A Union Authentication Protocol of Cross-domain Based on Bilinear Pairing

Shen-Gang Hao
Dept of Computer and Information Technology, Nanyang Normal University, Nanyang, China
Email:nythhsg@sina.com

Li Zhang
Dept of Computer and Information Technology, Nanyang Normal University, Nanyang, China
Email: hnnyzli@bit.edu.cn

Ghulam Muhammad
School of Computer, Beijing Institute of Technology, Beijing, China
Email: gm.shaikh1@gmail.com

***Abstract*—With the development of network service technology such as grid computing, cloud computing, the cooperation among multiply domains is needed for these intelligent services that have the unlimited space and the unlimited speed. This paper proposes a new union authentication protocol of cross-domain that can ensure the security of resource access in different domains, where the register keys of members in one domain are submitted to the key authentication center, rather than the private keys. This authentication protocol can avoid the shortcoming that it is complex to deliver certification in the traditional cross-domain authentication based on PKI and prevent the authority counter from pretending to be a member to access resources in other domains in the current identity-based authentication. The performance analysis shows that the proposed authentication protocol has good anonymity and can track the entities when there are the inconsistent cases. At last, a prototype system that can implement the authentication protocol is given.**

***Index Terms*—multi-domain cooperation; union authentication; elliptic curve; bilinear pairing**

I. Introduction

Multi-domain union (MDU) is used in large networks, its services and access-points are distributed in multiple domain. In the distributed network environment, the companies and the agencies have their own shared resource. In order to prevent unauthorized users from accessing the shared resource, every company or agency sets up the local authentication service. So every entry has a relatively independent trust domain, in which the users trust the local authentication center and the local authentication service is conveniently provided for the local user. However, the single domain can not satisfy the great deal of service requests. For example, the requirement for accessing resources is great in cloud computing environment, and the multi-domain resource request is needed. It is noted that the shared resource requests not only come from the internal domain, but also from the outer domain. Therefore, the problem of cross-domain identity authentication will occur when the users in the foreign trust domain access the resources in the local trust domain.

There are many applications which are based on the cross-domain authentication, such as entity authentication among the multiple heterogeneous domains in the virtual organization of the grid environment, mobile access authentication in wireless network environment. The existing cross-domain authentication frameworks in special environments mainly include the Symmetric key Infrastructure (such as Kerberos [1]) and the traditional Public Key Infrastructure [2][3][4] (PKI for shot). The former has disadvantage that the symmetric key management and key negotiation is very complex, which can not effectively deal with the anonymous problem. The later has shortcoming that the costs of certification management is expensive, such as certification status checking, certification path construction and certification delivery. The authentication center's network easily becomes a bottleneck if the frequency of cross-domain resource access is high. The multi-domain authentication models based on identity were proposed in the references [5][6]. It is precondition that the foreign authentication centers are trusted and the key negotiation parameters of each domain must keep same in this proposed mode, which lead to the limitation that the foreign authentication center is not prevented from pretending to be a member of local domain. References [7][8][9] used the identity-based signature method to realize the internal resource access authentication in the same domain, but this method can not work in the cross-domain. Lu [10] improved the Malone-Lee’s method and implemented it between domains. However, its precondition is suppose

Manuscript received October 28, 2012; revised November 25, 2012; accepted December 30, 2012.
Corresponding author: Hao Shen-Gang.

doi:10.4304/jsw.8.5.1094-1100

that each Public key Generator (PKG for short) is honest, because PKG has the private key of others domains and the user's identity authenticity and the private key security could not be guaranteed if the PKG is malware.

This paper proposes a union authentication protocol of cross-domain which is based on the signature verification between two domains. In the signature method, the parameters generated in the different authentication centers for multiply domains may be not same and the register keys, rather than the private keys of members within one domain are submitted. So there are no private keys in the authentication center, which can prevent the authentication center from pretending to be a local member to access resources of other domains. This proposed authentication protocol has better anonymity and can avoid all kinds of attacks and it support that members can be traced when there are the inconsistencies in accessing the resources.

II. The Basis Of Finite Group Theory

A. Automorphism Groups in the Finite Group

Suppose that G represents a group and $AutG$ denotes an automorphism group of G, $C(G)$ is defined as the center of G and the cyclic group labeled as $<g>$ is generated by the element g. If G is a finite group whose order is labeled as $|G|$ that represents the number of elements included in G and there is the equation that is $|G| = p^n$ (n>0) to be true (p is a prime number), G is called p-group and the subgroups whose order is equal to the several power of p are called p-subgroups. If H is a p-subgroup of the finite group G and $|G| = p^k *m$, $|H| = p^k$ and $(p^k, m) = 1$, H is called the ***sylow*** p-subgroup of G.

