情報保護學會論文誌
第 23 卷 第 1 號, 2013. 2

개선된 원 라운드 인증 그룹 키 합의 프로토콜

김 호 희,†‡ 김 순 자
경북대학교 IT대학 전자공학부

An Improved One Round Authenticated Group Key Agreement

Ho-hee Kim,†‡ Soon-ja Kim
Kyungpook National University

요 약

많은 인증 키 합의 프로토콜이 제안되어 왔다. 여전히 안전한 인증키 합의 프로토콜을 설계하는 것이 이슈화되고 있다. 이 논문에서는, 전형적인 ID 기반의 암호화 시스템의 공개키와 개인키 뿐 아니라 하나 더 많은 공개키와 개인키를 사용하는 원 라운드 인증 그룹키 합의 프로토콜을 제안한다. 제안된 프로토콜은 Shi et al. 프로토콜과 He et al. 프로토콜을 수정 보완하였다. 제안된 프로토콜의 공개키 개인키와 서명 과정은 그들의 프로토콜보다 단순하다. 제안한 프로토콜은 안전하며, 통신과 계산 비용 면에서 그들의 프로토콜보다 더 효율적이다.

ABSTRACT

Several identity-based and authenticated key agreement protocols have been proposed. It remains at issue to design secure identity based and authenticated key agreement protocols. In this paper, we propose a one round authenticated group key agreement protocol which uses one more key pair as well as the public key and private key of typical IBE(Identity-Based Encryption) system. The proposed protocol modified Shi et al.'s protocol and He et al.'s protocol. The public and private keys and the signature process of our protocol are simpler than them of their protocols. Our protocol is secure and more efficient than their protocols in communication and computation costs.

Keywords: Bilinear pairings, AGKA

I. Introduction

Background. Key agreement is a fundamental cryptographic primitive for establishing a secure communication. It is a process of computing a shared secret contributed by two or more users such that no single user can predetermine the resulting value. An authenticated key agreement is attained by combining the key agreement protocol with digital signatures. This avoids man-in-the-middle attack.

In a traditional Public Key Cryptosystems(PKC), the association between a user's identity and his public key is obtained through a digital certificate issued by a Certifying Authority(CA). The CA checks the credentials of a user before issuing a certificate to him. Hence, the process of certificate management requires high computational and storage efforts. To simplify the certificate management process, Shamir

접수일(2012년 7월 5일), 수정일(2012년 11월 16일), 게재확정일(2012년 12월 24일)
† 주저자, brtcloud@naver.com
‡ 교신저자, brtcloud@naver.com

introduced the concept of ID-based cryptosystem in 1984[1]. In such cryptosystems the public key of a user is derived from his identity information and his private key is generated by a trusted third party called Key Generation Center (KGC). The advantage of ID-based cryptosystems is that it simplifies the key management process which is a heavy burden in the traditional certificate based cryptosystems. However, they suffer from an inherent drawback of key escrow i.e. KGC knows the users' private keys. They also require a secure channel for key issuance between KGC and user. The ID-based cryptosystems require the users to authenticate themselves to their KGC in the same way as they would authenticate themselves to a CA in traditional PKC.

Boneh and Franklin have proposed two ID-based encryption (IBE) schemes which potentially allow the replacement of a PKI with a system where ones identity becomes the public key and a trusted KGC helps to generate users' private key[2]. After that, many ID-based cryptographic protocols were developed based on pairings and is currently an area of very active research. There are many ID-based two-party or three-party key agreement protocols based on pairing.

Another direction of research on key agreement is to generalize the two-party or three-party key agreement to multi-party setting. As a result of the increased popularity of group oriented applications, the design of an efficient ID-based authenticated group key agreement protocol (ID-AGKA) has recently received much attention in the literature.

Related Work. Choi *et al.* and Du *et al.* have proposed two rounds ID-AGKA protocols, which are based on bilinear pairings and Burmester and Desmedt scheme[3-5]. However, Zhang *et al.* have pointed out an impersonation attack on the two protocols[6]. Then Du *et al.* improved their ID-AGKA protocol to resist this attack[7]. One defect of the scheme is that group users must keep loose synchronization. If groups are dynamic, new users' counters must keep up with that of the group users.

