International Journal of Security and Its Applications
Vol.9, No.12 (2015), pp.211-220
http://dx.doi.org/10.14257/ijsia.2015.9.12.19

Inter-domain Alliance Authentication Protocol Based on Blind Signature

Zhang Jie[1], Zhang Qi-kun[1], Gan Yong[1], Yin Yifeng[1] and Tan Yu-an[2]

[1]*Institute of Computer and Communication Engineering, Zhengzhou University of Light Industry, 450002 Zhengzhou, China*
[2]*School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China*
zhangqikun04@163.com

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 secure cross domains to access resources among these computers in different domains, this paper proposes a multi-domain union authentication protocol. The protocol adopts blind signature to achieve mutual authentication among entities in different domains. This scheme overcomes the complexity of certificate transmission and the network bottlenecks in the scheme of PKI-based. It can trace the entity identity and supports two-way entities anonymous authentication, which avoid the authority counterfeiting its member to access other domain's resources. Analysis shows that its advantages on security and communication-consumption.

Keywords: *Inter-domain authentication; blind signature; bilinear group*

1. Introduction

Multi-domain alliance authentication 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 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 multi-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

ISSN: 1738-9976 IJSIA

traditional [7-9], 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[10-12] 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 [16] extends the scheme of reference [15], 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 multi-domain authentication alliance protocol proposed in this paper is designed based on inter-domain signature, 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. multi-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 2, we introduce the relative knowledge of this paper. In Section3, we define the system model. In Section4, we propose the multi-domain signature scheme. Then, we present multi-domain authentication protocol based on multi-domain signature in Section 5. We provide security analysis, and further analyze the experiment results and performance in Section6. Finally, we conclude the paper in Section 7.

2. Preliminaries

2.1 Bilinear Group

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 , $p \geq 2^k + 1, k$ 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 ,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 $e(u, v) \neq 1$.

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 $e(\varphi(u), v) = e(u, \varphi(v))$.

2.2. Gap Diffie-Hellman group

We first introduce the following problems in G_1 and G_2 [17].

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

Definition 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 $g_1^{\ ab}$.

Definition 3. Bilinear Inverse Diffe-Hellman Problem (BIDHP):The BIDH problem is given g_1, ag_1 and cg_1 for some $a, c \in Z_p^*$ to comput $e(g_1, g_1)^{\frac{1}{a}c}$.

Definition 4. Modified Bilinear Inverse Diffe-Hellman Problem (MBIDHP): The BIDH problem is given g_1, ag_1, bg_1 and cg_1 for some $a, b, c \in Z_p^*$ to compute $e(g_1, g_1)^{\frac{1}{a+b}c}$.

2.3. Multi-Linear Mapping

Multi-linear Diffie-hellman hypothesis: Firstly given the definition of multi-linear mapping [2]. Suppose that the discrete logarithm problem of G_1 and G_2 is hard.

Definition 5: Let G_1, G_T be two groups of the same prime order p. The mapping $e_1: G_1^m \to G_T$ is called m multi-linear mapping, if it satisfies the following properties:

1 multi-linearity: For any of $a_1, a_2, ...a_m \in Z_p^*$ and any of $g_1, g_2, ...g_m \in G_1$, there is $e_1(a_1 g_1, a_2 g_2, ...a_m g_m) = e_1(g_1, g_2, ...g_m)^{a_1 a_2 ... a_m}$.

2 Non-degeneracy: If $g \in G_1$ is a generator of G_1, then $e_1(g, g, ...g)$ is also a generator of G_T.

3 Computability: For all $u_1, u_2, ..., u_m \in G_1$, there exits a efficient way to calculate $e(u_1, u_2, ..., u_m)$.

Definition 6: Decisional multi-linear Diffie-Hellman(DMDH) problem is that given $g, a_1 g, a_2 g, ...a_{m+1} g \in G_1$ and $\forall z \in G_T$, it is to determine if there is $z = e_1(g, g, ...g)^{a_1 a_2 ... a_{m+1}}$.

Definition 7: Hypothesis of decisional multi-linear diffie-hellman is that solving decisional multi-linear diffie-hellman problem is difficult. That is to say that there cannot be a probability polynomial time algorithm which can solve Diffie-Hellman problem.

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 , DLP or BIDHP with non-negligible advantage within polynomial time.

