

基于联盟链的跨域认证方案

牛建林, 任志宇, 杜学绘

(信息工程大学, 河南 郑州 450001)

摘要: 针对传统跨域认证易单点失效、过度依赖第三方等安全问题, 提出了一种结合基于身份的密码(IBC, identity-based cryptography)体制与联盟链的跨域认证方案。通过设计包括实体层、代理层、区块链层、存储层在内的分层跨域认证架构, 在跨域认证场景中引入联盟链, 从而能够使两者较好地融合, 增加了联盟链在跨域认证场景中的适应性。在存储层, 设计摘要数据格式, 将其存储于链上, 摘要数据对应的完整数据存储在链下的星际文件系统, 从而形成一种安全可靠的链上链下分布式存储方案, 解决引入区块链后存在的链上存储受到限制的问题。提出一种基于永久自主权身份和临时身份的身份管理方案, 解决结合IBC体制后身份难以注销和匿名身份难以监管的问题。在此基础上, 设计完整的跨域全认证、重认证以及密钥协商协议以实现跨域认证流程。在安全性方面, 使用SVO逻辑对认证协议进行分析, 证明了跨域认证协议的安全性。通过仿真对计算负载性能、通信负载以及联盟链性能进行了测试与分析。分析表明, 与相关方案相比, 协议在满足安全性的同时, 在服务端和用户端均有较好的计算负载表现。在通信效率上, 相较于其他方案有不错的表现。通过联盟链工具对链上读写时延进行了测试, 结果表明所提方案有良好的可用性。

关键词: 跨域认证; 联盟链; 基于身份的密码体制; 身份管理

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022036

Cross-domain authentication scheme based on consortium blockchain

NIU Jianlin, REN Zhiyu, DU Xuehui

Information Engineering University, Zhengzhou 450001, China

Abstract: To solve the security problems of traditional cross-domain authentication schemes, such as single point of failure and excessive dependence on third parties, a cross-domain authentication scheme was proposed which combines IBC and consortium blockchain. The consortium blockchain was introduced into the cross-domain

收稿日期: 2021-09-12; 修回日期: 2022-03-02

通信作者: 任志宇, en_ktzy@163.com

基金项目: 国家重点研发计划(2018YFB0803603); 国家自然科学基金(61702550, 61802436)

Foundation Items: The National Key R&D Program of China (2018YFB0803603), The National Natural Science Foundation of China (61702550, 61802436)

引用格式: 牛建林, 任志宇, 杜学绘. 基于联盟链的跨域认证方案[J]. 网络与信息安全学报, 2022, 8(3): 123-133.

Citation Format: NIU J L, REN Z Y, DU X H. Cross-domain authentication scheme based on consortium blockchain[J]. Chinese Journal of Network and Information Security, 2022, 8(3): 123-133.

authentication scene by designing the layered cross-domain authentication architecture including entity layer, proxy layer, blockchain layer and storage layer. In the storage layer, abstract data format was designed and stored in the chain, and the complete data corresponding to the abstract data was stored in the interplanetary file system under the chain. This safe and reliable on-chain distributed storage scheme solved the limitation problem of on-chain storage caused by introduction of blockchain. Besides, an identity management scheme based on permanent autonomy identity and temporary identity was proposed to solve the challenges that it is difficult to cancel identity and to supervise anonymous identity after combining IBC system. On this basis, complete cross-domain full authentication, re-authentication and key negotiation protocols were designed to implement the cross-domain authentication process. In terms of security, SVO logic was used to analyze the authentication protocol, and the security of the cross-domain authentication protocol was proved. The performance of calculation overhead, communication overhead and consortium blockchain were tested and analyzed by simulation. Analysis results showed that the protocol satisfies the security requirements and has improved calculation overhead performance on both server and client sides, comparing with other related works. In terms of communication overhead, it also has better performance. The query/write latency was tested by the consortium blockchain tool, and the results showed that the scheme has good usability.

Keywords: cross-domain authentication, consortium blockchain, identity-based cryptography, identity management

0 引言

跨域认证一直是网络安全界尤为关注的问题。尽管目前有许多关于跨域访问的解决方案,不同信任域的不同设备可以很容易地在当前网络框架下互联,但是仍有许多信任与安全的问题尚待解决。目前,多数认证的解决方案是基于公钥基础设施(PKI, public key infrastructure)^[1]的。在 PKI 中,引入证书权威机构(CA, certificate authority)作为可信第三方(TTP, trusted third party)。随着实体的数目增加,伴随而来的大量证书的管理,给系统带来了不小的负担。此外,PKI 体系面临诸多风险,尤其是 CA 易受到攻击^[2]。近几年由于误操作导致的 CA 泄露事件也层出不穷^[3]。传统的跨域解决方案过度依赖于可信第三方,导致敏感数据被集中地存储起来。被集中存储的海量敏感数据对攻击者而言也是个不小的诱惑。

联盟链(consortium blockchain)是一种准入型区块链^[4]。它有保存着分布式账本的多个节点,但是每个节点必须得到验证后才能加入联盟链。联盟链保留着公有链的诸多特性,如能够建立节点间信任、链上数据不易篡改等。此外,相较于公有链,联盟链具有交易速度更快、能够更好保护数据隐私等特性,已在解决多方信任问题中得

到一些应用^[5]。联盟链通过密码学算法建立分布式账本,具有“组织”的概念,这与跨域认证场景中“域”的概念是相契合的。相较传统的引入多中心的方法而言,它具有防篡改、便于审计等优势。因此,借助联盟链的这些特性来解决跨域认证中的域间信任问题,不失为一种好的方法。