Shi *et al.* presented a one round ID-AGKA protocol under a modified IBE system[8]. But, their protocol has no signature verification process. He *et al.* pointed out that Shi *et al.*'s protocol is weak against impersonation attack and disparate session keys attack[9]. They proposed a modified one round authenticated group key agreement. But, their protocol uses the complicated public and private keys and signature verification process with many parameters and frequent hash functions and more messages.

Contribution. So, we present a one round AGKA protocol which modified Shi *et al.*'s and He *et al.*'s protocol. Our protocol uses the simple public and private keys including the public and private key of typical IBE system[10]. Also, it uses the simpler signature verification process than that of their protocol.

II. Technical Backgrounds

2.1. Bilinear Pairings

We let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q. We assume that the *discrete logarithm problem*(DLP) in both G_1 and G_2 are hard. We let $e : G_1 \times G_1 \rightarrow G_2$ be a pairing which satisfies the following properties:

1. Bilinear : $e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q)$, $e(P, Q_1 + Q_2) = e(P, Q_1)e(P, Q_2)$ *i.e.*,

$e(aP,bQ)=e(P,Q)^{ab}$where $a,b\in Z_q^*$, $P,Q\in G_1$.

2. Non-degenerate : There exists $P\in G_1$ such that $e(P,P)\neq 1$.
3. Computability : There is an efficient algorithm to compute $e(P,Q)$ for all $P,Q\in G_1$.

2.2. Diffie-Hellman Problem

We let the Diffie-Hellman(DH) tuple in G_1 be $(P,\ xP,yP,zP)\in G_1$ for some $x,y,z\in Z_q^*$ satisfying $z=xy \bmod q$.

1. The Decision Diffie-Hellman(DDH) problem: Given $P,\ xP,yP,zP\in G_1$, decide if it is a valid DH tuple. This can be solved in polynomial time by verifying $e(xP,yP)=e(P,zP)$.
2. The Computational Diffie-Hellman(CDH) problem: Given any three elements from the four elements in DH tuple, compute the remaining element.

CDH Assumption: There exists no algorithm running in expected polynomial time, which can solve the CDH problem with non-negligible probability.

3. The Bilinear Diffie-Hellman(BDH) problem: Given $P,xP,yP,zP\in G_1$, compute $e(P,P)^{xyz}\in G_2$, where $x,y,z\in Z_q^*$. An algorithm is said to solve the BDH problem with an advantage of ε if

$$\Pr[A(P,xP,yP,zP)=e(P,P)^{xyz}]\geq \varepsilon.$$

BDH Assumption: There exists no algorithm running in expected polynomial time, which can solve the BDH problem in $<G_1,G_2,e>$ with non-negligible probability.

III. The Shi *et al.*'s protocol

〔Table 1〕 shows the notations used in this paper.

The KGC(Key Generation Center) generates the system parameters and all users' public and private keys. The KGC's public keys are $P_{pub}=s_1P$ and $P_{pub}'=s_2P$. The public key of a user $U_i(1\leq i\leq n)$ is $Q_i=(I_is_1+s_2)P$ and the private key is $S_i=(I_is_1+s_2)^{-1}P$.

〔Table 1〕 The notations

n	The number of group users
ID_i	Identity of a user U_i
p,q	Prime number
G_1,G_2	Two cyclic groups with prime order q
P	The generator G_1
P_{pub}	sP, the KGC's public key
e	$e: G_1\times G_1\rightarrow G_2$, a bilinear map
$H_1()$	Hash function, $H_1: \{0,1\}^*\rightarrow Z_q^*$
$H_2()$	Hash function, $H_2: G_1\rightarrow Z_q^*$
I_i	$H_1(ID_i)$
GID	Group identifier.
$s,\ s_1,\ s_2$	Random number chosen from Z_q^* as the master key

The KGC sends S_i to the U_i securely.

