计算机科学
COMPUTER SCIENCE

基于多级承诺协议的联盟链身份认证方案研究

孙敏, 李新宇, 张鑫

引用本文

孙敏, 李新宇, 张鑫. 基于多级承诺协议的联盟链身份认证方案研究[J]. 计算机科学, 2024, 51(11A): 240200079-7.

SUN Min, LI Xinyu, ZHANG Xin. Study on Identity Authentication Scheme of Alliance Chain Based on Multi-level Commitment Protocol [J]. Computer Science, 2024, 51(11A): 240200079-7.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240200079

基于多级承诺协议的联盟链身份认证方案研究

孙 敏 李新宇 张 鑫
山西大学计算机与信息技术学院 太原 030006
(minsun@sxu.edu.cn)

摘 要 针对现有方案在差异化隐私保护场景下仅支持粗粒度的属性保护策略,提出了一种基于多级承诺协议的身份认证隐私保护方案(Iascb-Mcp),旨在允许用户根据需求选择性地公开或保密其属性信息,以满足不同隐私场景下的保护需求。该方案通过多级承诺结构实现对用户属性的保护。首先,每个用户属性被分配一个隐私等级,根据隐私等级设计了相应的承诺协议。其次,根据不同隐私级别的用户属性采用不同的身份验证方式,利用零知识证明确保在用户高隐私级别属性不暴露的情况下仍能进行有效身份认证。最后,利用 Iascb-Mcp 方案构建了一个基于联盟链身份验证的系统,解决了链下用户属性的隐私验证以及链上不同群组之间交易的安全性问题。安全分析与实验结果表明,在身份认证过程中其他用户无法获取证明者的高隐私级别属性;与群签名方案相比,Iascb-Mcp 的验证时间降至 1~3 s;与双环签名方案相比,新生成的证明文件大小是原文件大小的 1/10 左右。

关键词:区块链;零知识证明;承诺协议;身份验证;隐私保护
中图分类号 TP309

Study on Identity Authentication Scheme of Alliance Chain Based on Multi-level Commitment Protocol

SUN Min,LI Xinyu and ZHANG Xin
School of Computer and Information Technology,Shanxi University,Taiyuan 030006,China

Abstract As existing schemes only support coarse-grained attribute protection policies in differentiated privacy protection scenarios,an identity authentication privacy protection scheme based on multi-level commitment protocol(Iascb-Mcp) is proposed in this paper,which aims to allow users to selectively disclose or keep secret their attribute information according to requirements,so as to meet the protection requirements in different privacy scenarios. The scheme realizes the protection of user attributes through multi-level commitment structure. First,each user attribute is assigned a privacy level,and the corresponding commitment protocol is designed according to the privacy level. Secondly,different authentication methods are adopted according to the user attributes of different privacy levels,and zero-knowledge proof is used to ensure that the user's high privacy attributes can still be effectively authenticated without being exposed. Finally,the Iascb-Mcp scheme is used to construct a system based on alliance chain authentication,which solves the privacy authentication of off-chain user attributes and the security of transactions between different groups on the chain. The results of security analysis and experiment show that other users cannot obtain the high privacy attribute of the prover in the authentication process. Compared with the group signature scheme,the authentication time of Iascb-Mcp is reduced to 1s to 3 s. Compared with the two-ring signature scheme,the newly generated proof file is about one-tenth of the size of the original file.

Keywords Blockchain,Zero-knowledge proof,Commitment agreement,Identity authentication,Privacy protection

1 引言

近年来,随着互联网的迅猛发展,各种技术层出不穷,这也使得互联网产生的数据与日俱增。身份认证作为信息安全领域的一个关键议题日益凸显着其重要性,有效的身份认证对于确保访问控制、安全审计、入侵防范等安全机制的实施至关重要。但在身份认证的过程中,恶意敌人也可能利用各种手段窃取认证数据,并以同样的方式推断出有用的信息[1],从而获取到不属于他们的信息。随着区块链技术的出现,其去中心化信用和不可篡改的特性使得它逐渐被应用到金融业务、医疗、物联网、教育、追踪溯源、身份认证等领域[2-4]。然而,由于区块链管理尚不完善,目前仍然面临着许多问题。对于区块链上的非法数据,尚未形成一套正式的规则机制,尤其在隐私保护方面,公有链需要公开整个网络的相关交易信息,以便网络中的节点达成共识,这可能会带来隐私泄露的风险。联盟链通常由一组预选的节点共同管理区块链网络,这意味

基金项目:山西省基础研究计划项目(20210302123455,201701D121052)
This work was supported by Shanxi Province Basic Research Program,China(20210302123455,201701D121052).
通信作者:孙敏(minsun@sxu.edu.cn)

