An Improved ID-based Authenticated Group Key Agreement Scheme

Xinjun Du, Ying Wang, Jianhua Ge and Yumin Wang
Key Laboratory of Computer
Networks and Information Security
Xidian University
Xi'an 710071, P.R. China

Abstract. Authenticated group key agreement problem is important in many modern collaborative and distributed applications. There are two ID-based authenticated group key agreement schemes have been proposed by Choi *et al*. and us, which are based on bilinear pairings and BD scheme. Recently, Zhang and Chen propose an impersonation attack on the two schemes, which means the schemes are not fully authenticated. In this paper, we propose an improved ID-based authenticated group key agreement scheme which can resist this attack.

Keywords: Authenticated group key agreement, Bilinear pairings, Identity-based cryptography

1. Introduction

A group key agreement protocol allows a group of users to share a key which may later be used to achieve some cryptographic goals. Authenticated group key agreement problem is important in many modern collaborative and distributed applications. Since Shamir [1] asked for identity-based encryption and signature scheme to simplify key management procedures in certificated-based public key infrastructure, many ID-based cryptosystem schemes have been proposed [2], among which there are several ID-based key agreement protocols[3,4,5,6]. Recently, we propose a bilinear variant of Burmester and Desmedt scheme [7] in [8] for multi-party key agreement. Similar scheme is proposed by Choi, Hwang and Lee [9]. However, an impersonation attack on the two schemes is proposed by Zhang and Chen [10], in which any two malicious users can impersonate a user if there two malicious users have the authentication transcripts of this user. So, the two schemes can not provide the authenticity.

In this paper, we propose an improved ID-based authenticated group key agreement scheme. In this scheme, each user in a group holds a synchronous counter, which is increased by one after a successful group key agreement. The improved scheme can resist the collusive impersonation attack [10], and dose not increase the computation and communication cost enormously.

2. The two previous ID-based authenticated group key agreement Schemes

We first review the two ID-based authenticated group key agreement schemes in brief. Both of the schemes take advantage of the Hess's ID-based signature scheme [11] to assure the authenticity.

2.1 ID-based Public Key Infrastructure

The schemes are based on the ID-based Public Key Infrastructure, which involves a Key Generation Center (KGC) and users. The basic operations consist of **Set Up** and **Private Key Extraction**. KGC generates the system parameters $params = \{G_1, G_2, q, P, P_{pub}, H, H_1\}$, here G_1 is a cyclic additive group with order q and G_2 is a cyclic multiplicative group with the same order q. $e: G_1 \times G_1 \to G_2$ is a bilinear pairing. H, H_1 are two cryptographic hash

functions, $H:\{0,1\}^* \to \mathbb{Z}_q^*, H_1:\{0,1\}^* \to G_1$.

— **Set Up**: KGC chooses a random number $s \in \mathbb{Z}_q^*$ and set $P_{pub} = sP$, and keeps s as master-key, which is know only by itself.

— **Private Key Extraction**: A user submits his identity information ID to KGC. KGC computer the user's public key as $Q_{ID} = H_1(ID)$, and returns his private key $S_{ID} = sQ_{ID}$ as his private keys.

Let $ID_1, ..., ID_n$ be the users which are going to agree to some session keys and each has a unique identifier $ID_i, 1 \le i \le n$. With the ID-based public key infrastructure, each user has its public key and private key: $Q_i = H_1(ID_i)$ and $S_i = sQ_i$. The pair (Q_i, S_i) is the ID_i's static key pairs.

2.2 Our previous scheme

-Round 1. Each user ID_i computes and broadcasts $< z_i = N_i P, T_i = H(z_i)S_i + N_i P_{pub} >$ to all others and keeps $N_i \in \mathbb{Z}_q^*$ secret.

-Round 2. Each entity ID_i verifies:

$$e(\sum_{j\in\{1,...,n\}\setminus\{i\}} T_j, P) = e(\sum_{j\in\{1,...,n\}\setminus\{i\}} (H(z_j)Q_j + z_i), P_{pub}).$$

Then, it computes and broadcasts $X_i = e(P_{pub}, N_i(z_{i+1} - z_{i-1}))$.

-Key Computation. Each user ID_i now computes the session key:

$$K = e(P_{pub}, nN_i z_{i-1}) \cdot X_i^{n-1} \cdot X_{i+1}^{n-2} \cdots X_{i-2} = e(P,P)^{(N_1N_2 + N_2N_3 + \cdots N_nN_1)s}.$$

2.3 Choi *et al.*'s Scheme

Choi *et al.*'s scheme is similar with ours, but in Round 2 the verification equation is:

$$e(T_{i-1} + T_{i+1} + T_{i+2}, P) = e(\sum_{j=\{i-1,i+1,i+2\}} H(z_j)Q_j + z_j, P_{pub}),$$

and $X_i = e(-N_i z_{i-1}, z_{i+1}) \cdot e(N_i z_{i+1}, z_{i+2})$. The result session key is:

$$K = e(nN_i z_{i-1}, z_{i+1}) \cdot X_i^{n-1} \cdot X_{i+1}^{n-2} \cdots X_{i-2} = e(P,P)^{N_nN_1N_2 + N_1N_2N_3 + \cdots + N_{n-1}N_nN_1}.$$

