计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.191100068

云环境下基于代理盲签名的高效异构跨域认证方案

江泽涛　徐娟娟
桂林电子科技大学广西图像图形与智能处理重点实验室　广西 桂林 541004
(394503704@qq.com)

摘　要　针对现有不同体系公钥基础设施(Public Key Infrastructure,PKI)和无证书公钥密码体系(CertificateLess public key Cryptography,CLC)的跨域身份认证方案不能满足身份盲化性以及高效的异构跨域认证问题,提出代理盲签名的高效异构跨域认证方案。该方案重新构造了一个高效、安全的跨域身份认证模型并结合代理签名和盲签名的优点,在云间引入一个可信认证中心CA给予第三方合法代理者可信的代理权限来执行代理盲签名操作。此代理者不仅减少了云间认证中心CA的通信负载,实现不同域授权代理盲签名用户和请求代理盲签用户之间的信息交互,还满足了双向实体身份同步认证的盲化性以及代理盲签名的可识别性,提高了认证安全性。分析结果表明,该方案基于数学困难性问题满足抗替换性攻击、抵抗重放攻击、抗中间人攻击和身份不可追踪性等性能,完成了异域用户之间高效、高安全性的跨域身份认证。

关键词:异构体系跨域认证;代理盲签名;盲化性;可识别;跨域身份认证模型
中图法分类号　TP309

Efficient Heterogeneous Cross-domain Authentication Scheme Based on Proxy Blind Signature in Cloud Environment

JIANG Ze-tao and XU Juan-juan
Key Laboratory of Image and Graphic Intelligent Processing in Guangxi,Guilin University of Electronic Technology,Guilin,Guangxi 541004,China

Abstract　In order to solve the problem of identity blindness and efficient heterogeneous cross-domain authentication,an efficient heterogeneous cross-domain authentication scheme based on proxy blind signature is proposed. The scheme reconstructs an efficient and secure cross-domain identity authentication model. Combined with the advantages of proxy signature and blind signature,a trusted certification authority CA is introduced in the cloud to give the third party legal agent the trusted agency authority to perform the proxy blind signature operation. This agent not only reduces the communication load of the inter-cloud certification authority CA,realizes the information interaction between the authorized agent blind signer in different domains and the requesting agent blind signer,but also satisfies the blindness of bidirectional entity identity synchronous authentication and the identifiability of the proxy blind signature,and improves the authentication security. The results show that based on the mathematical difficulty,the scheme can meet the performance of anti-substitution attack,resist replay attack,man-in-the-middle attack,identity untraceability and so on,and complete the cross-domain identity authentication with high efficiency and security between foreign users.

Keywords　Heterogeneous architecture cross-domain authentication,Proxy blind signature,Blindness,Identifiability,Cross-domain authentication model

1　引言

云环境[1]是以嵌入可信平台模块(Trusted Platform Module,TPM)为核心的用户智能卡片。移动通信设备的广泛使用、云中大量的计算资源,以及存储和软件资源链接导致了网络的复杂性,使信息安全跨域认证技术成为各行业关注的焦点。资源服务在开放的互联网环境中会面临四面八方的网络攻击、用户数据安全和隐私保护问题,使得跨管理、跨地域的协作至关重要。不同密码体系之间的频繁交互主要以立体防御、深度防御为核心确保信息机密,以该核心思想进入加

到稿日期:2019-11-11　返修日期:2020-01-07　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61876049,61762066,61572147);广西科技计划项目(AC16380108);广西图像图形智能处理重点实验项目(GIIP201701,GIIP201801,GIIP201802,GIIP201803);广西研究生教育创新计划资助项目(2019YCXS043)
This work was supported by the National Natural Science Foundation of China (61876049,61762066,61572147),Guangxi Science and Technology Project (AC16380108), Key Laboratory Project of Image and Graphics Intelligent Processing in Guangxi (GIIP201701, GIIP201801, GIIP201802,GIIP201803) and Funded by the Guangxi Graduate Education Innovation Program(2019YCXS043).
通信作者:徐娟娟(1903281466@qq.com)

强安全保障的信息时代。鉴于云计算多样性、部署复杂、开放性的特点，迫切需要研究云环境下异构体系之间的跨域身份认证技术，来确保各异构体系之间用户身份的完整和安全性，建立可信链接关系。

公钥基础设施[2]（PKI）是典型的安全基础服务设施，用于数据机密、完整性、不可否认性、用户身份鉴别等安全性能，绑定所属域用户的身份信息和公钥进行可信通信。基于标识的密码系统（Identity-Based Cryptography，IBC）是基于 PKI 发展而来的，其使得安全应用更易于部署和使用，而无证书公钥密码体制[3]（CLC）是为解决基于系统通信过程中的密钥托管问题。可信域引入一个可信的密钥生成中心（Key Generation Center，KGC）为其所在域用户生成部分私钥。安全实现两种主流的密码体制 PKI－＞CLC 的身份认证是异构用户跨域通信的前提。Binu 等[4]基于数字证书的云端身份认证，使用多个因素加强认证，实现了云环境远程用户身份验证，但由于频繁验证证书，增加了计算负载量。Dong 等[5]基于无证书密码体制匿名身份的认证，使用户和服务器能够相互匿名认证，并建立安全通道，但因不满足抗中间人攻击，无法保证用户身份的真实性。Yang 等[6-7]基于云跨域身份认证，实现了用户与云服务提供商的身份真实性鉴别，完成了双向认证会话密钥协商，但无法满足异构体系之间的跨域认证。Xie 等[8]构建一种新的信息服务实体跨域认证模型，解决了身份即时撤销的问题，但认证模型不满足异构域认证。此外，Wang 等[9]基于虚拟有线的异构跨域认证模型，实现了 PKI 和 Kerberos 异构域用户之间的安全认证，但不满足认证过程身份的盲化性。Ma 等[10]基于区块链技术的跨域认证，实现了异构域安全高效的跨域认证，但无法满足身份的盲化性、同步和匿名性。

目前现有大部分身份认证方案[11]和跨域设计模型[12]不支持异构域之间用户的跨域认证和高效认证过程中身份的盲化性，因此本文提出了一种云环境下基于代理盲签名的公钥基础设施和无证书密码体制高效跨域身份认证方案。根据重新构建的跨域认证模型，利用代理签名的优势和盲签名算法盲化性[13]的特点，利用由云间认证中心 CA 认证的合法代理授权服务机构进行双向实体的代理盲签名算法[14-16]，减少了云间认证中心的通信负载。请求代理盲签名用户通过审核代理盲签名的合法性来判断异域授权代理用户的真实性，以实现异构域双向用户盲化身份合法性验证，并在认证过程中完成对用户真实身份的匿名性、代理盲签名可识别性以及时间有效性，对恶意用户保持可控性来实现高效、高安全的跨域认证。最后计算会话密钥建立可信安全通信链接。

2 相关知识点

（1）CDH（Computational Diffie-Hellman）问题：对于给定的 $P, aP, bP \in G_1$，可以计算 abP，其中 P 是 G_1 加法循环群的生成元，元素 $a, b \in Z_q^*$。