基于身份的密码体制(IBC, identity-based cryptography)方案可以有效规避证书管理等方面的问题,自 Shamir^[6]提出 IBC 后,2001 年,Boneh 等^[7]提出了更为实用的身份加密方案,他们利用双线性映射完成了基于身份的加密和签名。此后,有不少学者基于 IBC 针对跨域认证问题提出了解决方案。彭华熹^[8]提出一种基于 IBC 的跨域认证方案,但由于其中存在大量的双线性映射的运算,并不适合轻量化的场景使用。Bellare 等^[9]利用椭圆曲线加法群提出了一种基于身份的签名算法,避免了复杂的双线性对运算,提高了基于身份的认证效率。罗长远等^[10]在此基础上,改进了验证部分,并证明了其安全性。Yuan 等^[11]提出一种跨 IBC 和 PKI 域的 EIMAKP 方案,但计算负载和通信负载较大。

随着区块链技术研究的发展,基于区块链的跨域认证方案被提出。周致成等^[12]设计了一种基于区块链的 PKI 跨域认证方案。马晓婷等^[13]据此设计了一种基于联盟链的跨异构域认证方案,有

效降低了计算和通信负载，但在实际上仍旧是基于证书体系的认证方案，且未对链上读写性能进行分析。Shen 等^[14]将联盟链与 IBC 结合，提出了针对工业物联网的跨域认证方案。

基于此，本文将改进的 IBC 体制与联盟链结合，提出一种新的方法来解决跨域认证的问题。但这样的结合会引发一些新的问题待解决，面临的挑战如下。

1) 区块链的可存储数据限制。由于写入链上数据需要共识，且账本在每个节点上都有一份副本。倘若存储的数据过大，必然导致链上写入时延过大和数据冗余^[15]。

2) IBC 中的身份注销问题。由于 IBC 中身份由用户自己定义，因此身份注册后如何将其注销是一个需要解决的问题。

3) 身份隐私的保护。链上信息公开，若身份信息完全不加以处理地上链，则其隐私无法得到保护。

4) 匿名身份难以监管。对身份进行匿名后，虽然隐私受到保护，但存在匿名身份难以监管的问题。

为解决上述问题和应对这些挑战，本文提出了一种基于联盟链的跨域认证方法。本文工作和创新点如下。

1) 针对跨域应用场景，设计身份认证和密钥协商方案。

2) 设计了一种身份管理方法，解决 IBC 中身份难以注销的问题和匿名身份难以监管的问题。

3) 针对链上的存储限制，基于 IPFS 提出一种安全可靠的分布式链下存储方案。

1 跨域认证方案设计

本节介绍跨域认证方案的细节。在跨域认证场景中假定有两个安全域，分别为域 A 和域 B，如图 1 所示。

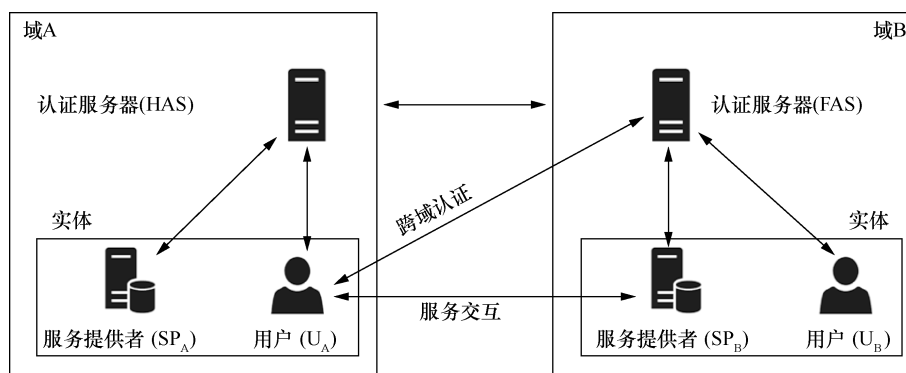


图1 跨域认证场景
Figure 1 A cross-domain authentication scenario

1.1 整体架构

本文方案使用联盟链为不同的安全域构建信任关系，避免了可信第三方的引入。在进行跨域认证时，联盟链能够保证各个域数据的一致性，且能够成为跨域认证的可靠数据共享平台。

本文的跨域认证方案使用多中心的方式，缓解了在进行跨域访问时只有一个认证中心的密钥托管和单点失效等问题。对于域内访问，本文方案并未解决中心化带来的问题，如域内只有一个 KGC 导致的密钥托管问题和单点失效问题。但如果在域内设置多个中心，必然导致计算负载急剧上升。目前的方案是在安全性与可用性之间进行折中的结果。

整个方案分为 4 层架构^[14]，分别为：实体层、代理层、区块链层和存储层。整体架构如图 2 所示。

(1) 实体层

实体层包含用户客户端、服务提供者 (SP, service provider)、认证服务器 (AS, authentication server) 和 KGC。用户客户端主要是用户用于访问服务的设备，如计算机、手持终端设备等。它们的主要行为是访问服务和在需要认证时请求 KGC 为自己生成密钥。SP 是各个域中的服务提供者，为用户提供资源访问服务。在一个域中，只有一个 KGC，它为本域内的用户和 SP 生成认证所需的私钥。在认证过程中，KGC 与认证服务

器和区块链代理服务器一起完成认证的工作。在认证的过程中,还需要进行签名和验签的工作,这些工作同样在 KGC 服务器上完成,在图中将两者分立开来是为了更清楚地表示它们的分工关系。为便于区分,本文将用户归属域的认证服务器称为 HAS (home authentication server),将跨域访问目标域的认证服务器称为 FAS (foreign authentication server)。

