# 基于身份密码系统和区块链的跨域认证协议

魏松杰[1),2)] 李莎莎[1)] 王佳贺[1)]

[1)](南京理工大学计算机科学与工程学院 南京 210094)

[2)](南京理工大学网络空间安全学院 南京 210094)

**摘 要** 随着信息网络技术的快速发展和网络规模的持续扩张,网络环境中提供的海量数据和多样服务的丰富性和持久性都得到了前所未有的提升.处于不同网络管理域中的用户与信息服务实体之间频繁交互,在身份认证、权限管理、信任迁移等方面面临一系列安全问题和挑战.本文针对异构网络环境中用户访问不同信任域网络服务时的跨域身份认证问题,基于 IBC 身份密码系统,结合区块链技术的分布式对等网络架构,提出了一种联盟链上基于身份密码体制的跨信任域身份认证方案.首先,针对基于 IBC 架构下固有的实体身份即时撤销困难问题,通过加入安全仲裁节点来实现用户身份管理,改进了一种基于安全仲裁的身份签名方案 mIBS,在保证功能有效性和安全性的基础上,mIBS 性能较 ID-BMS 方案节省 1 次哈希运算、2 次点乘运算和 3 次点加运算.其次,本文设计了区块链证书用于跨域认证,利用联盟链分布式账本存储和验证区块链证书,实现域间信任实体的身份核验和跨域认证.所提出的跨域认证协议通过安全性分析证明了其会话密钥安全,并且协议的通信过程有效地减轻了用户端的计算负担.通过真实机器上的算法性能测试,与现有同类方案在统一测试标准下比较,本文方案在运行效率上也体现出了明显的优势.

**关键词** 区块链;身份密码;数字签名;安全仲裁;可信共识

**中图法分类号** TP309 **DOI 号** 10.11897/SP.J.1016.2021.00908

《计算机学报》

# A Cross-Domain Authentication Protocol by Identity-Based Cryptography on Consortium Blockchain

WEI Song-Jie[1),2)] LI Sha-Sha[1)] WANG Jia-He[1)]

[1)](*School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing* 210094)

[2)](*School of Cyberspace Security, Nanjing University of Science and Technology, Nanjing* 210094)

**Abstract** With the exciting growth of global Internet services and applications in the past decades, tremendous amount of various data and service resources are prevailing on network and attracting users from different administration domains all over the world. The Internet cyberspace is never short of security threats and resource abusers. Reliable and efficient network entity authentications and identification verifications are the corner stones for all types of secure network application environments and usage scenarios. Especially how to verify an entity's identity outside its origin, and how to extend such authentication capability across different administration domains in network without obvious security weak point or performance bottleneck, it is a realistic challenge for traditional cryptography based authentication schemes. Either the encryption key based or the PKI certificate based approaches suffer the threats on credential managements and the inefficiency revocation. Towards the problem of cross-domain authentication when users in heterogeneous network environments access network services from different trust domains, this paper proposes

收稿日期:2019-11-30;在线发布日期:2021-01-22.本课题得到国家自然科学基金(61802186,61472189)、赛尔网络下一代互联网创新项目(NGII20180103)、上海航天科技创新基金(SAST2019-033)资助.**魏松杰**,博士,副教授,中国计算机学会(CCF)会员,主要研究方向为网络安全、区块链技术、网络协议分析.E-mail:swei@njust.edu.cn.**李莎莎**,硕士研究生,主要研究方向为区块链技术、分布式系统.**王佳贺**(通信作者),硕士,主要研究方向为区块链技术、协议设计、身份认证.E-mail:jhwang@njust.edu.cn.

a new design of blockchain certificate to implement cross-domain authentication based on the identity-based cryptosystem and the distributed architecture of blockchain technology. A novel cross-trust-domain authentication scheme based on IBC system is constructed and evaluated. Firstly, to solve the problem of instantaneous entity identity revocation based on the IBC architecture, a security-mediator based identity signature scheme, mIBS, is proposed with optimized identity management scheme. A security mediator serves in a trust domain to approve or decline any authentication attempt. By retaining part of each entity's identity authentication key in the domain, the security mediator can quickly collaborate with other nodes to either verify the entity's identity or fail its request for authentication, i. e. revocation. The proposed mIBS algorithm for IBC-based intro-domain authentication, ensures entity authentication functionality and security, with the computation overhead reduced greatly compared with the ID-BMS scheme. The cross-domain authentication is supported and implemented on a consortium blockchain system. We optimize the PKI certificate structure and design a blockchain certificate to record domain credential on blockchain. Blockchain certificate authorities, just like CAs in X.509, are organized and coordinated together to run the consortium ledger as the domain credential storage, verification and exchange platform. Compared with the centralized CA organization, the distributed ledger on blockchain nodes has better replication of certificate data, higher scalability, cryptography-guaranteed information integrity, and decentralized consensus calculation capability. The proposed mIBS algorithm and the blockchain-based authentication protocol are thoroughly evaluated for security and efficiency. Theoretical analysis and deduction show the new scheme holds the same security strength as the original IBC system, but saves some on the operation execution overhead. The state-of-the-art distributed user authentication schemes in literature are used as benchmarks to evaluate the proposed blockchain-based distribution authentication. The new scheme is robust enough to survive any typical network attacks and interruptions, and with significantly improved computation overhead efficiency when being measured alive on experimental machines.

**Keywords**　blockchain; identity-based cryptography; digital signature; security mediator; trust consensus

《计算机学报》

## 1　引　言

以 Internet 为代表的信息网络技术,极大地拓展了数字服务用户行为的持续时间和延展范围,让原本属于不同服务区域、用户体系、业务流程的信息,能够依托网络基础设施而自由流动、广泛传播. Internet 作为海量异构网络的融合连接体,造就了网络资源的全球覆盖与服务应用域的全面联通,在带来数字服务繁荣普及的同时,也使得用户在不同应用服务域间的信息交互愈发频繁. 用户在跨域访问网络资源时,由于身份认证和权限验证过程所带来的额外开销不可避免,因而设计面向全域网络环境的身份认证机制,实现身份的有效验证、一致认证、统一管理显得尤为重要. 针对 Internet 等大规模网络应用场景下,特定数字空间范围内不同信息服务实体(Information Service Entity,ISE)间繁杂的交互过程,实现用户在不同 ISE 间的跨域认证过程具有广泛的应用意义和工程价值.

跨域认证,即用户在多个可信区域之间完成一致的身份验证过程,既要保证全域信任关系建立的可信性、高效认证的可用性、认证过程的可靠性等,又要实现多信任域内的认证系统对有效用户的及时统一认证和即时管理[1]. 在分布式系统的实施场景下,出现了三种主流的跨域认证框架和实践方案:(1)应用对称密钥技术设计认证架构;(2)采用公钥基础设施(Public Key Infrastructure,PKI)实施分布式认证;(3)基于身份密码学(Identity-based Cryptography,IBC)设计认证架构. 这三种架构方案所采用的密码学技术具有特质差异,适用于不同场景,也造成各自不同的优劣效果. 基于传统对称密钥技术的方案运行速度快、认证效率高,但面临密钥

泄露的安全风险.鉴于网络空间内的恶意攻击和安全威胁愈加复杂多样和广泛持久[2],这类方案的应用场景具有局限性.采用PKI体系的认证架构有效避免了对称密钥难以管理的困境,尤其适合于分布式应用场景,具有优良的系统扩展性和实践灵活性[3].但PKI认证过程在数字证书的管理、分发过程中存在计算复杂、开销冗杂现象,性能不佳.基于IBC的认证方案直接以实体本身的有效标识作为公钥,使得认证过程不再囿于证书机制,简化了实体身份对应密钥的管理过程.但IBC认证系统的实体私钥依赖密钥生成中心(Key Generation Center,KGC)集中计算产生,依然需要密钥托管,因此IBC方案适用于小规模信任域网络中.现有IBC方案中实体身份撤销是通过KGC定期停止提供私钥来实现,撤销过程缺乏即时有效能力.总之,目前的实体跨域认证方案或技术均未能兼顾有效性、安全性、高效性,无法支撑用户与ISE间跨域认证的完整需求[4].