CDH 假设：对于存在的任意概率多项式算法 A，不存在能成功解决 CDH 问题的概率。

（2）CTCDH（Chosen-Target Computational Diffie-Hellman）问题：对于 q 阶生成元为 P 的循环群 G_1，给定信息（P，aP），$a \in G_1$ 和敌手 A，其中 A 可以向目标预言机和帮助预言机进行询问。A 攻破 CTCDH 问题的概率为：经过 N_1，N_2（$N_1 < N_2$）次目标预言机和帮助预言机询问，A 可以成功输出 $N(N_1 \leqslant N \leqslant N_2)$ 对元组的概率，并满足等式 $Q = aZ_i'(1 \leqslant i \leqslant N)$，其中 Q 为帮助预言机返回值，Z_i' 为目标预言机返回的随机点。

CTCDH 假设：时间算法 A 能以不可忽略的概率多项式解决 Chosen-Target CDH 问题。

3 基于代理盲签名的异构跨域身份认证新方案

3.1 重构跨域身份认证信任模型

本文方案重新构建了如图 1 所示的跨域身份认证信任模型。本模型主要设计 PKI 和 CLC 两个不同的密码体制来实现异构跨域认证。可信 PKI 系统中存在证书颁发机构 CA_1 和用户 U；密钥生成中心 KGC 和信息服务提供商 ISP 在同一安全域 CLC 系统内；盲签名代理者 BSP 和 CA 存在于云间。证书颁发机构 CA_1 负责生成管理数字证书以及授权证书的更新、吊销等服务，同域中用户可通过证书库查询或下载相应证书。在可信 CLC 系统中，KGC 负责系统部分密钥的生成、保存、更新、查询等密钥服务，并解决分布式大规模密码技术密钥管理问题；同域中用户可通过注册申请获取部分密钥。认证中心 CA 是云间具有权威性和公正性的第三方可信服务机构，保证可信的授权信息传递，为减少自身的计算负担和时间，在云间引入可信代理者以支持生成代理盲签名密钥，并对请求代理盲签名者进行盲签名操作，增加了身份的安全性和真实完整性，减少了用户的计算负载，提高了系统的运作效率。

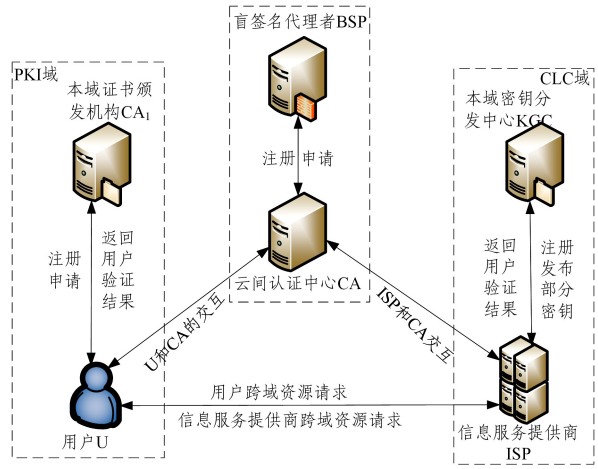


图 1 重构跨域身份认证信任模型

Fig. 1 Reconstructing cross-domain authentication trust model

本重构跨域模型主要包括 6 个参与实体。1）云间认证中心 CA：不仅为云间代理者 BSP 验证身份、颁发合法数字证书，还负责验证跨域用户的身份合法性。2）盲签名代理者 BSP：通过盲签名算法为身份合法者的信息执行代理盲签名操作。3）证书颁发机构 CA_1：认证本地域用户身份的合法性，在用户注册列表中保存合法用户身份信息并负责用户证书的申请、颁发、撤销和查询等操作。4）用户 U：从 CA_1 中通过下载证书来完成自身在本地安全域中的身份认证，并通过授权

代理盲签名实现 ISP 的身份认证。5)密钥生成中心 KGC:被所在域中的所有用户信任,负责为其本地域用户完成身份认证并保存合法用户身份信息,生成并颁发部分私钥,并解决密钥托管问题。6)信息服务提供商 ISP:通过授权代理完成跨域用户的身份认证,并为可信用户提供云资源信息服务。

3.2 代理盲签名跨域身份认证的基本流程

为实现异构体系中用户跨域资源访问的身份认证,重构如图 2 所示的代理盲签名跨域认证基本流程。通过云间第三方代理者为合法用户执行身份盲签名的操作,完成双向跨域实体身份盲传递的认证。该跨域模型的设计实现了 PKI 信任域到 CLC 信任域用户高效、高安全性的跨域认证。

