Cross-domain Authentication Alliance Protocol Based on Isomorphic Groups

Qikun Zhang
School of Computer Science and Technology, Beijing Institute of Technology, Beijing, China
Email: zhangqikun04@163.com

Jun Zheng, YuanTan, Ruifang Wang, Yuanzhang Li
School of Computer Science and Technology, Beijing Institute of Technology, Beijing, China
Email: zhengjun@bit.edu.cn

***Abstract*—With the development of information technology in distributed network, such as cloud computing and grid computing. They need mutual coordination resources among the various areas to meet the requirement in infinite speed and infinite space of information technology for people. To ensure secure access resources among areas, the paper proposes a cross-domain authentication alliance-agreement. This agreement constructs a large prime group over elliptic curve, and uses direct product decomposition of the large prime group to construct multiple automorphism groups. Each automorphism group is made as a different key parameter in different domains to overcome the defect of key parameters consistency in the alliance-domain of the existing programs, and all the members must register with blinded keys in their domains to avoid the authority faking the members to cross-domain access resources of the existing programs, and uses the bilinear automorphism group for inter-domain signcrypt to achieve the cross-domain alliance certification, to overcome the complexity of certificate transmission and bottlenecks in the scheme of PKI-based. Analyses show that this scheme has anonymity, security and supporting mutual anonymous authentication.**

***Index Terms*—inter-domain signcryption; alliance-certification; direct product decomposition; bilinear groups**

I. INTRODUCTION

Along with the rapid development of information technology, the information service requirement of people is continual growing. There has developed some huge distributed networks recent years, such as grid computing, cloud computing, etc, which unite a lot of computers to intensify mutual cooperation for meeting the information requirement of infinite speed and space of people. The features of these networks is that lots of computers within the network work together and access each other's resource in differences domains to obtain sufficient resource to provide sufficient services. Within this background, it relates to the security issue of resource access among different domains. Each domain would configure its local authentic service mechanism to provide authentic services and therefore, every organization has established relatively independent trust domain, users within a domain trust the local authentic center, authentic center of each domain provides convenient authentic services for local users. Single domain does not satisfy large amount of service requirements, so it is necessary to request multi-domain resources. Therefore, the request of shared resources comes not only from members within the domain, but also from members outside the domain. Here exist the problems of cross-domain authentication when users of other domains access resources of this trust domain.

Applications of cross-domain authentication, such as the authentication among multiple heterogeneous domains within a virtual organization under the grid environment[1], the roaming access authentication under the environment of wireless network, etc. there are mainly two cross-domain authentication frameworks under specific environments: one is authentication framework (such as Kerberos)[2] based on the symmetric key system. This scheme relates to the complexity of symmetric key management and key consultations, and cannot deal with the anonymous problem effectively. The other is authentication framework based on traditional PKI [3][4][5], the procedures of credentials under public key cryptography is a heavy burden, specifically, the consumptions is caused by the construction of credential paths and the query of the status of credentials and transfer of credentials .It can also cause the network bottleneck of authentication center when under frequent cross-domain accesses. References [6][7][8] purposed an identity-based multi-domain authentication model, which is based on the trust of the authority of the other side, and it requires the key agreement parameters of all domains to be same, this have limitations and could not avoid the authority faking the members to cross-domain access resources. Reference [9][10] adopt signcryption to implement the authentication when users access resource each other within the same domain, it is confined to a single domain, and reference [11] extends it to enable the members from the difference

Manuscript received November 20, 2010; revised December 10, 2010; accepted January 10, 2011.

© 2011 ACADEMY PUBLISHER
doi:10.4304/jcp.6.4.650-656

domains to authenticate each other, but the precondition of this solution is the hypothesis that PKG of every domain is honest. PKG possesses the private keys of all the members within its domain, and if PKG is malicious, the truth identity of user and the confidential of private key could not be guaranteed.