3. The Impersonation Attack

The impersonation attack against the two schemes is proposed by Zhang and Chen in [10]. Assume the user A had agreed some session key in group $\mathcal{G}_\infty$ before and his authentication transcript (z_A, T_A) can be obtained by any one. Suppose B, C obtained this information and then they can collude to impersonate A to agreement some session keys in a new group $\mathcal{G}_\in$ or a new group key agreement protocol in $\mathcal{G}_\infty$ (B, C can block A's communications). In our previous scheme, the transcript (z_A, T_A) can satisfy the verification in Round 2, and the computation of X_i is not only able to be computed by user ID_i, but also computed by ID_{i-1}, ID_{i+1}, this is because of

$$\begin{aligned} X_i &= e(P_{pub}, N_i(z_{i+1} - z_{i-1})) \\ &= e(N_i P, s(z_{i+1} - z_{i-1})) \\ &= e(z_i, (N_{i+1} - N_{i-1})P_{pub}) \end{aligned}$$

. Then ID_{i-1}, ID_{i+1} can impersonate ID_i to share a group session key without being detected by other users in group $\mathcal{G}_\infty$ or $\mathcal{G}_\in$. Analogously in Choi *et al.*'s scheme, X_i can be computed by ID_{i-1}, ID_{i+2}, and with ID_i's previous authentication transcript, ID_{i-1}, ID_{i+2} can impersonate ID_i.

4. The Improved ID-based Authenticated Group Key Agreement Scheme

In this section we propose an improved scheme using synchronous counters held by the group members based on our previous scheme. Each user in the group held a counter, of which the initial value is 1, and after a successful key agreement, counters are increased by 1. The improved scheme is as follows:

-Round 1. First, each user ID_i updates its private key $S_i = c(sQ_i)$, where c is the current value of the counter. Then, it computes and broadcasts $< z_i = N_i P, T_i = H(z_i)S_i + N_i P_{pub} >$ to all others and keeps $N_i \in \mathbb{Z}_q^*$ secret.

-Round 2. Each entity ID_i verifies:

$$e(\sum_{j \in \{1,\ldots,n\} \setminus \{i\}} T_j, P) = e(\sum_{j \in \{1,\ldots,n\} \setminus \{i\}} (H(z_j)cQ_j + z_i), P_{pub}).$$

Then, it computes and broadcasts $X_i = e(P_{pub}, N_i(z_{i+1} - z_{i-1}))$.

-Key Computation. Each user ID_i now computes the session key:

$K = e(P_{pub}, nN_i z_{i-1}) \cdot X_i^{n-1} \cdot X_{i+1}^{n-2} \cdots X_{i-2} = e(P,P)^{(N_1N_2+N_2N_3+\cdots N_nN_1)s}$, and updates the value of the counter to $c+1$.

From the improved scheme we can see the user ID_i's previous authentication transcript (z_i, T_i) can not satisfy the verification in the following key agreement or in a different group, because the ID_i's static key pair (Q_i, S_i) is updated according to the value of the counter at the beginning of the next key agreement procedure. Other security attributes are not affected by the existing of the counters. Compared with the previous scheme, the computation cost is increased by only one scalar multiplication.

5. Conclusion

In the improved ID-based authenticated group key agreement scheme, each user in a group holds a synchronous counter, which is increased by one after a successful group key agreement, and the users' static key pairs are updated along with the counters. This measure can resist the collusive impersonation attack [10], however, dose not increase the computation and communication cost enormously. One defect of the scheme is that group members must keep loose synchronization. If groups are dynamic, new users' counters must keep up with that of the group members.

Reference

[1] A. Shamir. Identity-based cryptosystems and signature schemes. Advances in Cryptology-Crypto 84, LNCS 196, pp.47-53, Springer-Verlag, 1984.

[2] Martin Gagne. Identity-Based Encryption: a Survey. RSA Laboratories Cryptobytes, Vol. 6, No. 1, Spring 2003.

[3] S. Al-Riyami and K. Paterson. Authenticated three party key agreement protocols from pairings. Cryptology ePrint Archive, Report 2002/035, available at http://eprint.iacr.org/2002/035.

[4] F. Zhang, S. Liu and K. Kim. ID-Based One Round Authenticated Tripartite Key Agreement Protocol with Pairings. Cryptology ePrint Archive, Report 2002/122, 2002.

[5] L. Chen and C. Kudla. Identity Based Authenticated Key Agreement from Pairings. Cryptology ePrint Archive, Report 2002/184, 2002.

[6] N. Smart. An Identity Based Authenticated Key Agreement Protocol Based on the Weil Pairings. Electronics Letter, Vol 38, pp 630-632, 2002.

[7] Mike Burmester and Yvo Desmedt. A secure and efficient conference key distribution system. In I.B.Damgard, editor, Advances in Cryptology-EURO-CRYPT'94, Lecture Notes in Computer Science, Springer-Verlag, Berlin Germany, 1994.

[8] X. Du, Y. Wang, J. Ge and Y. Wang. ID-based Authenticated Two Round Multi-Party Key

Agreement, Cryptology ePrint Archive: Report 2003/247.

[9] K. Y. Choi, J. Y. Hwang and D. H. Lee. Efficient ID-based Group Key Agreement with Bilinear Maps, 2004 International Workshop on Practice and Theory in Public Key Cryptography (PKC2004, IACR).

[10] Fangguo Zhang and Xiaofeng Chen. Attacks on Two ID-based Authenticated Group Key Agreement Schemes. Cryptology ePrint Archive: Report

[11] F. Hess. Exponent Group Signature Schemes and Efficient Identity Based Signature Schemes Based on Pairings. Cryptology ePrint Archive, Report 2002/012, 2002.