Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFICIENT CERTIFICATELESS AUTHENTICATED KEY AGREEMENT

[1]YUXIU-YING , [2]HEDA-KE , [3]ZHANG – WENFANG
[1,2,3]School of Information Science and Technology, South West Jiao Tong University,
E-mail: [1]xyyu@home.swjtu.edu.cn , [2]dkhe@home.swjtu.edu.cn, [3]wfzhang@home.swjtu.edu.cn

ABSTRACT

Key agreement is very important in information and data security. To overcome the key escrow property of identity-based cryptography **AND** combines the advantages of the traditional PKI and the identity-based cryptography, certificateless public key cryptography is proposed. This paper proposed a new certificateless two-party key agreement protocol and gives the comparisons with other comparable schemes in security and efficiency. The new proposed scheme achieves almost all of the desired security attributes and is more practicable.

Keywords: *Authenticated Key Agreement, Identity-Based , Certificateless-Based Encryption*

1. INTRODUCTION

In the traditional public key infrastructure (PKI), certificates are used to provide an assurance of the relationship between public keys and the identities that hold the corresponding private keys. However, a PKI faces many challenges in practice, such as the scalability of the infrastructure and certificate management. To address the shortcomings of PKI and to simplify key management, Shamir [1] introduced the concept of identity based cryptography (IBC) and proposed the first identity based signature scheme in which the public keys are derived from the users' identities, such as username or an e-mail address, and the private keys are generated by a trusted third party called Key Generate Center (KGC). Identity based cryptography serves as an efficient alternative to PKI because no certificate is needed to validate the public key of a user.

But problems still exist since KGC knows every user's private key and also be able to trace each user's transaction and may cause loss of privacy if it's not trusted. Certificateless Cryptography(CLC) was introduced by Al-Riyami [2] to reduce the trust level of KGC and thus to find an effective remedy to the key escrow problem in IBC.

Key agreement is a cryptographic protocol, where two or more participants who each have a long-term key, establish a secret key over an open network with each other. The first two-party key agreement protocol is the Diffie – Hellman protocol [4] which does not authenticate the two communicating entities and is insecure against active attacks. Authenticated key agreement (AKA) is a key agreement protocol enhanced to prevent active attacks.AKA can be realized in the PKI or identity-based cryptography setting. However, the former suffers from a heavy certificate management burden while the latter is subject to the so-called key escrow problem because all parties must fully trust KGC. With the introduction of CLC, several certificateless two-party AKA protocols [5-8] have been presented which does not need an additional certificate to bind the user to the public key and also avoids the key escrow problem. Nevertheless, none of them has been proven secure with a formal proof. As for efficiency, most of the existing protocols suffer from heavy pairing computation. Thus, it is essential to build certificateless two-party AKA protocols which are provably secure and efficient.

Our contribution: In this paper,we persent security analysis of two certificateless key agreement schemes newly proposed in[6,8] which we call W-AKA and L-AKA, and point out that the previous one is not strong type II secure while the next one is not meet the Known session-specific temporary information security. furthmore we proposed a new certificateless authenticated two-party key agreement protocol.

Organization: In section 2 we tell the background knowledge used in this paper.In section 3, two rivised protocol s are analized. Then we proposed a new certificateless authenticated two-party key agreement protocol in section 4. The

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

security analysis is given in section 5. Finally we conclude our paper in section 6.

2. BACKGROUND KNOWLEDGE

2.1 Security Definitions

The following security properties are commonly required in a certificateless key establishment protocols in general[5].

Known session key security. Each run of a key agreement protocol between two parties A and B should produce a unique session key. If some of the session keys were leaked,this should not compromise the key secrecy of any other session key.

Unknown Key-Share (UKS) seurity. If A thinks that he is sharing a key with an entity B, then it should not happen that A is actually sharing that key with another entity M where M≠B.

Forward secrecy. If the private keys of A and B are compromised, the secrecy of previously established session keys by those entities is not compromised; this is sometimes also called perfect forward secrecy. A weaker notion is partial forward secrecy: the compromise of either A's or B's private key does not endanger the secrecy of previously established session keys.