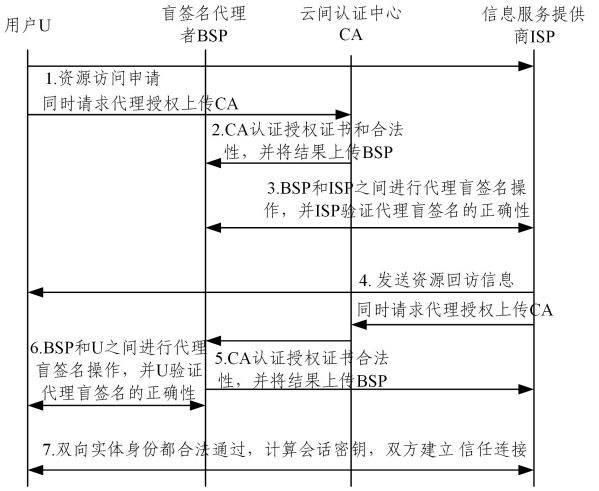


图 2 代理盲签名跨域身份认证的基本流程

Fig. 2 Basic flow chart of proxy blind signature cross-domain authentication

本模型设计主要以用户 U 跨域访问信息服务提供商 ISP 为例,描述认证过程。1)安全域 PKI 和 CLC 中的用户分别完成在所属域的身份合法认证。2)PKI 域中的用户 U 对异构域 CLC 中的信息服务提供商 ISP 发出访问资源申请,同时用户 U 向云间 CA 发送代理授权证书信息;CA 对收到的代理授权证书进行验证,并将验证结果发至代理者 BSP;BSP 验证获取的结果,若结果通过,则生成代理盲签名密钥,完成用户 U 与 BSP 之间的代理授权操作。3)ISP 收到用户 U 的访问资源申请,先判断是否是访问申请,若是,则查看用户注册列表中是否存在该用户消息,若存在,则执行重复跨域认证,否则向 CA 发出代理信息;CA 收到代理信息对 ISP 进行身份验证,若身份合法,则 CA 将结果和 ISP 的代理信息发至 BSP;BSP 查看验证结果,若通过,则执行代理盲签名操作:BSP 将授权文件发至 ISP,ISP 随机选取盲化因子对身份进行盲化计算,并将盲化消息返回至 BSP,BSP 对其盲化身份消息进行代理盲签名计算,并将代理盲签名消息返回给 ISP,完成代理盲签名。4)ISP 根据收到的代理盲签名消息恢复原始签名信息,并验证盲签名的合法性,若盲签名合法,则说明用户 U 的身份合法并为其提供信息服务。5)同理,ISP 将回访消息发至用户 U,同时向 CA 发送代理授权证书信息;CA 根据授权证书验证 ISP 的合法性,并将验证结果上传 BSP;BSP 查看收到的结果,若结果通过,则生成代理盲签名密钥,完成 ISP 与 BSP 之间的代理授权。6)用户 U 收到回访消息,并将代理盲签名申请消息上传至 CA;CA 对用户 U 的身份进行验证,若验证通过,则将结果和用户 U 的代理盲签名申请上传至 BSP;BSP 查看结果,若结果通过,则将授权证书发至用户 U;用户根据随机性选取盲化因子对身份计算身份盲化消息,并将身份盲化消息返回至 BSP;BSP 对盲化消息进行盲签名,且将代理盲签名返回至 U,完成用户 U 与 BSP 的代理盲签名操作。7)用户 U 对代理盲签名恢复出原始签名,根据盲签名验证代理盲签名的正确性,若正确,则相信 ISP 为可信信息提供者并接受信息提供。8)完成双向实体跨域认证,计算会话密钥,建立 PKI→CLC 异构系统用户之间的信任链接。

3.3 新方案的具体描述

本文方案主要分为系统初始化、用户注册、异构跨域身份信任认证和重复跨域身份认证 4 个部分。可信域分别完成两个异构系统参数的选择,所属安全域用户身份的注册,利用代理盲签名算法完成 PKI→CLC 各用户的身份认证,建立信任连接,利用建立的会话密钥完成重复跨域认证。

3.3.1 系统初始化

输入系统安全参数 $\Re$,定义两个 q 阶循环群 G_1, G_2,q 为素数,P 是 G_1, G_2 的生成元,选择两个安全的哈希函数 $H_1: \{f_1\}^{p-1} \rightarrow G_1, H_2: \{f_2\}^{p-1} \rightarrow G_2$,其中 f_1, f_2 属于循环群中的随机数,$\|$ 为字符串连接操作符。

(1)云间认证中心 CA 选取一个随机值 $x_{CA} \in Z_q^*$ 作为系统主私钥,计算系统公钥 $P_{CA} = x_{CA} P$,CA 的公私钥对为 (x_{CA}, P_{CA});公开系统参数 $para = \{G_1, G_2, q, e, P, H_1, H_2, P_{CA}\}$。

(2)PKI 域的 CA_1 选择一个随机系统密钥值 $x_{CA} \in Z_q^*$,计算该域公钥 $P_{CA_1} = x_{CA_1} P$,公私钥对为 (x_{CA_1}, P_{CA_1}),并公开该域参数 $para1 = \{G_1, G_2, q, e, P, H_1, H_2, P_{CA_1}\}$。

(3)CLC 域的 KGC 选择一个随机系统密钥值 $x_K \in Z_q^*$,计算该域公钥 $P_{KGC} = x_K P$,公私钥对为 (x_K, P_{KGC}),并公开该域参数 $para2 = \{G_1, G_2, q, e, P, H_1, H_2, P_{KGC}\}$。

3.3.2 所属域用户注册

(1)云间 BSP-CA 的申请注册

云间盲签名代理者 BSP 选择一个随机秘密值 $x_B, r \in Z_q^*$ 作为私钥,计算公钥 $P_{BSP} = x_B P$,并对真实身份 ID_{BSP} 进行隐私加密,得到临时身份 $TID_{BSP} = H_1(ID_{BSP} \| rP)$,读取时间戳 T_{BSP},将申请注册消息 $\{T_{BSP}, ID_{BSP}, P_{BSP}, rP, TID_{BSP}\}_{P_{CA}}$ 加密并通过安全通道送至云间认证中心 CA。

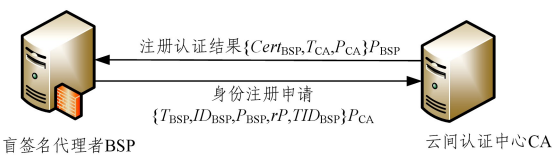


图 3 云间代理者注册申请

Fig. 3 Application for registration of agents between clouds

CA 安全接收 BSP 的注册申请消息并通过自身私钥解密,验证 ID_{BSP} 身份的真实性:先检查用户注册列表中是否存在该 ID_{BSP} 身份消息,若存在,则已验证通过该申请注册用户是可信用户;若不存在,CA 首次验证临时身份的合法性

$TID_{BSP}=?H_1(ID_{BSP}\|rP)$并检查时间戳 T_{BSP} 的有效范围。若验证失败，则终止协议，反之验证通过，则 ID_{BSP} 是可信身份。CA 随机选择计算参数 $a_{CA}\in Z_q^*$，计算 $E=a_{CA}P$，并对可信用户的临时身份进行签名加密 $\theta_{CA}=a_{CA}x_{CA}H_1(TID_U\|T_U)$；CA 为用户颁发一个合法的数字证书 $Cert_{BSP}=\{\theta_{CA},TID_{BSP},E,P_{BSP},T_{begin1},T_{end1}\}$，其中 T_{begin1}，T_{end1} 为证书有效的起止日期，读取证书时间戳 T_{CA} 在同时在用户注册列表中保存消息（$Cert_{BSP}$，ID_{BSP}，T_{CA}，TID_{BSP}，rP），将数字证书消息 $\{Cert_{BSP},T_{CA},P_{CA}\}_{P_{BSP}}$ 返至 BSP。

BSP 安全下载证书解密，验证证书合法性 $\theta_{CA}P^2=?EP_{CA}H_1(TID_{BSP}\|T_{BSP})$以及证书时间戳 T_{CA}的有效性，若都通过，BSP 接受证书，完成 BSP－＞CA 的注册，说明 BSP 也是一个可信的云间用户。

（2）U-CA_1 的申请注册

用户 U 选择随机参数 x_U，$x\in Z_q^*$，其中 x_U 作为私钥，计算用户公钥 $P_U=x_UP$ 和临时身份 $TID_U=H_1(ID_U\|xP)$，用户从证书库下载 CA_1 自签名根证书，提取 CA_1 公钥 P_{CA_1}，并读取本地时间戳 T_U。用户发送通过公钥 P_{CA_1} 加密的申请注册消息$\{ID_U,P_U,TID_U,xP,T_U\}_{P_{CA_1}}$ 给所属域 CA_1。

