A Dynamic ID-based Authenticated Group Key Agreement Protocol

Jun ZHENG[1,a], Cheng YANG [1,b], Jinrong XUE[2,c], Can ZHANG[1]

[1] Beijing Institute of Technology, Beijing 100081, China

[2] National Computer System Engineering Research Institute of China, Beijing, 102209, China

[a]zhengjunbit@gmail.com, [b]yangcheng33@126.com, [b]xuejinrong_zdls@sina.com

Keywords: Group key agreement, Dynamic, ID-based, Authenticated.

Abstract. Through the group key agreement, all group members could negotiate a common session key which is used in later secure communication. While simple GKA cannot provide enough security to resist the adversary's attack, and the malicious damage during the agreement makes the authenticated key agreement particularly important. In identity-based authentication, user's unique identity information is used as the public key, which makes it exempt from a series of management of the certification in public-key infrastructure. Thereby, the identity-based key agreement can simplify the key management procedures and reduce the risk of failure at the certification authority.

Recently, several identity-based group key agreement protocols have been proposed, however most of them are either vulnerable to impersonation and replay attack or inefficient and unscalable. This paper proposes a novel authenticated group key agreement protocol which is based on bilinear pairings. It needs two rounds to negotiate the session key, and the low computational complexity makes the protocol efficient and scalable. Meanwhile, our protocol also ensures the forward and backward secrecy and the key independence. Under the Decisional Diffie-Hellman assumption, our protocol is proved to be secure against the adversary.

1. Introduction

Today, distributed application technology based on group communication has been widely used in network video conference, group instant chat and other systems. Various secure and reliable group key management protocols have emerged as the times require. The main target of group key management (GKA) protocol is to make sure the key generation, distribution and management among the group members in an open and untrusted network. GKA could be classified into three kinds: centralized, decentralized and distributed [1], the former two are susceptible to network bottlenecks and single point failure of key distribution center (KDC), so in this work we focus on distributed GKA protocols that the session key is derived as a function of contributions provided by all group members.

To establish a safe and efficient distributed group network need to meet the following requirements: data confidentiality, data integrity, authentication and scalability. In an authenticated GKA protocol, group members must provide the reliable proof of their identities to prevent external malicious users participating in the negotiation process. Different from the traditional certificate-based public key authentication system, Shamir first proposed the identity-based public key cryptosystem (ID-based PKC) [3], the public key of entity in the system comes from identity information which is chosen by the user, such as email address. Soon some ID-based signature schemes have been proposed, but all of them are lack of effective and practical. Until 2001, Boneh et al. [4] proposed an effective identity authentication scheme based on weil parings over the elliptic curve, the scheme uses bilinear pairings to construct the cryptosystem based on identity and soon became the main research direction in the field of research. However, most of the researches are about two-party or tripartite key agreement protocols. Ever since two-party Diffie-Hellman key exchange was first proposed in 1976, massive works have attempted to solve the problem of securely distributing a session key among a group of multi-parties. Unfortunately, most of them suffer from one or more of the shortcomings, such as too many rounds of communication, superfluous broadcast messages per round, and lack of forward secrecy.

In this paper, we will propose an authenticated two-round ID-based group key agreement protocol. The protocol is based on the protocol of Burmester and Desmedt [5], and each round contains authentication that prevents the impersonation attack and replay attack. This paper is organized as follows: we firstly introduces the related work in section 2 and describes the preliminaries about our protocol in section 3, then our protocol will be detailed described in section 4, and section 5 will give the analysis, section 6 will give a brief conclusion.

2. Related Work

In 1994, Burmester and Desmedt (BD) proposed a group key exchange protocol based on the two-party Diffie-Hellman protocol [5], the protocol could negotiate the group key in two rounds by using the broadcast, but it is lack of authentication function. Choi et al. [6] and Du et al. [7] improved the scheme by joining the bilinear pairings, which make it can be authenticated. While Zhang and Cheng [8] proposed an impersonation attack on the two protocols, in their scheme, any two malicious users could impersonate an entity to agree some session keys in new group if they have the previous communication transcripts.

