面向文化资源可信共享的多因子身份认证方案

王苗苗，芮兰兰，徐思雅
（北京邮电大学网络与交换技术国家重点实验室，北京 100876）

摘 要：为解决传统单因子认证造成的数据泄露和身份冒充等问题，针对文化资源可信共享提出基于区块链的多因子身份认证方案。考虑多种身份因素，利用区块链分布式账本的不可篡改性和分布性构造异构数字身份模型。通过非对称加密算法和异或运算，实现异构数字身份的可信复用和多元主体的快速认证。安全分析和仿真结果表明，所提方案在安全性和效率方面优于已有的多因子认证方案，能有效降低身份认证成本。

关键词：文化资源可信共享；多因子身份认证；数字身份；区块链
中图分类号：TN918
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2023185

Multi-factor identity authentication scheme for trusted sharing of cultural resources

WANG Miaomiao, RUI Lanlan, XU Siya
State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: To solve the problems of data leakage and identity impersonation caused by traditional single factor authentication, a multi-factor identity authentication scheme based on blockchain was proposed for the trusted sharing of cultural resources. Considering a variety of identity factors, a heterogeneous digital identity model was constructed using the tamper resistance and distribution of the blockchain distributed ledger. Through asymmetric encryption algorithm and exclusive OR (XOR) operation, the trusted reuse of heterogeneous digital identity and fast authentication of multi-agent access were realized. Security analysis and simulation results show that the proposed scheme outperforms existing multi-factor authentication schemes in terms of security and efficiency, and can effectively reduce the cost of identity authentication.

Keywords: trusted sharing of cultural resources, multi-factor identity authentication, digital identity, blockchain

0 引言

随着中华民族的不断发展，中国文化越来越丰富多彩，文化资源数据日益庞大。根据现行的团体标准[1]，文化资源数据是指对人类文化中传承下来并可以传播利用的文化进行数字化采集后，所得到的用于识别和展现文化的图像、文字、声音、动画、影片、三维全景、三维模型等数据。为保障共享文化资源的安全性，接入方的可信身份认证成为首要解决的问题。

计算机技术的发展日新月异，市场主体变得多元化，越来越多的市场主体构建了系统，其认证方式多种多样，有基于密码的认证、基于个人身份识别码（PIN, personal identification number）的认证、基于证书的认证等。这些认证信息均存储在各系统的服务器中，构成了认证信息孤岛，无法有效进行统一接入认证和信息流通[2]。在弱信任环境下，多元市场主体存量系统接入文化资源数据共享体系

收稿日期：2023−05−29；**修回日期：**2023−08−18
通信作者：芮兰兰，llrui@bupt.edu.cn
基金项目：国家重点研发计划基金资助项目（No.2021YFF0901703）
Foundation Item: The National Key Research and Development Program of China (No.2021YFF0901703)

成本高，不同市场主体的安全等级不同，主体用户可信度差异大，文化资源数据共享体系难以对不同市场主体不同用户的身份进行安全可信管理，现有的身份认证方案无法基于异构身份进行统一身份认证。另外，对于新接入文化资源数据共享体系的用户，缺乏能够兼容存量系统用户身份的统一身份认证算法。

传统的单因子认证存在较高风险，恶意节点可以通过离线字典攻击获取用户密码等，容易造成数据泄露和身份冒充[3]。近年来，为了加强认证的安全性，有些系统采用了双因子认证方案，例如，银行柜员登录柜面系统时需要输入密码和指纹进行双重验证以确保银行资产的安全性。在欧盟，一些国家的数据保护部门已经建议使用多因子身份认证，作为遵守欧盟数据保护指令中“采取适当的技术和组织措施来保护个人数据”义务的一种手段[4]。身份认证因子可以分为三类：基于记忆的，如口令、安全问题等；基于持有物的，如数字证书、U 盾等；基于生物特征的，如指纹、声纹等。攻击者很难破坏所有认证因素，聚合多种认证因子验证接入者的身份，能够大幅提高身份认证的安全性和可靠性。身份认证方案的演变如图 1 所示。

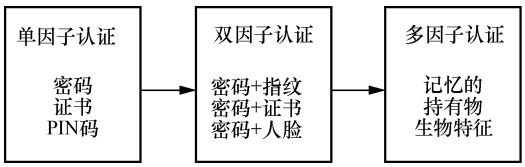

图 1　身份认证方案的演变

目前，有些学者研究了基于多因子的身份认证方案。文献[5]研究了基于属性的多授权中心身份认证方案，采用基于属性的加密算法可以抵抗 $t-1$ 个授权中心的合谋攻击，但该方案采用昂贵的双线性配对运算进行身份认证，降低了认证效率。文献[6]提出了一种用于车联网的轻量级多因子身份认证方案，采用物理不可克隆函数和一次性动态伪身份的组合作为身份验证因素实现身份认证，但该方案需采用防篡改设备，增加了认证成本。文献[7]提出了一种基于多因子认证的数据备份方案，通过组合存储在用户智能卡和笔记本电脑中的分段密钥重建密钥进行身份认证，也能通过密码和生物识别技术找回密钥，但该认证方案需要 2 种额外的设备配合，成本较高。文献[8]设计了基于混沌映射的多因子认证密钥协商协议，通过扩展混沌映射算法和动态身份实现用户认证的匿名性，但该方案采用额外的移动存储设备，并且仅能通过密码和生物特征进行认证，成本较高且灵活性差。基于多因子的身份认证方案的研究对于提高接入者身份的安全性具有重要意义。然而，上述多因子认证方案均依赖可信第三方或智能设备等，存在数据集中泄露或智能设备被盗导致身份冒用的风险。并且，对于文化资源可信交互场景，如何复用存量系统的多因子认证信息进行统一接入认证还缺少具体方案。

区块链是一种分布式账本技术，具有去中心化、数据防篡改和交易可追溯等特点，适合解决信任问题[9]。采用分布式账本存储加密身份因子信息能够避免数据集中泄露和智能设备身份冒用的风险，同时，能降低采用智能设备产生的额外成本。考虑到不同存量系统的认证方式不同和单因子认证安全性差的问题，本文设计了基于区块链的多因子身份认证方案，利用分布式账本的分布性和不可篡改性存储多因子身份信息，解决存量系统多因子身份数据孤岛问题，保证身份信息的分布式可用性，结合轻量级的异或运算和非对称加密算法，聚合多因子身份信息认证文化资源系统接入方的身份，能够提升文化资源可信共享的安全性和效率。

本文主要的贡献如下。

1) 提出基于区块链的多因子认证架构，该架构能够兼容存量系统的多因子认证信息，降低存量系统的接入成本。分布式账本的不可篡改性和分布性能够保障多因子身份信息的真实性和可用性，为文化资源可信共享提供异构数字身份认证基础。

2) 设计轻量级的多因子身份认证方案，利用非对称加密算法和异或运算聚合多因子身份信息实现快速的身份认证，不局限于某一个或几个特定的身份因子，提高了身份认证的灵活性、安全性和效率。

3) 对所提方案进行 BAN 逻辑安全分析和仿真实验，结果表明该方案具有良好的安全性和较高的认证效率。

1　预备知识

1.1　区块链

2008 年，Nakamoto[10]提出了点到点（P2P, peer-to-peer）网络解决方案，即区块链技术。区块链是一种分布式账本技术，用于转移所有权、保存