着身份管理往往由这些实体集中控制。这可能导致中心化的身份认证系统降低了用户对自身身份数据的控制权，增加了数据被泄露和滥用的风险。在联盟链中，参与者之间需要共享一定的身份信息以便进行交易，但如果身份信息存储在区块链上，可能会导致信息泄露；而如果采用加密技术进行身份信息存储，又可能影响交易的效率和可用性。在上述参与者共享身份信息进行交易时会暴露参与者的身份属性信息，而目前的研究缺乏针对属性信息进行差异化隐私保护。针对这些问题，本文提出了一种多级承诺协议身份认证方案。其主要贡献如下：

1)实现了更加细粒度的控制，对证明者属性信息按照隐私级别划分为 3 种等级，针对不同级别的隐私等级进行相应的承诺协议。

2)为了确保用户属性信息在验证过程的安全，设计了一种多级承诺协议以保护证明者的属性信息，并编写了智能合约用于自动验证。

3)设计了一种零知识证明协议，协议选择使用哈希函数代替随机预言机来实现 Fiat-Shamir 启发式方法[5]生成非交互式零知识证明。该协议在证明用户拥有某些高隐私级别的属性时，无需实际披露这些属性的具体数值或细节，从而保证了数据从链下到链上传输的安全性。

2 相关工作

区块链技术的广泛应用使得身份认证中的隐私问题成为研究热点。为了应对这一挑战，国内外学者开展了大量关于隐私保护的研究工作。文献[6]提出了一种基于同态加密的属性访问控制方案来保证属性和策略的隐私性，但在解密过程中，将解密任务分配给了多个区块链节点，导致链上运行时间较长。文献[7]提出了一种基于智能合约的可验证隐私保护方案，该方案在不需要可信第三方的前提下可以实现隐私信息的保护，但该方案中存在信息串通的风险，并且要求多次提交数据，导致计算和通信开销较大。文献[8]提出了基于群签名的零知识证明身份方案，文献[9]在此基础上提出了一种环签名身份认证方案。尽管这两种方案解决了计算复杂度的问题，但在验证过程中却依赖于签名成员的数量，一定程度上增加了验证的时间。针对上述问题，本文提出了一种多级承诺协议方案(Iascb-Mcp)，用于对不同隐私等级的用户属性进行身份验证。该方案支持对用户属性进行细粒度的验证，并提供相应的保护策略。

3 预备知识

3.1 区块链

区块链[10]是一种去中心化的分布式数据库技术，基本特征包括不可篡改性、分布式共识、透明性和去中心化。核心概念是由区块构成的链式数据结构，每个区块包含多个交易记录，并通过加密技术和共识算法确保数据的安全性和一致性。联盟链是区块链的一种形式，其特点是由几个预选的节点或实体组成，这些节点之间相互信任并共同管理区块链网络。与公有链不同，联盟链的参与者通常具有已知身份，并且需要经过许可才能加入网络。联盟链的优势在于其更高的效率和可扩展性，以及更好的隐私保护作用，适用于身份认证等领域。

3.2 零知识证明

零知识证明[11]是一种重要的密码学工具。证明者可以通过一系列复杂的交互过程，向验证者证明某个声明的真实性。在这个过程中，验证者无需了解具体信息，就可以确信这个声明是正确的。本文主要用到的零知识证明是基于离散对数的证明：证明者能够在不泄露 x 值的情况下向验证者证明其满足等式 $y=g^x$。一般来说，设计一种新的零知识证明都是首先构建 sigma 协议。这种协议通常用于在不安全的通信环境中确保信息的机密性和完整性。sigma 协议表示为图 1 中的 3 个阶段：1)证明者向验证者发送一个承诺 *commit*；2)验证者向证明者发送一个随机数代表挑战 *challenge*；3)证明者根据验证者发送的挑战作出回应。对于这种零知识证明协议，两个恶意证明者在合作的情况下可以恢复解出证明的隐私信息，而大多数比较常见的验证情况需要满足完美零知识性。

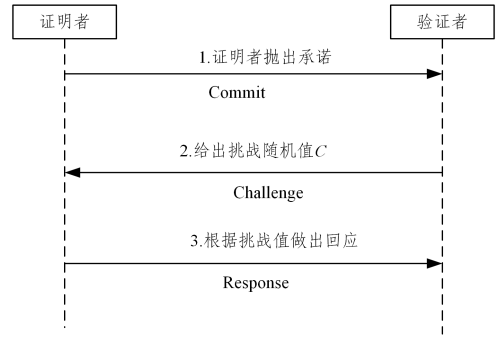

图 1 Sigma 协议图

Fig. 1 Sigma protocol diagram

3.3 Merkle 树

Merkle[12]树，也称为默克尔树，是一种树状数据结构，由叶子节点、内部节点和根节点组成，通常用于有效地验证大量数据块的完整性，而无需传输或存储整个数据集。验证过程通常是将所有数据块的哈希值排列成叶子节点，构建出 Merkle 树的底层，通过将相邻的叶子节点的哈希值组合成父节点，逐层向上构建 Merkle 树，直到计算出根节点的哈希值。这种结构使得可以快速而有效地检查数据的完整性，即使在数据量很大的情况下也能够高效验证。