CA_1 收到申请注册消息后，先通过自身的私钥解密该消息，并验证 ID_U 的身份合法性，检查用户注册列表中是否已经存在 ID_U，如存在，则说明已经验证过 ID_U 身份合法，否则检查用户临时身份的正确性 $TID_U=?\ H_1(ID_U\|xP)$和时间戳 T_U 的有效性，若验证通过，则 ID_U 身份合法。CA_1 随机选择参数 $a\in Z_q^*$，计算 $A=aP$ 和对用户身份的签名消息 $\theta_{CA_1}=ax_{CA_1}H_1(TID_U\|T_U)$；为用户临时身份颁发合法证书 $Cert_U=\{\theta_{CA_1},TID_U,A,P_U,T_{begin},T_{end}\}$，其中 T_{begin}，T_{end} 分别为证书的起效日期和截至日期。CA_1 在用户注册列表中保存首次验证合法身份信息$\{ID_U,TID_U,T_{CA_1},xP\}$，并将证书存储到证书库中，其中 T_{CA_1} 为对用户颁发证书的时间戳。CA_1 将颁发证书消息$\{Cert_U,T_{CA_1},P_{CA_1}\}_{P_U}$ 发送至用户 U。

用户 U 收到颁发证书消息并通过自身私钥解密下载证书，验证证书的合法性，判断 $\theta_{CA_1}P^2=?AP_{CA_1}H_1(TID_U\|T_U)$是否成立，并验证时间戳 T_{CA_1} 的有效性，若都通过，用户接受证书，完成 PKI 中用户的身份合法性验证。

（3）ISP-KGC 的申请注册

信息服务提供商 ISP 随机选取秘密值 $r_{ISP}\in Z_q^*$，计算 ISP 的临时身份 $TID_{ISP}=H_1(ID_{ISP}\|r_{ISP}P)$，其中 ID_{ISP}为 ISP 的真实身份；ISP 向密钥生成中心 KGC 发送加密的注册申请消息$\{ID_{ISP},TID_{ISP},P_{ISP},r_{ISP}P\}_{P_{KGC}}$。

KGC 收到消息利用自身的私钥 x_K 对其进行解密，并验证 ISP 身份 ID_{ISP}在安全域 CLC 中的合法性，判断临时身份的正确性 $TID_{ISP}=?H_1(ID_{ISP}\|r_{ISP}P)$。若验证通过，密钥生成中心 KGC 选取随机数 $r_{KGC}\in Z_q^*$，计算 $R=r_{KGC}P$，并读取本地域的时间戳 T_{KGC}，对 ISP 的临时身份进行签名计算 $\theta_{ISP}=x_KH_1(TID_{ISP}\|T_{KGC})$，KGC 计算部分密钥 $D=r_{KGC}+\theta_{ISP}$；并将消息$\{ID_{ISP},TID_{ISP},P_{ISP},r_{ISP}P,T_{KGC}\}$保存至用户注册列表中，此时返回消息$\{D,R,P_{KGC}\}$给 ISP。

信息服务提供商 ISP 收到返回消息，验证 $DP=?\ R+H_1(TID_{ISP}\|T_{KGC})P_{KGC}$，若验证通过则接收部分密钥 D，ISP 计算私钥 $x_{ISP}=D+r_{ISP}$和公钥 $P_{ISP}=x_{ISP}P$。

3.3.3 异构跨域身份信任认证

根据图 4 的跨域代理盲签名认证信任模型可知，异构跨域身份信任认证主要通过资源请求、授权代理密钥生成、代理盲签名、代理盲签名验证 4 个阶段来完成异构域双向实体之间高效、安全的认证。最后计算会话密钥建立双向实体信息交互的信任链。

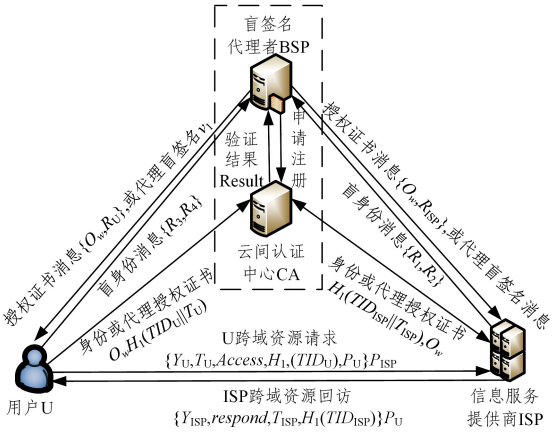


图 4 重构跨域代理盲签名认证信任模型

Fig. 4 Reconstruction of cross-domain proxy blind signature authentication trust model

为了便于描述，本文主要以用户 U 访问信息服务提供商 ISP 为例，对双向实体跨域身份进行认证。

（1）信息服务提供商 ISP 验证用户 U 的身份

1）第一阶段资源请求

根据异构域用户注册，已知 PKI 域用户 U 的真实身份 ID_U、临时身份 TID_U 和公私钥对（x_U，P_U）；用户随机选取参数 $a_U\in Z_q^*$，计算会话密钥协商参数 $Y_U=a_UP$，并获取本地域时间戳 T_U。用户发送跨域资源申请访问消息$\{Y_U,T_U,Access,H_1(TID_U),P_U\}_{P_{ISP}}$至 CLC 域中的信息服务提供商 ISP。同时进行第二阶段的授权代理密钥生成部分。

2）第二阶段授权代理密钥生成

用户 U 要对第三方代理盲签名者 BSP 授权代理操作，才能执行合法的代理盲签名以增加身份的私密性。用户 U 计算代理授权证书 $O_\omega=x_UH_2(\omega)$，其中 ω 为公开授权文件。用户将代理授权证书消息$\{O_\omega,P_U,\omega\}_{P_{CA}}$加密并发送给云间可信认证中心 CA。

云间认证中心安全接收用户 U 的代理授权消息，利用自身私钥解密此消息以获取公开授权文件，验证代理授权证书 O_ω 的安全性，即验证式（1）是否成立：

$$O_\omega P=x_UH_2(\omega)P=P_UH_2(\omega) \tag{1}$$

若等式成立，CA 相信用户 U 是可信用户，并将授权验证结果$\{Result1,O_\omega\}_{P_{BSP}}$送至盲签名代理者 BSP。

BSP 解密并验证 Result1 的输出结果，若输出结果为“⊥”，则接收代理授权证书 O_ω，并根据有效的代理授权证书生成代理盲签名密钥 $SK_{U\text{-}BSP}=(O_\omega,x_B)$，完成代理授权；反之，则结束代理协议。

3）第三阶段代理盲签名

信息服务提供商 ISP 安全接收 U 的跨域资源申请访问

消息并用其自身的私钥 x_{ISP} 解密。先判断 Access 是否是申请访问消息，T_U 是否在有效范围内；若都通过，且 ISP 查看用户注册列表中不存在 $H_1(TID_U)$，则 ISP 计算 $\sigma_{ISP}=x_{ISP}H_1(TID_{ISP}\parallel T_{ISP})$ 并发送代理盲签名请求消息 $\{Blind\ Signature, \sigma_{ISP}, H_1(TID_{ISP}\parallel T_{ISP}), T_{ISP}, P_{ISP}\}_{P_{CA}}$ 至云间认证消息 CA。