3. The Multi-Domain Authentication Model

In multi-domain authentication system, the type of authentication is chosen for each domain by them demands, without need a unified authentication model. And inter-domain authentication should try to adopt a common authentication way to achieve multi-domain access interoperability. This multi-domain authentication system model is designed in Figure 1.

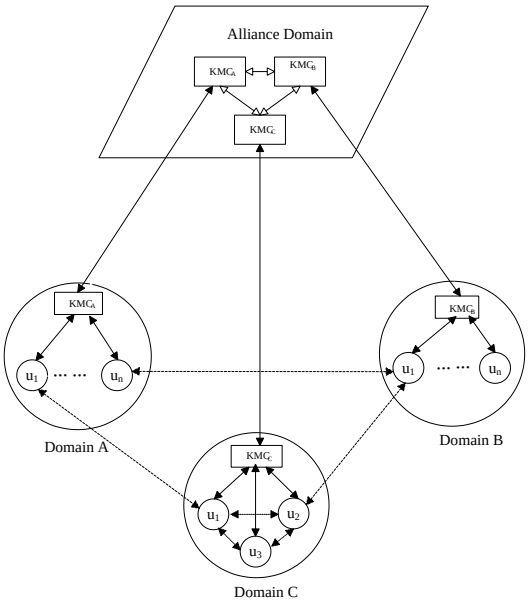

Figure 1. Multi-Domain Authentication System Model

In this model, the system is composed by multiple domains, each domain is independent and autonomous. Each domain consists of a KMC (key management 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 these members in each domain may need to cross-domain cooperation. KMC distributes and manages some keys of their members within its domain, and open the public key of KMC 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. Multi-Domain Blind Signature Scheme

Suppose G_1 and G_2 are multiplicative groups with the same prime order p . g_1 is a generator of G_1 . $e: G_1 \times G_1 \to G_2$ is an efficiently computable bilinear mapping, $e_1 : G_1^n \to G_T$ is an efficiently computable multi-linear mapping $h_0 : G_T \to Z_p^*$ and $h_1 : \{0,1\}^* \to Z_p^*$ are hash function.

4.1. Alliance Domain Key Agreement

Suppose there have n domains in the alliance system, all the $KMC_i\ (1 \le i \le n)$ in each domain negotiate a pair of alliance public/private keys.

Firstly, each $KMC_i\ (1 \le i \le n)$ selects a numbers $\lambda_i \in Z_p^*$ randomly and calculates $\gamma_i = \lambda_i g_1$, then broadcasts γ_i to other $KMC_j (1 \le j \le n, i \ne j)$. According to multi-linear mapping, each KMC_i can computes a pair of alliance public/private keys. The processes are as the follows:

Each KMC_i calculates the alliance private sa with the parameters λ_i and $\gamma_j = \lambda_j g_1\ (1 \le j \le n, i \ne j)$ that sends by other numbers KMC_j.

4.2. Blind Signature

Suppose KMC_i is the key management center of domain D_i ,and the private key of KMC_i is s_i, and the public key is $P_i = g_1^{s_i}$,where $s_i \in Z_p^*$ .All the KMC_i in the alliance network system negotiated alliance public/private key pair is(sa , Pa). Suppose each member u_i 's private key is $x_i \in Z_p^*$ in the domain D_i and the corresponding public key is $y_i = g_1^{x_i}$, ID_i is the identity of u_i. The blind signature is as follows:

(1) Each KMC_i selects a numbers $t_i \in Z_p^*$ randomly, and computes $\eta = g_1^{t_i \cdot s_i / sa}$ and then sent η to all the members in its domain.

(2) Each member u_j of the domain received the η, and calculates the value $\delta_j = \eta^{x_i}$, and then sent (δ_j, ID_i) to its KMC_i.

(3) The KMC_i received each member u_j sent messages (δ_j, ID_i) ,and calculates the value $R_j = \delta_j^{-t_i}$, then verifies the whether value and $e(R_j, pa) \stackrel{?}{=} e(y_j, P_i)$ is equation, If it is correct, KMC_i can ensure that δ_j is sent by u_j, and y_j is unique within that domain , then KMC_i can register with R_j as register key. KAC_i store (R_j, y_j, ID_i) for tracking.

(4) KMC_i sends R_j to u_j as the register key. All members of each domain register in this way.

5. Multi-Domain Authentication Protocol based on Blind Signature

In the multiple domains networks, to ensure secure access resource cross different domains, members from different domains need to be authenticated each other.