3.4 承诺协议

承诺协议[13]是一种用于确保某一主体在未来按照其事先承诺的方式作出行为的协议。此类协议涉及两个主要实体，即承诺者和验证者。在协议中，承诺者对某一数值或信息进行承诺，并生成相应的承诺，随后将其传递给验证者。在未来的某个时刻，验证者有权要求承诺者公开其所承诺的值，并验证其是否与先前所生成的承诺一致。其数学定义如下。

承诺方案是 PPT(Probabilistic Polynomial Time Algorithm)算法的元组 $\tau=(Setup,Commit,Open)$，其中：$Setup(1^\lambda)\rightarrow pp$ 采用安全参数 λ 生成公共参数 pp；$Commit(pp;m)\rightarrow(C;r)$ 获取秘密消息 m 并输出公开承诺 C 和秘密打开提示 r。$Open(pp,C;m,r)\rightarrow b\in\{0,1\}$ 利用打开提示 r，验证承诺 C 对消息 m 的打开。

承诺协议的核心要求在于确保承诺的不可伪造性和隐私

性。不可伪造性保障了承诺者无法否认其过去的承诺，定义如下所示：

$$Pr\left[b_0=b_1\neq 0\wedge m_0\neq m_1:\begin{cases}pp\leftarrow Setup(1^{\lambda})\\(C,m_0,m_1,r_0,r_1)\leftarrow Д(pp)\\b_0\leftarrow Open(pp,C,m_0,r_0)\\b_1\leftarrow Open(pp,C,m_1,r_1)\end{cases}\right]$$

而隐私性则确保在未来之前无法获取承诺的实际值，定义如下所示：

$$\left|Pr\left[b_0=b':\begin{cases}pp\leftarrow Setup(1^{\lambda})\\(m_0,m_1,st)\leftarrow Д(pp)\\b_0\leftarrow\{0,1\}\\(C_b;r_b)\leftarrow Commit(pp;m_b)\\b'\leftarrow Д(pp,st,C_b)\end{cases}\right]-\frac{1}{2}\right|=$$

$$negl(\lambda)$$

4　方案设计

方案的组成部分包括证明者、区块链和智能合约。各自的功能描述如下。

证明者：在本方案中证明者根据自己属性的隐私级别进行身份证明。

区块链：区块链是该身份认证方案设计的底层平台，主要负责完成智能合约的部署、链下证明者的身份验证，以及链上双方交易的共识。本方案采用的共识算法是 PBFT(Practical Byzantine Fault Tolerance)[14]。

智能合约：智能合约扮演着验证者的角色，能够自动验证来自证明者的陈述是否有效。

4.1　方案模型

在该模型中，合约管理者生成公开参数，并接受证明者用户的公开参数申请。用户提交要证明身份的属性，根据隐私级别执行不同程度的承诺。可以公开的身份属性信息以明文形式提交，而含有隐私信息的属性则需发送零知识证明请求。链上的 Group1 和 Group2 公共节点负责部署验证合约，并通过验证零知识证明请求检验证明者身份的合法性。验证通过后，证明者用户可成为联盟链中的一员。当联盟链中的 Group1 和 Group2 发送交易请求时，发送交易请求的节点将该群组内所有节点构建出新的默克尔树，并计算根哈希值来让接受交易的群组节点进行验证。交易群组的节点根据提供的根哈希值进行计算比较它们是否一致，如果一致，则不同群组发送交易的信息可信。Iascb-Mcp 方案的模型设计架构如图 2 所示。

