Heterogeneous Cross-Domain Identity Authentication Scheme Based on Signcryption Algorithm

Chen Yang, Wenju Liu, Ze Wang

Abstract—**This paper designs a heterogeneous cross-domain identity authentication model based on the signcryption algorithm. User U and cloud service provider CSP register their identities in their respective trust domains and generate real identities through a hierarchical ID tree structure, and obtain the system according to random parameters in the domain. After the key, a temporary identity is generated by binding the real identity and the timestamp to achieve anonymity during trust transmission; in the first cross-domain authentication stage, the signcryption algorithm is used to further strengthen the security of the real identity and simplify the calculation of cross-domain authentication. In the process, a third-party cloud authentication center CAI is introduced to complete the mutual authentication of identity information between user U and cloud service provider CSP in different trust domains. User U and cloud service provider CSP directly accept the identity authentication results of the third-party cloud authentication center CAI, reducing The computational overhead of user U is reduced; while the signcryption algorithm is used to simplify the calculation process, it can effectively resist other network attack methods such as replay, intermediary and replacement, and achieve a dynamic balance between the security and computational overhead of the cross-domain authentication scheme. The model analysis tool AVISPA simulation experiment and comparative experiment method are compared with the existing cross-domain authentication schemes, showing that the scheme proposed in this paper has excellent security capability and low computational cost.**

Index Terms— **Signcryption;Heterogeneoussystem; Cross-domain authentication;Cloudcomputing.**

Manuscript received April 28, 2022

Chen Yang, School of Computer Science and Technology, Tiangong University,TianJin,China

Wenju Liu, School of Computer Science and Technology, Tiangong University,TianJin,China

Ze Wang, School of Computer Science and Technology, Tiangong University,TianJin,China

I. INTRODUCTION

Due to the many characteristics of cloud computing's own structure, it is convenient for the majority of users to access and share data. But cloud service providers face the danger of being attacked by malicious hackers while providing services to users. In order to ensure efficient data sharing and access for users in various domains, there are various types of cloud servers participating in computing, and their locations are relatively scattered [1]. Due to these characteristics of cloud servers, nodes cannot be effectively controlled, and resource services will face user data security and privacy protection issues in an open World Wide Web environment. The identity authentication technology verifies the identity of the user and the cloud service provider to ensure that the identity is legal when the user accesses data, so the identity authentication scheme based on various public key cryptographic algorithms begins to appear [2]. For the current new idea of completing cross-domain identity authentication through different cryptographic algorithms [3], it is necessary to study the heterogeneous cross-domain identity authentication technology between different cryptographic algorithms to ensure the identity security and verifiability of users and cloud service providers. , establish a trust connection, register and save the identities of legitimate users, facilitate repeated cross-domain authentication, and reduce computational redundancy. Reference [4], a certificateless encryption scheme is proposed based on the standard model, but the model does not consider attacks from malicious KGCs. Reference [5] constructed an anonymous identity authentication based on a certificateless cryptosystem, but it cannot effectively resist man-in-the-middle attacks. Reference [6] constructed a cloud identity authentication based on digital certificates, and adopted multi-factor authentication technology to strengthen remote user authentication in the cloud environment. However, because the certificate needs to be issued and revoked frequently during the verification process, the overall identity authentication model is computationally overloaded. big. Reference [7] proposed a cross-domain identity authentication scheme based on proxy re-signature

algorithm to realize cross-domain identity authentication between heterogeneous cryptosystems. However, the authentication process of this scheme is complex and the user computing overhead is large, resulting in low overall cross-domain efficiency. Reference [8] proposed an authentication key agreement protocol combined with heterogeneous signcryption algorithm, which has better security and efficiency, but does not design a cross-domain authentication model, which cannot meet the information interaction between users and cloud servers. Reference [9] proposes a new cross-domain authentication model using blockchain technology, and designs a cross-domain authentication protocol on top of this model, but the cross-domain authentication protocol can only be authenticated in a homogeneous domain, without Consider access between heterogeneous trust domains. Reference [10] proposes the trust access authentication of the Internet of Vehicles based on the blockchain technology, and realizes network collaborative sharing for vehicles in different trust domains, but does not consider the issues of cross-domain access and identity trust between vehicles. Reference [11] proposes a cross-domain scheme based on blockchain technology in order to achieve multi-domain access, which enables trust domains that have not established a secure connection to establish connections with other trust domains, but this model does not consider the relationship between different domains. inter-trust connections and cross-domain access issues.

Based on Wang [8], this paper proposes a key agreement scheme based on the signcryption algorithm, which takes advantage of the advantage that signcryption can realize both signature and encryption techniques in one algorithm. In the absence of public key certificate verification and key management problems Next, an efficient and secure identity cross-domain authentication scheme is proposed. In order to protect the real identities of users and cloud service providers from being exposed, real identities are generated through a hierarchical ID tree, and random parameters and generators are used to bind the real identities of users and cloud service providers to generate temporary identities. Signcrypting the identity further enhances the security of the identity. By comparing the experimental methods, it is shown that the scheme proposed in this paper has excellent security capabilities. In terms of computing performance, the signcryption algorithm is used in identity cross-domain authentication for the first time. Compared with the existing related identity authentication schemes, since bilinear and exponential operations are not required in the user registration stage, the computing efficiency is greatly improved. This paper is the first to use signcryption algorithm to conduct research in cross-domain identity authentication, and achieve high research results.

Section II of this paper briefly introduces the basic knowledge of the paper design, Section III introduces the cross-domain authentication of heterogeneous systems, Section IV introduces the security performance and technical overhead of this scheme, and compares it with other related literatures. Section V gives draw conclusions

II. Preliminary Knowledge

A. Bilinear Mapping

Let $G1$ and $G2$ be cyclic groups of order d, d is a prime number, and g is a generator of $G1$. Defifine bilinear mapping e: $G1 \times G1 \longrightarrow G2$.

B. Assumptions of the Security Theory

Computational CDH (Computational Diffiffiffie-Hellman) problem: for a given triplet (d, ad, bd) $\in$ G1, for any $a, b \in Z_q^*$ compute $\beta = dab$.

Defifinition 1 (CDH hypothesis): The probability that there exists any probabilistic polynomial-time algorithm M that can solve the CDH problem is $\mathrm{Adv_{BDH}(M)} = \Pr[\mathrm{M(d, ad, bd)} = \mathrm{abd} \in \mathrm{G_1}, \mathrm{a.b} \in \mathrm{Z_q^*}]$, If $\mathrm{Adv_{BDH}(M)}$is negligible, then CDH is said to be a difficult problem.

Computational BDH (Bilinear Diffiffiffie-Hellman) problem: for a given triplet (d, ad, bd,cd) $\in$ G1, for any $a, b, c \in Z_q^*$ compute $\alpha = e(d, d)^{abc}$, $\alpha \in$ G2.

