A Cross-domain Authentication Protocol based on ID

Zheng Jun[1*], Guo Xianchen[1,2*], Zhang Quanxin[1], Zhang Qikun[1]
[1]Beijing Engineering Research Center of Massive language information processing and cloud computing, School of Computer Science and Technology, Beijing Institute of Technology, Haidian 100081, Beijing, P. R. China

[2]The Sixth Research Institute of China Electronics Corporation, Haidian 100083, Beijing, P. R. China

Abstract

In large distributed networks, many computers must be mutual coordination to complete some works Under the certain conditions, these computers may come from different domains. For ensuring the safety to access resources among these computers in different domains, we propose a cross-domain union authentication scheme. We compute a large prime cyclic group by elliptic curve, and use the direct decomposition of this group to decompose n automorphism groups ,and design an signcryption scheme between domains by bilinear of automorphism group to achieve cross-domain union authentication. this scheme overcome the complexity of certificate transmission and bottlenecks in the scheme of PKI-based, and it can trace the entities and supports two-way entities anonymous authentication, which avoid the authority counterfeiting its member to cross-domain access resources. Analyses show that its advantages on security and communication-consumption .

Key words: *signcryption,cross-domain authentication, elliptic curve,bilinear group.*

Ⅰ. Introduction

Cross-domain alliance is needed in large networks, which services and access points are located in multiple domains. In a distributed network environment where companies and institutions have their own sharing resource, in order to prevent unauthorized users to access these shared resources, every institution will set up a local certification service equipment to provide certification services when users access resources. Therefore, a relatively independent trust domain is formed in every institution, and the users that in a domain trust their certification center, and the certification center provides convenient authentication service for local users to access shared resources. However, in the case of in a large number of demand services, such as the demands of cloud computing, users need anytime and anywhere to access resources .In this case, a single domain is unable to meet the needs of resource requests, therefore it is need many domains mutual cooperation to achieve this requests. For this the requests of shared resource are not only from the internal members of the domain, but also from the other domains. When the foreign entities access to the resources in local domain ,there involve the scheme of cross-domain authentication.

The applications of cross-domain authentication in many fields, such as the authentication among multiple heterogeneous domains within a virtual organization under the grid and cloud computing environment[1][2], the roaming access authentication under the environment of wireless network, etc[3][4]. There are mainly two cross-domain authentication frameworks under specific environments: one is authentication framework (such as Kerberos)[5] [6]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 [7][8][9], The management of credentials under public key cryptography is a heavy burden in this scheme; 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[10][11][12] proposed 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 it could not avoid the authority faking members in its domain to cross-domain access resources. Reference [13][14] adopt signcryption to implement the authentication when users access resource each other within the same domain, it is confined to a single domain, so it is difficult to meet the needs of large-scale distributed computing. Reference [15] extends the scheme of reference [13],and make it to enable the members from the difference 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.

The cross-domain authentication alliance protocol proposed in this paper is designed based on inter-domain signcryption, in which each inter-domain authentication centers do not have to set the same parameters for their keys, and the members in a domain register their identities with blind keys other than their private keys to avoid the authentication center faking and cheating his members to access resource from other domains. At the same time it has good anonymity, and it can trace entities when there occurred dispute between two entities for accessing resources, and it has a good defense for various protocol attacks. cross-domain authentication protocol purposed in the paper can achieve the features as follows:

Correctness: a legal user in a domain can be valid verified by all the users when they compute the authentication algorithm of the Cross-domain authentication protocol.

unforgeability: it is infeasible that a faked member generates an algorithm to pass a valid authentication by computing, even if the member is a server of a domain.

Anonymity: except the server of the domain, it should be infeasible that anyone determine the identity of a prover by computing.

Traceability: the KMC of the domain can determine the identity of any prover within its domain.

Anti-attack: Cross-domain authentication protocol should have extensive security and provably secure .

Organization. The rest of paper is organized as follows: In Section II, we introduce the relative knowledge of this paper. In Section III we define the system model. Then, we present our scheme in Section Ⅳ. We provide security analysis, and further analyze the experiment results and performance in SectionⅣ. Finally, we conclude the paper in Section Ⅵ.

