, the security requirements of the group key agreement protocol, in addition to the basic security requirements, are listed as follows:

- Anonymity: A group member's identity should be protected from outside eavesdroppers.
- Unlinkability: A group member's activities in two different group key agreement sessions are unlinkable to the outside adversary.
- Group Forward Secrecy: A previous group member should have no access to group communication content any more.
- Group Backward Secrecy: A group member should have no access to group communication content that happens before he joins the group.
- Perfect Forward Secrecy: Previous group session keys should be still secured even if the long-term secrets are compromised by the adversary. Note this requirement is essentially different from *group forward secrecy*.

C. Adversary Model

We assume a globally passive attacker that is capable of eavesdropping traffic of the entire wireless network. The attacker can eavesdrop, inject, modify, drop messages within the network at will. However, the attacker has only bounded computation capability, and is not capable of breaking the ID-based encryption system. That is, the ECDH problem and the BDH problem are assumed to be hard.

IV. Anonymous ID-based Group Key Agreement Protocol for Wireless Networks

In this section, we describe our group key agreement protocol based on ID-based encryption. Based on the BD mechanism and ID-based encryption cryptosystems, this scheme provides better user-friendliness since the public keys are users' identities. It does not require certificate and avoids difficulty of certificate revocation. Moreover, it offers flexibility on delegation of private keys.

A. System Setup

We assume a trusted server S is responsible for private key generation for users in the system. The server selects two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of order q for some large prime q (160-bit long). A bilinear mapping $\hat{e}$: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ maps a pair from $\mathbb{G}_1$ to $\mathbb{G}_2$. The mapping satisfies the following properties:

1) Bilinear: $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is bilinear if $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$ and all $a, b \in \mathbb{Z}$.
2) Non-degenerate: There exists a pair $P, Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq 1$.
3) Computable: An efficient algorithm to compute $\hat{e}(P, Q)$ exists for any $P, Q \in \mathbb{G}_1$

A generator $P \in \mathbb{G}_1$ and a master secret $s \in \mathbb{Z}_q^*$ are also randomly chosen by the server. The server computes a public value $P_{pub} = sP$, and publishes the public parameters $\langle q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub}, H_1 \rangle$ to all users in the system, where H_1 is a hash function. The private key generated by the server for a user with identity U_i is $sH_1(U_i)$, while the corresponding public key is just the user's identity U_i.

In the system, we assume the hardness of bilinear Diffie-Hellman problem:

Bilinear Diffie-Hellman Problem:
Given $\langle P, aP, bP, cP \rangle$ for some $a, b, c \in \mathbb{Z}_q^*$, to compute $W = \hat{e}(P, P)^{abc} \in \mathbb{G}_2$.

A number of notations used in the report are listed in the following table:

U_i	The ith user
$E_i(*)$	ID-based encryption using U_i's identity as the public key
$E_K(*)$	Symmetric encryption with K
Nym_i	Pseudonym for user U_i
r_i	Random number selected by U_i
SIG_i	Signature computed over the corresponding message by U_i
h	A hash function mapping from $\mathbb{G}_2 \times \mathbb{G}_1 \rightarrow \{0,1\}^k$, where k is the security parameter.

B. The ID-based Group Key Agreement Scheme

Suppose a user U_1, the initiator of the protocol, knows a set of users $U_2, U_3, ..., U_n$ and wants to have a private session with them. Since U_1 knows all the users' identities, she knows these users' public key as well. So she starts the session in the following steps:

1) User U_1 as the session initiator chooses a pseudonyms Nym_i for user U_i and a random number r_1. Then U_1 encrypts a concatenation of all users' identities and pseudonyms with their public keys respectively, i.e. their identities. At the end, she sends each user the following request:

$$U_1 \rightarrow U_i : E_i(U_1||U_2||...||U_n||Nym_1||Nym_2|| ...||Nym_n||SIG_1), r_1P. \quad (1)$$