交易记录、跟踪资产等，通过共识算法确保各类交易的透明度、信任度和安全性[11]。智能合约是一种执行合约条款的计算机交易协议，它是区块链 2.0 的代表性技术，允许无第三方的可信交易，交易可追溯且不可逆。区块链分为公有链、私有链和联盟链，公有链是指任何个人或组织都能发送交易或参与交易共识的区块链；私有链是指其写入权利由个人或组织独享的区块链，具有更快的交易速度和更高的隐私性；联盟链是介于公有链和私有链之间的一种区块链，针对某些特定成员，区块的生成由预选节点共同决定。

区块链已广泛用于众多领域，可提供更高的安全保障[12]。

1.2 模糊提取器

2004 年，Dodis、Reyzin 和 Smith[13]首次提出了模糊提取器（FE, fuzzy extractor），用于提取随机源中均匀分布的随机字符串。模糊提取器能够将有噪声的随机源转化成均匀随机的字符串，并且精确再生，这使其可以应用于人类生物特征提取中。人类的生物特征包括指纹、声纹、虹膜、人脸等，每次读取的生物特征会有一些偏差，通过模糊提取器还原生物特征，能够将生物特征用于身份认证。

模糊提取器包括生成算法 Gen 和再生算法 Rep，可表示为 FE=(Gen, Rep)，如图 2 所示。Gen 输入生物特征的一次采样字符串 w，输出一个字符串 R 和一个帮助字符串 P。Rep 输入生物特征的另一次采样字符串 w' 和 Gen 的帮助字符串 P，输出一个字符串 R'。FE 的正确性要求是如果两次采样 w 和 w' 的距离足够近，那么 $R=R'$，安全性要求是如果生物特征有足够多的熵，那么 R 是均匀随机的。

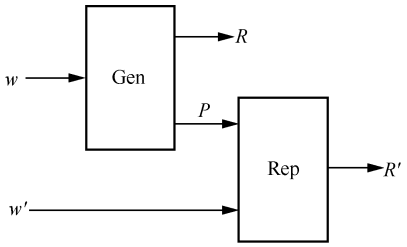

图 2 模糊提取器

2 系统概况

2.1 系统模型

当用户需要访问文化资源服务时，必须先进行身份认证。基于区块链的多因子身份认证架构如图 3 所示，主要由四部分组成，分别为注册中心（RA, registration authority）服务器、区块链、存量系统和用户。

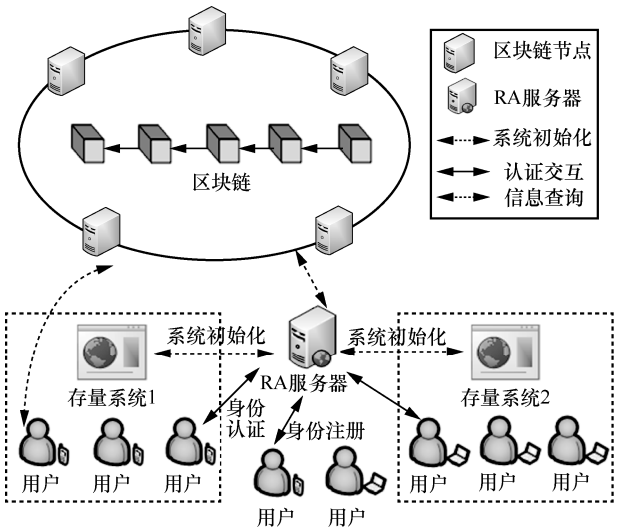

图 3 基于区块链的多因子身份认证架构

1) RA 服务器。RA 服务器作为认证系统的核心角色，是完全可信的，负责系统初始化、用户身份注册、用户身份认证等功能。RA 服务器仅负责身份认证相关的计算工作，不存储用户的密钥和身份信息。

2) 区块链。该方案采用联盟区块链，由文化资源数据中心、监管机构等权威机构节点维护。分布式账本用来存储系统参数、用户分布式身份标识（DID, distributed identifier）、用户公钥和用户多因子身份信息的哈希值等，这些信息不会暴露用户的隐私。分布式账本的不可篡改性能够保证身份信息的真实性，其分布性也提高了身份信息的可用性。

3) 存量系统。存量系统是指多元市场主体已构建的系统，它们拥有自己的用户，在认证系统初始化时可以将存量系统中的用户身份信息导入分布式账本，以方便存量系统用户访问文化资源服务。

4) 用户。用户是指需要访问文化资源服务的实体，分为存量系统用户和普通用户。经过系统初始化后，存量系统用户可以直接使用原有的身份信息进行身份认证，普通用户在身份认证前需要先进行身份注册。用户客户端程序具有身份注册和生成可验证凭证（VP, verifiable presentation）功能。注册身份信息并通过身份认证的用户才能访问文化资源服务。

2.2　数据模型

多因子身份数据模型是实现多因子身份认证的基础，利用身份管理智能合约在链上聚合异构数字身份，构建具有兼容性的身份统一管理模型，能够降低认证系统改造迁移的建设成本[14]。身份数据模型如图 4 所示，其中，DID 是用户信息的身份标识，由标识（如“did”）、组织（如“bupt”）、标识字符串（如“2020010123”）组成，该身份标识具有全球唯一性。公钥为用户的公钥信息，身份信息表示用户的多种身份因子，如口令、指纹、证书等。为兼容存量系统的多种身份因子信息，并确保身份因子的机密性，以 JSON（JavaScript object notation）格式存储身份因子的类型及其哈希值。身份数据模型以 DID 为账本 ID，公钥和身份信息为账本值，通过智能合约发布到分布式账本中。

图 4　身份数据模型

2.3　威胁模型

考虑到所提方案的安全性，本文使用了著名的 Dolev Yao 对手模型[15]，威胁模型描述如下，本文将在第 4 节对其进行分析。

1) 对手可以在网络中重复传输与身份验证相关的数据。

2) 对手可以窃取与身份验证相关的数据。

3) 对手可以篡改与身份验证相关的数据。

2.4　设计目标

面向文化资源可信共享需求，身份认证方案应该满足以下设计目标。

1) 身份认证方案应兼容存量系统，复用已有的身份因子信息，降低存量系统用户接入成本。

2) 身份认证方案应实现多因子认证，避免单因子认证造成的数据泄露和身份冒用，提高身份认证的安全性。

3) 身份认证方案应具备灵活性，不局限于某一个或几个特定的身份认证因子。

4) 身份认证方案应能够抵御常见的攻击，具备较高的安全性。

5) 身份认证方案应具备高效性，通过轻量级的计算开销和通信开销提高身份认证效率。

3　多因子身份认证方案

多因子身份认证方案共分为 5 个阶段，分别为系统初始化、身份注册、身份认证、身份因子更新、身份因子撤销，方案涉及的符号如表 1 所示。

表 1　方案涉及的符号

符号	含义
PK_U	U 的公钥
SK_U	U 的私钥
H_0	哈希函数
σ	使用公钥或私钥对某个信息加密后的值
$\mathrm{sign}(\mathrm{sth}, K)$	使用密钥 K 加密 sth
$\mathrm{verify}(\sigma, K)$	使用密钥 K 验证加密 σ
$\oplus$	异或运算
$\|\|$	连接操作
N	随机整数
S	随机混淆值
f	身份因子
TS	时间戳
ΔT	消息的有效期
P	生物特征对应的帮助字符串