为解决现有身份认证方案在大规模跨域场景应用过程中存在的问题,本文在IBC认证系统的基础上进行改进,结合区块链分布式存储与共识的特性,设计了区块链证书结构以支撑跨域认证过程,创新性地构造了基于身份密码体制的跨信任域认证方案.具体工作内容和研究成果包括:(1)针对原有IBC架构下实体身份难以及时撤销的问题,改进设计了基于安全仲裁的身份签名方案mIBS;(2)结合身份密码体制与区块链技术设计并实现了分布式跨域认证方案,IBC模式用于域内认证,借鉴联盟链分布式共识方法实现了域间认证,采用区块链证书支持跨域身份认证的完整过程;(3)设计了一种多域信任的身份认证协议,既保证了密钥协商过程的安全性,又有效降低网络通信与节点计算开销,提高了认证效率,满足用户与ISE间在大规模分布式应用场景下的跨域认证需求.

## 2 相关工作

异军突起的区块链技术,提供了一种具有多中心、防篡改、可追溯、易扩展特点的分布式数据记录实现方法.不断扩增的数据单元按照顺序组织起来,其间通过哈希摘要相关联,以数据发布者、记录者和确认者的电子签名为保障[5].通过数据加密、离散共识、时序关联等手段,区块链实现了去中心化的点对点可信事务交互,提供了融合数据可用、内容可验、操作可溯能力的分布式安全应用服务,是信用进化史上继生物血亲、贵重金属、国家货币信用后的第四座里程碑[6].

基于身份的密码技术IBC脱胎并借鉴于PKI技术,同样采用公钥密码认证体系,但以用户身份信息来绑定生成公钥,避免了PKI体系中依赖证书的公钥认证管理过程.以此为基础,众多学者针对分布式应用场景下如何处理不同信任域间的认证传递问题,即跨域身份认证技术,展开了研究并取得了一系列成果.例如一种方案[7]提出利用PKI体制构建新型虚拟网桥CA(Certification Authority)信任模型,用以实现虚拟企业间有效的跨域认证过程.这类方案采用分布式可验证秘密共享协议和基于椭圆曲线密码系统的签名算法,实施简单且应用场景广泛.基于PKI体系搭建分布式跨域信任平台,实现域间可信的CA控制与管理,进而支持多CA环境下的信任传递[8].此外,一些方案利用逐步成熟的IBC体制构建无证书的跨域认证系统和认证协议,实现多域WMN环境下安全高效的实体认证和通信功能[9].国内已有科研人员设计了基于身份的签名算法,尝试利用椭圆曲线加法群上运算实现身份匿名条件下的跨域认证过程[10].Wang等人给出了一种认证密钥协商协议[11],结合异构签密实现了IBC和PKI系统之间的认证转换,具有更高的安全性和更好的可用性.

区块链技术在比特币等数字货币应用领域取得广泛成功,其相关设计理念和系统架构也为众多研究者们在探索跨域身份认证问题提供了新的思路.Wang等人[12]采用区块链技术提出了跨域认证模型BlockCAM及其跨域认证协议,将根证书颁发机构作为验证节点组织在联盟链上,解决了用户在访问多域资源时面临的安全和效率问题,展现了优于基于PKI体系的跨域身份验证能力.国内研究者结合区块链技术、IBC域和PKI体系设计跨异构域认证方案,采用国密SM9和区块链代理协同生成密钥,同样通过构造联盟链提供跨域认证过程的可靠性,实现可SOV逻辑证明的协议安全性与实用性[13].区块链技术极大地拓宽了解决跨域认证问题的探索空间,技巧性地融合了自证身份、互证信任、共证真实等一系列信息安全功能.本文基于联盟区块链技术尝试解决相互独立的IBC系统间的跨域认证和信任传递问题,实现用户身份多域一致性的安全保证.

《计算机学报》

## 3　基于身份密码体制的签名算法

首先对跨域认证模型中基于 IBC 的域内认证方案进行改进，设计了基于仲裁的身份签名和认证算法，简要称为 mIBS. 本节给出基于仲裁的 IBC 域结构设计，描述了 mIBS 方案的实现原理和方法，并对其进行安全性分析.

### 3.1　基于仲裁的 IBC 域结构设计

高可靠性的用户身份认证和权限管理系统，必不可少地需要支持用户身份的实时可信验证、有效控制与及时撤销. 在 IBC 系统中，公钥是基于用户身份信息关联生成的，理论上可以通过撤销用户身份来使得对应的公钥失效[14]. 但用户身份信息作为公开数据被广泛发布用于验证，也正是 IBC 系统的特色所在，实际应用中难以直接核销用户身份. 因此，类似 PKI 体系中的证书撤销机制，对于 IBC 系统无法有效适用[15]. 既然身份验证是为了对用户行为和权限进行限定，也可以设置权限仲裁，通过控制某一身份用户在 IBC 系统中服务权限验证结果，来实现密钥管理和身份撤销的效果[16]，即基于安全仲裁(Security Mediator，SEM)的 IBC 域内方案. 这里 KGC 和 SEM 在系统内分立，KGC 密钥生成中心为系统内用户生成私钥，SEM 在系统运行过程中给用户使用密码服务提供信令，如图 1 所示. 相比于基于“$ID \| $有效期”的公钥撤销方式，KGC 和 SEM 的分立能够提供更高细粒度的安全控制，提高系统的访问控制灵活性. 这里的 IBC 认证过程仅在域内采用，节点数量和网络规模可控，而 SEM 信令仅运行一个数据量不大的简单运算，因此整体运算负载和网络开销不大，性能可控.

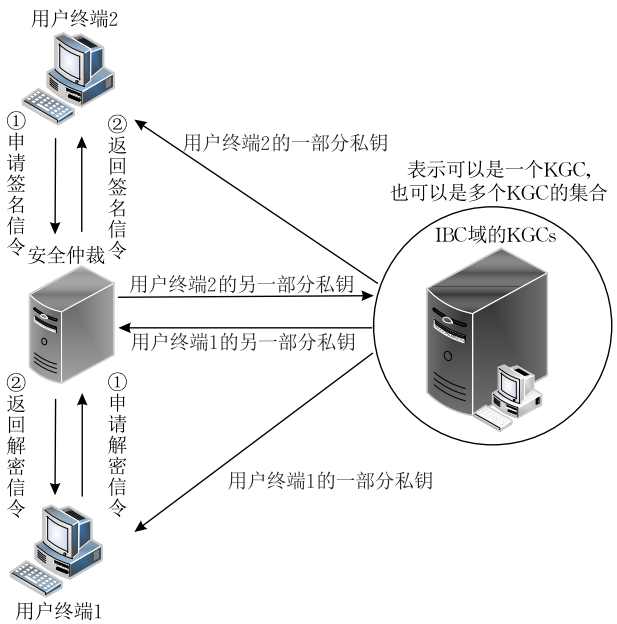


图 1　基于仲裁的 IBC 域结构

### 3.2　基于仲裁的身份签名方案

借鉴身份签名 IBS 算法，本文方案同样根据双线性映射构造 mIBS 数字签名，并保证以下两点：(1) mIBS 算法在 SEM 签发签名信令前能够验证签名请求消息的来源合法性，即判断是否来自合法用户；(2) 用户发送给 SEM 作为验证签名的依据不为明文，需要隐藏好待签的明文信息[17]. 整个方案包括参数生成(Setup)、密钥生成(KeyGen)、签名(Sign)和验证(Verify)四个算法，具体描述如下.

**Setup 阶段：**

设置安全系数 $\lambda$，初始化得到阶为大素数 $p(p>2^{\lambda})$ 的循环群 $(G_1,+)$，$(G_2,\times)$，这里 $G_1$ 的生成元为 $P$. 选取双线性映射 $e:G_1\times G_1\rightarrow G_2$，满足双线性对的可计算性、非退化性和双线性要求. 选取哈希函数 $H_1:\{0,1\}^*\rightarrow G_1^*$ 和 $H_2:\{0,1\}^*\times G_2^*\rightarrow Z_N^*$，$G_1^*$ 和 $G_2^*$ 代表 $G_1/\{0\}$ 和 $G_2/\{1\}$. KGC 随机选取 $s\in[1,p-1]$ 作为系统主密钥，并计算群 $G_1$ 的元素 $P_{\text{public}}=[s]P$ 作为系统主公钥，[ ]为取整运算，系统主密钥对为 $(s,P_{\text{public}})$. KGC 保存系统私钥 $s$，并公开系统参数为 $(p,P,G_1,G_2,e,P_{\text{public}},H_1,H_2)$；消息空间 $M=(0,1)^n$，签名空间 $Sign=G_1^*\times Z_N^*$.