Cross-domain authentication union protocol should achieve security authentication among domains and also ensure the anonymity of each side Correspondent. Given a cross-domain authentication protocol, the verifier can not figure out the identity of the prover, this is called anonymity of cross-domain authentication. Manager of each domain can track the identity of the prover within the domain, and this is called the traceable problem. Along with the research of cross-domain authentication, more and more features required of the cross-domain authentication mechanism. Cross-domain authentication protocol purposed in this article can achieve the features as follows:

Correctness: a legal member within a domain can definitely pass the authentication among domains through authentication algorithm of the cross-domain authentication alliance protocol.

unforgeability: it is computationally infeasible that a member fake others to generate an algorithm that can be passed the authentication by the cross-domain alliance authentication, even if the member is a manager of a domain.

Anonymity: except for the manager of the domain, it will be computationally infeasible for anyone to determine the identity of the prover.

Traceability: for anonymous authentication, the manager of the domain can determine the identity of the prover.

Anti-attack:cross-domain authentication alliance protocol should adopt strict logical authentication process, which can defenses various attacks.

II. PRELIMINARIES

A. Self-isomorphic Group of Finite Group [12]

Let G be a group, $AutG$ represents self-isomorphic group of G, $C(G)$ is the center of G, $\langle g \rangle$ is an $Abel$ group generated by g. If G is a finite group, $|G|$ is the order of G. If G is a finite group and $|G| = p^n (n > 0)$, and G is defined as $p-$gr oup（p is a prime）.

Let H be a $p-$Subgroup of a finite group G, and H is the highest exponentiation of p in the factorization of $|G|$, H is defined as $sylow\ p-subgroup$ of G

Theorem 1[12]: let G be a finite $Abel$ group, $p_1, p_2, ..., p_n$ are all prime factors of $|G|$, $G_{p_i} (1 \le i \le n)$ are the $sylow\ p-$subgr oups of G, which gives direct product decomposition: $G = G_{p_1} \times G_{p_2} \times ... \times G_{p_i}$.

Theorem 2[12]: let $G = G_1 \times G_2 \times ... \times G_n$, if K_i is a sub-group of G_i $(1 \le i \le n)$, and $K_1, K_2, ..., K_n$ are isomorphic to each other, and then G has n sub-groups which are isomorphic to each other.

Theorem 3[12]: let $G_1 = \langle g_1 \rangle$, $G_2 = \langle g_2 \rangle$ are cyclic groups, and m, n are the order of G_1 and G_2 respectively, if $(m, n) = 1$, then $G_1 \times G_2$ is a cyclic group with the order of mn.

B. Bilinear Group [13]

Let G_1 and G_2 be a pair of bilinear groups, let $G_1 = \langle g_1 \rangle$, $G_2 = \langle g_2 \rangle$, and G_3 is a cyclic group with high prime order p, φ is the isomorphic mapping from G_1 to G_2, $\varphi(g_1) = g_2$, e is a computable mapping, $e: G_1 \times G_2 \to G_3$ has the following properties:

Bilinearity: For all $u \in G_1$, $v \in G_2$ and $a, b \in Z_p$, $e(au, bv) = e(u, v)^{ab}$.

Non-degeneracy: $e(g_1, g_2) \ne 1$.

C. M ulti-linearMapping

Multi-linear Diffie-Hellman hypothesis:paper [14] give the definition of l-multi-linear mapping, let G_1 be an addition group, G_2 be a multiplicative group, the discrete logarithmic over G_1 and G_2 is hard to solve.

Definition 1: mapping $e_1 : G_1^L \to G_2$ is defined L multi-linear mapping, if it has the following properties:

a) G_1 and G_2 have the same prime order p;

b) For all $a_1, a_2, ... a_l \in Z_p$, $g_1, g_2, ... g_l \in G_1$, there exists $e_1(a_1 g_1, a_2 g_2, ... a_l g_l) = e_1(g_1, g_2, ... g_l)^{a_1 a_2 ... a_l}$

c) non- degeneracy: if g is one of generators of G_1 $(g \in G_1)$, then $e_1(g, g, ... g)$ is also one of generators of G_2.

Definition 2: Determinable multi-linear Diffie-Hellman problem (DMDH) is that, given $e(g, a_1 g, a_2 g, ... a_{l+1} g)$ and $\forall z \in G_2$, whether determine $e_1(g, g, ... g)^{a_1 a_2 ... a_{l+1}}$.

