计 算 机 研 究 与 发 展
Journal of Computer Research and Development
DOI: 10.7544/issn1000-1239.202440302
61(11): 2681−2692, 2024

# 基于区块链的群智感知双向信誉评估隐私保护

邓清勇[1] 左清华[1] 李哲涛[2] 王 恩[3] 郭 斌[4]
[1](教育区块链与智能技术教育部重点实验室(广西师范大学) 广西桂林 541004)
[2](暨南大学信息科学技术学院 广州 510632)
[3](符号计算与知识工程教育部重点实验室(吉林大学) 长春 130012)
[4](西北工业大学计算机学院 西安 710129)
(qydeng@gxnu.edu.cn)

# Privacy-Preserving Bilateral Reputation Evaluation in Blockchain Based Crowdsensing

Deng Qingyong[1], Zuo Qinghua[1], Li Zhetao[2], Wang En[3], and Guo Bin[4]
[1](*Key Lab of Education Blockchain and Intelligent Technology* (*Guangxi Normal University*), *Ministry of Education*, *Guilin*, *Guangxi* 541004)
[2](*College of Information Science and Technology*, *Jinan University*, *Guangzhou* 510632)
[3](*Key Laboratory of Symbolic Computation and Knowledge Engineering* (*Jilin University*), *Ministry of Education*, *Changchun* 130012)
[4](*College of Computer Science*, *Northwestern Polytechnical University*, *Xi'an* 710129)

**Abstract** Reputation management is an effective way to improve the quality of data collection in mobile crowdsensing, but existing subjective evaluation-based schemes are difficult to realize the real evaluation of worker reputation under privacy protection. To this end, we propose a bilateral reputation evaluation privacy-preserving (BREPP) scheme based on blockchain. The scheme firstly adopts random interference and Pedersen Commitment to hide the parameters of the workers' reputation update, and utilizes the compact linkable spontaneous anonymous group (CLSAG) signature to anonymously verify the reputation update process. Besides, it employs a combination of Bulletproofs and Schnnor signature to verify the reputation feedback process of the workers. Then, the sub-address method is adopted to achieve fast location retrieval when the identities of the workers and requesters are anonymized. Finally, a prototype system is deployed on Hyperledger Fabric to evaluate the performance of the reputation update. The simulation results show that compared with existing reputation privacy protection schemes, BREPP scheme reduces the total reputation management delay and reputation evaluation error rate by at least 2.00% and 24.96%, respectively. Compared with schemes without privacy protection, our scheme achieves a better balance between reputation evaluation accuracy and total delay.

**Key words** mobile crowdsensing; reputation management; blockchain; privacy preserving; anonymous verification

**摘 要** 在移动群智感知系统中,信誉管理是提高数据收集质量的有效途径,但现有基于主观评价的方案难以实现隐私保护下的工人信誉真实评估.为此,提出了一种基于区块链的分布式群智感知双向信誉评估隐私保护(bilateral reputation evaluation privacy-preserving, BREPP)方案.首先采用随机干扰、佩德森承

**收稿日期**: 2024-04-26; **修回日期**: 2024-07-31
**基金项目**: 广西自然科学基金重点项目(2023GXNSFDA026003); 国家自然科学基金项目(62076214, 62032020, U23B2027); 广西研究生教育创新计划项目(XYCSR2024100)
This work was supported by the Guangxi Natural Science Foundation (2023GXNSFDA026003), the National Natural Science Foundation of China (62076214, 62032020, U23B2027), and the Innovation Project of Guangxi Graduate Education (XYCSR2024100).
**通信作者**: 李哲涛(liztchina@hotmail.com)

诺隐藏工人信誉更新的参数,利用紧凑型可链接自发匿名群签名匿名验证了信誉更新过程,联合 Bulletproofs 范围证明与 Schnnor 签名验证了工人的信誉评估过程;然后,采用子地址方法实现工人和请求者身份匿名下的快速定位检索;最后在 Hyperledger Fabric 上部署了实验原型系统并进行了性能评估.结果表明,BREPP 方案与已有信誉隐私保护方案相比,信誉管理总时延和信誉评估误差率分别至少降低了 2.00 个百分点和 24.96 个百分点;与无隐私方案相比,在信誉评估准确率与总时延之间取得了较好均衡.