3.1　系统初始化

在身份注册和身份认证之前需要先进行系统初始化，初始化工作由 RA 服务器负责。方案中的加解密操作采用 RSA 算法，首先，RA 服务器任意选择 2 个不同的大素数 p 和 q，计算得到 $n=pq$，$\varphi(n)=(p-1)(q-1)$，选择一个大整数 e 满足 $\gcd(e,\varphi(n))=1$。然后，计算解密密钥 d，满足 $de \bmod \varphi(n)=1$，确定 RA 服务器的私钥为 $\mathrm{SK}_{\mathrm{RA}}=\{n,d\}$，公钥为 $\mathrm{PK}_{\mathrm{RA}}=\{n,e\}$。接下来，选择安全的哈希函数 $H_0:\{0,1\}^*$。最后，将公开初始化参数 $\mathrm{Params}=\{\{n,e\},H_0\}$ 发布到分布式账本，$\mathrm{SK}_{\mathrm{RA}}$ 由 RA 服务器保存在本地，模糊提取器由 RA 服务器参照文献[16]实现。

系统参数初始化之后还需要将存量系统中的身份认证信息同步到分布式账本，以复用存量多因子认证信息。多因子身份认证平台仅对存量系统做出整体要求，存量系统中用户的选择由存量系统决定，可以是申请访问文化资源平台的用户，也可以是信誉值高且申请访问文化资源平台的用户。根据存量系统的安全

等级的不同，多因子身份认证平台要求其同步不同种类和数量的身份因子信息，例如，在初始化时，安全等级高的存量系统仅需同步用户的一种基于记忆的身份因子和一种基于生物特征的身份因子到分布式账本中，而安全等级低的存量系统同步用户的一种基于记忆的身份因子、一种基于生物特征的身份因子和一种基于持有物的身份因子到分布式账本中。存量系统首先构建用户 DID，并将数据库中用户的身份信息和公钥以文件的形式安全地发送给 RA 服务器。RA 服务器收到用户批量身份数据信息后，首先，将生物特征信息采用模糊提取器提取生物特征，保存用户 DID 和帮助字符串 P 的关联信息，并对全部身份信息进行哈希运算，构建身份数据模型；最后，将其发布到分布式账本，完成存量系统用户身份信息的初始化。

3.2 身份注册

对于一般用户来说，身份认证之前需要进行身份注册，注册算法如下。

1) 用户构建 DID，并在本地生成公私钥对 PK_U 和 SK_U，查询 RA 服务器公钥，使用其对自己的公钥进行签名得到 $\sigma_k=\mathrm{sign}(\mathrm{PK}_U,\mathrm{PK}_{\mathrm{RA}})$，接着，向 RA 服务器发送身份注册请求 register: {DID, σ_k, info}。

2) RA 服务器收到注册请求后，首先查询分布式账本以确保该 DID 未进行身份注册，并使用自己的私钥解密得到用户公钥 $\mathrm{PK}_U=\mathrm{verify}(\sigma_k,\mathrm{SK}_{\mathrm{RA}})$；随后，生成随机数 N，使用用户公钥签名随机数得到 $\sigma_N=\mathrm{sign}(N,\mathrm{PK}_U)$，根据 DID 的组织类型判断其需要录入的身份因素种类和最小数量，然后将 σ_N 和多因子身份认证需求返回给用户。

3) 用户使用自己的私钥验证收到的 σ_N 得到 $N=\mathrm{verify}(\sigma_N,\mathrm{SK}_U)$，并使用自己的私钥对 N 进行签名得到 $\sigma_N=\mathrm{sign}(N,\mathrm{SK}_U)$，获取当前的时间戳 TS，使用自己的私钥对时间戳签名得到 $\sigma_T=\mathrm{sign}(\mathrm{TS},\mathrm{SK}_U)$。然后，根据需求录入多个身份认证因子 $\{f_1,f_2,\cdots\}$，使用私钥对多个身份因子签名得到 $\sigma_1=\mathrm{sign}(f_1,\mathrm{SK}_U)$，$\sigma_2=\mathrm{sign}(f_2,\mathrm{SK}_U)$。最后，将多个签名值 $\{\mathrm{DID},\sigma_N,\sigma_T,\sigma_1,\sigma_2,\cdots\}$ 发送给 RA 服务器。

4) RA 服务器收到签名后使用用户的公钥分别对其进行验证得到 N'、TS'、f_1、f_2。首先，比较 N' 与之前自己生成的 N 是否相等，若相等，则获取当前的时间戳 TS，计算并判断 $\mathrm{TS}-\mathrm{TS}'\leqslant\Delta T$ 是否成立，若成立，则说明该身份信息在有效时间内。然后，查验身份信息是否满足要求。若满足要求，则通过模糊提取器对用户的生物信息进行特征提取作为该身份因子的特征，并保存用户 DID 与帮助字符串 P 的关联信息，计算全部身份因子的哈希值，将 $\{\mathrm{DID},\mathrm{PK}_U,H_0(f_1),H_0(f_2),\cdots\}$ 发布到分布式账本中，将结果返回给用户。

3.3 身份认证

用户访问文化资源服务时需要先通过身份认证。身份认证流程如图 5 所示，算法如下。

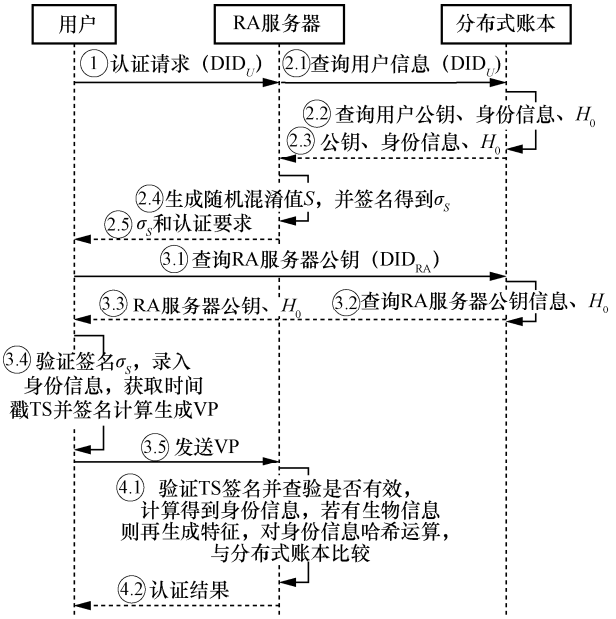

图 5 身份认证流程

1) 用户首先向 RA 服务器发送自己的 DID_U 并请求身份认证。

2) RA 服务器验证用户 DID_U 存在后从分布式账本查询用户的公钥、身份信息和哈希函数 H_0，根据 DID_U 的组织类型确定其需要认证的身份因子种类和数量，并生成随机混淆值 S，使用自己的私钥对其签名，再使用用户公钥对签名值加密得到 $\sigma_S=\mathrm{sign}(\mathrm{sign}(S,\mathrm{SK}_{\mathrm{RA}}),\mathrm{PK}_U)$，并将身份认证因子要求和 σ_S 返回给用户。

