

An Novel Anonymous Authenticated and Key Exchange Protocol

Hui Cui¹

¹School of Computer, China University of Mining and Technology, Xuzhou, China
snager@163.com

Tianjie Cao²

²School of Computer, China University of Mining and Technology, Xuzhou, China
tjcao@cumt.edu.cn

Abstract—Because of the growing importance in the fields of computer networks, how to keep user's privacy has drawn more and more concerns in recent years. In this paper, we first point out that the two given anonymous password-based authenticated and key exchange protocols are vulnerable to the anonymity attack. Then based on a ring signature scheme, we propose a new secure anonymous authenticated and key exchange protocol, which inherits all the good virtues of the previous protocols. Furthermore, we discuss the security attributes of our new scheme. Finally, we give an extension of our new scheme's application and make a conclusion of this paper.

Index Terms—ring signature; anonymous authentication; key exchange

I. INTRODUCTION

Due to the growing importance in the application of computer networks [1], authentication supporting key exchange has been widely used to protect resource from illegal access. However, traditional authentication supporting key exchange schemes require that the identity of a user be explicitly specified to facilitate authentication and further key exchange, which may violate user's privacy in some privacy-sensitive applications, such as online drug stores. In order to solve such seemingly paradoxical issue (proving the legitimacy of a user without revealing his identity), many schemes have been proposed, but most of them exist some security vulnerabilities.

A. Anonymity in Authentication Scheme

As far as user privacy and anonymity is concerned, research on this topic usually focuses on two issues: anonymous communication and user anonymity [2]. Anonymous communication [3] usually provides a communication channel that resists traffic analysis, so that the communicating parties can be anonymous against the eavesdroppers. Research on anonymous communication focuses on providing a communication channel that is immune to traffic analysis so that the communicating parties can be anonymous against the eavesdroppers. A more complicated and seemingly paradoxical issue is user anonymity, which aims at providing the users anonymity while they are using the

network by letting them hide their identity from the communicating peers. In this paper we will discuss user anonymity in authentication scheme.

User anonymity existing in an anonymous authentication scheme [4] is a protocol that allows a member called a prover of a group to convince a verifier that he is a member of the group without revealing any information about his identity. An immediate way to achieve user anonymity is to assign an alias name to each user, and a user will use his alias name to login to perform key exchange with the server, instead of using his real identity. However, such idea does not work since the server could always match user's alias name with his real identity.

User anonymity is first addressed in the setting of digital signature with the introduction of group signature [5]. A group signature allows each group members to sign on behalf of the whole group anonymously without revealing his own identity. So the verifier of the group signature could not tell who is the real signer in the group. User anonymity is also achieved in ring signature proposed by Rivest, Shamir and Tauman [6], where a signer takes a list of public key of other people as input to sign a message, and a signature verifier could not spot the real signer in the public key list.

Both ring and group signatures share the same idea of achieving user anonymity. The idea is to hide one's own identity among a group of identities. The difference between ring signature and group signature is that the group is formed more freely in the setting of ring signature [7]. In ring signature, the public key list which implicitly defines a group is composed by a signer himself without the help of a group manager, and the signer needs not to inform or interact with people involved in the list. While in the setting of group signature, a user must join the group first by interacting with a group manager to obtain a group membership. Therefore, it is more attractive to achieve user anonymity in a ring fashion.

B. Related works

Authentication schemes that deal with anonymous issue are proposed by Chien.H.Y., Chen.C.H. [8] and Viet,D.Q., Yamamura.A. and Tanaka.H [9] respectively. However, the former in deed deals with anonymous

communications but not user anonymity, and the latter uses password tables at server side and needs lots of exponential operations. Jing Yang et al. [10] firstly points out the vulnerabilities of both Viet et al. and Shin et al. distributed anonymous PAKE protocols, and then proposes a new anonymous password-based authenticated and key exchange (JZH) protocol. Zhenchuan Chai et al. [11] also propose an efficient password-based authentication and key exchange (CHCL) scheme to preserve user privacy. Both of them try to achieve user anonymity without using the group or ring signature schemes, however, through analysis, we find that their user anonymity both exist security defects.

C. Our Contributions

Our contributions in this paper can be summarized as three points.

Firstly, we analyse two anonymous authenticated and key exchange protocols, CHCL and JZH protocols, and find out the vulnerabilities of them.

Secondly, we propose a new anonymous password-based authenticated and key exchange protocol with using a ring authenticated encryption scheme, NAAKE.

Finally, we analyse the security attributes of our new scheme, and then based on role based access control, we make an extension of this new scheme's application.

D. Requirements to Evaluate Anonymous Authentication and Key Exchange Protocol

We intend to design an efficient authentication scheme, which is expected to inherit all the good virtues of the previous schemes and support Diffie-Hellman key exchange. Here we summarize all these requirements to evaluate our new scheme as follows:

User Anonymity: The scheme should preserve user's real identity, namely, a server could not tell a user's real identity. In CHCL and JZH schemes, once the connection between the user and the server has been established, the probability of the server to guess the user's real identity is $1/n$, where n is the number of ring members.

Mutual Authentication: The scheme should assure that not only can server verify the legal users, but users can verify the server. As in authenticated protocols, mutual authentication is an important attribute, our scheme can also be in favor of it perfectly.

Forward Security: The scheme should satisfy forward security, namely, If the session key generated in j period has been leaked, the attacker can't forge any session key generated before j period. Therefore, the scheme can defeat some attacks like replay attack and so on.