Definition 3: Determinable multi-linear Diffie-Hellman hypothesis is that it is hard to solve determinable multi-linear Diffie-Hellman problem. This means that there does not a probabilistic polynomial time algorithm to solve Diffie-Hellman problem.

© 2011 ACADEMY PUBLISHER

III. CROSS-DOMAIN AUTHENTICATION MODEL

In order to ensure resource network to provide infinite information resource, space resource and computation speed, it is necessary that resources distributed in every domain of the network to coordinate and cooperate. Cross-domain authentication is a kind of inter-domain authentications that ensure the security of communication and resource sharing among domains, resource network model is shown in Fig1.

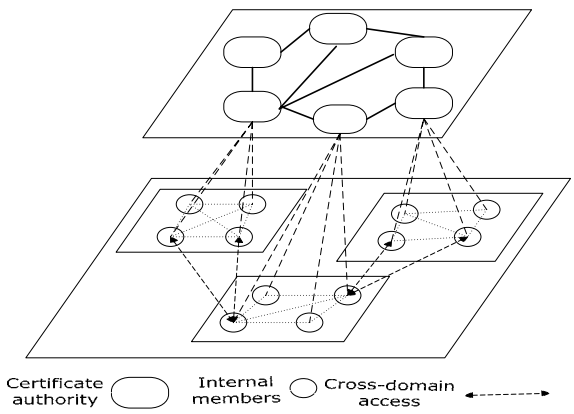


Figure 1. the modal of network

In this model, system is composed of multiple domains, and each domain is independent and autonomous. Each domain is composed of an key authentication center (KAC) and many internal members, KAC like to the traditional CA or PKG, members of alliance-domain are both provider and user of the resources, internal members of each domain need cross-domain access resource in the case of collaborative computing. Each KAC select one of automorphism cyclic groups to design its key parameters, KAC distribute and manage the key of the members within the domain. For the authentication and access resource among domains, the KAC need announce the public key of its domain. In order to trace entity conveniently, members need to register in the domain when they enrolled in a domain.

IV. INTER-DOMAIN SIGNCRYPTION SCHEMES

A. Initiation of The System

Choose R big primes that mutual prime each other constitute a set $R_S = \{r_i \mid (2 \le i \le R)\}$, Choose a big prime P, compute a hypersingular elliptic curve $E/GF(P)$ that satisfies WDH security hypothesis, G is a sub-group of $E/GF(P)$ with high prime order q ($q = r_1 \times r_2 \times \ldots \times r_i$). Let $G_{r_i}(1 \le i \le R)$ be $sylow$ $p-\text{subgroups}$ of G, The direct product decomposition of $G: G = G_{r_1} \times G_{r_2} \times \ldots \times G_{r_i}$. Construct R sub-groups of G that are isomorphism to each other according to the Theorem 2, let the set of $sub-groups$ $GK = \{G_k \mid (1 \le k \le R)\}$. Under the multi-domain unite architecture, each domain select a different sub-group $G_k(1 \le k \le R)$ from set GK as the key generator parameter of the domain. Let generators of each cyclic group are respectively: $g_1, g_2, \ldots g_R$, and the private key of each KAC in alliance-domain are $x_1, x_2, \ldots, x_3$ respectively, the corresponding public keys are: $p_1 = x_1 g_1, p_2 = x_2 g_2, \ldots, p_R = x_R g_R$ respectively, public keys are published. According to the multi-linear mapping theorem, each KAC calculates the key of alliance-domain as follows:

$$\begin{aligned} s_0 &= e_1(x_1, p_2, \ldots, p_R) \\ &= e_1(p_1, x_2, \ldots, p_R) \\ &= \ldots \\ &= e_1(p_1, p_2, \ldots, x_R) \\ &= e_1(g_1, g_2, \ldots, g_R)^{x_1 x_2 \ldots x_R} \end{aligned}$$