Defifinition 2 (BDH hypothesis): The probability that there exists any probabilistic polynomial-time algorithm M that can solve the BDH problem is $Adv_{BDH}(M) = Pr[M(d, ad, bd, cd) = e(d, d)^{abc} \in G_2, a.b, c \in Z_q^*]$.

C. CK SecurityModel

CK (Canetti-Krawczyk) securitymodel defines two attack models as the AM modelfor authenticated links and the UM model for unau thenticated links. In the ideal model AM, any attackercannot forge, tamper, and replay messages and can only passthe same message once and has the ability to query sessionkey, call operation, compromise protocol participants, expose the session key, and test the session key.

Definition 3. Given that A is any attacker in the AM, if the session key of the authentication protocol is safe in the AM,

the properties below are satisfied.

Property 1. Both parties can obtain the same session key after they are not compromised and execute the agreement successfully.

Property 2. The attacker A makes the test of attacking the session key query, and according to the result, A can correctly determine whether the output value of the session key is a random value or A real value with the probability not exceeding (1/2) + ε (ε represents any value that can be ignored within the security parameter range).

III. Heterogeneous Cross-Domain Authentication Scheme Based on Signcryption Algorithm

A. Heterogeneous cross-domain identity authentication based on Signcryption Algorithm

The environment of the random World Wide Web is

becoming more and more complex. For information encryption in different scenarios, it is most suitable to formulate a special cryptographic system according to the special environment. For the problem that efficient cross-domain authentication cannot be performed between different cryptographic systems with frequent interactions, this section An identity authentication model based on heterogeneous signcryption algorithm composed of 5 entities is proposed.

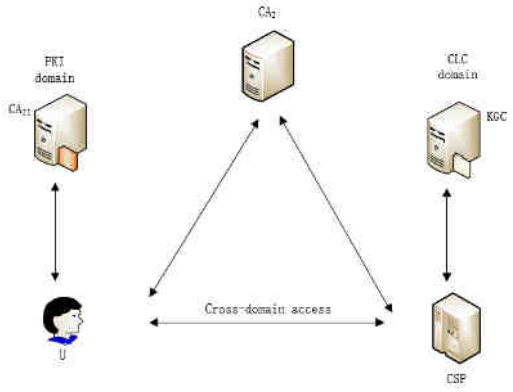
(1) Cloud-to-Cloud Authentication Center CAI: CAI is responsible for the decryption and sign-crypto verification between different security cryptosystems, and is also responsible for the identity authentication between heterogeneous cryptosystems, and generates the authentication result and sends it to the user U and the cloud service provider CSP.

(2) Certification Center CAII: The CAII in the PKI domain is mainly responsible for the generation and issuance of certificates for users in the domain, and registers the real identity of the user, calculates the temporary identity, and signs the temporary identity of the user to obtain the signature parameters.

(3) User U: The user completes the verification of his own identity in the CLCI domain, initiates a cross-domain access request to the foreign cloud service provider after the verification is passed, and uses the signcryption algorithm to encrypt the cross-domain resource access request message to exchange information with the CSP.

(4) Key distribution center KGC: KGC performs temporary identity signatures on CSPs in the CLC domain to complete registration and storage, and completes the generation and distribution of some keys.

(5) Cloud service provider CSP: completes its own identity verification in the CLC domain, and provides cloud resource services for legitimate visitors who have passed the identity verification.



The scheme model is shown in Figure 1:

Figure1： Heterogeneous cross-domain authentication model

B. Scheme Description

This solution is mainly divided into four stages: system initialization, user registration, heterogeneous cross-domain identity authentication, heterogeneous and repeated cross-domain identity authentication, system parameter selection, identity registration of users in the security domain, and ciphertext generation by the signcryption algorithm is completed. Cross-domain authentication of heterogeneous systems and verification of the legitimacy of repeated cross-domain identities. Table 1 describes the meaning of all parameters.

Table 1: Symbol Description

Symbol	Meaning of the symbol
U	User
CSP	cloud service provider
PKI	public key infrastructure
CLC	Certificateless Public Key Infrastructure
KGC	Key generation center in the CLC domain
CA_I	Certification Center
CA_{II}	Certificate Authority in PKI Domain
DM_α	ID of CA_{II}
DM_U	User's identity
DM_β	KGC's identity
DM_{KGC}	Identity of the CSP
ID_U	User's real identity
TID_U	User's temporary identity
s_I	The master key of the cloud authentication center
s_{II}	The master key of the certificate authority in the PKI domain
s_{III}	The master key of the key generation center in the CLC domain
ID_{CSP}	The real identity of the cloud service provider
TID_{CSP}	Temporary identity for cloud service providers
P_{CA_I}	The public key of the cloud authentication center
P_{KGC}	The public key of the key issuing center
P_{CSP}	Cloud service provider's public key

$P_{CA_{II}}$	The public key of the certificate authority in the PKI domain
sk_U	User's private key
pk_U	User's public key
sk_{CSP}	Cloud service provider's private key
pk_{CSP}	Cloud service provider's public key

C. System Initialization

In the system initialization stage, the security parameters R are randomly input. G1 and G2 are an additive and multiplicative cyclic group of order q, and d is a generator of the additive cyclic group G1. According to G1 and G2, the bilinear mapping e:G1 × G2→ G2, and at the same time define three secure hash functions according to the calculations required by this scheme: $H_I: \{0,1\}^* \rightarrow G_I, H_{II}: \{0,1\}^n \rightarrow Z_q^*$, $H_{III}: G_{II} \rightarrow \{0,1\}^n$, the temporary identity of the user is generated by H_I calculation, the signature information of the temporary identity is calculated by H_{II} and the signcryption calculation is performed by H_{III} In order to ensure that the output value of the hash function is any element inZ_q^*, define: Z_q^*={0,1,2.....q-1}, where n<q. The symbol "||" represents the concatenation operation of strings.

(1) CAI selects the parameter $s_I \in Z_q^*$as its own system master key, and generates a system public key$P_{Pub} = s_I d$ according to the system master key calculation, and then discloses the system public parameters obtained by its own calculation. The public parameters are : $pa_I\{G_1, G_2, e, q, d, P_{pub}, H_I, H_{II}, H_{III}\}$.

(2) CAII selects the parameter $s_{II} \in Z_q^*$ as its own system master key, and calculates and generates a system public key $P_{CA_{II}} = s_{II} d$ according to the system master key, and then discloses the system public parameters obtained by its own calculation, The public parameters are: $pa_{II}\{G_1, G_2, e, q, d, P_{CA_I}, H_I, H_{II}, H_{III}\}$.

(3) KGC selects a random parameter $s_{III} \in Z_q^*$as the master key of theKGC_{II} system, and generates a system public key $P_{KGC} = s_{III} d$ according to the system master key, and then discloses the system public key obtained by its own calculation Parameters, public parameters are: $pa_{III}\{G_1, G_2, e, q, d, P_{KGC}, H_I, H_{II}, H_{III}\}$.