CA 安全接收代理盲签名请求消息并解密，验证 ISP 身份合法性 $\sigma_{ISP}P=?P_{ISP}H_1(TID_{ISP}\parallel T_{ISP})$ 和时间戳 T_{ISP} 的有效性。若都通过，说明 ISP 为合法用户，CA 将验证结果 $\{Result2, Blind\ Signature, P_{ISP}\}$ 发至 BSP。

BSP 安全接收消息，先检查接收消息是否是代理盲签名请求消息 *Blind Signature*，若是，则验证 *Result2* 的输出结果是否为“⊥”，若为“⊥”则执行代理盲签名操作：BSP 随机选一个参数 $\alpha\in Z_q^*$，计算 $R_{ISP}=\alpha O_\omega R_{ISP}=\alpha O_\omega$，返回消息 (O_ω, R_{ISP}) 至 ISP。

ISP 安全接收 (O_ω, R_{ISP}) 并随机选取 3 个参数 $\beta, d_1, d_2\in Z_q^*$，然后计算 $R'=\beta R_{ISP}$，并对其自身临时身份信息进行盲化操作 $R_1=d_1H_1(TID_{ISP}\parallel O_\omega\parallel T_{ISP})d_2P$，$R_2=d_1\beta$，并将盲化身份信息 $\{R_1, R_2\}$ 通过安全通道发送至 BSP。BSP 安全接收并用代理密钥对 ISP 的盲化身份消息进行代理盲签名操作 $V=x_B^2R_1R_2R_{ISP}$，并将 V, Q_1 通过安全通道返回给 ISP。

ISP 对收到来自 BSP 的代理盲签名消息进行去盲化 $V'=d_1^2d_2P_{BSP}^{-V}$，得到代理盲签名 $\delta_{ISP}=(TID_{ISP}, O_\omega, T_{ISP}, R', V')$，并验证其时间戳 T_{ISP} 是否前后一致且在有效范围内。如满足前后一致且在有效范围内，ISP 进行第四阶段的代理盲签名验证。

4）第四阶段代理盲签名验证

信息服务提供商 ISP 根据获取的 $\delta_{ISP}=(TID_{ISP}, O_\omega, T_{ISP}, R', V')$ 来验证式(2)的正确性。

$$\begin{aligned}V'P&=d_1^2d_2P_{BPS}^{-1}(x_B^2R_1R_2\alpha O_\omega)P\\&=d_1^2d_2P_{BPS}^{-1}(d_1^2d_2\beta\alpha O_\omega H_1(TID_{ISP}\parallel O_\omega\parallel T_{ISP})x_BP_{BSP})P\\&=\beta\alpha O_\omega H_1(TID_{ISP}\parallel O_\omega\parallel T_{ISP})x_BP\\&=\beta\alpha O_\omega PH_1(TID_{ISP}\parallel O_\omega\parallel T_{ISP})P_{BSP}\\&=\beta\alpha O_\omega H_1(TID_{ISP}\parallel O_\omega\parallel T_{ISP})P_{BSP}\\&=P_{BSP}R'H_1(TID_{ISP}\parallel O_\omega\parallel T_{ISP})\end{aligned}\tag{2}$$

若式(2)验证通过，则 ISP 接收代理盲签名，即接收 U 的跨域访问资源请求，ISP 在用户注册列表中保存合法用户信息 $\{P_U, H_1(TID_U), T_U, \delta_{ISP}, number\}$，并为合法用户 U 提供信息资源服务。

(2)用户 U 验证信息服务提供商 ISP 的身份

1）ISP 选取随机数 $a_{ISP}\in Z_q^*$，计算密钥协商参数 $Y_{ISP}=a_{ISP}P$，读取本地时间戳 T_{ISP}，并将回访消息 $\{Y_{ISP}, respond, T_{ISP}, H_1(TID_{ISP})\}_{P_U}$ 返至用户 U；同时 ISP 根据上述第二阶段的授权代理密钥生成算法进行如下操作。

2）ISP 计算代理授权证书 $O_\omega=x_{ISP}H_2(\omega)$，将代理授权证书 $\{O_\omega, P_{ISP}, \omega\}_{P_{CA}}$ 发送给云间可信认证中心 CA。

CA 验证代理授权证书 O_ω 的安全性，即验证式(3)是否成立。

$$O_\omega P=x_{ISP}H_2(\omega)P=P_{ISP}H_2(\omega)\tag{3}$$

若式(3)成立，CA 相信 ISP 是可信信息提供者，并将授权验证结果 $\{Result3, O_\omega\}_{P_{BSP}}$ 送至盲签名代理者 BSP。

BSP 解密验证 Result3 的输出结果，若输出结果为“⊥”，则接收代理授权证书 O_ω，生成代理盲签名密钥 $SK_{ISP\text{-}BSP}=(O_\omega, x_B)$，其中 ω 为公开授权证书文件，完成代理授权继续执行以下操作，否则代理协议终止。

3）用户 U 收到回访消息并用自身私钥解密此消息，获取并判断 respond 是否是回应消息，且时间戳 T_{ISP} 是否在有效范围内。若两个条件均满足，那么同理，继续验证 ISP 身份的合法性：进行同上述第三阶段的代理盲签名阶段，即用户 U 读取本地时间戳 T_U，计算 $\sigma_U=x_UH_1(TID_U\parallel T_U)$ 并发送盲签名请求消息 $\{Blind\ Signature1, \sigma_U, H_1(TID_U\parallel T_U), T_U, P_U\}_{P_{CA}}$ 至云间认证消息 CA。

CA 接收盲签名请求消息并解密，验证 U 身份的合法性 $\sigma_UP=?P_UH_1(TID_U\parallel T_U)$ 和时间戳 T_U 的有效性。若都满足，则说明 U 为合法用户，CA 则将验证结果 $\{Result4, Blind\ Signature1, P_U\}$ 发至 BSP。

BSP 安全接收验证结果消息，并确认 *Blind Signature*1 为代理盲签名请求消息，且 Result4 的输出结果是“⊥”，则 BSP 执行代理盲签名操作。BSP 随机选一个参数 $\chi\in Z_q^*$，计算 $R_U=\chi O_\omega$，发送 (O_ω, R_U) 至用户 U。

U 安全接收信息 (O_ω, R_U) 然后随机选取 3 个参数 $\beta_1, d_3, d_4\in Z_q^*$，并计算 $R_U'=\beta_1R_U$，再通过对用户 U 的临时身份信息进行盲化操作，来增加临时身份认证过程的安全性，即计算 $R_3=d_3H_1(TID_U\parallel O_\omega\parallel T_U)d_4P$ 和 $R_4=d_3\beta_1$，用户 U 通过安全通道发送盲化身份信息 $\{R_3, R_4\}$ 至 BSP。

盲签名代理者 BSP 安全接收并用代理密钥对用户 U 的盲化身份进行代理盲签名计算 $V_1=x_B^2R_3R_4R_U$，然后将 V_1 通过安全通道返回给用户 U。

U 对收到来自 BSP 的代理盲签名进行去盲化操作 $V_1'=d_3^2d_4P_{BSP}^{-V_1}$，得到代理盲签名 $\delta_U=(TID_U, O_\omega, T_U, R_U', V_1')$，若时间戳在有效范围且前后一致，则用户 U 验证的代理盲签名消息 δ_U 的正确性，即执行下一步。