(2) 代理层

在代理层设区块链代理服务器 (BAS, blockchain agent server)。在每个域中,需要设置一个联盟链的节点用于维护全局账本。这个节点在本域的信息进行变更时需要将新的域信息写入

区块链,在认证其他域的实体的访问信息时查询此域的链上信息。倘若这些工作全由 KGC 完成,势必给 KGC 服务器带来较大负担。因此,需要引入 BAS 单独完成读写链上数据的任务。

(3) 区块链层

在区块链层,本文方案使用联盟链作为其底层架构。各个域的信息将存储于联盟链。在认证过程中,不同的域根据域 ID 向联盟链查询相关安全域的数据。可以预见的是,域内信息的数据量会比较大。由于区块链中存储较大的数据量必然导致交易时延过大以致不可接受,所以选择将数据的摘要存储于链上,具体域内的数据信息则存储于存储层。

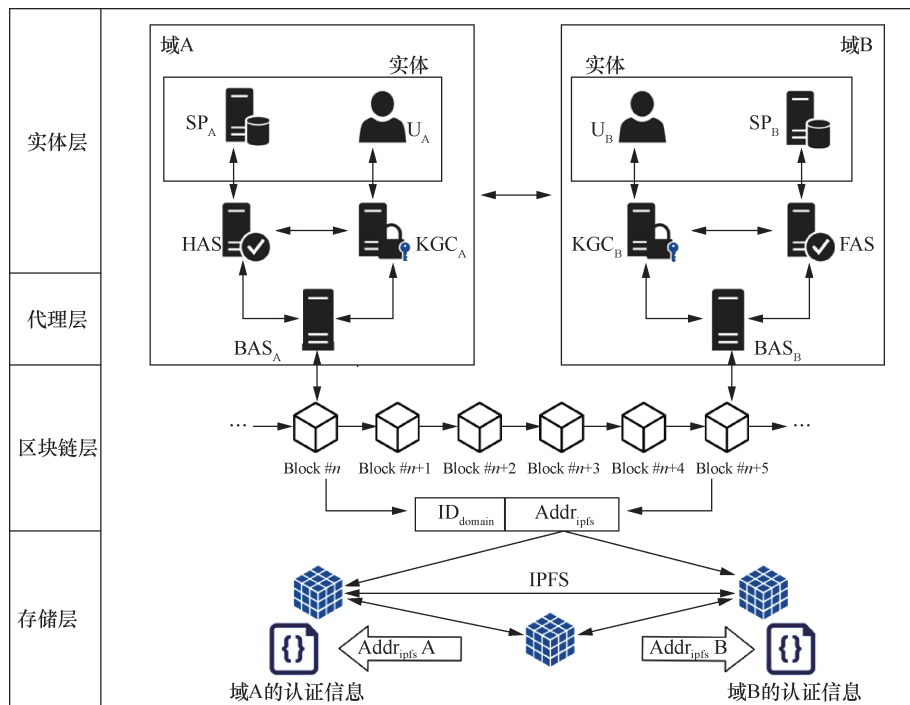


图 2 认证方案架构

Figure 2 Architecture of authentication scheme

链上存储的域内信息数据以 Key-Value 的形式进行存储,数据存储格式如图 3 所示。

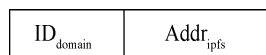


图 3 链上数据存储格式

Figure 3 Data field on blockchain

ID_{domain} 是安全域的唯一标识符。Addr_{ipfs} 是数据在 IPFS 上的地址。由于 IPFS 是一种基于内容寻址的方式,文件系统根据文件的摘要生成其唯

一的地址。这样设计,既保证了链上数据不至于过大,又避免了文件被篡改。

(4) 存储层

实际的域内信息数据被存储于一个 JSON 文件。域内信息包括安全域的名称、域内主要公开的系统参数、域内主公钥和域内实体的公钥列表。这个公钥列表中存储的是临时身份,用于跨域认证。这个 JSON 文件将被存储于区块链外的 IPFS^[16]存储系统。IPFS 是一种基于内容寻址的系

统，它将文件内容经过摘要算法和编码算法计算得到一个唯一的地址。若文件被修改，此地址将发生巨大变化。这种在链上存储 IPFS 地址信息、在 IPFS 中存储实际数据的方式，能够防篡改和突破链上存储限制。

1.2 身份管理方案

由上文可知，IBC 方案将用户的身份作为用于认证的公钥。在此，提出永久的自主权身份和临时身份。永久的自主权身份由用户自主控制，而临时身份的有效期限很短，用于跨域认证时使用。

1) 永久的自主权身份。用户在加入这个安全域时，先向 KGC 进行注册。出于隐私保护的考虑，将身份属性信息的摘要存储于链上，身份信息数据存储于用户自己的设备。一旦注册，用户拥有对身份数据的完全控制权。KGC 根据这个身份对用户进行管理。用户也可以根据需要，自主选择是否向 SP 披露个人属性信息以及披露多少信息。

2) 临时身份。用户设备生成随机数 N ，再将此随机数与永久身份结合发送给 KGC。KGC 在其后面加上身份期限再用监管公钥对其加密，生成临时身份公钥。KGC 再根据此身份公钥生成私钥。例如，用户生成随机数 N 来构造临时身份，KGC 据此生成公钥 $PK_{temp} = \{N \| PK \| T_e\}_{PK_s}$ ，其中 PK_s 为监管公钥， PK 为永久公钥， T_e 为过期时间。若需要监管，则监管方通过监管私钥解密，可恢复出临时身份对应的永久身份，达到监管和审计的目的。随后，生成私钥 sk_{temp} 。临时身份有效时间较短，可根据具体安全需求来确定（如 7 天）。

