Research Journal of Information Technology 5(3): 81-86, 2013
DOI:10.19026/rjit.5.5791
ISSN: 2041-3106; e-ISSN: 2041-3114

Submitted: April 08, 2013 Accepted: May 03, 2013 Published: September 01, 2013

Research Article

Mutual-anonymity and Authentication Key Agreement Protocol

[1]Tao Feng, [1]Chuang Zou, [2]Chunyan Liu and [1]Zheng Hao
[1]School of Computer and Communication,
[2]School of Economics and Management, Lanzhou University of Technology, Lanzhou 730050, China

Abstract: According to the characteristics of trusted computation, we proposed an efficient pseudonym ring signature-based authentication and key agreement protocol with mutual anonymity. The use of ring signature can hide the identity information of communicating parties and effectively prevent the leakage of private information. Finally we derive a shared session key between them for their future secure communication especially in the trusted computation environment. Our protocol reaches the level of universally composable security and is more efficient.

Keywords: Anonymity, authentication and key agreement, ring signature, trusted computation, universally composable

INTRODUCTION

According to some of the more special cryptography applications, key agreement protocol also needs to protect the privacy of the communication. For instance, in trusted computing environment, protecting the privacy of the communication is one of the important functions of the trusted system. Trusted Computing Group (2009) released the TPM v 1.1 Privacy CA scheme and TPM v 1.2 Direct Anonymous testimony (DAA) scheme to realize the mutual anonymity to avoid their behavior tracking between the Trusted Platform Modules when they authenticate each other.

Anonymous digital signatures such as ring signatures (Xu *et al*., 2004; Bender *et al*., 2006), Direct Anonymous Attestation (Brickell and Li, 2010; Chen *et al*., 2010) and anonymous credentials (Camenisch and Lysyanskaya, 2004.) play an important role in privacy enhanced technologies. They allow an entity (e.g., a user, a computer platform, or a hardware device) to create a signature without revealing its identity. Anonymous signature also enable anonymous entity authentication.

Ring signatures, first introduced by Rivest, Shamir and Tauman, enable a user to sign a message so that a ring of possible signers (of which the user is a member) is identified, without revealing exactly which member of that ring actually generated the signature. In contrast to group signatures, ring signatures do not require any central authority or coordination among the various users(indeed, users do not even need to be aware of each other); Furthermore, ring signature schemes grant users fine-grained control over the level of anonymity associated with any particular signature.

In the existing key agreement protocol, Chow and Choo (2007) adopted the user group and identity-based cryptography to construct a two-way anonymous authentication key agreement protocol, but it needs more multiplication operation. Walker and Li (2010) realized an authentication key agreement protocol on the basis of the DAA, but it only realized unidirectional anonymity between communicating parties. Wei *et al*. (2011) put forward a higher efficiency anonymous authentication key agreement protocol based on password, which could satisfy mutual anonymity but did not made a formalized security analysis. In this study, we first construct a ring signature ideal functionality $F_{P\text{-}R\text{-}SIG}$ based on pseudonym and an anonymous authentication key agreement ideal functionality $F_{A\text{-}AKE}$. Finally we propose a mutual-anonymity and authentication key agreement protocol, which has a high efficiency and is more security. The proposed protocol is better suitable for the environment of trust computation and the derived session key can be used for their future secure communications.

PROBLEMS HYPOTHESIS

The scheme of this study is mainly based on the elliptic curve cryptosystem (Enge, 2013), discrete logarithm, bilinear pairings (Su *et al*., 2012) and strong impact resistance of one-way hash function. The definitions and related problems hypothesis as follows: Elliptic curve E (Fp) and p is a big prime number, not less than 160 bit. Let G a multiplicative cyclic group in E (F_p) of order p, P :a generator of G.

Definition 1: Computational Diffie-Hellman Problem: Given (P, aP, bP), compute abP.

Corresponding Author: Tao Feng, School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China

Key Generation

Let $C_{pi}(S_{pi})$ to be the pseudonym of $C_i(S_i)$,S is an adversary. Upon receiving a value (KeyGen,C_{pi} ,sid) from C_i , verify that sid = (C_{pi} ,sid') for sid'. If not, then ignore the request. Else, hand (KeyGen,C_{pi} ,sid) to the S. Upon receiving (VerKey,sid,C_{pi} ,y_i) from S, output them to C_i, record (C_{pi} ,y_i). C = {C_{p1},C_{p2}…C_{pN}} is a identity collection of pseudonym user who has executed the key generation process, the corresponding public key is Y = {y_1,y_2,…,y_N}.