D. Identity Generation

This scheme obtains the identities of users and cloud service providers according to the hierarchical ID tree in [56]. In the PKI domain, the root node represents the identity of CAII, and the leaf node represents the identity of U and CSP. If the ID of CAII is $ID_{CA_{II}} = DM_\alpha$, and the ID of user U is DM_U, then the real ID of user U is $ID_U = DM_\alpha || DM_U$. In the CLC domain, the root node represents the identity of KGC, and the leaf nodes represent the identity of U and CSP. If the ID of KGC is $ID_{KGC} = DM_\beta$, and the ID of CSP isDM_{CSP}, then the real ID of CSP is $ID_{CSP} = DM_\beta || DM_{CSP}$. Hierarchical ID tree as shown in Figure 2 and Figure 3:

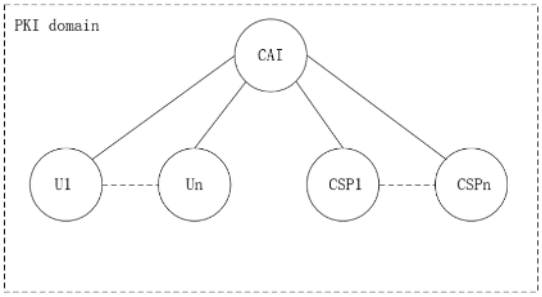


Figure 2:ID Spanning Tree in PKI Domain

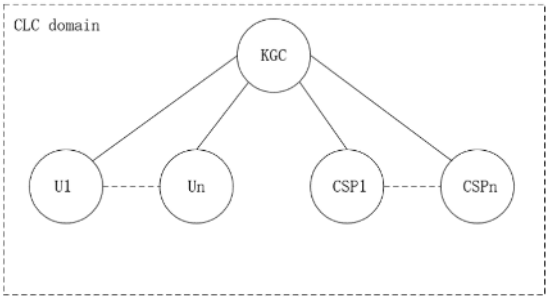


Figure 3: ID Spanning Tree in CLC Domain

E. Key Generation

(1) User registration in the PKI domain: According to the hierarchical ID tree structure, the real identity of user U is obtained as ID_U, and the temporary identity of user U is generated by the generator d and a random parameter r_u selected by the user. $TID_U = H_I(ID_U || r_U d)$, where $r_u \in Z_q^*$, then encrypt the application registration message through CAII's system public key and transmit it to CAII. The transmission information is: $en\{ID_U, ID_{CA_{II}}, TID_U, r_U d\}_{P_{CA_{II}}}$. CAII uses its own private key to decrypt the transmitted information and then reads the user's temporary identity TID_U and verifies it. If the verification is successful, it will query whether the identity data of the user U is stored in the user registration list. If the user is not queried. Identity information, the anonymous certificate issued for the temporary identity of the user is: $Cert_U = \{ID_{CA_{II}} TID_U, T_{begin}, T_{end}, P_U, m_U\}$, where$m_U$ is the user's certificate information, and T_{begin} and T_{end} represent the certificate's Valid date, then CAII reads the local timestamp T_U and uses the system random parameter s_II to perform signature calculation on the temporary identity of the user, obtain the signature ciphertext information $\delta_U = s_I H_{II}(TID_U || T_U)$, and then store the user's certificate in the In the certificate store and in the identity information store and user registration list. After CAII encrypts $en\{Cert_U, \delta_U, T_U\}_{P_U}$ with the private key and transmits it to the user, the user U downloads his own certificate. Compared with the literature [22], this scheme generates the system parameter $r_U d$ through the point multiplication operation at this stage, and cancels the signature calculation in the

re-signature algorithm, reduces the exponential operation and the bilinear operation, thereby reducing the computational cost.

(2) User registration in the CLC domain: According to the hierarchical ID tree structure, the real identity of the cloud service provider CSP is obtained as ID_{CSP}, and the generator d and the cloud service provider select a random parameterr_{CSP} to calculate and generate the cloud service provider's Temporary identity $TID_{CSP} = H_I(ID_{CSP}||r_{CSP}d)$, where $r_{CSP} \in Z_q^*$, and then encrypt the registration application message with KGC' s system public key and transmit it to KGC. The transmission information is: $en\{ID_{CSP}, TID_{CSP}, P_{CSP}, r_{CSP}d\}_{P_{KGC}}$. KGC decrypts the received message with its own private key and obtains the temporary identity TID_{CSP} of the cloud service provider CSP and verifies whether it is legal. If the verification is legal, it queries whether the identity data of the cloud service provider is stored in the user registration list. If the identity information of the cloud service provider is not queried, KGC calculates the cloud service provider signature ciphertext information $\delta_{CSP} = s_{III}H_{II}(TID_{CSP}||T_{CSP})$ according to the timestamp T_CSP and the system random parameter s_{III}, and generates the calculation part according to the temporary identity of the CSP The parameters of the private key $Q_{CSP} = H_{II}(TID_{CSP})$, the partial private key $D_{CSP} = s_{III}Q_{CSP}$ is calculated through the system random parameters s_{III} andQ_{CSP}, and then the private key parameters and identity information are stored in the user registration list. The message $en\{Q_{CSP}, D_{CSP}, \delta_{CSP}\}P_{CSP}$ is returned to CSP, and CSP randomly selects a secret value $x_{CSP} \in Z_q^*$, and calculates the complete private key $SK_{CSP} = x_{CSP}s_{III}Q_{CSP}$, $P_{CSP} = x_{CSP}d$ as the public key. Compared with the literature [22], this scheme generates the system parameter $r_{CSP}d$ through the point multiplication operation at this stage, and cancels the signature calculation in the re-signature algorithm, reduces the exponential operation and bilinear operation, and thus reduces the computational cost.