Key control. Neither party should be able to influence the outcome of the key more than the other. While this is an ideal attribute for key agreement schemes, it is very difficult to design a method which has perfect key control. This is because it's necessary for one party to choose its input key first, thus granting the other the possibility of estimating a certain number of bits by trying different input combinations.

Known session-specific temporary information security.The compromise of private temporary information should not compromise the secrecy of the generated session key where the ephemeral secret was not used. Although overlooked in many security analyses, exposure of such information can occur in practical implementations if ephemeral keys are precomputed or stored insecurely.

Resistance to leakage of ephemeral secrets to the KGC. If a malicious KGC learns the ephemeral secrets of any session, the KGC should not be able to compute the session key.

Resistance to Key-Compromise Impersonation (KCI) attacks. The compromise of A's private key will allow an adversary to impersonate A,but it should not allow the adversary to establish a session key with A by masquerading as a different entity B.

2.2 Bilinear Maps And Related Problems

2.2.1 Bilinear Maps on Elliptic Curve Groups

Let G_1 be an additive group (identity O) with prime order q and let G_2 be a multiplicative group (identity 1) of the same order.A bilinear map on (G_1, G_2) is then a function e: $G_1 \times G_1 \rightarrow G_2$ that must satisfy the following properties.

1. Bilinearity: Given any $P, Q, R \in G_1$, we have $e(P,Q + R) = e(P,Q) \cdot e(P, R)$ and $e(P + Q, R) = e(P, R) \cdot e(Q, R)$.

Thus, for any $a, b \in Z_q^*$: $e(aP, bQ) = e(P, Q)^{ab} = e(abP, Q) = e(P, abQ)$.

2. Non-degeneracy: $e(P, P) \neq 1$. If P is a generator for G_1, then e (P, P) is a generator for G_2.

3. Computability: There is an efficient algorithm to compute e(P,Q) for all $P, Q \in G_1$.

2.2.2 Diffie-Hellman Problems

Definition 2.2.1 (Discrete Logarithm Problem). Given $Q \in G_1$ where P is a generator of G1, find an element $a \in Z_q^*$ such that aP = Q.

Definition 2.2.2 (Computational Diffie-Hellman Problem). Given<P,aP,bP>in G1 where $a, b \in Z_q^*$, compute abP.

Definition 2.2.3 (Decisional Diffie-Hellman Problem). Given $(P, aP, bP, abP) \in G_1^4$ where $a, b, c \in Z_q^*$, determine if abP = cP.

3. ANALYSIS OF TWO PROPOSED PROTOCOLS

First we give a description of W-AKA as follows:

Setup: On input a security parameter l, this algorithm runs as follows:

(1) Select a cyclic additive group G_1 of prime order q, a cyclic multiplicative group G_2 of the same order, a generator g,h,t of G_1, and a bilinear map e : $G_1 \times G_1 \rightarrow G_2$.

(2) Choose a random master-keys $\alpha \in Z_q^*$ and set $g_1 = g^{\alpha}$.

Private-Key-Extract: For the master-key s and an entity's identity $ID_i \in \{0,1\}^*$, generates the partial private key for the entity as follows.

Choose $r_{ID} \in Z_P$,compute $h_{ID} = (ht^{-rID})^{1/(\alpha - ID)}$,outpute $d_{ID} = < r_{ID}, h_{ID} >$

Key-Agreement: Assume that an entity A with identity ID_A , an entity B with identity ID_B run the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

protocol as follows.

$g_A = g_1^{-IDA}$, $g_B = g_1^{-IDB}, t_T = e(g,t)$

IDA choose $x \in Zp$, compute $T_{A1} = g_B^x$, $T_{A2} = t_T^x$, send TA =TA1‖TA2 to IDB

IDB choose $y \in Zp$, compute $T_{B1} = g_A^y, T_{B2} = t_T^y$, send TB =$T_{B1}||T_{B2}$ to IDA;

IDA compute: $K_{AB1} = e(T_{B1}, hA) \cdot (T_{B2})^{rA} \cdot e(g,h)^x$, $K_{AB2} = T_{B2}^x$