1.3 基于身份的密码体制

考虑将标识密码算法应用于本文方案，但由于此方案引入区块链代理和临时身份，需要在密钥生成阶段对此算法加以改进。

系统初始化：KGC 生成的系统参数包括椭圆曲线识别符 cid ，椭圆曲线基域 F_q 的参数；椭圆曲线方程参数 a 和 b ；扭曲曲线参数 β ；曲线阶的素因子 N 和相对于 N 的余因子 cf ；曲线 $E(F_q)$ 相对于 N 的嵌入次数 k ； $E(F_{q^{d_1}})(d_1 \text{ 整除 } k)$ 的 N 阶循环子群 G_1 的生成元 P_1 ； $E(F_{q^{d_2}})(d_2 \text{ 整除 } k)$ 的 N

阶循环子群 G_2 的生成元 P_2 ；双线性对 e 的识别符 eid ；同态映射 $\psi: G_2 \rightarrow G_1$ ；双线性对 e 的值域为 N 阶乘法循环群 $G_1 \times G_2 \rightarrow G_T$ ；签名私钥生成函数识别符 hid 。

产生私钥：KGC 先选择签名主私钥 $ks \in [1, N-1]$ ，随后计算签名主公钥 $P_{pub-s} = [ks]P_2$ ，其中 $P_{pub-s} \in G_2$ ，KGC 妥善秘密保管 ks ，公开 P_{pub-s} 。假设用户 A 的标识为 ID_A ，生成临时公钥 $PK_{temp-A} = \{N \| PK \| T_e\}_{PK_s}$ ，KGC 计算 $t_1 = H_1 \cdot (PK_{temp-A} \| hid, N) + ks$ 。若 $t_1 \neq 0$ ，计算用户私钥 $sk_{temp-A} = [ks \cdot t_1^{-1}] + ks$ ，否则，重新产生签名主私钥，计算公开 P_{pub-s} ，并将已有用户的私钥全部更新。

参数公开与链上存储：将生成的系统参数与更新后的 PK_{temp} 列表存储至 IPFS 文件系统，并将此 IPFS 地址与本域 ID 打包发送至 BAS 以存储于链上。

1.4 全认证

全认证包括临时身份生成和跨域认证（如图 4 所示）两个阶段。做以下规定： $[M]_{Alice}$ 表示使用 Alice 私钥进行的签名； $\{M\}_{Alice}$ 表示使用 Alice 公钥加密的信息。

(1) 临时身份生成阶段

Msg 1 $U_A \rightarrow HAS: \{text_1, [text_1]_{U_A}\}_{PK_{HAS}}$
 $text_1 = N \| ID_{temp-A}$

域 A 中的用户 U_A 需要首先确认自己的临时身份是否过期。若过期，按照身份管理方案重新生成临时身份 ID_{temp-A} 。 U_A 生成随机数 N ，向 HAS 发送请求，申请临时身份。HAS 收到后，若消息新鲜，则验证身份，并请求 KGC 根据私钥生成规则生成公私钥对 $(PK_{temp-A}, sk_{temp-A})$ 。

Msg 2 $HAS \rightarrow BAS_A: text_2, [text_2]_{HAS}$
 $text_2 = ID_{domain} \| Addr_{ipfs}$

HAS 生成公私钥对后，更新存储本域信息的 JSON 文件，重新存储于 IPFS，并向 BAS_A 发送请求，将新生成的 IPFS 地址更新至链上。HAS 将更新后的文件信息通过更新接口 `update()` 写入联盟链分布式账本中。

Msg 3 $BAS_A \rightarrow HAS: response(success)$

得到部署成功的信息之后， BAS_A 将给 HAS

发送是否成功信息。

Msg 4 $HAS \rightarrow U_A : \{PK_{temp-A}, sk_{temp-A}\}_{PK_{U_A}}$

HAS 收到链上写入数据成功的消息后, 给 U_A 秘密发送公私钥对 $(PK_{temp-A}, sk_{temp-A})$ 。

(2) 跨域认证阶段

Msg 5 $U_A \rightarrow FAS : \{text_5, [text_5]_{sk_{temp-A}}\}_{PK_{FAS}}$

$text_5 = N \parallel ID_{domain} \parallel PK_{temp-A} \parallel ext$

U_A 生成随机数 N , 构造消息 $text_5$ 。将构造的消息进行签名后加密发送至 SP_B , 随后转发至 FAS。其中, ext 为扩展字段, 可以用来传递扩展信息或者密钥协商信息。

Msg 6 $FAS \rightarrow BAS_B : query(ID_{domain})$

FAS 收到 U_A 的认证请求后, 根据 ID_{domain} 向

BAS_B 发送链上查询请求。

Msg 7 $BAS_B \rightarrow FAS : response(Addr_{ipfs})$

BAS_B 将查询到的域 A 的地址发送给 FAS。FAS 随后根据 IPFS 地址去获取域内信息。随后根据获得的 A 域的信息, 验证 U_A 的签名。若验证通过, FAS 中建立临时账户记录 $(Index_{U_A}, PK_{temp-A}, lifetime)$ 。此账户供将来重认证时使用。lifetime 为此账户的有效期, 其值可以根据安全需要设定, 若超过此有效期, FAS 删除此账户记录。

Msg 8 $FAS \rightarrow U_A : \{text_8\}$

FAS 验证通过后, 向 U_A 发送验证成功信息 $text_8 = (N \parallel index_{U_A} \parallel lifetime \parallel ext_8)$ 。其中, $index_{U_A}$ 为用户的身份索引, U_A 将以此作为之后重认证的凭证。