Signature Generation

Upon receiving a value (P-R-Sign,sid,C_{pi} ,m) from C_i, verify that sid = (C_{pi} ,sid') for sid'. If not, or C_{pi} is not the subset of C, then ignore the request. Else send (P-R-Sign,sid,C_{pi},m) to S. Upon receiving (P-R-Signature,sid,S_{pi} ,m,σ) from S, verify that no entry (m,σ,y_i ,0) is recorded. If it is, then output an error message to C_i, else output (P-R-Signature,sid, C_{pi} ,m,σ) to C_i , and record the entry (m,σ,y_i ,1).

Signature Verification

Upon receiving a value (P-R-Sign-Verify,sid,m, S_{pi} ,σ,y_i) from S_i , hand it to S. Upon receiving (P-R-Sign-Verified,sid,m, S_{pi} ,σ, y_i ,φ) from S do:

- If y_i is the subset of Y, and the entry (m,σ,y_i,1) is recorded, then set f = 1
- Else ,if y_i is the subset of Y, and no enry (m,σ,y_i ,1) is recorded, then set f = 0,and record the entry (m,σ,y_i,0)
- Else, if there is an entry (m,σ,y_i ,f'), then let f = f'
- Else let f = φ and record the entry (m,σ, y_i ,φ). At last output (P-R-Sign-Verified,sid, S_{pi} , m,f) to S_i

Fig. 1: Ring signature ideal functionality based on pseudonym $F_{P\text{-}R\text{-}SIG}$

- When received (KeyGen,C_{pi} ,sid) from C_i, verify that sid = (C_{pi} ,sid') for sid'. If not, then ignore the request. Else, run the key generation algorithm KeyGen, save secret key x_i, then output (Verkey,sid,C_{pi} ,y_i). When received (P-R-Sign,sid,C_{pi} ,m) from C_i, execute P-R-Sign algorithm and obtain signature σ, then output (P-R-Signature,sid,C_{pi} ,m,σ).
- When received a value (P-R-Sign-Verify,sid,S_{pi} ,m,σ,Y') from verifier S_i, execute P-R-verify algorithm and obtain a verification value f, then output (P-R-Sign-Verified,sid,S_{pi} ,m,σ,Y',f).
- Wait to receive values (P-R-Sign-Verified, sid,C_{pi} ,m,σ,Y',f) or (P-R-Sign-Verified, sid,S_{pi}, m, σ, Y' ,f) from the parties C_i, S_i and an adversary S. Upon receiving the messages from the parties C_i or S_i, forward this message to S.
- After having received values (P-R-Sign-Verified, sid, C_{pi}, m, σ, Y' ,f) or (P-R-Sign-Verified, sid, S_{pi} ,m, σ, Y', f) from the parties C_i, S_i and S, proceed as follows:
  - If both C_i and S_i are uncorrupted, choose k'← $\{0,1\}^k$, k: a security parameter.
  - If at least one of the parties C_i and S_i is corrupted, send a message (choose-key, sid) to the adversary S. Upon receiving an answer (key, sid, k') from S, extract the value k' from it: Once k' is set, send (key, sid, k') to C_i and S_i, and send (key, sid) to the adversary S. Then halt.

Fig. 2: Anonymous authentication key agreement ideal functionality $F_{A\text{-}AKE}$

Definition 2: Decisional Diffie-Hellman Problem: Given (P, aP, bP, cP), decide whether c = ab.(a, b and c be elements of group Z_p).

Definition 3: The discrete logarithm problem: The discrete logarithm problem is the problem of finding the least positive integer a such that equation $h = g^a$ holds, when the element g, h∈G are given, provided this integer exists.

Let G_1, G_2 be two groups of the same prime order q. We view G_1 as an additive group and G_2 as a multiplicative group. Let P be an arbitrary generator of G_1. A mapping e: $G_1 \times G_1 \rightarrow G_2$ satisfying the following properties is called a bilinear map from a cryptographic point of view:

Definition 4: Bilinearity: e (aP, bQ) = $e(P,Q)^{ab}$ for all P,Q∈ G_1 and a, b∈Z*p.