**KeyGen 阶段：**

对于一个用户标识为 $ID\in\{0,1\}^*$，KGC 为其计算公钥 $P_{ID}$ 和私钥 $d_{ID}$：

$$P_{ID}=H_1(ID)\in G_1^* \tag{1}$$

$$d_{ID}=[s]P_{ID} \tag{2}$$

然后 KGC 对该用户私钥进行切分，先随机选择 $s_{ID}\in[1,p-1]$，并根据下式计算：

$$d_{ID}^{\text{user}}=[s_{ID}]P_{ID} \tag{3}$$

$$d_{ID}^{\text{SEM}}=d_{ID}-d_{ID}^{\text{user}}=[(s-s_{ID})]P_{ID} \tag{4}$$

$d_{ID}^{\text{user}}$ 由 KGC 发送给用户，$d_{ID}^{\text{SEM}}$ 发给 SEM.

**Sign 阶段：**

给定消息 $m\in M$，计算消息 $m$ 的正确签名如下：

(1) 用户签名消息 $m$ 之前

① 随机选择任意点 $P_1\in G_1$ 和任意整数 $k\in[1,p-1]$，计算群 $G_2$ 中元素 $q$，

$$q=e(kP_1,P) \tag{5}$$

② 计算整数 $g$，

$$g=H_2(m,q) \tag{6}$$

③ 计算签名 $S_{\text{user}}$，

$$S_{\text{user}}=kP_1+gd_{ID}^{\text{user}} \tag{7}$$

《计算机学报》

④向 SEM 发送请求 $Request=(q,g,S_{\text{user}})$.

(2) SEM 收到用户签名后

①首先检索该用户的身份 $ID$,查看是否属于被撤销的情况,若已撤销则停止服务.

②接着计算签名信令 $S_{\text{SEM}}$,拼接得到完整的消息 $m$ 的签名 $S_m$,

$$S_{\text{SEM}}=gd_{ID}^{\text{SEM}} \tag{8}$$

$$S_m=S_{\text{user}}+S_{\text{SEM}} \tag{9}$$

③SEM 根据式(1)计算 $P_{ID}$ 并验证元素 $q$ 的正确性:

$$q'=e(S_m,P)\cdot e(P_{ID},-P_{\text{public}})^g \tag{10}$$

若 $q'=q$,则证明消息 $m$ 的签名申请是合法的,$S_{\text{SEM}}$ 可由 SEM 发送给用户. 根据哈希函数的特性,如果需要签名的消息 $m_1\neq m_2$,那么签名信令 $S_{\text{SEM1}}\neq S_{\text{SEM2}}$,即信令难以被重用.

(3)用户签名

为了验证目标信令 $S_{\text{SEM}}$ 的有效性,用户在收到 $S_{\text{SEM}}$ 后,计算 $S_m$ 和 $q'$,$q'=q$ 时输出签名 $\langle S_m\rangle$.

**Verify 阶段:**

对签名 $\langle S_m\rangle$ 的验证过程是根据 $q'$ 计算 $g'$,

$$g'=H_2(m,q') \tag{11}$$

$g'=g$ 时证明该签名 $\langle S_m\rangle$ 正确.

### 3.3 安全性证明

为了检验更高细粒度下跨域身份认证过程的可靠性和有效性,下面对 mIBS 签名算法从计算和算法设计两方面作简要安全证明.

(1)计算安全性证明

群 $G_1$ 中生成系统和用户的密钥,群 $G_2$ 中产生用户和 SEM 签名,攻击者利用 $sH_1(ID)$ 和 $s_{ID}H_1(ID)$ 推导 $s$ 和 $s_{ID}$ 的难度等同于求解椭圆曲线上离散对数难题. 同理,由签名信令 $S_{\text{SEM}}$ 通过式(12)求解 $(s+s_{ID})$ 的难度也相当,因此离散对数难题与哈希函数的安全性假设保障了方案的计算安全性.

$$S_{\text{SEM}}=gd_{ID}^{\text{SEM}}=g(s+s_{ID})H_1(ID) \tag{12}$$

(2)算法安全性证明

在 mIBS 方案中,判断签名申请的合法性和判断 $S_{\text{SEM}}$ 签名结果的有效性都需要验证 $q'=q$,因此只需要证明 $q'=q$ 成立便能保证可信域内的身份双向安全认证,即式(13). 用户在向 SEM 申请消息 $m$ 签名 $\langle S_m\rangle$ 时发送 $Request=(q,g,S_{\text{user}})$,不包含原始消息,这也保证了待签名消息 $m$ 的隐私性.

$$\begin{aligned}q'&=e(S_m,P)e(P_{ID},-P_{\text{public}})^g\\&=e(kP_1+gd_{ID}^{\text{user}}+gd_{ID}^{\text{SEM}},P)\cdot e(P_{ID},-P_{\text{public}})^g\\&=e(kP_1+gd_{ID},P)\cdot e(P_{ID},-P_{\text{public}})^g\\&=e(gsP_{ID},P)\cdot e(kP_1,P)\cdot e(P_{ID},-P_{\text{public}})^g\\&=e(P_{ID},sP)^g\cdot e(kP_1,P)\cdot e(P_{ID},P_{\text{public}})^{-g}\\&=e(kP_1,P)=q\end{aligned} \tag{13}$$

## 4 基于区块链的跨域身份认证模型

mIBS 算法可以在域内实现基于 IBC 的用户身份认证,本节利用区块链技术实现用户和信息服务实体间跨域的交互认证过程,设计了区块链系统模型,并描述了区块链证书的结构和认证工作原理.

### 4.1 跨域认证协议设计

本文设计的基于 IBC 和区块链架构的跨域认证模型,遵循如下设计目标:

(1)基于区块链的分布式系统架构[18],将多个 IBC 信任域在链上组织起来作为跨域信任机制的共同参与者.

(2)通过区块链交易共识的方式建立域间的信任验证和身份管理. 每个 IBC 域的代理服务器作为区块链节点参与交易传播和共识,同时依照区块链记录交易的方式对信任授权进行管理.

(3)在区块链上存储目标域证书,用于快速组装和验证跨域身份认证交易[19].

本文采用联盟区块链架构来设计跨域身份认证模型,采用基于身份的方式来认证分属于不同 IBC 信任域的用户实体和信息服务实体. 如图 2 中所示,域内信息服务实体的私钥通过 KGC 密钥拆分两部分后,分发给仲裁机构 SEM 和实体本身. 作为区块链的区域代理节点,在每个 IBC 域设有区块链证书服务器(Blockchain Certificate Authority,BCCA).

信息服务实体 ISE 与用户间的认证过程如下:

(1)当用户请求同域内某信息服务时,首先向 ISE 发出认证请求,ISE 随即向 SEM 发起请求,收到 SEM 签名信令后完成一系列签名操作,签名结果发到域内身份验证服务器(Identity Authentication Server,IAS)进行认证[20]. 如需撤销一个 ISE 的身份,则可要求 SEM 停止为其发送签名信令. 最后,用户可以根据 IAS 发回的认证响应决定 ISE 是否通过认证. 同域内的认证过程可视为跨域认证的特殊情况,具体过程描述从略.