B. Inter-domain Signcrypt Scheme

a) Let D_1 and D_2 be two domains in the alliance-domain, D_1 select cyclic group $G_{d1} = \langle g_1 \rangle$ as the key generator parameter of its domain, an D_2 select cyclic group $G_{d2} = \langle g_2 \rangle$ as the key generator parameter of its domain ($g_1, g_2 \in R_S$) , G_{d1}, G_{d2} are two isomorphism prime groups in set GK, φ is the isomorphism mapping from G_{d2} to G_{d1}, $\varphi: \varphi(kg_2) \to kg_1, k \in_R Z_P^*$, $e: G_{d1} \times G_{d2} \to G_p$ is an efficiently computable bilinear mapping, $h: \{0,1\}^* \to Z_p$ is a hash function, public-private key pairs of the two domains are $(x_1, x_1 g_1)$ and $(x_2, x_2 g_2)$ respectively, $x_1, x_2 \in_R Z_P^*$.

b) Key distribution and key registration of members of internal domain: assume that domain D_1 has n members, KAC_{D_1} is the key authentication center of D_1, x_1 is a private key of KAC_{D_1}, and the corresponding public key is $p_1 = x_1 g_1$. s_0 is a private key of alliance-domain and the corresponding public key is $p_p = s_0 g$. The mapped public key of alliance-domain in domain D_1 is $p_0 = s_0 g_1$. KAC_{D_1} compute $\frac{1}{(s_0 + x_1)} g_1$ and then sent to all the members in its domain ,each member U_m of the domain select $x_m, k_m (x_m, k_m \in_R Z_P^*)$ randomly

© 2011 ACADEMY PUBLISHER

after received $\frac{1}{(s_0+x_1)}g_1$, and compute the register key $A_m=\frac{x_m}{s_0+x_1}g_1$, the public-private key pair of the member is $(x_m, x_m g_1)$, and then sent public key $y_m = x_m g_1$ and $A_m=\frac{x_m}{s_0+x_1}g_1$ to his KAC_{D_1}, KAC_{D_1} verify the received value $e(A_m,(p_1+p_0))\overset{?}{=}e(y_m,g_1)$,If the check success and y_m is unique within that domain, , then U_m can register with A_m as register-key. KAC_{D_1} store (A_m, y_m) for tracking. All members of each domain register in this way.

c) Given inter-domain public key $dpk=(p_1,p_0,A_m,y_m,g_1,\varphi)$, and the private key x_m and register key A_m of the prover, and the signature message $m\in\{0,1\}*$, member holding the key pair (A_m, y_m) operates as follows:

1) Choose $u,v\in_R Z_P^*$ randomly;

2) Compute

$$T_1 \leftarrow ug_1$$

$$T_2 \leftarrow vy_m$$

3) Compute the question value

$$c \leftarrow h(T_1,T_2,m)$$

4) Compute

$$b_1 \leftarrow u+cx_m$$

$$b_2 \leftarrow vA_m cx_m$$

5) $\sigma=(T_1,T_2,b_1,b_2,c)$ as the inter-domain signcryption to signature message m generated by prover.

d) Verify: given domain public key $dpk=(p_1,p_0,A_m,y_m,g_1,\varphi)$, signature message m and signature σ. The verifier verifies the signature as follows:

1) Compute

$$e(A_m,(p_1+p_0))\overset{?}{=}e(y_m,g_1)$$

$$c' \leftarrow h(T_1,T_2,m)$$

$$b_1 g_1 \overset{?}{=} T1 + c' y_m$$

$$e(\frac{1}{c'}(p_1+p_0),b_2)\overset{?}{=}e(y_m,T_2)$$

2) If the signature satisfies above 3 expressions, it is valid signature. Else, it is not valid signature.

V. Cross-domain alliance authentication and key consultation protocol

To ensure the security, members from different domains need to be authenticated when they access resources each other. There is a KAC in every domain. To speed up the resource access, and to avoid the bottleneck problem during the authentication, this paper purposed a inter-domain alliance authentication protocol, which enables direct authentication between members and does not need the ticket transfer through the authentication center. Let two domains in the alliance-domain are D_1 and D_2 respectively, the cyclic group G_{d1} of D_1 generated by g_1 and cyclic group G_{d2} of D_2 generated by g_2, the public-private key pair of KAC in D_1 is (x_1,p_1) and public-private key pair of KAC in D_2 is (x_2,p_2), and the public-private key pair of alliance-domain is (x_0,p_0). U,V are internal members of D_1 and D_2 respectively. x_u is the private key of U ,and A_u is the register key of U ,and $y_u = x_u g_1$ is the public key of U. x_v is the private key of V ,and A_v is the register key of V ,and $y_v = x_v g_2$ is the public key of V .The public key between the two domains is $dpk=(p_0,p_1,A_u,y_u,g_1,\varphi)$ (any public key between two domains is dynamic, it is determined by the register key and public key of prover). When U want to access resource from V, the process of cross-domain authentication is described as follows:

$$U \xrightarrow{dsk,T_1,T_2} V \quad (1)$$

$$U \xleftarrow{c=h(T_1,T_2,m)} V \quad (2)$$

$$U \xrightarrow{b_1,b_2,c} V \quad (3)$$

$$U \xleftarrow{x_v y_u, y_v} V \quad (4)$$

$$U \xrightarrow{x_u y_v} V \quad (5)$$

$$U \xleftarrow{x_u x_v g_1} V \quad (6)$$

The expression (1): prover U send the public key $dpk=(p_0,p_1,A_u,y_u,g_1,\varphi)$ of theirs and the related authentication parameters T_1,T_2 to verifier V, V verifies whether p_1 is a public key of KAC in the alliance-domain and whether y_u is a public key of a member that belongs to this domain by whether the expressions $e(A_u,(p_1+p_0))\overset{?}{=}e(y_u,g_1)$ and $\varphi(p_0)\overset{?}{=}p_0^{'}$ ($p_0^{'}$ is a mapping public key of p_0 in domain D_2, $p_0^{'}=s_0 g_2$) are satisfaction. The expression (2): V sends question value c to U after verification, The expression (3): U compute b_1,b_2 after

© 2011 ACADEMY PUBLISHER

having received the question value c, and send the result b_1, b_2 together with the question value c back to V. The expression (4): V verifies if expression $b_1 g_1 \overset{?}{=} T1 + c' y_u$ and $e(\frac{1}{c'}(p_1 + p_0), b_2) \overset{?}{=} e(y_u, T_2)$ （ $c' = h(T_1, T_2, m)$ ） are satisfaction. If the signature satisfies above 4 expressions, it is valid inter-domain signature. The expressions (5)and(6) are the session key agreement of them .They can compute $p_{vu} = x_v y_u = \varphi(x_u y_v) = p_{uv} = x_u x_v g_1$ as their session key.

VI. PERFORMANCE ANALYSIS

A. Correctness Analysis

Cross-domain alliance authentication protocol is established based on inter-domain signature. In order to ensure the safe authentication when the domains access resources each other, the correctness of the signature must be ensured for first time:(1) KAC that is not in the alliance-d domain cannot be valid inter-domain signature, (2) members that are not in the domains cannot be valid inter-domain signature, (3) ensure the uniqueness of the internal member in a domain.

a) $e(A_m, (p_1 + p_0))$

$$= e(\frac{x_m}{(s_0 + x_1)} g_1, (s_0 g_1 + x_1 g_1))$$

$$= e(\frac{x_m}{(s_0 + x_1)} g_1, (s_0 + x_1) g_1)$$

$$= e(g_1, g_1)^{\frac{x_m}{(s_0 + x_1)}(s_0 + x_1)}$$

$$= e(g_1, g_1)^{x_m}$$

$$= e(x_m g_1, g_1)$$

$$= e(y_m, g_1)$$

b) $b_1 g_1 = (u + c x_m) g_1$

$$= u g_1 + c x_m g_1$$

$$= T1 + c y_m$$

c) $e(\frac{1}{c}(p_1 + p_0), b_2)$

$$= e(\frac{(s_0 + x_1)}{c} g_1, v A_m c x_m)$$

$$= e(\frac{(s_0 + x_1)}{c} g_1, v \frac{x_m}{(s_0 + x_1)} g_1 c x_m)$$

$$= e(g_1, g_1)^{\frac{(s_0 + x_1)}{c} v \frac{x_m}{(s_0 + x_1)} c x_m}$$

$$= e(g_1, g_1)^{v x_m x_m}$$

$$= e(x_m g_1, v x_m g_1)$$

$$= e(y_m, T_2)$$

B. Security Analysis

The security of cross-domain alliance authentication protocol has two aspects: one is the security of the inter-domain signature, the other is the security of the authentication protocol. The security of the signature method purposed in this article relies on the elliptic curve discrete logarithmic problem.

a) unforgeability: any member or KAC that is out of the alliance-domain can not fake the KAC that is in the alliance-domain, and any member within a domain can not fake other members to achieve cross-domain access resource.