Non-degeneracy: If P is a generator of G_1, then e (P, P) is a generator of G_2. In other words, e(P,P) ≠1.

Computable: There exists an efficient algorithm to compute e (P, Q) for all P, Q∈ G_1.

ANONYMOUS KEY AGREEMENT PROTOCOL SECURITY MODEL

Universally Composable (UC) security framework is a formal model based on the computational complexity theory to design and analyze security protocols (Canetti and Krawczyk, 2002a; Canetti, 2005a). The most outstanding properties is that it adopts the designing thought of modularization: we can design cryptographic protocols separately, as long as each sub-protocol meets UC safety, it can guarantee the security of assembling, parallel running with other protocols (Canetti *et al*., 2005b).

Ring signature anonymous authentication makes the receiver certitude that the sending party is a legal member in the ring, but don't know the specific identity. Because the identity of the signer will be recorded in the session identification (sid), others can know his true identity through the sid. In order to achieve anonymity, we use pseudonym to instead of the true signer's identity information in the sid. Here, we learn the signature thought from Canetti (2004) and use pseudonym technology instead of the specific identity of the members; we first construct a ring signature ideal functionality based on pseudonym $F_{P\text{-}R\text{-}SIG}$, as shown in Fig. 1:

As need to construct an anonymous authentication key agreement ideal functionality, the concept is learned from Canetti and Krawczyk (2002b) and Hofheinz *et al*. (2003), the constructed anonymous authentication key agreement ideal functionality $F_{A\text{-}AKE}$ is show in Fig. 2:

THE NEW ANONYMOUS AUTHENTICATION KEY AGREEMENT PROTOCOL

The network model of the protocol is shown in Fig. 3, each user and server has a unique identity in the trusted environment. All users need to be registered on the servers before performing key agreement, besides; all users and servers are needed to be divided into groups. In the key agreement process, the users and the

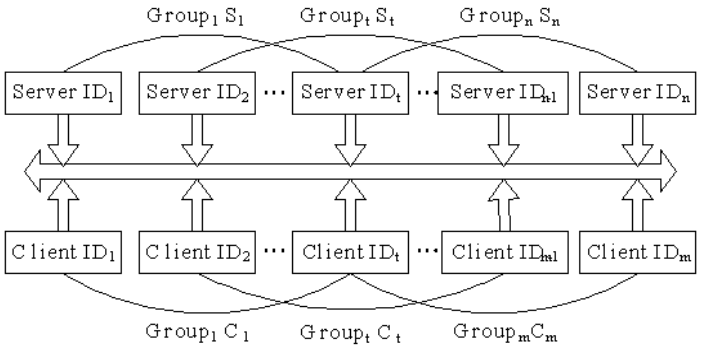

Fig. 3: The network model of the protocol

Table 1: The symbols and their meanings in this study

Symbol	Meaning
H_u: $\{0,1\}^t_u \rightarrow G$	Collision-resistance one-way hash function, generate identity information
H_m: $\{0,1\}^* \rightarrow Z^*p$	Collision-resistance one-way hash function, generate message information
ID_{si}	Server identity
ID_{ci}	User identity
S	Identity collection of all the servers in the network
C	Identity collection of a group of users

servers both communicate using pseudonym. The symbols and their meanings in this study are shown in Table 1.

In this study, the mutual anonymous authentication key agreement protocol based on pseudonym ring signature is divided into three phases:

- System initialization
- Registration phase
- Key agreement

System initialization: The Trusted third party is responsible for generating system parameters in the network. The specific steps are as follows:

- TTP chooses a large prime p, $p \geq 2^{160}$, constructs the cyclic group G and the elliptic curve E (F_p) as in the second chapter
- Bilinear map: e: $G \times G \rightarrow G_T$, G of order p is a multiplication cyclic group, g is a generator of G.
- Assume that there exist n servers S = $\{ID_{s1}, ID_{s2}, \ldots, ID_{sn}\}$ in the trusted network
- TTP publishes the system parameters (p, q, e, E, G, G_T, g, H_u, H_m)

Registration phase: Each user in the user group C = $\{ID_{c1}, ID_{c2}, \ldots, ID_{cm}\}$ needs to be registered in the servers of S, every user group is assigned to a server group by the server administrator and produces a ring signature on the server group identity set. Accordingly every user can also produces a ring signature on the user group identity set.