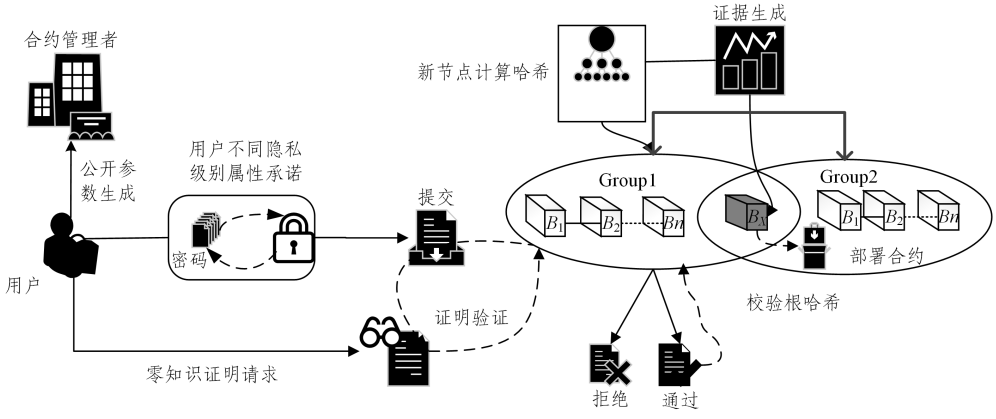

图 2　Iascb-Mcp 方案模型图

Fig. 2　Diagram of Iascb-Mcp solution model

方案的主要执行流程包括参数初始化、定义用户属性和隐私级别、多级承诺、身份验证、链上通信验证 5 个阶段。具体步骤如下：

参数初始化。首先建立联盟链网络，合约管理者编写验证的智能合约并部署于联盟链网络中，生成证明者与智能合约通信的相关公开参数。

定义用户属性和隐私级别。证明者将自己所需验证的属性按照隐私级别划分为高隐私级别属性与低级别隐私属性。高隐私级别表示该属性包含敏感信息，在验证过程中必须予以隐私保护；而低隐私级别表示属性的信息不属于敏感范畴，在验证过程中可以选择是否披露。

多级承诺。为了更加灵活和细粒度地为用户验证的属性提供隐私保护，设计了一种层级承诺机制，能够维护高隐私级别属性的保密性，还允许对低隐私级别属性进行选择性的公开。多级承诺结构图如图 3 所示。

身份验证。针对需要公开的用户属性，方案通过向智能合约提交明文属性，由合约执行重新计算承诺的操作，并对其合法性进行验证。系统能够在验证阶段实现透明性和可靠性，而且为用户属性的合法性提供了可验证的机制。针对高级别隐私的用户属性，引入了零知识证明协议，以在验证过程中实现对具体用户属性的非泄露性。采用零知识证明协议使得验证者能够确认用户拥有某一属性，而无需了解该属性的具体数值。

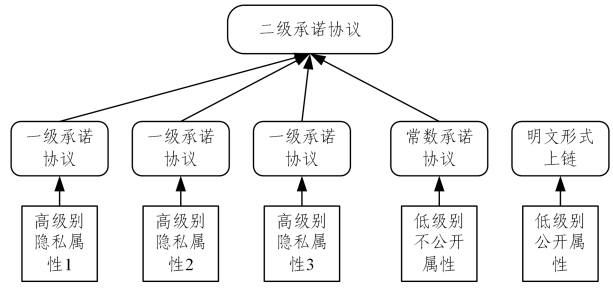

图 3　多级承诺结构图

Fig. 3　Diagram of multilevel commitment protocol structure

链上通信验证。用户在通过身份属性验证后，成为群

组 1 的一部分，并获取得到自己的节点 ID 与公钥地址。首先，由群组 1 的主节点构建包含新添加节点的 Merkle 树，并重新计算根哈希。接着，群组 1 生成零知识证明，包括节点哈希和 Merkle 树验证路径。然后，群组 1 部署证明合约给公共节点，群组 2 验证公共节点数据证明的有效性和 Merkle 树的根哈希一致性。如果证明有效且根哈希一致，群组 2 认为新节点存在于群组 1 中，双方可以互相传递数据，并保护节点交易内容的隐私。

4.2 具体方案设计

4.2.1 方案描述

Iascb-Mcp 方案主要设计符号及其定义如表 1 所列。

表 1 方案符号说明

Table 1 Scheme symbol description

符号	描述
p	循环群的阶
g	循环群的生成元
π	零知识证明证据
v	零知识认证的随机值
t	零知识认证的承诺值
H	安全的哈希函数
a_i	待验证的用户属性
r_i	承诺协议过程随机因子
C_{ai}^1	用户属性第一次的承诺值
C_{ai}^2	用户属性第二次的承诺值
$H(\pi)$	证据加密后的数字表示
res	零知识认证的回应值
$data$	低隐私级别的属性集合
com	承诺函数

4.2.2 参数初始化

采用 FISCO BCOS 平台作为底层区块链搭建双群组的八节点联盟链，并设置了 PBFT 共识协议，同时检查区块链和共识协议的运行状态。由合约管理者向证明者和验证者公开双方的公共参数。公开参数生成的过程如下。

$Setup(1^n)\rightarrow pp$：输入安全参数 n，生成公共参数 $pp=(G,g,p)$。G 是乘法循环群，g 是该循环群的生成元，p 是该循环群的阶。

4.2.3 用户属性和隐私级别

为描述每个证明用户所具备的属性，方案引入一个属性集合 A，其中每个元素 a_i 代表用户的一个特定属性。同时，引入了属性隐私级别 L，该级别用于划分属性的隐私敏感性。考虑 n 个不同的属性时，将其形式化为 $A=\{a_1,a_2,\cdots,a_n\}$。对于每个属性 a_i，其隐私级别由 $L(a_i)$ 表示，其中 $L(a_i)$ 有两种取值：高和低。