2. Preliminaries

2.1 Self-isomorphic group of finite group [16]

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, and $|G|$ is the order of G and $|G| = p^n (n > 0)$, then G is defined as $p-$group（p is a prime）.

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

Theorem 1[16]: 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 $sylow\ p-$subgroups 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 for each other, and then G has n sub-groups which are isomorphic for each other.

Theorem 3[16]: let $G_1 = \langle g_1 \rangle$ and $G_2 = \langle g_2 \rangle$ be cyclic groups, and m and 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 .

2.2. Bilinear group [17].

Firstly ， we give the definition of bilinear map, assuming that G_1, G_2 and G_T are multiplicative groups with same prime order p , $p \ge 2^k + 1, k$ is the security parameter, let $G_1 = \langle g_1 \rangle$ be generated by g_1 and $G_2 = \langle g_2 \rangle$ be generated by g_2 , φ is the isomorphic mapping from G_1 to G_2 : $\varphi(g_1) = g_2$,the solution of discrete logarithm over the G_1 and G_2 and G_T is hard. and e is a computable mapping, and $e: G_1 \times G_2 \to G_T$ has the following properties:

1.Bilinear: For all the $u \in G_1$, $v \in G_2$ and $a, b \in Z_p$,then $e(u^a, v^b) = e(u, v)^{ab}$.

2.Non-degeneracy: There exists $u \in G_1$, $v \in G_2$ such that $e(u, v) \ne 1$.

3. Computable: There is an efficient algorithm to compute $e(u, v)$ for all $u \in G_1$, $v \in G_2$.

Corollary1: for all the $\forall u_1 \in G_1, \forall u_2 \in G_1$, $\forall v \in G_2$,then $e(u_1 u_2, v) = e(u_1, v) e(u_2, v)$.

Corollary2: for all the $\forall u, v \in G_2$,then $e(\varphi(u), v) = e(u, \varphi(v))$.

2.3 Gap Diffie-Hellman Group

We first introduce the following problems in G_1 and G_2 [18].

1. Discrete Logarithm Problem (DLP): if given u and v , to find $n \in Z_p$ from $u = v^n$.

2. Computation Diffie-Hellman Problem (CDHP): Given $(g_1, g_1{}^a, g_1{}^b) \in G_1$, for $a, b \in Z_p$,to compute $g_1{}^{ab}$.

3. Decisional Diffie-Hellman Problem (DDHP:. Give $(g_1, g_1{}^a, g_1{}^b, g_1{}^c) \in G_1$, for $a, b, c \in Z_p$, to decide whether

$c = ab \bmod p$.

We call G_1 and G_2 are GDH groups if DDHP can be solved in polynomial time but no polynomial time an algorithm can solve CDHP or DLP with non-negligible advantage within polynomial time.

3.The cross-domain authentication model

In multi-domain authentication system, the type of authentication is chosen for each domain by themselves demand ,without need a unified authentication model. and inter-domain authentication should try to adopt a common authentication way to achieve cross-domain access interoperability [19]. This cross-domain authentication system model is designed by the paper.

3.1 System Framework.

In this model, the system is composed by multiple domains, each domain is independent and autonomous. Each domain consists of a DAC (domain authority center) and a number of members within the domain, and the domain authority center are similar to traditional CA (Certificate Authority). Every member in a domain not only provides its resources for others but also access resources from others, and they constitute the resource alliance. In the case of collaborative computing, the members of mutual cooperation are not only from a domain, but also from other domains ,for this members in each domain may need to cross-domain cooperation. let $Gset = \{G_k \,|(k = 1, 2, ..., R)\}$ be a large prime set of the automorphism group. In the multi-domain alliance system, each DAC select a different subgroup $G_k (1 \le k \le R)$ from $Gset$ to make key generation parameters for its domain. DAC distributes and manages some keys of their members within its domain, and open the public key of DAC in order to mutual visits and certification. When members join in a domain they need to register with their true identities for entity tracking.