Lemma 1[11]: Suppose that G is a finite *Abel* group and $p_1,p_2,\ldots\ldots p_n$ are all the prime of $|G|$ and $G_{pi}(1 \leqslant i \leqslant n)$ is the ***sylow*** p-subgroup of G, the equation that $G = G_{p1} \ast G_{p2} \ast \ldots \ast G_{pn}$ follows.

Lemma 2[11]: Suppose that if $G = G_1 \ast G_2 \ast \ldots \ast G_n$, K_i is a subgroup of G_i, and $K_1, K_2,\ldots, K_n$ are isomorphic, G has the number n of isomorphic subgroups.

Lemma 3[11]: Suppose that $G_1 = <g_1>$ represents a cyclic group whose order is m and $G_2 = <g_2>$ represents a cyclic group whose order is n. If $(m, n) = 1$, $G_1 \ast G_2$ denotes a cyclic group whose order equal $m *n$.

B. Bilinear Group

The definition of bilinear mapping [12] is given firstly.

Suppose that G_1 labeled as $G_1 = <g_1>$ is a cyclic multiplicative group whose order is p, G_2 labeled as $G_2 = <g_2>$ is a cyclic multiplicative group whose order is q and G_3 is a group, the bilinear mapping is defined as

$$e : G_1 \times G_2 \to G_3$$

that has the following properties.

Property 1: It is bilinear which refers to the equation that $e(u^a,v^b) = e(u,v)^{ab}$ follows for all the elements $u \in G_1$, $v \in G_2$ and $a,b \in Z$.

Property 2: It is nonsingular which refers to $e(g_1,g_2) \neq 1$

Property 3: It is calculable which refers to $e(g_1,g_2)$ can be computed within the finite time.

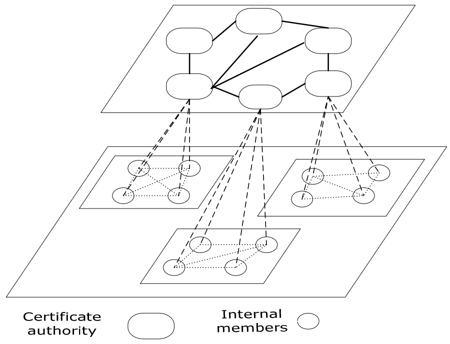

Figure 1 Union authentication system model for cross-domain

III. The Union Authentication System Model

In the authentication system of multiply trust domains, the internal authentication type of each domain could be separately chosen according to its own demand while the mode of authentication among domains should have a uniform definition in order to make the interoperability of across-domains convenient. This paper designs the union authentication system model of cross-domain (see Fig. 1) . The internal authentication of one domain will be not discussed in this paper.

In Fig. 1, the union authentication system is composed of multiple domains. Each domain is independent, autonomous and it consists of a key authentication center (KCA for short) and many internal domain members. The function of KCA is as same as that of the traditional authentication center (CA or PKG for short). The internal members are the owners and visitors of the resources. They need to access the across-domain resources when they work together. The basic idea of cross-domain union authentication protocol is that each authentication center selects one group from multiple heterogeneous cyclic groups, generates its own key parameters based on this cyclic group, distributes and manages the key of local domain, and opens its public key at the same time in order to realize resource access and authentication between two domains. When a new member joins one domain, he needs to register his identity for entity tracking.

IV. The Anonymous Signnature Scheme Among Multiply Domains

A. Innitialization of System

The number Q of big prime numbers are selected and constitute the set labeled as

$$Q_{set} = \left\{ Q_i \middle| (2 \le i \le Q) \right\},$$

from which a big prime number P is chosen, and a super-singular elliptic curve $E/GF(p)$ is found which meets the security assumptions of WDH. Subsequently, G is generated which is the subgroup of $E/GF(p)$. The order of G is q and $q = l_1 * l_2 * \ldots l_3$. Suppose that $G_{li}(1 \leqslant i \leqslant Q)$ is the *sylow* p-subgroup of G, then $G_{l1} \ast G_{l2} \ast \ldots \ast G_{li}$ is a direct product decomposition of G. Based on the Lemma

2 above, we construct the number Q of subgroups of G which are isomorphic to each other and the set of these subgroup is labeled as

$$G_{set} = \left\{ G_j \left| (1 \le j \le Q) \right. \right\}.$$

In multi-domain union, every domain selects a different subgroup labeled as $G_k(1 \leqslant k \leqslant Q)$ from G_{set} that is used as the key generation parameters of the local domain.