F. Cross-domain authentication

In order to realize the cross-domain identity authentication of foreign users between different cryptosystems, this scheme signcrypts the temporary identities of users and cloud service providers, introduces the inter-cloud identity authentication center to verify the decryption and signcryption, and verifies the temporary identities of foreign users. In this process, the security of the identity information of users and cloud service providers is guaranteed, and the cross-domain identity authentication of heterogeneous cryptosystem systems is realized, The flow chart is shown in Figure 4:

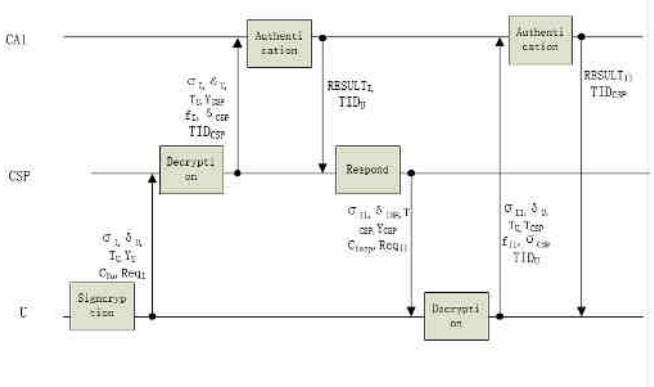


Figure 4: Flow chart of heterogeneous cross-domain identity authentication scheme

1. In the PKI domain, the user's real identity is ID_u, the private key is SK_U, and the temporary identity is TID_u. The user randomly selects the secret parameters again: $\alpha_u \in \{0,1\}^n, C_{Y_u} \in Z_q^*, a \in Z_q^*$, and according to the secret random parameter a and generator d to calculate and establish the session key negotiation parameters: $Y_u = ad$,according to the known parameters to calculate the signcryption ciphertext parameters:

$$\beta_I = \alpha_u + H_{II}(TID_u),$$

$$\varpi_I = H_{III}\ (e(P_{KGC}, Q_{CSP})^{\beta_I}, \beta_I P_{CSP}\ ),$$

$$A_I = \beta_I d, S_I = \beta_I + SK_U H_{II}(TID_U)$$

generate sign-ciphertext $\sigma_I = ((S_I)_{P_{CSP}}, A_I, \varpi_I)$, the user sends an application for cross-domain resource access to CSP through a secure encrypted channel Request information $\{\sigma_I, \delta_U, Y_U, T_U, C_{Y_U}, request_I\}$, where C_{Y_U} is to ensure freshness of session messages random parameters.

2. After the cloud service provider CSP receives the access request information of the user U, it decrypts the received ciphertext information according to its own private key sk_{CSP}, and obtains request$_I$ in the decrypted information to determine whether it is an access request , if not, the subsequent verification will not be performed and the user's request will be rejected. If it is an access request, it will first verify whether the user's timestamp T_U has expired, and the CSP will de-sign and encrypt the ciphertext information again according to its own private key. Obtain the parameter $A_I$based on the information after de-signcryption to calculate the parameters required for de-signcryption verification: $f_I = H_{III}(e(D, A_I), x_{CSP}A_I)$, then read the local timestamp T_{CSP} , use its own public key to The message $\{S_I, A_I, \varpi_I, f_I, \delta_U, \delta_{CSP}, T_U, T_{CSP}, TID_{CSP}\}_{P_{pub}}$ is encrypted and uploaded to CAI, the identity authentication center between clouds.

3. CAI uses its own private key to decrypt the ciphertext encrypted by CSP. The operation steps performed by CAI are divided into the following 4 steps:

(1) Verify whether $\delta_{CSP}d = P_{KGC}H_{II}(TID_{CSP}||T_{CSP})$ is established, this equation verifies the identity of the uploader, if the verification is passed, the identity of the uploader is legal. Then proceed to verification 2 below.

(2) Verify that$f_I = \omega_I$ holds, $f_I = H_{III}(e(D, A_I), x_{CSP}A_I)$. The proof is as follows:

$$H_{III}(e(D, A_I), x_{CSP}A_I) = H_{III}(e(s_{II}Q_{CSP}, \beta_I d), x_{CSP}\beta_I d)$$
$$= H_{III}(e(Q_{CSP}, s_{II}d)^{\beta_I}, \beta_I P_{CSP}) =$$
$$H_{III}(e(Q_{CSP}, P_{KGC})^{\beta_I}, \beta_I P_{CSP})$$

If the equation can be verified, proceed to step 3 below.

(3) Verify that $V_I = A_I$ is established, $V_I = S_I d - H_{II}(TID_U)P_U$. The proof is as follows:

$$V_I = S_I d - H_{II}(TID_U)P_U$$

$$= (\beta_I + SK_U H_{II}(TID_U))d - H_{II}(TID_U)P_U = \beta_I d = A_I$$

If the equation can be verified and passed, then proceed to the following step 4.

(4) Verify whether the identity of user U is legal $\delta_u d = P_{CA_{II}}H_{II}(TID_U||T_U)$. If the verification results of the above four steps are all successful, the verification success parameter $RESUTL_I$is output, and if the verification result fails, the verification failure parameter "$\perp$" is output. The CAI returns the message $\{RESUTL_I, TID_U\}$ to the CSP.

4. After the CSP receives the CAI message, it reads the verification result parameters. If the verification parameter is "$\perp$", it means that the identity of the foreign user is illegal. After reading the verification result parameters, the CSP refuses to provide cloud resource services for the illegal user. If the result is$RESUTL_I$, it means that the identity of the foreign user is legal, and the CSP provides cloud resource services for the user after reading the verification result parameters. The CSP selects the secret random parameters again: $\alpha_{CSP} \in \{0,1\}^n, C_{Y_{CSP}} \in Z_q^*, b \in Z_q^*$, and calculates and establishes the session key negotiation parameters according to the secret random parameter b and the generator d: $Y_{CSP} = bd$, calculate the signcrypted ciphertext according to the known parameters:

$$\beta_{II} = \alpha_{CSP} + H_{II}(TID_{CSP}), A_{II} = \beta_{II}d,$$

$$S_{II} = \beta_{II} + H_{II}(TID_{CSP})SK_{CSP}, \varpi_{II} = H_{III}(P_{KGC}, P_U)^{\beta_{II}},$$

$$\sigma_{II} = ((S_{II})_{P_U}, A_{II}, \varpi_{II})$$

After generating the signcrypted ciphertext σ_{II} , the parameters $\{\mathrm{TID}_U, \delta_U, \mathrm{Num}_i, \mathrm{T}_U\}$ are stored in the user registration list. Then the cloud service provider encrypts the parameter information with the user's public key and responds to the user. The transmission information is: $\{\sigma_{II}, \delta_{CSP}, Y_{CSP}, T_{CSP}, C_{Y_{CSP}}, request_{II}\}$.

5. After receiving the encrypted information from the CSP, the user decrypts it with the private key and obtains the parameters, and then verifies whether the timestamp $\mathrm{T_{CSP}}$ of the CSP is within the validity period. If the timestamp is within the valid range, the signcryption encryption begins. The user calculates the required parameters for de-signcryption verification according to the parameters $\mathrm{A_{II}}$ obtained from the de-signcryption: $f_{II} = H_{III}(e(SK_U P_{KGC}, A_{II}))$, encrypts the following transmission information, and then uploads it to CAI. $\{S_{\mathrm{II}}, \mathrm{A_{II}}, \varpi_{\mathrm{II}}, \mathrm{f_{II}}, \delta_U, \delta_{\mathrm{CSP}}, \mathrm{T_{CSP}}, \mathrm{TID}_U, \mathrm{T}_U\}_{P_{Pub}}$.