3) 用户收到上述参数后，首先从分布式账本查询 RA 服务器的公钥和哈希函数 H_0，先使用自己的私钥解密 σ_S，再使用 RA 服务器的公钥对其验证，得到混淆值 $S=\mathrm{verify}(\mathrm{verify}(\sigma_S,\mathrm{SK}_U),\mathrm{PK}_{\mathrm{RA}})$。然后，获取当前时间戳 TS，并计算时间戳签名 $\sigma_T=\mathrm{sign}(\mathrm{TS},\mathrm{SK}_U)$。接着，录入身份信息，如 f_1、f_2，计算 $\mathrm{VP}=\{\mathrm{DID}_U,f=(f_1\|f_2)\oplus H_0(S),\sigma_T\}$。最后，将 VP 发送给 RA 服务器进行身份认证。

4) RA 服务器收到 VP 后，首先使用用户的公

钥验证时间戳签名得到 $\mathrm{TS}'=\mathrm{verify}(\sigma_T,\mathrm{PK}_U)$，并获取当前时间戳 TS，判断 $\mathrm{TS}-\mathrm{TS}'\leqslant\Delta T$，若成立，则说明认证信息在有效时间内。然后，通过异或运算得到身份信息 $(f_1\|f_2)=f\oplus H_0(S)$，若 f_1、f_2 中存在生物信息，则 RA 服务器从本地数据库中查询其帮助字符串 P_U，通过模糊提取器的再生算法和 P_U 重新生成生物特征，并计算 $H_0(f_1)$、$H_0(f_2)$，与查询到的分布式账本中身份信息哈希值进行比较，若相等且符合认证因子要求，则身份认证通过，允许用户访问文化资源服务。

在身份认证过程中，RA 服务器根据用户 DID 的组织类型给出用户需要验证的身份因子种类和数量，而不限定于某几个特定的身份因子，例如，一种基于记忆的身份因子和 2 种基于生物特征的身份因子。用户可以选择密码或安全问题等基于记忆的身份因子，再选择录入 2 个基于生物特征的身份信息，如指纹、人脸、虹膜等。这种认证方式相较于基于智能卡等特定身份因子认证具有一定的灵活性。

3.4　身份因子更新

用户的某个身份因子泄露后可以对其进行更新，以用户更新身份因子 f_1 为例，更新算法如下。

1) 用户首先录入已有的身份因子 f_1 和更新后的身份因子 f_1'。然后，使用 RA 服务器的公钥对 2 个身份因子加密，再使用自己的私钥对其签名得到 $\sigma_f=\mathrm{sign}(\mathrm{sign}(f_1\|f_1',\mathrm{PK}_{\mathrm{RA}}),\mathrm{SK}_U)$。接着，获取当前的时间戳 TS，并计算 $\sigma_T=\mathrm{sign}(\mathrm{TS},\mathrm{SK}_U)$。最后，向 RA 服务器发送身份因子更新请求 update: $\{\mathrm{DID}_U,\sigma_f,\sigma_T\}$。

2) RA 服务器收到请求后，首先验证 DID_U 存在并获取其公钥。然后，获取当前时间戳 TS，并使用其公钥和自己的私钥对收到的签名进行验证，得到 $(f_1\|f_1')=\mathrm{verify}(\mathrm{verify}(\sigma_f,\mathrm{PK}_U),\mathrm{SK}_{\mathrm{RA}})$，使用用户的公钥验证签名得到 $\mathrm{TS}'=\mathrm{verify}(\sigma_T,\mathrm{PK}_U)$。判断 $\mathrm{TS}-\mathrm{TS}'\leqslant\Delta T$ 是否成立，若成立，则说明更新请求在有效时间内。若 f_1 中为生物信息，则 RA 服务器从本地数据库中查询其帮助字符串 P_{U_1}，通过模糊提取器的再生算法和 P_{U_1} 重新生成生物特征，并计算 $H_0(f_1)$，将其与分布式账本中的 $H_0(f_1)$ 进行比较，若相等，则将分布式账本中 $H_0(f_1)$ 的信息更新为 $H_0(f_1')$，并将更新结果返回给用户。

3.5　身份因子撤销

用户决定不再使用某个身份因子后可以对其进行撤销，以用户撤销身份因子 f_1 为例，撤销算法如下。

1) 用户首先录入身份因子 f_1。然后，使用 RA 服务器的公钥对身份因子加密，使用自己的私钥对其签名得到 $\sigma_f=\mathrm{sign}(\mathrm{sign}(f_1,\mathrm{PK}_{\mathrm{RA}}),\mathrm{SK}_U)$。接着，获取当前的时间戳 TS，并计算 $\sigma_T=\mathrm{sign}(\mathrm{TS},\mathrm{SK}_U)$。最后，向 RA 服务器发送身份因子撤销请求 revoke: $\{\mathrm{DID}_U,\sigma_f,\sigma_T\}$。

2) RA 服务器收到请求后，首先验证 DID_U 存在并获取其公钥。接着，获取当前时间戳 TS，使用其公钥和自己的私钥对收到的签名进行验证，得到 $f_1=\mathrm{verify}(\mathrm{verify}(\sigma_f,\mathrm{PK}_U),\mathrm{SK}_{\mathrm{RA}})$，使用用户的公钥验证签名得到 $\mathrm{TS}'=\mathrm{verify}(\sigma_T,\mathrm{PK}_U)$。计算并判断 $\mathrm{TS}-\mathrm{TS}'\leqslant\Delta T$ 是否成立，若成立，则说明撤销请求在有效时间内。若 f_1 为生物信息，则 RA 服务器从本地数据库中查询其帮助字符串 P_{U_1}，通过模糊提取器的再生算法和 P_{U_1} 重新生成生物特征 f_1，计算 $H_0(f_1)$，将其与分布式账本中的 $H_0(f_1)$ 进行比较，若相等，则将撤销分布式账本中 $H_0(f_1)$ 的信息，并将撤销结果返回给用户。

4　安全分析

4.1　BAN 逻辑安全分析

BAN 逻辑是 Burrows、Abadi 和 Needham[17]在 1989 年提出的一种基于信念的模态逻辑，通常用于分析协议是否能够达到预期目标。BAN 逻辑中使用的符号如表 2 所示，逻辑规则如表 3 所示。以用户 U 需要验证身份信息 f_1、f_2 为例，本节使用 BAN 逻辑对所提身份认证方案进行安全分析。

表 2　BAN 逻辑符号

序号	符号	含义
N1	$P\|\equiv X$	P 相信 X
N2	$P\|\sim X$	P 曾经说过 X 或者 P 发送过 X
N3	$P\lhd X$	P 看到或接收 X
N4	$P\|\Rightarrow X$	P 对 X 有管辖权
N5	$\#(X)$	X 是新的
N6	$\xrightarrow{K}P$	K 是 P 的公钥
N7	$\{X\}_K$	使用 K 对 X 加密
N8	(X,Y)	X 或 Y 是消息的一部分
N9	$(X)_H$	使用 H 对 X 进行哈希处理
N10	$<X>_Y$	X 与公式 Y 结合

