云环境下基于代理重签名的跨域身份认证方案

杨小东[1),2)] 安发英[2)] 杨 平[2)] 刘婷婷[2)] 肖立坤[2)] 王彩芬[2)]

[1)](密码科学技术国家重点实验室 北京 100878)

[2)](西北师范大学计算机科学与工程学院 兰州 730070)

摘 要 云计算是当前发展十分迅速的战略性新兴产业,但云计算面临着诸多关键性的安全问题,并且已经成为制约其发展的重要因素,其中身份认证问题首当其冲.身份认证是云计算安全的基础,为用户和云服务提供商的身份提供保证,阻止非法用户进入云系统,限制非法用户访问云资源.当前各类云服务已开始呈现出整合趋势,越来越多的云服务需要与其它异域的云服务互联,云服务提供商利用跨域身份认证机制来识别异域用户身份.目前大部分云计算平台采用用户名/口令组合认证,但这种认证方式存在两个主要的弊端:一是安全系数低,很容易被截取和监听;二是如果不同平台使用统一的用户名和密码,很容易造成用户身份信息的泄露.PKI(Public Key Infrastructure)为云计算环境下身份认证问题的解决提供了可行途径,是目前公认的保障网络社会安全的最佳体系,能在开放的网络环境中提供身份认证服务,确定信息网络空间中身份的唯一性、真实性和合法性,保护网络空间中各种主体的安全利益,已经广泛应用于电子商务、电子政务、网上银行等领域.但现有的基于 PKI 的跨域身份认证技术在可实施性、可扩展性、灵活性、互操作性和证书验证等方面都存在严重的不足,它在对可扩展性、动态性、开放性等方面都有较高要求的云计算环境中难以得到应用.针对现有基于 PKI 的跨域身份认证机制存在信任路径长、证书验证效率低、域间信任路径构建复杂等问题,利用代理重签名技术提出了一种云环境下的跨域身份认证方案,实现用户与云服务提供商之间的双向身份认证.用户与云服务提供商基于数字证书的合法性和认证消息的有效性完成双方身份的真实性鉴别,并在认证过程中协商了会话密钥;"口令+密钥"的双因子认证过程,进一步增强了跨域身份认证系统的安全性;通过半可信代理者直接建立域间的信任关系,避免了复杂的证书路径构建和验证过程,减少了信任路径长度.基于计算性 Diffie-Hellman 问题和哈希函数的抗碰撞性,在标准模型下对新方案的强不可伪造性和完备性进行了证明.分析结果表明,文中的跨域身份认证方案具有匿名性、会话密钥的前/后向安全性、匿名的可控性等性质,并能抵抗重放攻击和替换攻击;在保留 PKI 技术优势的同时,简化了交互认证过程,提高了跨域身份认证效率,其性能更适用于大规模的云计算环境.

关键词 云计算;跨域身份认证;代理重签名;强不可伪造;标准模型

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2019.00756

Cross-Domain Authentication Scheme Based on Proxy Re-Signature in Cloud Environment

YANG Xiao-Dong[1),2)] AN Fa-Ying[2)] YANG Ping[2)] LIU Ting-Ting[2)] XIAO Li-Kun[2)] WANG Cai-Fen[2)]

[1)](*State Key Laboratory of Cryptology*, *Beijing* 100878)

[2)](*College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070)

Abstract Cloud computing is an emerging strategic industry that is currently experiencing extremely rapid development. However, cloud computing faces a number of critical security issues, which are the dominant factors restricting its growth. Identity authentication problem is the most serious of these security issues. In addition, identity authentication is the foundation of cloud

收稿日期:2016-12-11;在线出版日期:2017-07-09.本课题得到国家自然科学基金(61662069,61562077,61262057)、中国博士后科学基金(2017M610817)、甘肃省科技计划资助项目(145RJDA325,1506RJZA130)、国家档案局科技项目(2014-X-33)、甘肃省高等学校科研项目(2014-A011)、兰州市科技计划项目(2013-4-22)、西北师范大学青年教师科研能力提升计划项目(NWNU-LKQN-14-7)资助.**杨小东**,男,1981 年生,博士,副教授,中国计算机学会(CCF)会员,主要研究方向为云计算安全、密码学.E-mail:y200888@163.com.**安发英**,男,1991 年生,硕士研究生,主要研究方向为环签名、信息安全.**杨 平**,男,1993 年生,硕士研究生,主要研究方向为代理重签名、大数据安全.**刘婷婷**,女,1994 年生,硕士研究生,主要研究方向为隐私保护.**肖立坤**,男,1994 年生,硕士研究生,主要研究方向为代理签名.**王彩芬**,女,1963 年生,博士,教授,博士生导师,主要研究领域为密码学、数据安全.

computing security, which ensures the identities of users and cloud service providers, restricts the entry of unauthorized users from entering cloud systems and accessing cloud resources. At present, various cloud services are beginning to exhibit a trend of integration, in which an increasing number of cloud services become interconnected with cloud services in other trusted domains. Hence, cloud service providers require the implementation of cross-domain identity authentication mechanisms to authenticate the identities of users from other trusted domains. Most of the existing cloud computing platforms adopt the authentication mechanism of username/password combination, but there are two main disadvantages in this type of authentication method. One is the weak security performance, which is easily intercepted and monitored. Another is that if the user uses the same username and password on different platforms, then it is easy to cause disclosure of the user's identity information. Public key infrastructure (PKI) offers a feasible solution to address identity authentication problem in cloud computing environment. Moreover, PKI can provide identity authentication services, and it is well accepted as the current best mechanism to ensure security of open network environment. The main purpose of PKI is to confirm the exclusive, authenticity and the validity of each user identity information and to protect the security interests of various entities in cyberspace. Thus, PKI has been widely implemented in e-commerce, e-government, e-banking, and other fields. However, the existing PKI-based cross-domain authentication mechanism has serious deficiencies in its implementation, scalability, flexibility, interoperability and certificate validation, so it is difficult to be applied in cloud computing environment with high requirements such as extensibility, dynamics and openness. Specifically, the existing PKI-based cross-domain authentication mechanism has many problems such as long trust path, low efficiency of certificate verification, and complex inter-domain trust path construction. Therefore, a cross-domain authentication scheme in the cloud environment, which uses proxy re-signature technology, was proposed to realize bidirectional authentication between the user and cloud provider in this paper. Based on the legitimacy of the digital certificate and validity of the authentication message, the user and cloud provider can complete the authentication of identities of both parties and negotiate the session key during the authentication process. Furthermore, the dual-factor authentication process of "password+key" enhances the security of the cross-domain authentication system. In addition, the complicated certificate path construction and verification process could be avoided, and the length of the trust path can be reduced through direct establishment of an inter-domain relationship using a semi-trusted agent. The strong unforgeability and completeness of the proposed scheme are proved in the standard model based on the computational Diffie-Hellman problem and the collision-resistance property of hash function. Analysis results show that the proposed cross-domain authentication scheme has properties of anonymity, forward/backward security of session key, and controllability of anonymity, and it can resist replay and replacement attacks. Besides retaining the advantages of PKI technology, this scheme also simplifies the interactive authentication process and improves the efficiency of cross-domain authentication at the same time, and its performance is more suitable for large-scale cloud environment.

Keywords　cloud computing; cross-domain authentication; proxy re-signature; strong unforgeability; standard model

1　引　言

云计算将各种分布的计算、存储及应用资源进行整合，使其具有强大的计算能力和海量的数据存储能力，并有效地将各类资源以服务的形式提供给用户. 身份认证是云计算安全的基础，为用户和云服务提供商的身份真实性提供保证. 但由于云计算具

有超大规模、虚拟化、开放性等特点，使得传统的安全技术无法适应云计算环境的安全需求，因此迫切需要研究云计算环境下的身份认证技术，确保用户和云服务提供商身份的可信性和完整性[1-2].

当前各类云服务已开始呈现出整合趋势，越来越多的云服务需要与其它异域的云服务互联，云服务提供商利用跨域身份认证机制来识别异域用户身份. 在主流的身份认证技术中，“用户名/口令”组合认证是一种安全级别较低的认证方式，如果不同平台使用统一的用户名和密码，将造成用户身份信息的泄露，无法保证云环境下跨域身份认证的安全性[3-4]. 在基于 kerberos 协议的身份认证机制中，认证服务器和票据授权服务器很容易成为系统的性能瓶颈和安全瓶颈，并存在密钥存储管理复杂、用户信息泄露等问题[5]. 公钥基础设施 PKI(Public Key Infrastructure)是公认的保障网络社会安全的最佳体系，能在开放的网络环境中提供身份认证服务，确定信息网络空间中身份的唯一性、真实性和合法性，保护网络空间中各种主体的安全利益，已经广泛应用于电子商务、电子政务、网上银行等领域，也是目前云计算领域使用最广泛的身份认证机制[6]. 但现有基于 PKI 的跨域身份认证技术存在公钥证书验证效率低，域间信任路径构造复杂等问题. 基于身份密码体制的认证机制能有效解决公钥证书管理开销过大等问题，但存在密钥托管和用户公钥撤销等问题，在开放性的大规模云计算环境中应用具有一定的局限性[7]. 此外，如果每个信任域建立各自的身份鉴别机制，用户在不同信任域切换身份时将会出现用户身份的多重性，从而使云环境下的跨域身份认证变得异常复杂. 随着云计算的快速发展，跨域身份认证已经成为云计算领域亟待突破的重要问题，其重要性与紧迫性已不容忽视，因此有必要探索新方法来构建更加简单、高效且适用于云环境的跨域身份认证方案.

代理重签名[8]为研究面向云计算的跨域身份认证提供了一种新思路. 本文利用代理重签名具有转换签名的特性，将 PKI 认证体系与代理重签名相结合，提出一种适用于云计算环境的跨域身份认证方案. 如图 1 所示，当其它信任域的用户访问本域的云资源时，云服务提供商仅与半可信第三方直接建立联系，将异域用户的数字证书发送给第三方；利用不同信任域间的重签名密钥，半可信第三方将异域的用户证书转换为与云服务提供商属于同一信任域的用户新证书；云服务提供商通过用户新证书来确认异域访问用户身份的合法性，从而实现证书在不同信任域间的传递与跨域认证. 每个云用户通过一个合法的数字证书和半可信的第三方，实现跨域云资源的访问，不仅能提高证书验证的效率，还可避免重复认证带来的额外开销.

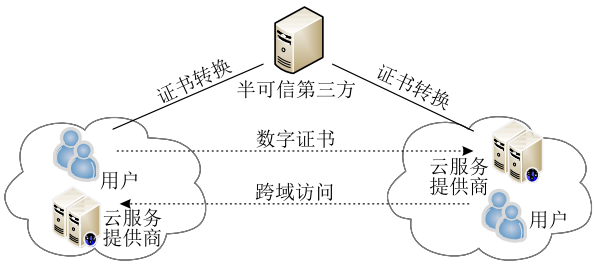

图 1 异域证书转换

1.1 相关工作

PKI 是基于公钥密码算法的安全基础服务设施，通过可信认证中心 CA(Certification Authority)签发的数字证书，将用户的身份信息和公钥进行绑定，利用 CA 对证书的签名实现用户身份与公钥的唯一对应关系. 在数字证书可信性的验证过程中，验证者需要构造一条连同通信双方的证书路径，并利用预先存储的根 CA 自签名证书来验证路径中的证书链，以确保证书持有者的身份和公钥的拥有权. 建立域间信任关系是实现跨域认证的前提，Sun[9]提出了基于严格二叉树的域间信任模型，但随着信任域规模的增大，证书路径长度也急剧增大. 文献[10]提出建设一个公共服务器的思想，所有 CA 在该服务器上注册全部服务资源访问地址，便于其它信任域的用户访问与查询. 文献[11]提出基于 XKMS 的域间信任建立方法，但需要一个完全可信的第三方提供证书的查询与验证等服务. 证书撤销是 PKI 体系可靠性的关键保障，文献[12]利用了单向广播信道传播证书撤销列表(Certificate Revocation List，CRL)具有及时、低成本等特点. 文献[13]改进了已有的证书撤销机制，并建议组合使用多种撤销方法来满足不同用户环境的安全需求. 但在现有基于 PKI/CA 的跨域身份认证技术中[6,9,11,13-14]，证书验证时需要从待验证书一直检测到根证书，层层递推，从而导致验证路径过长、路径验证效率较低，大大影响了跨域身份认证技术的应用范围.