Assume that user $ID_{c\pi}$ ($ID_{c\pi} \in C$) needs to communication with server $ID_{s\pi}$ ($ID_{s\pi} \in S$), the registration process would be: The server administrator selects t servers as a server group from n servers randomly, records as $S_\pi = \{ID_{s1}, ID_{s2}, \ldots, ID_{st}\}$ and server $ID_{s\pi}$ must be selected as the default server. At here, we learn the ring signature scheme thought from Yu *et al*. (2012), the specific signature steps are as follows:

- $ID_{s\pi}$ randomly selects integer $s \in_R Z^*_p$, computes $g_1 = g^s$, selects $g_2 \in_R G$, $u' \in_R Z_p$,let $U = (u_i)$ for t_u dimensional vector, $u_i \in_R Z_p$, publishes the system parameters $P_{pub} = (p, g, g_1, g_2, u', U, H_u, H_m)$,master key $k_{mk} = g^s_2$
- Suppose $v_j = H_u(ID_{sj})$, $v_j[i]$ is the ith bit of $v_j \subset \{1, \ldots, t_u\}$, also satisfies that $v_j[i] = 1$ and the collection of subscript i. Randomly selects $r_{uj} \in Z_p$, computes $f_j[u] = u' + \sum_{i \in u_j} u_i \bmod p$, so the secret key of ID_{sj} is $d_j = ((g^s_2 g^{f_j(u)})^{r_{uj}}, g^{r_{uj}}) = (d_{j1}, d_{j2})$
- $ID_{s\pi}$ signs on the message M, its secret key is $d_{s\pi} = (d_{\pi 1}, d_{\pi 2})$, computes $m = H_m(S_\pi, M)$, the signature process: for $j \in \{1,2,\ldots,t\} / \{\pi\}$, selects $r_j \in_R Z^*_p$ and computes $R_j = g^{rj}$, $h_j = H_m(S_\pi, m, R_j)$; When $j = \pi$, selects $l, r_\pi \in_R Z^*_p$, computes $R_\pi = g^{r_\pi} (g^{r_{u\pi}})^l$, $h_\pi = H_m(S_\pi, m, R_\pi)$; Then computes $S = d^{lgh_\pi}_{\pi 1} g^{\sum_{j=1}^{n} f_j(u) r_j h_j}$, $Z = g^{lgh_\pi}_2$; The ring signature on message M is $\sigma = (Z, S, R_1, R_2, \ldots, R_t)$
- And further, the server $ID_{s\pi}$ randomly selects integer s, $x_S, 2 \leq x_S \leq q-1$,computes $X_S = g^{xS} \bmod p$, $S_p = (S_\pi, H_n(s))$, S_p is the pseudonym of server $ID_{s\pi}$, used for communication between with the users later, finally, the server $ID_{s\pi}$ sends $M, S_\pi, \sigma, X_S, s, S_p$ to the user $ID_{c\pi}$ through a appropriate safe way

- Upon receiving the messages, $ID_{c\pi}$ computes $S'=S/\prod_{j=1}^{t} R_j^{f_j(u)h_j}$ j = 1, 2, …, t, $S'_p = (S_\pi, H_n(s))$. Verifies whether e(S', g) = e(g_1,Z) and $S_p = S'_p$ are established. If established, keeps X_S safely; Else, re-registers
- User $ID_{c\pi}$ uses the same signature methods and steps as the server $ID_{s\pi}$: let $C_\pi = \{ID_{c1}, ID_{c2}, \ldots, ID_{ct}\}$ for t users identity list, the actual identity of the signer is $ID_{c\pi} \in C_\pi, (\pi \in \{1,2,\ldots,n\})$ and then the ring signature on message M is $\sigma = (Z', S'', R'_1, R'_2, \ldots, R'_t)$
- And further, the user $ID_{s\pi}$ randomly selects integer c, x_c, $2 \le x_c \le q-1$,computes $X_c = g^{xC} \bmod p$, $C_p = (C_\pi, H_n(c))$, C_p is the pseudonym of user $ID_{c\pi}$, used for communication between with the servers later, finally, the user $ID_{c\pi}$ sends M, C_π,σ', X_C, c, C_p to the user $ID_{s\pi}$ through a appropriate safe way
- When server $ID_{s\pi}$ receives the messages, computes S'', $C'_p = (C_\pi, H_n(c))$, verifies whether e (S'',g) = e (g_1,Z') and $C_p = C'_p$ are established. If established, keeps X_C safely; else, re-registers.