**关键词** 移动群智感知;信誉管理;区块链;隐私保护;匿名验证

**中图法分类号** TP391

随着移动智能设备的流行,结合了移动感知和众包思想的移动群智感知系统[1]应运而生.移动群智感知系统通常由 3 类实体组成:请求者、工人和云服务器平台,其中请求者在平台上发布任务,工人接受任务并上传感知数据,云服务器平台负责工人与请求者的双边通信[2].由于工人感知能力的差异性和自私性,其不可避免地会上传虚假的感知数据骗取报酬,从而导致请求者所获得的感知任务结果可靠性降低[3].因此,为了有效评估感知数据质量,很多学者提出了使用信誉值来评估工人历史行为的可行方案,以此判断工人上传的感知数据是正确的还是伪造的[4-6].在上述方案中,信誉成为工人最重要的隐私保护信息,高信誉能够增加工人被选取的概率,如果信誉泄露会使其在竞争中处于不利地位[7-8].

目前已有大量基于可信第三方的集中式信誉管理方案[9-11],提出将信誉值存储在可信第三方,由工人提供密文信誉值并申领任务.首先云服务器与可信第三方交互实现密文信誉下的工人筛选;然后利用工人提供的感知数据进行信誉反馈;最后由可信第三方在接收到信誉反馈后进行信誉更新.上述工作实现了包含存储、更新、验证的信誉隐私保护,但引入的可信第三方易受到内部或外部攻击的影响,一旦被恶意控制,信誉的正确性将无法得到保证,甚至会造成单点故障.为解决信誉管理的单点故障,研究者提出将区块链技术融入到群智感知框架中[12-16],利用区块链来完成信誉存储、信誉更新以及基于信誉的工人挑选.其核心思想是将信誉以密文形式存储在区块链中,由请求者进行评分实现信誉的更新.前提条件是请求者是诚实可靠的,不会伪造信誉评分.然而在基于信誉的激励机制中,这种假设往往是不成立的,请求者倾向于降低工人的信誉以减少任务支付成本.

虽然有众多基于区块链的群智感知信誉管理方案,但仍存在进一步研究的空间,主要体现在 2 个方面:1)智能合约实现密文任务评分.虽然智能合约能自动化执行任务评分,从而减少恶意行为的空间,但由于区块链上的数据需保持加密状态以保护隐私,如何在隐私保护前提下实现对工人信誉的准确评分成为一大挑战.2)信誉计算的透明性与隐私保护之间的矛盾.在区块链上,信誉评分的更新过程需要既透明可验证,又不泄露个人隐私,在加密环境下很难同时满足.为了解决以上问题,我们提出了一种基于区块链的分布式群智感知双向信誉评估隐私保护方案,具体的贡献有 3 个:

1)利用随机干扰、佩德森承诺(Pederson Commitment)、紧凑型可链接自发匿名群签名(compact linkable spontaneous anonymous group signature, CLSAG)匿名验证了工人的信誉更新过程,联合 Bulletproofs 范围证明与 Schnnor 签名验证了工人的信誉反馈过程.

2)采用子地址技术实现了工人和请求者的身份匿名,并为信誉更新过程提供了定位检索,提高了信誉更新效率.

3)在 Hyperledger Fabric 上构建了一个原型测试系统,与已有信誉隐私保护方案相比,信誉管理总时延和信誉评估误差率分别至少降低了 2.00 个百分点和 24.96 个百分点;与无隐私方案相比,在至多损失 29.75% 的信誉评估准确率的情况下,总时延至少降低了 48.53%.

## 1 相关工作

Cheng 等人[9-10]使用佩德森承诺和零知识证明实现了信誉值下的密文验证,通过可信第三方接收请求者的质量反馈和云服务器的密文信誉反馈实现了信誉更新.Li 等人[11]设计了一种安全比较协议保护了信誉隐私并减少了信任机构的参与度.为了提高信誉评估的准确性,Tang 等人[17]提出了一种集中式下的双向信誉评估方案.我们此前的工作设计了一种信任评估方法消除了对主观经验的依赖,并提出了一个双层信任评估模型[18-19],但上述评估过程均是在明文下进行的,且均引入了可信第三方,易造成单点故障,需设计分布式信誉管理以解决上述问题.