Reveal User's Identity: The scheme should be able to reveal the user's identity, namely, after the protocol, if the user wants reveal his own identity, he can reveal it to the server. In some cases, the server may not believe that the user is the real user, so it is necessary for the user to reveal his identity to the server after the protocol.

E. Organization

Following above discussions, we address the user anonymity issue in authentication by presenting a

concrete scheme using ring signature in this paper. Our scheme acquires user anonymity by hiding a user's identity among a list of identities which is composed by the user in ring fashion.

The rest of paper is organized as follows. In Section 2, we give a brief review of some basic concepts, which will be used in our new protocol. In Section 3, we present an attack against two afore-mentioned anonymous PAKE protocols. In Section 4, we present our new scheme in detail. Finally a conclusion is drawn in Section 5.

II. PRELIMINARY

Here, we review some fundamental backgrounds used throughout this paper, and then define some requirements to evaluate our scheme.

A. Diffie-Hellman Key Exchange Protocol

In 1976, Diffie and Hellman proposed a well-known key exchange scheme, which allows two parties to negotiate a secret session key over insecure networks. The protocol works as follows:

1. Alice secretly chooses $x \in {}_R Z_p^*$, and sends $X = g^x \bmod p$ to Bob, where p is a large prime and g is a primitive element in Z_p^* .

2. Meanwhile, Bob secretly chooses $y \in {}_R Z_p^*$, and sends $Y = g^y \bmod p$ to Alice.

3. Alice computes $K = X^y \bmod p$. Bob computes $K' = Y^x \bmod p$.

After the protocol, Alice and Bob indeed share a secret session key $K = K' = g^{xy} \bmod p$.

B. Ring Authenticated Encryption Scheme

Rivest et al. [6] introduce the notion of a ring signature, which makes it possible to specify a set of possible signers without revealing which member actually produced the signature. In his ring signature scheme, he defines a family of keyed combining functions $C_{k,v}(y_1, y_2, \dots, y_n)$ which are still very useful in our new schemes. Every keyed combining function $C_{k,v}(y_1, y_2, \dots, y_n)$ takes as input the key k , an initialization b -bit value v , and arbitrary values y_1, y_2, \dots, y_n . Given any fixed values for k and v , each such combining function uses E_k as a sub-procedure, and outputs a b -bit value z , which has the following three properties:

- (1) For each $s, 1 \leq s \leq n$, and for any fixed values of all the other inputs $y_i, i \neq s$, the function $C_{k,v}(y_1, y_2, \dots, y_n)$ is a one-to-one mapping from y_s to the output z .

- (2) For each $s, 1 \leq s \leq n$, given a value z and the values for all inputs y_i except y_s , it is possible to efficiently find a value y_s for such that $C_{k,v}(y_1, y_2, \dots, y_n) = z$.

- (3) Given k, v and z , it is infeasible for an adversary to solve the equation $C_{k,v}(g_1(y_1), g_2(y_2), \dots, g_n(y_n)) = z$ for x_1, x_2, \dots, x_n if the adversary cannot invert any of the trap-door functions $g_1(\cdot), g_2(\cdot), \dots, g_n(\cdot)$.

J.Lv et al. [12] propose a new authenticated encryption scheme called ring authenticated encryption, which combines the two notations of ring signature and authenticated encryption together, and they also presented a ring authenticated encryption scheme based on discrete logarithm problem. Ring authenticated encryption has the

following security properties: semantic security, recipient designation, verification dependence, verification convertibility, recipient ambiguity, recipient verifiability, signer ambiguity and signer verifiability. T.Cao et al. [13] found Lv et al.'s scheme doesn't actually achieve signer-verifiability and recipient-verifiability properties, and they propose improved scheme to eliminate the weaknesses. In Cao et al.'s improved ring signature authenticated encryption scheme, they utilize the DL-based ring signature [14] and the method presented in [15] to achieve signer verifiability property, and use the signature based on zero-knowledge proof of knowledge (SPK) to achieve recipient verifiability property in recipient proof stage.

III. ANALYSIS OF TWO ANONYMOUS PASSWORD-BASED AUTHENTICATED KEY EXCHANGE PROTOCOLS

In this section, we analyze Chai et al.'s password-based authentication and key exchange scheme (CHCL) and Yang et al.'s anonymous password-based authenticated and key exchange protocol (JZH).

A. The Attack against CHCL Protocol

The process of CHCL protocol can be introduced as follows. Assume that the server S holds a secret key z ($|z|$

= 1) that is used to generate user-dependent secret information, and each user U has an identity ID and a password PW . The following are the notations used in it:

(1) Registration Phase

In this phase, a new user U submits his identity ID and password PW to S , and then receives a tamper-proof smart card issued by S .

1. User U submits his identity ID and a password PW to the remote server S for registration, S first checks the validity of ID and then computes user-dependent information s_{ID} :

$$s_{ID} = h(ID||z) \oplus h(PW).$$

2. Server S stores the parameters $(s_{ID}, g, p, h(\cdot), H(\cdot))$ to a smart card.

3. S issues the smart card to the user U via a secure channel.

(2) Anonymous Authentication and Key Exchange Phase

In this phase, user U will establish an authenticated session key and achieve mutual authentication anonymously with S in three rounds, see Fig 1.