IDB compute: $K_{BA1} = e(T_{A1}, hB) \cdot (T_{A2})^{rB} \cdot e(g,h)^y$, $K_{BA2} = T_{A2}^y$

And $K_{AB1} = K_{BA1} = e(g, h)^{x+y}$, $K_{AB2} = K_{BA2} = e(g, t)^{xy}$,

Finally, A computes the session key $sk = H_2(ID_A||ID_B||T_A||T_B||e(g,h)^{x+y}||e(g,t)^{xy})$

In this protocol, assume that PKG choose $t=g^y$ in system setting, it can get all the session key between A and B. as we see, PKG can attack by parameter constructing .Since the session key is only relate to the temporary information x and y, an adversary with x and y also can compute the former session without the private keys, therefore the protocol W-AKA is not safe.

2010, Lei Zhang[8] proposed a new certificateless two-party authenticated key agreement protocol, description as follows:

Setup: On input a security parameter l, this algorithm runs as follows.

(1) Select a cyclic additive group G_1 of prime order q, a cyclic multiplicative group G_2 of the same order, a generator P of G_1, and a bilinear map $e: G_1 \times G_1 \rightarrow G_2$.

(2) Choose a random master-keys $\in Z_q^*$ and set $P_0 = sP$.

(3) Choose cryptographic hash functions $H_1: \{0,1\}^* \rightarrow G_1; H_2: \{0,1\}^{*2} \times G_1^3 \times G_2 \times G_1^4 \rightarrow \{0,1\}^l$

The system parameters are params = (G_1, G_2, e, P, P_0, H_1, H_2, l). The master-key is $s \in Z_q^*$

Partial-Private-Key-Extract: For the master-key s and an entity's identity $ID_i \in \{0,1\}^*$, generates the partial private key for the entity as follows.

(1) Compute Qi= H(IDi).

(2) Output the partial private key Di = sQi.

Set-Secret-Value: This algorithm takes as input params, an entity's identity IDi, and a random value $x_i \in Z_q^*$. It outputs xi as the entity's secret value.

Set-Private-Key: This algorithm takes as input params, an entity's identity IDi, the entity's partial private key Di and the entity's secret value $x_i \in Z_q^*$. The output of the algorithm is the private key Si =(xi , Di).

Set-Public-Key: This algorithm takes as input params, an entity's identity IDi , and the entity's secret value$x_i \in Z_q^*$ to produce the entity' s public key Pi = xiP.

Key-Agreement: Assume that an entity A with identity ID_A has private key $S_A = (x_A, D_A)$ and public key $P_A = x_A P$, an entity B with identity ID_B has private key $S_B = (x_B, D_B)$ and public key $P_B = x_B P$,. A and B run the protocol as follows.

(1) A randomly chooses $r_A \in Z_q^*$, computes $R_A = r_A P$ and sends (ID_A, P_A, R_A)to B.

(2) When B receives (ID_A, P_A, R_A)from A, she selects $R_B = r_B P$ and sends (ID_B, P_B, R_B)to A.

(3) Finally, A computes the session key

$K_{AB}=H_2(ID_A, ID_B, R_A, R_B, r_A R_B, e(R_A+Q_A, r_B P_0+D_B), P_A, P_B, r_A P_B, x_A R_B)$

And B computes the session key

$K_{BA}= H_2(ID_A, ID_B, R_A, R_B, r_B R_A, e(R_A+Q_A, r_B P_0+D_A), P_A, P_B, x_B R_A, r_B P_A)$

This protocol achieves most of the well-known security attributes, but does not achieve known session-specific temporary information security. Our analysis is as follows:

In[5], a certificateless key agreement scheme is Strong Type II secure if every probabilistic, polynomial-time adversary M has negligible advantage in winning the game subject to the following constraints:

1) M is given the master secret key s at the start of the game,

2) M may corrupt at most one additional type of secret per party participating in the test query.

Assume a malicious KGC who knows the master-key and get the ephemeral secret r_A and r_B, he can do the computation as follows:

$x_A R_B = r_B P_A$, thus the KGC can compute $x_A R_B$ with $r_B P_A$,

$e(R_A+Q_A, r_B P_0+D_B) = e(R_A+Q_A, r_B P+Q_B)^s$, thus the KGC can easily compute it out since it has nothing

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to do with xA.