In this section, purposed a multi-domain alliance authentication protocol based on short signature, which enables direct authentication between members and does not need the ticket transfer through the authentication center. Let D_1 and D_2 be two domains in the alliance-domain respectively, the KMC_1 and KMC_2 are key management centers of D_1 and D_2 respectively. The public/private key pair of KMC_1 is (s_1, P_1), and public/private key pair of is (s_2, P_2) , and the public/private key pair of alliance-domain that all the $KMC_i (1 \le i \le n)$ negotiated is (sa, Pa). Suppose u_i, v_j are internal members of D_1 and D_2 respectively. x_i is the private key of u_i ,and R_i is the register key of u_i ,and

$y_i = g_1^{x_i}$ is the public key of u_i. x_j is the private key of v_j ,and R_j is the register key of v_j ,and $y_j = g_1^{x_j}$ is the public key of v_j. When u_i want to access resource from v_j, the process of multi-domain authentication and session key agreement are described as follows:

(1) u_i in domain D_1 calculates $sign_i = y_j^{x_i}$ and sends the public information $(sign_i, P_i, R_i, y_i)$ to verifier v_j.

(2) after receiving the messages $(sign_i, P_i, R_i, y_i)$, v_j with its private key x_j to calculates $ver_j = (sign_i)^{-x_j}$,and verifies whether $ver_j = y_i$,then verifies P_i is a public key of KAC_i in the alliance-domain and whether y_i is a public key of a member that belongs to domain D_1 by whether the expressions $e(R_i, pa) \stackrel{?}{=} e(y_i, P_i)$ is satisfaction.

(3) If $ver_j = (sign_i)^{-x_j}$ and $e(R_i, pa) = e(y_i, P_i)$, v_j can ensure $(sign_i, P_i, R_i, y_i)$ are sent by u_i ,and u_i is a member in the domain D_1, then v_j calculates $sign_j = y_i^{x_j}$ and sends the public information $(sign_j, P_j, R_j, y_j)$ to verifier u_i.

(4) after receiving the messages $(sign_j, P_j, R_j, y_j)$, u_i with its private key x_i to calculates $ver_i = (sign_j)^{-x_i}$,and verifies whether $ver_i = y_j$,then u_i verifies whether P_j is a public key of KAC_j in the alliance-domain and whether y_j is a public key of a member that belongs to domain D_2 by whether the expressions $e(R_j, Pa) \stackrel{?}{=} e(y_j, P_j)$ is satisfaction.

If $ver_i = (sign_j)^{-x_i}$ and $e(R_j, Pa) = e(y_j, P_j)$, u_i can ensure $(sign_j, P_j, R_j, y_j)$ are sent by v_j ,and v_j is a member in the domain D_2 .The cross authentication in the multi-domain system are successful.

6. Performance Analysis

6.1. Correctness Analysis.

In this paper, the multi-domain alliance authentication protocol is established based on blind 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:

Theory 1: Each legal member u_i with a legal register key R_i in the domain D_i can be authenticated successfully.

Proof: since $g_1^{x_i \cdot s_i / sa}$, and the properties of the bilinear pairings, we have

$$\begin{aligned} & e(R_i, Pa) \\ & = e(g_1^{x_i \cdot s_i / sa}, Pa)) \\ & = e(g_1^{x_i \cdot s_i / sa}, g_1^{sa)}) \\ & = e(g_1, g_1)^{x_i s_i} \\ & = e(g_1^{x_i}, g_1^{s_i}) \\ & = e(y_i, P_i) \end{aligned}$$

Since $sign_i = y_j^{x_i}$, we have

$$ver_j = (sign_i)^{-x_j} = (y_j^{x_i})^{-x_j}$$
$$= (y_j^{-x_j})^{x_i} = (g_1^{x_j - x_j})^{x_i} = y_i$$

Thus, the equation $e(R_i, Pa) = e(y_i, P_i)$ and $ver_j = y_i$.

6.2. Security Analysis

(1) Unforgeability. Any member u' that is out of the alliance-domain or in the alliance-domain can not fake any other member u_i to achieve resource access.

Theory 2: any members u_k that in the domains D_i cannot forge other member $u_i (i \neq k)$ to access resource.