PKI 具有提供强认证、适合大规模部署等优点，但面临数字证书的存储、分发和撤销等问题. 文献[15-17]提出了基于身份的直接匿名认证方案，但方案的计算效率较低，并且基于身份的方案存在密钥托管问题，无法避免密钥生成中心的恶意行为. 文

献[18-20]提出了基于无证书密码体制的云端用户身份认证方案，但未进行跨域认证方面的相关研究. 虽然这些方案以不同的方式验证用户身份的真实性，但存在用户身份的唯一性、用户公钥的撤销等问题，无法直接应用于大型的云计算平台.

代理重签名由 Blaze 等人[8]在 1998 年欧洲密码会议上提出，并由 Ateniese 等人[21]给出其规范的形式化安全定义. 在代理重签名中，半可信代理者利用重签名密钥将受托者的签名转换为委托者对同一个消息的签名，但无法单独代表受托者或委托者生成消息的合法签名. 所谓半可信，指的是仅仅相信代理者一定会按方案进行签名的转换. 国内外学者提出了一系列在随机预言模型下可证安全的代理重签名方案[21-23]，但当具体的哈希函数实例化随机预言机时，这些方案在现实中不一定是安全的. 由于标准模型下方案的安全性只依赖于困难问题假设以及哈希函数在现实中可以实现的特性[24]，所以在标准模型下可证明安全的代理重签名算法具有更加可靠的安全性. Shao 等人[25]构造了一个不依赖于随机预言机的代理重签名方案，然而 Kim 等人[26]发现该方案的重签名算法存在安全漏洞，并提出了一个改进方案. Yang 等人[27]提出了门限代理重签名方案，防止代理者滥用签名转换的权限. Tian[28]构造了基于格的代理重签名方案，用于抵抗量子计算的攻击. Yang 等人[29]提出了可分离的在线/离线代理重签名方案，有效改善了代理重签名的实时性. 为了降低验证者的计算开销，文献[30-31]分别构造了在随机预言模型和标准模型下安全的服务器辅助验证代理重签名方案. 然而，现有的代理重签名方案[8,21-32]几乎都满足存在性不可伪造性，只能确保攻击者无法伪造新消息的签名. Vivek 等人[33]提出了强不可伪造的双向代理重签名方案，但方案不满足多用性. 强不可伪造的代理重签名具有更强的安全性，能阻止攻击者对已经签名过的消息进行伪造签名，但相关的公开方案较少. 强不伪造的代理重签名能有效防止数字证书的篡改，更适用于构造跨域身份认证系统.

为满足云计算环境下跨域身份认证的安全需求，本文基于 CDH(Computational Diffie-Hellman)和 CRF(Collision Resistant Hash)假设，提出了一个标准模型下强不可伪造的服务器辅助验证代理重签名算法，将签名验证的大部分计算任务委托给服务器执行，验证者只需进行少量的计算便可完成签名的合法性验证，大大降低了签名验证算法的计算复杂度，在效率上优于已有的同类算法. 基于 PKI 认证体系和本文提出的代理重签名算法，构造了一个云计算环境下安全高效的跨域身份认证方案，完成用户与云服务提供商之间的双向身份认证，确保通信双方身份信息的真实性、合法性和可信性. 采用“口令＋密钥”的双因子认证过程，进一步提升了方案的安全性；引入临时身份和匿名数字证书，保证了访问用户在认证过程中的匿名性，同时对用户的恶意匿名行为具有可控性；建立基于半可信代理者的跨域身份认证信任模型，保留了 PKI 技术的优点，降低了 PKI 交互认证的复杂性，提高了跨域身份认证效率. 分析显示，本文的跨域身份认证方案能抵抗重放攻击和替换攻击，具有较高的计算性能和安全性能，使其更适用于云计算环境. 通过对相关领域的文献搜索，目前还没有关于基于服务器辅助验证代理重签名的跨域身份认证研究的公开文献.

1.2　本文结构

第 2 节介绍相关的预备知识；第 3 节给出强不可伪造的服务器辅助验证代理重签名算法；第 4 节提出云环境下的跨域身份认证方案；第 5 节分析方案的性能；第 6 节是总结.

2　预备知识

2.1　双线性映射

设 G_1 和 G_2 是阶为素数 p 的循环群，g 是 G_1 的一个生成元，若 $e:G_1\times G_1\rightarrow G_2$ 满足以下条件，则称 e 是一个双线性映射[21].

(1) 双线性：对任意的 $a,b\in Z_p^*$，满足 $e(g^a,g^b)=e(g,g)^{ab}$.

(2) 非退化性：$e(g,g)\neq 1_{G_2}$，这里 1_{G_2} 是 G_2 的单位元.

(3) 可计算性：对任意的 $g_1,g_2\in G_1$，存在一个有效的算法计算 $e(g_1,g_2)$.

2.2　安全性理论假设

本文方案的安全性基于 CDH(Computational Diffie-Hellman)假设和 CRH(Collision Resistant Hash)假设，具体定义如下.

群 G_1 上的 CDH 问题：给定三元组 $(g,g^a,g^b)\in G_1^3$，这里 $a,b\in Z_p^*$ 是未知的，计算 $g^{ab}\in G_1$.

定义 1(CDH 假设).　任何一个概率多项式时间算法 $\mathcal{B}$ 成功求解 CDH 问题的概率为 $Adv_{\mathrm{CDH}}(\mathcal{B})=\Pr[\mathcal{B}(g,g^a,g^b)=g^{ab}:g\in G_1,a,b\in Z_p^*]$，若 $Adv_{\mathrm{CDH}}(\mathcal{B})$ 是可忽略的，则称 G_1 上的 CDH 问题是困难的[24].

定义 2(CRH 假设). 假设一个抗碰撞的哈希函数族 $H_k:\{0,1\}^*\rightarrow\{0,1\}^{n_k}$,其中 k 是一个指标,n_k 是输出消息的长度.任何一个概率多项式时间算法 $\mathcal{B}$ 成功找到 H_k 的一对碰撞的概率为 $Adv_{\mathrm{CRH}}(\mathcal{B})=\Pr[\mathcal{B}(k)=(m_0,m_1):m_0\neq m_1,H_k(m_0)=H_k(m_1)]$,如果 $Adv_{\mathrm{CRH}}(\mathcal{B})$ 是可忽略的,则称 H_k 是抗碰撞的[34].

基于 CDH 假设,很容易构造抗碰撞的哈希函数[35].由于本文方案的哈希函数不需要模拟随机预言机,因此可使用标准的抗碰撞哈希函数,如 SHA-2、SHA-3 等.

2.3 安全模型

本文构造的跨域身份认证方案借鉴了双向服务器辅助验证代理重签名的思想,因此根据双向强不可伪造代理重签名[33]、服务器辅助验证代理重签名[30-31]的安全模型,本文方案的安全性主要考虑以下两类攻击:

(1)强不可伪造攻击:攻击者不能伪造一个新消息的签名,也不能伪造一个已进行过签名询问消息的签名.

(2)完备性攻击:攻击者具有签名密钥或重签名密钥,但无法让验证者确信一个非法签名是合法的.

3 强不可伪造的服务器辅助验证代理重签名算法

本节提出一个双向的服务器辅助验证代理重签名算法,允许半可信代理者 Proxy 将受托者 Alice 的签名转换为委托者 Bob 的签名,验证者 Verifier 借助具有强大计算能力的服务器完成签名的合法性验证.

(1)系统参数生成

令 G_1 和 G_2 分别是两个阶为素数 p 的循环群,g 是 G_1 的生成元,双线性映射 $e:G_1\times G_1\rightarrow G_2$.符号"$\|$"表示字符串的连接操作,$n_m$ 和 n_c 表示字符串的固定长度.选择两个抗碰撞的哈希函数 $H_1:\{0,1\}^*\rightarrow\{0,1\}^{n_c}$ 和 $H_2:\{0,1\}^*\rightarrow\{0,1\}^{n_m}$,这里 $n_m<p,n_c<p$,使得哈希函数的输出是 Z_p 中的一个元素.随机选择三个元素 $g_2,g_3,u\in G_1$,并在 G_1 中随机选择 n_m 个元素 $(u_1,\cdots,u_{n_m})$,公开系统参数 $cp=(G_1,G_2,p,e,g,g_2,g_3,u,\{u_i\}_{i=1}^{n_m},H_1,H_2)$.

(2)密钥生成

随机选择 $a\in Z_p^*$ 作为私钥 sk,计算对应的公钥 $pk=g^a$.

(3)重签名密钥生成

给定 Alice 的私钥 $sk_A=\alpha$ 和 Bob 的私钥 $sk_B=\beta$,使用文献[21]的安全通信协议为 Proxy 生成一个重签名密钥 $rk_{A\rightarrow B}=g_2^{\beta-\alpha}$.

(4)签名

对于消息 $m\in\{0,1\}^*$,受托者 Alice 随机选择 $s\in Z_p$,计算 $M=H_2(m)=(M_1,\cdots,M_{n_m})\in\{0,1\}^{n_m}$,$\varpi=u\prod_{i=1}^{n_m}(u_i)^{M_i}$ 和 $h=H_1(m\|g^s)$,用私钥 $sk_A=\alpha$ 生成消息 m 的签名 $\sigma_A=(\sigma_{A,1},\sigma_{A,2})=((g_2)^{sk_A}(\varpi g_3^h)^s,g^s)=(g_2^{\alpha}(\varpi g_3^h)^s,g^s)$.

(5)重签名

给定 Alice 的公钥 pk_A,消息 m 和签名 $\sigma_A=(\sigma_{A,1},\sigma_{A,2})$,如果 Proxy 验证 σ_A 不是一个对应于 pk_A 关于 m 的合法签名,输出 $\perp$;否则利用重签名密钥 $rk_{A\rightarrow B}=g_2^{\beta-\alpha}$,生成一个对应于公钥 pk_B 关于消息 m 的重签名 $\sigma_B=(\sigma_{B,1},\sigma_{B,2})=(rk_{A\rightarrow B}\sigma_{A,1},\sigma_{A,2})$.

(6)签名验证

给定公钥 pk 和消息 m 的签名 $\sigma=(\sigma_1,\sigma_2)$,验证者 Verifier 计算 $M=H_2(m)\in\{0,1\}^{n_m}$,$\varpi=u\prod_{i=1}^{n_m}(u_i)^{M_i}$ 和 $h=H_1(m\|\sigma_2)$,并验证等式 $e(\sigma_1,g)=e(g_2,pk)e(\varpi g_3^h,\sigma_2)$ 是否成立.如果等式成立,输出 1;否则输出 0.

(7)服务器辅助验证参数生成

验证者 Verifier 随机选择 $x\in Z_p^*$,计算 $K_0=g_2^x$,秘密保存 $VString=(x,K_0)$.

(8)服务器辅助验证协议

给定一个公钥 pk 和一个消息签名对 $(m,\sigma=(\sigma_1,\sigma_2))$,验证者 Verifier 和服务器之间的交互协议如下:

① Verifier 计算 $h=H_1(m\|\sigma_2)$ 和 $\sigma'=(\sigma_1',\sigma_2')=((\sigma_1)^x,(\sigma_2)^x)$,将 (m,h,σ') 发送给服务器.

② 收到 (m,h,σ') 后,服务器计算 $K_1=e(\sigma_1',g)$ 和 $K_2=e(\varpi g_3^h,\sigma_2')$,并将 (K_1,K_2) 返回给 Verifier.

③ Verifier 利用 $VString=(x,K_0)$ 验证等式 $K_1=e(K_0,pk)K_2$ 是否成立.若等式成立,Verifier 相信 σ 是一个合法签名,输出 1;否则输出 0.