4）用户 U 验证式(4)是否成立，若成立，则相信代理盲签名是合法的，即接收信息服务提供商提供的资源。

$$\begin{aligned}V_1'P&=d_3^2d_4P_{BSP}^{-1}(x_B^2R_3R_4R_U)P\\&=d_3^2d_4P_{BSP}{}^{-1}(d_3^2d_4\beta_1\chi O_\omega H_1(TID_U\parallel\omega\parallel T_U)x_BP_{BSP})P\\&=\beta_1\chi O_\omega H_1(TID_U\parallel O_\omega\parallel T_U)x_BP\\&=\beta_1\chi O_\omega PH_1(TID_U\parallel O_\omega\parallel T_U)P_{BSP}\\&=\beta_1\chi P_{ISP}H_2(\omega)H_1(TID_U\parallel O_\omega\parallel T_U)P_{BSP}\\&=P_{BSP}R_U'H_1(TID_U\parallel O_\omega\parallel T_U)\end{aligned}\tag{4}$$

(3)会话密钥的建立

以上安全认证协议，若 PKI→CLC 中的用户验证身份都可信，则 PKI 用户和 CLC 用户建立信任连接，并计算用户和信息服务提供商之间的会话密钥 $Y=a_Ua_{ISP}P$。U 和 ISP 分别保存会话密钥用于重复跨域认证，以减少验证计算负担。

信息服务提供商 ISP 要访问用户的资源，也要进行 4 个阶段，即资源请求、授权代理密钥生成、代理盲签名、代理盲签

名验证，认证过程与上述过程相似，在此不加以赘述。

3.3.4 重复跨域身份认证

当成功完成首次异构跨域身份认证时，为了在执行重复跨域资源访问时减少计算负载量和时间，信息服务提供商 ISP 和用户 U 会在用户注册列表中记录相关的信息，除去云间认证中心和第三方代理盲签名的计算量，用户 U 和信息服务提供商 ISP 通过验证会话密钥的正确性来进行高效、安全、简洁的重复跨域认证过程。

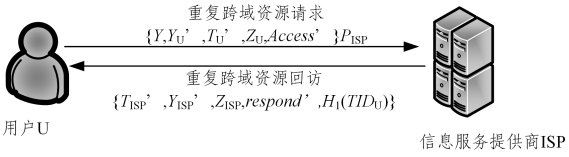


图 5 重复跨域认证请求

Fig. 5 Repeated cross-domain authentication requests

(1)用户 U 重复异构跨域认证随机选取参数 a_U'，$Z_U \in Z_q^*$，计算会话密钥协商参数 $Y_U' = a_U' P$ 和 $H_1(TID_U)$，用户获取本地域时间戳 T_U 和初次会话的信任链接的会话密钥 Y，发送跨域资源重复申请访问消息 $\{Y, Y_U', T_U', Z_U, Access'\}_{P_{ISP}}$ 至 CLC 域中的信息服务提供商 ISP。

(2)ISP 安全收到消息后，先判断 $Access'$ 是否是重复申请访问消息，若是则检查 Z_U 会话参数的新鲜性，则若新鲜，读取用户注册列表中是否存在此用户消息 $\{Y, P_U, H_1(TID_U), T_U, \delta_{ISP}, number\}$，若存在，ISP 判断此用户发送的会话密钥与保存的会话密钥是否一致，若不一致，异构跨域身份重复认证失败，若一致，则检查 T_U'，Z_U 的新鲜性和重复跨域次数是否在 T_U，$number$ 规定的范围内，只有都通过，才认为重复跨域身份认证成功。同时更新异构跨域认证次数为 $number+1$，并更新时间戳为 T_U' 和会话消息的新鲜性为 Z_U。ISP 选取随机数 a'_{ISP}，$Z_{ISP} \in Z_q^*$，计算会话密钥协商参数 $Y'_{ISP} = a'_{ISP} P$，读取本地时间戳 T'_{ISP}，ISP 回应消息 $\{T'_{ISP}, Y'_{ISP}, Z_{ISP}, respond', H_1(TID_U)\}$ 至用户。

(3)用户 U 安全收到 ISP 的回访消息后，首先检查 $respond'$ 是否是回访消息，如是，则检查 T'_{ISP}，Z_{ISP} 的有效性，若都在有效范围内，则判断收到的 $H_1(TID_U)$ 是否前后一致，只有所有验证均通过，用户 U 才会接收 ISP 的云资源提供，并且计算新的信任链接会话密钥 $Y^* = a_U' a'_{ISP} P$，完成 PKI→CLC 的重复跨域身份认证。

4 安全与性能分析

4.1 安全性分析

安全性分析主要是基于跨域代理盲签名认证信任模型以及困难性问题，以用户 U 访问信息服务提供商 ISP 的云资源为例说明本方案的安全性；信息服务提供商 ISP 回访用户 U 的安全分析同理可证得安全性。

4.1.1 盲化性

该代理盲签名的异构跨域身份认证方案具有盲化性，在跨域代理盲签名信任模型认证过程中，签名者无法得到关于被签名者的任何信息，并且无法否认该签名信息不是它进行的签名。因为任意有效的签名身份信息 $\{TID_{ISP}, O_\omega, R', V'\}$ 总是存在唯一的盲化因子 (b_1, b_2, β) 使得等式 $R' = \beta R_{ISP}$，$R_1 = d_1 H_1(TID_{ISP} \| O_\omega \| T_{ISP}) d_2 P$，$R_2 = d_1 \beta$，$V' = d_1^2 d_2 P_{BSP}^{-V}$ 成立，并且根据 $R' = \beta R_{ISP}$ 可以推导 β 的唯一存在性，同理也存在唯一的盲化因子 (b_1, b_2, β) 并且等式满足困难性问题 $V' P^2 = P_{BSP} P_U R' H_1(TID_{ISP} \| O_\omega \| T_{ISP})$，因此总是存在盲因子 (b_1, b_2, β) 使得攻击者能成功解决的概率仍为 1/2，本方案具有盲化性。

4.1.2 可识别性

由于 U 访问 ISP 时，ISP 在验证代理盲签名的过程中获取到代理盲签名者 BSP 的公钥和用户的授权证书 (P_{BSP}, O_ω)，根据获取的消息 ISP 可以很好地将代理盲签名者和用户区分开来，并且确认授权代理方是用户 U，而 BSP 是被授权代理方。同理，ISP 回访消息时，U 通过验证代理盲签名获取的公钥 (P_{BSP}, O_ω) 来很好地区分授权代理方和被授权代理方，实现参与认证方和代理盲签名方的可识别。