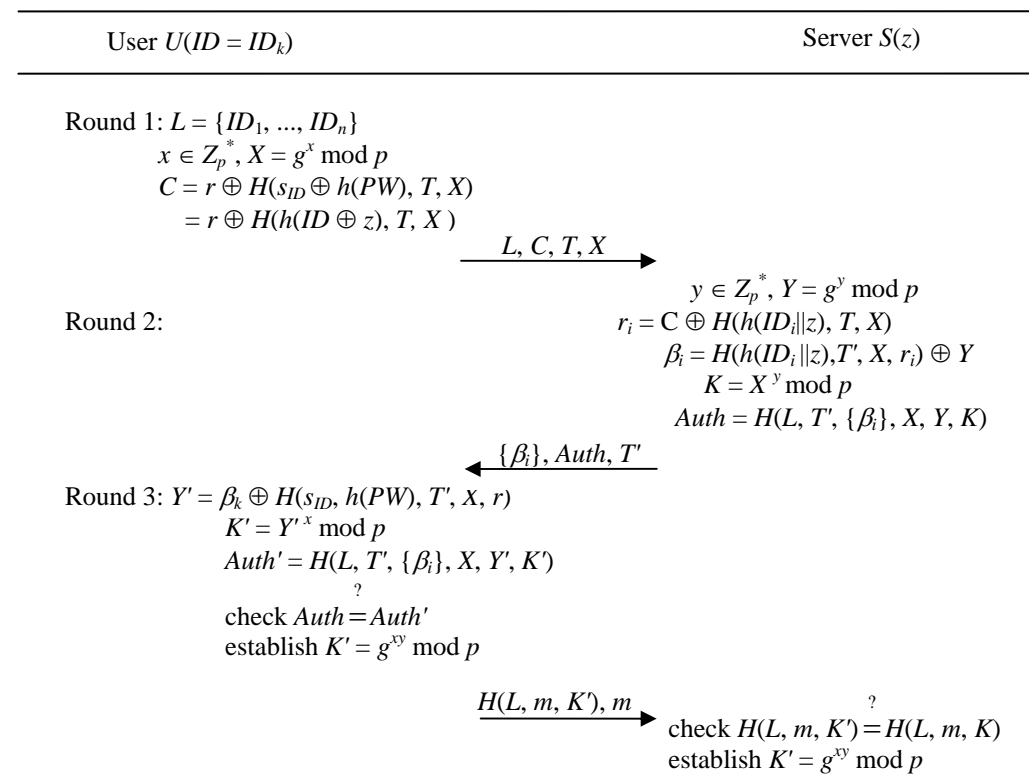


Fig.1 Anonymous Authentication and Key Exchange Phase

However, there is an attack in this protocol, so anonymity can't be achieved perfectly. If S sends false messages to U , and this connection can be established successfully, then S will know U 's identity (see Fig.2). The detail is shown as follows.

Round1: When U wants to login to the remote server anonymously, he attaches his smart card to the login device and keys in his ID and PW . Then,

1. collect a group of n identities, and compose an identity list $L = \{ID_1, \dots, ID_n\}$, including U 's own identity $ID = ID_k$ for some $k \in [1, n]$.

2. select a random exponent $x \in Z_p^*$, and compute $X = g^x \text{ mod } p$.

3. select a l -bit random number r , and compute

$$C = r \oplus H(s_{ID} \oplus h(PW), T, X) = r \oplus H(h(ID \oplus z), T, X),$$

where T is the current time stamp of login device.

4. send the request message $M = (L, C, T, X)$ to the remote server.

Round2: After receiving the request message M , S checks the time interval between T and receiving time, if the interval is beyond the reasonable transmission delay, the login request will be rejected. Otherwise, S will continue as follows:

1. select a random exponent $y \in Z_p^*$, and compute $Y = g^y \text{ mod } p$.

2. compute

$$r_k = C \oplus H(h(ID_k||z), T, X),$$

$$\beta_k = H(h(ID_i||z), T', X, r_k) \oplus Y,$$

where T' is the current time stamp of server.

3. compute

$$K = X^y \text{ mod } p,$$

$$Auth = H(L, T', \{\beta_i\}, X, Y, K),$$

where $\{\beta_i\}(i = 1, \dots, n)$ are β_k and $n - 1$ random numbers.

4. S sends $(\{\beta_i\}, Auth, T')$ back to U .

Round3: After receiving S 's reply, U checks the time interval between T' and receiving time, if the interval is beyond the reasonable transmission delay, U aborts the protocol. Otherwise, U will continue as follows:

1. compute $Y' = \beta_k \oplus H(s_{ID}, h(PW), T', X, r)$.

2. compute $K' = Y'^x \text{ mod } p$, and $Auth' = H(L, T', \{\beta_i\}, X, Y', K')$.

3. checks whether $Auth' = Auth$ holds or not. If it holds, U accepts $K' = Y'^x = g^{xy} \text{ mod } p$ as valid session key, and sends back $(H(L, m, K'), m)$ for S to confirm the authenticated session key K , where m could be some message payloads. Otherwise, U aborts the protocol.

From the above analysis, we can find that the security depends on the identities'number n U collecting. If n is very large, the calculated amount will be very large while it will be difficult for adversary to attack.