Then the KGC can get the session key $K_{AB}=H_2(ID_A, ID_B, R_A, R_B, r_AR_B, e(R_A+Q_A,r_AP_0+D_A), P_A, P_B, r_AP_B, x_AR_B)$

As we mentioned, the protocol proposed in[6] is not Strong Type II secure and it not meets the requirement of known session-specific temporary information security .

4. AN EFFICIENT CERTIFICATELESS TWO-PARTY KEY AGREEMENT

We propose a new A new certificateless two-party key agreement. The protocol involves three entities, the communicating users A and B and the key generation center (KGC) from which the protocol participants are issued their respective partial private keys. The protocol description is as follows:

System setup:

this algorithm runs as follows.

(1) Select a cyclic additive group G_1 of prime order P, a cyclic multiplicative group G_2 of the same order, generator g and h of G_1, and a bilinear map $e : G_1 \times G_1 \rightarrow G_2$.

(2) Choose cryptographic hash functions $H: \{0,1\}^* \rightarrow \{0,1\}^k$,where k=|SK|.

(3) KGC chooses a master-key $\alpha \in Z_p^*$, computes $g_1 = g^{\alpha}$, publish the parameters (g, g_1, h)

4) For each party ID_i, KGC computes $h_{ID} = g^{1/(\alpha \cdot ID_i)}$

Then each party randomly chooses $x_{ID} \in Z_p^*$, generates his private key $d_{ID} =< x_{ID}, h_{ID} >$

Key agreement:

A computes $g_A = (g_1)^{ID_A x_A}$, B computes $g_A = (g_1)^{ID_B x_B}$ As their public keys .

1) A randomly chooses $x \in Z_p^*$, computes $T_{A1} = H_{ID_A}{}^{x/x_A} = g^{x/(\alpha \cdot ID_A \cdot x_A)}$ $T_{A2} = g_T^{x}$ $T_{A3} = g_T^{x_A}$ and send $(ID_A, g_A, T_{A1}, T_{A2}, T_{A3})$ to B

2) B randomly chooses $y \in Z_p^*$, computes $T_{B1} = H_{ID_B}{}^{y/x_B} = g^{y/(\alpha \cdot ID_B \cdot x_B)}$ $T_{B2} = g_T^{y}$ $T_{B3} = g_T^{x_B}$ and send $(ID_B, g_B, T_{B1}, T_{B2}, T_{B3})$ to A

3) A receives (ID_B,g_B,T_B) and computes:

$$K_{AB1} = e(T_{B1}, g_B{}^{x}) = e(g^{\frac{y}{\alpha \cdot ID_B \cdot x_B}}, g^{x\alpha x_B ID_B}) = e(g,g)^{xy}$$

$$K_{AB2} = (T_{B2} \cdot T_{B3})^{(x+x_A)} = (g_T{}^{y} \cdot g_T{}^{x_B})^{(x+x_A)} = e(g,g)^{(y+x_B)(x+x_A)} = e(g,g)^{xy+x_Bx+yx_A+x_Ax_B}$$

B receives (ID_A,g_A,T_A) and computes:

$$K_{BA1} = e(T_{A1}, g_A{}^{y}) = e(g^{\frac{x}{\alpha \cdot ID_A \cdot x_A}}, g^{x\alpha x_A ID_A}) = e(g,g)^{xy}$$

$$K_{BA2} = (T_{A2} \cdot T_{A3})^{(y+x_B)} = (g_T{}^{x} \cdot g_T{}^{x_A})^{(y+x_B)} = e(g,g)^{(x+x_A)(y+x_B)} = e(g,g)^{xy+x_Bx+yx_A+x_Ax_B}$$

obviously,

$K_{AB1} = K_{BA1} = e(g,g)^{xy}$

$K_{AB2} = K_{BA2} = e(g,g)^{xy+x_Bx+yx_A+x_Ax_B}$

Therefore, the session key which ID_A and ID_B agreed is :

$$SK = H(T_{A1}||T_{B1}||g_T{}^{xy}||g_T{}^{xy+x_Bx+yx_A+x_Ax_B})$$

5. PROTOCOL ANALYSIS

5.1 Security Analysis

In this section, we discuss the attributes described in section 2.1 the proposed protocols possess.

