Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080347

A Cross-Domain Alliance Authentication Scheme based on Bilinear Group

Qikun Zhang[1,*], *Ruifang Wang*[2], *Yong Gan*[1] *and Yifeng Yin*[1]

[1] Institute of Computer and Communication Engineering, Zhengzhou University of Light Industry, 450002 Zhengzhou, China
[2] library, Zhengzhou University of Light Industry, 450002 Zhengzhou, China

Received: 18 Jun. 2013, Revised: 23 Oct. 2013, Accepted: 24 Oct. 2013
Published online: 1 May. 2014

Abstract: With the development of grid computing, cloud computing and other large distributed network technology, users need them to provide services of unlimited space and unlimited speed. In order to meeting this request of users, all the domains in these large distributed networks need coordination for each other. For ensuring the safety to access resources in all 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 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 domain certificate authority counterfeiting its member to access cross-domain resources. Analyses show that its advantages on security and communication-consumption.

Keywords: Inter-domain signcryption, Union certification, Elliptic curve, Bilinear group underwater communications

1 Introduction

Cross-domain authentication exist in many fields, such as the authentication among multiple heterogeneous domains within a virtual organization in the grid environment [1], the roaming access authentication in the environment of wireless network, etc. there are mainly two cross-domain authentication frameworks in specific environments: one is authentication framework (such as Kerberos)[2] based on the symmetric key system. The other is authentication framework based on traditional [3, 4, 5], The management of credentials in 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 . References [6, 7, 8] 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 [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, so it is difficult to meet the needs of large-scale distributed computing. Reference [11] extends the scheme of reference [9], 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. The cross-domain authentication alliance protocol proposed in this paper, which designs based on inter-domain signcryption. Each inter-domain authentication centers do not have to set the same parameters for their keys in the system, 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.

* Corresponding author e-mail: zhangqikun04@163.com

2 Preliminaries

2.1 Self-isomorphic Group of Finite Group

Let G be a group, $AutG$ represents self-isomorphic group of G, $C(G)$ is the center of G, $< g >$ 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 *sylowp*-subgroup of G.

Theorem 1[12]. let G be a finite *Abel* group, $p_1, p_2, \ldots, p_n$ are all prime factors of $|G|$, $G_{p_i} (1 \leq i \leq n)$ are the *sylowp*-subgroups of G, which gives direct product decomposition: $G = G_{p_1} \times G_{p_2} \times \cdots \times G_{p_i}$.

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

2.2 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 $G_1 =< g_1 >$ be generated by g_1 and $G_2 =< g2 >$ 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 [13]:

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 $u \in G_1$, $v \in G_2$.

3 Cross-domain Alliance Authentication Scheme Between Domains

In multi-domain alliance 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 [14].

3.1 System Initialization

Let the alliance domain contain R domains, and selects R pairwise relatively prime large prime numbers to form a set of $R_s = r_i | (i = 1, 2, \ldots, R)$; 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 ($q = r_1 \times r_2 \times \cdots \times r_i$), that $|G| = q$. Let $r_1, r_2, \ldots\ldots, r_n$ be all the prime factors of $|G|$, that $q = r_1 \times r_2 \times \cdots \times r_n$. Let $G_{r_j} (1 \leq j \leq n)$ be $sylow_{r_j}$-subgroups of G. From Theorem 1, we know the direct product decomposition of G: $G = G_{r_1} \times G_{r_2} \times \cdots \times G_{r_i}$, and we can construct R sub-groups of G that are isomorphism to each other according to the Theorem 2, let this set of *sub*-groups be $Gset = G_k | (1 \leq k \leq R)$. In the multi-domain unite architecture, each domain select a different sub-group $G_k (1 \leq k \leq R)$ from set G as the key generator parameter of the domain.