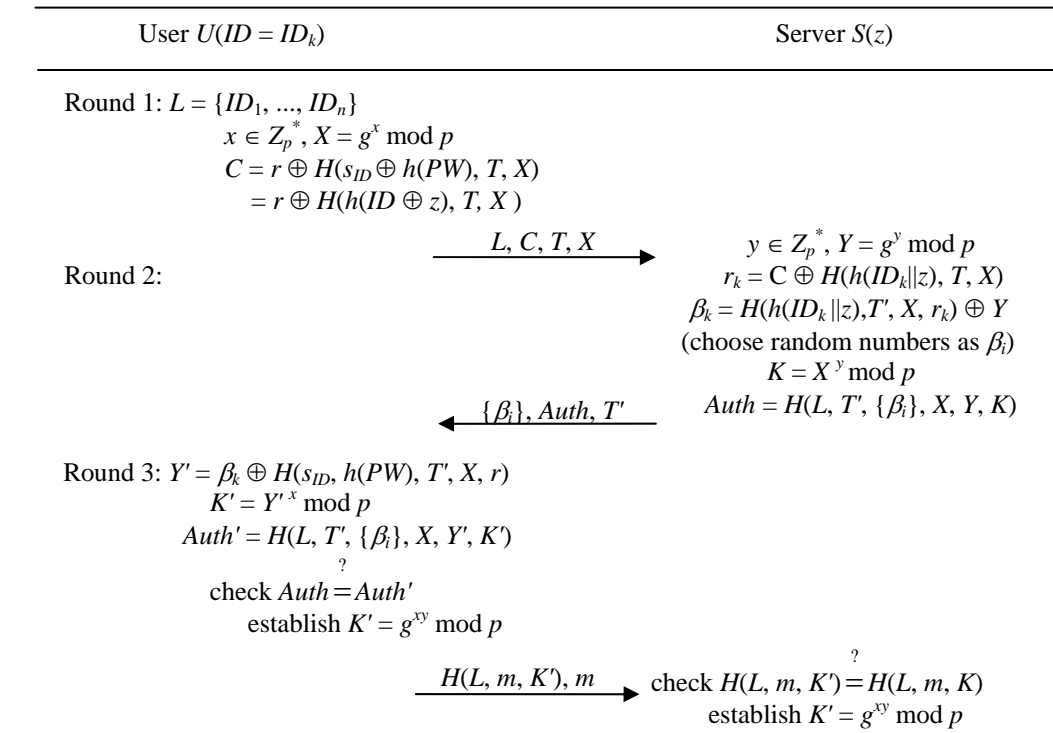


Fig.2 The Attack To Anonymous Authentication and Key Exchange Protocol

B. The Attack against JZH Protocol

The process of JZH is showed in Fig.3. Assume the two entities have already agreed on the client group Γ before a protocol run. $G = \langle g \rangle$ is a finite, cyclic group of prime order q . $S: \{0, 1\}^* \rightarrow G$ is a full-domain hash function, and $H_0, H_1: \{0, 1\}^* \rightarrow \{0, 1\}^l$ are two random hash functions, with l denoted as a security parameter. pw_i is a password shared between the client C_i and the server S , and $PW_i = S(i, pw_i)$.

1. The server S chooses $r_S \in \mathbb{R}Z_q$, and for all n clients in Γ generates $A_j = PW_j^{r_S}$ with $1 \leq j \leq n$. Then S sends $(S, \{A_j\}_{1 \leq j \leq n})$ to client C_i .

2. C_i checks all the values in $\{A_j\}$ are different from each other. If not, C_i aborts the protocol. Otherwise, C_i picks A_i from $\{A_j\}$, and draws two random values r_c and x from Z_q . Then C_i computes $X = g^x, Z = A_i^{r_c}$, and generates $X^* = Z \cdot X$ and $B = PW_i^{r_c}$. After that, C_i sends (X^*, B) to S .

3. S computes $Z' = B^{r_s}$ with the random value r_s and recovers $X' = X^*/Z'$. Then he chooses y randomly from Z_q , and computes $Y = g^y$ and $K' = X'^y$. And he generates the authenticator $Auth_S = H_1(Trans||Z'||K')$ and the session key

$sk = H_0(Trans||Z||K')$, where $Trans = \Gamma||S||\{A_j\}||X^*||B||Y$. Finally he sends $(Y, Auth_S)$ to C_i .

4. C_i computes the Diffie-Hellman value $K = Y^x$, and then check that whether $Auth_S$ equals to $H_1(Trans||Z||K)$. If not, he aborts the protocol. Otherwise, he computes the session key $sk = H_0(Trans||Z||K)$ and accepts it.