Key agreement: After registration, it is assumed that user $ID_{c\pi}$ and server $ID_{s\pi}$ need to conduct the anonymous key agreement, procedure is as follows:

- Server $ID_{s\pi}$ selects two random integer r_S, a, $2 \le r_S$, $a \le q-1$ and then computes $M_S = X_S^{r_S} \bmod p = g^{x_S r_S} \bmod p$, $N_S = g^a \bmod p$, $S_S = x_S r_S + x_S + a \bmod q$ and next sends (M_S,N_S,S_S) to user $ID_{c\pi}$
  After user $ID_{c\pi}$ received (M_S, N_S, S_S): Computes "·" $S'_S = g^{S_S} \bmod p = g^{x_S r_S + x_S + a} \bmod p$; Computes $X'_S = S'_S M_S^{-1} N_S^{-1} \bmod p$ and compares it with X_S, if equal, user $ID_{c\pi}$ selects two random integer r_C,b,$2 \le r_C$, $b \le q-1$ and then computes $M_C = X_C^{r_C} \bmod p = g^{x_C r_C} \bmod p$, $N_C = g^b \bmod p$, $S_C = x_C r_C + x_C + b \bmod q$ and next sends (M_C, N_C, S_C) to server $ID_{s\pi}$. Calculates the session key: $k_e = M_S^{x_C r_C} \bmod p = g^{x_S r_S x_C r_C} \bmod p$
- After server $ID_{s\pi}$ received (M_C, N_C, S_C): Computes $S'_C = g^{S_C} \bmod p = g^{x_C r_C + x_C + b} \bmod p$; Computes $X'_C = S'_C M_C^{-1} N_C^{-1} \bmod p$ and compares it with X_C, if not equal, terminates the agreement, else, calculates the session key: $k_e = M_C^{x_S r_S} = g^{x_C r_C x_S r_S} \bmod p$

Finally, the user and the server consult out a consistent session key $k_S = H_m(k_e, M_S, M_C, S_S, S_C)$.

SECURITY ANALYSIS OF THE PROTOCOL

There are several tests to prove the security of the protocol:

- Any input from the environment machine Z will be transmitted to A, any output of A is copied to Z's output (to be read by Z).
- Whenever S receives a message (KeyGen, sid,C_{pi}) from $F_{P\text{-}R\text{-}SIG}$, it does: if sid is not of the form (C_{pi}, sid') then ignores this request. Otherwise, S selects y_i and records it, returns (Verification key, sid, C_{pi}, y_i) to $F_{P\text{-}R\text{-}SIG}$.
- Whenever S receives a message (P-R-Sign, sid, C_{pi}, C', m) from $F_{P\text{-}R\text{-}SIG}$, if sid = ($C_{pi}$, sid') and there is a recorded signing key y_i, then S computes σ = sig(y_i,m), and hands (P-R-Signature, sid,C_{pi}, m, C', σ) back to $F_{P\text{-}R\text{-}SIG}$. Otherwise, it does nothing.
- Whenever S receives(P-R-Sign-Verify,sid, C_{pi}, m, C', y_i) from $F_{P\text{-}R\text{-}SIG}$, it returns (P-R-Sign-Verified, sid, C_{pi}, m, C', y_i, σ).
- When A corrupts some party C_i, S corrupts C_i in the ideal process. If C_i is the signer, then S reveals the signing key s as the internal state of C_i.

Fig. 4: Simulator S

- Prove that our pseudonym-based ring signature protocol ρ_{rs} safely realizes the ideal functionality $F_{P\text{-}R\text{-}SIG}$
- Prove that our anonymous authentication key agreement protocol π' safely realizes the ideal functionality $F_{A\text{-}AKE}$ in the $F_{P\text{-}R\text{-}SIG}$-hybrid model
- Use universally composable theorem, put ρ_{rs} and π' together and prove that the combined protocol is equivalent of protocol π: pseudonym ring signature-based authentication and key agreement protocol with mutual anonymity and safely realizes $F_{P\text{-}R\text{-}SIG}$ and $F_{A\text{-}AKE}$ in the real life model

Lemma 1: If CDH assumption is established, the corresponding ring signature protocol ρ_{rs} UC realizes the ideal ring signature functionality $F_{P\text{-}R\text{-}SIG}$.