表 3 BAN 逻辑规则

序号	名称	符号	含义
R1	消息含义规则	$\dfrac{P\mid\equiv \xrightarrow{K} Q, P\lhd\{X\}_{K^{-1}}}{P\mid\equiv Q\mid\sim X}$	如果 P 相信 K 是 Q 的公钥，并且拥有在 K^{-1} 下加密的消息 X，那么 P 相信 Q 曾经说过 X
		$\dfrac{P\mid\equiv Q\overset{Y}{\rightleftharpoons} P, P\lhd\langle X\rangle_Y}{P\mid\equiv Q\mid\sim X}$	如果 P 相信秘密 Y 与 Q 共享，并且看到$\langle X\rangle_Y$，那么 P 相信 Q 曾经说过 X
R2	随机数验证规则	$\dfrac{P\mid\equiv \#(X), P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$	如果 P 相信 X 是最近说的，而 Q 曾经说过 X，那么 P 相信 Q 相信 X
R3	管辖权规则	$\dfrac{P\mid\equiv Q\mid\Rightarrow X, P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$	如果 P 相信 Q 对 X 有管辖权，并且 P 相信 Q 相信 X，那么 P 相信 X
R4	信念规则	$\dfrac{P\mid\equiv X, P\mid\equiv Y}{P\mid\equiv (X,Y)}$	如果 P 单独相信 X 和 Y，则 P 相信集合公式(X,Y)
		$\dfrac{P\mid\equiv (X,Y)}{P\mid\equiv X}$	如果 P 相信集合公式(X,Y)，则 P 单独相信 X

1) 安全目标。所提身份认证方案能够认证身份信息 f_1、f_2 是用户的有效身份信息，因此，安全目标为

G1: $\mathrm{RA}\mid\equiv f_1$

G2: $\mathrm{RA}\mid\equiv f_2$

2) 理想化。所提身份认证方案主要包括用户和 RA 服务器进行信息交互、用户和 RA 服务器分别向分布式账本查询信息。消息的理想化为

I1: $U\rightarrow \mathrm{RA}:\{\mathrm{request},\mathrm{DID}_U\}$

I2: $\mathrm{RA}\rightarrow \mathrm{DL}:\{\mathrm{DID}_U\}$

I3: $\mathrm{RA}\rightarrow U:\{\mathrm{requirement},\mathrm{DID}_{\mathrm{RA}},\sigma_S\}$

I4: $U\rightarrow \mathrm{DL}:\{\mathrm{DID}_{\mathrm{RA}}\}$

I5: $U\rightarrow \mathrm{RA}:\{\mathrm{VP}=\{\mathrm{DID}_U, f,\sigma_T\}\}$

3) 假设。用户和 RA 服务器分别拥有自己的私钥，且无法被他人获取。鉴于分布式账本的不可篡改性，本文认为用户和 RA 服务器从分布式账本中查询到的信息都是可靠的，即根据消息 I2 和 I4，有假设 A3、A4、A13 和 A14。根据所提身份认证方案做出如下假设。

A1: $\xrightarrow{\mathrm{PK}_U} U$

A2: $\xrightarrow{\mathrm{PK}_{\mathrm{RA}}} \mathrm{RA}$

A3: $U\lhd H_0$

A4: $\mathrm{RA}\lhd H_0$

A5: $\#(S)$

A6: $\mathrm{RA}\mid\sim S$

A7: $\sigma_S=\{\{S\}\mathrm{PK}_{\mathrm{RA}}^{-1}\}_{\mathrm{PK}_U}$

A8: $\sigma_T=\{\mathrm{TS}\}_{\mathrm{PK}_U^{-1}}$

A9: #(TS')

A10: $f=(f_1,f_2)\oplus(S)_{H_0}$

A11: $U\mid\Rightarrow f_1$

A12: $U\mid\Rightarrow f_2$

A13: $\mathrm{RA}\mid\equiv(f_1)_{H_0}$

A14: $\mathrm{RA}\mid\equiv(f_2)_{H_0}$

4) 分析。基于上述理想化和假设，对所提身份认证方案分析如下。

D1：从消息 I1、I2，假设 A1，可以推断

$\mathrm{RA}\mid\equiv \xrightarrow{\mathrm{PK}_U} U$

从假设 A5、A6、A7，可以得到消息 I3。

D2：从消息 I4，假设 A2，可以推断

$U\mid\equiv \xrightarrow{\mathrm{PK}_{\mathrm{RA}}} \mathrm{RA}$

D3：从消息 I3，假设 A1、A6，推演 D2，应用规则 R1，可以推断

$U\mid\equiv \mathrm{RA}\mid\sim S$

D4：从假设 A5，推演 D3，应用规则 R2，可以推断

$U\mid\equiv \mathrm{RA}\mid\equiv S$

从假设 A3，推演 D4 可知，U 可以计算 $(S)_{H_0}$，结合 A11、A12，U 可以计算 A10。

D5：从消息 I5，假设 A8，推演 D1，应用规则 R1，可以推断

$\mathrm{RA}\mid\equiv U\mid\sim\mathrm{TS}$

结合假设 A9，RA 判断 $\mathrm{TS}-\mathrm{TS}'\leqslant\Delta T$ 是否成立，若成立，则 VP 有效，继续身份验证。

从 A4、A6 可知，RA 可以计算 $(S)_{H_0}$。

D6：从消息 I5，假设 A10，推演 D4、D5，结合异或运算的性质，应用规则 R1，可以推断

$$\mathrm{RA}\mid\equiv U\mid\sim(f_1,f_2)$$

从假设 A11、A12，可以推断

$$\mathrm{RA}\mid\equiv U\mid\Rightarrow(f_1,f_2)$$

D7：从推演 D6，假设 A13、A14，根据哈希运算的特性，比较哈希值，应用规则 R4，可以推断

$$\mathrm{RA}\mid\equiv U\mid\equiv f_1$$

$$\mathrm{RA}\mid\equiv U\mid\equiv f_2$$

$$\mathrm{RA}\mid\equiv U\mid\equiv(f_1,f_2)$$

D8：从推演 D6、D7，应用规则 R3，可以推断

$$\mathrm{RA}\mid\equiv(f_1,f_2)$$

D9：从推演 D8，应用规则 R4，可以推断

$$\mathrm{RA}\mid\equiv f_1$$

$$\mathrm{RA}\mid\equiv f_2$$

从推演 D9 可以看出，安全目标已经实现，完成了 RA 服务器对用户 U 的多因子身份验证。

4.2　非正式安全分析

本节从重放攻击、窃听攻击、伪装攻击和分布式拒绝服务（DDoS, distributed denial of service）攻击 4 个方面对第 2 节提出的威胁模型进行非正式的安全分析。

1) 重放攻击。重放攻击是指对手向目的方发送重复包以欺骗系统。这是第一个威胁模型假设，对手向 RA 服务器发送重复的 VP，意图通过该 VP 进行身份认证以非法访问文化资源服务。在本文认证方案中，用户生成 VP 时，首先获取当前时间戳，并使用自己的私钥对其签名。RA 服务器收到 VP 后，先验证用户的签名，并将收到的时间戳与当前的时间戳进行对比，若发现其无法通过验证或已过期，则拒绝通过该 VP 进行身份认证，因此，重放攻击失败。