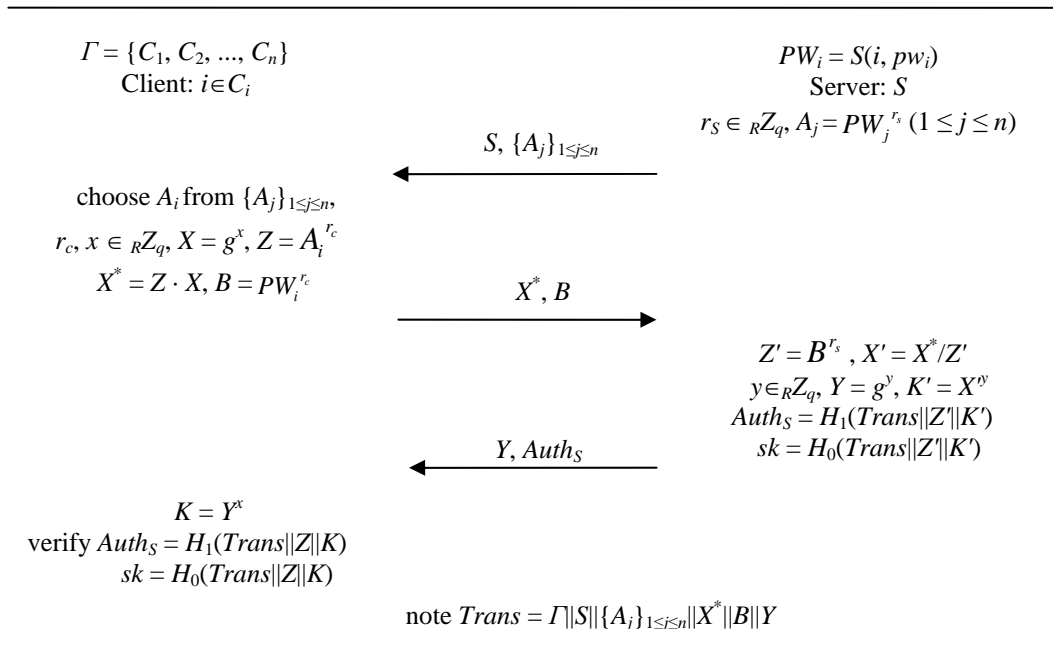


Fig.3 The JZH Protocol

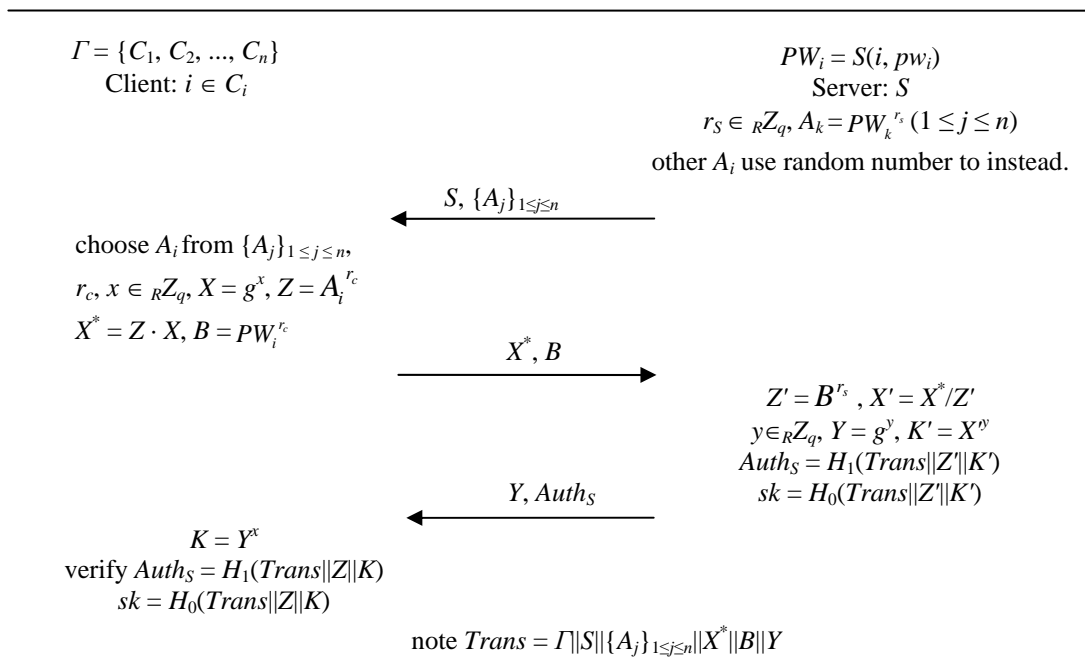


Fig.4 The Attack to JZH Protocol

The attack against this protocol can be described as follows (see Fig.4), which is similar to the attack of CHCLPAKE. A new user A agrees on a client group $\Gamma = \{A, B, C\}$ with S .

1. The server S chooses $r_S \in {}_R Z_q$, and for C in Γ generates $A_c = PW_c^{r_S}$, S choose random numbers a and b instead of A_A and A_B . Then S sends $(S, \{a, b, A_c\})$ to client C .

2. C checks the values in $(S, \{a, b, A_c\})$ are different from each other. If not, C aborts the protocol. Otherwise, C_i picks one from $\{a, b, A_c\}$, and draws two random values r_c and x from Z_q . Then C computes $X = g^x$, $Z = A_i^{r_c}$, and generates $X^* = Z \cdot X$ and $B = PW_i^{r_c}$. After that, C sends (X^*, B) to S .

3. S computes $Z' = B^{r_S}$ with the random value r_S and recovers $X' = X^*/Z'$. Then he chooses y randomly from Z_q , and computes $Y = g^y$ and $K' = X'^y$. And he generates the authenticator $Auth_S = H_1(Trans||Z||K')$ and the session key $sk = H_0(Trans||Z||K')$, where $Trans = \Gamma||S||\{A_j\}||X^*||B||Y$. Finally he sends $(Y, Auth_S)$ to C .

4. C computes the Diffie-Hellman value $K = Y^x$, and then check that whether $Auth_S$ equals to $H_1(Trans||Z||K)$. If not, C aborts the protocol. Otherwise, he computes the session key $sk = H_0(Trans||Z||K)$ and accepts it.