Zheng [9] proposed a two-round authenticated GKA protocol, the protocol is based on Elgamal signature algorithm, it can prevent replay attack and satisfy the forward security, but it needs to broadcast too much messages that may cause high network load. The asymmetric anonymous GKA scheme proposed by Zhang [10] is also facing the same problem. Shi [11] and Zhong [12] both proposed a one-round ID-based GKA scheme, but they have changed the ID-based authentication protocol that the public keys of members are not their identity strings. Yao [13] put forward a three-round ID-based GKA protocol, the first round is for identity authentication, the second round is for key agreement, and the third round is for key confirmation, and it is provably secure in the random oracle model. In terms of Identity-Based Encryption, Huang [14] proposed a hybrid encryption scheme, compared to the Boneh's scheme, it has a higher computational efficiency.

3. Preliminaries

3.1 Bilinear Pairing

Let G_1 and G_2 denote two cyclic groups of large prime order *q*. G_1 is a cyclic additive group and G_2 is a cyclic multiplicative group. $P \in G_1$ is a generator of G_1, and let $e: G_1 \times G_1 \to G_2$ be a bilinear map which satisfies the following conditions:

1. *Bilinearity:* $e(aP, bQ) = e(P, Q)^{ab}$, $\forall P, Q \in G_1$, $\forall a, b \in Z_q^*$. For $\forall P, Q, R \in G_1$, we have $e(P+Q, R) = e(P, R) \cdot e(Q, R)$ and $e(P, Q+R) = e(P, Q) \cdot e(P, R)$.
2. *Non-degeneracy:* If P is the generator of G_1, thus the $e(P, P)$ is the generator of G_2, so $e(P, P) \neq 1$.
3. *Computability:* $\forall P, Q \in G_1$, $e(P, Q)$ is efficiently computable.

3.2 Decisional Diffie-Hellman (DDH) assumption

Let *a, b, c* be the random number chosen from Z_q^* , given $P, aP, bP, cP \in G_1$, decide if $c = ab \bmod q$, which equals to decide if $e(aP, bP) = e(P, cQ)$.

4. Our Proposed Protocol

4.1 Group Key Agreement

The ID-based cryptosystem involves a private key generator (PKG) to setup the system parameters and generate the users' private keys. Let $u=\{u_1,u_2,\cdots,u_n\}$ be a set of users who want to generate a common session key by participating in our GKA protocol.

Setup: Given the security parameter 1^k, the PKG generates the system common parameters $\{q,G_1,G_2,P,e,P_{pub},H_0,H_1,E_K,D_K\}$.

G_1 is a cyclic additive group and G_2 is a cyclic multiplicative group of large prime order q, $P\in G_1$ is a generator of G_1, $e:G_1\times G_1\to G_2$ is a bilinear map. The random number $s\in Z_q^*$ is the PKG's private key, and the PKG's public key is $P_{pub}=sP$. $H_0:\{0,1\}^*\to G_1$ and $H_1:\{0,1\}^*\to\{0,1\}^k$ are the hash functions. E_K and D_K are the symmetric encryption and decryption algorithms.

Extract: Given u_i's public identity information ID_i $(1\le i\le n)$, compute $Q_i=H_0(ID_i)$ as the role of the public key, and then compute the corresponding secret private key as $S_i=sQ_i$. And ID denotes the current connection ID string $ID_1\,|\,ID_2\,|\cdots|\,ID_n$.

The protocol could be performed in two rounds as follows:

Round 1:

Every participant u_i chooses two random numbers $a_i,r_i\in Z_q^*$, and precomputes $P_i=a_iP$.

For the left neighbor u_{i-1}, u_i uses the private key S_i to compute $w_{i-1}=e((r_i+1)S_i,Q_{i-1})$, and the symmetric encryption key is $K=H_1(w_{i-1}\,|\,T_1)$, T_1 means the timestamp in round 1. Then it computes $U_{i-1}=r_iQ_i$, $m_{i-1}=H_1(P_i\,|\,U_{i-1}\,|\,ID)$, $V_{i-1}=E_K(P_i\,|\,m_{i-1})$, and finally obtain U_{i-1} and V_{i-1}.

For the right neighbor u_{i+1}, it could use the same method to get U_{i+1} and V_{i+1}. Then u_i broadcasts $D_i=(U_{i-1},V_{i-1},U_{i+1},V_{i+1},T_1)$.