B. Anonymous Signature Scheme between Two Domains

(1) Parameters selection

Suppose that the cyclic groups $G_1 = <g_1>$ and $G_2 = <g_2>$ are respectively selected as the key generation parameters for two domains D_1 and D_2 in the union domain. G_1 and G_2 are the prime isomorphism groups in the set G_{set}. g_1 and g_2 are the generation elements of G_1 and G_2 respectively. $e: G_1 \times G_2 \to G_p$ is the calculable bilinear mapping. $h:\{0,1\}^* \to Z_p$ is a hash function. For arbitrary elements $\xi_1, \xi_2 \in_R Z_P^*$, $(\xi_1, g_1^{\xi_1})$ and $(\xi_2, g_2^{\xi_2})$ are respectively used as the public/private key pairs of the certification centers in the domains D_1 and D_2. $H = e(g_1^{\xi_1}, g_2^{\xi_2})$ is the mapping value of the two public keys.

(2) Keys distribution among internal members within one domain

Suppose that there are the number n of members in the domain D_1, and ξ_1 is the private key of the Key domain authentication center (KCA$_1$) that belong to D_1, and the corresponding public key of ξ_1 is $P_1 = g_1^{\xi_1}$. KCA$_1$ delivers the value $Y = g_1^{\frac{1}{\xi_1}}$ to every member in the domain D_1. The member U_i selects $x_i \in_R Z_P^*$ as his private key and the corresponding public key is $P_{u_i} = g_1^{x_i}$. Then U_i calculates the value $reg_i = (Y)^{x_i}$ which is used as the key to register in KCA$_1$. Thus KCA$_1$ will establish the correspondences relationship between reg_i and the identity of U_i so that the identity of members can be traced. For every other domain, the case is similar.

In addition, suppose that the member U_1 within the domain D_1 has the public/private key pair labeled as (x_1, P_{u_1}) and the register key labeled as reg_1 and the message labeled as $m \in \{0,1\}^*$ while the member U_2 within the domain D_2 has the public/private key pair labeled as (x_2, P_{u_2}) and the register key labeled as $reg2$. When U_1 accesses the resources of U_2, the signature procedure is described as follows:

① U_1 chooses two arbitrary elements $\alpha, \beta \in_R Z_P^*$ and computes the following values:

$T_1 \leftarrow P_1^\alpha$;

$T_2 \leftarrow P_2^\beta$;

$T_3 \leftarrow H^{(\alpha+\beta)}$;

$T_4 \leftarrow reg_1 H^{\alpha\beta}$;

$\delta_1 \leftarrow x_1 \alpha$;

$\delta_2 \leftarrow x_1 \beta$.

② The following equations are calculated by using these arbitrary elements $r_\alpha, r_{\beta,} r_{x,} r_{\delta_1}, r_{\delta_2} \in_R Z_P^*$

$R_1 = P_1^{r_\alpha}$;

$R_2 = P_2^{r_\beta}$;

$R_3 = e(T_4, g_1)^{r_x} e(P_1, H)^{-r_\alpha - r_\beta} e(H, g_1)^{-r_{\delta_1} - r_{\delta_2}}$;

$R_4 = T_1^{r_x} . P_1^{-r_{\delta_1}}$;

$R_5 = T_2^{r_x} . P_2^{-r_{\delta_2}}$.

③The identification value labeled as

$$c \leftarrow h(m, T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5),$$

$c \in_R Z_P^*$ is calculated.

④ The following equations are calculated based on those values mentioned above

$s_\alpha = r_\alpha + c\alpha$

$s_\beta = r_\beta + c\beta$;

$s_x = r_x + cx_1$;

$s_{\delta_1} = r_{\delta_1} + c\delta_1$;

$s_{\delta_2} = r_{\delta_2} + c\delta_2$

⑤The signature is generated that is labeled as

$$\sigma = (T_1, T_2, T_3, T_4, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2}).$$

(3) Signature verification

By using the public key of inter-domain labeled as $dpk = (g_1, P_{u_1}, reg_1, P_1, P_2, H)$, the signature σ can be verified by arbitrary receivers of the message m . The verification steps are as follows:

$aH^{(\sigma_1+\sigma_2)} \overset{?}{=} T_3 P_u$

$R_1 \overset{?}{=} P_1^{s_\alpha} / T_1^c$

$R_2 \overset{?}{=} P_2^{s_\beta} / T_2^c$

$R_3 \overset{?}{=} e(T_4, a)^{s_x} e(P_1, H)^{-s_\alpha - s_\beta} e(H, a)^{-s_{\delta_1} - s_{\delta_2}} ((e(T_3, P_1))^2 / e(T_4, P_1))^c$