2) 窃听攻击。窃听攻击是指对手企图在网络交互中窃取隐私信息。这是第二个威胁模型假设，对手窃听用户和 RA 服务器之间的交互信息。在本文认证方案中，用户和 RA 服务器进行了 3 次交互，分别为 DID_U、σ_S 和 VP，这些信息均为非隐私信息或者需要用户私钥解密才能获取的有效信息，且无法从中推断用户隐私信息。因此，本文认证方案能够抵抗窃听攻击。

3) 伪装攻击。伪装攻击是指对手以虚假的身份获取目标系统的访问权限。这是第三个威胁模型假设，对手采用虚假的 VP 向 RA 服务器进行身份认证。在本文认证方案中，对手没有用户的私钥，无法对签名 σ_s 进行验证从而获取混淆值 S，同时，也无法伪造用户对当前时间戳 TS 的签名，进而无法生成可用的 VP。因此，本文认证方案能够抵抗伪装攻击。

4) DDoS 攻击。DDoS 是指多个攻击者同时攻击一个或多个目标，或者一个攻击者控制多台机器同时攻击受害者[18-19]。区块链具有分布式的特点，节点保存区块链的完整账本。当少于三分之一的节点无法工作时，分布式账本的使用不会受到影响，RA 服务器仍然可以访问账本中的信息进行身份认证。当被攻击的节点恢复正常时，它可以从其他正常节点检索整个账本的信息，并再次成为具有认证功能的正常节点。因此，所提身份认证方案能够抵抗 DDoS 攻击。

5　仿真实验与分析

5.1　仿真环境

仿真程序部署在 Ubuntu 18.04（64 位）虚拟系统上，其物理机的配置为 Intel® Core™ i5-10400 CPU@2.90 GHz 处理器和 16 GB RAM。

5.2　性能分析

为了分析所提方案的性能，本节从身份注册、身份认证、身份因子更新和身份因子撤销 4 个方面分析其计算开销。每个模块均涉及用户端和 RA 服务器端的计算，分析结果如表 4 所示，其中 $T_{\mathrm{A}}\approx0.003$ ms、$T_{\mathrm{h}}\approx0.000\,3$ ms、$T_{\mathrm{B}}\approx0.92$ ms 分别表示非对称加解密运算、哈希运算和生物特征提取算法的运行时间，p 为身份因子的个数，q 为基于生物特征的身份因子的个数。根据实际的多因子认证场景分析，通常 p 取值为 2 或 3，q 取值为 0、1、2 或 3，本文中 p 取值为 2.5，q 取值为 1。认证方案计算时延如图 6 所示，各模块的计算时延均在 1～1.2 ms，性能较好。

表 4　　方案计算开销

模块	计算开销	
	用户端	RA 服务器端
身份注册	$(4+p)T_{\mathrm{A}}$	$(4+p)T_{\mathrm{A}}+T_{\mathrm{h}}+qT_{\mathrm{B}}$
身份认证	$3T_{\mathrm{A}}+T_{\mathrm{h}}$	$3T_{\mathrm{A}}+(1+p)T_{\mathrm{h}}+qT_{\mathrm{B}}$
身份因子更新	$3T_{\mathrm{A}}$	$3T_{\mathrm{A}}+T_{\mathrm{h}}+T_{\mathrm{B}}$
身份因子撤销	$3T_{\mathrm{A}}$	$3T_{\mathrm{A}}+T_{\mathrm{h}}+T_{\mathrm{B}}$

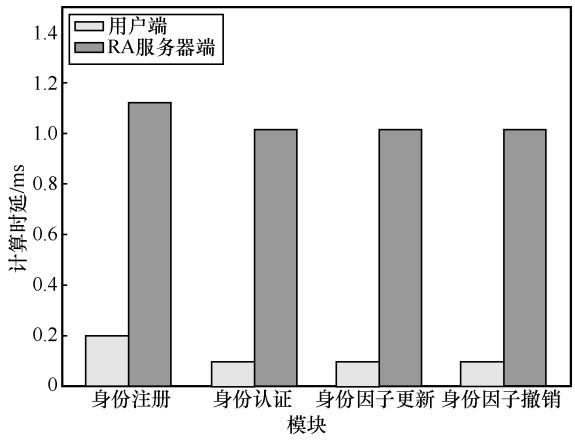

图 6 认证方案计算时延

5.3 区块链仿真分析

本文采用 Hyperledger Fabric 区块链平台构建异构数字身份模型，在上述仿真环境中搭建了 Fabric 2.3 系统，通过智能合约实现数字身份的发布和查询等功能。为全面测试多因子身份认证的效率，本文设置了 2 种不同的虚拟机配置，配置 1 采用 2 核 CPU、4 GB 内存，配置 2 采用 4 核 CPU、8 GB 内存，数字身份信息查询时延如图 7 所示。同一配置下，不同并发数的数字身份信息查询时延区别较小，而配置 2 环境下的查询时延明显低于配置 1 环境下的查询时延，约为 2 ms。可见，提高区块链环境配置可以提升数字身份信息的查询效率。本文的仿真实验受到实验环境的限制，在实际的应用中，可以搭建环境配置较高的区块链平台以满足身份认证性能要求。

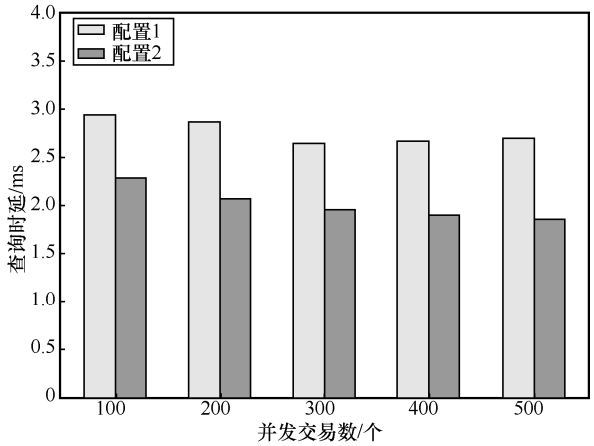

图 7 数字身份信息查询时延

5.4 安全仿真分析

本文采用 AVISPA 工具进行安全仿真，在上述物理机中部署了 SPAN1.6 程序。AVISPA 是用于建立安全协议模型和分析安全协议的工具，融合了 4 种不同的分析终端：OFMC、ATSE、SATMC 和 TA4SP，采用 HLPSL（high level protocol specification language）建立安全协议的分析模型，可以通过协议模拟、入侵者模拟和攻击模拟来检测安全协议是否达到预期的安全目标[20]。

本文将所提多因子身份认证方案转换为由 HLPSL 建立的分析模型。由于该方案中涉及异或操作，因此，本文采用支持异或操作的 OFMC 终端和 ATSE 终端进行安全仿真分析，结果如图 8 和图 9 所示。安全仿真分析结果表明，所提多因子身份认证方案是安全的。