算法的正确性分析过程如下:

(1)重签名的正确性

对于Alice的签名 $\sigma_A=(\sigma_{A,1},\sigma_{A,2})=(g_2^{\alpha}(\varpi g_3^h)^s,g^s)$ 和重签名密钥 $rk_{A\rightarrow B}=g_2^{\beta-\alpha}$,则重签名 $\sigma_B=(\sigma_{B,1},\sigma_{B,2})=(rk_{A\rightarrow B}\sigma_{A,1},\sigma_{A,2})=(g_2^{\beta-\alpha}(g_2^{\alpha}(\varpi g_3^h)^s),g^s)=(g_2^{\beta}(\varpi g_3^h)^s,g^s)$,于是有 $e(\sigma_{B,1},g)=e(g_2^{\beta}(\varpi g_3^h)^s,$

$g)=e(g_2,g^{\beta})e(\varpi g_3^h,g^s)=e(g_2,pk_B)e(\varpi g_3^h,\sigma_{B,2})$. 如果签名 σ_A 和重签名密钥 $rk_{A\to B}$ 是合法有效的，则重签名算法生成的 σ_B 满足签名验证等式.

(2) 服务器辅助验证签名的正确性

若重签名 $\sigma_B=(\sigma_{B,1},\sigma_{B,2})=(g_2^{\beta}(\varpi g_3^h)^s,g^s)$ 和 $VString=(x,K_0=g_2^x)$，则 $\sigma'_B=(\sigma'_{B,1},\sigma'_{B,2})=((\sigma_{B,1})^x,(\sigma_{B,2})^x)=((g_2^{\beta}(\varpi g_3^h)^s)^x,(g^s)^x)=(g_2^{\beta x}(\varpi g_3^h)^{sx},g^{sx})$，$h=H_1(m\|\sigma_{B,2})$，$K_2=e(\varpi g_3^h,\sigma'_2)=e(\varpi g_3^h,g^{sx})$，于是有

$$K_1=e(\sigma'_1,g)=e(g_2^{\beta x}(\varpi g_3^h)^{sx},g)$$
$$=e(g_2^x,g^{\beta})e(\varpi g_3^h,g^{sx})=e(K_0,pk_B)K_2.$$

从上面推导过程可知，如果 $VString$ 不公开，则服务器无法让验证者确信一个非法签名是合法的.

4　基于代理重签名的跨域身份认证新方案

4.1　跨域身份认证信任模型

如图 2 所示为本文方案基于半可信代理者的跨域身份认证信任模型，主要包括 4 个参与实体. (1) 认证中心 CA. 负责所管辖信任域内证书的申请、审批、颁发、撤销、查询、CRL 的发布与管理等；(2) 半可信代理者 Proxy. 拥有域间的重签名密钥，能够将一个信任域内的合法证书转换为另外一个信任域的证书，直接建立域间信任关系，实现证书在不同信任域间的传递与认证；(3) 云服务提供商 Server. 为用户提供各种云服务，并使用 TPM(Trusted Platform Module)安全芯片进行密钥和证书等敏感数据的存储、数据加密与签名等；(4) 用户 User. 利用支持便携式 TPM(Portable TPM，PTPM)安全模块的任意终端设备访问云服务，并完成与云服务提供商之间的跨域身份认证过程. TPM 和 PTPM 能确保身份

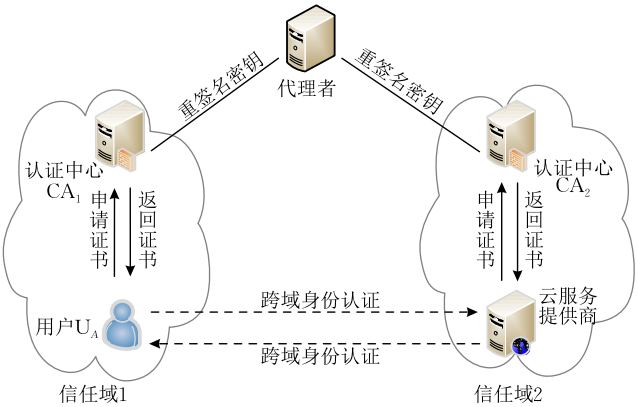

图 2　跨域身份认证信任模型

认证的可信性和认证结果的正确性；通过数字证书的合法性来鉴别双方身份的真实性，并利用证书获取对方的正确公钥.

4.2　方案描述

为了便于描述，假设任意两个可信域分别为信任域 1 和信任域 2，CA_1 是信任域 1 的认证中心，CA_2 是信任域 2 的认证中心，Proxy 是负责两个信任域之间证书转换的半可信代理者，U_A 是信任域 1 中的任意一个用户，$Server_B$ 是信任域 2 中的任意一个云服务提供商；以 U_A 访问 $Server_B$ 的跨域资源为例，通过持有的数字证书完成两者之间的双向身份认证. 每个信任域部署独立的 PKI 系统，其结构示意图如图 3 所示.

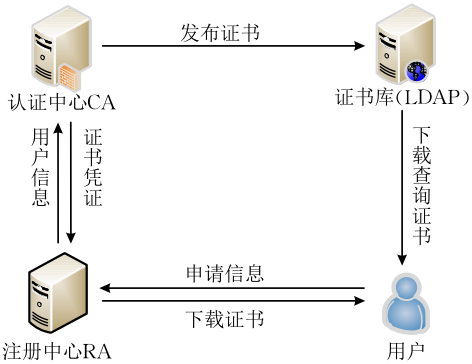

图 3　PKI 的基本构成及结构示意图

在 PKI 系统中，注册中心 RA(Registry Authorit)主要负责审核本区域用户身份信息的真实性，管理用户的数字证书及受理各种 PKI 服务(如证书的吊销、更新等)，并将合法的申请信息上传到认证中心. 认证中心 CA 是 PKI 系统的核心，主要负责签发用户的数字证书，发布本信任域的 PKI 策略及证书撤销列表，授权代理者实现与其他认证中心的交叉认证等. 用户通过轻量级目录访问协议 LDPA(Lightweight Directory Access Protocol)来访问证书库，可下载、查询用户的数字证书.

HMAC(keyed-Hashed for Message Authentication Code)[36]是一种将密钥和哈希函数相结合的消息认证码算法，具有速度快、实现效率高且易于改进等特点，其安全性主要取决于所关联哈希函数的安全性，并作为身份认证模块广泛应用于 IPSec、WTLS 等安全协议. 本方案的重复跨域认证过程采用 HMAC 算法代替签名算法，可以减少认证的计算开销和通信开销.

4.2.1　系统建立

与第 3 节的系统参数生成算法相同，产生系统参数 $cp=(G_1,G_2,p,e,g,g_2,g_3,u,\{u_i\}_{i=1}^{n_m},H_1,$

H_2). 定义 $Enc()$和 $Dec()$为一个公钥加密/解密算法(如 ECC 等),$E()$和 $D()$为一个对称加密/解密算法(如 AES 等). 认证中心 CA_1 随机选择 $a_1 \in Z_p^*$ 作为私钥 sk_{CA_1},计算公钥 $pk_{CA_1}=g^{a_1}$. 与 CA_1 生成密钥的过程相似,CA_2 的公私钥对表示为(pk_{CA_2},sk_{CA_2}),U_A 的公私钥对为(pk_A,sk_A),$Server_B$ 的公私钥对为(pk_B,sk_B). 用 ID_A 和 TID_A 分别表示用户 U_A 的真实身份标识和临时身份标识,ID_P 是代理者 Proxy 的身份标识,ID_B 表示云服务提供商 $Server_B$ 的身份标识. 为了解决单个代理者转换证书的性能瓶颈问题,认证中心可以授权多个代理者进行异域证书的转换,如图 4 所示. 由于每个代理者具有相同的代理重签名密钥,彼此之间相互独立且互不影响,这种平行授权方式使得每个代理者具有相同的转换证书权限,因此本文仅讨论基于单个代理者的跨域身份认证方案,很容易推广到多个代理者的情形,并能保留单个代理者的所有安全性能.

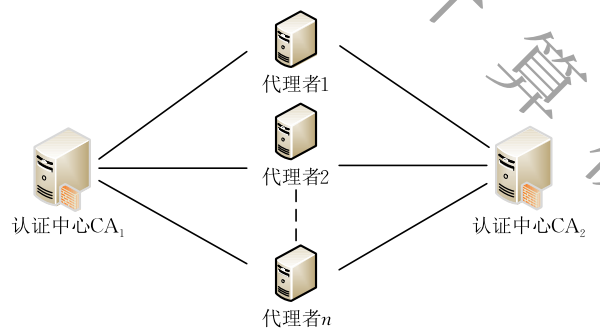

图 4 认证中心授权多个代理者进行证书转换

假设认证中心和代理者之间有安全的通信信道,代理者 Proxy 运行第 3 节的重签名生成算法,生成认证中心 CA_1 和 CA_2 之间的重签名密钥 $rk_{CA_1\to CA_2}=(g_2)^{sk_{CA_2}-sk_{CA_1}}$,具体过程如下:(1) Proxy 随机选择 $r_k \in Z_p^*$,计算并发送 $R_k=g^{r_k}$ 给 CA_1;(2) CA_1 通过私钥 sk_{CA_1} 计算并发送 $R_{k1}=R_k g_2^{sk_{CA_1}}$ 给 CA_2;(3) CA_2 利用私钥 sk_{CA_2} 计算 $R_{k2}=g_2^{sk_{CA_2}}/R_{k1}$,将 R_{k2} 返回给 Proxy;(4) Proxy 计算自己的重签名密钥 $rk_{CA_1\to CA_2}=R_k R_{k2}=g_2^{sk_{CA_2}-sk_{CA_1}}$.

4.2.2 证书申请

访问用户和云服务提供商向各自所属的认证中心完成数字证书的申请,具体过程如图 5 所示.

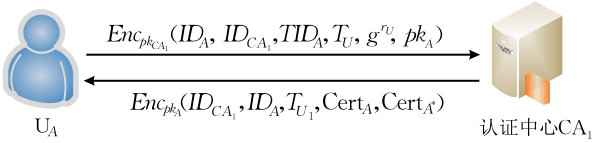

图 5 数字证书申请流程

(1) 用户 U_A 随机选择参数 $r_U \in Z_p^*$,利用真实身份 ID_A 计算临时身份 $TID_A=H_1(ID_A \| g^{r_U})$;通过 LDAP 从证书库下载安装所属认证中心 CA_1 的自签名根证书,并提取 CA_1 的公钥 pk_{CA_1};读取本地时间戳 T_U 和公钥 pk_A,发送证书申请信息 $Enc_{pk_{CA_1}}(ID_A, ID_{CA_1}, TID_A, T_U, g^{r_U}, pk_A)$ 给 CA_1.

(2) CA_1 用私钥 sk_{CA_1} 解密 U_A 发送的申请信息,首先根据 ID_A 等信息验证 U_A 是否为本域的合法用户,然后在已注册用户信息表中查询 ID_A 是否已注册,验证等式 $TID_A=H_1(ID_A \| g^{r_U})$ 是否成立,并检查时戳 T_U 的新鲜性. 如果 U_A 已注册或以上验证有一项未通过,则 CA_1 将申请失败的消息返回给 U_A;否则,CA_1 运行第 3 节的签名算法,随机选择 $s_{CA_1\to A} \in Z_p$,生成由颁发者 CA_1、证书有效起始日期 T_{begin} 和终止日期 T_{end}、使用者 TID_A、公钥 pk_A 等构成的证书信息 $m_{CA_1\to A}$,计算 $M_{CA_1\to A}=H_2(m_{CA_1\to A})=(M_{CA_1\to A,1},\cdots,M_{CA_1\to A,n_m}) \in \{0,1\}^{n_m}$,$\varpi=u\prod_{i=1}^{n_m}(u_i)^{M_{CA_1\to A,i}}$ 和 $h=H_1(m_{CA_1\to A} \| g^{s_{CA_1\to A}})$,用 CA_1 的私钥 sk_{CA_1} 生成证书消息 $m_{CA_1\to A}$ 的签名 $\sigma_{CA_1\to A}=(\sigma_{CA_1\to A,1},\sigma_{CA_1\to A,2})=((g_2)^{sk_{CA_1}}(\varpi g_3^h)^{s_{CA_1\to A}}, g^{s_{CA_1\to A}})$,并基于 X.509 等证书格式为用户 U_A 签发一个匿名证书 $Cert_A=\{TID_A, pk_A, T_{begin}, T_{end}, m_{CA_1\to A}, \sigma_{CA_1\to A}, ID_{CA_1}\}$. 虽然匿名证书 $Cert_A$ 隐藏了用户的真实身份 ID_A,但为了提升用户身份的匿名强度,可设置匿名证书 $Cert_A$ 的有效期比较短. CA_1 根据 U_A 的真实身份 ID_A 和 pk_A 等信息签发实名证书 $Cert_{A^*}=\{ID_A, pk_A, T_{begin}^*, T_{end}^*, m_{CA_1\to A}^*, \sigma_{CA_1\to A}^*, ID_{CA_1}\}$,用于提升匿名证书的签发效率和避免 CA_1 重复审核用户的相关身份资料. 当认证中心通过实名证书确认用户身份的真实性后,可直接根据用户递交的新临时身份签发对应的新匿名证书.