Proof:

Assume that any member u_k in the domain D_i fakes another member u_i to access the resource from the member v_j within another domain D_j . Because the private key x_i of u_i is not published, even if u_k can fake the identity of member u_i with identity u_i' to send $(sign_i', P_i, R_i, y_i)$ to v_j .After receiving the messages, v_j verifies $e(R_i, pa) = e(y_i, P_i)$ and this can only prove that u_i' is a member in the domain D_i , but u_k do not know the private key x_i of u_i , therefore the verification signature of u_i' will be fail when v_j verifies $ver_j = y_i$.

Therefore, members u_k that in the domains D_i cannot forge other member $u_i (i \neq k)$ to access resource

(2) Anonymity. Proposed protocol has the anonymity. When two members access resources, any member can only determine another member is a sole member in a certain domain, but the identity of the member can not be determined.

Theory3: When there two members u_i and v_j access resources mutually, v_j can only determine that u_i is a sole member of a certain domain D_i , but the identity ID_i of the member u_i cannot be determined, and only his KMC_i can determine the identity ID_i of the member u_i through registered identity.

Proof:

1) User u_i sends public information $(sign_i, P_i, R_i, y_i)$ to v_j , and v_j determines u_i from which domain by verifying the equation $e(R_i, pa) = e(y_i, P_i)$, and u_i in the domain that with the public key P_i , and u_i in this domain with the public key y_i .

2) v_j can only determine u_i is a sole member in the domain with the public key y_i , and it can not be faked by others through verification whether $e(R_i, pa) = e(y_i, P_i)$ and $ver_j = y_i$,but does not know the identity ID_i of the member u_i .

6.3. Traceability

The traditional method to design a cross multiple domains authentication protocol based on trust scheme, it is impractical to let members to trust the KMC_i that is from different domains. This paper provides a reliable certification to trace illegal entity when

the disputes are occurred. The traceability is according to the verifier v_j to verify the expression $e(R_i, pa) = e(y_i, P_i)$,and ensure the relationship among $sign_i, P_i, R_i$ and y_i, then sends the messages $(sign_i, P_i, R_i, y_i)$ to KMC_i, KMC_i further to trace the identity of entity u_i by the registration information (R_i, y_i, ID_i) in KMC_i.

7. Consumption Analyses

Computation and communication complexity are two important indicators for evaluating the performance of protocols. The paper analyzed the latest research, and also compared the multi-domain authentication protocol proposed in this paper with the latest research programs in terms of computation complexity and communication overhead. We compared our scheme with the literature [18-19] 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.

Table 1. 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 [18]	0	12	11	8	32ml
literature [19]	0	0	23	10	23ml
Ours scheme	1	2	0	0	6ml

For more intuitive analysis of the energy consumption in each scheme, the literature [20] 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 consume 47.0 mJ. It uses 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 7.51μJ. 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[18] 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 [18] and literature [19] when an entity wants to access resources from another entity in different domain it must be checked by the third-party, so it is very complex.

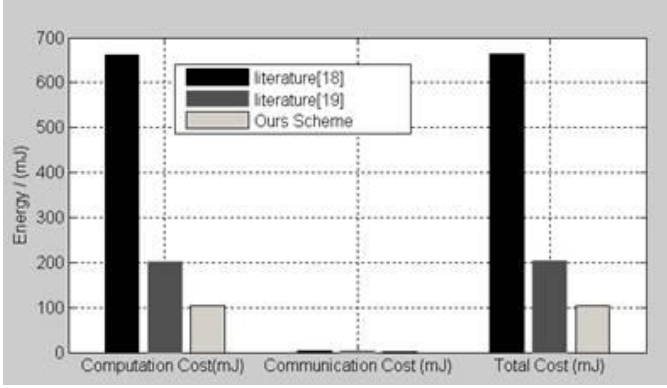

Figure 1. Energy Consumption

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.

8. Conclusion

Multi-domain alliance authentication is required for security in multi-domain network environment. The scheme of multi-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 different domains resources needless the intervention of the key management center, which provides good flexibility. It can avoid the bottleneck problem and the complexity of the transfer tickets of the traditional pattern based on PKI, and it can trace the entities and supports two-way entities anonymous authentication, which avoid the domain certificate authority counterfeiting its member to access cross-domain resources. Analyses show that its advantages on security and communication-consumption.