4.2.4 多级承诺

在一级承诺中，对于隐私级别高的属性，采用哈希函数和生成元来生成承诺值。使用随机数作为承诺协议的随机因子，生成高隐私级别属性的承诺值。对于隐私级别低的属性，提供了一种选择性的公开机制。若在验证时需要公开该属性，则在向智能合约提交数据时，选择以明文形式进行提交。如果用户选择保持该属性的隐私性，将其替代为随机常数 k 并不进行实质性的承诺。具体如式(1)所示：

$$k=com(data) \tag{1}$$

在二级承诺中，对第一级承诺中的高隐私级别属性和低隐私级别不公开属性进行了合并，并进行了二次承诺。确保对合并后的属性集合生成一个更为综合的承诺值。对每一个用户的高级别隐私属性分别进行第一次承诺，$r1$ 是第一次承诺的随机因子，之后对每一个用户的高级别隐私属性分别进行第二次承诺，$r2$ 是第二次承诺的随机因子，具体如式(2)、式(3)所示：

$$C_{ai}^1=g^{h(a_i,r1)} \tag{2}$$

$$C_{ai}^2=g^{h(C_{ai}^1,r2)} \tag{3}$$

4.2.5 身份验证

对于隐私级别低的用户不公开属性，可选择通过打开承诺的方式进行验证。验证者根据用户提供的数据($data$，k，)重新计算 $com(data)$，将计算的结果与 k 进行等值比较，检验数据是否发生改变或者丢失。

对于高隐私级别用户属性，在验证过程中需要保持零知识性，具体的验证过程如下。

证明者用户将两次承诺生成的总数据作为零知识证明的证据提交上链。

$$\pi=g^{C_{ai}^2} \tag{4}$$

生成随机数 v 作为本次零知识证明通信的安全通道。

$$t=g^v \bmod p \tag{5}$$

证明者给出关于本次验证的挑战值，利用 Fiat-Shamir 启发式[15]将发送的挑战值和证据进行绑定，记作 $H(\pi)$，并在验证者接收到挑战值之后发送回应值 res。

$$res=v-H(\pi)\times C_{ai}^2 \tag{6}$$

验证者在接收到上述来自证明者的 t，$H(\pi)$，res 信息之后进行零知识证明验证，检验证明者关于隐私信息的陈述是否正确，并根据接收到的回应值进行等值比较。如果相等，则认为用户所证明的属性可靠，该用户可以作为联盟链上群组中的一个成员；否则，验证不予以通过。

$$g^{res}\times\pi^{H(\pi)}(\bmod p)?=t \tag{7}$$

4.2.6 链上通信验证

证明者在成为群组 1 中的节点之后，获取得到自己的节点 ID 和公钥地址。主节点开始构建新的 Merkle 树，并验证重新生成的根哈希值与证明者提供的哈希值是否一致，检验算法设计如算法 1 所示。该部分的具体步骤如下。

步骤 1 $DataAuth(node_{ID},PK_i)\rightarrow sign_h$：输入新加入群组验证的节点编号和公钥地址，将生成一个哈希值 $h_{ID}=H(node_{ID},PK_i)$ 并利用私钥进行签名 $sign_{h_i}=(SK_i,h_{ID})$。

步骤 2 $ConstraintCircuit(X,ID,PK_i)\rightarrow C$：根据新加入群组的节点 $leaf$ 重新构建新的默克尔树，并计算新的根哈希值。

步骤 3 $ZKP\text{-}Prove(C,Path,X)\rightarrow proof$：默克尔树构建完毕之后，通过算数电路计算生成零知识证明 $proof$。使用零知识证明 Zk-Snark 协议将所需节点的哈希值与 Merkle 路径中的所有哈希值组成生成一个证明。

步骤 4 $ZKP\text{-}Verify(proof,root,Path)\rightarrow(1/0)$：生成证据之后部署合约到公共节点，由智能合约自动验证比对证明者提供的根哈希值是否一致，当验证通过时输出 1，否则输出 0。

算法 1 Merkle 树验证算法

输入：root，leaf

输出：1 or 0

```
1. Init(初始化节点编号)
2. for i←1 to i <Tree. high by i++ do
3. if(左节点编号>右节点编号) then
4.      swap(交换左右节点编号)
5.    end if
6.    if(群组的新节点编号为 0) then
7.      left←Cal(left,leaf)/*新节点作为左节点与叶子节点计算新的哈希*/
8.      Create(path,Proof)/*从默克尔树左边路径编号创建证据*/
9.    else
10.     right←Cal(right,leaf) /*新节点作为右节点与叶子节点计算新的哈希*/
11.     Create(path,Proof) /*从默克尔树右边路径编号创建证据*/
12. end for
13. if(证明者计算的根哈希与默克尔树根哈希一致)then
14.   return 1
15. else
16.   return 0
17. end
```