Theorem 1. The protocol has Resistance to Key-Compromise Impersonation (KCI) attacks provided the CDHP assumption holds and the hash functions are modelled as random oracles. The compromise of A's private key should not allow the adversary M to establish a session key with A by masquerading as a different entity B.

Proof. Asuume that A_l can attack with the private key by an arithmatic F_l ,the challenger C can solve the CDHP problem with the forge capability of A_l.

CDHP problem. give $g_T^{x_A}$, g_T^{y}, compute $g_T^{x_Ay}$

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

C run the system setting and get the public parameters.C keep some lists named $ListH_0$, List-g_{ID_i} ,List-T. according to ID_i , A_I run the queries and achieve the responses as follow:

1）H_0 queries: with a given user ID_i ,C run the steps as follow:Response A_I with D_i if（ID_i, D_i）already exist in $ListH_0$,otherwise compute （ID_i, D_i）,record in $ListH_0$ and response to A_I.

2）public key queries: with a given user ID_i ,C check the List-g_{ID_i},response A_I with g_{ID_i} if （ID_i, * , * ）exist, otherwise C choose $x_{ID_i} \in Z_p^*$ randomly,compute $g_{ID_i} = g_T^{ID_i}$, response A_I with g_{ID_i} and record it in List-g_{ID_i}.

3）session key queries:with a given user ID_i , C check the List-T,response A_I with (g_{ID_i}, T_{ID_i1}, T_{ID_i2}) if（ID_i, *, *, *） exist ,otherwise Cchoose $x \in Z_p^*$,compute $T_{ID_i1} = D_{ID_i}^{\ x}$ $T_{ID_i2} = g_T^x$,response A_I with g_{ID_i}, T_{ID_i1}, T_{ID_i2} and record （ID_i, g_{ID_i}, T_{ID_i1}, T_{ID_i2}） in List-T.

4) key agreement:with given users B and A ,C first get the public key of A and B by H_0,then get user B's private key S_B from list. A_I choose $x^* \in Z_p^*$,compute $T_{A1}{}^* = D_A{}^{x^*}$ $T_{A2}{}^* = g_T^{x^*}$ send (ID_A, g_A, $T_{A1}{}^*$, $T_{A2}{}^*$) to C, C check the list and response (ID_B, g_B, T_{B1}, T_{B2}) to A_I.

Assume that A_I finish the queres and successfully generate a session secret with user B pretending A, then C can get formulas as follows.

$$K_{A_IB1} = K_{BA_I1},\quad K_{A_IB2} = K_{BA_I2}\ ,$$

Thus

$$K_{A_IB2} = e(g,g)^{yx_A^* + x_A^* x_B} = e(g,g)^{x_A(y+x_B)}$$

$$e(g,g)^{x_A^* y} = (e(g,g)^{x^* y})^{(x^*)^{-1}x_A^*}$$

Then compute

$$e(g,g)^{x_A y} = \frac{e(g,g)^{x_A^*(y+x_B)}}{e(g,g)^{x_A x_B}} = \frac{e(g,g)^{x_A^* y} e(g,g)^{x_A^* x_B}}{e(g,g)^{x_A x_B}} = \frac{(e(g,g)^{x^* y})^{(x^*)^{-1}x_A^*} e(g,g)^{x_A^* x_B}}{e(g,g)^{x_A x_B}}$$

Therefore, C can solve the CDHP problem with the capability of A_I if A_I can successfully generate a session secret with user B.

Theorem 2. The protocol has **Known session-specific temporary information secrecy** provided the CDHP assumption holds and the hash functions are modeled as random oracles. The compromise of the ephemeral secrets x and y of each entity should not affect the security of session key.

Proof. Asuume that A_I can attack with ephemeral secrets by an arithmatic F_I ,the challenger C can solve the CDHP problem with the forge capability of A_I.