(2)当请求用户和实体服务资源分属不同信任域时,通过区块链来进行跨域信任传递,完成用户与 ISE 间的认证过程. 在图 2 中,假设用户 $U_1$ 与 $ISE_2$ 进行交互,认证过程如下. $IBC_1$ 域和 $IBC_2$ 域前期通过 $BCCA_1$ 和 $BCCA_2$ 基于区块链证书完成域间认

计算机学报

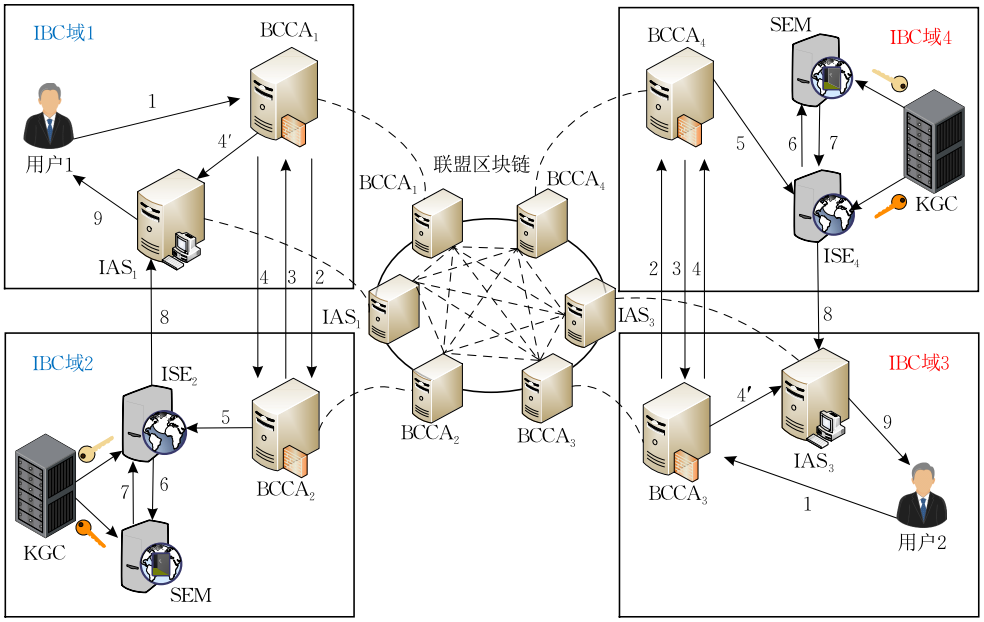


图 2　跨域认证系统模型(步骤 1:跨域认证请求 Req.,步骤 2、3、4:IBC 域间公共参数交换,步骤 4′:发送会话密钥 SK,步骤 5、6、7:信息服务实体 ISE 权限认证,步骤 8、9:会话密钥 $K'$认证)

证,同时交换两个域认证系统的公开参数和公钥生成算法. $BCCA_1$ 会为用户生成会话密钥,发送给身份认证服务器 $IAS_1$. $ISE_2$ 收到认证请求后,向本域内的 SEM 申请签名信令,方法参照 3.2 节中的相关描述. 通过 SEM 认证后,$ISE_2$ 会将完整签名结果发送给用户所在访问域的 $IAS_1$,待其验证签名信息后将认证结果返回用户. 这时用户即可根据认证结果来访问 $ISE_2$ 中的相应服务.

### 4.2　区块链证书设计

为了解决 3.1 节 $IBC_1$ 域和 $IBC_2$ 域代理 $BCCA_1$ 和 $BCCA_2$ 的可信认证问题,本文利用区块链的不可篡改性来完善数字证书,将设计的区块链证书作为信任凭证支撑身份跨域认证过程. 具体地,区块链证书依照 PKI 体系中 X.509 数字证书标准进行改进,由各域中参与联盟链的 BCCA 生成并记录在链上. 针对于身份跨域认证需求,图 3 比较了本文构造的区块链证书和原始 X.509 数字证书,具体改进内容如下:

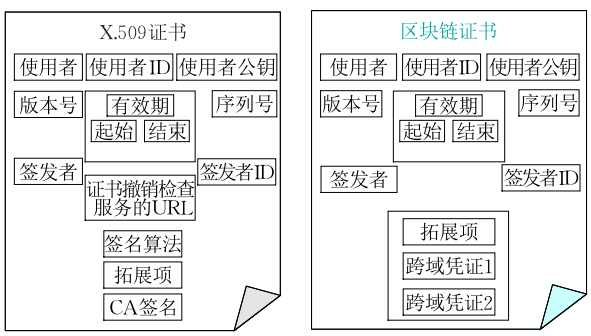


图 3　区块链证书

(1)省略了 X.509 数字证书中的签名算法内容. 签名算法用于验证证书的真实一致性. 区块链本身已经采用相应密码学方法实现了链上数据的原始真实性、完整一致性保障. 各个域中的 BCCA 区块链代理,只需要生成区块链证书后将其哈希值记入区块链账本中,证书可以在链上查验. 传统 X.509 数字证书的签名和验证过程被链上证书的存储和查验操作所替代,这有助于提高用户认证的效率.

(2)取消了 X.509 证书中用于撤销检查服务的统一资源定位符 URL 模块. 区块链证书直接存储在数据时序关联的联盟链上,随时可通过检索链上数据来查询证书状态,或者通过发送交易来记录新数据,不再需要提供在线证书状态协议 OCSP 和证书吊销列表 CRL 管理服务. 可以通过向链上发送交易签发(Issue)和交易撤销(Revoke)两种类型的数据操作来管理证书的实时状态. 这避免了传统 X.509 使用 OCSP 和 CRL 带来的通信和查询开销.

## 5　基于区块链的跨域认证协议

针对基于区块链的跨域身份认证模型,本节描述了用户跨域认证协议,详细给出了身份跨域认证中双方会话密钥的具体协商步骤,同时采用理论分析和实验测试方法,评估协议的安全性和有效性.

### 5.1 跨域认证协议设计

作为协议运行的初始状态，假定所有 IBC 域的 KGC、SEM 和 IAS 等服务节点都是诚实可靠的，域内实体间认证已经完成. 每个 KGC 公开一致性参数$(p,P,G_1,G_2,e,P_{\text{public}},H_1,H_2)$，但各 KGC 系统显然具有不同的主公钥 $P_{\text{public}}$ 和主密钥 $s$. 联盟区块链上可以提供各域 BCCA 的证书状态查询.

如图 2 中所示，以 $\text{IBC}_1$ 域中用户 $\text{U}_1$ 访问 $\text{IBC}_2$ 域中信息服务资源 $\text{ISE}_2$ 为例，描述协议的跨域认证工作过程. $\text{KGC}_1$ 和 $\text{KGC}_2$ 分别为两个域的密钥生成中心，主密钥分别为 $s_1$ 和 $s_2\in[1,p-1]$，对应的系统公钥分别为 $P_{\text{public1}}=[s_1]P$ 和 $P_{\text{public2}}=[s_2]P$. 表 1 中定义了以下协议过程描述用到的重要符号.

**表 1 协议符号定义**

| 符号 | 定义 |
|---|---|
| $A\rightarrow B:\{m\}$ | 从实体 $A$ 到实体 $B$ 发送消息 $m$ |
| $Encry(m)$ | 对消息 $m$ 实施非对称加密计算 |
| $IBS(m)$ | 对消息 $m$ 实施基于身份的签名计算 |
| $IBE(m)$ | 对消息 $m$ 实施基于身份的加密计算 |
| $Cert_{\text{BCCA}m}$ | $\text{IBC}_m$ 域的区块链证书 |

(1) $\text{U}_1\rightarrow\text{BCCA}_1:\{ID_{\text{U}_1},ID_{\text{ISE}_2},T_1,Request_1,IBS(ID_{\text{U}_1}\|ID_{\text{ISE}_2}\|Request_1\|T_1)\}$

$\text{U}_1$ 向 $\text{BCCA}_1$ 发起 $\text{ISE}_2$ 身份认证请求，$T_1$ 为时间戳，为证明自己的合法性，使用自身私钥对消息进行 IBS 签名操作.

(2) $\text{BCCA}_1\rightarrow\text{BCCA}_2:\{Encry(ID_{\text{ISE}_2},T_2,Cert_{\text{BCCA}_1},Request_2)\}$

$\text{BCCA}_1$ 收到请求后确认用户 $\text{U}_1$ 合法身份，确认 $T_1$ 在有效范围内，并在链上查询 $\text{ISE}_2$ 对应的域代理 $\text{BCCA}_2$. $\text{BCCA}_1$ 选取时间戳 $T_2$、$ID_{\text{ISE}_2}$、区块链证书 $Cert_{\text{BCCA}_1}$、认证请求，加密后发送给 $\text{BCCA}_2$.

(3) $\text{BCCA}_2\rightarrow\text{BCCA}_1:\{Encry(P_{\text{public2}},T_3)\}$

$\text{BCCA}_2$ 收到并解密 $\text{BCCA}_1$ 的消息，验证 $T_2$ 后，与 IAS 联合查验 $Cert_{\text{BCCA}_1}$ 的合法性，若证书有效则响应 $Request_2$；同时 $\text{BCCA}_2$ 将所在域的系统主公钥 $P_{\text{public2}}$ 与时间戳 $T_3$ 加密后返回给 $\text{BCCA}_1$.

