Attack on Two ID-based Authenticated Group Key Agreement Schemes

Fangguo Zhang[1] and Xiaofeng Chen[2]

[1] School of Information Technology and Computer Science
University of Wollongong, NSW 2522 Australia
fangguo@uow.edu.au
[2] International Research center for Information Security (IRIS)
Information and Communications University(ICU),
58-4 Hwaam-dong Yusong-ku, Taejon, 305-732 KOREA
crazymount@icu.ac.kr

Abstract. Authenticated group key agreement problem is important in many modern collaborative and distributed applications. Recently, there are two ID-based authenticated group key agreement schemes have been proposed, one is Choi *et al.*'s [2] scheme, the other is Du *et al.*'s [3] scheme. They are all constructed from bilinear pairings based on Burmester and Desmedt scheme [1]. In this paper, we propose an impersonation attack on the two schemes. We show that any two malicious users can impersonate an entity to agree some session keys in a new group if these two malicious users have the previous authentication transcripts of this entity. So, the two ID-based authenticated group key agreement schemes can not provide the authenticity as claimed. We propose a proposal to repair these schemes.

Keywords: *Authenticated group key agreement, Bilinear pairings, ID-based cryptography, Attack*

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. In addition to this basic tool an authentication mechanism provides an assurance of key-sharing with intended users. A protocol achieving these two goals is called an authenticated group key agreement protocol. In many modern collaborative and distributed applications, authenticated group key agreement problem is important. Recently, Choi, Hwang and Lee [2] proposed two group key agreement schemes which use bilinear pairings: one is a bilinear variant of Burmester and Desmedt scheme [1] and the other is ID-based authenticated scheme based on the former protocol. Similar scheme is proposed by Du, Wang, Ge and Wang [3]. However, in this paper, we propose an attack on the two ID-based authenticated group key agreement schemes. We show that any two malicious users can impersonate an entity to agree some session keys in a new group if these two malicious users have the previous authentication transcripts of this entity. So, these schemes can not provide the authenticity in some situations. We propose a proposal to repair these schemes.

2 Choi *et al.*'s and Du *et al.*'s ID-based Authenticated Group Key Agreement Schemes

We first review Choi *et al.*'s and Du *et al.*'s ID-based authenticated group key agreement schemes in brief.

The system parameters are $\{\mathbb{G}_1, \mathbb{G}_2, e, q, P, H, H_1\}$, here $\mathbb{G}_1$ is a cyclic additive group generated by P, whose order is a prime q, and $\mathbb{G}_2$ is a cyclic multiplicative group with the same order q. $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is a bilinear pairing. H, H_1 are two cryptographic hash functions, $H : \{0,1\}^* \rightarrow \mathbb{Z}_q$ and $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$.

- **Setup:** The Key Generation Center (KGC) chooses a random number $s \in \mathbb{Z}_q^*$ and sets $P_{pub} = sP$, and keeps s as the *master-key*, which is known only by itself.
- **Extraction:** A user submits his identity information $ID \in \{0,1\}^*$ to KGC. KGC computes this user's public key as $Q_{ID} = H_1(ID)$, and returns $S_{ID} = sQ_{ID}$ as his private keys.

Let $U_1, U_2, \ldots, U_n (n > 2)$ be a set of users who want to establish a session key. $ID_1, ID_2, \ldots, ID_n$ are identities of $U_1, U_2, \ldots, U_n$, respectively. The indices are subject to modulo n. U_i's long-term public key and private key are $\langle Q_i = H_1(ID_i), S_i = sQ_i \rangle$.

Choi *et al.***'s Scheme:**

- **Round 1.** Each user U_i picks a random integer $a_i \in \mathbb{Z}_q^*$ and computes $P_i = a_iP$, $h_i = H(P_i)$ and $T_i = a_iP_{pub} + h_iS_i$. Each user U_i broadcasts $\langle P_i, T_i \rangle$ to all others and keeps a_i secret.
- **Round 2.** Upon the receipt of $\langle P_{i-1}, T_{i-1} \rangle$, $\langle P_{i+1}, T_{i+1} \rangle$ and $\langle P_{i+2}, T_{i+2} \rangle$, each user U_i verifies as follows:

$$\begin{aligned} & e(T_{i-1} + T_{i+1} + T_{i+2}, P) \\ &= e(P_{i-1} + P_{i+1} + P_{i+2} + h_{i-1}Q_{i-1} + h_{i+1}Q_{i+1} + h_{i+2}Q_{i+2}, P_{pub}) \end{aligned}$$

  If the above equation is satisfied, then U_i computes

$$D_i = e(a_i(P_{i+2} - P_{i-1}), P_{i+1})$$

  and broadcasts D_i to all others. Otherwise U_i stops.
- **Key Computation.** Each user U_i computes the session key,

$$K_i = e(a_iP_{i-1}, P_{i+1})^n D_i^{n-1} D_{i+1}^{n-2} \cdots D_{i-2}.$$

About the correctness of key computation and the security analysis of the scheme refer to [2].