$R_4 \overset{?}{=} T_1^{s_x} / P_1^{s_{\delta_1}}$

$R_5 \overset{?}{=} T_2^{s_x} / P_2^{s_{\delta_2}}$

V.The Union Authentication Protocol Of Across-Domain

A member in one domain needs to be authenticated when he accesses the resources of other domains for safety's sake. However, there is only one authentication center in every domain, which is easy to become a bottleneck when lots of authentication activities need to be handled. In order to improve the speed of resource access and make full use of resources, this paper designs an authentication protocol of across-domain union, in which the authentication operation isn't executed by the authentication center when the members access the resources of cross-domain. That is to say, a member in one domain can be directly authenticated by a member in other domain.

Suppose that *D₁* and *D₂* are the domains of the domains union set, *U₁* is the member of *D₁* and *U₂* is the member of *D₂*, *P₁*,*P₂* are the public keys of the authentication center in *D₁* and *D₂* respectively. *reg₁*, *P_{u1}* are respectively the registration key and the public key of *U₁*. If *U₁* wishes to access resources of *U₂*, the authentication protocol is designed as follows:

$$U_1 \rightarrow U_2 : type, dpk(g_1, P_{u_1}, reg_1, P_1, P_2, H); \qquad (1)$$

$$U_1 \rightarrow U_2 : (T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5); \qquad (2)$$

$e(reg_1, P_1) = e(g_1, P_{u_1})$ is calculated by U_2; (3)

$$U_2 \rightarrow U_1 : c = h(m, T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5); \qquad (4)$$

$$U_1 \rightarrow U_2 : \sigma = (s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2}); \qquad (5)$$

U_2 verifies the signature based on

$$(dpk, T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5, c); \qquad (6)$$

The detailed authentication procedure of cross-domain is described as the following steps:

(1) *U₁* sends the resource access type, the public key of the local authentication center, the public key of another domain which will be accessed and other parameters shown as formula (1) and (2) to *U₂*;

(2) *U₂* verifies that *U₁* is a member of *D₁* indeed by calculating formula (3), but only the public key of *U₁* is known and other identity information don't be known at this moment;

(3) *U₂* selects an arbitrary message m and uses the parameters shown as formula (2) to calculate the identification value c based on the formula (4), and sends it to *U₁;*

(4) *U₁* generates the signature parameters by using the received value *c*, and sends them to *U₂;*

(5) *U₂* uses those signature parameters to identify that *U₁* is a given member of *D₁*, which prevents the authentication center from pretending and conceals the detailed identity information of *U₁*.

In addition, we give the overview of the procedure of negotiating the session key.

Step 1: *U₂* selects an arbitrary integer $X_B \in_R Z_P^*$, then calculates $P_1^{X_B}$ and sends the value pair $(P_{u_2}, P_{u_1}^{X_B})$ to *U₁;*

Step 2: *U₁* uses its own private key x_1 to decrypt $P_{u_1}^{X_B}$ and gets $P_{u_1}' = g_1^{X_B}$ because of $P_{u_1} = g_1^{x_1}$;

Step 3: *U₁* selects an arbitrary integer $X_A \in_R Z_P^*$, calculates $P_{u_2}^{X_A}$ and sends it to *U₂;*

Step 4: *U₂* uses his own private key x_2 to decrypt $P_{u_2}^{X_A}$ and get $P_{u_2}' = g_2^{X_A}$ because of $P_{u_1} = g_1^{x_1}$;

Step 5: *U₁* and *U₂* calculate the temporary session key.

VI. PERFORMANCE ANALYSIS OF THE AUTHENTICATION PROTOCOL

A. *Correctness Analysis*

The authentication protocol is based on the signature, so we must guarantee the signature is correct if we want to verify the authenticated user is a member of a given domain in the domain union. The correctness of signature is deduced as follows:

$$g_1 H^{(\sigma_1+\sigma_2)} = g_1 H^{(\alpha+\beta)x_i} = H^{(\alpha+\beta)} g_1^{x_1} = T_3 P_{u_1}$$

$$P_1^{s_\alpha} / T_1^c = P_1^{(r_\alpha + c\alpha)} / P_1^{\alpha c} = P_1^{r_\alpha} = R_1$$

$$P_2^{s_\beta} / T_2^c = P_2^{(r_\beta + c\beta)} / P_2^{\beta c} = P_2^{r_\beta} = R_2$$

$$R_3 = e(T_4, a)^{r_x} e(P_A, H)^{-r_\alpha - r_\beta} e(H, a)^{-r_{\delta_1} - r_{\delta_2}}$$