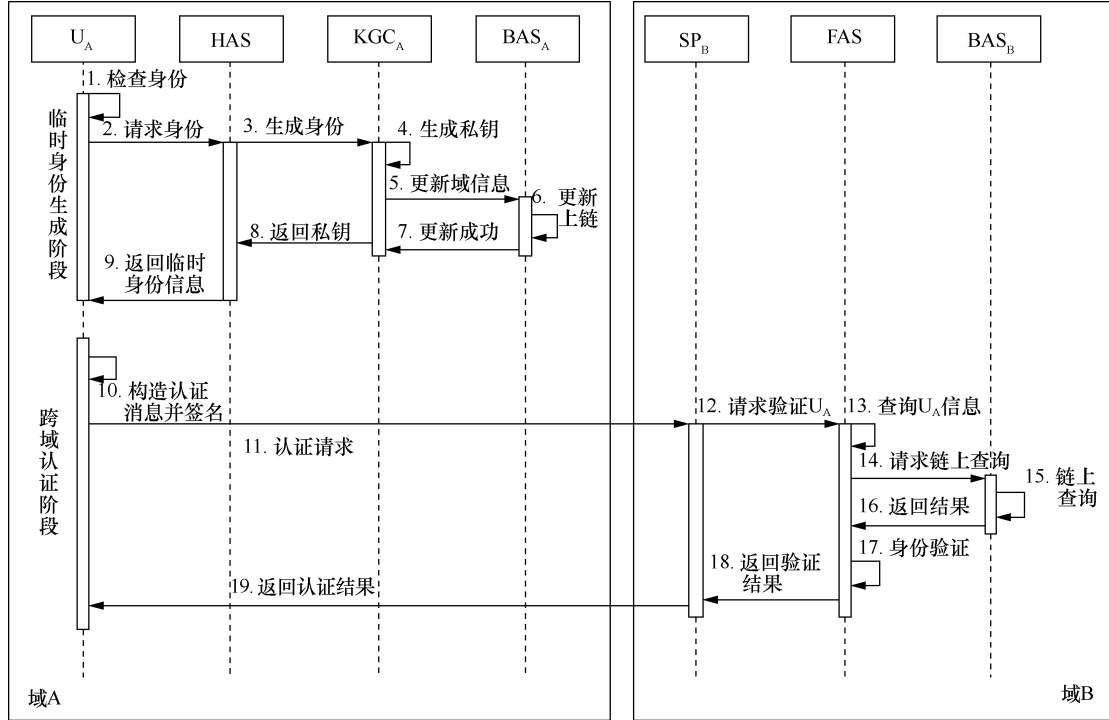


图 4 跨域认证过程

Figure 4 Cross-domain authentication process

1.5 重认证

在身份有效期内, 用户再次访问域 B 中的资源提供者 SP_B 。此时可以直接通过 FAS 对用户快速认证。重认证过程如下。

Msg1' $U_A \rightarrow FAS : \{text_1', [text_1']_{sk_{temp-A}}\}_{PK_{FAS}}$

$text_1' = N \parallel Index_{U_A} \parallel ext_1'$

用户生成随机数 N 与自己的身份索引

$index_{U_A}$ 和扩展信息, 扩展信息中包含协商密钥。

将上述信息使用临时身份密钥进行签名后, 秘密发送给 FAS。FAS 根据身份索引查找本地记录, 若查到, 则根据此用户记录和本地数据库中域 A 的系统参数, 对用户进行验证。若存在用户记录和签名验证成功, 通过用户认证。

Msg2' $FAS \rightarrow SP_B : \{ext_1'\}$

FAS 向 SP_B 发送包含协商密钥的扩展信息， SP_B 生成自己的协商密钥，随后计算会话密钥。

Msg3' $SP_B \rightarrow FAS: \{ext_3'\}$

SP_B 将自己生成的协商密钥放于 ext_3' ，发送给 FAS。

Msg4' $FAS \rightarrow U_A: \{success||ext_4'\}$

FAS 向 U_A 发送验证成功信息和包含密钥协商信息的扩展信息。 U_A 根据此计算会话密钥。

至此重认证过程结束。

1.6 密钥协商

用户访问资源服务时需要通过加密来保证信息传输的安全，但为了传输效率，不可能使用非对称的加密方式。因此，需要通过协商会话的对称加密密钥，保证信息传输安全和完全正向保密 (PFS, perfect forward secrecy)。在此，使用短时 Diffie-Hellman 体制进行密钥交换。

以用户 U_A 和 SP_B 典型的密钥交换过程为例，基本过程如下： U_A 选择自己的秘密指数 a ， SP_B 选择自己的秘密指数 b ， U_A 发送 $g^a \bmod p$ 给 SP_B ， SP_B 发送 $g^b \bmod p$ 给 U_A 。最终双方分别计算后，协商出共享的会话密钥 $K_s = g^{ab} \bmod p$ 。

通常，上述的短时 Diffie-Hellman 体制极易遭到中间人攻击，所以将此密钥协商过程放在认证过程中进行。可以将上述信息放至扩展信息 ext 中，以满足对安全性的需求。

2 安全性分析

2.1 协议的安全性证明

SVO 逻辑属于 BAN 类逻辑，是一种较为成熟可靠的形式化分析工具^[17]。本节基于 SVO 逻辑，对协议进行形式化证明。在 SVO 逻辑中，证明分为初始假设、协议目标和协议分析 3 个部分。

(1) 基本公理

这里仅列举本文在证明此协议安全性时涉及的基本公理^[18]。

A1: $(P \models \alpha \wedge P \models \psi) \equiv (P \models \alpha \wedge \psi)$;

A3: $(P \triangleleft \{X\}_K \wedge P \ni \tilde{K}) \supset P \triangleleft X$;