4.1.3 双向实体身份认证

在本方案的异构跨域身份认证过程中，当用户 U 访问信息服务提供商 ISP 时，用户 U 能够授权合法签名文件消息给可信第三方代理者 BSP，且 ISP 能够通过 BSP 对其身份信息代理盲签名判断等式 $V'P = ?d_1^2 d_2 P_{BPS}^{-1}(x_B^2 R_1 R_2 \alpha O_\omega) P$ 的合法性，来证明用户的可信性，当 ISP 回访消息，用户 U 也能通过 BSP 对其身份的代理盲签名判断等式 $V_1' P = ?d_3^2 d_4 P_{BSP}^{-1}(x_B^2 R_3 R_4 R_U) P$ 的正确性，来确认 ISP 是否是合法者。同理，实体信息服务提供商 ISP 访问用户 U 也是通过代理盲签名信息来进行双方的身份认证。本方案满足用户 U 和信息服务提供商 ISP 双向实体身份认证。

4.1.4 身份匿名追踪性

用户 U 和信息服务提供商 ISP 以及盲签名代理者在整个系统交互过程中都是以临时身份 $(TID_U, TID_{ISP}, TID_{BSP})$ 来代替真实身份 $(ID_U, ID_{ISP}, ID_{BSP})$ 信息，以实现双向实体的异构跨域身份认证。若信息服务提供商 ISP 接收用户 U 的访问消息是非法信息，ISP 会将身份 TID_U 提交至 PKI 域中的 CA_1，CA_1 通过验证 $TID_U = ?H_1(ID_U \| xP)$ 并查询为 U 签发合法证书时保存用户真实身份的注册列表来确定 TID_U 是真实身份 ID_U 的临时身份信息。为确定 ISP 提供的服务是非法恶意，将其 TID_{ISP} 发送至 KGC，KGC 通过 $TID_{ISP} = ?H_1(ID_{ISP} \| r_{ISP} P)$ 验证 ID_{ISP} 是临时身份 TID_{ISP} 的拥有者。方案满足身份匿名追踪性。

4.1.5 同步性

跨域认证过程中，对于用户 U 和 ISP 的临时身份 (TID_U, TID_{ISP})，使用时间戳 (T_U, T_{ISP}) 来保持会话以及身份的有效性，U 和 ISP 绑定临时身份 $H_1(TID_U \| O_\omega \| T_U)$ 和 $H_1(TID_{ISP} \| O_\omega \| T_{ISP})$，若 ISP 获取的代理盲签名消息 $\delta_{ISP} = (TID_{ISP}, O_\omega, T_{ISP}, R', V')$ 中的时间戳 T_{ISP} 和临时身份 $H_1(TID_{ISP} \| O_\omega \| T_{ISP})$ 前后不一致，则跨域认证失败，以确保临时身份和时间戳的一致同步性。同理，用户 U 根据获取的代理盲签名 $\delta_U = (TID_U, O_\omega, T_U, R_U', V_1')$ 的时间戳对比绑定的时间戳 $H_1(TID_U \| O_\omega \| T_U)$ 是否是有效时间，来达到身份验证和时间戳的一致性，有效实现实体双方验证身份的同步性。

4.1.6 抗替换攻击

本方案中用户和信息服务提供商都选取秘密值 $x\in Z_q^*$，$r_{ISP}\in Z_q^*$ 对真实身份进行绑定得到 $TID_U=H_1(ID_U\parallel xP)$ 和 $TID_{ISP}=H_1(ID_{ISP}\parallel r_{ISP}P)$，并在建立初次会话时，所属域中的 CA_1 和 KGC 对用户、信息服务提供商的合法临时身份通过签名进行了绑定 $\theta_{CA}=ax_{CA}H_1(TID_U\parallel T_U)$，$\theta_{ISP}=x_KH_1(TID_{ISP}\parallel T_{KGC})$。攻击者想要替换可信用户的临时身份签名信息，就需要先获取随机参数 a 和私钥(x_{CA}，x_K)。而在整个异构认证模型中，除了用户利用自身私钥对身份进行签名，不会泄露随机参数和私钥，攻击者则无法获取所属域中用户的秘密值和私钥，若攻击者替换相互认证的用户身份，则无法通过验证。故本方案满足抵抗替换攻击。

4.1.7 抵抗重放攻击

本方案在域内以及异构跨域身份交互传递信息认证过程中加入了用户选取的秘密值参数以及有效的时间戳，只有读取的时间戳在规定有效范围内以及随机参数正确时，参与认证方才能认为消息是有效、安全的。若恶意攻击者截取交互消息重放到认证系统中欺骗认证用户，由于用户每次选取的时间戳不同以及秘密值的随机性，则攻击者通过截取的消息将无法完成合法认证，因此本方案满足抵抗重放攻击。

4.1.8 抗中间人攻击

在交互认证通信过程中，目的方都是通过获取随机参数加密消息并通过安全通道将消息传输至参与认证方，防止中间人对认证消息参数的获取；参与认证方只有通过自身的私钥才能进行解密认证消息以获取安全的认证消息参数，实现了抗中间人攻击。

4.1.9 机密性

本方案基于数学困难性问题 CDH 问题(根据 abP，无法获取随机数 $a,b\in Z_q^*$)和 CTCDH 问题(敌手 A 根据获取消息(P,aP)，$a\in G_1$，想攻破 CTCDH 问题的概率为：A 可以成功输出 $N(N_1\leqslant N\leqslant N_2)$对元组的概率，其中 N_1，N_2 ($N_1<N_2$)为目标预言机和帮助预言机询问次数，并满足等式 $Q=aZ_i'(1\leqslant i\leqslant N)$来确保认证过程数据的安全性)。用户 U 和信息服务提供商 ISP 每次交互都会选取随机的秘密参数和本地时间戳来确保信息的机密性，并通过安全通道对消息加密来确保交互的认证机密性。在重复跨域认证阶段选取了会话协商有效参数以确保会话密钥的安全机密性。

4.2 安全性能分析

本方案基于数学困难性问题以及可信认证中心，利用盲签名的特点引入一个可信代理者操作代理盲签名，来安全实现 PKI 域和 CLC 域在云环境下用户交互身份认证。如表 1 所列，本方案与文献[10-11,17]相比，除了满足双向实体身份机密同步的匿名追踪认证、抗中间人攻击、抗重放性攻击、抗替换攻击，还满足双向用户身份的盲化性和代理盲签名的可识别性。表 1 中的数据表明，本方案安全性能更高。

表 1 异构系统跨域身份认证的安全性能分析

Table 1 Analysis of cross-domain authentication security performance of heterogeneous systems

方案	抗中间人攻击	双向实体认证	抗重放性攻击	抗替换攻击	身份同步性	匿名追踪性	机密性	盲化性	可识别性
文献[10]	√	√	√	√	×	×	√	×	×
文献[11]	√	√	√	×	×	×	√	×	×
文献[17]	√	√	√	×	×	×	√	×	×
本方案	√	√	√	√	√	√	√	√	√

注：若方案满足对应安全性能则用“√”表示，反之用“×”表示

4.3 效率分析

在效率分析方面，系统用户交互认证过程中除了要考虑安全性，还要减少异构域中算法与用户的计算开销，以提高认证效率。而基于数学困难性问题双线性计算和指数计算的开销较大，点乘运算开销较小。方案中的运算都是在加法循环群和乘法循环群的基础上进行的操作。