   The ID-based encryption used in this message must be anonymous, which means it is impossible to identify the intended recipient from the ciphertext and the public key. SIG_1 is computed over the respective message by U_1 with its private key.
2) After user $U_i, (i \neq 1)$ receives the request from U_1, he does a series decryption trial using his private key to check if he is one of the users requested by U_1. If he successfully decrypts one ciphertext and finds out his identity is in the ID list, then he looks for his Nym_i and sends the following message to U_{i-1} and U_{i+1}:

$$U_i \rightarrow U_{i-1}, U_{i+1} : Nym_i, r_iP, \quad (2)$$

   where r_i is a random number chosen by U_i.
3) When U_i receives the above messages from U_{i-1} and U_{i+1}, he first verifies that these are U_{i-1} and U_{i+1}'s pseudonyms according to the pseudonym list he decrypted in message (1). If the verification is successful, he calculates two keys using his private key $s \cdot H_1(U_i)$ as follows:

$$k_i = h(\hat{e}(H_1(U_{i+1}), sH_1(U_i))||r_i r_{i+1} P),$$

$$k_{i-1} = h(\hat{e}(H_1(U_{i-1}), sH_1(U_i))||r_i r_{i-1} P),$$

Then U_i computes $X_i = k_i/k_{i-1}$ and broadcast the following message to all the other users:

$$U_i \rightarrow * : Nym_i, X_i = k_i/k_{i-1}. \quad (3)$$

Otherwise, he just ignores the message. In this message, the division operation as well as the subsequent multiplication is computed modulo p.

4) U_i waits until he receives all $X_j (j \neq i)$, and checks the pseudonyms $Nym_j (j \neq i)$ are valid. Then he computes $k_{i+1} = k_i X_{i+1}$, $k_{i+2} = k_{i+1}X_{i+2}$,...,$k_{i+n-1} = k_{i+n-2}X_{i+n-1}$. U_i verifies $k_{i+n} = k_{i+n-1}X_{i+n} = k_i$. Then U_i computes the group session key as $K = H(k_1||k_2||k_3||...||k_n)$, where H is defined from $\{0,1\}^*$ to $\{0,1\}^k$. Finally, each user $U_i (i \neq 1)$ sends $H(K||U_1||U_2||...||U_n)$ to U_1, and U_1 verifies all other users derive the same group key K by checking $H(K||U_1||U_2||...||U_n)$.

In above messages, all subscript number of identities are calculated modulo n, i.e. $U_0 = U_n$, $U_1 = U_{n+1}$, etc. And as stated earlier, the multiplication operations are performed modulo p.

C. Group Member Join

Suppose $U_1, U_2, ..., U_n$ are having a private meeting using the protocol described above. Now U_1, the initiator of the meeting, wants another user U_{n+1} to join the group meeting. U_1 can start the group member joining process as follows:

1) U_1 informs U_n and U_{n+1} about U_{n+1}'s joining. He sends the following messages to U_n and U_{n+1} respectively:

$$U_1 \rightarrow U_n : E_n(U_{n+1}||Nym_{n+1}||SIG_1), \quad (4)$$

$$U_1 \rightarrow U_{n+1} : E_{n+1}(U_1||Nym_1||r_1P$$

$$||U_n||Nym_n||r_nP||U_{n+1}||Nym_{n+1}||SIG_1). \quad (5)$$

2) U_{n+1} receives the invitation from U_1, then he decrypts the message using his private key to retrieve his pseudonym selected by U_1. After that, he chooses a random number r_{n+1}, and computes $k_{n+1} = h(\hat{e}(H_1(U_1), sH_1(U_{n+1}))||r_{n+1}r_1P)$ and $k'_n = h(\hat{e}(H_1(U_n), sH_1(U_{n+1}))||r_{n+1}r_nP)$. He calculates $X_{n+1} = k_{n+1}/k'_n$ and sends the following message to both U_1 and U_{n+1}:

$$U_{n+1} \rightarrow U_1, U_n : Nym_{n+1}, r_{n+1}P, X_{n+1}. \quad (6)$$

3) After U_1 and U_n receives the above message from U_{n+1}, they can compute $k_{n+1} = h(\hat{e}(H_1(U_{n+1}), sH_1(U_1))||r_1r_{n+1}P)$ and $k'_n = h(\hat{e}(H_1(U_{n+1}), sH_1(U_n))||r_nr_{n+1}P)$, respectively. Then they compute $X'_1 = k_1/k_{n+1}$ and $X'_n = k'_n/k_{n-1}$. U_n sends X'_n to U_1:

$$U_n \rightarrow U_1 : X'_n, \quad (7)$$

and U_1 sends the following message to U_{n+1}:

$$U_1 \rightarrow U_{n+1} : E_{n+1}(X'_1||X_2||...||X_{n-1}||X'_n). \quad (8)$$

U_1 also broadcast the following message to all other members:

$$U_1 \rightarrow * : E_K(X'_1||X_{n+1}||X'_n||SIG_1). \quad (9)$$

An important point of this protocol is that a member should join a group anonymously, i.e. without disclosing which group he wants to join. Therefore, we should not send out X_i, Nym_i in clear in the group member joining protocol, since they have been sent in the group key agreement protocol in plaintext. Otherwise the attacker can link the group member joining protocol and the group key agreement protocol by X_i.