Round 2:

Upon the receipt of $D_1,D_2,\cdots,D_n$ from other users, each user u_i first checks whether T_1 is timeout or not. To verify u_{i-1}, u_i computes the symmetric decryption key $K=H_1(w_{i-1}\,|\,T_1)$, which $w_{i-1}=e(U_i+Q_{i-1},S_i)$.Then it could get P_{i-1} and m_{i-1} through decrypting V_{i-1} by $D_K(V_{i-1})$. Now it can verify whether $m_{i-1}=H_1(P_{i-1}\,|\,U_{i-1}\,|\,ID)$ holds or not.

By the same way, u_i could verify u_{i+1} and acquire P_{i+1}. If the verification fails, the protocol execution should be terminated and a failure notification will be broadcasted. Otherwise, u_i continues the following computation.

u_i selects another random number $t_i\in Z_q^*$ and computes $X_i=e(P_{i+1}-P_{i-1},P_i)$, $Y_i=t_iQ_i$, $h_i=H_1(X_i\,|\,Y_i\,|\,T_2\,|\,ID)$, $Z_i=(t_i+h_i)\cdot S_i$, then broadcast $G_i=(X_i,Y_i,Z_i,T_2)$.

Key Computation:

After having received all the messages G from other users, u_i checks whether T_2 is timeout or not, then do the batch verification by checking the correctness of the following equation:

$$e\left(\sum_{k\neq i}Z_k,P\right)=e\left(\sum_{k\neq i}(Y_k+h_kQ_k),P_{pub}\right).$$

If the verification succeeds, u_i can compute the session key $K_s = H_1\left(k \mid G_1 \mid G_2 \mid \cdots \mid G_{\mathrm{n}}\right)$ through $k = e\left(P_{i-1}, nP_i\right) X_i^{n-1} X_{i+1}^{n-2} \cdots X_{i-2}$.

4.2 User Joining Phase

When a user u_j wants to join the group, it must send a request to the PKG to ensure its legitimacy. Once the PKG approves the users' joining request, it broadcasts the joining message and u_j's identity to all members in the group.

In round 1, the new user u_j only needs to communicate with u_{j-1} and u_{j+1}, after verification, u_j could obtain P_{j-1} and P_{j+1}. Then in round 2, all group members must pick a new random number $r' \in Z_q^*$, compute and broadcast $G_i' = \left(X_i, Y_i, Z_i, T_2\right)$. The following key computation phase is the same as our GKA protocol described before.

4.3 User Leaving Phase

When a user u_j leaves the group, it also needs PKG to approve and broadcast its leaving request. Only the two neighbors of u_j need to communicate and verify each other. Then all group members also have to pick a new random number $r' \in Z_q^*$, the following steps are the same as joining phase.

5. Protocol Analysis

5.1 Security Analysis

Theorem 1 If all the honest members calculate correctly, they could obtain the common session key.

Proof. Since $X_i = e\left(P_{i+1} - P_{i-1}, P_i\right) = e\left(P, P\right)^{a_i a_{i+1} - a_{i-1} a_i}$, we have

$$k = e\left(P_{i-1}, nP_i\right) X_i^{n-1} X_{i+1}^{n-2} \cdots X_{i-2} = e\left(P, P\right)^{na_{i-1}a_i + (n-1)\left(a_i a_{i+1} - a_{i-1} a_i\right) + \cdots + a_{i-2} a_{i-1} - a_{i-3} a_{i-2}}$$

$$= e\left(P, P\right)^{a_1 a_2 + a_2 a_3 + \cdots + a_{i-1} a_i}.$$

Because all the members have the same $G_1 \mid G_2 \mid \cdots \mid G_{\mathrm{n}}$, they can compute the common session key $K_s = H_1\left(k \mid G_1 \mid G_2 \mid \cdots \mid G_{\mathrm{n}}\right)$.

Theorem 2 The protocol is authenticated and secure.

Proof. At the beginning of round 2, each user verifies the others by the equation $e\left(Q_{i-1} + Q_i, sQ_i\right) = e\left(\left(r_i + 1\right) sQ_{i-1}, Q_i\right)$. Assuming that an adversary could impersonate a normal user u_j, it must compute sQ_j to make the equation hold. While, it is impossible to be achieved under the assumption of DDH.