Thus, S can confirm the client is C , and C fails to conceal its identity.

The same as CHCL protocol, its calculated amount also depends on the identities' number n of the group. If n is very large, the calculated amount will be very large, but it will be difficult for adversary to attack.

IV. THE NOVEL ANONYMOUS AUTHENTICATION AND KEY EXCHANGE PROTOCOL

In this section, based on T.Cao et al.'s improved ring signature authenticated encryption scheme [13], we propose a new anonymous authenticated and key exchange protocol, NAAKE, as mentioned previously, which is secure against the above attack. Furthermore, we analyse the security of our new scheme and give an example of our scheme's application.

A. Protocol Description

Before proceeding, we assume the existence of a publicly defined symmetric encryption algorithm E such that for any key k , the function E_k is a permutation over b -bit strings. And we also assume the existence of a family of keyed combining functions $C_{k,v}(y_1, y_2, \dots, y_n)$ (defined in the ring signature scheme of Rivest et al. [4]) and a publicly defined collision-resistant hash function $H(\cdot)$ that maps arbitrary inputs to strings of constant length, which are used as keys for $C_{k,v}(y_1, y_2, \dots, y_n)$.

Initialization: For the user U_i who wants to generate a session key with the server S , he uses a ring of n logged-on users, and does follows.

Step 1. Chooses the following parameters: a large primes p_i such that it is hard to compute discrete

logarithms in $GF(p_i)$, another large prime q_i such that $q_i | p_i - 1$, a generator g_i in $GF(p_i)$ with order q_i .

Step 2. Chooses $x_{A_i} \in Z_{q_i}$ as his private key, and computes the public key $y_{A_i} = g_i^{x_{A_i}} \text{ mod } p_i$.

Step 3. Defines a trap-door function $f_i(\alpha, \beta) = \alpha \cdot y_{A_i}^{\alpha \text{ mod } q_i} \cdot g_i^\beta \text{ mod } p_i$; its inverse function $f_i^{-1}(y)$ is defined as $f_i^{-1}(y) = (\alpha, \beta)$, where α and β are computed as follows (K is a random integer in Z_{q_i}).

$$\alpha = y_{A_i} \cdot g_i^{-K \cdot (g_i^K \text{ mod } p_i) \text{ mod } q_i} \text{ mod } p_i \quad (1)$$

$$\alpha^* = \alpha \text{ mod } q_i \quad (2)$$

$$\beta = K \cdot (g_i^K \text{ mod } p_i) - x_{A_i} \cdot \alpha^* \text{ mod } q_i \quad (3)$$

U_i makes p_i, q_i, g_i and y_{A_i} public, and keeps x_{A_i} secret.

The server S chooses a large prime p such that it is hard to compute discrete logarithms in $GF(p)$, another large prime q such that $q | p - 1$, a generator g in $GF(p)$ with order q , and a random integer x_B from from Z_q as his private key, computes his public key $y_B = g^{x_B} \text{ mod } p$, and publishes (y_B, p, q, g) .

Key Exchange: This phase is initiated by U , and ends in three rounds, resulting in an authenticated session key between U and S .

Round 1: When the t th user U_t wants to generate a session key on behalf of n ring members U_1, U_2, \dots, U_n , where $1 \leq t \leq n$. U_t does the following.

Step 1. Chooses a random integer x_1, x_a from Z_q^* , computes

$$R = g^{x_1} \text{ mod } p,$$

$$Q = y_B^{x_1} \text{ mod } p \text{ mod } q,$$

$$X = g^{x_a} \text{ mod } p,$$

$$V = X \cdot g^{-Q} \text{ mod } p.$$

and computes l as $l = H(X, Q, V, y_B, T)$.

Step 2. Chooses a pair of values (α_i, β_i) for every other ring member $U_i (1 \leq i \leq n, i \neq t)$ in a pseudorandom way, and computes $y_i = f_i(\alpha_i, \beta_i) \text{ mod } p_i$.

Step 3. Picks randomly a b -bit initialization value v , and solves out y_t from equation $C_{k,v}(y_1, y_2, \dots, y_n) = v$.

Step 4. Computes $(\alpha_t, \beta_t) = f_t^{-1}(y_t)$ by using the trap-door information of f_t : first, chooses a random integer $K \in Z_{q_t}$, computes α_t by (1), and keeps K secret;

second, computes α_t^* by (2); finally, computes β_t by (3).

Step 5. The ring signature σ on X is $(U_1, U_2, \dots, U_n, v, V, R, (\alpha_1, \beta_1), (\alpha_2, \beta_2), \dots, (\alpha_n, \beta_n))$.

Finally, the user U_t sends σ and T to the server S .

Round 2: S does the following to recover and verify X from the signature σ .

Step 1. Computes $Q = R^{x_B} \text{ mod } p \text{ mod } q$, recover X as $X = V \cdot g^Q \text{ mod } p$, and hash X, Q, V , and y_B to recover l as $l = H(X, Q, V, y_B, T)$.

Step 2. Computes $y_i = f_i(\alpha_i, \beta_i) \bmod p_i$, for $i = 1, 2, \dots, n$.

Step 3. Checks whether $C_{k,v}(y_1, y_2, \dots, y_n) = v$. If it holds, S accepts X as valid (otherwise, S rejects X), and then does the following: chooses a random integer x_b from Z_q^* , and computes

$$Y = g^{x_b} \bmod p,$$

$$K_s = X^{x_b} \bmod p,$$

$$h = H(K_s, X, Y, T'),$$

and then sends $\{h, Y, T'\}$ to U_t .