CA_1 在已注册用户信息表中保存$\{ID_A, TID_A, g^{r_U}, pk_A\}$,读取时间戳 T_{U_1},并发送证书申请响应消息 $Enc_{pk_A}(ID_{CA_1}, ID_A, T_{U_1}, Cert_A, Cert_{A^*})$ 给 U_A.

(3) 用户 U_A 通过私钥 sk_{CA_1} 解密收到的响信息,检验时戳 T_{U_1} 的新鲜性,若用根证书 CA_1 的公钥 pk_{CA_1} 验证实名证书 $Cert_{A^*}$ 和匿名证书 $Cert_A$ 是合法的,则在 PTMP 中安全存储(pk_A,sk_A,$Cert_{A^*}$,$Cert_A$);否则,拒绝接受证书.

与上述 U_A 申请证书的过程相同,云服务提供商 $Server_B$ 获得 CA_2 签发的证书 $Cert_{B^*}$ 和 $Cert_B$.

4.2.3 跨域认证

用户出于保护自己的隐私,利用匿名证书向

云服务提供商证明其身份的真实性；但为了提升服务的品质和影响力，云服务提供商采用实名证书完成与远程用户的跨域身份认证，具体过程如图 6 所示.

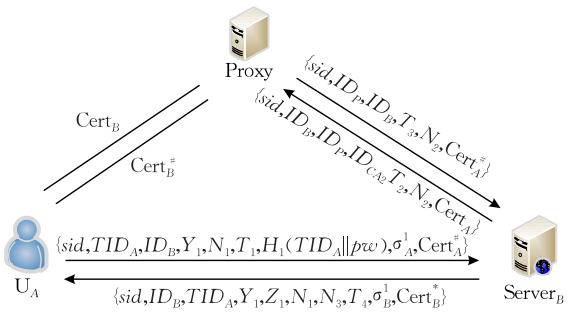

图 6　跨域身份认证流程

(1) 用户 U_A 选择一个口令值 pw，随机选取 y_1，$N_1 \in Z_p$，计算密钥协商参数 $Y_1 = g^{y_1}$；读取时间戳 T_1，令 $m_1 = (sid \| TID_A \| ID_B \| Y_1 \| N_1 \| T_1 \| H_1(TID_A \| pw))$，这里 sid 是会话标识；运行第 3 节的签名算法，随机选择 $s_A \in Z_p$，计算 $M_1 = H_2(m_1) = \{M_{1,i}\}_{i=1}^{n_m} \in \{0,1\}^{n_m}$，$h_1 = H_1(m_1 \| g^{s_A})$ 和 $\varpi_1 = u\prod_{i=1}^{n_m}(u_i)^{M_{1,i}}$，利用私钥 sk_A 生成消息 m_1 的签名 $\sigma_A^1 = (\sigma_{A,1}^1, \sigma_{A,1}^1) = ((g_2)^{sk_A}(\varpi_1 g_3^{h_1})^{s_A}, g^{s_A})$；读取临时身份证书 $Cert_A$，发送认证请求信息 $\{sid, TID_A, ID_B, Y_1, N_1, T_1, H_1(TID_A \| pw), \sigma_A^1, Cert_A\}$ 给云服务提供商.

(2) $Server_B$ 收到 U_A 的认证请求消息后，执行如下的验证操作.

① 在认证列表中查询是否存在 TID_A 的相关信息，如果存在，说明 U_A 是已经进行过身份认证的用户，直接执行重复跨域认证的相关操作；否则，转入步骤②进行首次身份认证.

② 检查时戳 T_1 的新鲜性，并从有效期、CRL 等方面对证书 $Cert_A$ 的状态进行有效性验证，如果证书过期或出现在证书撤销列表中，终止认证过程；否则转入步骤③验证 $Cert_A$ 中 CA_1 对证书签名的合法性.

③ 检查证书 $Cert_A$ 的颁发者是否与自己所属的认证中心 CA_2 相同，如果相同，说明 U_A 和 $Server_B$ 属于同一个信任域，则直接提取根证书 CA_2 的公钥 pk_{CA_2}，并对 $Cert_A$ 中的签名 $\sigma_{CA_1 \to A}$ 进行合法性验证；否则，转入步骤④进行异域证书转换操作.

④ 随机选择 $N_2 \in Z_p$，读取时间戳 T_2，发送证书转换信息 $\{sid, ID_B, ID_P, ID_{CA_2}, T_2, N_2, Cert_A\}$ 给代理者. 对于云服务提供商 $Server_B$ 发送的证书转换信息，代理者 Proxy 首先检查时戳 T_2 的新鲜性，然后利用 CA_1 的公钥 pk_{CA_1} 来验证 $Cert_A$ 的合法性，如果验证不通过，终止转换过程；否则，利用 CA_1 和 CA_2 之间的重签名密钥 $rk_{A\to B} = (g_2)^{sk_{CA_2} - sk_{CA_1}}$，将 $Cert_A$ 中 CA_1 对证书的签名 $\sigma_{CA_1 \to A} = (\sigma_{CA_1 \to A,1}, \sigma_{CA_1 \to A,2}) = ((g_2)^{sk_{CA_1}}(\varpi g_3^h)^{s_{CA_1 \to A}}, g^{s_{CA_1 \to A}})$ 转换为认证中心 CA_2 对证书的签名 $\sigma_{CA_2 \to A} = (\sigma_{CA_2 \to A,1}, \sigma_{CA_2 \to A,2}) = (rk_{A\to B}\sigma_{CA_1 \to A,1}, \sigma_{CA_1 \to A,2}) = ((g_2)^{sk_{CA_2}}(\varpi g_3^h)^{s_{CA_1 \to A}}, g^{s_{CA_1 \to A}})$，进一步基于证书格式将 CA_1 签发的证书 $Cert_A$ 转换为 CA_2 签发的临时证书 $Cert_A^{\sharp}$. 为了区分 $Cert_A^{\sharp}$ 是代理者转换的证书而不是 CA_2 自身签发的证书，可设置 $Cert_A^{\sharp}$ 的有效期非常短，并在证书的扩展项中添加代理者的身份标识 ID_P 等标记信息. 由于认证中心 CA_1 和 CA_2 都是可信赖的、公正的第三方机构，因此代理者无法联合任何一个认证中心发起合谋攻击. 由第 3 节的重签名生成算法可知，代理者 Proxy 不能单独通过重签名密钥 $rk_{CA_1 \to CA_2} = g_2^{sk_{CA_2} - sk_{CA_1}}$ 计算出认证中心的私钥 sk_{CA_1} 或 sk_{CA_2}，因而无法代替认证中心 CA_1 和 CA_2 签发合法的数字证书；重签名算法 $\sigma_B = (\sigma_{B,1}, \sigma_{B,2}) = (rk_{A\to B}\sigma_{A,1}, \sigma_{A,2})$ 确保了代理者只能转换已有的异域合法数字证书，不能独立生成新的数字证书，并且对已有用户证书信息的任意修改都无法通过证书的合法性验证. 因此，代理者转换用户原始证书所生成的临时数字证书，不会影响认证中心 CA_1 和 CA_2 的权威性.

Proxy 读取时间戳 T_3，发送证书转换响应信息 $\{sid, ID_P, ID_B, T_3, N_2, Cert_A^{\sharp}\}$ 给 $Server_B$.

⑤ $Server_B$ 检查证书转换响应消息中的 N_2 是否与证书转换消息中的随机数相同，如果不一致，终止认证过程；否则检查时戳 T_3 的新鲜性，并运行第 3 节的签名验证算法，提取根证书 CA_2 的公钥 pk_{CA_2} 来验证临时转换证书 $Cert_A^{\sharp}$ 中签名 $\sigma_{CA_2 \to A} = (\sigma_{CA_2 \to A,1}, \sigma_{CA_2 \to A,2})$ 的正确性，即计算

$$e(\sigma_{CA_2 \to A,1}, g) = e(g_2, pk_{CA_2})e(\varpi g_3^h, \sigma_{CA_2 \to A,2})$$

是否成立. 如果等式成立，说明 $Cert_A^{\sharp}$ 是合法的临时证书，$Server_B$ 接受用户 U_A 的身份证书 $Cert_A$，进入步骤⑥验证签名 σ_A^1 的合法性；否则，终止认证过程.

⑥ 提取证书 $Cert_A$ 中 U_A 的公钥 pk_A，计算 $m_1 = (sid \| TID_A \| ID_B \| Y_1 \| N_1 \| T_1 \| H_1(TID_A \| pw))$，验证 $e(\sigma_{A,1}^1, g) = e(g_2, pk_A)e(\varpi_1 g_3^{h_1}, \sigma_{A,2}^1)$ 是否成立，如果等式不成立，终止认证过程；否则，说明 U_A 的签名 σ_A^1 是有效的，完成对 U_A 的匿名身份认证，并

在认证列表中保存$\{TID_A, H_1(TID_A \| pw), \mathrm{Cert}_A, Num1, Date1\}$，其中 $Num1$ 和 $Date1$ 分别是 U_A 重复跨域认证的次数和有效时间，并进入步骤⑦发送响应消息.

⑦ 随机选择 $z_1, N_3 \in Z_p$，计算密钥协商参数 $Z_1 = g^{z_1}$；在 TPM 中提取证书 Cert_B^* 和对应的私钥 sk_B，读取时间戳 T_4，令 $m_2 = (sid \| ID_B \| TID_A \| Y_1 \| Z_1 \| N_3 \| T_4))$，运行第 3 节的签名算法，通过私钥 sk_B 生成 m_2 的签名 $\sigma_B^1 = (\sigma_{B,1}^1, \sigma_{B,2}^1)$；发送认证响应信息$\{sid, ID_B, TID_A, Y_1, Z_1, N_1, N_3, T_4, \sigma_B^1, \mathrm{Cert}_B^*\}$给 U_A，并计算与 U_A 之间的会话密钥 $K_1 = (pk_A)^{sk_B}(Y_1)^{z_1} = g^{sk_A sk_B + y_1 z_1}$.

(3) 用户 U_A 检查认证响应消息中的 N_1 是否与认证请求消息中的随机数相同，如果不一致，终止认证过程；否则，与上述 Server_B 验证 U_A 身份的过程相同，U_A 基于证书 Cert_{B^*} 和签名 σ_B^1 来验证 Server_B 身份的真实性，以确认 Server_B 是其议定的云服务提供商；U_A 完成云服务提供商的身份认证后，在认证列表中保存$\{ID_B, \mathrm{Cert}_B^*\}$，并计算会话密钥 $K_1 = (pk_B)^{sk_A}(Z_1)^{y_1}$.

由于用户 U_A 的计算能力有限，因此 U_A 可运行第 3 节的服务器辅助验证协议，委托一个云端服务器去执行验证签名 σ_B^1 合法性的大部分计算任务，降低用户的计算负载.