4. Alliance signature scheme between domains

4.1 System initialization.

Let the alliance domain contain R domains,and selects R pairwise relatively prime large prime numbers to form a set of $R_S = \{r_i \,|(i = 1, 2, ..., R)\}$;and choose a big prime p , compute a elliptic curve $E / GF(P)$ that satisfies WDH security hypothesis, G is a sub-group of $E / GF(P)$ with high prime order q ($q = r_1 \times r_2 \times ... \times r_i$),that $|G| = q$. Let $r_1, r_2, ..., r_n$ be all the prime factors of $|G|$,that $q = r_1 \times r_2 \times ... \times r_n$ .Let $G_{r_j} (1 \le j \le n)$ be $sylow_{r_j} -$subgroups of G .

From Theorem 1 we known the direct product decomposition of G : $G = G_{r_1} \times G_{r_2} \times ... \times G_{r_i}$,and we can Construct R sub-groups of G that are isomorphism to each other according to the Theorem2,let this set of $sub-groups$ be $Gset = \{G_k \,|(1 \le k \le R)\}$.

Under the multi-domain unite architecture, each domain select a different sub-group $G_k (1 \le k \le R)$ from set $Gset$ as the key generator parameter of the domain.

4.2 inter-domain signatures.

(1) Let D_1 and D_2 be two domains of alliance-domain ,and D_1 selects cyclic group $G_1 = \langle g_1 \rangle$ as the key generation parameter of its domain, D_2 selects cyclic group $G_2 = \langle g_2 \rangle$ as the key generation parameter of its domain , g_1 and g_2 are the generators of the two cyclic groups respectively .and G_1 and G_2 are the isomorphic group in $Gset$,and $e : G_1 \times G_2 \to G_p$ is an efficiently computable bilinear mapping, and $h : \{0,1\}^* \to Z_p$ is a hash function, and the private /public key pairs of the two domains are $(\xi_1, g_1^{\xi_1})$ and $(\xi_2, g_2^{\xi_2})$ respectively($\xi_1, \xi_2, \in Z_p$),and $H = e(g_1^{\xi_1}, g_2^{\xi_2})$ is the mapping value of the two public keys $g_1^{\xi_1}$ and $g_2^{\xi_2}$.

(2) Key distribution and register of members in a domain: assume that domain D_1 has n members within the domain, and DAC_1 (domain authority center) is the domain authority center of the domain D_1 with private key ξ_1 , and the corresponding public key is $P_{D_1} = g_1^{\xi_1}$,. DAC_1 compute $y = g_1^{\frac{1}{\xi_1}}$ and sent y to every member in the domain D_1 ,and each member U_{D_i} in the domain selects $x_i \in Z_p$ as its own private key, and

the corresponding public key is $P_{u_i} = g_1^{x_i}$,and it computes $reg_i = (y)^{x_i}$,and sent reg_i to the DAC_1 as its register key to register. The DAC_1 establishes the relationship between reg_i and identity of U_{D_i} in order to track the certification.

(3) Suppose a member U_{D_1} of the domain D_1 wants to access resources from the member U_{D_2} of the domain D_2. Assume that the private/ public key pair of U_{D_1} is (x_1, P_{u_1}) ,and it's registered key is reg_{u_1}. The private/ public key pair of U_{D_2} is (x_2, P_{u_2}), and it's registration key is reg_{u_2}.The public key of DAC_1 in domian D_1 is P_{D_1} ,and The public key of DAC_2 in domian D_2 is P_{D_2} ,Certification process is as follows:

1) U_{D_1} Selects $\mu \in Z_p$, and computes

$T_1 = g_1^{\mu}, U_{D_1} \xrightarrow{P_{D_1}, P_{u_1}, reg_{u_1}, T_1} U_{D_2}$;

2) U_{D_2} check whether $e(P_{D_1}, reg_{u_1}) = e(P_{u_1}, g_1)$,if the equation are equal to each other then Selects the message $m \in \{0,1\}*$, and computes the question value

$c \leftarrow h(T_1, m)$,$U_{D_1} \xleftarrow{c} U_{D_2}$;

3) U_{D_1} computes $s_1 \leftarrow \mu + cx_1$

$U_{D_1} \xrightarrow{s_1} U_{D_2}$

4) U_{D_2} verifies the signature on the message m, whether $g_1^{s_1} = T_1 P_{u_1}^{\ c}$

If the signature is correct, it is valid inter-domain signature.