$$= e(T_4, a)^{s_x - cx_i} e(P_A, H)^{-s_\alpha - s_\beta + c\alpha + c\beta} e(H, a)^{-s_{\delta_1} - s_{\delta_2} + c_{\delta_1} + c_{\delta_2}}$$

$$= e(T_4, a)^{s_x} e(P_A, H)^{-s_\alpha - s_\beta} e(H, a)^{-s_{\delta_1} - s_{\delta_2}}$$

$$e(T_4, a)^{-cx_i} e(P_A, H)^{c\alpha + c\beta} e(H, a)^{c_{\delta_1} + c_{\delta_2}}$$

$$= e(T_4, a)^{s_x} e(P_A, H)^{-s_\alpha - s_\beta} e(H, a)^{-s_{\delta_1} - s_{\delta_2}}$$

$$e(P_A, H)^{c(\alpha+\beta)} e(H, a)^{c(\delta_1 + \delta_2)} / e(T_4, a)^{cx_i}$$

$$= e(T_4, a)^{s_x} e(P_A, H)^{-s_\alpha - s_\beta} e(H, a)^{-s_{\delta_1} - s_{\delta_2}}$$

$$e(P_A, H^{(\alpha+\beta)})^c e(H, a)^{cx_i(\alpha+\beta)} / e(T_4, a)^{cx_i}$$

$$= e(T_4, a)^{s_x} e(P_A, H)^{-s_\alpha - s_\beta} e(H, a)^{-s_{\delta_1} - s_{\delta_2}}$$

$$e(P_A, T_3)^c e(T_3, a^{x_i})^c / e(T_4, a^{x_i})^c$$

$$= e(T_4, a)^{s_x} e(P_A, H)^{-s_\alpha - s_\beta} e(H, a)^{-s_{\delta_1} - s_{\delta_2}}$$

$$e(P_A, T_3)^c e(T_3, P_A)^c / e(T_4, P_A)^c$$

$$= e(T_4, a)^{s_x} e(P_A, H)^{-s_\alpha - s_\beta} e(H, a)^{-s_{\delta_1} - s_{\delta_2}}$$

$$((e(P_A, T_3))^2 / e(T_4, P_A))^c$$

$$T_1^{s_x} / P_1^{s_{\delta_1}} = T_1^{r_x + cx_i} / P_1^{r_{\delta_1} + c\delta_1} = P_1^{\alpha(r_x + cx_i)} / P_1^{r_{\delta_1} + c\delta_1}$$

$$= P_1^{\alpha r_x} / P_1^{r_{\delta_1}} = T_1^{r_x} / P_1^{r_{\delta_1}} = R_4$$

$$T_2^{s_x} / P_2^{s_{\delta_2}} = T_2^{r_x + cx_i} / P_2^{r_{\delta_2} + c\delta_2} = P_2^{\beta(r_x + cx_i)} / P_2^{r_{\delta_2} + c\delta_2}$$

$$= P_2^{\beta r_x} / P_2^{r_{\delta_1}} = T_2^{r_x} / P_2^{r_{\delta_2}} = R_5$$

B. *Unforgeability Analysis*

None member and nor authentication center within the domain can pretend to be another member to access resources of cross-domain. The reason is that the private key of every member of a domain is not the public information. Suppose that the authentication center *KCA₁* in the domain *D₁* want to visit the resources of a member *U₂* within another domain *D₂* , he pretends to be a member *U₁* and then sends the public key of inter-domain $dpk = (g_1, P_{u_1}, reg_1, P_1, P_2, H)$ to *U₂*. Because he could not provide the private key x_1 of U_1, he is only verified that he is a member of D_1, but his signature verification is not successfully.

C. Anonymity Analysis

The authentication protocol can guarantee that the authentication center don't know the detailed identity information of a foreign member U_1 while he can confirm that U_1 comes from a given domain. The reason is that the authentication union protocol of cross-domain includes two authentication steps, which can satisfy the anonymous requirement. The first step is a member U_1 sends his public key of cross-domain to a member U_2 and U_2 verifies that U_1 comes from the domain D_1. The second step is U_1 send his signature to U_2, U_2 verifies the signature of $U_1$is correct and knows he is the given member whose information could be used for tracing when there are inconsistent problems.

D. Traceability Analysis

The proposed authentication protocol has the traceability. The tracing information is the register key reg_1 that is included in the public key of cross-domain $dpk = (g_1, P_{u_1}, reg_1, P_1, P_2, H)$ provided by the resource visitor U_1. The owner of the register key is the authentication center of local domain, so the resource provider U_2 can identify the member comes from the domain D_1 by calculating $e(reg_1, P_1) = e(g_1, P_{u_1})$ when the tracing is needed, then U_2 calculates $reg_1 \leftarrow T_4 / e(T_1, T_2)$ and sends the result to the authentication center of D_1, KCA_1 finally traces the member U_1 based on the register key reg_1.