In the phase of key computation, due to the bilinearity of the pairing, the users do not exchange ephemeral keys a_i, but $a_i P$. It is hard to determine $e\left(P, P\right)^{a_i a_j}$, which relies on the computation hardness of DDH assumption [7].

Theorem 3 The protocol can resist the impersonation attack and replay attack.

Proof. The verifications in round 2 and key computation phase both utilize the current ID connection string and the timestamp, which could make this two attacks unavailable.

Theorem 4 The protocol can achieve the forward and backward secrecy.

Proof. According to our user joining and leaving scheme, when a user wants to join or leave the group, other users must pick a new random number r' to compute $G_i' = \left(X_i, Y_i, Z_i, T_2\right)$, which makes the disclosure of a key couldn't compromise past keys. So the new user cannot use the new session

key and the previous transcripts to decrypt the message transferred before, the user who has left also cannot use the old session key and the following transcripts to decrypt the message transferred later.

5.2 Performance Analysis

Table 1 gives the number of computations per entity in our protocol. The computations include: scalar multiplication, pairing, hashing and addition over G_1.

Table 1. Computation of each entity

Scalar Multiplication	Pairing	Hashing	Addition
n + 4	6	n + 4	3n + 1

6. Summary

In this paper, we proposed a dynamic ID-based authenticated agreement protocol. The protocol only needs two rounds and each round uses the authentication to provide the security. Besides, it not only has the low computational complexity that makes the protocol more efficient, but also ensures the forward secrecy and key independence.

Acknowledgement

This paper is supported by the National Natural Science Foundation of China (No. 61272511).

References

[1] Rafaeli S, Hutchison D. A survey of key management for secure group communication[J]. Acm Computing Surveys, 2003, 35(3):309--329.

[2] Cao X, Kou W, Du X. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges[J]. Information Sciences, 2010, 180(15):2895-2903.

[3] Shamir A. Identity-Based Cryptosystems and Signature Schemes[J]. Lecture Notes in Computer Science, 1985, 21(2):47-53.

[4] Dan Boneh, Franklin M. Identity-Based Encryption from the Weil Pairing[J]. Siam Journal on Computing, 2003, 32(3):213-229.

[5] Burmester M, Desmedt Y. A secure and efficient conference key distribution system[M]// Advances in Cryptology — EUROCRYPT'94. Springer Berlin Heidelberg, 1995:275-286.

[6] Choi K Y, Hwang J Y, Lee D H. Efficient ID-based group key agreement with bilinear maps[M]//Public Key Cryptography–PKC 2004. Springer Berlin Heidelberg, 2004: 130-144.

[7] Du X J, Wang Y, Ge J H, et al. ID-based authenticated two round multiparty key agreement[J]. Iacr Cryptology Eprint Archive, 2003.

[8] Zhang F, Chen X. Attack on Two ID-based Authenticated Group Key Agreement Schemes[J]. Iacr Cryptology Eprint Archive, 2003, 2003.

[9] Zheng S, Wang S, Zhang G. A dynamic, secure, and efficient group key agreement protocol[J]. Frontiers of Electrical & Electronic Engineering in China, 2007, 2(2):182-185.

[10] Zhang Q, Wang R, Tan Y. Identity-Based Authenticated Asymmetric Group Key Agreement[J]. Journal of Computer Research & Development, 2014.

[11] Shi Y, Chen G, Li J. ID-based one round authenticated group key agreement protocol with bilinear pairings[C]//Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on. IEEE, 2005, 1: 757-761.

[12] Zhong Yan-tao, Ma Jian-feng. Identity based group key management scheme for LEO / MEO double-Layer space information network[J]. Journal of Astronautics , 2011, 32(07):1551-1556.

[13] Yao G, Wang H, Jiang Q. An Authenticated 3-Round Identity-Based Group Key Agreement Protocol[C]// Availability, Reliability and Security, 2008. ARES 08. Third International Conference on. IEEE, 2008:538-543.

[14] Huang Y, Jianzhu L U. A New Identity-based Authenticated Encryption Scheme[J]. Computer Engineering, 2007, 33(7):149-152.