将文献[14,18]的算法与本方案的代理盲签名算法进行计算开销比较，结果如表 2 所列，其中，Bi 表示一次双线性运算，Index 表示一次指数运算。因为本方案主要利用点乘算法不需要双线性运算和指数运算，具有计算开销小的优势，所以与文献[14,18]相比，本方案的设计满足高效、高安全性。

表 2 代理盲签名算法的计算开销比较

Table 2 Comparison of calculation cost of proxy blind signature algorithms

方案	签名计算开销	盲化计算开销	验证计算开销
文献[14]	4Bi+7Index	6Index	4Bi
文献[18]	3Bi+6Index	2Bi	4Bi+2Index
本算法	0	0	0

如表 3 所列，本文方案主要考虑双线性与指数运算的计算开销。故与文献[6,7,19-21]方案相比，本方案提高了整个跨域模型系统在身份认证过程和重复跨域身份认证过程中的可信高效认证性。

表 3 用户跨域身份认证效率及性能分析

Table 3 Efficiency and performance analysis of user cross-domain authentication

方案	用户注册阶段	首次跨域认证阶段	重复跨域认证阶段	实现异构系统	代理盲签名
文献[6]	2Bi+2Index	3Bi+4Index	3Index	×	×
文献[7]	5Index	4Bi+10Index	3Index	×	×
文献[19]	3Index	3Bi+5Index	3Index	×	×
文献[20]	0	0	×	×	×
文献[21]	0	3Bi	0	√	×
本方案	0	0	0	√	√

结束语 基于传统公钥基础设施 PKI 和无证书公钥密码体系 CLC 存在的异构认证问题，结合云环境的内部安全部署和结构分布的复杂性、灵活性，本文提出了云环境下基于代理盲签名的高效异构跨域认证方案。该方案为提高安全性和认证效率，在跨域模型中引入一个可信的云间认证中心 CA，为了避免恶意用户和代理者，CA 负责代理用户和授权用户

的身份认证以及信息传递；为减少云间认证中心的计算负载，代理者通过云间 CA 完成申请注册并生成代理盲签名密钥和执行盲签名算法操作。与现有的跨域认证方案相比，本方案在困难性问题的基础上增加了认证用户身份的盲化性和代理盲签名的可识别性功能，防止攻击者获取用户身份以及伪造代理盲签名，达到跨域认证的高安全性。在高安全性的前提下，本方案利用点乘的优势减少计算负载，提高了跨域认证效率，实现了双向实体高效、高安全性的信息交互跨域认证。下一步将研究无可信云间认证中心的云环境下异构跨域身份认证方案。

参 考 文 献

[1] FENG D G，ZHANG M，ZHANG Y，et al. Study on Cloud Computing Security[J]. Journal of Software，2011，22(1)：71-83.

[2] LIN J Q，JING J W，ZHANG Q L，et al. Recent advances in PKI technologies[J]. Journal of Cryptologic Research，2015，2(6)：487-496.

[3] ZHANG F T，SUN Y X，ZHANG L，et al. Research on Certificateless Public Key Cryptography[J]. Journal of Software，2011，22(6)：1316-1332.

[4] BINU S，MOHAMMED M，RAJ P. A Mobile Based Remote User Authentication 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.

[5] DONG Z，ZHANG L，LI J. Security Enhanced Anonymous Remote User Authentication and Key Agreement for Cloud Computing[C]// Proceedings of the 17th International Conference on Computational Science and Engineering. IEEE Computer Society Press，2014：1746-1751.

[6] YANG X D，AN F I，YANG P，et al. Cross-domain Identity Authentication Scheme in Cloud Based on Certificateless Signature[J]. Computer Engineering，2017，43(11)：128-133，145.

[7] YANG X D，AN F Y，YANG P，et al. Cross-Domain Authentication Scheme Based on Proxy Re-signature in Cloud Environment[J]. Chinese Journal Of Computers，2017，42(4)：82-97.

[8] XIE Y R，MA W P，LUO W. New cross-domain authentication mode for information services entity[J]. Computer Science，2018，45(9)：177-182.

[9] WANG Y，WANG Y L. A Heterogeneous Cross-Domain Authentication Model Based on Access Tickets in Virtual Cable Television Network[J]. Applied Mechanics and Materials，2015，742：717-720.

[10] MA X T，MA W P，LIU X X. A Cross Domain Authentication Scheme Based on Blockchain Technology[J]. Acta Electronica Sinica，2018，46(11)：13-21.

[11] HE D，ZEADALLY S，KUMAR N，et al. Anonymous Authentication for Wireless Body Area Networks With Provable Security[J]. IEEE Systems Journal，2016，11(4)：2590-2601.

[12] ZHOU Z C，LI L X，LI Z H. Efficient cross-domain authentication scheme based on blockchain technology[J]. Journal of Computer Applications，2018，38(2)：316-320，326.

[13] SHI Y H，LI W S. A Survey of Blind Signature Studies[J]. Computer Engineering & Science，2005，27(7)：83-85.

[14] YANG X D，CHEN C L，YANG P，et al. Partially blind proxy re-signature scheme with proven security[J]. Journal on Communications，2018，39(2)：65-72.

[15] ZHAI Z Y，GAO D Z，LIANG X Q，et al. Certificate-based proxy blind signature scheme[J]. Computer Engineering and Applications，2014，50(4)：57-62.

[16] WANG C F，XU Q B，LIU C，et al. Partial Blind Signcryption Scheme in CLPKC-to-TPKI Heterogeneous Environment[J]. Journal of Electronics & Information Technology，2019，41(8)：77-85.

[17] NI L，CHEN G，LI J，et al. Strongly secure identity-based authenticated key agreement protocols without bilinear pairings[J]. Information Sciences，2016，37(2)：205-217.

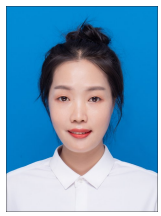
[18] GE R L，GAO D Z，LIANG J L，et al. Security analysis and improvement of certificateless proxy blind signature[J]. Journal of Computer Applications，2012，32(3)：705-706，714.

[19] WANG Z H，HAN Z，LIU J Q，et al. ID authentication scheme based on PTPM and certificateless public key cryptography in cloud environment[J]. Journal of Software，2016，27(6)：1523-1537.

[20] LIU S，ZHU S H. Identity Authentication Scheme in Multi-server Environment[J]. Computer Engineering，2015，41(3)：120-124.

[21] YUAN C，ZHANG W，WANG X，et al. Heterogeneous Cross-Domain Authenticated Key Agreement Protocols in the EIM System[J]. Arabian Journal for Science & Engineering，2017，42(8)：3275-3287.

JIANG Ze-tao，born in 1961，Ph.D，professor. His main research interests include image processing，computer vision，and network information security.



XU Juan-juan，born in 1994，postgraduate. Her main research interests include network information security and so on.