(4) $\text{BCCA}_1\rightarrow\text{BCCA}_2:\{Encry(P_{\text{public1}},T_4)\}$

$\text{BCCA}_1\rightarrow\text{IAS}_1:\{IBE(K,T_5,Request_3)\}$

$K=H_1(ID_{\text{U}_1}\|ID_{\text{ISE}_2})\cdot[s_1]\cdot P_{\text{public2}}$

$\text{BCCA}_1$ 收到并解密 $\text{BCCA}_2$ 发送的消息，验证 $T_3$ 有效后，保存 $\text{IBC}_2$ 域的系统公钥 $P_{\text{public2}}$. $\text{BCCA}_1$ 同样需要将自身域的系统公钥 $P_{\text{public1}}$ 与一个时间戳 $T_4$ 加密后返回给 $\text{BCCA}_2$，同时 $\text{BCCA}_1$ 根据上式计算会话密钥 $K$，IBE 加密后发送给 $\text{IAS}_1$.

(5) $\text{BCCA}_2\rightarrow\text{ISE}_2:\{IBE(K',T_6,Request_4)\}$

$K'=H_1(ID_{\text{U}_1}\|ID_{\text{ISE}_2})\cdot[s_2]\cdot P_{\text{public1}}$

$\text{BCCA}_2$ 收到 $\text{BCCA}_1$ 的消息，验证 $T_4$ 有效后，保存 $\text{IBC}_1$ 域的系统公钥 $P_{\text{public1}}$. $\text{BCCA}_2$ 计算会话密钥 $K'$(显然 $K'=K$)，IBE 加密后发给 $\text{ISE}_2$.

(6) $\text{ISE}_2\rightarrow\text{IAS}_1:\{C,\langle S_m\rangle\}$，$C=m\oplus K'$

$\text{ISE}_2$ 获得 $\text{BCCA}_2$ 发送的消息，验证 $T_6$ 有效后，保存会话密钥 $K'$. 根据 mIBS 算法，$\text{ISE}_2$ 通过仲裁获得消息 $m$ 的完整签名$\langle S_m\rangle$. 最后，$\text{ISE}_2$ 计算密文 $C$ 后，同签名结果$\langle S_m\rangle$一起发给 $\text{IAS}_1$.

(7) $\text{IAS}_1\rightarrow\text{U}_1:\{IBE(\text{True},K,T_7)\}$

在步骤(4)中，$\text{IAS}_1$ 会解密来自 $\text{BCCA}_1$ 的消息，验证 $T_5$ 后获得会话密钥 $K$，通过 $K$ 解密 $C$ 获得消息 $m$，就可以用 mIBS 签名算法验证$\langle S_m\rangle$获知 $\text{ISE}_2$ 的合法性. 验证通过后，$\text{IAS}_1$ 将成功认证消息、会话密钥 $K$ 及时间戳基于身份加密后发送给用户 $\text{U}_1$，否则中止验证过程.

### 5.2 安全性分析

#### 5.2.1 会话密钥安全证明

会话密钥 $K=K'$ 的安全性是基于攻击者 UM 模型提出的. 在这个模型中，会话密钥需具备如下安全性质[21].

**性质 1.** 若通信双方都没有被攻陷且会话匹配，则双方获得的会话密钥是一致的.

**引理 1.** 假定 $Encry(m)$ 采用 ECC 加密算法，$IBS(m)$ 和 $IBE(m)$ 基于椭圆曲线的双线性映射实现，均为选择密文攻击(Chosen Ciphertext Attack, CCA)安全的. 若 U、ISE、SEM、IAS 及 BCCA 等实体或节点都未被攻陷，则会话密钥 $K=K'$ 将能够在协议执行过程中被成功地协商.

证明. 反证法. 假设攻击者成功伪造协议认证过程中实体间传递的消息的概率 $\varepsilon$ 不可忽略，那么对于上述协议各个步骤的破解概率为：

第(1)步攻击者成功伪造消息的概率等同于破解 IBS 算法的概率 $\varepsilon_{\text{IBS}}$；

第(2)和(3)步中，攻击者伪造消息的成功概率，等同于破解 ECC 加密算法的概率 $\varepsilon_{\text{ECC}}$；

第(4)和(5)步，攻击者伪造消息的成功概率，等同于破解 IBE 算法的概率 $\varepsilon_{\text{IBE}}$；

第(6)步，攻击者伪造消息的成功概率，等同于破解 IBS 算法的概率 $\varepsilon_{\text{mIBS}}$；

第(7)步，攻击者伪造消息的成功概率，等同于破解 IBE 算法的概率 $\varepsilon_{\text{IBE}}$；

综上，$\varepsilon\leq\varepsilon_{\text{IBS}}+2\varepsilon_{\text{ECC}}+3\varepsilon_{\text{IBE}}+\varepsilon_{\text{mIBS}}+\cdots$，概率 $\varepsilon$

计算机学报

不可忽略,因此证明性质 1 成立.　　证毕.

**性质 2.**　攻击者不能以不可忽略的优势在会话测试询问过程中,辨别随机数和会话密钥.

**引理 2.**　假定 $IBE(m)$ 算法符合 CCA 安全,则攻击者不能以不可忽视优势辨别随机数和会话密钥.

证明.　为了达到在协议运行过程中辨别随机数和会话密钥的目标,攻击者在步骤(4)和(5)中不可避免地要解密 $IBE(m)$ 算法,以便得到会话密钥 $K$ 和 $K'$. 引理肯定 $IBE(m)$ 算法符合 CCA 安全,所以攻击者不可能以不可忽视的优势,辨别出协议执行过程中的随机数和会话密钥,因此性质 2 成立.　证毕.

在整个会话密钥的协商过程中,各个 IBC 域的主密钥 $s_1$ 和 $s_2$ 是不能被攻击者所轻易获取的,尽管攻击者可以得到 $P_{\text{public1}}=[s_1]P$ 和 $P_{\text{public2}}=[s_2]P$,但仍然不能计算出 $[s_1][s_2]P$ 的值,所以最终也就不能计算得到会话密钥 $K$. 所以本文的跨域认证协议是会话密钥安全的.

### 5.2.2　协议安全证明

以下采用安全协议的博弈论机制[22]来证明协议安全性. 假设 $M$ 给 $N$ 发送消息,$Q$ 为攻击者,CE(Communication Environment)为通信环境,$P$ 代表参与者集合,记作 $P=\{M,N,Q,CE\}$,且 $P'=P/\{CE\}$. 假设 $Q$ 获得消息的概率至多为 $\gamma$,$M$ 确定只有 $N$ 获得消息的概率为 $\beta$,$N$ 确定消息发出者是 $M$ 的概率为 $\alpha$. 各个参与者都理性地选择策略来尽可能最大化自身收益. 当系统激活以后,不考虑参与者主动退出,$M$ 可选择发送正确加密消息 $m$ 或非正确加密消息 $m^*$ 至网络;$Q$ 截获消息后,获得消息明文的概率为 $\gamma$;$N$ 收到消息后,从中解出正确明文的概率为 $\beta$,最后验证是 $M$ 发出该消息的概率为 $\alpha$.

图 4 中博弈树表达可见,博弈达到纳什均衡 $(\alpha,\beta,\gamma)$ 的最优结果为 $(q_1q_2q_3q_4q_5q_7q_9)$,显然安全通信阶段的密码算法直接影响博弈结果. 由表 2 可见,本文构造的跨域认证协议同时使用加密算法和签名算法,满足安全协议的博弈论机制的双重要求.