Acknowledgements

This work is supported by National Natural Science Foundation of China under Grant No. (61272511 and 61340059), the PhD Research Fund of the Zhengzhou University of Light Industry , the Science and Technology Plan of Zhengzhou(No. 131PPTGG411-5), the Science and Technique Research Program of Henan Educational Committee (No. 15A520032 and 14A520022) and National High-tech R&D Program of China (863 Program) (Grant No. 2013AA01A212) Vol.30,

References

[1] R. Butler, V. Welch, D. Engert, I. Foster, S. Tuecke, J. Volmer, C. Kesselman, A National-Scale Authentication Infrastructure [J].IEEE Computer**(2000),** Vol 33，No. 12,pp.60-66.
[2] Z. Qikun, L.Yuanzhang, S. Danjie,T. Yuan. Alliance-Authentication Protocol in Clouds Computing Environment. China Communications**(2012)**, No.7,pp.42-54.
[3] Q. Zhang,Y. Tan, L. Zhang, and R. Wang. A Combined Key Management Scheme inWireless Sensor Networks, SENSOR LETTERS**(2011)**, Vol 9, No.4,pp.1501-1506
[4] J-S Lee, C-C Chang, P-Y Chang, Chin-Chen Chang. Anonymous authentication scheme for wireless communications. International Journal of Mobile Communications **(2007)**, pp.590-601.
[5] Lv Chao, L. Hui, M. Jianfeng, N. Ben. Vulnerability Analysis of Elliptic Curve-Based RFID Protocol[J]. China Communications**(2011)**, Vol 8, No.4, pp. 153-158
[6] J. Tang, S. Liu, Z. Gu, C. Liu, J-L Gaudiot. Prefetching in Mobile Embedded System Can be Energy Efficient[J]. IEEE Computer Architecture Letters **(2011)**, Vol 10, No.1,pp. 8-11.
[7] P Huaxi. An identity-based authentication model for multi-momain[J]. Chinese Journal of Computers**(2006)**, Vol 29, No.8, pp.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)**, pp.260-275.
[9] N. 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] L. Xiaoming, Feng Dengguo. An identity-ba sed authentication model formulti-doma in grids[J]. Chinese Journal of Electronics**(2006)**, Vol 34, No.4, pp.577-582.
[12] Z. Longjun, Xia, Ang. Cross-domain authentication protocol based on certificate signcryption in Ipv6 Network[J], International Journal of Advancements in Computing Technology**(2012)**, Vol 4, No.21,pp.34-41.
[13] Boneh D. and Franklin M.. Identity based encryption from the Weil pairing [J]. SIAM Journal on Computing**(2003)**, Vol 32, No.3,pp.586-615.
[14] W. Zhang, H. Zhang,B. Zhang ,Yan Yang .An Identity-Based Authentication Model for Multi-domain in Grid Environment[C]. Computer Science and Software Engineering**(2008)**, No. 3, pp.165-169.
[15] L. Xiaoming, F. Dengguo. An identity-based authentication model for multi-domain grids [J]. Chinese Journal of Electronics**(2006)**, Vol 34, No.4,pp. 577-582.
[16] C., Liqun; L. Hoon Wei; Y. Guomin. Cross-domain password-based authenticated key exchange revisited[J], ACM Transactions on Information and System Security**(2014)**, Vol 16,4,pp.12-20.
[17] Q-k Zhang, Y-A Tan, Y-Z Li, X-La Zhang. Cross-domain Alliance Authentication Scheme Based on Bilinear Group. Applied Mathematics & Information Sciences**(2014)**, Vol 8, No.3,pp.1313-1317.
[18] L. Xiaoming, F. Dengguo. An identity-ba sed authentication model formulti-doma in grids[J]. Chinese Journal of Electronics**(2006)**, Vol 34, No. 4, pp.577-582.
[19] H. Shen-Gang; Z. Li; Muhammad, Ghulam. A union authentication protocol of cross-domain based on bilinear pairing [J]. Journal of Software**(2013)**, Vol 8, No. 5, pp. 1094-1100.
[20] E. Makri, E. Konstantinou. Constant round group key agreement protocols: A comparative study[J] .computers and security**(2011)** , No.30, pp. 643-678.

Authors

Zhang Jie, associate professor Ph.D. Zhengzhou University of Light Industry, Zhengzhou. China. His research interests include information security and cryptography

Zhang Qikun, Ph.D. Zhengzhou University of Light Industry, Zhengzhou. China. His research interests include information security and cryptography.