If the verification holds, then the U_{D_2} can prove that U_{D_1} is a number of league domain ,and its the public key is P_{D_1} ,this achieves the results of across multiple domains authentication.

4.3 Session key agreement.

1) U_{D_2} chooses a random number $k_2 \in Z_p$, and compute $f_1 = P_{u_1}^{\ k_2}$. $U_{D_2} \rightarrow U_{D_1} : (P_{u_2}, f_1)$;

2) U_{D_1} can compute $P_{u_1}{}' = g_1^{k_2}$ from $f_1 = P_{u_1}^{\ k_2}$ with his private key x_1, and then choose a random number $k_1 \in Z_p$, and compute $f_2 = P_{u_2}^{\ k_1}, U_{D_1} \rightarrow U_{D_2} : f_2$;

3) U_{D_2} can compute $P_{u_2}{}' = g_2^{k_1}$ from $f_2 = P_{u_2}^{\ k_1}$ with his private key x_2;

4) U_{D_1} and U_{D_2} compute their temporary session key $P_{D_1 D_2} = e(P_{u_1}{}', P_{u_2}{}') = e(g_1, g_2)^{k_1 k_2}$.

5. Performance analysis

5.1. 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) DAC that is not in the alliance-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.

$$e(P_{D_1}, reg_{u_1}) = e(g_1^{\xi_1}, g_1^{\frac{x_1}{\xi_1}})$$
$$= e(g_1, g_1)^{x_1} = e(g_1^{x_1}, g_1)$$
$$= e(P_{u_1}, g_1)$$
$$g_1^{s_1} = g_1^{(\mu + cx_1)} = g_1^{\mu} g_1^{cx_1} = T_1 P_{u_1}^c$$

5.2 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 DAC 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_{D_1} sends inter-domain public key $dpk = (g_1, P_{u_i}, reg_i, P_{D_1}, H)$ to U_{D_2}, and U_{D_2} determines U_{D_1} from which domain with the equation $e(P_{D_1}, reg_{u_1}) = e(P_{u_1}, g_1)$.

2) U_{D_1} sends its signature to U_{D_2}, and U_{D_2} can determine U_{D_1} is a specific member that not be faked by

others through verification whether $g_1^{s_1} = T_1 P_{u_1}^{\ c}$, but does not know the identity of the member U_{D_1} .

5.3 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 DAC 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 U_{D_2} verify the expression $e(P_{D_1}, reg_{u_1}) = (P_{u_1}, g_1)$ to ensure the relationship among $P_{D_1}, reg_{u_1} and P_{u_1}$,further to trace the identity of entity U_{D_1} by the registration information in DAC_1 .

5.4 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 proposed in this article relies on the elliptic curve discrete logarithmic problem. The security of this authentication protocol as follows:

5.4.1 Against $MITM$ **.** Assume that mediator U_{D_3} attempt to attack this protocol, it can not achieve the consistency session key to U_{D_1} and U_{D_2} ,because U_{D_3} does not have the private key x_1 of U_{D_1} , and he can not compute $P_{u_1}' = g_1^{k_2}$ when $U_{D_2} \to U_{D_1} : (P_{u_2}, f_1)$. Obviously he also can not compute $P_{u_2}' = g_2^{k_1}$. U_{D_3} and U_{D_1} or U_{D_3} and U_{D_2} can not achieve the consistent session key $P_{D_1 D_2} = e(P_{u_1}', P_{u_2}') = e(g_1, g_2)^{k_1 k_2}$ at last.

5.4.2 unforgeability

Any member or DAC' that is out of the alliance-domain can not fake the DAC 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 DAC' that is out of the alliance-domain can fake the public key P_{D_1} of DAC_1 in domain D_1 .He has not the corresponding private key of DAC_1 ,and the verification $e(P_{D_1}, reg_{u_1}) = e(P_{u_1}, g_1)$ will be fail. If a number U_{D_3} fake the number U_{D_1} to achieve cross-domain access resource, the signature of U_{D_3} will be fail.