E. Security Analysis

The signature scheme used in the authentication protocol of cross-domain is based on the theory of bilinear group and its security depends on the complex nature of the problems that include calculating discrete logarithms of the large prime and of the elliptic curve. In our cryptosystem, cyclic groups are generated by using the large prime in the elliptic curve as the generation element. Therefore, the security of the register key sent to KCA by members in local domain is guaranteed by the complex nature of the problem that is calculating the discrete logarithm of the large prime and the security of the session key negotiation procedure is guaranteed by the complex nature of the problem that is calculating the discrete logarithm of the elliptic curve. Based on the security above, the middleman attacks, spoofing attacks and replay attacks can be avoided.

(1) Preventing middleman attack: Assume that the middleman tries to attack this protocol, it is impossible to reach an agreement during negotiating the session key, because the public key is verified by the signature. When the step $U_2 \rightarrow U_1 : (P_2, P_{u_1}{}^{X_B})$ is executed, U_3 doesn't have the private key x_1 of U_1 to decrypt $P_{u_1}{}^{X_B}$, so $P_{u_1}' = g_1{}^{X_A}$ and $P_{u_2}' = g_2{}^{X_B}$ could not to be calculated, U_3 and U_1 or U_3 and U_2 could not calculate the agreed temporary session key $P_{u_1 u_2} = e(P_{u_1}', P_{u_2}') = e(g_1, g_2)^{X_A X_B}$

(2) Preventing spoofing attacks: Assume that user U_3

$U_3(U_1) \rightarrow U_2 : type, dpk(g_1, P_{u_1}, reg_1, P_1, P_2, H)$

$U_2 \rightarrow U_3(U_1) : c = H(m, T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5)$;

pretends to be U_1 to access resource of U_2, that is to say,

$U_3(U_1) \rightarrow U_2 : \sigma = (s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$, it is impossible

for U_2 to verify the signature of U_3 based on the parameters $(dpk, T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5, c)$.

(3) Preventing replay attack: The temporary session key is used one time when two members in different domains communicate with each other, which could prevent replay attack.

The analysis above shows that the authentication protocol is correct and that it could prevent effectively spoofing attack. It could achieve authentication when two members that communicate with each other don't know the identification of the other, so it has good anonymity. When the issue occurs, the entity could be traced and attacks could be prevented effectively, so the protocol has good security.

VII. Implementation Of The Authentication Protocol

A. Communication Protocol and Programming Environment

For proposed authentication protocol, we design and implement a prototype system. This prototype system uses point to point encryption based on the TCP/IP communication protocol, which improves the portability of system and is easier to be implemented. In addition, point to point encryption can provide protection for the continuous data transmission between two end users located in different domains. For the middle users at the transmission chain, the messages are encrypted.

The object-oriented program-developing tool named Visual C++ 6.0 is selected as our programming language to implement the prototype system and the Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL for short) is also used to generate the user signature and execute the authentication. Finally, the prototype system runs on Windows XP operating system.

B. The Structure of Prototype System

Fig.2 shows the algorithm structure of our prototype system. All algorithms are encapsulated in the classes. For example, the big integer arithmetic at the low level composes the main functions of the Big Class and the Enc Class includes all the elliptic curve operations at the middle level, which are already be implemented in the MIRACL. Therefore, the prototype system is easier to be implemented based on the MIRACL.

C. Implementation of Communication between Two Entries

In our prototype system, there are three types of communication entries, including the KCA, the resource visitor and the resource provider. For the resource provider, it is possible to be both a server and a client during the communication based on the TCP/IP protocol while the KCA must be a server and the resource visitor is a client. The server and the client establish the connection between them by using the Windows Socket, where four functions such as Socket(), Bind(), Listen() and Accept() are used to the server process and two functions such as Socket() and Connect() are used to the client process. Fig. 3 shows the communication process between a server and a client.