D. Group Member Leave

Now we discuss how to deal with group member leaving. If a group member leaves the private meeting, and he should not access the conference content after that, then the group key should be updated accordingly.

Let's say U_i is leaving the group, and the group key should be updated for the remaining $n-1$ users. The protocol runs as follows to update the group key:

1) U_1 informs U_{i-1} and U_{i+1} that U_i is leaving, and they should recompute their k_{i-1} and k_i respectively.

$$U_1 \rightarrow U_{i-1}, U_{i+1} : E_K(U_i||Nym_i||$$

$$U_{i-1}||Nym'_{i-1}||U_{i+1}||Nym'_{i+1}||SIG_1) \quad (10)$$

This message is encrypted with the old group key, and the message is signed by U_1.

2) U_{i-1} and U_{i+1} receive the message from U_1 and verifies the signature's validity. If the verification is successful, U_{i-1} and U_{i+1} exchange their random value r'_{i-1} and r'_{i+1}.

$$U_{i-1} \rightarrow U_{i+1} : Nym'_{i-1}, r'_{i-1}P \quad (11)$$

$$U_{i+1} \rightarrow U_{i-1} : Nym'_{i+1}, r'_{i+1}P \quad (12)$$

Then they calculate the new k'_{i-1} and k'_i respectively:

$$k'_{i-1} = h(\hat{e}(H_1(U_{i+1}), sH_1(U_{i-1}))||r'_{i-1}r'_{i+1}P),$$

$$k'_i = h(\hat{e}(H_1(U_{i-1}), sH_1(U_{i+1}))||r'_{i+1}r'_{i-1}P).$$

In above equations, $k'_{i-1} = k'_i$ since U_i leaves the group.

3) Then they calculate $X'_{i-1} = k'_{i-1}/k_{i-2}$, $X'_{i+1} = k_{i+1}/k'_i$, then they sends X'_{i-1} and X'_{i+1} to U_1.

$$U_{i-1} \rightarrow U_1 : X'_{i-1}, \quad (13)$$

$$U_{i+1} \rightarrow U_1 : X'_{i+1}. \quad (14)$$

4) U_1 broadcasts X'_{i-1}, X'_{i+1} to all other users, and they compute the new group key.

$$U_1 \rightarrow * : E_K(U_i||U_{i-1}||U_{i+1}||X'_{i-1}||X'_{i+1}||SIG_1). \quad (15)$$

The new group key is computed as $K' = H(k_1||k_2||...||k'_{i-1}||k_{i+1}||...||k_n)$.

Similar to the group member joining process, we intend to protect privacy on who is leaving which group. Therefore, previously used pseudonyms should not be reused in group

member leaving. In group member leaving protocol, new pseudonyms Nym'_{i-1} and Nym'_{i+1} are generated by U_1 to ensure anonymity. U_{i-1} and U_{i+1} themselves generate random numbers r'_{i-1} and r'_{i+1} to avoid reusing r_{i-1} and r_{i+1}.

E. Discussion

In this section, we present a detailed analysis on the security and privacy of the protocol. Specifically, we analyze the anonymity, unlinkability, group key secrecy, group forward/backward secrecy, and perfect forward secrecy of the protocol.

Anonymity In messages of this scheme, identities are either encrypted so that no identity-related information is leaked, or there is impossible to infer any information from the messages. In the first message, identities of users are encrypted using ID-based encryption with their public keys, and we require the encryption scheme be anonymous so that it is impossible to obtain any information from only the ciphertext. Nym_i in the second message is selected by U_1 and obtained by U_i by decrypting the first message, itself does not leak information on its identity. Since an adversary knows all these Nym_i, he may want to guess the users' identities and verify his guess by message(1). However, it is impossible to do that as we use an anonymous encryption scheme. From message (3), the adversary knows X_i which are calculated from users' identities and private keys. Though X_i contains identity information, the adversary cannot retrieve any of them without knowing the master secret s or a user's private key $sH_1(U_i)$.