3.2 Inter-domain Authentication

1) Let D_1 and D_2 be two domains of alliance-domain , and D_1 selects cyclic group $G_1 =< g_1 >$ as the key generation parameter of its domain, D_2 selects cyclic group $G_2 =< g_2 >$ 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 $y = g_1^{\frac{1}{\xi}}$ 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 its registered key is reg_{u_1}. The private/public key pair of U_{D_2} is (x_2, P_{u_2}), and its registration key is reg_{u_2}. The public key of DAC_1 in domain D_1 is P_{D_1}, and The public key of DAC_2 in domain 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 $s_1 \leftarrow \mu + cx_1$, $UD_1 \xrightarrow{s_1} U_{D_2}$;

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.

3.3 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; U_{D_1} and U_{D_2} compute their temporary session key $P_{D_1D_2} = e(P_{u_1^{'}, P_{u_2}^{'}}) = e(g_1, g_2)^{k_1 k_2}$.

4 Performance Analysis

4.1 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.

$$\begin{aligned} e(P_{D_1}, reg_{u_1}) &= e(g_1^{\xi_1}, g_1^{\frac{x_1}{\xi_1}}) \\ &= e(g_1, g_1)^{x_1} \\ &= e(g_1^{x_1}, g_1) \\ &= e(P_{u_1}, g_1) \end{aligned} \tag{1}$$

$$g_1^{s_1} = g_1^{(\mu + cx_1)} = g_1^{\mu} g_1^{cx_1} = T_1 P_{u_1}^c \tag{2}$$

4.2 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}.

4.3 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.

4.4 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:

1) Against *MITM*

Assume that mediator U_{D_3} attempt to attack this protocol, it cannot 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 cannot compute $P_{u_1}^{'} = g_1^{k_2}$ when $U_{D_2} \rightarrow U_{D_1} : (P_{u_2}, f_1)$. Obviously he also cannot compute $P_{u_2}^{'} = g_2^{k_1}$. U_{D_3} and U_{D_1} or U_{D_3} and U_{D_2} cannot achieve the consistent session key $P_{D_1D_2} = e(P_{u_1}^{'}, P_{u_2}^{'}) = e(g_1, g_2)^{k_1 k_2}$ at last.

2) Unforgeability

Any member or $DAC^{'}$ that is out of the alliance-domain cannot fake the *DAC* that is in the alliance-domain, and any member within a domain cannot 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 $dpt = (g_1, P_{u_i}, reg_i, P_{D_1}, H)$ 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.

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.

4.5 Consumption Analysis

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

Table 1: Computation Consumptions of The Protocol

Times of computation of key agreement	Times of computation of authentication protocols	Type of computation
1	2	Bilinear pairing
4	2	Multiplication
0	3	Exponentiation
0	1	Hash
0	0	Addition

protocol needs 2 bilinear pairing, 2 multiplications, 3 exponentiation computation, 1 hash and 1 addition for the process of the signature verification and it needs 4multiplications, 1 bilinear pairing for the process of the session key consultation. The communication: 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.

5 Conclusion

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.

Acknowledgement

Research supported by the National Natural Science Foundation of China under Grant No.61272511 and 61272038.

The authors are grateful to the anonymous referee for a careful checking of the details and for helpful comments that improved this paper.

References

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

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

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

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

[5] Noel McCullagh, Paulo S. L. M. Barreto. A new two-party identity-based authenticated key agreement. http://eprint.iacr.org/2004/122.pdf

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

[7] Lu Xiaoming, Feng Dengguo. An identity-based authentication model formulti-doma in grids. Chinese Journal of Electronics, **34**, 577-582 (2006).

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

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

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

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

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

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

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

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

Yong Gan Ph.D. Professor, School of Computer and Communication Engineering, Zhengzhou University of Light Industry. His research interests include multimedia communications, image processing, coding and network engineering.

Ruifang Wang born in 1982 . Zhengzhou University of Light Industry, Zhengzhou, China. Her research interests include information security and cryptography.

Yifeng Yin Vice Professor, PhD. School of Computer and Communication Engineering, Zhengzhou University of Light Industry. His research interests include information security and cryptography.