5　方案分析

5.1　正确性分析

在执行完毕 sigma 协议计算过后进行相等性数据验证，由式(4)－式(7)可以推出：

$$g^{res}\times\pi^{H(\pi)}\equiv t(\mathrm{mod}\ p) \tag{8}$$

5.2　链上交易分析

由于 ZK-Snark[16] 不能直接用于解决所有的计算问题，因此，在进行验证时首先需要将验证的问题转换为算数电路对应的算数逻辑表达式。

$$u_in_1+u_in_2+\cdots+u_in_j=1,i\in\{1,2\},j\in\{1,2,\cdots,n\} \tag{9}$$

通过引入中间变量的方式，将算术逻辑表达式转换为算术电路。式(9)对应的算术电路表示如下：

$$\begin{cases}mco_1=u_in_1+u_in_2\\mco_2=u_in_1+u_in_2\\\cdots\\out=mco_{j-2}+u_in_j\end{cases} \tag{10}$$

其中，mco_i 表示中间门电路的输出；u_in_j 表示群组 i 中的第 j 个节点的哈希数据；out 代表最终的算术电路输出，当输出的结果为 1 时表明验证合法，否则不合法。

将上述的算术电路转换为 QAP(Quadratic Assignment Problems)。QAP 的定义如下。

一个度数为 d、大小为 m 的二次算术程序 Q 由多项式 $\{L_j(X)\},\{R_j(X)\},\{O_j(X)\},j\in[0,\cdots,m-1]$ 和一个目标多项式 $T(X)=\prod(X-i)_{i=0}^{d-1}$ 组成。当赋值 $(1,x_i,\cdots,x_{m-1})$ 满足 Q 时，$T(X)|P(X)$，且 $P(X)=L(X)\cdot R(X)-O(X)$。

根据式(10)的算术电路定义一组向量集合 $\boldsymbol{s}$。

$$\boldsymbol{s}=[one,u_in_1,\cdots u_in_i,mco_1,\cdots,mco_{j-2},out] \tag{11}$$

其中，One 表示常量。以第一步算术电路为例 $mco_1=u_in_1+u_in_2$，执行 QAP 转化则存在一组向量 $(\boldsymbol{l},\boldsymbol{r},\boldsymbol{o})$ 满足 $\boldsymbol{sl}*\boldsymbol{sr}=\boldsymbol{so}$。

$$\begin{cases}l=[0,1,1,\cdots,0]\\r=[1,0,0,\cdots,0]\\o=[0,\cdots,0,1,\cdots,0]\end{cases} \tag{12}$$

将向量 $(\boldsymbol{l},\boldsymbol{r},\boldsymbol{o})$ 代入计算可以得到转换后的表达式与原始算术电路相等。针对式(12)存在的多组向量，可以利用拉格朗日插值表达式将向量表达式转换为多项式，将所有向量看作是一个多项式的解，通过多项式数组 $L(x),R(x),O(x)$ 来确定门电路对应的向量组。假设存在目标多项式 $T(X)$ 可以整除 $P(X)$，从而得到验证的 QAP 方程式为：

$$L(X)\cdot R(X)-O(X)=T(X)H(X) \tag{13}$$

通过验证该算式来证明提交的证明证据信息是有效合法的。

5.3　安全性分析

本节分析攻击者在多项式时间内破解隐私信息的可能性。假设对于任意在概率多项式时间内攻击者能够解出隐私信息的可能性均可忽略，则认为方案满足安全性。分析过程如下：

如果存在攻击者 A 和攻击者 B 尝试协同破解该隐私信息，由攻击者 A 作出自己的零知识回应信息：此时有 $res_1=v_1-H(\pi)\times C_{a_i}^2$，类似地，攻击者 B 也执行同样的操作得到 $res_2=v_2-H(\pi)\times C_{a_i}^2$，此时对于该零知识证明攻击的过程存在两种情况。

情况 1：如果在概率 θ 的情况下两个攻击者得到的随机值相同，即 $v_1=v_2$，根据式(6)可以得出：

$$res_1=v_1-H(\pi)\times C_{a_i}^2 \tag{14}$$

$$res_2=v_2-H(\pi)\times C_{a_i}^2 \tag{15}$$

由式(14)和式(15)作差可以得知：

$$res_1-res_2=0 \tag{16}$$

情况 2：在 $1-\theta$ 的概率得到的随机值不同的情况下，即 $v_1\neq v_2$，式(14)和式(15)作差可以得知：

$$res_1-res_2=v_1-v_2 \tag{17}$$

根据式(16)和式(17)可知，以上两种情况下均不含有隐私信息。因此，根据上面两种对于随机值的分析情况，在本文方案中攻击者无法破解证明者的隐私信息。协议具有安全性。