A4: $P \triangleleft X \supset P \ni X$;

A5: $P \xleftarrow{K} Q \equiv Q \xleftarrow{K} P$

(2) 初始假设

H1. 系统初始化已经完毕，且各个域的实体

已经完成认证，拥有公私钥。

H2. 联盟链中节点间是可信的。

H3. $U_A \models PK(HAS, PK_{HAS})$

H4. $U_A \models HAS \mid \Rightarrow \{PK_{U_A}, sk_{U_A}, P_{pub-s}\}$

H5. $HAS \models PK(U_A, PK_{U_A})$

H6. $BAS_A \models SV([s], PK_{HAS}, HAS)$

H7. $HAS \models SV([s], PK_{BAS_A}, BAS_A)$

H8. $U_A \models PK(FAS, PK_{FAS})$

H9. $FAS \triangleleft Msg5$

H10. $BAS_B \models SV([s], PK_{FAS}, FAS)$

H11. $FAS \models SV([s], PK_{BAS_B}, BAS_B)$

(3) 协议目标

G1. $FAS \models U_A \ni PK_{U_A}$

G2. $U_A \models U_A \xleftarrow{K_s} SP_B$

G3. $SP_B \models U_A \xleftarrow{K_s} SP_B$

(4) 协议分析

Step 1 由 Msg1 和假设 H1、H3、H4、H5、公理 A3，可得

R1: $HAS \triangleleft ID_{temp-A}, \#(Msg1)$

Step 2 由 Msg2、Msg3 和 R1，根据假设 H2、H6、H7，可得

R2: $BAS_A \triangleleft text_2, HAS \triangleleft text_3$

Step 3 根据 Msg4，由假设 H3、H4、H5，结合 R2，利用公理 A4，可得

R3: $HAS \models U_A \ni (PK_{temp-A}, sk_{temp-A})$

Step 4 根据 Msg6、Msg7，由假设 H8、H9，结合 R3，利用公理 A5，可得

R4: $BAS_B \triangleleft Msg6, FAS \triangleleft text_5,$

$SP_B \models U_A \xleftarrow{K_s} SP_B$

此时达到协议目标 G3。

Step 5 利用 R3、R4 结论，FAS 利用查询得到的信息，对 U_A 签名进行验证，由假设 H10、H11，利用公理 A1、A4，可得

R5: $FAS \models HAS \mid \Rightarrow \{PK_{U_A}, sk_{U_A}, P_{pub-s}\},$

$FAS \models U_A \ni PK_{U_A}$

此时达到协议目标 G1。

Step 6 利用 Msg8，由假设 H8，公理 A5，可得

R6: $U_A \models U_A \xleftarrow{K_s} SP_B$

此时达到协议目标 G2。

至此已达到所有协议目标。

2.2 安全属性分析

(1) 协议安全性

在构建信任方面, 本文方案通过联盟链这种可准入链的方式为不同安全域的实体建立信任。经过 SVO 证明, 表明协议是安全的。另外使用的密钥协商方案在认证建立时进行密钥协商, 使用短时密钥协商, 保证了完全正向保密安全。

(2) 抗重放攻击

在认证过程中, 使用随机数来保证消息新鲜。即使消息被敌手从中间截获, 也会由于消息不具有实效性而导致认证失败。这样能够有效阻止攻击者通过重放来进行攻击。

(3) 抗中间人攻击

在认证过程中, 实体之间的重要消息通过先签名后加密的方式进行传输。签名不可伪造。信道中的攻击者若对消息篡改, 将使验签无法通过。通过此方法, 有效地阻止了中间人攻击。

(4) 身份匿名性

在此方案中, 认证时使用的是临时身份。临时身份生成的过程使身份具有一定的匿名性, 而且一段时间后, 身份将不再可用, 避免了身份被恶意跟踪, 保证了一定限度上的身份匿名性。

(5) 可审计

在身份管理方案中, 加入了可监管公私钥, 在发生恶意事件时, 可对身份信息和身份的行为进行监管和审计。

3 性能分析

3.1 负载性能分析

为合理地比较本文方案与其他方案的性能, 参考 Kilinc 等^[19]的实验, 对运算时间进行模拟分析。其实验环境为: Intel Pentium Dual CPU E2200 2.2 GHz, 2048 MB RAM, Ubuntu 12.04.1 LTS 32 bit 操作系统。

在签名方案中, 设置参数如下。

使用 256 bit 的 BN 曲线, 椭圆曲线方程

$$E(F_p): y^2 = x^3 + 5$$

基域特征 $p(t) = 36t^4 + 36t^3 + 24t^2 + 6t + 1$

群的阶 $N(t) = 36t^4 + 36t^3 + 18t^2 + 6t + 1$

嵌入次数 $k=12$

(1) 计算负载

在认证过程中, 实体会执行相关的密码学算法运算。做以下规定: 公钥加密为 PE, 公钥解密为 PD, 非对称签名 AS, 非对称验签 AV, 点乘 PM, 选择随机数 RNG, 基于身份签名 IBS, 基于身份验签 IBV, 密码杂凑算法 H。

根据认证过程, 统计分析得出从临时身份获取到密钥协商的总计算负载如表 1 所示。

表 1 计算负载
Table 1 Computation overhead

实体	临时身份获取	跨域认证	密钥协商	总耗时/ms
U _A	PE+AS	PE	RNG+PM	14.315
KGC _A	/	IBS	/	23.866
HAS	AS+PE+AV	/	/	7.893
BAS _A	AS+AV	/	/	4.043
SP _B	/	/	RNG+PM	2.765
FAS	/	AS+IBV+H	/	9.724
BAS _B	/	AS	/	4.043