Proof: Assume that ring signature protocol ρ_{rs} can't UC realizes the ideal ring signature functionality $F_{P\text{-}R\text{-}SIG}$, this is done by constructing an environment Z and a real-life adversary A such that for any ideal-process adversary S, Z can tell whether it is interacting with A and ρ_{rs} or with S in the ideal process for $F_{P\text{-}R\text{-}SIG}$. The simulation process is shown in Fig. 4:

If an attacker can forge a ring signature, for the given input (P-R-Sign-Verify, sid, m, C', σ, Y'), according to the output record under the execution of S, Z can tell whether it is interacting with real-life protocol ρ_{rs} or the ideal protocol $F_{P\text{-}R\text{-}SIG}$. Therefore, the probability of forging successfully is negligible, contradicting with the assumption. So the lemma 1 is proved.

Lemma 2: If DDH assumption is established, Then protocol π' securely realizes the $F_{A\text{-}AKE}$ in the hybrid model.

Proof: Construct an attacker S (Fig. 5) in the ideal environment first, make any of the environment machine Z can't tell whether it is interacting with attacker H and π' in the $F_{P\text{-}R\text{-}SIG}$-hybrid model, or with S

Table 2: The calculation cost comparison of anonymous authentication key agreement protocol

Scheme	Problems Hypothesis	The Calculation Cost	Security Model
Chow and Choo (2007)	Elliptic Curve Crptograhpy; Bilinear Pairings; Bilinear Diffie-Hellman Problem	$2(2m+1)T_{emul}+2T_{ebp}=(29(2m+1)/120+14)T_{exp}$	Indistinguishability-based model of Canetti and Krawczyk
Wei *et al*. (2011)	RSA	$mT_{mul}+(7+m)$ $T_{exp}=(1/240+7+m)\ T_{exp}$	Random Oracle Model
Our protocol	RSA algorithm; Elliptic Curve Crptograhpy; Computational Diffie-Hellman and Decisional Diffie-Hellman Problem	4 Tmul +8 Texp = (1/60+8) Texp	Universally compostable model

S run H, H is an attack in the hybrid model, the rules are as follows:

- Any input from Z will be passed to H, and all the outputs of H will be seen as the outputs of S, Z can read their outputs.
- When S receives (sid, C_{pi}, S_{pi}, role) from $F_{A\text{-}AKE}$, it indicates that C_i launched the authentication key agreement, so let S simulate out π' that interacts with H in the $F_{P\text{-}R\text{-}SIG}$ and $F_{P\text{-}R\text{-}SIG}$-hybrid model. And given the same input, S lets C_i and H interact with Z according to the execution rules of π'.
- In order to simulate the implementation of π', $F_{P\text{-}R\text{-}SIG}$ can be activated by S to get the corresponding signature value σ, S can also computes k = prf (r, •), r is the output key of C_i and S_i in $F_{A\text{-}AKE}$.
- When C_i produces a local output, and S_i is not corrupted, S will sends the output of $F_{A\text{-}AKE}$ to C_i; If S_i has be corrupted, the key value is decided by S, and S uses the previous output of C_i to determine the local output of simulated C_i and S_i .
  When H executes the operation of capturing C_i , S also captures C_i . If $F_{A\text{-}AKE}$ has sent a key to C_i, S will get the key; If both of the C_i and S_i do not produce a local output, S sends its internal state to H, as well as their secret selected value; If either C_i or S_i has produced a local output, their temporary private keys will be wiped out, S directly passes the local key to H.