CDHP problem. give $g_T^{x_A}$, g_T^y, compute $g_T^{x_A y}$

C run the system setting and get the public parameters.C keep some lists named $ListH_0$, List-g_{ID_i} ,List-T1. according to ID_i , A_I run the queries and achieve the responses from C as follow:

1）H_0 queries: with a given user ID_i ,C run the steps as follow:Response A_I with D_i if（ID_i, D_i）already exist in $ListH_0$,otherwise compute （ID_i, D_i）,record in $ListH_0$ and response to A_I.

2）public key queries: with a given user ID_i ,C check the List-g_{ID_i},response A_I with g_{ID_i} if （ID_i, * , * ）exist, otherwise C choose $x_{ID_i} \in Z_p^*$ randomly,compute $g_{ID_i} = g_T^{ID_i}$, response A_I with g_{ID_i} and record it in List-g_{ID_i}.

3）ephemeral secrets queries: with a given user ID_i ,C check the List-T1,response A_I with t_{ID_i} if （ID_i, *） exist, otherwise C choose $x \in Z_p^*$ as t_{ID_i} randomly, response A_I with t_{ID_i} and record （ID_i, t_{ID_i}） in List-T1.

that A_I finish the queres and successfully get K_{AB1} and K_{AB2} ,then C can compute as follows:

$$e(g,,g)^{x_B x} = g_B^x\ ,$$

$$e(g,,g)^{x_A y} = g_A^y$$

$$K_{AB1} = e(g,g)^{xy}\ ,$$

$$K_{AB2} = e(g,g)^{xy + x_B x + y x_A + x_A x_B}$$

Then C compute

$$K_{AB2}\cdot(g_B^x)^{-1}\cdot(g_A^y)^{-1}\cdot(K_{AB1})^{-1}$$

$$= e(g,g)^{xy + x_B x + y x_A + x_A x_B}\cdot e(g,g)^{-xy}$$

$$\cdot e(g,g)^{-x_B x}\cdot e(g,g)^{-y x_A}$$

$$= e(g,g)^{x_A x_B} = g_T^{x_A x_B}$$

Therefore, C can solve the CDHP problem with the capability of A_I if A_I can successfully get the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

session secret .

Lippold[5] also pointed out that it is important to keep the resistance to disclosure of ephemeral secrets even it is compromised to the KGC. Based on CDH problem ,the security is kept in our protocol.

Meanwhile, our protocol also meets the other properties as follows:

Known session key security:An adversary M may learn previous session keys but cannot learn any information about the session key held by a fresh oracle since each session key is computes with ephemeral secrets x and y $\in Z_p^*$ which are randomly chosen by parties A and B. This will make sure that different session key will be agreed in different turn even the same parties participate.

Unknown Key-Share (UKS) seurity. If A thinks that he is sharing a key with an entity B, then it should not happen that A is actually sharing that key with another entity M where M≠B since he has the real identity of the other participate B which will be used in the key agreement.

Forward secrecy. Assume the private keys of A and B are compromised, an adversary M can not computes the session key without the ephemeral secrets x and y, since he will meets the CDH problem when computing the $K_{AB1} = K_{BA1} = e(g,g)^{xy}$ or the$K_{AB2} = K_{BA2} = e(g,g)^{xy+x_Bx+yx_A+x_Ax_B}$.

Table 1 Security Properties Comparison

Protocol	**Security Properties**				
	PFS	KCI-R	UKS-R	KSSTIS	KRA-R
Protocol [6]	×	√	√	×	√
Protocol [7]	√	√	√	×	×
Protocol [11]	×	√	√	×	×
Protocol [12]	√	×	√	√	×
Our Protocol	√	√	√	√	√

Key control. Neither party should be able to influence the outcome of the key to be a specific value since the session key involves each utility's private key and randomly choosed ephemeral key which cannot be controlled by the others, thus our protocol satisfies the property of no key control generally

We give the comparison in security properties with some proposed protocol[6,7,11,12] as follows from which we show that our protocol is secure with all security properties satisfied.(PFS: Perfect Forward secrecy; KCI-R: Resistance to Key-Compromise Impersonation attacks; UKS-R: Unknown Key-Share (UKS) security; KSSTIS: Known session-specific temporary information secrecy; KRA-R: Resistance to key-replicating attack)

5.2 Efficiency analysis

We evaluate the efficiency by the comparison to existing AKA schemes in table 2 . Our protocol is not the optimal one but it has advantage in efficiency with all the security attributes satisfied.