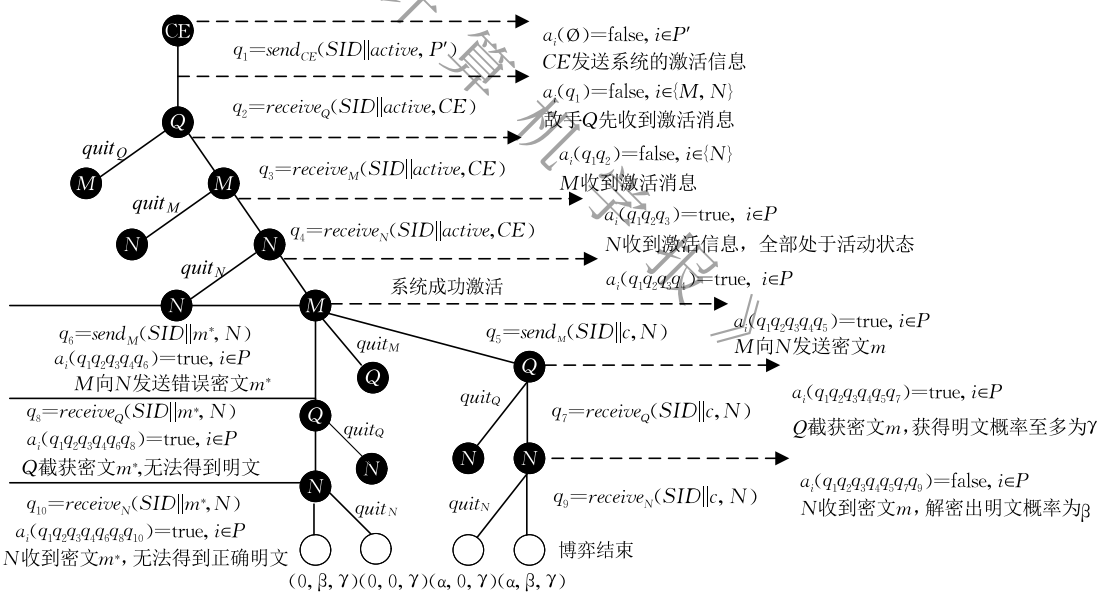


图 4　安全协议博弈树

**表 2　协议算法对安全博弈影响对比**

| 算法 | 保密 | 认证 | 纳什均衡 |
|---|---|---|---|
| 加密 | ✓ | × | $q_1q_2q_3q_4q_5quit_Qquit_N$ |
| 签名 | × | ✓ | $q_1q_2q_3q_4quit_Mquit_Qquit_N$ |
| 本文 | ✓ | ✓ | $q_1q_2q_3q_4q_5q_7q_9$ |

### 5.2.3　协议安全性对比

以下列出针对身份认证系统的主流攻击模式,逐一分析本文方案在各种攻击场景下的安全程度,并通过表 3 与其他方案进行安全性对比.

(1) 内部攻击. 本文方案基于联盟区块链实现跨域身份信息传递和认证,区块链的哈希函数、签名算法等均提供了数据信任机制和匿名化能力. 不同域的用户身份均通过该域的 BCCA 代理进行链上验证. 这些都可以帮助抵抗内部攻击.

(2) 假冒攻击. 各域的 BCCA 和 IAS 都对用户身份进行验证,可识别假冒用户. 只有在签名验证通过后,通信双方才能互信身份. BCCA 之间传递信息是通过非对称加密算法保护的. 无论是伪造签名还是破解加密、推导私钥,都是相当计算困难的. 因此本文方案可以抵抗假冒攻击.

(3)重放攻击. 在整个协议交互过程中都引入了时间戳机制,用以验证消息的时效性,且未带来显著通信负担[23]. 同时在交互签名的过程中同时引入了随机数. 因此本文方案可以有效抵抗重放攻击.

(4)欺骗攻击. mIBS 签名算法设计有仲裁验证机制和身份撤销能力,这都可以抵抗身份不明或失效实体进行欺骗攻击.

(5)双向实体认证. 本文方案中域内采用基于 IBC 身份认证的方式,域间通过代理节点在联盟链网络中查询及验证区块链证书交易,最终实现跨域认证功能. 域间可双向发布授权交易到区块链上,因此支持跨域实体之间的双向身份认证.

(6)分布式拒绝服务攻击:本文跨域认证方案基于区块链的去中心化架构,具有分布式系统的分散性、动态调节性、冗余性、容错能力,无单点失效的脆弱点,可抵抗分布式拒绝服务攻击.

**表 3 模型协议的安全性对比**

| 方案 | 安全性 | | | | | |
|---|---|---|---|---|---|---|
| | 抵抗内部攻击 | 抵抗假冒攻击 | 抵抗重放攻击 | 抵抗欺骗攻击 | 双向实体认证 | 抵抗分布式拒绝服务攻击 |
| 文献[7] | ✓ | ✓ | × | × | ✓ | ✓ |
| 文献[12] | ✓ | × | ✓ | × | ✓ | ✓ |
| 文献[24] | ✓ | ✓ | ✓ | × | × | ✓ |
| 文献[11] | ✓ | ✓ | ✓ | ✓ | ✓ | × |
| 本文方案 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

## 5.3 性能分析

### 5.3.1 mIBS 算法性能分析

mIBS 算法用于对信息服务实体进行身份验证和权限管理,在整个跨域身份认证协议过程中反复执行. 因此首先对 mIBS 的签名和验证过程执行效率进行评估,再与基于仲裁的身份签名算法 ID-BMS[25]进行比较. 二者 Setup 算法过程都是在有限域上椭圆曲线和双线性映射下实现,无需比较. 身份签名过程两者都采用 SEM 进行一致性仲裁,包含用户密钥生成 KeyGen 算法、签名 Sign 算法(包括用户预签名、SEM 签名、用户签名)、用户签名验证 Verify 算法三部分,以下对签名过程进行拆解,分析各子阶段中的计算开销. 拆解出的运算操作包括如下六种:

$e$:双线性对运算;

$H_1$:哈希运算 $H_1:\{0,1\}^* \rightarrow G_1^*$;

$H_2$:哈希运算 $H_2:\{0,1\}^* \times G_2^* \rightarrow Z_N^*$;

$M_G$:群 $G$ 上的乘法运算(群 $G_1$ 和群 $G_2$ 的点乘运算开销基本一致,合并考虑);

$A_G$:群 $G$ 上的加法运算(群 $G_1$ 和群 $G_2$ 的点乘运算开销基本一致,同样合并考虑);

$E_G$:指数操作运算.

表 4 与图 5 中可以看到,本文 mIBS 算法与 ID-BMS 算法相比,签名过程效率更高. mIBS 指数运算增加了 1 次,却节省了哈希运算 $H_2$ 1 次,减少了群 $G$ 上的乘法运算 4 次、加法运算 3 次,并且实现了 IBC 系统内实体身份撤销功能. ID-BMS 方案在用户预签名阶段运算量极小,但它在签名过程直接将消息明文 $m$ 提交给 SEM 进行验证,面临用户隐私的泄露风险. 本文 mIBS 算法增加 1 次双线性对运算和 1 次哈希运算用于隐藏签名消息 $m$ 原文,以有限计算开销换取了显著的安全提升. 实际应用过程中,用户可以针对群 $G_2$ 提前计算元素 $q$ 的值 $e(kP_1,P)$,因而用户预签名阶段的运算时间开销对整个签名过程的性能影响是可以忽略的. 在用户签名和用户验证阶段,mIBS 方案对比 ID-BMS 方案具有明显的计算操作节省. 综上所述,本文 mIBS 在安全和效率上相较 ID-BMS 方案具有更均衡更优异的性能.

**表 4 mIBS 和 ID-BMS 算法各阶段效率对比**

| 阶段 | 方案 | |
|---|---|---|
| | ID-BMS 方案 | mIBS 方案 |
| 密钥生成 | $1H_1+2M_G+1A_G$ | $1H_1+2M_G+1A_G$ |
| 用户预签名 | $1M_G$ | $1e+1H_2+2M_G+1A_G$ |
| SEM 签名 | $2e+1H_2+3M_G+2A_G$ | $2e+1H_1+2M_G+1A_G+1E_G$ |
| 用户签名 | $2e+1H_2+3M_G+3A_G$ | $2e+1A_G$ |
| 用户验证 | $1H_1+1H_2+1M_G+1A_G$ | $1H_2$ |

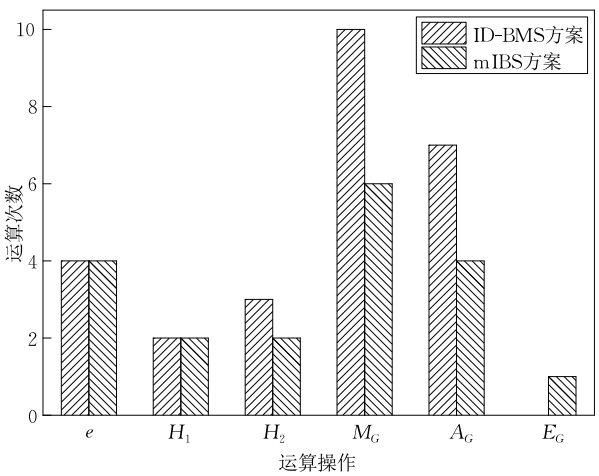


图 5 mIBS 方案性能对比

《计算机学报》

### 5.3.2　跨域认证协议性能分析

假定跨域身份认证过程中,协议中实体交互通信的相关字段如表 5 所示,以下评估协议的通信负载和计算开销两方面性能.