Unlinkability Anonymity would be meaningless without unlinkability. The adversary can still trace an unknown user without knowing his real identity given only anonymity. In our protocol, including the joining/leaving protocol, we use different pseudonyms for users in every independent execution of the protocol. A pseudonym is never reused, and cannot be used to link two different protocol executions.

Group Key Secrecy The final session key for all group members $K = H(k_1||k_2||...||k_n)$ is computed from each k_i, which is generated from each user's private key. An attacker has to obtain at least one k_i in order to compromise the group session key. In the case of our protocol, an attacker even doesn't know identities of group users, but only the random numbers r_i. Hence the attacker is unable to compute the correct k_i without identities U_i. Even if the attacker knows the identities of group users, he still has to obtain the master secret or the private key of a user to calculate k_i. Under the BDH assumption, it is impossible to obtain k_i without knowing the master secret or the private key, which guarantees group key secrecy of our scheme. Furthermore, our protocol ensures that all group members derive the same group key at the end, which means group key confirmation is guaranteed in the protocol.

Group Forward/Backward Secrecy When a group member leaves the group or a new user joins the group, the protocol should guarantee group forward/backward secrecy. In our protocol, this is achieved by the group member joining protocol and the group member leaving protocol. Whenever group membership is changed because a user joins or leaves the group, the group key is updated and the new group key is unrelated to the old one. As a result, a new group member cannot decrypt previous communication content, and an old group member cannot decrypt communication content encrypted by the new group key.

Perfect Forward Secrecy As discussed earlier, perfect forward secrecy represents security in case of long-term secret compromise. In our protocol, perfect forward secrecy is achieved from hardness of the ECDHP problem. Even if the master secret is compromised by the adversary, without the ephemeral secret r_i, r_{i+1} the adversary cannot compute $r_i r_{i+1} P$ under the ECDHP assumption.

F. Performance Analysis

Group Key Agreement Process We first look at the communication cost of the group key agreement protocol. The protocol comprises of three messages in the four steps. The first message is unicast to each of other $n-1$ users, which is n unicast in total. For the second message, each user unicast a message to two other users, and this results in $2n$ unicast. Each user then broadcast the third message to all other users, which are n broadcast in total.

As for the computation cost, we only consider ID-based encryption, pairing computation and point multiplication. U_1 has to calculate 1 signature and do $n-1$ ID-based encryption. Then every other user U_i has to decrypt the first message sent from U_1, and computes $r_i P$ from a random number r_i. After that, they need to compute k_i and k_{i-1} which cost 2 pairing computation and 2 point multiplication.

Group Member Joining Process During the group member joining process, there are 6 unicast messages and 1 broadcast message. To compute a new group key, U_1 has to do 3 ID-based encryption and 1 pairing computation. U_n needs to do 1 ID-based decryption, 1 pairing computation, and 1 division. U_{n+1} has to do 2 ID-based decryption, 2 pairing computation, 1 division, and n multiplication to derive the group key.

Group Member Leaving Process The group member leaving process requires 6 unicast messages and 1 broadcast message. When U_i leaves the group, U_1 as the initiator has to compute 2 signature, and U_{i-1} and U_{i+1} verify the signature sent from U_1 independently. U_{i-1} and U_{i+1} also has to do 1 pairing computation and 1 division respectively. Every other users verifies the signature from U_1 and then derives the new group key.

The following table gives a comparison between our protocol and three other ID-based group key agreement protocols. It can be seen from the table that our protocol has comparable efficiency in terms of computation and communication.

V. CONCLUSION

In this paper, we presented a comprehensive review of existing ID-related group key agreement protocols, and proposed a new ID-based group key agreement scheme with privacy protection in wireless networks. The proposed scheme achieves anonymity, group key secrecy, forward/backward secrecy for the group session key. It can establish a group key within

TABLE I
COMMUNICATION AND COMPUTATION COST COMPARISON

	Rounds	Computation	Communication
Our protocol	3	$(1\mathcal{D}+2\mathcal{P}+1\mathcal{V}+3\mathcal{M})n$	$4n$
CAGAKE-KE [9]	$\log n$	$3n\mathcal{P}$	$4n-4$
ID-AGKA [4]	$\log n$	$(2n-2)\mathcal{P}$	$4n-4$
ID-EGKA [12]	2	$4n\mathcal{P}$	$2n$

$\mathcal{D}$-Encryption/Decryption, $\mathcal{P}$-Pairing computation, $\mathcal{V}$-Signature verification, $\mathcal{M}$-Point Multiplication,

only three rounds. And it supports dynamic membership, and group members can join/leave the group. More important, all these tasks can be accomplished anonymously without leaking information on who is joining/leaving the group.