6. The CAI decrypts the encrypted message after receiving it. The operation steps performed by CAI are divided into the following 4 steps:

(1) CAI first verifies $\delta_u d = P_{CA_{II}}H_{II}(TID_U||T_U)$, this equation represents the uploading user identity, if the verification is passed, it means that the uploading to the identity is legal. Then proceed to verification 2 below.

(2) Verify that $f_{II} = \varpi_{II}$ holds, $f_{II} = H_{III}(e(SK_U P_{KGC}, A_{II}))$. The proof is as follows:

$$H_{III}(e(SK_U P_{KGC}, A_{II})) = H_{III}(e(x_U d, s_{II}P)^{\beta_{II}}$$

$$= H_{III}(e(P_U, P_{KGC})^{\beta_{II}}).$$

If the verification passes, proceed to verification 3 below.

(3) Verify that $V_{II} = A_{II}$ is established, $V_{II} = S_{II}d - H_{II}(TID_{CSP})P_{CSP}P_{KGC}$. The proof is as follows:

$$V_{II} = \beta_{II}d + H_{II}(TID_{CSP})SK_{CSP}d - H_{II}(TID_{CSP})P_{CSP}P_{KGC}$$
$$= \beta_{II}d + x_{CSP}QH_{II}(TID_{CSP})s_{II}d$$
$$- H_{II}(TID_{CSP})P_{CSP}P_{KGC} = A_{II}$$

If the equation can be verified, then perform the following step 4

(4) Verify whether the identity of the cloud service provider is legal: $\delta_{CSP}d = P_{KGC}H_{II}(TID_{CSP}||T_{CSP})$ If the verification results of the above four steps are all successful, the verification success result $RESUTL_{II}$ is output, and if the verification result fails, the failure verification failure symbol "$\perp$" is output. The CAI returns the message { $RESUTL_{II}$, TID_{CSP}} to user U.

7. When the user U receives the information from the CAI, it first determines the verification result. If the verification result is a failure message, it refuses to establish a session channel with the CSP and ends the access process. If the verification result is $RESUTL_{II}$, the user starts to calculate With the session key between the CSP, the user establishes a trusted connection session channel with the cloud service provider, and receives cloud services from the cloud service provider..

G. Repeated cross-domain authentication

After the user U and the cloud service provider CSP complete the first cross-domain authentication, the CSP will store the legal user's identity information in the registration list for subsequent repeating the cross-domain authentication

process. Repeated cross-domain authentication uses the signcryption algorithm to authenticate the same cryptographic system. It checks whether the session key calculated by the user during the first cross-domain authentication is stored in the user registration list of the CSP for verification, and the number of cross-domain authentication is Num_1. Whether and timestampT_U are in a limited period for further verification, if the above verification is passed, repeating the cross-domain identity authentication process does not require the inter-cloud authentication center to participate in the calculation, saving communication overhead, and users and cloud service providers do not need a large number of Cryptographic computation and verification. Compared with literature [22], this scheme generates session key parameters through dot product operation at this stage: $Y'_u = a_i d$、$Y'_{\mathrm{CSP}} = b_i d$、$Y = a_i b_i d$, and cancels the literature [22], which reduces the computational overhead by reducing the large number of exponential operations and bilinear operations run at this stage in the literature [22]. The model for repeating cross-domain is shown in Figure 5:

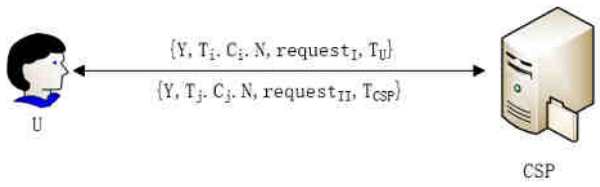


Figure 5: Repeated cross-domain authentication

The process of repeating the cross-domain model is as follows:

(1) User U updates the local timestamp to T_i after completing the first cross-domain authentication, and then selects random parameters: $a_i \in Z_q^*, N \in Z_q^*, C_i \in Z_q^*$, according to the generator d and the random parameter a_i Calculate the new session key $Y'_u = a_i d$, encrypt the relevant parameters with the CSP's public key and send the cross-domain resource access $en\{Y, Y', T_i, C_i, N, request_I\}_{P_{CSP}}$ again, In the related parameters, Y is the session key stored when the user performs cross-domain authentication for the first time.

(2) After the CSP receives the repeated cross-domain request from the foreign user U again, it starts the repeated cross-domain authentication process: the CSP first decrypts the access request according to its own private key, and then determines whether $request_I$ is the cross-domain access request information after obtaining the relevant parameters. , and then verify the parameter C_i to determine the freshness of the session, and then query whether the user's identity information $\{TID_U, Y, \sigma_I, \mathrm{Num}_1, T_U\}$ has been stored in the user registration list. Whether the session key Y received by repeated cross-domain authentication is equal to the session key stored in the user's first cross-domain authentication, and then check whether the heterogeneous cross-domain times parameters Num_1 are within the legal times and timestamps Whether T_i is within the validity period. If the above verification result is successful, the repeated cross-domain authentication is successful, and the CSP re-updates the relevant parameters of the repeated cross-domain authentication: Num_1、T_1、C_1, and the parameters are updated to: $\mathrm{Num}_i = \mathrm{Num}_1 + 1$、$\mathrm{T}_i$、$C_i$. CSP selects random parameters again: $b_i \in Z_q^*, C_j \in Z_q^*$, updates the new session key $Y'_{\mathrm{CSP}} = b_i d$ and encrypts the parameters $\{Y'_{\mathrm{CSP}}, \mathrm{T}_j, \mathrm{C}_j, \mathrm{N}, \mathrm{request}_{\mathrm{II}}\}_{P_U}$ with the user's public key returned to the user.

(3) After user U decrypts the CSP's return message with its own private key, it determines whether $\mathrm{request}_{\mathrm{II}}$ in the decrypted message is a response message, and then checks the timestamp T_j to keep the session fresh. Whether the parameters C_j and random number N are consistent, only after these three parameters are successfully verified, U will accept the information sent by the CSP, and at the same time update the session key $Y = a_i b_i d$ to complete the PKI-CLC of repetition across domains.

IV. CASE ANALYSIS

A. *Security Analysis*

This scheme adopts the proof method of literature [27], and describes the cross-domain authentication process of heterogeneous cryptosystems as the protocol ψ in AM. In this paper, a secure and difficult-to-solve signcryption algorithm is used to analyze the security of the protocol ψ of this scheme on the basis of the CK security model. Document [55] proves that the algorithm is unforgeable, then the session key in AM is secure, and the protocol ψ is also secure. prove:

1. During the authentication process of the cross-domain identity authentication protocol ψ, since the message participant user, inter-cloud authentication center and cloud service provider of this cross-domain authentication protocol are not breached by the attacker X in the AM, the user and cloud service The provider can normally obtain the key negotiation parameters Y_U and Y_{CSP} that have not been tampered with by the attacker X through the secure channel, and calculate and obtain the consistent session key parameter Y, so this heterogeneous cross-domain authentication model satisfies Definition 3. Session key The first nature of safety.