Li 等人[20]使用智能合约验证工人信誉，但其信誉仍以明文存储. Zhang 等人[21]采用可验证秘密共享方案保护信誉计算过程中的隐私. Shen 等人[22]通过密钥服务器分发密钥实现了信誉验证. 在上述研究中，信誉由于未被验证仍然存在被篡改的风险. 为此，Zhao 等人[23]设计了一种两阶段信誉更新方案. Feng 等人[24]利用英特尔软件防护扩展提出了一种基于信任评估的匿名信任认证方案. Wu 等人[25]采用随机地址与多层次可链接自发匿名群签名(multi-layered linkable spontaneous anonymous group signature, MLSAG)实现了工人的匿名信誉更新验证. 在上述研究中，因信誉由请求者主动评价且未受监管，因此容易引发恶意评估的风险. 为此，An 等人[26]在 BCDToken 中实现了一个基于同态加密的安全真相发现和可靠性评级机制来监管请求者的评分行为. 然而其信誉值以明文存储，且信誉验证需多次同态交互，难以适应于复杂、节点资源受限的去中心化信誉管理场景.

综上所述，现有工作忽视了在保护信誉隐私的前提下，如何应对请求者恶意行为以准确评估工人信誉的问题. 本文旨在实现隐私保护下的同时，对工人信誉进行准确且高效的评估，从而提高信誉管理效率与信誉评估准确性.

## 2 预备知识

本节将简要介绍佩德森承诺、Schnnor 签名、CLSAG 签名和 Bulletproofs 范围证明.

### 2.1 佩德森承诺

佩德森承诺方案允许一方隐藏其真实值且能向另一方证明其值的正确性[27]. 它是基于具有基点 $G$ 的椭圆曲线(elliptic curve, EC)建立的，具有同态加性，加密步骤为：

1)随机选取椭圆曲线上的基点 $H$，其中 $H\neq G$.

2)计算佩德森承诺 $C(x, a)=xG+aH$，其中 $x$ 是致盲因子，$a$ 是隐藏的值.

### 2.2 Schnnor 签名

Schnnor 签名允许签名者证明自己拥有私钥 $k$，对应的接收方可以使用签名者公钥 $K$ 验证其身份[28].

1)签名

①产生一个随机数 $r$ 并计算其公钥 $R=rG$，随后计算挑战值 $c=H_n(\xi, R)$，其中 $H_n$ 是一个哈希函数.

②定义响应值 $s=r+ck$，用户将发布签名 $\sigma=(R, s)$.

2)验证

①计算挑战值 $c'=H_n(\xi', R)$，随后计算 $S=sG$ 和 $S'=R+c'K$.

②若 $S=S'$，则签名被验证.

### 2.3 CLSAG 签名

CLSAG 签名算法[29]包括 3 个算法，分别是初始化算法、签名算法和签名验证算法.

1)初始化算法. 输入椭圆曲线的基点 $G$ 和阶数 $l$，输出哈希函数 $H^s$，$H^p$，其中 $H^s$ 被用来计算隐藏后的值，$H^p$ 被用来计算交易输入的密钥镜像.

2)签名算法. 给定消息 $\xi$，$d$ 个交易环，每个环包含 $n$ 个混淆的交易，设公钥集合为 $Q=\{Z_{u,v}\}$，其中 $u=0, 1, \cdots, n-1$，$v=0, 1, \cdots, d-1$. 令 $\pi$ 为交易环中真正签名者的索引，其拥有私钥集合 $SK_\pi=\{z_{\pi,v}\}$，将 $z_{\pi,0}$ 视为链接键，对应的公钥 $Z_{\pi,0}$ 为主公钥，其余的公钥均为辅助公钥. 首先，签名者计算链接标签 $\Im=z_{\pi,0}H^p(z_{\pi,0})$，辅助元件 $D_v=z_{\pi,v}H^p(z_{\pi,0})$，$v$=1, 2, …, $d$–1，辅助元件累加和 $D_{\text{sum}}=\sum_v D_v$. 其次，计算聚合系数 $u_x=H^s(0\|Q\|\Im\|D_{\text{sum}})$，$u_v=H^s(v\|Q\|\Im\|D_{\text{sum}})$. 然后，计算聚合公钥 $\Re=u_xH^p(z_{\pi,0})+\sum_v u_vD_v$，$W_u=u_xZ_{0,u}+\sum_v u_vZ_{u,v}$，$u$=1, 2, …, $n$–1. 最后，随机选取 $\alpha\in\{0, 1, \cdots, l-1\}$，计算 $L_\pi=\alpha G$，$R_\pi=\alpha H^p(Z_{\pi,0})$，$c_{\pi+1}=H^s(0\|Q\|\xi\|L_\pi\|R_\pi)$，进一步随机选取 $s_u\in\{0, 1, \cdots, l-1\}$，计算 $L_u=s_uG+c_uW_u$，$R_u=s_uH^p(Z_{u,0})+c_u\Re$，$c_{u+1}=H^s(0\|Q\|\xi\|L_u\|R_u)$，$u=\pi+1, \pi, \cdots, n-1, 0, 1, \cdots, \pi-1$，其中 $u=n-1$ 时，令 $c_n=c_0$，可以得到 $s_\pi=\alpha-c_\pi w_\pi$. 输出签名 $\sigma(\xi)=(c_0, s_0, s_1, \cdots, s_{n-1}, \Im, D_1, \cdots, D_{d-1})$.