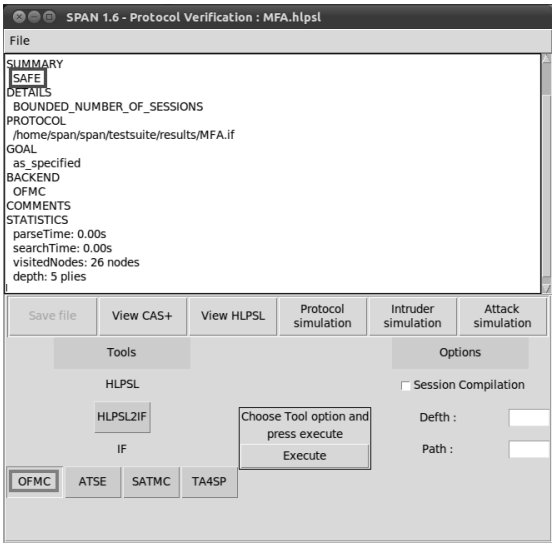

图 8 基于 OFMC 终端的 AVISPA 安全仿真分析结果

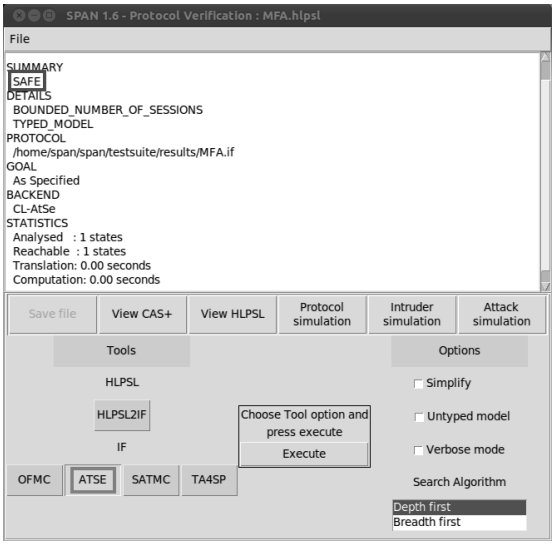

图 9 基于 ATSE 终端的 AVISPA 安全仿真分析结果

5.5 方案对比分析

为全面分析方案性能，本节从计算时延、通信开

销和安全性等方面将所提方案与已有多因子认证方案 IoMT 方案[21]、LMAAS-IoT 方案[22]、SELAMAT 方案[23]、AV5G 方案[24]、IoD 方案[25]进行对比分析。

身份认证算法的计算时延和通信开销对认证效率具有重大影响，本节将所提方案和上述多因子认证方案进行对比分析，结果如表 5 所示。其中，T_{ecc}、T_{puf}、T_{bp}、T_S 分别表示椭圆曲线标量点乘运算、物理不可克隆算法、双线性配对运算和对称加解密运算的运行时间，在上述实验环境下，$T_{ecc} \approx 0.003$ ms，$T_{puf} \approx 0.12$ ms，$T_{bp} \approx 4.2$ ms，$T_S \approx 0.016$ ms。不同方案的认证计算时延和通信开销对比如图 10 和图 11 所示。在计算时延方面，所提方案与 IoMT 方案、LMAAS-IoT 方案、AV5G 方案、IoD 方案的计算时延均为 1 ms 左右，明显低于 SELAMAT 方案。在通信开销方面，所提方案认证过程中涉及的通信信息为 2 次 DID、2 个签名和一个身份信息，共 512 bit，小于其他几种方案。综合来说，所提方案在计算开销和通信开销方面具有优势。

表 5　　计算时延和通信开销对比分析

认证方案	计算时延/ms	通信开销/bit
IoMT 方案	$10T_h + 6T_{ecc} + T_B$	2 848
LMAAS-IoT 方案	$30T_h + T_B$	1 696
SELAMAT 方案	$T_{bp} + 7T_h + 12T_S$	1 336
AV5G 方案	$28T_h + 12T_{ecc} + 2T_{puf} + T_B$	2 112
IoD 方案	$3T_{ecc} + 25T_h + T_B$	2 374
所提方案	$6T_A + 4.5T_h + T_B$	512

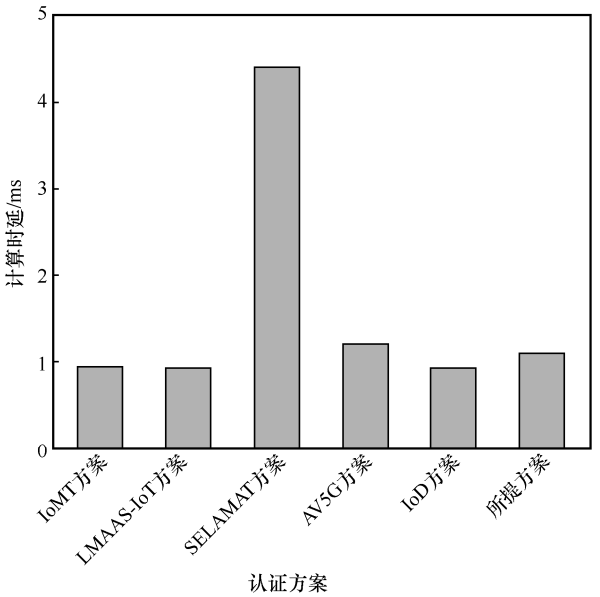

图 10　认证方案计算时延对比

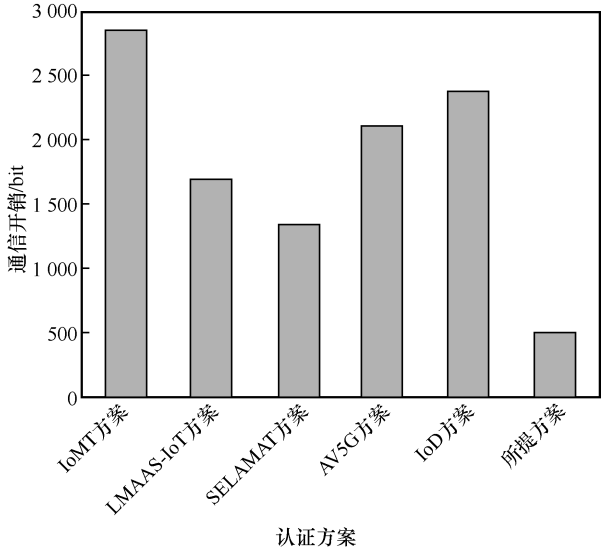

图 11　认证方案通信开销对比

安全性是身份认证系统中最基本的需求，本节将所提方案与上述多因子身份认证方案进行了安全性对比分析。表 6 给出了几种常见的安全性对比分析结果，前 5 种方案均基于哈希运算和智能卡等用户设备实现，认证信息加密后存储在智能设备中，一旦设备丢失将无法实现身份认证，而所提方案基于区块链技术实现，存储身份因子的分布式账本具有分布性使其能够抵御分布式拒绝服务攻击。前 5 种方案均将全部身份因子联合加密后写入智能设备，身份认证时必须输入全部的身份因子，并且部分方案未能实现身份的更新或撤销。而所提方案的身份因子独立存储在分布式账本中，可以灵活地根据文化资源共享系统接入者的所在组织选择其中的某几种身份因子进行认证。综合来说，所提方案安全性更强。