2. Suppose the malicious hacker X in the guessing game AM initiates Q rounds of guessing. Through an algorithm A, the random result of the malicious hacker X can be used to guess with probability ε what the session key in the cross-domain authentication protocol ψ is. The real value is still a random value. Randomly select t rounds of sessions in Q rounds of guessing where, t∈{1,2,3....Q}, the input value of algorithm A in the selected tth round of sessions is（Y_U^*，K^*，Y_{CSP}^*）, where Y_U^* is the key negotiation parameter

calculated when the user makes a cross-domain access request, and Y_{CSP}^{*} is the key calculated in the message returned by the cloud service provider to the user after authenticating the user. Key negotiation parameters, K^{*} is the query response. So there are the following 2 situations:

(1) Select the malicious hacker X in the t-th session. The malicious hacker X can guess whether the input value is a real value or a random value with a probability of 1/2+ε, so that the algorithm A can use 1/2+ The probability of ε guesses whether the input value is a real value or a random value. Because if the input value guessed by algorithm A is the real session message, the response to the malicious hacker X is also the real session key Y, and if it is a random value, the malicious hacker X also obtains a random value.

(2) In the t-th round of session testing, the malicious hacker X is not selected, but the test sessions outside the t-th round are selected. Algorithm A can guess whether the input value is a real value or a random value with a probability of 1/2. The probability that the t-th round session is selected is 1/q, and the probability that the malicious hacker X can correctly guess that the test session is the true value is 1/2+ε. The probability that the t-th round session is not selected is 1-1/q, and the probability that the malicious hacker X can correctly guess that the test session is the true value is 1/2, so the probability that the malicious hacker X guesses successfully is 1/ q(1/2+ε)+(1-1/q)1/2 . Therefore, algorithm A judges that the probability of the input session key being successful is 1/2+ε/q , which satisfies the second property of definition 3.

B. *Anonymous Tracking of Entity Identity*

Users and cloud service providers in foreign domains establish their own temporary identities by selecting random numbers to ensure the security of their real identities, and then signcrypt the temporary identities to obtain signcrypted ciphertexts S_I and S_{II}. When the cloud service provider receives a cross-domain identity authentication request from a foreign user, it cannot correctly determine whether the identity of the user U is legal, so the CSP transmits the sign-ciphertext S_I and the user's temporary identity TID_U to the inter-cloud identity authentication center CAI Verify: $\delta_{CSP}d = P_{KGC}H_{II}$ （$TID_{CSP}||T_{CSP}$）， $S_I = A_I$, no matter what the verification result is, CAI will send the verification result to CSP, CSP uses the private key to decrypt and obtain the verification result parameter for judgment, if the parameter is "⊥", it means that the verification failed, if the parameter is RESULT, it means that the verification is successful. When the CSP sends a cloud resource provisioning response to the user, the user continues to verify the signcrypted information S_{II} and TID_{CSP} of the CSP in the inter-cloud authentication center CAI in the same way: $S_{II} = A_{II}$， $\delta_{CSP}d = P_{KGC}H_{II}(TID_{CSP}||T_{CSP})$, send the authentication result to U, and if the verification passes, the user accepts the cloud resources provided by the CSP. Therefore, this scheme can realize the anonymous tracking of the identity of two-way entities.

C. *Antireplay attack*

If a user initiates a cross-domain request, a malicious hacker intercepts the information m by monitoring and other means next to the cross-domain authentication communication channel. After waiting for a period of time, the intercepted information m is replayed into the communication channel. After receiving the information sent by user U, the CSP in the CLC domain uses its own private key to decrypt the information to obtain the timestamp, because the timestamp and the random parameters for maintaining session freshness have changed after the malicious hacker performs the replay attack, which exceeds the validity period. And lead to parameter verification error, through the above two parameter verification, CSP will fail to authenticate the information m, so this scheme can effectively resist replay attack.

D. *Antireplacement Attacks*

Users and cloud service providers in foreign domains establish their own temporary identities by selecting random numbers to ensure the security of their real identities, and then signcrypt the temporary identities to obtain the signcrypted ciphertexts S_I and S_{II} , which once again strengthens the understanding of the real identity. The strength of identity protection. If a malicious hacker wants to replace the real identity or temporary identity and then verify it, the verification will fail because the malicious hacker cannot obtain the private key of the legitimate user and the cloud service provider and cannot crack the signcrypted information and the signature of the temporary identity.

E. *Anti-Man-in-the-Middle Attacks.*

When user U crosses the domain to access the cloud service provider, user U includes in the message the signature by CA1 on its temporary identity and encrypts the message through the public key of the CSP in the communication. 3e CSP can decrypt the message only by means of its own private key and then verifies the message, thus ensuring that the identity is real. Man-in-the-middle attacks are resisted.

This article compares the cross-domain solution in recent years with this solution. From Table 2 below, we can see the advantages of this solution in terms of security performance. Among them, "NO" means that the document cannot meet this performance, and "YES" means that the document meets this performance.

This scheme generates the real identities of users in the PKI domain and cloud service providers in the CLC domain through a hierarchical ID tree, and then uses random parameters and generators to bind the real identities of users and cloud service providers to generate temporary identities, realizing anonymity. Sexual tracking. Compared with the literature [16-17], this scheme signs the temporary identity by selecting random parameters and timestamps that keep the session fresh. Changes beyond the validity period lead to parameter verification errors, which can effectively resist replay attacks. Compared with the literature [13], this scheme only causes its own temporary identity to become invalid when the time stamp expires during the cross-domain process

of the cloud service provider. Using this method of binding the timestamp with the temporary identity can ensure the synchronization of the timestamp and the identity authentication. Compared with literature [12], this scheme can effectively resist man-in-the-middle attacks, making it scheme closer to today's complex cloud environment.

more secure. Compared with the literature [14], this scheme can realize the cross-domain identity authentication function under the heterogeneous cryptosystem, making the cross-domain authentication

Table 2: Security comparison

Scheme	Anonymous Tracking	Anti-man-in-the-middle Attack	Antireplay Attacks	Antireplacement Attacks
[16]	NO	NO	NO	YES
[17]	NO	NO	NO	YES
[18]	NO	YES	YES	YES
[13]	NO	YES	YES	YES
[12]	NO	YES	YES	YES
[14]	NO	YES	YES	NO
[15]	NO	YES	YES	NO
Our Scheme	YES	YES	YES	YES