6　实验分析

6.1　实验环境

本节对设计的零知识证明协议进行了环境部署和性能测试。实验采用 Ubuntu20.04 操作系统，内存 4 GB，使用 Fisco Bcos2.9.2 搭建多节点联盟链平台，Solidity0.8.18 编写验证智能合约，Circom2.1.6 编写零知识证明算术电路。

6.2　链下验证时间分析

文献[9]中的协议提供了一次运行 sigma 协议的通用定义，并形式化了完整性和健全性。然而，该方案中没有解决恶意验证者可能带来的零知识性和顺序组合性问题。文献[8]中的协议允许证明者从多方计算协议构建有效的零知识协议，并没有讨论零知识的特殊合理性。为了方便比较性能，本文分别比较了密钥长度为 512，1 024，2 048，3 072，4 096，8 192 比特下的验证时间消耗。为了排除实验数据的偶然性，表中的数据均为 100 轮次测试的平均值，密钥的长度越长，意味着安全性也越高。从图 4 中可以知道，随着密钥长度的增加，验证的时间也相应增加，但方案 Iascb-Mcp 的优势更明显。

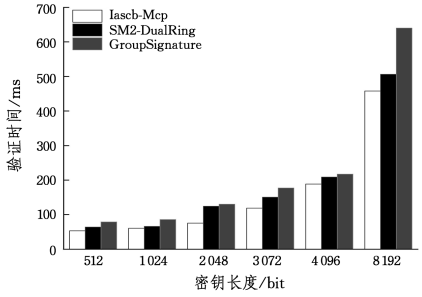

图 4 不同密钥长度时的消耗时间

Fig. 4 Time consumption with different key lengths

6.3 证明证据分析

Iascb-Mcp 方案在验证不同群组交易产生的证据时，只需要对新加入的节点进行哈希运算，重新生成 Root 哈希，解决了文献[9]中采用群签名验证的方式需要对所有数据进行重新哈希，从而导致签名时间过长、证据生成时间过长等问题。从图 5 可知，随着群组中节点数量的增加，按照 Merkle 树生成的零知识证明文件大小是群签名验证文件的 1/10～1/100。

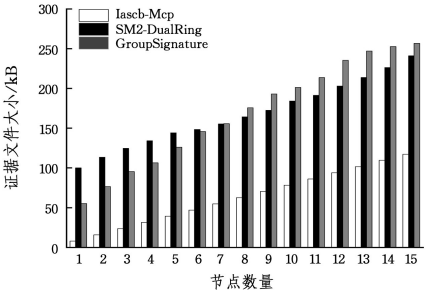

图 5 证据文件大小对比图

Fig. 5 Evidence file size comparison chart

6.4 链上验证时间分析

相较于群签名方案，方案 Iascb-Mcp 在验证时不需要每次重新计算所有群组节点的哈希值，只需对新加入的群组成员进行零知识证明。实验分别设置了 1～15 层默克尔树的节点数量进行验证时间测试，从图 6 可知，Iascb-Mcp 方案的验证时间总体维持在 1～3 s 之间，随着节点数量的不断增加，群签名验证方案验证消耗的时间呈指数级增加，方案 SM2-DualRing 相比群签名验证所消耗的时间也较少，总体维持在 1～6 s 之间。

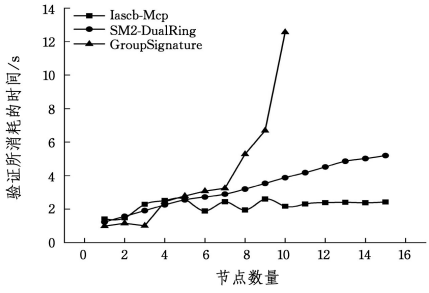

图 6 不同请求数的吞吐量对比图

Fig. 6 Throughput comparison diagram for different requests

6.5 区块链压力测试

衡量区块链性能的指标之一是 TPS(Transactions Per Second)，代表每秒可以处理的交易数量，Iascb-Mcp 的交易吞吐量测试方法是：设置不同的 QPS(Queries Per Second)请求数量，分别为 1000，3000，5000，7000，9000，10000。总交易量为 10000，观察联盟链群组 1 和群组 2 的交易吞吐量，Group1 在方案中由于需要同时负责 Sigma 合约和 Zk-Snark 合约的部署，因此吞吐量略低于 Group2。部署的合约的 TPS 总体维持在 247～410 之间。具体测量的 TPS 情况如图 7 所示。