3)签名验证算法. 给定公钥集合 $Q$、消息 $\xi$ 和签名值 $\sigma$，验证者首先计算聚集系数和聚集公钥，然后迭代计算 $L_u$，$R_u$，$c_{u+1}$，验证 $c_n=c_0$ 是否成立，若成立，则签名被验证.

### 2.4 Bulletproofs 范围证明

Bulletproofs 范围证明是一种零知识证明算法，允许证明者在不暴露原始值的情况下证明其值所属的范围[30]. 例如，$v$ 是待证明范围的值，利用佩德森承诺隐藏 $v$ 的值，$V=xG+vH$，现有证明者 $P$，向其他参与者证明其拥有满足 $V=xG+vH$ 且 $v\in[0, 2^n-1]$ 的证据. 证明包括 3 个算法：

1)初始化参数. 输入要证明的值 $v$，输出系统公开的承诺值 $V$.

2)证明. 输入系统公开的承诺值 $V$，输出承诺值和响应值参数 *Params*.

3)验证. 给定承诺值 $V$ 以及参数 *Params*，验证者计算给定参数下的响应值，并验证响应值是否相等. 若相等，输出 accept，表明证明有效；反之，则证明无效. 在此过程中原始值以承诺的方式向外公开，验证者

在未知原始值的情况下验证其值是否在所属的范围内.

## 3 BREPP 方案

本节首先介绍了如图 1 所示的基于区块链群智感知的双向信誉评估的系统架构及流程 BREPP (bilateral reputation evaluation privacy-preserving), 然后详细描述了在实现工人和请求者信誉管理方面的隐私保护方案.

### 3.1 系统模型

基于区块链群智感知的双向信誉评估的系统架构包括 3 种实体, 即请求者、工人和基于区块链的群智感知平台. 其中基于区块链的群智感知平台由双区块链构成, 按照存储的业务类型分为感知链和信誉链. 特别地, 感知链被用来存储任务的感知数据, 信誉链被用来存储工人和请求者的信誉值. 具体而言, 基于区块链群智感知的双向信誉评估包括 7 个步骤:

1)注册. 请求者和工人在本地生成公私钥对, 请求者利用本地公钥生成的地址在感知链和信誉链中注册, 注册完后可发布任务. 工人利用本地公钥生成地址在信誉链中注册, 注册完可参与感知任务. 特别地, 请求者和工人的信誉在信誉链中均被初始化为默认值.

2)发布任务. 请求者按照任务发布合约发布任务, 在发布任务前, 需用私钥对交易进行签名, 签名被验证后, 任务将会在感知链中被广播.

3)申请任务. 工人接收到感知链中广播的任务后, 根据自身的偏好, 选择申请任务.

4)招募工人. 请求者在招募时间内接收工人的申请, 根据自身的偏好选择多个可靠的工人, 并发布任务挑选结果到感知链中.

5)上传数据. 被选中的工人按照数据提交合约上传感知数据, 利用请求者的公钥对信息进行加密.