2) Assume that the member DAC_1 in the domain D_1 fakes the number U_{D_1} to access the resource of member U_{D_2} within another domain D_2 , because the private key x_1 of U_{D_1} is not published, even if the DAC_1 of domain D_1 can fake the identity of member U_{D_1} with identity U_{D_1}' to send $dpk = (g_1, P_{u_i}, reg_i, P_{D_1}, H)$ to U_{D_2} , and this can only prove that U_{D_1}' is a member in the domain D_1 , but U_{D_1}' do not know the private key x_1 of U_{D_1} , therefore the verification signature of U_{D_1}' will be fail.

5.4.3 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.

5.4.4 Comparative analysis

Compared with the existing cross-domain authentication, our advantages are as follows:

(1) authentication protocol in communication and computation is smaller than SAP scheme,and the efficiency of the certification is higher than SAP scheme .

(2) our scheme greatly simplifies the system architecture compare with the traditional PKI-based authentication framework, and saves system cost.

(3) Compare with the literature [19] in the certification framework, this paper proposed protocol can provide mutual authentication in different trust domains ,and the application is broader, more in line with the actual needs of a distributed network environment.

(4) This paper proposed authentication protocol has forward security, and in the literature [19] the non-interactive authentication session key is static, if an attacker controls a user's private key, he can calculate the session key that between this user and any entity , it does not have forward security.

5.5 consumption analysis.

computation and communication complexity are two important indicators for evaluating the performance of protocols. We analyzed the latest research ,and we also compared the Cross-domain authentication protocol proposed in this paper with the latest research programs in computation complexity and communication overhead . We compared our scheme with the literature [20] [21] in computational complexity, as shown in Table1. These several programs are elliptic curve public key cryptosystem. It is known that 1024-bit keys in conventional cryptosystems offer the same level of security as 160-bit keys in elliptic curve cryptography. In particular, in the case of elliptic curves, we can assume that the exchanged messages have size only 160 bits, since only the x coordinate is necessary for the computation of the point (x, y). We assume that the length of each communication unit is ml = 160 bits in these programs.

Table1 *Complexity analysis of cross-domain authenticated protocols*

authenticated protocols	Number of exponentiations	Number of pairings	Number of scalar multiplications	Number of hash	Number of sent And received messages
literature [31]	0	12	11	8	32ml
literature [33]	0	0	23	10	23ml
Ours scheme	3	2	3	1	6ml

For more intuitive analysis of the energy consumption in each scheme, the literature [22] provided a experiment that on a 133MHZ "Strong ARM" of microprocessor to perform a modular exponentiation arithmetic need to consume 9.1 mJ, to pure scalar multiplications need to consume 8.8 mJ. To perform a Tate Pairing computation need to consumes 47.0 mJ. It use a 100kbps transceiver module to transmit a bit of information need to consume 10.8 μJ and receive a bit of information need to consume 7.51 μJ. as shown in Table 2. We assume that the energy consumption of hash calculation is negligible. The total energy consumption comparison of these three programs is shown in Figure 1.

Table 2 *Energy Costs for Computation and Communication*

Computation cost of Modular Exponentiation	9.1 mJ
Computation cost of Scalar Multiplication	8.8 mJ
Computation cost of Tate Pairing	47.0 mJ
Communication cost for transmitting a bit	10.8 mJ
Communication cost for receiving a bit	7.51 mJ
DSA Signature	9.1 mJ
ECDSA Signature	8.8 mJ
DSA signature verification	11.1 mJ
ECDSA signature verification	10.9 mJ

The energy consumption is shown in figure 1,the scheme of literature[20] is the most in energy consumption, and ours is the minimum in energy consumption .the advantage of ours scheme is that any two entities can mutual authenticate and do key agreement directly, so it needn't the third-party to take part in. The cross-domain authentication scheme in literature [20] and literature[21] when an entity want to access resources from another entity in different domain it must be checked by the third-party, so it is very complex.