为进一步评价本协议的计算量, 将本文方案的跨域协议计算负载与其他方案进行比较, 如表 2 所示。在不同用户数时, 不同方案的耗时对比如图 5 和图 6 所示。对比分析发现, 本文协议用户端上的计算负载表现与文献[13]方案基本相同, 优于文献[10]方案和文献[12]方案; 在服务端, 略优于文献[10]方案, 明显好于文献[12]方案和文献[13]方案。

表 2 计算负载比较
Table 2 Comparison of computation overhead

方案	计算负载	耗时/ms
文献[10]方案	用户端	3PM
	服务端	4AS+4AV+2PE+2PD+3PM
文献[12]方案	用户端	2AS
	服务端	4AS+4AV+2H
文献[13]方案	用户端	PE
	服务端	2IBS+3AS+5PE+3AV+5PD+4PM+2Hn
本文方案	用户端	PE
	服务端	PE+IBS+2AS+AV+IBV+Hn

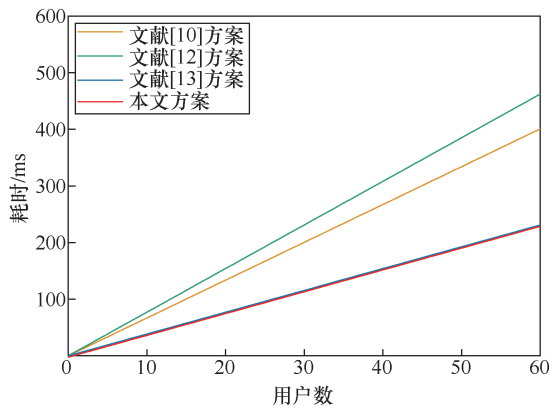


图5 用户端耗时比较
Figure 5 Time-consuming on user-side

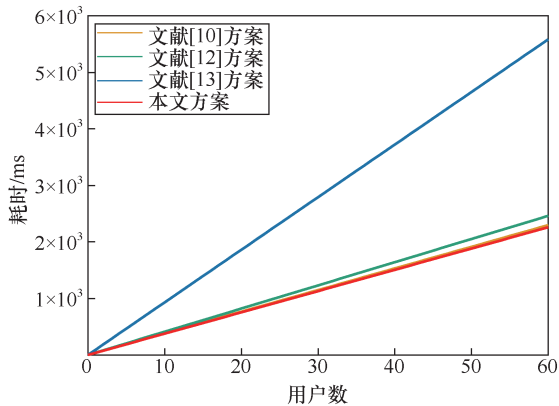


图6 服务端耗时比较
Figure 6 Time-consuming on server-side

(2) 通信负载

这一部分评估了本文方案认证过程中的通信负载。

在本文方案中,用户的临时身份大小为 32 byte,随机数为 2 byte,扩展信息为 32 byte,签名后的签名信息为 96 byte。据此推算, U_A 首先向 FAS 发送了 82 byte 的验证请求信息, FAS 查询 BAS_B 的通信过程为 66 byte,最后 U_A 收到的认证结果信息为 52 byte。统计上述负载,可以得到在认证过程的通信总负载为 296 byte。

相较于文献[13]方案(通信负载为 130 byte),本方案有较大的通信负载,但明显低于文献[12]方案(通信负载为 340 byte),因此本文方案在通信效率上是较高的。

3.2 联盟链性能分析

本文方案基于联盟链构建信任关系。在认证过程中,需要向链中写入和查询认证相关信息。因此,在联盟链中,写入和查询参数是一个对可

用性影响比较大的指标。为评估本文方案的可用性,借助 Hyperledger-Caliper,对 Hyperledger Fabric 的读写性能进行测试和分析。实验环境为: Intel Core i5 7500@3.4 GHz CPU; 8 GB RAM; Ubuntu 18.04 LTS 操作系统。

测试后的结果如图 7 和图 8 所示。易见,并发数对 query 操作时延的影响不大。query 操作的时延总是在极低的水平,基本在 10 ms 以内。因为在区块链中进行 query 操作时,会从本地存储的账本中直接读取数据,基本上没有时间上的损耗,所以 query 操作的时延能够如此之低。然而写操作的时延是随着并发数的增加不断增加的。并发数超过 50 时,时延开始增加得非常迅速。在并发数为 100 时,时延达到 5 s。得到这个结果也是意料之中的,因为随着并发数的增加,共识的压力在逐步增大,最终导致写时延增加。在本文方案中,write 操作只有在生成临时身份时才存在,操作并不频繁,时延能够满足需求。以上结果表明,联盟链在时延表现方面,具有良好的可用性。