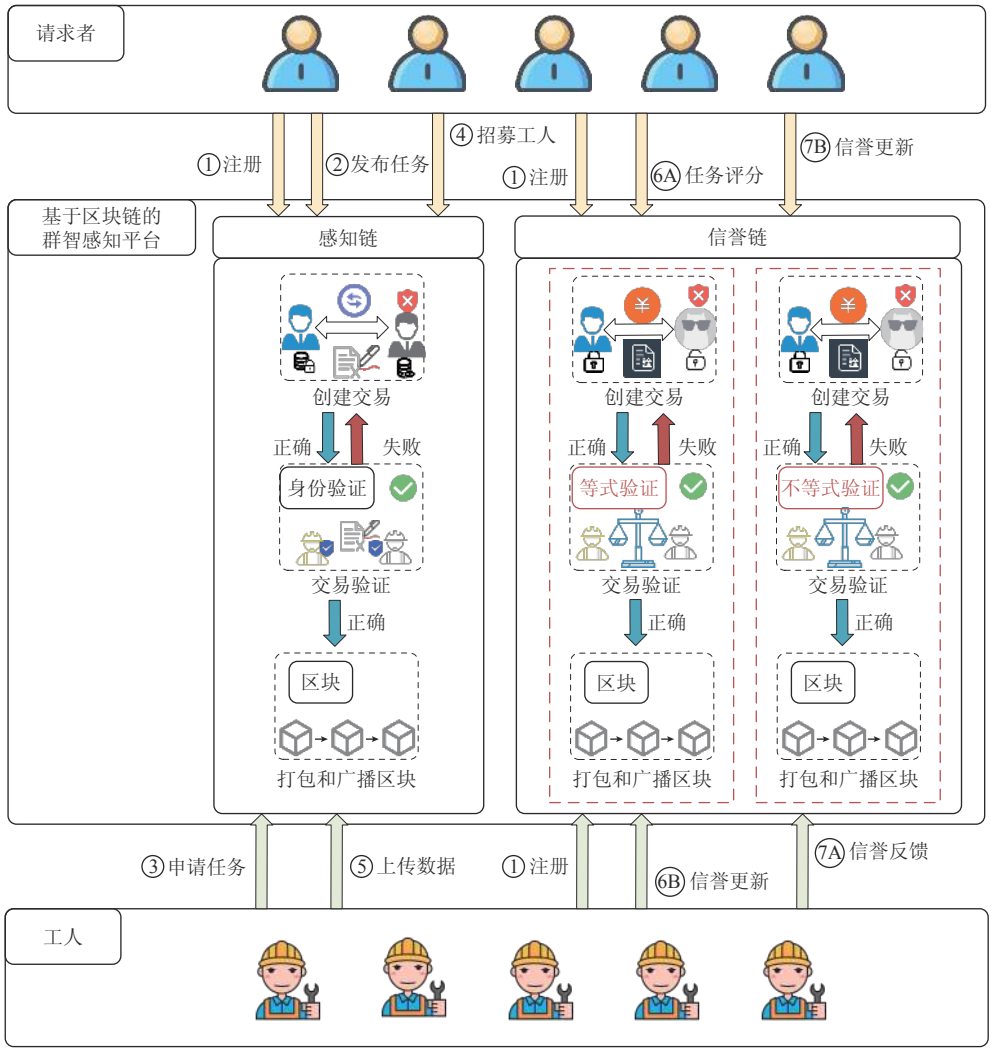



Fig. 1 Architecture and procedure of a bilateral reputation evaluation privacy-preserving (BREPP) scheme based on blockchain

图 1 基于区块链的双向信誉评估隐私保护方案的架构和流程

6)工人信誉更新. 请求者对工人进行信誉评分，其中发布的信誉评分以密文形式存放在信誉链中，只有对应的工人能够使用自己的私钥对其进行解密. 工人利用自己的私钥在信誉链中检索属于自己的信誉评分. 当达到系统阈值时，其自动进行信誉更新，并提供签名以供其他参与者的透明性验证，即等式验证.

7)请求者信誉更新. 工人对请求者进行信誉反馈，并提供零知识证明和 Schnnor 签名以供其他参与者的透明性验证. 请求者利用自己的私钥在信誉链中检索属于自己的信誉反馈，达到系统阈值后自动进行信誉更新.

### 3.2 威胁模型

本节描述了基于区块链群智感知的双向信誉评估的威胁模型. 在信誉管理系统中，工人和请求者分为好奇和恶意 2 类. 好奇的工人和请求者会按照系统所设置的规则监测并维护分布式账本，但会试图窥探其他参与者包括信誉评分等在内的隐私信息. 恶意的工人一方面会篡改自身信誉，以便在竞争任务过程中处于优先地位；另一方面因利益冲突会对请求者进行恶意信誉反馈，以此影响请求者信誉评分来获利. 恶意的请求者一方面会篡改自身信誉，以便在工人挑选任务过程中处于优先地位；另一方面出于自私性会恶意降低可靠工人的信誉评分，从而减少任务支付成本.