4.2.4 重复跨域认证

当用户与云服务提供商间的首次跨域身份认证完成后，后续的身份认证将不再重复发送数字证书和签名信息，通过 HMAC 算法实现双方身份的真实性认证，具体过程如图 7 所示.

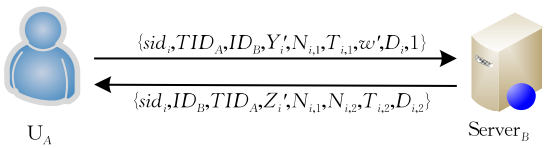

图 7 重复跨域认证流程

(1) 用户 U_A 从证书 Cert_B^* 中提取云服务提供商 Server_B 的公钥 pk_B；随机选择 $y_i, N_{i,1} \in Z_p$，计算密钥协商参数 $Y_i = g^{y_i}$ 和 $Y_i' = (pk_B)^{y_i}$；读取时间戳 $T_{i,1}$，输入口令值 pw，令 $k = (pk_B)^{sk_A} = g^{sk_A sk_B}$，计算 $w' = H_1(TID_A \| pw)$ 和 $D_{i,1} = HMAC_k(sid_i \| TID_A \| ID_B \| Y_i \| Y_i' \| N_{i,1} \| T_{i,1} \| w')$，这里 sid_i 是会话标识，发送重复认证请求信息$\{sid_i, TID_A, ID_B, Y_i', N_{i,1}, T_{i,1}, w', D_{i,1}\}$给云服务提供商 Server_B.

(2) Server_B 收到重复认证请求信息后，进行如下的身份认证操作.

① 检查时戳 $T_{i,1}$ 的新鲜性，根据 TID_A 在认证列表中查找$\{TID_A, H_1(TID_A \| pw), \mathrm{Cert}_A, Num1, Date1\}$，并判断存储的 $H_1(TID_A \| pw)$ 与收到的哈希函数值 w' 是否相同，若不同，则返回口令错误信息给 U_A.

② 计算 $Y_i = (Y_i')^{1/sk_B} = ((pk_B)^{y_i})^{1/sk_B} = ((g^{sk_B})^{y_i})^{1/sk_B} = g^{y_i}$；从 U_A 的证书 Cert_A 中提取公钥 pk_A，计算 $k = (pk_A)^{sk_B} = g^{sk_A sk_B}$ 和 $D_{i,1}' = HMAC_k(sid_i \| TID_A \| ID_B \| Y_i \| Y_i' \| N_{i,1} \| T_{i,1} \| w')$，验证 $D_{i,1}'$ 与收到的 $D_{i,1}$ 是否相等，如果不相等，则跨域重复认证失败.

③ 基于 $Num1$ 和 $Date1$ 检查认证信息的有效性，如果跨域认证次数 $Num1$ 大于规定的最大值或当前时间已超过有效时间 $Date1$，则终止认证过程.

如果以上 3 种情况都成立，则说明 Server_B 完成了对 U_A 的身份认证，即 U_A 是身份合法且可信的访问用户；更新 $Num1 = Num1 + 1$，并随机选择 $z_i, N_{i,2} \in Z_p$，计算密钥协商参数 $Z_i = g^{z_i}$ 和 $Z_i' = (pk_A)^{z_i}$；读取时间戳 $T_{i,2}$，计算 $D_{i,2} = HMAC_k(sid_i \| ID_B \| TID_A \| Y_i \| Z_i \| Z_i' \| N_{i,2} \| T_{i,2})$，发送重复认证响应信息$\{sid_i, ID_B, TID_A, Z_i', N_{i,1}, N_{i,2}, T_{i,2}, D_{i,2}\}$给 U_A，计算与 U_A 之间的会话密钥 $K_i = (pk_A)^{sk_B}(Y_i)^{z_i} = g^{sk_A sk_B + y_i z_i}$.

(3) U_A 收到认证响应消息后，检查时戳 $T_{i,2}$ 的新鲜性，判断 $N_{i,1}$ 是否与发送的随机数相同，计算 $Z_i = (Z_i')^{1/sk_A}$ 和 $D_{i,2}' = HMAC_k(sid_i \| ID_B \| TID_A \| Y_i \| Z_i \| Z_i' \| N_{i,2} \| T_{i,2})$，验证 $D_{i,2}'$ 与收到的 $D_{i,2}$ 是否相等. 如果以上验证都成功通过，则 U_A 完成了对 Server_B 的身份真实性验证，即 Server_B 是其议定的云服务提供商，并计算本次通信的会话密钥 $K_i = k \cdot (Z_i)^{y_i} = (pk_B)^{sk_A}(Z_i)^{y_i}$.

4.2.5 口令更新

假设 U_A 与 Server_B 经过身份认证后协商的会话密钥为 $K_i = g^{sk_A sk_B + y_i z_i}$，$U_A$ 持有密钥协商参数 $Y_i = g^{y_i}$，Server_B 持有密钥协商参数 $Z_i = g^{z_i}$. 如果 U_A 需要将口令 pw 更新为 pw'，则 U_A 首先读取时间戳 $T_{i,3}$，然后计算 $w_U' = H_1(TID_A \| pw')$，$k = (pk_B)^{sk_A} = g^{sk_A sk_B}$ 和 $D_{i,3} = HMAC_k(TID_A \| ID_B \| T_{i,3} \| w_U')$，最后给 Server_B 发送口令更新消息 $E_{K_i}(TID_A, ID_B, T_{iw}, w_U', D_{i,3})$. 云服务提供商 Server_B 用 K_i 解密

口令更新消息后，检查时戳 $T_{i,3}$ 的新鲜性，计算 $D'_{i,3}=HMAC_k(TID_A \| ID_B \| T_{i,3} \| w'_U)$，并验证 $D'_{i,3}$ 与收到的 $D_{i,3}$ 是否相等. 如果以上验证均成功通过，则在认证列表中查找 TID_A 对应的数据项 $\{TID_A, H_1(TID_A \| pw), \mathrm{Cert}_A, Num1, Date1\}$，并将 $H_1(TID_A \| pw)$ 替换为 $w'_U=H_1(TID_A \| pw')$.

5　方案分析

5.1　安全性分析

在本文提出的跨域身份认证方案中，证书申请阶段和跨域认证阶段的安全性取决于第 3 节提出的服务器辅助验证代理重签名算法；由于文献[36]已证明了 HMAC 算法的安全性，因此重复跨域阶段的安全性依赖于 HMAC 算法的密钥值 $k=g^{sk_A sk_B}$，而 k 的安全性取决于用户和云服务提供商之间利用服务器辅助验证代理重签名算法完成的首次跨域身份认证过程. 因此，如果攻击者能攻破第 3 节提出的服务器辅助验证代理重签名算法的安全性，则可攻破本文跨域身份认证方案的安全性. 针对第 2.3 节给出的两种攻击类型，将从强不可伪造性和完备性两个方面分析本文方案的安全性.

定理 1.　如果 CDH 假设和 CRH 假设成立，则本文方案在标准模型下是强不可伪造的.

定理 2.　本文新方案能抵抗服务器和签名者或代理者的合谋攻击，并在自适应性选择消息攻击下是完备的.

定理 1 和定理 2 的具体证明过程详见附录 1.

下面对方案基于的服务器辅助验证代理重签名算法、信任模型及跨域身份认证方案进行性能分析. 假设所有方案选择相同的群 G_1 和 G_2，阶为相同的素数 p. 由于乘法、加法、HMAC 算法及哈希函数的计算量相对比较小，因此下面的计算开销只考虑计算量较大的双线性对和指数运算. 用 Exp 表示一次指数运算，Pa 表示一次双线性对运算，Enc 表示运行一次公钥密码体制的加密算法，Dec 表示运行一次公钥密码体制的解密算法，Ver 表示运行一次签名验证算法，$|p|$ 表示 Z_p 中元素的长度，$|G_1|$ 和 $|G_2|$ 分别表示群 G_1 和 G_2 中元素的长度.

5.2　服务器辅助验证代理重签名算法的性能分析

文献[25-26,31-33]分别提出了标准模型下可证安全的代理重签名算法，下面将第 3 节给出的代理重签名算法与已有的 5 个算法进行计算开销和安全性能的比较，结果如表 1 所示.

表 1　代理重签名算法的计算开销与安全属性比较

方案	签名长度	重签名长度	签名算法的计算开销	重签名算法的计算开销	验证者的计算开销	多用性	强不可伪造
文献[25]算法	$2\|G_1\|$	$2\|G_1\|$	$3Exp$	$2Exp+3Pa$	$3Pa$	Yes	No
文献[26]算法	$2\|G_1\|$	$2\|G_1\|$	$3Exp$	$4Exp+3Pa$	$3Pa$	Yes	No
文献[31]算法	$2\|G_1\|$	$2\|G_1\|$	$3Exp$	$4Exp+2Pa$	$3Exp$	Yes	No
文献[32]算法	$2\|G_1\|$	$3\|G_1\|$	$2Exp$	$2Exp+2Pa$	$3Pa$	No	No
文献[33]算法	$2\|G_1\|+\|p\|$	$3\|G_1\|+\|p\|$	$4Exp$	$6Exp+3Pa$	$3Exp+5Pa$	No	Yes
本文新算法	$2\|G_1\|$	$2\|G_1\|$	$4Exp$	$Exp+3Pa$	$3Exp+Pa$	Yes	Yes

从表 1 可知，与文献[25-26,32-33]相比，本文新算法中验证者的计算开销最小；与文献[31]相比，本文新算法中验证者需要进行额外的一次双线性对运算，但文献[31]不满足强不可伪造性. 在以上 6 个算法中，只有本文新算法与文献[33]具有强不可伪造性，但文献[33]不满足多用性，导致其实用性较差；并且本文新算法具有更短的签名长度和重签名长度，重签名算法和验证者的计算开销也优于文献[33].

由于强不可伪造性能有效阻止代理者对用户数字证书的恶意篡改，因此下面对本文第 3 节所提出的新算法与文献[33]进行重签名生成的时间开销、验证者的时间开销与不同数量级长度消息的实验比较分析，结果如图 8 和图 9 所示. 本次实验运行的硬件环境：CPU 为英特尔酷睿 i7-6500 处理器，主频 2.5GHz，内存 8GB；软件环境：64 位的 Windows 10 操作系统和密码库 PBC-0.4.7-VC.

对于相同长度的签名消息，图 8 表明本文新算法生成重签名的时间开销低于文献[33]. 对于合法

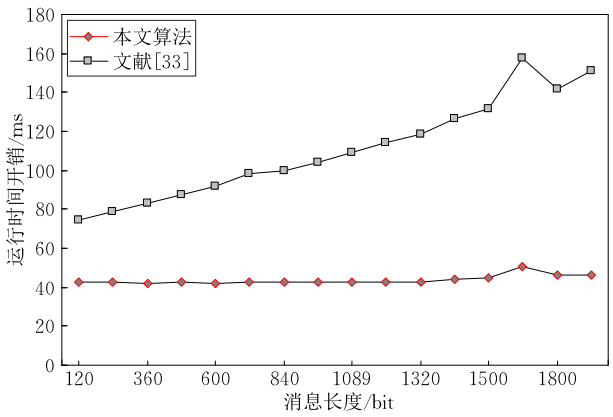

图 8　重签名生成的时间开销与消息长度关系

的原始签名，本文新算法执行群 G_1 上的一次乘法运算便可生成重签名. 当签名消息长度增大时，新算法生成重签名的时间开销增速也低于文献[33].

图 9 表明验证者在本文新算法中进行签名合法性验证的时间开销低于文献[33]，大大降低了验证者的计算开销；但随着消息长度的增加，验证者的时间开销增长速度比较缓慢.