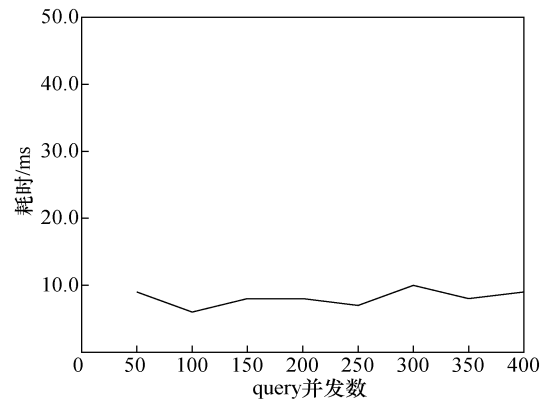


图7 链上 query 操作时延
Figure 7 Query latency on blockchain

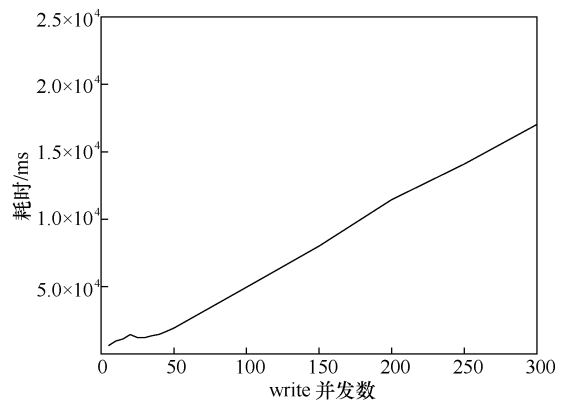


图8 链上 write 操作时延
Figure 8 Write latency on blockchain

4 结束语

针对目前跨域认证的依赖可信第三方、域间不易建立信任的安全难题,本文参考 IBC 体制,提出了一种基于联盟链的跨域认证机制。针对跨域场景,本文设计了包括全认证和重认证在内的跨域认证协议和密钥协商方案;设计了一套身份管理方法,在保证身份匿名性的同时,确保用户行为可监管、可审计。针对区块链的数据存储限制,本文结合 IPFS 提出了一种链下分布式认证信息数据存储方案。最后,使用 SVO 逻辑对认证协议的安全性进行了证明,表明其具有良好的安全性。分析了计算负载和通信负载,与现有的相关方案相比,有较低的计算负载和良好的通信负载。测试了联盟链的性能,分析表明,在时延表现方面,其具有良好的可用性。

参考文献:

- [1] HOUSLEY R, POLK W, FORD W, et al. Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) Profile: RFC3280[EB].
- [2] ELLISON C, SCHNEIER B. Ten risks of PKI: what you're not being told about public key infrastructure[J]. Computer Security Journal, 2000, 16(1): 1-7.
- [3] MATSUMOTO S, REISCHUK R M. IKP: turning a PKI around with decentralized automated incentives[C]//Proceedings of 2017 IEEE Symposium on Security and Privacy (SP). 2017: 410-426.
- [4] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]//Proceedings of Proceedings of the Thirteenth EuroSys Conference. 2018.
- [5] ZHANG Y H, DENG R H, BERTINO E, et al. Robust and universal seamless handover authentication in 5G HetNets[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(2): 858-874.
- [6] SHAMIR A. Identity-based cryptosystems and signature schemes[M]//Advances in Cryptology. Berlin Heidelberg: Springer, 1985: 47-53.
- [7] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[M]//Advances in Cryptology—CRYPTO 2001. Berlin Heidelberg: Springer, 2001: 213-229.
- [8] 彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报, 2006, 29(8): 1271-1281.
- PENG H X. An identity-based authentication model for multi-domain[J]. Chinese Journal of Computers, 2006, 29(8): 1271-1281.
- [9] BELLARE M, NAMPREMPRE C, NEVEN G. Security proofs for identity-based identification and signature schemes[M]//Advances in Cryptology - EUROCRYPT 2004. Berlin Heidelberg: Springer, 2004: 268-286.
- [10] 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[J]. 通信学报, 2011, 32(9): 111-115, 122.
- LUO C Y, HUO S W, XING H Z. Identity-based cross-domain authentication scheme in pervasive computing environments[J]. Journal on Communications, 2011, 32(9): 111-115, 122.
- [11] YUAN C, ZHANG W F, WANG X M. EIMAKP: heterogeneous cross-domain authenticated key agreement protocols in the EIM system[J]. Arabian Journal for Science and Engineering, 2017, 42(8): 3275-3287.
- [12] 周致成, 李立新, 李作辉. 基于区块链技术的高效跨域认证方案[J]. 计算机应用, 2018, 38(2): 316-320, 326.
- 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] 马晓婷, 马文平, 刘小雪. 基于区块链技术的跨域认证方案[J]. 电子学报, 2018, 46(11): 2571-2579.
- 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): 2571-2579.
- [14] SHEN M, LIU H S, ZHU L H, et al. Blockchain-assisted secure device authentication for cross-domain industrial IoT[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(5): 942-954.
- [15] 蔡振华, 林嘉韵, 刘芳. 区块链存储: 技术与挑战[J]. 网络与信息安全学报, 2020, 6(5): 11-20.
- CAI Z H, LIN J Y, LIU F. Blockchain storage: technologies and challenges[J]. Chinese Journal of Network and Information Security, 2020, 6(5): 11-20.
- [16] BENET J. IPFS-content addressed, versioned, P2P file system[EB].
- [17] 赖英旭, 刘岩, 刘静. 一种网络间可信连接协议[J]. 软件学报, 2019, 30(12): 3730-3749.
- LAI Y X, LIU Y, LIU J. Trusted connection protocol between networks[J]. Journal of Software, 2019, 30(12): 3730-3749.
- [18] 韩继红, 郭渊博, 王亚弟. 安全协议形式化分析方法[J]. 信息工程大学学报, 2008, 9(3): 272-276.

HAN J H, GUO Y B, WANG Y D. On methods and techniques for formal analysis of security protocols[J]. Journal of Information Engineering University, 2008, 9(3): 272-276.

- [19] KILINC H H, YANIK T. A survey of SIP authentication and key agreement schemes[J]. IEEE Communications Surveys & Tutorials, 2014, 16(2): 1005-1023.

[作者简介]



牛建林（1995- ），男，河南焦作人，信息工程大学硕士生，主要研究方向为网络与信息安全、区块链安全。



任志宇（1974- ），女，河南汤阴人，博士，信息工程大学副教授，主要研究方向为网络与信息安全。



杜学绘（1968- ），女，河南新乡人，博士，信息工程大学教授、博士生导师，主要研究方向为网络与信息安全、空间信息网络、云计算安全。