6　结束语

本文提出了面向文化资源可信共享的多因子身份认证方案。该方案能够兼容存量系统中的多种身份因子，解决了多元市场主体存量系统接入成本高的问题。并且该方案基于分布式账本构建异构数字身份数据模型，为多因子身份认证方案提供基础身份数据。多因子认证算法包括系统初始化、身份注册、身份认证、身份因子更新和身份因子撤销，利用非对称加密算法和异或运算实现了快速多因子身份认证，提高了多因子身份认证的灵活性，避免了单因子认证的安全风险。安全分析和仿真结果表明，该方案具有较高的安全性和认证效率。

表 6　　**安全性对比分析**

安全性	IoMT 方案	LMAAS-IoT 方案	SELAMAT 方案	AV5G 方案	IoD 方案	所提方案
身份保密性	√	√	√	√	√	√
抵御重放攻击	×	√	√	√	√	√
抵御窃听攻击	√	√	√	√	√	√
抵御伪造攻击	√	√	√	√	√	√
抵御 DDoS 攻击	×	×	×	×	×	√
身份可更新性	√	√	×	√	√	√
身份可撤销性	√	√	×	×	×	√
灵活性	×	×	×	×	×	√
多因子认证	√	√	√	√	√	√

另外，该方案不仅适用于文化资源可信共享场景，还能扩展应用于智能医疗、工业物联网等领域，实现基于多因子的身份认证，提升敏感信息可信共享的安全性和效率。

参考文献：

[1] 中国公共关系协会.文化资源数据分类与代码: T/CPRA 301—2021[S]. 2021.
China Public Relations Association. Classification & codes of cultural resource data: T/CPRA 301—2021 [S]. 2021.

[2] CHEN L Q, LIM H W, YANG G M. Cross-domain password-based authenticated key exchange revisited[J]. ACM Transactions on Information and System Security, 2014, 16(4): 1-32.

[3] ALSALEEM B O, ALSHOSHAN A I. Multi-factor authentication to systems login[C]//Proceedings of 2021 National Computing Colleges Conference (NCCC). Piscataway: IEEE Press, 2021: 1-4.

[4] ELIZABETH, KENNEDY, CHRISTOPHER, et al. Data security and multi-factor authentication: analysis of requirements under EU law and in selected EU member states[J]. Computer Law & Security Review, 2016, 32(1): 91-110.

[5] 唐飞, 包佳立, 黄永洪, 等. 基于属性的多授权中心身份认证方案[J]. 通信学报, 2021, 42(3): 220-228.
TANG F, BAO J L, HUANG Y H, et al. Multi-authority attribute-based identification scheme[J]. Journal on Communications, 2021, 42(3): 220-228.

[6] ALFADHLI S A, LU S F, CHEN K, et al. MFSPV: a multi-factor secured and lightweight privacy-preserving authentication scheme for VANETs[J]. IEEE Access, 2020, 8: 142858-142874.

[7] LIU Y, ZHONG Q, CHANG L, et al. A secure data backup scheme using multi-factor authentication[J]. IET Information Security, 2016, 11(5): 250-255.

[8] 王松伟, 陈建华. 基于混沌映射的多因子认证密钥协商协议[J]. 计算机应用, 2018, 38(10): 2940-2944, 2954.
WANG S W, CHEN J H. Multi-factor authentication key agreement scheme based on chaotic mapping[J]. Journal of Computer Applications, 2018, 38(10): 2940-2944, 2954.

[9] WANG M M, RUI L L, YANG Y, et al. A blockchain-based multi-CA cross-domain authentication scheme in decentralized autonomous network[J]. IEEE Transactions on Network and Service Management, 2022, 19(3): 2664-2676.

[10] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. 2008.

[11] ZHANG R, XUE R, LIU L. Security and privacy on blockchain[J]. ACM Computing Surveys, 2019, 52(3): 1-34.

[12] MONRAT A A, SCHELÉN O, ANDERSSON K. A survey of blockchain from the perspectives of applications, challenges, and opportunities[J]. IEEE Access, 2019, 7: 117134-117151.

[13] DODIS Y, REYZIN L, SMITH A. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data[C]//Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 523-540.

[14] 翁启. 一种基于区块链的数字身份认证方案[D]. 西安: 西安电子科技大学, 2019.
WENG Q. A blockchain-based digital identity authentication scheme[D]. Xi'an: Xidian University, 2019.

[15] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198-208.

[16] CANETTI R, FULLER B, PANETH O, et al. Reusable fuzzy extractors for low-entropy distributions[J]. Journal of Cryptology, 2021, 34: 1-33.

[17] BURROWS M, ABADI M, NEEDHAM R. A logic of authentication[J]. ACM Transactions on Computer Systems, 1989, 8(1): 18-36.

[18] LABIOD Y, KORBA A A, GHOUALMI-ZINE N. Detecting DDoS attacks in IoT environment[J]. International Journal of Information Security and Privacy, 2021, 15(2): 145-180.

[19] YU B, LI X F, ZHAO H. Virtual block group: a scalable blockchain model with partial node storage and distributed hash table[J]. The Computer Journal, 2020, 63(10): 1524-1536.

[20] 赵国威. 安全协议形式化自动验证工具 AVISPA 的研究[D]. 长春: 吉林大学, 2014.
ZHAO G W. Research on AVISPA, a formal automatic verification tool for security protocols[D]. Changchun: Jilin University, 2014.

[21] MAHMOOD K, AKRAM W, SHAFIQ A, et al. An enhanced and provably secure multi-factor authentication scheme for Internet-of-multimedia-things environments[J]. Computers & Electrical Engineering, 2020, 88: 106888.

[22] AYFAA B, APA C. LMAAS-IoT: lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment[J]. Journal of Network and Computer Applications, 2021, 192: 103177.

[23] KHALID H, HASHIM S J, AHMAD S M S, et al. SELAMAT: a new secure and lightweight multi-factor authentication scheme for cross-platform industrial IoT systems[J]. Sensors, 2021, 21(4): 1428.

[24] MIAO J, WANG Z, NING X, et al. Practical and secure multifactor authentication protocol for autonomous vehicles in 5G[J]. Software: Practice and Experience, 2022: doi.org/10.1002/spe.3087.

[25] 张敏, 许春香, 张建华. 无人机网络中基于多因子的认证密钥协商协议研究[J]. 信息网络安全, 2022(9): 21-30.
ZHANG M, XU C X, ZHANG J H. Research on authentication key agreement protocol based on multi-factor in Internet of drones[J]. Netinfo Security, 2022(9): 21-30.

[作者简介]

王苗苗（1989− ），女，河北廊坊人，北京邮电大学博士生，主要研究方向为区块链、信息安全等。

芮兰兰（1979− ），女，安徽潜山人，博士，北京邮电大学副教授、博士生导师，主要研究方向为网络管理、移动网络、边缘计算等。

徐思雅（1988− ），女，北京人，博士，北京邮电大学副教授、硕士生导师，主要研究方向为信息通信网络管理、SDN/NFV、移动边缘计算和人工智能等。