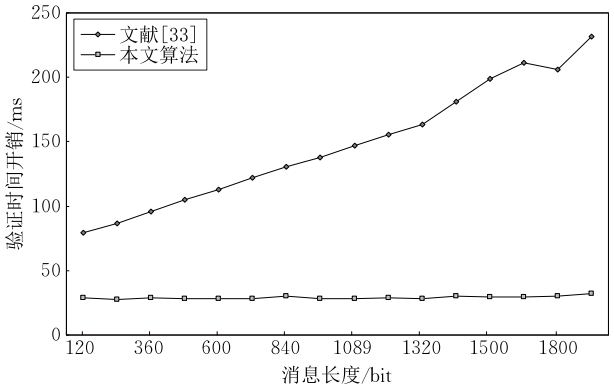

图 9 验证者的时间开销与消息长度关系

5.3 跨域身份认证方案的性能分析

由于云服务提供商具有强大的计算能力，下面对本文方案与文献[15-17]方案中用户的计算开销和消息交互轮数进行比较，结果如表 2 所示.

表 2 用户的计算开销与安全性能比较

方案	加入/申请证书阶段		首次跨域认证阶段		重复跨域认证阶段		标准模型	双因子认证
	计算开销	交换轮数	计算开销	交互轮数	计算开销	交互轮数		
文献[15]方案	$2Exp+Enc$	2	$7Exp+2Enc$	3	$7Exp+2Enc$	3	No	No
文献[16]方案	$3Exp+6Pa$	3	$8Exp+Pa$	4	$8Exp+Pa$	4	No	No
文献[17]方案	$3Exp$	2	$5Exp+Enc+Ver$	2	$2Exp+Enc+Ver$	2	No	No
本文新算法	$Exp+Enc+2Ver$	2	$6Exp+Ver$	4	$3Exp$	2	Yes	Yes

由表 2 可知，在加入/申请证书阶段，本文方案为了将用户的真实身份安全发送给云服务提供商，需要进行一次加密算法；为了验证由认证中心签发的实名证书和匿名证书的合法性，需要进行两次签名验证算法，但额外的运算能实现用户身份的隐私性，保留 PKI 技术的优点，使得新方案更适用于大规模的云计算环境. 在首次跨域身份认证阶段，新方案中用户与云服务提供商需要进行 2 轮的认证消息通信；为了验证云服务提供商的数字证书合法性，需要与代理者进行 2 轮的证书转换消息通信. 但由于申请证书和首次跨域身份认证过程是一次性的，因此这两个阶段产生的计算开销和通信开销对用户来说是可以接受的. 在重复跨域身份认证阶段，本文方案不需要运行加密算法和签名验证算法，也不需要进行证书的验证操作和复杂的双线性对运算，并且认证协议流程简洁，其性能全面优于对比方案. 此外，本文方案的安全性证明不依赖于理想的随机预言机，并且支持“口令＋密钥”的双因子认证过程，因此本文方案同时具有更好的安全性能.

为了衡量本文第 4 节所提出的跨域身份认证方案性能，下面对本文新方案与文献[17]中用户首次跨域认证的时间开销、重复跨域认证的时间开销、重复认证效率与不同数量级长度的消息进行实验分析比较，结果如图 10、图 11 和图 12 所示.

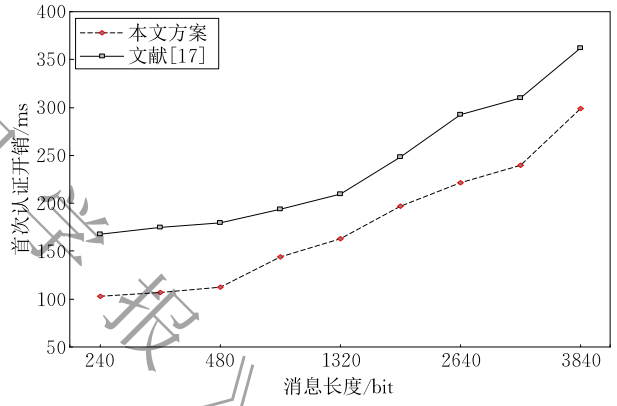

图 10 首次跨域认证的时间开销与消息长度关系

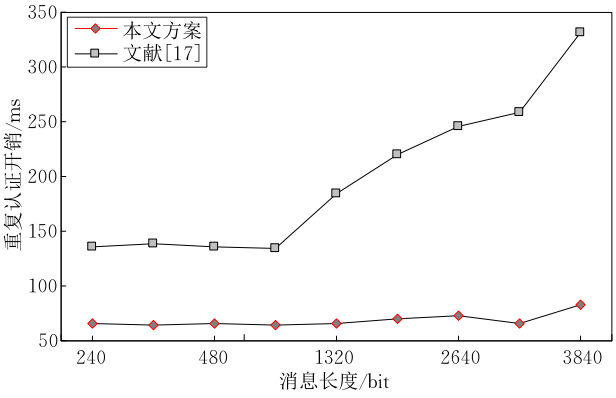

图 11 重复跨域认证的时间开销与消息长度关系

从图 10 可知，用户进行首次跨域身份认证时，由于两个认证方案都需要进行签名的生成算法与验证算法，所以身份认证时间开销随认证消息长度的

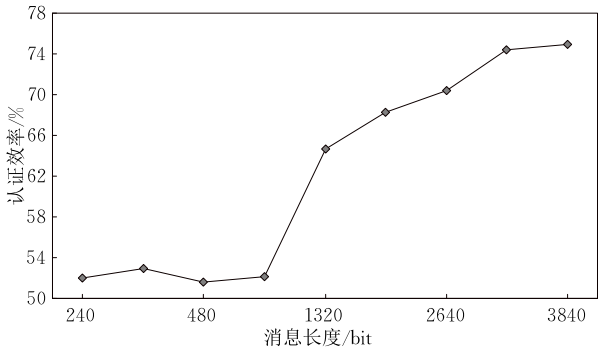

图 12　重复跨域身份认证效率与消息长度关系

增大而增大，但本文新方案不需要运行公钥加密算法（本次实验选取 ECC），使得首次跨域身份认证的时间开销低于文献[17].

在本文新方案的重复跨域认证阶段中，用 HMAC 算法代替签名算法，有效降低了认证的计算开销和通信开销. 图 11 表明用户在新方案中的重复跨域身份认证时间开销低于文献[17]，并且其增长速度趋于平稳.

从图 12 可知，本文新方案大大减少了用户的重复跨域认证时间开销，与文献[17]的跨域身份认证方案相比，新方案的重复跨域身份认证效率至少提高了 50%.

5.4　跨域身份认证信任模型的性能分析

将本文方案的信任模型与已有的 PKI 信任模型[3,9,11,14]进行性能对比分析，结果如表 3 所示.

表 3　信任模型的性能比较

方案	层次结构信任模型	交叉网状信任模型	混合型信任模型	桥 CA 信任模型	信任列表模型	本文信任模型
证书路径长度	较短	较长	较长	较短	较短	最短（长度仅为 1）
路径构造的复杂度	简单	复杂	简单	简单	简单	简单
证书管理维护	简单	复杂	复杂	复杂	复杂	简单
信任关系可信度	较高	较高	较高	较差	较差	较高
扩展新证书	较差	较好	较差	较差	较差	较好

从表 3 可知，本文的跨域身份认证方案通过一个半可信的代理者建立两个不同信任域间的直接信任关系，不存在复杂的信任路径构建和路径验证过程，证书路径长度仅为 1. 用户通过代理者将异域的用户证书转换为与自己属于同一信任域的新证书，用根 CA 的公钥直接进行新证书的合法性验证，从而完成异域用户的身份认证，不仅实现了“一个证书、全网通用”，降低证书管理和异域证书验证的复杂度，而且用户只信任本地域的根 CA，保证了用户之间的信任关系可信度比较高. 新加入的信任域只需与一个代理者相互认证并建立信任关系，即可与现有信任体系融合. 与已有的 PKI 信任模型相比，本文信任模型的证书路径长度、路径构造复杂度、证书验证效率等都与信任域的规模无关，因此本文信任模型具有更好的灵活性、健壮性和扩展性.

5.5　其他性能分析

（1）匿名的可控性

在首次跨域身份认证阶段，为了防止云服务提供商获取用户的真实身份 ID_A，用户使用匿名证书 Cert_A 替代实名证书 Cert_{A^*}；由于匿名证书包含了用户的临时身份、用户的公钥以及认证中心 CA_1 对证书的签名，因此匿名证书可以作为用户身份真实性鉴别的凭证. 在重复跨域身份认证阶段，使用临时身份 TID_A 实现用户身份的匿名性，云服务提供商通过 HMAC 值和临时身份/口令的哈希函数值来验证用户身份的真实性；只有成功完成首次跨域身份认证的用户，才能正确出示“临时身份/口令”的哈希函数值和 HMAC 函数的密钥值 k. 首次跨域身份认中用户的匿名性取决于匿名证书的有效时间，有效期越短则匿名性越强；重复跨域认证中用户的匿名强度取决于临时身份的新鲜性、允许重复认证消息的有效时间和最大次数.

如果云服务提供商 Server_B 收到用户 U_A 发送的虚假消息，则将 U_A 的临时身份 TID_A、匿名证书 Cert_A 和通信记录发送给认证中心 CA_1；CA_1 首先验证 Cert_A 的合法性和通信记录的有效性，然后根据 TID_A 在已注册用户信息列表中查找是否存在对应的数据项 $\{ID_A, TID_A, g^{r_U}, pk_A\}$，如果 $H_1(ID_A \| g^{r_U})$ 等于收到的 TID_A，则说明用户 U_A 发送了虚假消息，CA_1 将用户的匿名证书 Cert_A 和实名证书 Cert_{A^*} 同时添加到证书撤销列表 CRL 中，并将验证的结果反馈给云服务提供商. 因此，本文方案对访问用户的匿名行为是可控的，仅允许合法用户访问跨域云资源，能有效防止恶意用户行为的发生.

（2）会话密钥的前/后向安全性

本文方案在用户与云服务提供商实现双向身份认证的同时，完成了双方之间会话密钥的协商. 访问用户 U_A 拥有长期密钥 sk_A 和临时的密钥协商参数 y_i，云服务提供商 Server_B 拥有长期密钥 sk_B 和临时的密钥协商参数 z_i，只有双方共同参与才能生成会

话密钥 $K_i=g^{sk_A sk_B+y_i z_i}$. 此外,由于 y_i 和 z_i 均是随机选取的,因此会话密钥具有新鲜性和随机性. 如果攻击者截获了本轮会话密钥 K_i,不仅无法获取以前的会话密钥,也不能伪造后续的会话密钥,因此新方案的会话密钥满足前/后向安全性.

(3)抗重放、替换攻击

由于在身份认证消息和响应消息中均含有会话标识 sid_i,随机数 N_i 和时间戳 T_i,因此本文方案基于证书的合法性和消息的有效性验证,能够抵抗重放攻击.

在首次跨域身份认证阶段中,用户与云服务提供商的认证消息中都含有基于身份的签名和证书;在重复跨域身份认证阶段中,用户的认证消息绑定了临时身份和口令的哈希函数值 $H_1(TID_A \| pw)$,双方的认证消息中含有基于身份的 HMAC 值,并且 HMAC 算法的密钥值 $k=g^{sk_A sk_B}$ 与双方的长期密钥相关. 如果攻击者替换认证消息中的身份标识,则无法完成用户与云服务提供商间的双向身份认证. 因此,本文方案可抵抗替换攻击.

6 结论与下一步工作

本文基于 PKI/CA 认证体系,利用代理重签名提出了一种云环境下的跨域身份认证方案,并在标准模型下对新方案的强不可伪造性和完备性进行了证明. 访问用户与云服务提供商基于数字证书的合法性和认证消息的有效性,完成双方身份的真实性验证. 本文方案具有用户身份的匿名性及匿名的可控性、会话密钥的前/后向安全等特点的同时,能抵抗重放攻击和替换攻击. 分析结果表明,相对于传统的 PKI 信任体制,本文的跨域身份认证新方案在保留 PKI 技术的同时,具有更高的计算性能和安全性,适应云计算环境的安全需求. 然而,Shor[37] 已提出解决大整数分解和离散对数问题的量子多项式时间算法,本文方案的安全性基于计算 Diffie-Hellman 问题的困难性,因此新方案无法抵抗量子计算攻击. 下一步我们将在量子计算环境下,研究如何设计基于格或其他数学难题的跨域身份认证机制.

致 谢 感谢审稿专家和编辑老师的细致审阅!