### 3.3 隐私目标

1)工人信誉隐私. 工人的信誉值应以密文形式存储在信誉链中，且只有接收其感知数据的请求者才能解密. 此外，工人的信誉更新过程需要以密文形式供其他参与者验证.

2)请求者信誉隐私. 请求者的信誉值应以密文形式存储在信誉链中，且只有接收其感知数据的工人才能解密. 此外，请求者的信誉更新过程需要以密文形式供其他参与者验证.

### 3.4 方案设计

本节设计了基于区块链群智感知的双向信誉评估隐私保护方案，主要从工人信誉管理与请求者信誉管理 2 部分做详细描述，其中包含信誉的加密存储、检索、更新、等式验证以及不等式验证.

#### 3.4.1 工人信誉管理

工人信誉管理过程包括工人提交数据、任务评分发布、信誉更新和验证环节. 首先被选中的工人参与感知任务，通过使用表 1 所示的事务调用任务数据提交合约上传感知数据，任务数据包括 3 项：

1)Task ID，被用来唯一标识工人参与的感知任务.

2)$U=qG$，选择一个素数阶群范围内的随机数 $q$ 作为私钥生成交易公钥.

**Table 1 Structure of a Task Data Transaction**

**表 1 任务数据交易结构**

| 类型 | 项目 | 描述 |
|---|---|---|
| Token | Task ID | 任务标识 |
| | $U=qG$ | 交易公钥 |
| | $E_{H_n(qE)}(p_i, B_i, data, h_{tr})$ | 任务相关数据 |

3)$p_i$，工人提供的权重干扰噪声，被请求者用来隐藏信誉，特别地，工人在本地会存储一个权重干扰向量 $\boldsymbol{P}=(p_1, p_2, \cdots, p_i, \cdots, p_m)$，其中 $p_1+p_2+\cdots+p_m=0$；$B_i$，工人提供的子公钥，被请求者用来计算任务评分的交易地址，特别地，工人在本地会存储当前子公钥集合的索引 $g_w$；$data$，工人上传的感知数据；$h_{tr}$，工人最新信誉更新交易的区块位置；$E_{H_n(qE)}()$，使用私钥 $H_n(qE)$ 进行加密，其中 $H_n()$ 为哈希函数，$E$ 表示请求者提供的公钥.

当任务数据被请求者接收后，请求者通过自身私钥与工人提供的交易公钥计算对称密钥 $H_n(eU)$ 以解密隐私数据. 在进行任务真值聚集[31]后，通过使用表 2 所示的事务调用任务评分发布合约提交工人的任务评分.

**Table 2 Structure of a Task Score Transaction**

**表 2 任务评分交易结构**

| 类型 | 项目 | 描述 |
|---|---|---|
| Token | $K^{ow}=H_n(B_i)G$ | 一次性匿名交易地址 |
| | $s_i=s\oplus H_n(\text{“}t_task\text{”}, rB_i)$ | 加密评分 |
| | $R=rG$ | 交易公钥 |
| | $w'=w+p_i$ | 加噪信誉 |
| | $C(x, s)=xG+sH$ | 评分承诺 |
| | $C(v, s')=vG+s'H$ | 加噪评分承诺 |
| | $E_{H_n(qB_i)}=(F_i, h_{dr}, v')$ | 评分相关数据 |
| Extra | $\theta_i=(ms,s)$ | Schnnor 签名 |

任务评分包括以下项：

1)$K^{ow}$，利用工人提供的子公钥产生的一次性匿名交易地址.

2)$s_i$，通过同态加密计算的任务评分密文.

3)$R$，选择一个素数阶群范围内的随机数 $r$ 作为私钥生成交易公钥.

4)$w'$，利用工人提供的权重干扰噪声生成加噪信誉，隐藏请求者真实的信誉 $w$.

5)$C(x,s)$，任务评分的佩德森承诺，其中致盲因子 $x=H_n(\text{“}t_task\text{”}, rB_i)$.

6)$C(v,s')$，加噪评分的佩德森承诺，其中加噪评

分 $s'=s\times p_i$, 致盲因子 $v=H_n(\text{“}tw_task\text{”}, rB_i)$.