1) Assume that any KAC that is out of the alliance-domain can fake the public key p_1 of any domain D_1 .He has not the corresponding key s_0 of the alliance-domain, and the verification $e(A_m, (p_1 + p_0)) = e(y_m, g_1)$ will be fail.

2) Assume that the member U in the domain D_1 attempt to access the resource of member V within another domain D_2, because the private key x_u of U is not published, even if the KAC of domain D_1 can fake the identity of member U with identity U' to send $dpk = (p_0, p_1, A_u, y_u, g_1, \varphi)$ to V, and this can only prove that U' is a member in the domain D_1, but U' do not know the private key x_u of U, therefore the verification $b_1 g_1 = T_1 + c y_u$ will be fail.

b) Anonymity: there can only determine that a user is a specific member of a certain domain, but the identity of the member can not be determined, and only his KAC can determine the identity of the member through registered identity. The anonymity of cross-domain authentication alliance protocol is designed by two steps:

1) User U sends inter-domain public key $dpk = (p_0, p_1, A_u, y_u, g_1, \varphi)$ to V, and V determines U from which domain.

2) U sends the signature σ to V, and V can determine U is a specific member that not be faked by others through verification, but does not know the identity of the member.

c) Traceability: It is not an ideal method to design cross-domain authentication alliance protocol based on the trust, and it is impractical to let members to trust the KAC that is from different domains, and it is must to provide reliable certification to prove irregularities of a certain entity when the disputes are occurred. This protocol is traceable for that the verifier V verify the expression $e(A_u, (p_1 + p_0)) = e(y_u, g_1)$, and V sends A_u, y_u, p_1 and p_0 to the corresponding KAC ,and then the KAC can trace the entity by the registration information of the entity.

© 2011 ACADEMY PUBLISHER

d) Anti-attack: the defensives of the protocol in this article:

1) Against $MITM$: assume that mediator W attempt to attack this protocol, it can not achieve the consistency session key to U and V ,because W does not have the private key x_u of U , and he can not compute $p_{uv} = x_v x_u g_1$ when $V \to U : (y_v, x_v y_u)$. Obviously he also can not compute $p_{vu} = x_u x_v g_2$. W and U or W and V can not achieve the consistent session key $p_{uv} = \varphi(p_{vu}) = x_v x_u g_1$ at last.

2) Against Spoofing Attack: assume that user W fake U to access resource of V : $W(U) \to V : dsk = (p_0, p_1, A_u, y_u, g_1, \varphi)$; $V \to W(U) : c = h(T_1, T_2, m)$; $W(U) \to V$. $\sigma = (T_1, T_2, b_1, b_2, c)$ is the signature for message m generated by U within the domain, and V can verify that is valid signature according to $(dpk, T_1, T_2, b_1, b_2, m, c)$.

3) Against replay attack: The session key used during the communication between two domains is in one-time key, and thus it can defense replay attack.

C. consumption analysis

The consumption of computation and communication is from signature verification and key consultation. The computation consumptions are shown in Table 1.

TABLE I.

COMPUTATION CONSUMPTIONS OF THE PROTOCOL

Type of computation	Times of computation
Bilinear pairing	2
Multiplication	6
Isomorphic mapping	1
Hash	1
Addition	1

This protocol needs 2 bilinear pairing, 4 multiplications, 1 hash and 1 addition for the process of the signature verification and it needs 2 multiplications for the process of the session key consultation. The consumption of communication is mainly from the information exchange between the two sides of the protocol, this article only analysis the member of times of the information exchange between two sides. The communication can also be divided into two processes, one is signature verification and the other is key consultation, the signature verification needs 3 information transfers, and the key consultation needs 2 information transfers.

Analysis shows that this protocol is correct and can defense attack effectively and is not to need to know the identity of each other, which can achieve the effective authentication and good anonymous. The entity can be tracked when there have dispute occurs. It has a good security.