When a user U_i picks an ephemeral key $a_i\in Z_q^*$ and sends $T_{ij}=a_iQ_j$ to the user $U_j(1\leq j\leq n,\ j\neq i)$. Each user U_i computes the session key:

$$\begin{aligned}K&=e(T_{1i}+T_{2i}+\ldots+T_{i-1i}+a_iQ_i+T_{i+1i}+\ldots+T_{ni},S_i)\\&=e(Q_i,S_i)^{(a_1+a_2+\ldots+a_i+\ldots+a_{n-1}+a_n)}\\&=e(P,P)^{(a_1+a_2+\ldots+a_i+\ldots+a_{n-1}+a_n)}\end{aligned}$$

But, Shi *et al.*'s protocol has no signature verification process. Let assume that an attacker chooses $x'\in Z_q^*$ and sends $T_{ij}'=a_iQ_j+x'Q_j$ to the user U_j. Finally, all users share wrong session key $K'=e(P,P)^{(a_1+a_2+\ldots+a_{n-1}+a_n+x')}$〔11〕.

He *et al.* pointed out that Shi *et al.*'s protocol is weak against impersonation attack and disparate session keys attack〔9〕.

IV. The He *et al.*'s protocol

The KGC generates the system parameters and all users' public and private keys. The KGC's public keys are $P_{pub}=s_1P$ and $P_{pub}'=s_2P$. The public key of a user $U_i(1\leq i$

$\leq n$) is $Q_i = (I_i s_1 + s_2)P$ and the two private keys of a user U_i are $S_i = I_i s_1$ and $R_i = (I_i s_1 + s_2)^{-1} P$. The KGC sends S_i and R_i to the U_i securely.

When a user U_i picks an ephemeral key $a_i \in Z_q^*$ and sends $T_{ij} = a_i Q_j$, $X_i = a_i P$ and $Y_{ij} = H_2(H_1(GID)T_{ij})S_i + a_i P_{pub}$. to the $U_j (1 \leq j \leq n,\ j \neq i)$.

Each user U_j verifies as follows:

$e(Y_{ij}, P) = e((H_2(H_1(GID)T_{ij})H_1(ID_i) + X_i),\ P_{pub})$

If the above equation holds, then each user U_i computes the session key:

$$K = e(T_{1i} + T_{2i} + \ldots + T_{i-1i} + a_i Q_i + T_{i+1i} + \ldots + T_{ni}, R_i)$$
$$= e(Q_i, R_i)^{(a_1 + a_2 + \ldots + a_i + \ldots + a_{n-1} + a_n)}$$
$$= e(P, P)^{(a_1 + a_2 + \ldots + a_i + \ldots + a_{n-1} + a_n)}$$

In the signature verification process of their protocol, a user U_i has to send the same X_i to other users and a user U_j has to compute $H_1(ID_i)$ $(1 \leq i \leq n,\ j \neq i)$ of other users.

V. The Proposed Protocol

In this section, we describe a one round authenticated group key agreement protocol which uses one more key pair as well as the long term public and private keys of typical IBE system.

5.1 System Setup

〔Setup〕

The KGC generates the following system parameters:

{ q, G_1, G_2, P, P_{pub}, e, $H_1()$, $H_2()$ }

The KGC selects an elliptic curve E defined over $GF(p)$ with order q and a base point P. And then, chooses a master key $s \in Z_q^*$ and computes P_{pub} by $P_{pub} = sP$ and publishes system parameters.

〔Extract〕

A user $U_i (1 \leq i \leq n)$ picks a random integer $r_i \in Z_q^*$ and submits his identity ID_i and $r_i P$ to the KGC. $r_i P$ is a user's long term public key and r_i is a user's long term private key. The KGC computes $Q_i = H_1(ID_i)$ as a user's another long term public key and publishes $r_i P$ and Q_i. Then, computes a user's another long term private key as $S_i = sQ_i$ and sends S_i to the user U_i securely.

5.2. Key Generation

〔Signature〕

Each user U_i picks a random integer $a_i \in Z_q^*$ as his ephemeral key. Then he computes $T_{ij} = a_i r_j P$ ($1 \leq j \leq n,\ j \neq i$) and $Y_{ij} = H_2(T_{ij})S_i + r_i P_{pub}$. Each user U_i sends T_{ij} and Y_{ij} to the user U_j.