Fig. 5: Simulator S

- The probability of 1/2 to choose Q←{Q_0,Q_1}as D's input, recorded as(p, q, g, α*, β*, γ*);
- Randomly choose τ← {1,2,…l},l is the upper bound number that the attacker can initiate the conversations, and then simulates the interaction of H and Z with π' in $F_{P\text{-}R\text{-}SIG}$– hybrid.
- When H activates a new session t (t ≠ τ) that a participant established or receives a message, D represents this participant who conducts a normal interaction in $F_{P\text{-}R\text{-}SIG}$– hybrid in accordance with the protocol π'. If t = τ, then D represents that C_i sends message(C_{pi}, sid, α*) to S_j; When S_j receives (C_{pi},sid, α*),D calls $F_{P\text{-}R\text{-}SIG}$ for the corresponding calculations and sends (sid, β*,σ_j) to C_i; At last, D lets the output of C_i and S_j is (sid, C_{pi}, S_{pj}, γ*).
- If H captured a participant, then D sends the internal state of this participant back to H; If the corrupted participant is one of the participants of session t, then D outputs a random bit b' ← {0,1}, and terminates.

If the protocol π' in $F_{P\text{-}R\text{-}SIG}$-hybrid runs out, Z outputs b, then D outputs b' and terminates.

Fig. 6: Distinguisher D

and $F_{A\text{-}AKE}$ in the ideal-life. That is for any environment Z, we have $F_{P\text{-}R\text{-}SIG}$-$hybrid_{\pi',H,Z}\approx IDEAL_{F,S,Z}$.

Assume that under the execution of S, if there exists an environment machine Z, the probability of successfully distinguishing whether it is interacting with H and π' in the $F_{P\text{-}R\text{-}SIG}$-hybrid model or S and $F_{A\text{-}AKE}$ in the ideal-life can not be ignored. That is the probability of $F_{P\text{-}R\text{-}SIG}$-$hybrid_{\pi',H,Z}\neq IDEAL_{F,S,Z}$ is 1/2+ε and the value is much greater than 1/2, ε is the distinguished advantage of Z'. We construct a distinguisher D, as shown in Fig. 6. Using the environment machine Z' to crack the DDH problem.

Analyzing the execution of the distinguisher D, if its input (p, q, g, α*, β*, γ*) is selected from Q_0, then γ* is the real key of C_i and S_j after the execution of π', in this case, environment machine Z' saw the local output and its angle is equal to the execution of π' and H in $F_{P\text{-}R\text{-}SIG}$-hybrid; If (p, q, g, α*, β*, γ*) is selected from Q_1, then γ* is a random value, in this case ,the angle of the environment machine Z' is equal to the execution of S and $F_{A\text{-}AKE}$ in the ideal model. Because in the ideal model, the key that $F_{A\text{-}AKE}$ sends to C_i and S_j is just the random value selected by it. According the constructed principle of the distinguisher, the probability of successfully distinguishing is equal to the probability of environment machine Z' successfully discriminating the ideal and hybrid environment. Namely the probability of D successfully distinguishing Q_0 and Q_1 is 1/2 +ε and it contradicts with DDH assumption, so the lemma 2 is proved.

Theorem 1: In the real-life model, the protocol π securely realizes ideal functionality $F_{A\text{-}AKE}$ and for any environment machine Z, equation $REAL_{\pi,A,Z}\approx IDEAL_{FA\text{-}AKE,S,Z}$ is established, so the mutual-anonymity and authentication key agreement protocol is safety under UC model.

EFFICIENCY ANALYSIS

The system initialization and registration process of the new protocol can be obtained by pretreatment, we compare our protocol with Chow and Choo (2007) and Wei *et al*. (2011) and only consider the operations that the calculation cost is relatively large including modular exponentiation, point multiplication, inverse, bilinear pairings and modular multiplication operations. Let T_{exp},T_{emul}, T_{ebp},T_{mul}, respectively denote the cost of modular exponentiation, point multiplication, bilinear pairings and modular multiplication operations and m is the size of the group.

From Koblitz *et al*. (2000) and Chen *et al*. (2007), we can deduce: $T_{exp}\approx240\ T_{mul}$, $T_{emul}\approx29\ T_{mul}$,$T_{inv}\approx[0.3843lnq+1.47]T_{mul}$, $T_{ebp}\approx7\ T_{exp}$.Table 2 shows that our protocol has a higher execution efficiency.

CONCLUSION

This study puts forward a mutual-anonymous key agreement protocol based on pseudonym ring signature,

the scheme satisfies unconditional anonymity between the communicating parties and protects the privacy of communications, achieves universally composable security. The system initialization and registration process of the new program can be obtained by pretreatment and it has a high efficiency, can better meet the scenarios of the trusted computing environment.