VII. CONCLUSION

Multi-domain alliance-authentication is required for security in multi-domain network environment. The scheme of cross-domain alliance-authentication purposed in this article can ensure the security while share the resource among multiple domains. The anonymity can protect the privacy of each entity, and each entity can access cross-domain resources needless the intervention of the key authentication center, which provide good flexibility. It can avoid the bottleneck problem and the complexity of the transfer tickets of the traditional pattern based on PKI. It is safe and practical.

REFERENCES

[1] Sunan Shen, Shaohua Tang. Cross-Domain Grid Authentication and Authorization Scheme Based on Trust Management and Delegation[C]. Computational Intelligence and Security, vol.1,pp: 399 – 404,January 2008.

[2] Randy Butler, Von Welch, etc... A National-Scale Authentication Infrastructure [J].IEEE Computer, vol. 33,pp:60-66, December 2000.

[3] Jung-San Lee, Chin-Chen Chang, Pen-Yi Chang, Chin-Chen Chang. Anonymous authentication scheme for wireless communications[C]. International Journal of Mobile Communications.pp: 590 – 601, 2007.

[4] Miao Feng-man,Zhang Qiu-yu. Cross-Domain Authentication Model Based on Lattice[C].Information Engineering (ICIE), Vol. 1, pp: 115 – 118, January 2010.

[5] Zheng Xiaorong. Cross-Domain Authentication Model in SOA based on Enterprise Service Bus[C]. Computer Engineering and Technology (ICCET), Vol.5, pp: V5-78 - V5-82,2010.

[6] Peng Huaxi. An identity-based authentication model for multi-momain[J]. Journal of Computers, Vol. 29,pp: 1271-1281, August 2006.

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

[8] Noel McCullagh, Paulo S. L. M. Barreto. A new two-party identity-based authenticated key agreement[OL]. http://citeseerx.ist. psu. edu/viewdoc/download?doi=10.1.1.58.9294&rep=rep1&type=pdf.

[9] J Malone-Lee. Identity-based signcryption [OL]. http://eprint.iacr.org/2002/098.pdf.

[10] Wenbo Zhang ; Hongqi Zhang ; Bin Zhang ; Yan Yang ; An Identity-Based Authentication Model for Multi-domain in Grid Environment[C]. Computer Science and Software Engineering. Vol. 3, pp: 165 – 169, 2008.

[11] Lu Xiaoming, Feng Dengguo. An identity-based authentication model for multi-domain grids [J]. Chinese Journal of Electronics, Vol. 34,pp: 577-582, April 2006.

[12] Zhu Wen, He Mingxing. On automorphism group of finite groups[J].Journal of UEST of China, Vol.29,pp: 549-551,May 2000.

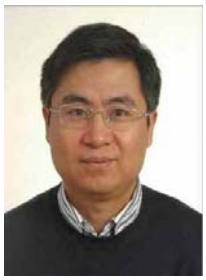
[13] Boneh D. and Franklin M.. Identity based encryption from the Weil pairing [J]. SIAM Journal on Computing. Vol. 32,pp: 586-615, March 2003.

[14] Dan Boneh A. S. .Applications of Multilinear Forms to Cryptography[D]. Contemporary Mathematics. pp: 324:71-90,2003.

© 2011 ACADEMY PUBLISHER

Qikun Zhang,born in 1980 . Ph.D. candidate. Beijing Institute of Technology, Beijing, China. His research interests include information security and cryptography.

Jun Zheng, born in 1969, Vice professor. Beijing Institute of Technology, Beijing, China. Her research interests include information security.



Yuan Tan, born in 1972 .Ph.D. Professor, Ph.D. Beijing Institute of Technology,Beijing,China .supervisor, senior member of China Computer Federation. His current research interests include Information Security and network storage.

Ruifang Wang, born in 1982 . Now she is working in Cityexpress of Beijing. Her research interests include information security and cryptography.

Yuanzhang Li,born in 1978 . Ph.D. candidate. Beijing Institute of Technology, Beijing, China. His research interests include information security and cryptography.

© 2011 ACADEMY PUBLISHER