参 考 文 献

[1] Feng Deng-Guo, Zhang Min, Zhang Yan, et al. Study on cloud computing security. Journal of Software, 2011, 22(1): 71-83(in Chinese)
(冯登国,张敏,张妍等. 云计算安全研究. 软件学报, 2011, 22(1): 71-83)

[2] Zhang Yu-Qing, Wang Xiao-Fei, Liu Xue-Feng, et al. Survey on cloud computing security. Journal of Software, 2016, 27(6): 1328-1348(in Chinese)
(张玉清,王晓菲,刘雪峰等. 云计算环境安全综述. 软件学报, 2016, 27(6): 1328-1348)

[3] He Song. Design and Implementation of Multi-Domain Unified Authentication and Authorization System Based on PKI [M. S. dissertation]. Beijing University of Posts and Telecommunications, Beijing, 2013(in Chinese)
(合松. 基于 PKI 的多域统一认证与授权系统设计与实现[硕士学位论文]. 北京邮电大学, 北京, 2012)

[4] Yassin A A, Jin H, Ibrahim A, et al. Cloud authentication based on anonymous one-time password//Proceedings of the International Conference on Ubiquitous Information Technologies and Applications, Da Nang, Vietnam, 2013: 423-431

[5] Ding Lin-Hua, Wang Jiu-Ru, Wang Xiao-Jie. Research on unified authentication model based on the kerberos and SAML//Proceedings of the 2015 International Conference on Advances in Mechanical Engineering and Industrial Informatics. Zhengzhou, China, 2015: 1053-1058

[6] Lin Jing-Qiang, Jing Ji-Wu, Zhang Qiong-Lu, et al. Recent advances in PKI technologies. Journal of Cryptologic Research, 2015, 2(6): 487-496(in Chinese)
(林璟锵,荆继武,张琼露等. PKI 技术的近年研究综述. 密码学报, 2015, 2(6): 487-496)

[7] Chen P L, Yang J H, Lin C I. ID-based user authentication scheme for cloud computing. Journal of Electronic Science and Technology, 2013, 11(2): 221-224

[8] Blaze M, Bleumer G, Struss M. Divertible protocols and atomic proxy cryptography//Proceedings of the EUROCRYPT'98. Helsinki, Finland, 1998: 127-144

[9] Sun Shang-Bo. Research on Trust Model and Certificate Path Construction Method of PKI [M. S. dissertation]. Shenyang Aerospace University, Shenyang 2011(in Chinese)
(孙尚波. PKI 信任模型与证书路径构造方法研究[硕士学位论文]. 沈阳航空航天大学. 沈阳, 2011)

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

[11] Ye Wei-Wei, Ou Qing-Yu, Bai Xiao-Wu. Research on authentication scheme of cryptographic service system based on service architecture. Netinfo Security, 2016, 12(5): 37-43(in Chinese)
(叶伟伟,欧庆于,柏小武. 基于服务架构的密码服务系统认证方案研究. 信息网络安全, 2016, 12(5): 37-43)

[12] Schulman A, Levin D, Spring N. Revcast: Fast, private certificate revocation over FM radio//Proceedings of the ACM Conference on Computer and Communications Security. Scottsdale, Arizona, USA, 2014: 799-810

[13] He Bin. Improvement and Research on Mechanism of Certificate Revocation Based on PKI [M. S. dissertation]. Shanghai Jiao Tong University, Shanghai 2015(in Chinese)
(何斌. PKI 中证书撤销机制的改进与研究[硕士学位论文]. 上海交通大学，上海，2015)

[14] Zhang Yan. Design of Cross-Domain Authentication System for Multiple Security Element Based on PKI [M. S. dissertation]. Taiyuan University of Technology, Taiyuan, 2015(in Chinese)
(张岩. 基于 PKI 的多安全要素跨域身份认证系统设计[硕士学位论文]. 太原理工大学，太原，2015)

[15] Yang Li, Ma Jian-Feng, Jiang Qi. Direct anonymous attestation scheme in cross trusted domain for wireless mobile networks. Journal of Software, 2012, 23(5): 1260-1271(in Chinese)
(杨力，马建峰，姜奇. 无线移动网络跨可信域的直接匿名证明方案. 软件学报，2012，23(5)：1260-1271)

[16] Chen L, Morrissey P, Smart N P. Pairings in trusted computing//Proceedings of the Pairing-Based Cryptography. London, UK, 2008: 1-17

[17] Zhou Yan-Wei, Yang Bo, Wu Zhen-Qiang, et al. Direct anonymous authentication scheme in cross-domain based on identity. Chinese Science: Information Science, 2014, 44(9): 1102-1120(in Chinese)
(周彦伟，杨波，吴振强等. 基于身份的跨域直接匿名认证机制. 中国科学：信息科学，2014，44(9)：1102-1120)

[18] Wang Zhong-Hua, Han Zhen, Liu Ji-Qiang, et al. ID authentication scheme based on PTPM and certificateless public key cryptography in cloud environment. Journal of Software, 2016, 27(6): 1523-1537(in Chinese)
(王中华，韩臻，刘吉强等. 云环境下基于 PTPM 和无证书公钥的身份认证方案. 软件学报，2016，27(6)：1523-1537)

[19] Zhang M, Zhang Y. Certificateless anonymous user authentication protocol for cloud computing//Proceedings of the 2015 International Conference on Intelligent Transportation, Big Data and Smart City. Halong Bay, Vietnam, 2015: 200-203

[20] Dong Z M, Zhang L, Li J T. Security enhanced anonymous remote user authentication and key agreement for cloud computing//Proceedings of IEEE 17th International Conference on Computational Science and Engineering. Chengdu, China, 2014: 1746-1751

[21] Ateniese G, Hohenberger S. Proxy re-signatures: New definitions, algorithms, and applications//Proceedings of the 12th ACM CCS. Alexandria, USA, 2005: 310-319

[22] Huang Ping, Yang Xiao-Dong, Li Yan, et al. Identity-based proxy re-signature scheme without bilinear pairing. Journal of Computer Applications, 2015, 35(6): 1678-1682(in Chinese)
(黄萍，杨小东，李燕等. 无双线性对的基于身份代理重签名方案. 计算机应用，2015，35(6)：1678-1682)

[23] Shao J, Wei G, Ling Y, et al. Unidirectional identity-based proxy re-signature//Proceedings of the IEEE International Conference on Communications. Kyoto, Japan, 2011: 1-5

[24] Paterson K G, Schuldt J C N. Efficient identity-based signatures secure in the standard model. Lecture Notes in Computer Science, 2006, 4058: 207-222

[25] Shao J, Cao Z, Wang L, et al. Proxy re-signature schemes without random oracles//Proceedings of the INDO-CRYPT 2007. Chennai, India, 2007: 197-209

[26] Kim K, Yie I, Lim S. Remark on Shao et al's bidirectional proxy re-signature scheme in Indocrypt'07. International Journal of Network Security, 2009, 8(3): 308-311

[27] Yang X, Gao G, Wang C. On-line/off-line threshold proxy re-signature scheme through the simulation approach. Applied Mathematics & Information Sciences, 2015, 9(6): 3251-3261

[28] Tian Miao-Miao. Identity-based proxy re-signatures from lattices. Information Processing Letters, 2015, 115(4): 462-467

[29] Yang X, Li C, Li Y, et al. Divisible on-line/off-line proxy re-signature. Applied Mathematics & Information Sciences, 2015, 9(2): 759-767

[30] Wang Z, Lu W. Server-aided verification proxy re-signature//Proceedings of the Trust, Security and Privacy in Computing and Communications. Melbourne, Australia, 2013: 1704-1707

[31] Yang Xiao-Dong, Li Ya-Nan, Gao Guo-Juan, et al. Sever-aided verification proxy re-signature scheme in the standard model. Journal of Electronics & Information Technology, 2016, 38(5): 1151-1157(in Chinese)
(杨小东，李亚楠，高国娟等. 标准模型下的服务器辅助验证代理重签名方案. 电子与信息学报，2016，38(5)：1151-1157)

[32] Chow S S M, Phan R C W. Proxy re-signatures in the standard model//Proceedings of the International Conference on Information Security. Taipei, China, 2008: 260-276

[33] Vivek S S, Selvi S S D, Balasubramanian G, et al. Strongly unforgeable proxy re-signature schemes in the standard model. IACR Cryptology ePrint Archive, 2012, 80: 1-23

[34] Tsai T T, Tseng Y M, Huang S S. Efficient strongly unforgeable ID-based signature without random oracles. Informatica, 2014, 25(3): 505-521

[35] Dan B, Shen E, Waters B. Strongly unforgeable signatures based on computational Diffie-Hellman//Proceedings of the International Conference on Theory and Practice of Public-Key Cryptography. New York, USA, 2006: 229-240

[36] Bellare M. New proofs for NMAC and HMAC: Security without collision-resistance//Proceedings of the Advances in Cryptology-CRYPTO 2006. Santa Barbara, USA, 2006: 602-619

[37] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 1996, 41(2): 1484-1509

附录 1.

定理 1. 如果 CDH 假设和 CRH 假设成立，则本文方案在标准模型下是强不可伪造的.

证明. 假设存在一个攻击者$\mathcal{A}$攻破了新方案的强不可伪造性，则存在一个算法$\mathcal{B}$作为挑战者，利用$\mathcal{A}$的伪造解决 G_1 上的 CDH 问题或违反 CRH 假设. 即攻击者$\mathcal{A}$在时间 t 内最多进行 q_S 次签名询问和 q_{RS} 次重签名询问后，如果能以 ε 的概率输出一个伪造，则挑战者$\mathcal{B}$在时间 $t+O((q_S+q_{RS})n_m\tau_1+(q_S+q_{RS})\tau_2)$ 内以 $\varepsilon''>\frac{\varepsilon}{2}$ 的概率找到哈希函数 H_1 的碰撞或以 $\varepsilon'>\varepsilon/(4(q_S+q_{RS})(n_m+1))$ 的概率解决 CDH 问题，这里 τ_1 和 τ_2 分别是 G_1 上一次乘法运算和一次指数运算所需要的时间，n_m 是签名消息的固定长度. 给定一个 CDH 问题实例 (g,g^a,g^b)，$\mathcal{B}$与$\mathcal{A}$进行如下的安全游戏，$\mathcal{B}$的目标是计算 g^{ab} 或找到 H_1 的一对碰撞.

系统建立：挑战者$\mathcal{B}$选择两个抗碰撞的哈希函数 $H_1:\{0,1\}^*\rightarrow\{0,1\}^{n_c}$ 和 $H_2:\{0,1\}^*\rightarrow\{0,1\}^{n_m}$，其中 H_1 和 H_2 是普通的哈希函数，不需要模拟随机预言机. $\mathcal{B}$设置 $l_m=2(q_S+q_{RS})$，满足 $l_m(n_m+1)<p$；随机选择 $k_m\in Z_{n_m}$，并在 Z_{l_m} 中随机选择 n_m+1 个元素 c' 和 $c_i(i=1,\cdots,n_m)$，在 Z_p 中随机选择 n_m+2 个元素 d,d' 和 $d_i(i=1,\cdots,n_m)$. 对于消息 m，令 $M=H_2(m)=(M_1,\cdots,M_{n_m})\in\{0,1\}^{n_m}$，$F(m)=c'+\sum_{i=1}^{n_m}c_iM_i-l_mk_m$ 和 $J(m)=d'+\sum_{i=1}^{n_m}d_iM_i$，则 $\varpi=u\prod_{i=1}^{n_m}(u_i)^{M_i}=g_2^{F(m)}g^{J(m)}$. $\mathcal{B}$设置目标用户的公钥 $g_1=g^a$，参数 $u'=g_2^{-l_mk_m+c'}g^{d'}$，$g_2=g^b$，$g_3=g^d$，$u_i=g_2^{c_i}g^{d_i}(1\leq i\leq n_m)$，发送系统参数 $(g,g_1,g_2,g_3,u,\{u_i\}_{i=1}^{n_m},H_1,H_2)$ 给攻击者$\mathcal{A}$.