Round 3: U_t verifies whether K_s' is from the server S .

U_t computes $K_s' = Y^{x_a} \bmod p$, and hashes K, X, Y to gets h' as $h' = H(K_s', X, Y, T')$. If $h' = h$, U_t accepts K_s as the session key.

User's Identity Revelation: If the actual user U_t is willing to disclose to the server S (or any third party Bob) that the signature is generated by him, then he does the following.

Step 1. U_t computes $M = g^K \bmod p_t$, and sends (M, y_{A_t}) to Bob $((M, y_{A_t}))$ and σ to the third party, respectively).

Step 2. Bob (the third party, respectively), who already knows (α_t, β_t) , computes $\alpha_t^* = \alpha_t \bmod q_t$, and checks $M^M = g_t^{\beta_t} \cdot y_{U_t}^{\alpha_t^*} \bmod p_t$. Only the equation holds will Bob (the third party, respectively) accepts that as the real signer of the signature.

B. Security Discussion

As we discussed earlier, our new anonymous authenticated and key exchange scheme satisfies the following security requirements.

User Anonymity: In our new scheme, for a given signature on X , any verifier can only be convinced that the ring signature is actually produced by at least one of the possible users. If the actual user does not reveal the seed K , then any verifier cannot determine who is the actual user. The limited anonymity is computational and depends on the security of the pseudorandom generator. Anyone cannot determine the identity of the actual user in a ring of size n with probability greater than $1/n$. As k and v are fixed in a ring signature, there are $(2^b)^{n-1} (x_1, x_2, \dots, x_n)$ satisfying the equation $C_{k,v}(y_1, y_2, \dots, y_n) = v$, and the probability of the generation of (x_1, x_2, \dots, x_n) is same ignoring the subjectivity of the user, so the signature can't leak the identity information of the user, namely it satisfies anonymity.

Mutual Authentication: In our scheme, not only can server verify the legal users, but users can verify the legal server. No one can impersonate a legal user inside a ring to login the server in our scheme. Because of the hardness of inverting hash function $f(\cdot)$, it is computationally infeasible for the attacker to calculate (α_i, β_i) , without which it is hard for an attack to forge a signature. Therefore, the attacker can not establish a session key

with server to authenticate himself as a member within the submitted ring.

If an attacker wants to masquerade as the server, he should compute $h = H(K_s, X, Y)$, so he need to get x_b in order to compute X , however, x_b is the private key of the server, and it is nearly impossible for the attacker to know it. Therefore, we can say it is only the server that can authenticate itself to a user.

Forward Security: As x_a and x_b are both selected randomly, the session key of every period has no relation with each other. Therefore, if the session key generated in j period has been leaked, the attacker can't get any information of the session key generated before j period.

Our scheme can defeat replay attack. The messages transmitted over the network in our scheme can not be intercepted for reuse, because of the involvement of timestamp. And the server could check the freshness of a received message by testing whether the transmission time is within legal transmission delay.

Reveal User's Identity: In our scheme, after the protocol, if the user wants to confirm his identity, the actual user could disclose his identity to the server (or any third party Bob). As K is a secret number chosen by the user himself, only he can compute $M = g^K \bmod p_t$. And Bob (the third party, respectively) who already knows (α_t, β_t) can compute $\alpha_t^* = \alpha_t \bmod q_t$, and checks $M^M = g_t^{\beta_t} \cdot y_{U_t}^{\alpha_t^*} \bmod p_t$. If it holds, Bob accepts that he is the real user of the message X . Thus, the user completes the revelation of his identity.

C. Application

In this section we will give an extension of our new scheme's application based on role-based access control (RBAC).

In RBAC, it is possible to simplify the complicated form of an organization's access control policy. Access decisions are based on the roles, which is part of an organization. RBAC is a non-discretionary access control in which the system administrator allows the role's permissions to the user by defining user, role, and permission. The system administrator divides roles according to operations in an organization. The administrator of the system or organization gives access permissions to roles and users are endowed with roles according to their responsibility and obligation. Users who are granted a role in system can manage their works with their role permissions. In case of changing access control policy, the system supervisor easily can grant a new permission or can eliminate the existing permission to the role. Because access permissions are granted to roles (permissions are associated with roles), not to users, it is possible to manage access control policy more efficiently. There are many variations of RBAC, but the basic architecture of RBAC is that permissions are assigned to roles (not directly to users) and roles are assigned to users [16].

It is apparent that a very important part of NAAKE is the generation of the ring. As it is the communication

between the user and the server, a general method is collecting the registered users to generate the ring. However, if the number of the users is very large, the calculated amount will also be very large. In order to solve such a problem, we can use the role-based access control technique.

First, we need to set different access control rights for each role. Suppose that all the users are divided into three types, general user, super user and administrator, and their rights to access the resources are different. And then, in order to reduce the calculation amount, we can do it as follows.

Given that a super user wants to generate a session key k_s with the server, he can generate a ring of the users belonging to the role of general user. Therefore, the ring number will be reduced to the number of super users instead of all the users.

Through this method, when the number of the user is very large, the calculation amount of the user would be greatly reduced. As the server doesn't know the user's role, the probability for him to guess the user's identity is still $1/n$, where n is the number of all the user.