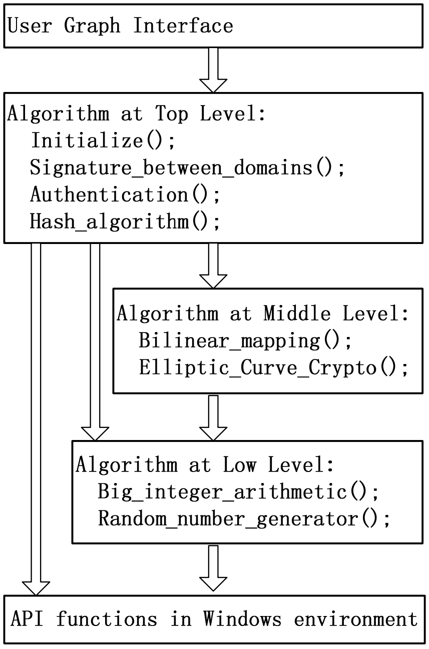

Fig.2 Algorithm level of prototype system

D. Implementation of Authentication Protocol

The proposed authentication protocol is implemented by using the sharing files and some main functions in the MIRCAL. These sharing files include four C++ source files such as big.cpp, ecn.cpp, zzn.cpp, zzn2.cpp and six header files such as big.h, ecn.h, miracle.h, mirdef.h, zzn.h, zzn2.h. The functions are described as follows:

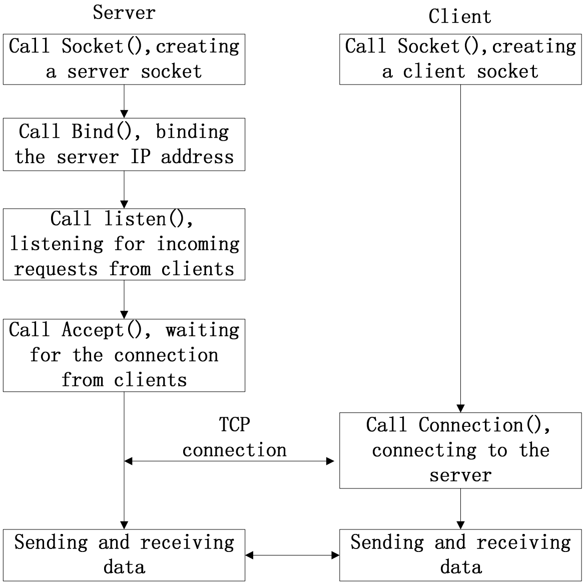
Server
Client
Call Socket(),creating a server socket
Call Socket(),creating a client socket
Call Bind(), binding the server IP address
Call listen(), listening for incoming requests from clients
Call Accept(), waiting for the connection from clients
TCP connection
Call Connection(), connecting to the server
Sending and receiving data
Sending and receiving data

Figure 3 Communication between server and client

(1) ecurve (0,1,p,MR_PROJECTIVE);

This is an initialization function of elliptic curve. The initialized elliptic curve is $y^2 = x^3 +1$.

(2) void extract(ECn& A,ZZn& x,ZZn& y)

This function extracts the points on the elliptic curve A to match with the corresponding points in the coordinate system ZZn.

(3) void g(ECn&A, ECn&B, ZZn2&Qx, ZZn2&Qy, ZZn2& num)

This function defines the operation of summing and multi point arithmetic in the elliptic curve arithmetic.

(4) BOOL fast_tate_pairing(ECn& P,ZZn2& Qx,ZZn2& Qy,Big& q,ZZn2& res)

This function computes fast the Tate Pairing on the elliptic curve.

(5) BOOL ecap(ECn& P,ECn& Q,Big& order,ZZn2& cube,ZZn2& res)

This is a main encryption function.

(6) Void shs256-hash(sha256 *sh, char hash[32])

This is a hash function that mainly achieves the number system conversion.

With the following steps, the detailed authentication protocol is implemented.

Step 1: The initial parameters of each trust domain are generated. The main function file is para_set.cpp. When the authentication system is initialized, a nine-bit binary number needs to be input which represents the ID of this domain. Then the bilinear pairing and other initial parameters are generated and stored into the file common.para, except that the master key is stored in the file master.para.

Step 2: The register keys of members in one domain are generated. Each member selects randomly a big prime as its private key and stores it into the file private.para,. Then the register key is computed based on the master key and other system parameters that are generated in the previous step. At last, each member submits its register key to the KCA of the local domain. The file that achieves this function is register.cpp.

Step 3: The resource visitor computes its signature based on the identification value c that is sent by the resource provider. The implementation of this step refers to the formulas (1)-(5) described in section V.