**表 5　跨域认证协议的相关字段大小**

| 字段 | 长度 | 字段 | 长度 |
|---|---|---|---|
| 消息 | 80 | 对称加解密密文 | 128 |
| 身份 | 80 | 非对称加解密密文 | 160 |
| 时间戳 | 16 | 签名消息 | 160 |
| mIBS 群 | 160 | 证书密文 | 160 |

本文对比了其他跨域认证方案,表 6 给出了各个协议在通信量和运算量方面的统计,其中将协议的计算开销分解成用户端、ISE端和其他服务器端各自单独进行统计. 表 7 是对表 6 中各类运算含义的详细说明,其中时间数据是在一台配置有 i7-10710U 处理器、16 GB 内存、64 位 Windows 10 操作系统的计算机上实验测试得到.

Yuan[24] 和 Wang 等人[12] 的跨域认证方案在论文中缺少对设计的协议所使用的具体算法的描述. 为了采用统一标准来比较表 6 中的三个协议,本文在实验过程中假设三个协议均采用相同类型的加/解密算法. 采用 AES 算法作为对称加/解密算法实现,基于椭圆曲线的 ECC 算法进行非对称加/解密和签名实现,BF-IBE 作为基于身份的加/解密和签名算法实现. 图 6 展示了各端在不同方案中的跨域身份认证过程计算时间开销统计.

**表 6　身份跨域认证协议通信量和计算量对比**

| 方案 | 性能 | | | |
|---|---|---|---|---|
| | 总通信量/bits | 用户端计算量 | ISE 端计算量 | 其他端计算量 |
| Yuan 等方案[24] | 1808 | $T_{IBV}+T_{AS}+2T_{AE}+T_{AD}+T_{SE}+T_{IBD}$ | $T_{IBV}+2T_{IBE}+T_{SE}+T_{SD}$ | $2T_{IBS}+T_{IBD}+T_{AS}+2T_{AV}+T_{AE}+2T_{AD}$ |
| Wang 等方案[12] | 2720 | $2T_{AS}$ | | $2T_{AV}$ |
| 本文方案 | 1616 | $T_{IBS}$ | $2T_e+2T_{PM}+2T_{AM}+T_{IBV}$ | $2T_{AE}+2T_{AD}+2T_{IBE}+2T_{IBD}+2T_{PM}+2T_{AM}+T_E$ |

**表 7　各种运算时间消耗量**

| 操作 | 时间/ms |
|---|---|
| 基于身份签名 $T_{IBS}$ | 1.684 |
| 基于身份签名验证 $T_{IBV}$ | 1.723 |
| 基于身份加密 $T_{IBE}$ | 1.643 |
| 基于身份解密 $T_{IBD}$ | 1.608 |
| 对称加密 $T_{SE}$ | 0.004 |
| 对称解密 $T_{SD}$ | 0.004 |
| 非对称加密 $T_{AE}$ | 0.836 |
| 非对称解密 $T_{AD}$ | 0.836 |
| 非对称签名 $T_{AS}$ | 0.834 |
| 非对称签名验证 $T_{AV}$ | 0.072 |
| 双线性对 $T_e$ | 1.112 |
| 点乘运算 $T_{PM}$ | 0.407 |
| 点加运算 $T_{AM}$ | 0.003 |
| 指数运算 $T_E$ | 0.131 |

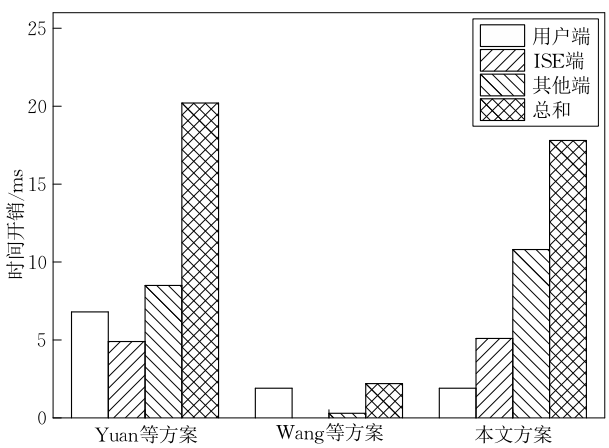


图 6　协议时间开销对比

结合两个图表,可见本文方案在通信量方面均小于 Yuan 等人、Wang 等人的方案,体现了本文跨域协议在通信复杂性上的优势. 在计算时间方面,Wang 等人的方案耗时极小,但是该协议却存在和 ID-BMS 算法一样的安全弱点,即在用户认证的全过程中消息都是以明文的形式进行转发,节省消息的编码计算时间却带来了消息内容暴露缺陷. 相对于 Yuan 等人提出的方案,本文所提出的协议在用户端的计算开销更小,将用户端的计算量向信息服务实体和其他服务节点进行了转移. 实际应用中资源受限的用户终端,对计算开销更敏感,而其他服务器类实体或节点反而可以承担更多计算工作. 综合来看,本文方案通过区块链域代理服务器 BCCA、仲裁服务器 SEM 等多方共同辅助完成实体的双向认证过程,更多地将协议计算开销承载于用户之外的服务器端,计算量和通信量都比 Yuan 等人的方案总体有所降低,更适用于大规模跨信任域的主流用户的真实应用场景.

本文方案的跨域认证过程,主要是相关节点在联盟链上对用户的身份信息进行查验. 区块链各代理节点都会有完整数据拷贝,快速认证过程仅是链上交易的本地查询操作,可以快速在本地进行链上数据读取[26]. 快速认证模式下的认证时间在实验过程中始终维持在 0.2 s～0.25 s 之间. 当终端用户的

《计算机学报》

跨域认证请求次数或者 IBC 信任域的数量增加时，对于分布式架构的联盟链系统，也不会因为盟员增加导致双方跨域认证过程中公钥算法次数的增加. 增加联盟成员数量的确会由于区块链联盟维护账本而需要更多哈希运算次数. 针对这个问题，本文在同等配置的机器上进行测试，如图 7 所示，对于 1 MB 大小文件多次运行测试程序并记录时间消耗发现，ECDSA-192 的耗时约为 RSA-1024 的 2 倍，SHA-256 仅为 RSA-1024 的 10%左右. 跨域过程中哈希运算速度要远高于公钥算法运算，所以即使在节点数量众多的信任域联盟认证场景下，本文方案实现跨域认证的运算效率与认证吞吐率也有所保证.

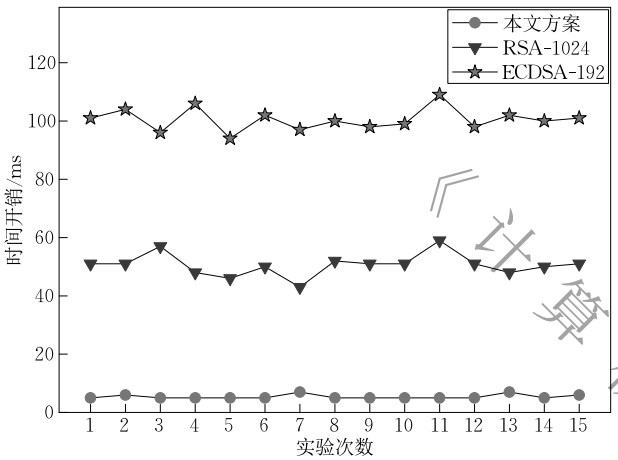


图 7 跨域认证过程哈希运算时间对比

## 6 总 结

面向多域信息网络系统中用户身份验证和跨域认证迁移的需求，本文针对现有基于 PKI 和 IBC 身份认证机制在跨域认证应用方面的局限性，在 IBC 方案的基础上，采用区块链技术构建可以分布式发布和即时查验区块链证书的跨域认证系统，提供了一种基于身份密码体制的跨信任域认证方案. 针对 IBC 架构下实体身份撤销不及时、不方便的问题，引入安全仲裁节点和步骤进入域内身份签名验证过程. 方案实现了系统性能和安全性的有效均衡，能够满足大规模网络环境和众多服务实体情况下，用户与信息服务实体间跨域认证的频繁需求处理. 对于所提出的跨域身份认证方案，理论分析了方案的安全性和有效性，实验测试并与同类对比了具体方案的关键步骤实施运算效率. 未来计划构造联盟链网络原型进行实验，完整实现并实际运行各方案，度量异域用户到实体间访问交互全过程完整跨域认证协议执行所需系统开销，通过对多组不同的数据（计算时延、消息数量、存储开销等）进行测试来实现典型应用场景中的效果评估.