V. CONCLUSION

User anonymity is attached great importance in recent years to preserve user privacy in wired or wireless network environments. In this paper, as for the anonymous password-based AKE, we analyse the vulnerabilities of CHCL and JZH protocols, pointing out their vulnerability that they both can't achieve the anonymity perfectly.

After analysing two existed anonymous authenticated and key exchange schemes, we proposed a new anonymous authenticated and key exchange protocol, NAAKE. Furthermore, we analyse the security of our new scheme and make an extension of this new scheme's application.

ACKNOWLEDGMENT

This work is supported by the Jiangsu Provincial Natural Science Foundation of China (BK2007035), the open research fund of National Mobile Communications Research Laboratory, Southeast University (W200817) and the Science and Technology Foundation of CUMT (0D080309).

REFERENCES

- [1] Liao.I.E., Lee.C.C., Hwang.M.S.: A password authentication scheme over insecure networks. *J. Comput. System Sci.* (2005).
- [2] Bo.Z., Wan.Z.G., Kankanhalli.M.S., Feng.B., Deng.R.H.: Anonymous secure routing in mobile ad-hoc networks, *Local Computer Networks*, 2004. 29th Annual IEEE International Conference on 16-18 Nov. (2004) 102- 108
- [3] Arjan Duresi. Anonymous communications in the Internet. *Cluster Comput* (2007) 10: 57–66, DOI 10.1007/s 10586-007-0006-y
- [4] Viet.D.Q., Yamamura.A., Hidema.T.: Anonymous Password-Based Authenticated Key Exchange. In: Maitra, S., Veni Madhavan, C.E., Venkatesan, R.(eds.) *INDOCRYPT 2005*. LNCS, vol. 3797, pp. 244-257. Springer, Heidelberg (2005)
- [5] Chaum.D., Heyst.E.V.: Group signatures. *Advances in Cryptology EUROCRYPT'91*, LNCS, Vol. 547, Berlin: Springer-Verlag,(1991) 257-265
- [6] Rivest.R., Shamir.A., Tauman.Y.: How to leak a secret. *Advances in Cryptology ASIACRYPT'01*, LNCS, Vol. 2248, Springer-Verlag, Berlin Heidelberg New York (2001) 552-565
- [7] Dodis.Y., Kiayias.A., Nicolosi.A., Shoup.V.: Anonymous identification in ad hoc groups. *Advances in Cryptology-EUROCRYPT 2004*, LNCS Vol. 3027, Berlin: Springer-Verlag, (2001) 609 -626
- [8] Chien.H.Y., Chen.C.H.: A remote authentication scheme preserving user anonymity, In: *Proceedings of the 19th International Conference on Advanced Information Networking and Applications-AINA 2005*, 245-248
- [9] Viet.D.Q., Yamamura.A., Tanaka.H.: Anonymous password-based authenticated key exchange, *Advances in Cryptology INDOCRYPT 2005*, LNCS, Vol. 3797, Berlin: Springer-Verlag, (2005) 244-257
- [10] Jing Yang, Zhenfeng Zhang. A new anonymous password-based authenticated key exchange protocol. D.R.Chowdhury, V.Rijmen, and A.Das (Eds.): *INDOCRYPT 2008*, LNCS 5365, pp.200-212, 2008. Springer-Verlag Berlin Heidelberg 2008
- [11] Zhenchuan Chai, Zhenfu Cao, and Rongxing Lu. Efficient password-based authentication and key exchange scheme preserving user privacy. X.Cheng, W.Li, and T.Znati (Eds.): *WASA 2006*, LNCS 4138, pp.467-477, 2006. Springer-Verlag Berlin Heidelberg 2006
- [12] J.Lv, K.Ren, X.Chen and K.Kim. "Ring authenticated encryption: a new type of authenticated encryption". *The 2004 Symposium on Cryptography and Information Security*, Sendai, Japan, Jan.27-30, 2004, pp.1179-1184
- [13] T.Cao, D.Lin and R.Xue. "Improved ring authenticated encryption scheme". *Tenth Joint International Computer Conference*, International Academic Publishers World Publishing Corporation, 2004, pp.341-346.
- [14] C.Gao, Z.Yao, L.Li. A Ring Signature Scheme Based on the Nyberg-Rueppel Signature Scheme. *Applied Cryptography and Network Security*, LNCS 2846, Springer-Verlag, 2003, 169-175
- [15] R.L.Rivest, A.Shamir, Y.Tauman, How to Leak a Secret. *Advances in Cryptology-ASIACRYPT2001*, LNCS 2248, Springer-Verlag, 2001, 257-265
- [16] R.Sandhu, E.J.Coynee, H.L.Feinstein, C.E.Youman. Role-based access control models. *IEEE Computer*, 29(2), Februar

Cao Tianjie, School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, Jiangsu, China. In 1986-1993 studied in the department of mathematics, Nankai University, and got Bachelor Degree of Science and Master Degree of Science.

In 2006 got Doctor Degree of Engineering in Key Laboratory of Information Security, Institute of Software Software, the Chinese Academy of Sciences State. 2007-2008 visited School of Computer Science, Purdue University of America. Now is a professor, Ph D adviser and the chairman of the Department of Information Safety, China University of Mining and Technology. The research direction is Cryptography and information security, and has published quite a lot of articles in international conferences, Chinese Journal of Electronics, IEEE Transactions on Dependable and Secure Computing, IEEE Communication Letters.