Table 3: The first cross-domain authentication calculation cost comparison

Scheme	The first cross-domain authentication stage	Heterogeneous cross-domain authentication	Use signcryption
[21]	5De+3Be+6H+6En	NO	NO
[20]	7Be+6H+4En	NO	NO
[15]	4De+4Be+8H+6En	YES	NO
[19]	5De+3Be+6H+4En	NO	NO
[12]	10De+4Be+6H+4En	YES	NO
[13]	4De+3Be+6H+4En	NO	NO
Our Scheme	4De+2Be+6H+4En	YES	YES

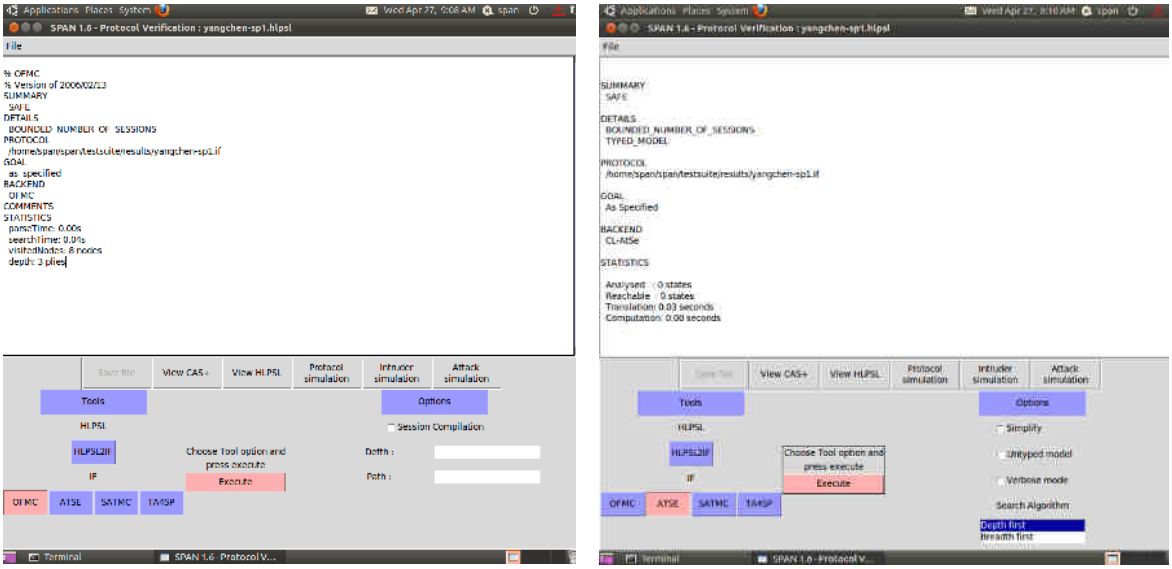


Figure 6: Validation results of OFMC and CL-AtSe analysis tools

F. Simulation Experiment

The performance of the cross-domain authentication scheme depends on the security and computational overhead. In order to verify the actual security performance of this scheme, several simulation experiments were carried out. The experimental environment was Windows10-x64 and vmware virtual machine software, and the Ubuntu10 operating system was installed in the vmware virtual machine for simulation experiments. Install the model analysis tool AVISPA with HLPSL language in Ubuntu, which can analyze whether there are security risks such as replay attacks and man-in-the-middle attacks. The simulation experiment is carried out on the security of the first cross-domain identity authentication in this scheme. The simulation experiment code defines the role specification of the authentication initiator user U, cloud server CSP, and cloud authentication center CA in detail. In order to perform anti-replay attack check on the protocol of this scheme, the presence of intruders is checked by passive search using CL-AtSe and OFMC analysis tools in AVISPA. Meanwhile, CL-AtSe and OFMC can also check for man-in-the-middle attacks. Several simulation experiments are carried out through CL-AtSe and OFMC analysis tools, which prove that this scheme can effectively resist other types of network attacks such as man-in-the-middle, replay and replacement attacks, and the verification results are all SAFE. The simulation results are shown in Figure 6 .

G. Performance Analysis

Due to the complexity of bilinear calculation and exponential calculation in the cross-domain process of this solution, the performance analysis and comparison mainly considers the amount of calculation involved in the user phase, the cross-domain phase and the repeated cross-domain phase. The following calculation cost comparison only considers Exponential operations, bilinear operations hash operations, and encryption/decryption pair operations. Among them, Be represents the time consumed by the bilinear calculation, De represents the time consumed by the exponential calculation, H represents the hash operation, and represents the encryption and decryption pair operations.

Table 3 shows the comparison results of the performance and calculation amount of this scheme and several other cross-domain schemes. Compared with the above-mentioned other literatures, this scheme does not require the overhead of bilinear and exponential calculation in the user registration stage and the repeated cross-domain stage, which greatly improves the overall calculation efficiency of the scheme.

During the first cross-domain authentication, the signcryption between the user and the cloud service provider requires 4 bilinear calculations, 2 exponential calculations, 6 hash calculations, and 4 encryption/decryption pair calculations. At the same time, the cross-domain authentication process is simple. When this scheme performs the first cross-domain authentication with the users in [19] and [20], bilinear and exponential operations are required, because this scheme does not use proxy re-signature during the first cross-domain authentication process Therefore, the calculation overhead of bilinear and exponential is reduced, and the calculation overhead of this scheme in the first cross-domain authentication process is

reduced. Compared with literature [12], this scheme transfers the authentication process and de-signcryption process to the cloud-to-cloud authentication center, which reduces the computing burden of users and improves the overall computing efficiency. Compared with this scheme, the computational overhead of scheme [13] is larger in the stages of user registration and repeated cross-domain authentication. The cost of the cross-domain authentication stage in the literature [15] is not much different from this paper, but it is impossible to perform cross-domain authentication for heterogeneous systems, and the overhead is relatively large, and there are security risks. . This paper and the literature [21] cannot satisfy the anonymous property and cannot perform cross-domain authentication.

In the field of cross-domain identity authentication scheme, this paper is the first to propose a heterogeneous cross-domain identity authentication scheme based on signcryption algorithm. This paper makes a detailed comparison of the number of exponential operations, the number of bilinear operations, the number of hash operations, and encryption and decryption in the first cross-domain authentication stage. The comparison results are shown in Figure 8:

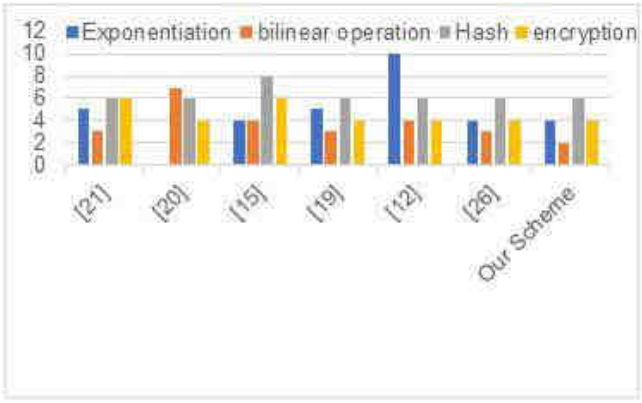


Figure 8: Comparison result of calculation cost of cross-domain authentication for the first time

V. CONCLUSION

This paper considers the problems of existing research on cross-domain identity authentication, and proposes a scheme that can realize cross-domain identity authentication between two different cryptosystems, PKI-CLC, based on the signcryption algorithm, and complete the identity through a third-party cloud authentication center The authentication and decryption signcryption process reduces the communication computing load between foreign users and improves the speed of information exchange between users and cloud service providers. Through several simulation experiments, it is proved that this scheme can effectively resist other types of network attacks such as man-in-the-middle, replay and replacement attacks, and the security of temporary keys not discussed in other related research literatures is discussed. For the follow-up research work, we can focus on the research of the cloudless third-party authentication center and the research on the heterogeneous cross-domain identity authentication scheme of the IBC cryptosystem.