ACKNOWLEDGEMENT

This work was supported in part by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government and by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy). Zhiguo Wan is supported in part by a research grant of the IBBT (Interdisciplinary institute for BroadBand Technology) of the Flemish Government.

REFERENCES

[1] M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution System," in *Proceedings of EUROCRYPT'94*, vol. LNCS 950, 1994, pp. 275–286.
[2] N. P. Smart, "Identity-based authenticated key agreement protocol based on weil pairing," *Electronics Letters*, vol. 38, no. 13, 2002.
[3] Y. Kim, A. Perrig, and G. Tsudik, "Simple and Fault Tolerant Key Agreement for Dynamic Collaborative Groups," in *Proceedings of ACM Conference on Computer and Communications Security'00*, 2000, pp. 235–244.
[4] K. C. Reddy and D. Nalla, "Identity Based Authenticated Group Key Agreement Protocol," in *Proceedings of INDOCRYPT'02*, vol. LNCS 2551, 2002, pp. 215–233.
[5] S. Lee, Y. Kim, K. Kim, and D.-H. Ryu, "An Efficient Tree-based Group Key Agreement using Bilinear Map ," in *Proceedings of ACNS'03*, vol. LNCS 2846, 2003, pp. 357–371.
[6] R. Barua, R. Dutta, and P. Sarkar, "Provably Secure Authenticated Tree Based Group Key Agreement Protocol Using Pairing," in *Proceedings of ICICS'04*, vol. LNCS 3269, 2004, pp. 92–104.
[7] R. Dutta and R. Barua, "Dynamic Group Key Agreement in Tree-Based Setting," in *Proceedings of ACISP'05*, vol. LNCS 3574, 2005, pp. 101–112.
[8] S.-T. Wu, J.-H. Chiu, and B.-C. Chieu, "Identity-Based Key Agreement for Peer Group Communication from Pairings," *IEICE Trans. Fundamentals*, vol. E88-A, no. 10, pp. 2762–2768, October 2005.
[9] S. Heo, Z. Kim, and K. Kim, "Certificateless Authenticated Group Key Agreement Protocol for Dynamic Groups," in *Proceedings of Globecom'07*, 2007.
[10] A. Joux, "The Weil and Tate Pairings as building blocks for public key cryp- tosystems," in *5th International Symposium on Algorithm Number Theory*, vol. LNCS 2369, 2002, pp. 20–32.
[11] D.-L. Vo and K. Kim, "Security Analysis of an ID-based Key Agreement for Peer Group Communication," *IEICE Trans. on Fundamentals*, 2007.
[12] K. Y. Choi, J. Y. Hwang, and D. H. Lee, "Efficient ID-based Group Key Agreement with Bilinear Maps," in *Proceeding of 2004 International Workshop on Practice and Theory in Public Key Cryptography (PKC04)*. Springer-Verlag, 2004.
[13] X. Du, Y. Wang, J. Ge, and Y. Wang, "Id-based authenticated two round multi-party keyagreement," 2003.
[14] ——, "An Improved ID-based Authenticated Group Key Agreement Scheme," IACR ePrint Archive Report 2003/260, 2003.
[15] L. Zhu, L. Liao, W. Li, and Z. Zhang, "An Authenticated Constant Round Group Key Agreement Protocol Based on Elliptic Curve Cryptography ," *International Journal of Computer Science and Network Security*, vol. 6, no. 8B, 2006.
[16] F. Zhang and X. Chen, "Attack on Two ID-based Authenticated Group Key Agreement Schemes," IACR ePrint Archive Report 2003/259, 2003.
[17] ——, "Attack on an ID-based authenticated group key agreement scheme from PKC 2004," *Information Processing Letters*, vol. 91, pp. 191–193, 2004.
[18] Y. Shi, G. Chen, and J. Li, "ID-Based One Round Authenticated Group Key Agreement Protocol with Bilinear Pairings," in *Proceedings of International Conference on Information Technology: Coding and Computing*, 2005.
[19] J. Kong and X. Hong, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks," in *ACM MOBIHOC'03*, 2003, pp. 291–302.