〔Verification〕

Each user U_j verifies T_{ij} and Y_{ij} as follows:

$$e(Y_{ij}, P) = e(H_2(T_{ij})S_i + r_i P_{pub},\ P)$$
$$= e(H_2(T_{ij})Q_i + r_i P,\ P_{pub})$$

If the above equation holds, then U_j accepts T_{ij} as the message from U_i.

〔Key Computation〕

Upon receiving $T_{1i}, T_{2i}, \ldots, T_{i-1i}, T_{i+1i}, \ldots, T_{ni}$ from other users, each user U_i computes the session key as follows:

$$K = K_i$$
$$= e(a_1 r_i P + a_2 r_i P + \ldots + a_i r_i P + \ldots + a_{n-1} r_i P + a_n r_i P,\ r_i^{-1} P)$$
$$= e(r_i P, r_i^{-1} P)^{(a_1 + a_2 + \ldots + a_i + \ldots + a_{n-1} + a_n)}$$
$$= e(P, P)^{(a_1 + a_2 + \ldots + a_i + \ldots + a_{n-1} + a_n)}$$

VI. Analysis

6.1. Security

Key Authentication: This property requires that only users of the group are allowed to know the key. In our protocol, the

only user to have the long term private keys r_i and S_i can deliver messages to other users owing to the signature verification process. If an adversary doesn't know r_i and a ephemeral key a_i, he can't compute the session key. According to the discrete logarithm hardness, the adversary cannot extract a_i from $T_{ij}=a_i r_j P$ and cannot compute $K_i=e(\sum_{k=1,k\neq i}^{n} T_{ki}+a_i r_i P, r_i^{-1}P)$.

Forward Secrecy: This property requires that disclosure of long term secret of a user does not compromise the previous session keys. Though the private keys r_i and S_i of U_i are disclosed, the adversary cannot extract a_i from $T_{ij}=a_i r_j P$ and he cannot compute $a_i r_i P$ and $K_i=e(\sum_{k=1,k\neq i}^{n} T_{ki}+a_i r_i P, r_i^{-1}P)$.

No Key-Compromise Impersonation: A protocol resists key-compromise impersonation when the compromise of one user's long term private key does not imply that the private keys of other users will also be compromised. Suppose that an adversary who knows the user U_i's long term private keys r_i and S_i wishes to impersonate the user U_j to all other users. He chooses an ephemeral key a'_j and computes $T'_{jk}=a'_j r_k P$ $(1\leq k\leq n, k\neq j)$, but he can't compute $Y'_{jk}=H_2(T'_{jk})S_j+r_j P_{pub}$ without the user U_j's long term private keys r_j and S_j. Therefore, the adversary may impersonate the compromised user in the subsequent protocols, but cannot impersonate other users.

Known Session Key Security: Since each run of the protocol computes a different session key $K=e(P,P)^{(a_1+a_2+\ldots+a_{n-1}+a_n)}$ with new ephemeral keys a_i ($1 \leq i \leq n$), the adversary having obtained some past session keys, gains no advantage toward computing

〔Table 2〕 Communication and Computation Costs

a. During Key Extract Process (By KGC)

	Multiplication	Hash	Multiplicative Inverse	Addition
Shi *et al.*'s protocol	$3n$	n	n	n
He *et al.*'s protocol	$3n$	n	n	n
Our protocol	$n+n$(by n users)	n	0	0

b. During Signature Process (By n users)

	Multiplication	Addition	Hash
He *et al.*'s protocol	$3n(n-1)+2n$	$n(n-1)$	$n(n-1)+n$
Our protocol	$3n(n-1)$	$n(n-1)$	$n(n-1)$

c. During Verification Process (By n users)

	Multiplication	Hash	Addition	Pairings
He *et al.*'s protocol	$2n(n-1)$	$2n(n-1)$	$n(n-1)$	$2n(n-1)$
Our protocol	$n(n-1)$	$n(n-1)$	$n(n-1)$	$2n(n-1)$

d. During Key Computation Process (By n users)

	Round	Multiplication	Pairings	Multiplicative Inverse	Addition
Shi et al.'s protocol	1	n	n	0	$n(n-1)$
He et al.'s protocol	1	n	n	0	$n(n-1)$
Our protocol	1	$2n$	n	n	$n(n-1)$

future session keys. Thus our protocol resists the known session key attack.