REFERENCES

[1] Massimiliano P, Smith S. Finding the PKI needles in the Internet haystack.[J]. Journal of Computer Security, 2010, 18(3): 397–420.

[2] Hong, Sunghyuck. Two-channel user authentication by using USB on Cloud[J]. Journal of Computer Virology & Hacking Techniques, 2016, 12(3):137-143.

[3] T. Varshney, N. Sharma, I. Kaushik and B. Bhushan, "Authentication & Encryption Based SecurityServices in Blockchain Technology," 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2019, pp. 63-68.

[4] Dent AW, Libert B, Paterson KG. Certificateless encryption schemes strongly secure in the standard model.In: Cramer R, eds. Proc.of the PKC 2008. LNCS 4939, Heidelberg: Springer-Verlag, 2008. 344−359.

[5] Hwang YH, Liu JK, Chow SSM. Certificateless public key encryption secure against malicious KGCattacks in the standard model.Journal of Universal Computer Science, Special Issue on Cryptography inComputer System Security, 2008,14(3):463−480.

[6] DONG Z,ZHANG L,LI J.Security Enhanced Anonymous Remote User AuthentiCA1tion and KeyAgreement for Cloud Computing[C]// Proceedings of the 17th International Conference on ComputationalScience and Engineering.[S 1.]: IEEE Computer Society Press,2014:1746-1751.

[7] BINU S,MOHAMMED M,RAJ P.A Mobile Based Remote User AuthentiCA1tion Scheme without Verifier Table for Cloud Based Services[C]//Proceedings of the 3rd International Symposium on Women in Computing and Informatics. New York, USA:ACM Press, 2015.502-509.

[8] Wang C, Chao L, Niu S, Li C, Xu W, editors. An authenticated key agreement protocol for cross-domain based on heterogeneous signcryption scheme. Wireless Communications & Mobile Computing Conference; 2017.

[9] Wang W, Hu N, Liu X. BlockCAM: A Blockchain-Based CrossDomain Authentication Model[C]//Proceedings of the 2018 International Conference on Data Science and Cyberspace (DSC).Piscataway,NJ:IEEE,2018: 896 -901.

[10] Guo Shaoyong，Hu Xing，Zhou Ziqiang，et al． Trust access authenti- cation in vehicular network based on blockchain［J］. China Commu- nications，2019，16(6) : 18-30.

[11] Wang Xinyan，Gao Feng，Zhang Jing，et al． Cross-domain authentication mechanism for power terminals based on blockchain and credibility evalu- ation［C］//Proc of the 5th International Conference on Computer and Communication Systems． Piscataway ，NJ: IEEE Press，2020: 936-940.

[12] Yang Xiaodong, An Faying, Yang Ping, Liu Tingting, Xiao Likun & Wang Caifen. (2019). A cross-domain identity authentication scheme based on proxy re-signature in cloud environment. Chinese Journal of Computers (04), 756-771

[13] Wang Zhonghua , Han Zhen , Liu Jiqiang , etc. Identity Authentication Scheme Based on PTPM and Certificateless Public Key in Cloud Environment [J]. Journal of Software, 2016,27(6):1523-1537.

[14] Ni L , Chen G , Li J , et al. Strongly secure identity-based authenticated key agreement protocols without bilinear pairings[J]. Information Sciences, 2016:176-193.

[15] WANG Yufeng，NAKAO A，VASILAKOS A V，et al. P2P Soft Security: on Evolutionary Dynamics of P2P Incentive Mechanism［J］. Computer Communications， 2011，34(3) : 241-249.

[16] Zhou Zhicheng, Li Lixin, Li Zuohui, et al. Efficient cross-domain authentication scheme based on blockchain technology [J]. Computer Applications, 2018, 02(v.38;No.330):18-22+28.

[17] Li Zheng, Chen Zemao, Qin Yanlin, et al. Cross-domain authentication scheme based on zero-knowledge proof[J]. Computer and Digital Engineering, 2014(03):446-449.

[18] Chen Y , Dong G , Bai J , et al. Trust Enhancement Scheme for Cross Domain Authentication of PKI System[C]// 2019 International Conference on Cyber- Enabled Distributed Computing and Knowledge Discovery (CyberC). 2019.

[19] Yang Xiaodong, An Faying, Yang Ping, et al. Cloud cross-domain identity authentication scheme based on certificateless signature [J]. Computer Engineering, 2017, 43(11): 128-133,145.

[20] Yang Li, Ma Jianfeng, Jiang Qi. A Direct Anonymous Proof Scheme Across Trusted Domains for Wireless Mobile Networks[J]. Journal of Software, 2012, 34(5):1260-1271.

[21] NOWAK M A，MAY R M. Evolutionary Games and Spatial Chaos［J］. Nature，1992，359 (6398) : 826-829.

Chen Yang Master of Tiangong University, School of Computer Science and Technology, research direction is network security and cryptography.

Wenju Liu Master of Nankai University, professor of School of Computer Science and Technology, Tiangong University, main research directions: enterprise informatization, computer network security, Academic Research: Liu Wenju, Shang Yuzhen, Zhang Yan, Wang Ze. An analysis of the improved EAP-AKA protocol. 2010 the 2nd International Conference on Computer Engineering and Technology (ICCET 2010). Vol.1:10-13, Chengdu, April, 2010.（EI:20104313316688）；

Wenju Liu,Xuejing Li,Ze Wang,Wei Zou. Power Level Based Key Management Scheme forWireless Sensor Networks . Journal of Computers Information Systems , Volume 9, Number 23,9637-9644, 2013（EI：20140517248441）.

Ze Wang Ph.D. from Northeastern University, Tiangong University, Vice Dean of the School of Computer Science and Technology; selected for the training program for young and middle-aged innovative talents in Tianjin universities; member of the China Computer Federation, member of the American ACM Society, long-term engaged in computer network technology, wireless network security mechanism, Internet + Research and development in application system development, mobile network perception computing, etc.