7) $F_i$, 请求者提供的子公钥, 被工人用来信誉反馈的交易地址; $h_{dr}$, 请求者最新信誉交易的区块位置; $v'$, 请求者用来加密信誉值的致盲因子, 工人可以根据致盲因子解密出请求者提供的信誉值.

由于所有的任务评分只有工人能够解密, 所以信誉更新过程由工人自动执行. 工人检查完成任务的个数是否达到系统预设的任务数量 $m$, 若达到则通过使用表 3 所示的事务调用工人信誉更新合约发布交易进行信誉更新. 工人利用多个任务评分的加权均值更新自身的信誉值:

$$\tau=\frac{\sum_{i=1}^{m}s_iw_i}{\sum_{i=1}^{m}w_i}. \tag{1}$$

**Table 3 Structure of a Worker Reputation Update Transaction**

**表 3 工人信誉更新交易结构**

| 类型 | 项目 | 描述 |
|---|---|---|
| Input | $A_1$<br>⋮<br>$A_m$ | 任务评分交易环 |
| Token | $U=qG$ | 交易公钥 |
| | $s_i=\tau\oplus H_n(\text{“}r_task\text{”}, qK)$ | 加密评分 |
| | $C(y,\tau)=yG+\tau H$ | 信誉承诺 |
| Extra | $\sigma_r=(ms, c_0, s_0, \cdots, s_{n-1}, \cdots)$ | CLSAG 签名 |

考虑到信誉计算是由工人在链下完成的, 为了验证工人信誉计算过程的正确性, 实现信誉计算的透明性, 工人需向外提供证明以供其他参与者在任务评分密文状态下验证其计算过程的正确性. 具体而言, 利用任务评分承诺的同态加法对式(1)进行转换:

$$C(y,\tau)+\frac{\sum_{i=1}^{m}C(v_i,s_i')}{\sum_{i=1}^{m}w_i'}-\frac{\sum_{i=1}^{m}w_i'C(x_i,s_i)}{\sum_{i=1}^{m}w_i'}=\left(y+\frac{\sum_{i=1}^{m}v_i}{\sum_{i=1}^{m}w_i'}-\frac{\sum_{i=1}^{m}w_i'x_i}{\sum_{i=1}^{m}w_i'}\right)G+\left(\tau+\frac{\sum_{i=1}^{m}s_i'}{\sum_{i=1}^{m}w_i'}-\frac{\sum_{i=1}^{m}w_i's_i}{\sum_{i=1}^{m}w_i'}\right)H=\left(y+\frac{\sum_{i=1}^{m}v_i}{\sum_{i=1}^{m}w_i'}-\frac{\sum_{i=1}^{m}w_i'x_i}{\sum_{i=1}^{m}w_i'}\right)G. \tag{2}$$

设 $z$ 表示式(3)中的私钥部分, 验证式(1)等价于验证式(3), 表示为:

$$C(y,\tau)+\frac{\sum_{i=1}^{m}C(v_i,s_i')}{\sum_{i=1}^{m}w_i'}-\frac{\sum_{i=1}^{m}w_i'C(x_i,s_i)}{\sum_{i=1}^{m}w_i'}=zG. \tag{3}$$

为进一步保护工人的信誉隐私, 我们采用轻量级 CLSAG 环形签名隐藏任务评分交易与工人的关联性, 实现工人信誉更新交易输入的不可链接性. 设 $\pi$ 表示环中真正签名者的索引, 签名者拥有私钥集合 $\{z, k_1, \cdots, k_i, \cdots, k_m\}$, 其中 $k_i=H_n(B_i)$, 将私钥 $z$ 视为签名的链接键, 进行 CLSAG 签名, 以提供等式验证. 若 CLSAG 环形签名验证成功, 更新后的交易将被打包成区块发布到信誉链中, 记为 $h_{tr}$.

上述过程描述了工人信誉计算的透明性验证, 工人信誉更新整体流程如算法 1 所述, 其中行①~⑤为工人利用本地存储的主公钥、主私钥以及当前的索引生成的用于信誉更新的任务评分交易地址, 此过程能够得到任务评分交易地址集合. 行⑥~⑱为工人利用任务评分与请求者的信誉进行信誉加权更新, 需遍历任务评分交易地址集合. 首先利用交易地址检索并获取区块, 然后解密任务评分与请求者信誉, 并计算加噪评分, 再进一步计算评分承诺与加噪评分承诺. 若通过评分承诺、加噪评分承诺以及请求者信誉验证, 确认其没有恶意篡改或非法计算, 则将此任务评分交易存储到本地, 并进行信誉更新计算. 遍历完后, 若发现本地缓存的合法评分交易数达到系统所设置的阈值, 则通过式(1)计算并返回更新后的信誉值, 否则返回–1, 表示不更新.