## 参 考 文 献

[1] Gogna M, Krishna C R. Cross-domain authentication and interoperability scheme//Proceedings of the Smart Systems and IoT: Innovations in Computing. Singapore, 2019: 451

[2] Chandra S, Mandal B, Alam S S, et al. Content based double encryption algorithm using symmetric key cryptography. Procedia Computer Science, 2015, 57: 1228-1234

[3] Canetti R, Shahaf D, Vald M. Universally composable authentication and key-exchange with global PKI//Proceedings of the IACR International Workshop on Public Key Cryptography (PKC). New York, USA, 2016: 265-296

[4] Gu P, Chen L. An efficient blockchain-based cross-domain authentication and secure certificate revocation scheme//Proceedings of the IEEE International Conference on Computer and Communications. Chengdu, China, 2020: 1776-1782

[5] Zheng Z, Xie S, Dai H N, et al. Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 2018, 14(4): 352-375

[6] Aste T, Tasca P, Di Matteo T. Blockchain technologies: The foreseeable impact on society and industry. Computer, 2017, 50(9): 18-28

[7] Zhang W, Wang X, Khan M K. A virtual bridge certificate authority-based cross-domain authentication mechanism for distributed collaborative manufacturing systems. Security and Communication Networks, 2015, 8(6): 937-951

[8] Yan Hai-Long, Yu Jian-Ping, Hu Qiang, et al. Research and implementation of distributed cross-domain trust platform based on PKI/CA. Computer Engineering and Design, 2013, 34(2): 686-690(in Chinese)
(颜海龙，喻建平，胡强等. 基于 PKI/CA 的分布式跨域信任平台研究与实现. 计算机工程与设计，2013，34(2)：686-690)

[9] Li Y, Chen W, Cai Z, et al. CAKA: A novel certificateless-based cross-domain authenticated key agreement protocol for wireless mesh networks. Wireless Networks, 2015, 22(8): 1-13

[10] Luo Chang-Yuan, Huo Shi-Wei, Xing Hong-Zhi. Identity-based cross-domain authentication scheme in a universal environment. Journal of Communications, 2011, 32(9): 111-115+122(in Chinese)
(罗长远，霍士伟，邢洪智. 普适环境中基于身份的跨域认证方案. 通信学报，2011，32(9)：111-115+122)

[11] Wang C, Liu C, Niu S, et al. An authenticated key agreement protocol for cross-domain based on heterogeneous signcryption scheme//Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC). Valencia, Spain, 2017: 723-728

《计算机学报》

[12] Wang W, Hu N, Liu X. BlockCAM: A blockchain-based cross-domain authentication model//Proceedings of the IEEE Third International Conference on Data Science in Cyberspace (DSC). Guangzhou, China, 2018: 896-901

[13] Ma Xiao-Ting, Ma Wen-Ping, Liu Xiao-Xue. Cross-domain authentication scheme based on blockchain technology. Chinese Journal of Electronics, 2018, 46(11): 2571-2579(in Chinese)
(马晓婷，马文平，刘小雪. 基于区块链技术的跨域认证方案. 电子学报，2018，46(11)：2571-2579)

[14] Kuzhalvaimozhi S, Rao G R. Public key encryption without using certificate based on identity based cryptography. International Journal of Scientific Engineering & Technology, 2014, 3(2): 139-143

[15] Blazy O, Kiltz E, Pan J. (Hierarchical) Identity-based encryption from affine message authentication//Proceedings of the Cryptology Conference. Berlin, Germany, 2014: 408-425

[16] Liang K, Liu J K, Wong D S, et al. An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing//Proceedings of the European Symposium on Research in Computer Security. Wroclaw, Poland, 2014: 257-272

[17] Bay A, Huang J, Vaudenay S. Improved linear cryptanalysis of reduced-round MIBS//Proceedings of the International Workshop on Security. Hirosaki, Japan, 2014: 204-220

[18] Hari A, Lakshman T V. The Internet blockchain: A distributed, tamper-resistant transaction framework for the Internet//Proceedings of the ACM Workshop on Hot Topics in Networks. Atlanta, USA, 2016: 204-210

[19] Xu Y, Zhao S, Kong L, et al. ECBC: A high performance educational certificate blockchain with efficient query//Proceedings of the International Colloquium on Theoretical Aspects of Computing. Hanoi, Vietnam, 2017: 288-304

[20] Li X, Niu J, Liao J, et al. Cryptanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update. International Journal of Communication Systems, 2015, 28(2): 374-382

[21] Elashry I, Mu Y, Susilo W. A resilient identity-based authenticated key exchange protocol. Security and Communication Networks, 2015, 8(13): 2279-2290

[22] Halpern J Y, Pass R. Game theory with costly computation: Formulation and application to protocol security//Proceedings of the Innovations in Computer Science (ICS). Beijing, China, 2010: 1

[23] Chou C H, Tsai K Y, Lu C F. Two ID-based authenticated schemes with key agreement for mobile environments. The Journal of Supercomputing, 2013, 66(2): 973-988

[24] Yuan C, Zhang W, Wang X. EIMAKP: Heterogeneous cross-domain authenticated key agreement protocols in the EIM system. Arabian Journal for Science and Engineering, 2017, 42(8): 3275-3287

[25] Santosh G, Mukhopadhyay D, Chowdhury D. Fault attack and countermeasures on pairing based cryptography. International Journal of Network Security, 2011, 12(1): 21-28

[26] Zhou B, Li H, Xu L. An authentication scheme using identity-based encryption & blockchain//Proceedings of the IEEE Symposium on Computers and Communications (ISCC). Murcia, Spain, 2018: 556-561

《计算机学报》

**WEI Song-Jie**, Ph. D., associate professor. His research interests include information and network security, Internet protocols design and analysis, blockchain.

**LI Sha-Sha**, M. S. candidate. Her research interests include blockchain application and distributed system.

**WANG Jia-He**, M. S. His main interests include blockchain technology, protocol design, and user authentication.

**Background**

Information and services are expanding across domains with the rapid growth of computer network scale and coverage. Users tend to interact with more domain-wide information services entities (ISE) more frequently, and the procedures are being threatened by various system attacks and service abuses if not enough authentication is guaranteed. While having been heavily researched in the field of cyberspace security, traditional centralized identity authentication technology is insufficient to satisfy entity authentication and access control requirements through complex network environments. Therefore, under the premise of security, decentralized identity authentication schemes with efficiency appear promising and attract close attentions in both academia research and industrial application.

Blockchain, as a distributed system with embedded trust, especially the consortium chain architecture based on group consensus, provides a new approach to implement identity authentication under the conditions of multi-party cooperation

in cyber scenarios. Therefore, in order to solve the limitations of the centralized identity authentication technology, this paper studies the distributed identity authentication problem, and proposes innovative identity authentication schemes combined with the blockchain technology.

While our proposed scheme applies IBC for intra-domain authentication, to alleviate the problem of identity revoking difficulty in IBC system, we first introduce a security mediator-based identity signature scheme. This adds a mediator server in each IBC authentication system. An identity's private key is partially distributed to the mediator for storage, and the mediator helps verifying its identity when an entity requests a full authentication signature, thereby controlling the user's access to achieve the purpose of revoking identities flexibly by the mediator. mIBS algorithm is designed to support such mediator-based authentication and identification verification.

We provide a more efficient cross-domain authentication scheme and protocol with a combination of identity-based cryptography and the blockchain. A type of blockchain certificate is proposed to implement cross-domain authentication using the distributed architecture of blockchain, which integrate IBC trust domains on a consortium blockchain. The IBC cross-domain authentication protocol is proved theoretically for robustness, and evaluated and benchmarked with algorithm analysis and experimental measures.

The presented work is partially supported by the funds from the National Natural Science Foundation of China under Grant Nos. 61802186 and 61472189, the CERNET Innovation Project NGII20180103, and the Shanghai Astronautics Innovation Fund SAST2019-033. The authors are grateful to these sponsorships.

《计算机学报》