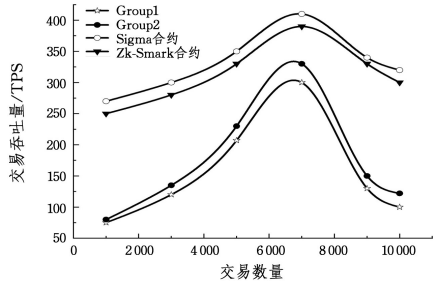

图 7 不同请求数的吞吐量对比图

Fig. 7 Throughput comparison diagram for different requests

结束语 本文针对用户属性隐私级别提出了一种多级承诺身份认证方案 Iascb-Mcp，对不同隐私级别的用户属性采用不同的身份验证方法。对低隐私级别的用户属性采用承诺计算的方式进行验证，而对于高隐私级别的用户属性通过零知识证明进行验证。与同类型协议相比，Iascb-Mcp 具有更高效率和更加安全的验证过程，能够保证从链下数据到链上不同群组数据的交易验证过程都保持零知识性。未来的工作重点将包括解决零知识证据文件大小的线性增加问题，以及分析用户属性隐私数据的可用性。

参 考 文 献

[1] LIU Y H, ZHANG J B, MUHAMMD S P, et al. Research on identity authentication system of Internet of Things based on blockchain technology[J]. Journal of King Saud University - Computer and Information Sciences, 2022, 34(10, Part B): 10365-10377.

[2] HUANG H, ZHU P, XIAO F, et al. A blockchain-based scheme for privacy-preserving and secure sharing of medical data[J]. Computers & Security, 2020, 99: 102010.

[3] YANG X, LI W. A zero-knowledge-proof-based digital identity management scheme in blockchain[J]. Computers & Security, 2020, 99: 102050.

[4] LI W, MEESE C, GUO H, et al. Blockchain-Enabled Identity Verification for Safe Ridesharing Leveraging Zero-Knowledge Proof[C]// 2020 3rd International Conference on Hot Information-Centric Networking(HotICN). 2020: 18-24.

[5] LIU Y, ZHOU Y, ZHANG R, et al. (Full) Leakage resilience of Fiat-Shamir signatures over lattices[J]. Frontiers of Computer Science, 2022, 16(5): 165819.

[6] WU N, XU L, ZHU L. A blockchain based access control scheme with hidden policy and attribute[J]. Future Generation Computer Systems, 2023, 141: 186-196.

[7] CHEN B, LI X, XIANG T, et al. SBRAC: Blockchain-based sealed-bid auction with bidding price privacy and public verifiability[J]. Journal of Information Security and Applications, 2022, 65: 103082.

[8] ŞAHIN M S, AKLEYLEK S. A constant-size lattice-based par-

tially-dynamic group signature scheme in quantum random oracle model[J]. Journal of King Saud University-Computer and Information Sciences，2022，34(10，Part B)：9852-9866.

[9] FENG M，LIN C，WU W，et al. SM2-DualRing：Efficient SM2-based ring signature schemes with logarithmic size[J]. Computer Standards & Interfaces，2024，87：103763.

[10] SANKA A I，CHEUNG R C C. A systematic review of blockchain scalability：Issues，solutions，analysis and future research [J]. Journal of Network and Computer Applications，2021，195：103232.

[11] KUMARI P L S，DEVI C H S，THIVAHARAN S，et al. A resilient group session key authentication methodology for secured peer to peer networks using zero knowledge protocol[J]. Optik，2023，273：170345.

[12] CASTELLON C，ROY S，KREIDL P，et al. Energy Efficient Merkle Trees for Blockchains[C]// IEEE The 20th International Conference on Trust，Security and Privacy in Computing and Communications (TRUSTCOM 2021). Los Alamitos：IEEE Computer Soc，2021：1093-1099.

[13] HAQ I，WANG J，ZHU Y，et al. A survey of authenticated key agreement protocols for multi-server architecture[J]. Journal of Information Security and Applications，2020，55：102639.

[14] TAN P L，WANG R S，ZENG W H，et al. Overview of blockchain consensus algorithms [J]. Computer Science，2023，50(S1)：691-702.

[15] FIAT A，SHAMIR A. How To Prove Yourself：Practical Solutions to Identification and Signature Problems[M]// ODLYZKO A M. Advances in Cryptology—CRYPTO' 86：Vol. 263. Berlin，Heidelberg：Springer Berlin Heidelberg，2006：186-194.

[16] LIPMAA H，SIIM J，ZAJAC M. Counting Vampires：From Univariate Sumcheck to Updatable ZK-SNARK[C]// Advances in Cryptology — ASIACRYPT 2022. Cham：Springer International Publishing Ag，2022：249-278.

SUN Min，born in 1966，master，professor. Her main research interests include blockchain and cryptography.