攻击者$\mathcal{A}$可以适应地向挑战者$\mathcal{B}$发起一系列如下的签名询问和重签名询问.

签名询问：$\mathcal{A}$可以询问 q_S 个消息 $m_1,\cdots,m_{q_S}$ 的签名，并获得 $m_i(1\leq i\leq n_m)$ 的签名 $\sigma_i=(\sigma_{i,1},\sigma_{i,2})$. 对于消息 m_i，$\mathcal{B}$进行如下的模拟操作：

(1) 如果 $F(m_i)=0 \bmod p$，则$\mathcal{B}$宣告失败，退出模拟.

(2) 如果 $F(m_i)\neq 0 \bmod p$，$\mathcal{B}$随机选择 $s_i\in Z_p$，计算 $M^i=H_2(m_i)=(M_1^i,\cdots,M_{n_m}^i)\in\{0,1\}^{n_m}$，$\varpi_i=u\prod_{j=1}^{n_m}(u_j)^{M_j^i}$，$\sigma_{i,2}=g_1^{\frac{-1}{F(m)}}g^{s_i}$，$h_i=H_1(m_i\|\sigma_{i,2})$ 和 $\sigma_{i,1}=g_1^{\frac{-J(m_i)-h_id}{F(m_i)}}(w_ig_3^{h_i})^{s_i}$，将消息 m_i 的签名 $\sigma_i=(\sigma_{i,1},\sigma_{i,2})$ 返回给攻击者$\mathcal{A}$.

重签名询问：对于$\mathcal{A}$发起的 (pk_i,g_1,m_i,σ_i) 重签名询问，如果 σ_i 是对应于公钥 pk_i 关于消息 m_i 的合法签名，$\mathcal{B}$进行 m_i 的签名询问，并将询问结果返回给$\mathcal{A}$；否则，输出 $\perp$.

伪造：$\mathcal{A}$最后输出一个消息 m^* 的伪造 $\sigma^*=(\sigma_1^*,\sigma_2^*)$，其中 $h^*=H_1(m^*\|\sigma_2^*)$，$M^*=H_2(m^*)=(M_1^*,\cdots,M_{n_m}^*)\in\{0,1\}^{n_m}$ 和 $\varpi^*=u\prod_{j=1}^{n_m}(u_j)^{M_j^*}$. 将攻击者的伪造分以下两种情况讨论：

第 1 类伪造：m^* 未进行过签名询问或重签名询问. 如果 $F(m^*)\neq 0 \bmod p$，$\mathcal{B}$宣告失败，退出模拟；否则 $F(m^*)=0 \bmod p$，$\mathcal{B}$计算

$$\frac{\sigma_1^*}{(\sigma_2^*)^{J(m^*)+h^*d}}=\frac{g_2^a(w^*g_3^{h^*})^{s^*}}{(g^{s^*})^{J(m^*)+h^*d}}=\frac{g_2^a(g_2^{F(m^*)}g^{J(m^*)}g_3^{h^*})^{s^*}}{(g^{s^*})^{J(m^*)}(g^{s^*})^{h^*d}}$$

$$=\frac{g_2^ag^{J(m^*)s^*}(g_3^{h^*})^{s^*}}{g^{J(m^*)s^*}(g_3^{h^*})^{s^*}}=g_2^a=g^{ab},$$

从而解决 CDH 问题的一个实例.

第 2 类伪造：m^* 进行过签名询问或重签名询问. 即攻击者已获得 m^* 的一个签名 $\sigma_i^*=(\sigma_{i,1}^*,\sigma_{i,2}^*)$，其中 $h_i^*=H_1(m^*\|\sigma_{i,2}^*)$. 如果 $h_i^*\neq h^*$，与第一类伪造相同，$\mathcal{B}$可以计算出 g^{ab}；否则，$h_i^*=h^*$ 且 $\sigma_{i,2}^*\neq\sigma_2^*$. 如果 $\sigma_{i,2}^*=\sigma_2^*$，则 $g^{s_i^*}=g^{s^*}$，于是 $s_i^*=s^*$，从而有 $\sigma_{i,1}^*=g_2^a(w^*g_3^{h_i^*})^{s_i^*}=g_2^a(w^*g_3^{h^*})^{s^*}=\sigma_1^*$，这说明攻击者$\mathcal{A}$伪造的签名 σ^* 就是以前询问过的签名 σ_i^*，$\mathcal{A}$并没有输出一个合法的伪造. 因此，如果$\mathcal{A}$输出第二类伪造，则$\mathcal{B}$可成功找到哈希函数 H_1 的一对碰撞 $(m^*\|\sigma_{i,2}^*,m^*\|\sigma_2^*)$.

与文献[30]的分析过程相似，如果攻击者$\mathcal{A}$以 ε 的概率攻破本方案的强不可伪造性，则$\mathcal{B}$将以 $\varepsilon'>\frac{\varepsilon}{4(q_S+q_{RS})(n_m+1)}$ 的概率解决 CDH 问题或以 $\varepsilon''>\frac{\varepsilon}{2}$ 的概率找到哈希函数 H_1 的一对碰撞. 在上述模拟过程中，$\mathcal{B}$需要进行 $O(n_m)$ 复杂度的乘法运算和 $O(1)$ 复杂度的指数运算，所以$\mathcal{B}$挑战成功的时间复杂度为 $t+O((q_S+q_{RS})n_m\tau_1+(q_S+q_{RS})\tau_2)$.

定理 2. 本文新方案能抵抗服务器和签名者或代理者的合谋攻击，并在自适应性选择消息攻击下是完备的.

证明. 攻击者$\mathcal{A}$代表一个具有强大计算能力的服务器，挑战者$\mathcal{C}$代表签名的验证者. 由于允许攻击者$\mathcal{A}$与签名者或代理者合谋，所以$\mathcal{A}$已掌握签名密钥或重签名密钥，可生成任意消息的合法签名或重签名. $\mathcal{A}$发送一个非法的消息签名对 (m^*,σ^*) 给挑战者$\mathcal{C}$，$\mathcal{A}$的目标是让$\mathcal{C}$确信 σ^* 是消息 m^* 的合法签名.

系统建立：$\mathcal{C}$首先运行系统建立算法，生成系统参数 $cp=(G_1,G_2,p,e,g,g_2,u,\{u_i\}_{i=1}^{n_m},H_1,H_2)$；然后随机选择 $\alpha^*\in Z_p^*$ 作为目标用户的私钥 sk^*，计算对应的公钥 $pk^*=g^{\alpha^*}$；随机选择 $x^*\in Z_p^*$，计算 $K_0^*=g_2^{x^*}$，并秘密保存 $VString=(x^*,K_0^*)$；最后将 (cp,sk^*,pk^*) 发送给$\mathcal{A}$.

查询：对于$\mathcal{A}$发起的每次询问 (m_i,σ_i)，$\mathcal{A}$充当服务器的角色，$\mathcal{C}$充当验证者的角色，$\mathcal{C}$与$\mathcal{A}$首先运行第 3 节的服务器辅助协议，然后$\mathcal{C}$将协议的运行结果返回给$\mathcal{A}$.

输出：经过有限次的适应性选择询问后，$\mathcal{A}$发送一个消息签名对 $(m^*,\sigma^*=(\sigma_1^*,\sigma_2^*))$ 给者$\mathcal{C}$，其中 σ^* 不是公钥 pk^* 关于消息 m^* 的合法签名. $\mathcal{C}$利用 $VString$ 计算 $(\sigma^*)'=((\sigma_1^*)',(\sigma_2^*)')=((\sigma_1^*)^{x^*},(\sigma_2^*)^{x^*})$ 和 $h'=H_1(m^*\|\sigma_2^*)$，并给$\mathcal{A}$发送 $(m^*,h',(\sigma^*)'=((\sigma_1^*)',(\sigma_2^*)'))$. $\mathcal{A}$计算 $M^*=$

$H_2(m^*)=\{M_i^*\}_{i=1}^{n_m}$，$w'=u'\prod_{i=1}^{n_m}u_i^{M_i'}$，$K_1^*=e((\sigma_1^*)',g)$ 和 $K_2^*=e(w'g_3^{h'},(\sigma_2^*)')$，将$(K_1^*,K_2^*)$返回给$\mathcal{C}$.

下面分析非法消息签名对(m^*,σ^*)满足等式 $K_1^*=e(K_0^*,pk^*)K_2^*$ 的概率是 $1/(p-1)$.

① 由于$(\sigma_1^*)'=(\sigma_1^*)^{x^*}$ 和$(\sigma_2^*)'=(\sigma_2^*)^{x^*}$，并且 x^* 是挑战者$\mathcal{C}$在 Z_p^* 中随机选取的，因此$\mathcal{A}$通过 σ^* 推导出$(\sigma^*)'$的概率为 $1/(p-1)$.

② 如果(K_1^*,K_2^*)满足 $K_1^*=e(K_0^*,pk^*)K_2^*$，则有 $K_1^*=e(K_0^*,pk^*)K_2^*=e(g_2^{x^*},pk^*)K_2^*=e(g_2,pk^*)^{x^*}K_2^*$，很容易得知 $x^*=\log_{e(g_2,pk^*)}K_1^*/K_2^*$；但 $x^*\in Z_p^*$，因此$\mathcal{A}$寻找 x^* 满足 $K_1^*=e(K_0^*,pk^*)K_2^*$ 的概率为 $1/(p-1)$. 由此可见，如果(m^*,σ^*)是一个非法的消息签名对，则$\mathcal{A}$能让$\mathcal{C}$确信 σ^* 是消息 m^* 的合法签名的概率是 $1/(p-1)$. 即新方案能抵抗服务器和签名者或代理者的合谋攻击，并在自适应性选择消息攻击下是完备的.

YANG Xiao-Dong, born in 1981, Ph. D., associate professor. His main research interests include cloud computing security and cryptography.

AN Fa-Ying, born in 1991, M. S. candidate. His current research interests include ring signature and information security.

YANG Ping, born in 1993, M. S. candidate. His current research interests include proxy re-signature and big data security.

LIU Ting-Ting, born in 1994, M. S. candidate. Her current research interests include privacy protection.

XIAO Li-Kun, born in 1994, M. S. candidate. His current research interest is proxy signature.

WANG Cai-Fen, born in 1963, Ph. D., professor. Her current research interests include cryptography and data security.

Background

Cloud computing can provide secure, fast and convenient data storage, computing, software application and other services, and will be gradually applied to various fields. Identity authentication is the foundation of cloud computing security. It identifies the authenticity of users and cloud service providers, and restricts illegal users from accessing cloud resources. With the rapid development of cloud computing, more and more users need to access cloud resources of different trust domains, and cloud service providers use cross-domain authentication mechanism to identify foreign users. However, the traditional cross-domain authentication mechanism is not suitable for large-scale cloud environment. The cross-domain authentication scheme based on proxy re-signature in cloud environment is less discussed in recent research.

According to the characteristics of cloud computing, we propose a sever-aided verification proxy re-signature algorithm in the standard model, and then construct a cross-domain identity authentication scheme in cloud environment by referring to PKI authentication system and utilizing the proposed proxy re-signature algorithm. Our scheme is proven to be strongly unforgeable and complete against adaptive chosen message and collusion attacks. Besides, the performance analysis also shows that the proposed cross-domain identity authentication scheme retains the advantages of PKI, simplifies the interactive authentication process and improves the efficiency of cross-domain authentication.

This research is supported by the National Natural Science Foundation of China under Grant Nos. 61662069, 61562077 and 61262057, the China Postdoctoral Science Foundation under Grant No. 2017M610817. the Natural Science Foundation of Gansu Province of China under Grant Nos. 145RJDA325 and 1506RJZA130, the Science and Technology Project of State Archives Administration of China under Grant No. 2014-X-33, the Research Fund of Higher Education of Gansu Province under Grant No. 2014-A011, the Science and Technology Project of Lanzhou City of China under Grant No. 2013-4-22, the Foundation for Excellent Young Teachers by Northwest Normal University under Grant No. NWNU-LKQN-14-7. The team has published several research articles about proxy re-signature, access control for cloud storage, privacy protection and cryptography, and registered six computer software copyrights.