No Unknown Key Share: A protocol satisfies the no unknown key share, if the all users do not share the session key with the adversary. If the adversary convinces a group of users, they share some session key with the adversary, and this protocol suffers from unknown key share attack. In our protocol, the adversary cannot share the session key without some users' long term private keys. Therefore, our protocol has the property of the no unknown key share.

No Key Control: The session keys in our protocol are determined jointly by n users, so that neither user alone can control the outcome of the session key by restricting it to lie in some predetermined small set. Therefore, there is no key control in our protocol.

6.2. Performance

〔Table 2〕 summarizes the communication and computation costs of Shi *et al.*'s, He *et al.*'s and our protocol. Because Shi *et al.*'s and He *et al.*'s protocol use more complicated public and private keys than them of our protocol, their protocols have more computation costs during the system setup and key extract process.

Moreover, during the signature verification process, He *et al.*'s protocol uses more parameters, more frequent hashes and more messages than our protocol. On the one hand, our protocol uses X_i and $H_1(ID_i)$ of He *et al.*'s protocol as the long term public keys of a user.

So, our protocol has less computation costs than their protocol.

During the key computation process, our protocol has a little more computation costs. From the result of performance analysis, our protocol makes higher performance than Shi *et al.*'s and He *et al.*'s protocol by using simple public and private keys and a simple signature verification process.

VII. Conclusion

This paper presents a one round authenticated group key agreement protocol which modified Shi *et al.*'s and He *et al.*'s protocol by using the simpler public and private keys and signature verification process than them of their protocols. So, our protocol is secure and more efficient than their protocols in communication and computation costs.

References

〔1〕 A. Shamir, "Identity-based cryptosystems and signature schemes," Advances in Cryptology- Crypto LNCS 196, pp.47-53, 1984.

〔2〕 D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," Advances in Cryptology- Crypto LNCS 2139, pp.213-229, 2001.

〔3〕 K. Y. Choi, J. Y. Hwang, and D. H. Lee, "Efficient ID-based group key agreement with bilinear maps," International Workshop on Practice and Theory in Public Key Cryptography (PKC2004, IACR), pp.1-14, 2004.

〔4〕 X. Du, Y. Wang, J. Ge, and Y. Wang, "An ID-based authenticated two round multiparty key agreement," IACR ePrint 2003-247, 2003.

〔5〕 M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system," Advances in Cryptology-EURO-CRYPT94, LNCS, pp.950, 1995.

〔6〕 F. Zhang and X. Chen, "Attack on ID-based authenticated group key agreement schemes," IACR ePrint 2003-259, 2003.

〔7〕 X. Du, Y. Wang, J. Ge, and Y. Wang, "An Improved ID-based authenticated group key agreement scheme," IACR ePrint 2003-260, 2003.
〔8〕 Y. Shi, G. Chen, and J. Li, "ID-based one round authenticated group key agreement protocol with bilinear pairings," Proc. ITCC'05. Vol. 1, pp. 757-761, 2005.
〔9〕 Y. Z. He and Z. Han, "An Efficient Authenticated Group key agreement protocol," Security Technology, IEEE International Carnahan Conference, pp.250-254, 2007.
〔10〕 X. Chen, F. Zhang, and K. Kim, "A new ID-based group signature scheme from bilinear pairings," IACR ePrint 2003-116, 2003.
〔11〕 K. K. R. Choo, "Revisit of McCullagh-Barreto two-party ID- based authenticated key agreement Protocols," International journal of network security, pp.154-160, Nov. 2005.

〈著者紹介〉

김 호 희 (Ho-hee Kim) 학생회원
1993년 2월: 경북대학교 전자공학과 졸업
1996년 2월: 경북대학교 전자공학과 석사
2003년 3월~현재: 경북대학교 전자공학과 박사과정
〈관심분야〉 정보보호, 전자공학

김 순 자 (Soon-ja Kim) 종신회원
1975년 2월: 경북대학교 수학교육과 졸업
1977년 2월: 경북대학교 수학교육과 석사
1988년 2월: 계명대학교 이학박사
1980년~현재: 경북대학교 전자공학부 교수
〈관심분야〉 정보보호 응용기술, 전자상거래 및 보안