ACKNOWLEDGMENT

This study is supported by The National Natural Science Foundation of China (60972078) and Universities Basic Scientific Research Operation Cost of Gansu Province (0914ZTB186) and The Ph.D. Programs Foundation of Lanzhou University of Technology (BS14200901).

REFERENCES

Bender, A., J. Katz and R. Morselli, 2006. Ring signatures: Stronger definitions and constructions without random oracles. In: Halevi, S., and T. Rabin (Eds.), TCC 2006. Sprigner, Heidelberg, LNCS, 3876: 60-79.

Brickell, E. and J.T. Li, 2010. A pairing-based DAA scheme further reducing TPM resources. Proceeding of the 3rd International Conference Trust and Trustworthy Computing. Springer, 6101: 181-195.

Camenisch, J. and A. Lysyanskaya, 2004. Signature schemes and anonymous credentials from bilinear maps. Adv. Cryptol., 3152: 56-72.

Canetti, R. and H. Krawczyk, 2002a. Universally composable notions of key exchange and secure channels. Adv. Cryptol., 2332: 337-351.

Canetti, R. and H. Krawczyk, 2002b. Security analysis of IKE's signature-based key-exchange protocol. Adv. Cryptol., 244: 143-161.

Canetti, R., 2004. Universally composable signature, certification and authentication. Proceeding of 17th IEEE Computer Security Foundations Workshop, Long Version. Retrieved from: http://eprint. iacr.org/ 2003/239.

Canetti, R., 2005a. Universally composable security: A new paradigm for cryptographic protocols. Proceedings of the 42nd Symposium on Foundations of Computer Science (FOCS), pp: 136-145. Full Version. Retrieved from: http://eprint.iacr.org/2000/067.

Canetti, R., S. Halevi and J. Katz, 2005b. Universally composable password based key exchange. Adv. Cryptol., 3494: 404-421.

Chen, L.Q., D. Page and N.P. Smart, 2010. On the design and implementation of an efficient DAA scheme. Proceeding of the 9th Smart Card Research Conference Advanced Application IFIP. Springer, Heidelberg.

Chen, L., Z. Cheng and N.P. Smart, 2007. Identity-based key agreement protocols from pairings. Int. J. Inform. Secur. Priv., 6(4): 213-241.

Chow, S.S.M. and K.K.R. Choo, 2007. Strongly-secure identity-based key agreement and anonymous extension. Inform. Secur., 4779: 203-220.

Enge, A., 2013. Elliptic Curve Cryptographic Systems. Handbook of Finite Fields.

Hofheinz, D., J. Muller-Quade and R. Steinwandt, 2003. Initiator-Resilient Universally Composable Key Exchange. Proceeding of European Symposium on Research in Computer Security (ESORICS, 2003).

Koblitz, N., A. Menezes and S. Vanstone, 2000. The state of elliptic curve cryptography. Designs, Codes Cryptograp., 19: 173-193.

Su, Z.T., C.H. Sun, H. Li and J.F. Ma, 2012. A method for efficient parallel computation of Tate pairing. Int. J. Grid Utility Comp., 3(1): 43-52.

Trusted Computing Group, 2009. Trusted Computing Group Home Page. Retrieved from: https:// www. trustedcomputinggroup.org/home.

Walker, J. and J. Li, 2010. Key exchange with anonymous authentication using DAA-SIGMA protocol. Proceedings of the 2nd International Conference on Trusted Systems. Springer-Verlag, Berlin, pp: 108-127.

Wei, F.S., C.G. Ma and Q.F. Cheng, 2011. Anonymous gateway-oriented password-based authenticated key exchange based on RSA. EURASIP J. Wirel. Comm., pp: 1-12, Doi: 10.1186/1687-1499-2011-162.

Xu, J., Z. Zhang and D. Feng, 2004. A ring signature scheme using bilinear pairings. Proceedings of the 5th International Conference on Information Security Applications. Springer-Verlag Berlin, 3325: 160-169.

Yu, T., Z. M. Zhao and X.F. Ren, 2012. Efficient identity-based ring signature in standard model. J. Comput. Appl., 32(7): 2015-2017.