Table 2 Efficiency Comparison

Protocol	**complexity**		
	Pairing	Multiplication	Exponentiation
Protocol [6]	1	0	4
Protocol [7]	4	2	1
Protocol [11]	1	2	1
Protocol [12]	1	3	0
Our Protocol	1	0	4

6 CONCLUSION

Based on the analysis of some proposed protocol, We give the construction for a strongly secure one round certificateless key agreement scheme and its security analysis with the computational bilinear Diffie-Hellman and the computational Diffie-Hellman assumptions hold. The proposed key agreement scheme is secure as long as each party has at least one uncompromised secret. Thus, our scheme is secure even if the KGC learns the ephemeral secrets of both parties. The protocol also satisfied with the known security properties meanwhile it keeps the nice efficiency.

Certificateless public key cryptography was only proposed in 2003, and thus many problems remain to be solved. One is to formalize a security model for certificateless authenticated two-party key agreement and establish a security proof for the proposed protocol which will be our future work.

SUPPORTED BY: National Natural Science Foundation of China (Grant No.61003245)， Fundamental Research Funds for the Central Universities(Grant No. SWJTU12CX099), Foundation of Sichuan Provincial Outstanding Young Academic Leaders Training Program（No. 2011JQ0027）

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCE

[1] Shamir A. Identity-based cryptosystems and signature schemes/ / Proceedings of the CRYPTO′84 , Lecture Notes in Computer Science 196. Berlin : Springer2Verlag , 1984 : 47253

[2] Boneh D , Franklin M. Identity-based encryption from t he Weil pairing/ / Proceedings of the CRYPTO′01 , Lecture Notes in Computer Science 2139. Berlin : Springer2Verlag ,2001 : 2132229

[3] Smart N. An ID-based authenticated key agreement protocol based on t he Weil pairing. Elect ronic Letters , 2002 , 38 (13) :6302632

[4] Smart N. An ID-based aut henticated key agreement protocol based on t he Weil pairing. lect ronic Letters , 2002 , 38 (13) :6302632

[5] Lippold G, Boyd C, Nieto JG. Strongly secure certificateless key agreement. In: Shacham H, Waters B, eds. Proc. of the Pairing-Based Cryptography (PAIRING 2009). LNCS 5671, Berlin/Heidelberg: Springer-Verlag, 2009. 206−230.

[6] WANG Sheng-Bao,CAO Zhen-Fu, DON G Xiao-Lei. Provably Secure Identity-Based Authenticated Key Agreement Protocols in the Standard Model [J]. CHINESE JOURNAL OF COMPUTERS,2007,30（10）:1842-1854.

[7] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Laih CS, ed. Proc. of the Advances in Cryptology (ASIACRYPT 2003). LNCS 2894, Berlin/Heidelberg: Springer-Verlag, 2003. 452−473.

[8] Lei Zhang, Futai Zhang, Qianhong Wu, Josep Domingo-Ferrer.Simulatable certificateless two-party authenticated key agreement protocol. Information Sciences ,2010, 1020–1030.

[9] Mandt TK, Tan CH. Certificateless authenticated two-party key agreement protocols. In: Okada M, Satoh I, eds. Proc. of the 11th Annual Asian Computing Science Conf. (ASIAN 2006). Secure Software and Related Issues, LNCS 4435, Berlin/Heidelberg: Springer-Verlag, 2008. 37−44.

[10] Wang SB, Cao ZF, Wang LC. Efficient certificateless authenticated key agreement protocol from pairings. Wuhan University Journal of Natural Sciences, 2006,11(5):1278−1282.

[11] Shi YJ, Li JH. Two-Party authenticated key agreement in certificateless public key cryptography. Wuhan University Journal of Natural Sciences, 2007,12(1):71−74.

[12] Wang SB, Cao ZF, Bao HY. Efficient certificateless authentication and key Agreement (CL-AK) for Grid computing. Int'l Journal of Network Security, 2008,7(3):342–347.