Du *et al.***'s Scheme:**

- **Round 1.** Each user U_i broadcasts $\langle Z_i = N_i P,\ T_i = N_i P_{pub} + H(Z_i)S_i \rangle$ to all others and keeps $N_i \in \mathbb{Z}_q^*$ secret.
- **Round 2.** Each user U_i verifies as follows:

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

  If the above equation is satisfied, then U_i computes

$$X_i = e(P_{pub},\ N_i(Z_{i+1} - Z_{i-1}))$$

  and broadcasts D_i to all others. Otherwise U_i stops.
- **Key Computation.** Each user U_i computes the session key,

$$K_i = e(P_{pub},\ N_i Z_{i-1})^n X_i^{n-1} X_{i+1}^{n-2} \cdots X_{i-2}.$$

3 Attacks

In Choi *et al.*'s scheme, note that the computation of D_i in **Round 2** can be computed not only by the user U_i, but also by U_{i-1} and U_{i+2}. This is because of

$$\begin{aligned} D_i &= e(a_i(P_{i+2} - P_{i-1}), P_{i+1}) \\ &= e(P, P)^{a_i a_{i+1}(a_{i+2} - a_{i-1})} \\ &= e(a_i P, a_{i+1} P)^{-a_{i-1} + a_{i+2}} \\ &= e(P_i, P_{i+1})^{-a_{i-1} + a_{i+2}} \end{aligned}$$

This means that any two malicious users can impersonate an entity to agree some session keys in a new group if these two malicious users have the previous authentication transcripts of this entity. So, an active adversary can collude these two malicious users to simulate the victim without being detected.

We describe this attack in detail as follows: Assume that user A had agreed some session keys in group $\mathcal{G}_1$ before and his authentication transcript (T_A, P_A) can be obtained by any one.[1] Suppose B and C obtained this information and then they can collude to impersonate A to agree some session keys in a new group $\mathcal{G}_2$. Without loss of generality, we assume that the index of B in the group $\mathcal{G}_\in$ is $i-1$, and C adjusts his index to be $i+2$. They impersonate A and join the

[1] In Choi *et al.*'s model, assumed that the malicious adversary may read the broadcast message or substitute of them.

group with the index i. So, (T_A, P_A) is (T_i, P_i) and it satisfies the verification in round 2. B and C can compute D_i instead of A as follows:

$$D_i = e(P_i, P_{i+1})^{-a_{i-1}} \cdot e(P_i, P_{i+1})^{a_{i+2}}.$$

Therefore, B and C can impersonate A to share a group session key without being detected by other users in $\mathcal{G}_2$.

In Du *et al.*'s scheme, note that the computation of X_i in **Round 2** can be computed not only by the user U_i, but also by U_{i-1} and U_{i+1}. This is because of

$$\begin{aligned} X_i &= e(P_{pub}, N_i(Z_{i+1} - Z_{i-1})) \\ &= e(N_i P_{pub}, Z_{i+1} - Z_{i-1}) \\ &= e(N_i P_{pub} + H(Z_i)S_i - H(Z_i)S_i, Z_{i+1} - Z_{i-1}) \\ &= e(T_i, Z_{i+1} - Z_{i-1}) \cdot e(-H(Z_i)S_i, Z_{i+1} - Z_{i-1}) \\ &= e(T_i, Z_{i+1} - Z_{i-1}) \cdot e(-H(Z_i)sQ_i, N_{i+1}P - N_{i-1}P) \\ &= e(T_i, Z_{i+1} - Z_{i-1}) \cdot e(-H(Z_i)Q_i, (N_{i+1} - N_{i-1})P_{pub}) \end{aligned}$$

Similar to the attack in Choi *et al.*'s scheme, Du *et al.*'s scheme can be attacked too, i.e., any two malicious users can impersonate a user if these two malicious users have the previous authentication transcripts of this user.

4 Conclusion

In this paper, we show that there is a security flaw in Choi *et al.* and Du *et al.*'s ID-based authenticated group key agreement schemes, i.e., they can not provide the authenticity in some situations. To provide the authenticity, we suggest to use a time parameter as a solution to this problem, *e.g.*, let $h_i = H(P_i||time||ID_1||\cdots||ID_n)$, where *time* is the time stamp.

References

1. M. Burmester and Y. Desmedt, *A Secure and Efficient Conference Key Distribution System*. Advances in Cryptology-EUROCRYPT'94, LNCS 950, pp.267-275, Springer-Verlag, 1994.
2. K. Y. Choi, J. Y. Hwang and D. H. Lee, *Efficient ID-based Group Key Agreement with Bilinear Maps*, to appear in the proceeding of 2004 International Workshop on Practice and Theory in Public Key Cryptography (PKC'04), Springer-Verlag, 2004.
3. X. Du, Y. Wang, J. Ge and Y. Wang, *ID-based Authenticated Two Round Multi-Party Key Agreement*, Cryptology ePrint Archive: Report 2003/247.