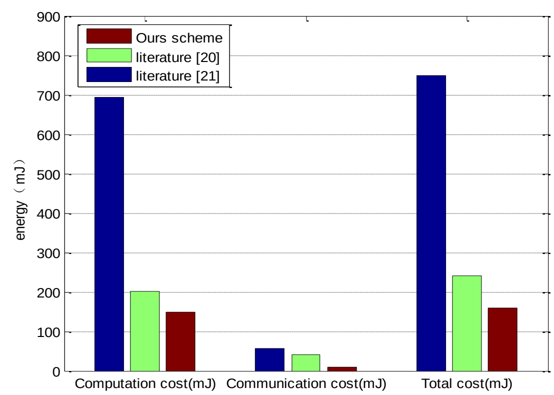

Fig.1 *energy consumption*

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. The computation and communication overhead is relatively low. It has a good security.

6. 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.

Acknowledgements

This work is supported by National Natural Science Foundation of China under Grant No. 61272511 and Innovation Group Project of Beijing Institute of Technology.

References

[1] Randy Butler, Von Welch, Douglas Engert, Ian Foster, Steven Tuecke, John Volmer, Carl Kesselman, A National-Scale Authentication Infrastructure [J].IEEE Computer, 2000, 33(12):60-66.

[2] Zhang Qikun, Li Yuanzhang, Song Danjie,Tan Yuan. Alliance-Authentication Protocol in Clouds Computing Environment. China Communications,2012,7,pp:42-54.

[3] Qikun Zhang,Yuan Tan, Li Zhang, and Ruifang Wang. A Combined Key Management Scheme inWireless Sensor Networks, SENSOR LETTERS,2011,9(4):1501-1506

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

[5] Lv Chao, Li Hui, Ma Jianfeng, Niu Ben. Vulnerability Analysis of Elliptic Curve-Based RFID Protocol[J]. China Communications 2011 Vol. 8 (4): 153-158

[6] Jie Tang, Shaoshan Liu, Zhimin Gu, Chen Liu, Jean-Luc Gaudiot. Prefetching in Mobile Embedded System Can be Energy Efficient[J]. IEEE Computer Architecture Letters, Volume 10, Issue 1 (2011), Page 8-11

[7] Peng Huaxi. An identity-based authentication model for multi-momain[J]. Chinese Journal of Computers, 2006,29(8):1271-1281.

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

[9] 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.

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

[11] Lu Xiaoming, Feng Dengguo. An identity-ba sed authentication model formulti-doma in grids[J]. Chinese Journal of Electronics 2006,34(4):577-582.) (in Chinese).

[12] Zhu Wen, He Mingxing. On automorphism group of finite groups[J].Journal of UEST of China, 2000,29(5):549-551.

[13] Boneh D. and Franklin M.. Identity based encryption from the Weil pairing [J]. SIAM Journal on Computing. 2003, 32(3): 586-615.

[14] 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. 2008, Volume: 3, pp: 165 – 169.

[15] Lu Xiaoming, Feng Dengguo. An identity-based authentication model for multi-domain grids [J]. Chinese Journal of Electronics 2006,34(4):577-582.).

[16] Zhu Wen, He Mingxing. On automorphism group of finite groups[J].Journal of UEST of China, 2000,29(5):549-551) (in Chinese).

[17] David Mandell Freeman, Converting Pairing-Based Cryptosystems from Composite-Order Groups to Prime-Order Groups, Springer Berlin / Heidelberg, 2010(6110):44-61.

[18] J. Cha and J. Cheon. An Identity-Based Signature from Gap Diffie-Hellman Groups. PKC 2003, LNCS 2567, Springer-Verlag, pp. 18–30,2003.

[19] I Foster, C Kesselman, G Tsudik, S Tuecke .A security architecture for computational GRID[A], In Proceedings of the 5th ACM Conference on Computer and Communications Security[C] .New York: ACM press, 1998,83 - 92.

[20] Lu Xiaoming, Feng Dengguo. An identity-ba sed authentication model formulti-doma in grids[J]. Chinese Journal of Electronics 2006,34(4):577-582..

[21] I Foster, C Kesselman, G Tsudik, S Tuecke .A security architecture for computational GRID[A], In Proceedings of the 5th ACM Conference on Computer and Communications Security[C] .New York: ACM press, 1998,83 - 92.

[22] Eleftheria Makri, Elisavet Konstantinou. Constant round group key agreement protocols: A comparative study[J] .computers and security ,2011, 30:643-678.