Step 4: The resource provider verifies the signature of the visitor. Based on the public parameters $(dpk, T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5, c)$, the signature of the visitor can be verified by performing the following steps:

$$aH^{(\sigma_1+\sigma_2)} \overset{?}{=} T_3 P_u \text{ ; } R_1 \overset{?}{=} P_1^{s_\alpha} / T_1^c \text{ ; } R_2 \overset{?}{=} P_2^{s_\beta} / T_2^c$$

$$R_3 \overset{?}{=} e(T_4, a)^{s_x} e(P_1, H)^{-s_\alpha - s_\beta} e(H, a)^{-s_{\delta_1} - s_{\delta_2}} ((e(T_3, P_1))^2 / e(T_4, P_1))^c ;$$

$$R_4 \overset{?}{=} T_1^{s_x} / P_1^{s_{\delta_1}} ; \; R_5 \overset{?}{=} T_2^{s_x} / P_2^{s_{\delta_2}}$$

VIII. CONCLUSION

The authentication of multi-domain union can ensure the security of sharing resources in multi-domain network environment. The proposed authentication protocol of cross-domain union in this paper can satisfy the secure requirement of accessing the resources in other domains while the resources in different domains can be shared. In addition, it has the anonymity that can protect the private information of members within one domain and the better flexibility because every member can visit the resources in other domains without the involvement of KCA in the local domain. What's more, this protocol has better security and practicality because it can avoid the bottlenecks and the complex certification delivery of traditional PKI model.

ACKNOWLEDGEMENTS

This work are supported by a grant from the Basic and Advanced Technology Research Program of He'nan Scientific Committee (No. 112300410196) and a grant from the Science and Technique Foundation of He'nan Scientific Committee of China (No. 122102310314)

REFERENCES

[1] Randy Butler, Von Welch, Douglas Engert. "A national scale authentication infrastructure," *IEEE Computer*, vol. 33(12), pp: 60- 66, 2000.

[2] Jung-San Lee, Chin-Chen Chang, Pen-Yi Chang, et,al. "Anonymous authentication scheme for wireless communications," *International Journal of Mobile Communications*, vol.16, pp: 590 – 601, 2007.

[3] Liu Wei-hong, Wang Li-bin, Ma Chang-she. "Improved cross-realm C2C-PAKE protocol," *Journal of Computer Engineering*, vol. 36(19), pp: 162-164, 2011.

[4] Mengbo Hou, Qiuliang Xu, Fengbo Lin." An Efficient Certificate Revocation and Verification Scheme from Multi-Hashing", *Journal of Computers*,vol.7(6), pp:1437-1444,2012.

[5] Peng Hua-xi. "An identity-based authentication model for multi-domain," *Journal of Computers*, vol. 29(8), pp: 1271-1281, 2011.

[6] L Chen, K Harrison, D Soldera. "Smart Applications of multiple trust authorities in pairing based cryptosystems," *In Proceedings of Infrastructure Security*. *Berlin*: *Springer -Verlag*, pp: 260-275, 2002.

[7] J Malone-Lee. "Identity-based signcryption," unpublished, http://eprint.iacr.org/2002/098.pdf, Sep. 2002.

[8] Wei Yuan, Liang Hu, Hongtu Li, Jianfeng Chu, Hui Wang. "Cryptanalysis and Improvement of an ID-Based Threshold Signcryption Scheme", *Journal of Computers*, vol.7(6), pp:1345-1352,2012.

[9] Wei Yuan, Liang Hu, Hongtu Li, Jianfeng Chu, Yuyu Sun. "Analysis and Enhancement of Three Identity-based Signcryption Protocols", *Journal of Computers*,vol.7(4), pp:1006-1013,2012.

[10] Lu Xiao-ming, Feng Deng-Guo. "An identity-based authentication model for multi-domain Grids," *Acta Electronica Sinica*, vol. 34(4), pp: 577-582, 2010.

[11] Zhu Wen, He Ming-xing. "On automorphism groups of finite groups," *Journal of University of Electronic Science and Technology of China*, vol. 29(5), pp: 549-551, 2005.

[12] David Freeman. "Converting pairing-based cryptosystems from composite-order groups to prime-order groups," *Springer Berlin / Heidelberg*, vol. 6110, pp: 44-61, 2010. [In Proceedings of Infrastructure Security, 2010].

Hao Shen-Gang is a lecturer at Nanyang Normal University, Henan Province, China. He was born in 1977. He has a B.S and M.S. in computer science. His recent research interests revolve around information security and computer network.

Zhang Li is a lecturer at Nanyang Normal University, Henan Province, China. She was born in 1978. She has a B.S and M.S. in computer science. Now she is a Ph.D. candidate at Beijing Institute of Technology, Beijing, China. Her recent research interests revolve around information security and digital forensics.

Ghulam Muhammad is a Ph.D. candidate at Beijing Institute of Technology, Beijing. He was born in Pakistan in 1985. He has gotten a B.S and M.S. in computer science from Mehran University of engineering and technology. Jamshoro. Sindh . Pakistan. His recent research interests revolve around information security and Network storage.