**算法 1.** 工人信誉更新.

输入: 工人主公钥 $K$, 主私钥 $k$, 当前子公钥集合的索引 $g_w$;

输出: 更新后的信誉值 $\tau$.

① $K'=\varnothing$, $n=m$; /* 初始化交易地址列表与系统所设阈值*/

② $A=\varnothing$, $\tau=0$, $w_{sum}=0$; /* 初始化输入交易列表与更新后的信誉值以及权重和*/

③ for $i=(g_w-m):g_w$

④ $b_i=H_n(K\|i)+k$, $B_i=b_iG$, $K'\leftarrow H_n(B_i)G$;

⑤ end for

⑥ for each $k'\in K'$

⑦ 检索并获取区块号 $h_{k'}$;

⑧ $s=s_t\oplus H_n(\text{“}t_task\text{”}, b_iR)$, $s'=s\times p_i$, $w=w_t\oplus v'$;

⑨ $C'(x, s)=H_n(\text{“}t_task\text{”}, b_iR)G+sH$;

⑩ $C'(v, s')= H_n(\text{“}tw_task\text{”}, b_iR)G+s'H$;

⑪ if $C'(x, s)==C(x, s)$ and $C'(v, s')==C(x, s')$ and $w+p_i==w'$ then /* 验证任务评分是否篡改以及加噪评分与加噪权值的正确性*/

⑫ $A\leftarrow h_{k'}$, $\tau=\tau+s\times w$, $w_{sum}=w_{sum}+w$, $n$−−;

⑬ end if

⑭ end for

⑮ if $n==0$

⑯ return $\tau=\tau/w_{sum}$;

⑰ end if

⑱ return −1.

### 3.4.2 请求者信誉管理

请求者信誉管理过程包括工人的信誉反馈、信誉更新和验证环节. 首先工人在信誉更新后, 按照规则对请求者的评分进行信誉反馈. 若请求者评分与工人更新后的信誉的误差在允许误差范围内, 则评定请求者是诚实的, 反之是恶意的, 如式(4)所示.

$$\begin{cases}|\tau-s_i|\leqslant\delta, & l_i=1,\\ |\tau-s_i|>\delta, & l_i=0.\end{cases} \tag{4}$$

工人完成信誉评定后, 通过使用表 4 所示的事务调用信誉反馈合约发布评分.

**Table 4 Structure of a Reputation Feedback Transaction**

**表 4 信誉反馈交易结构**

| 类型 | 项目 | 描述 |
|---|---|---|
| Input | $A_1$ | 信誉交易环 |
| | $A_2$ | 任务评分交易环 |
| Token | $K^{or}=H_n(F_i)G$ | 一次性匿名交易地址 |
| | $l_i=l\oplus H_n(\text{“}t_rep\text{”}, rF_i)$ | 加密反馈 |
| | $R=rG$ | 交易公钥 |
| | $C(u, l)=uG+lH$ | 反馈承诺 |
| | $C(x, l')=xG+l'H$ | 下界承诺 |
| | $C(x, l'')=xG+l''H$ | 上界承诺 |
| | $ZKP=(A, S, T_1, T_2,\cdots)$ | Bulletproofs 证明 |
| Extra | $\sigma_r=(ms, c_0, s_0, \cdots, s_{n-1},\cdots)$ | CLSAG 签名 |
| | $\theta_i=(ms, l)$ | Schnnor 签名 |

信誉反馈评分数据包括 9 项:

1) $A_1$, 由工人提供的自身信誉交易与其他 $n$−1 个参与者的信誉交易混淆而成的交易环;

2) $A_2$, 由工人评定的任务评分交易与其他 $n$−1 个参与者的任务评分交易混淆而成的交易环;

3) $K^{or}$, 利用请求者提供的子公钥产生的一次性匿名交易地址;

4) $l_i$, 通过同态加密计算的信誉反馈密文;

5) $R$, 选择一个随机数 $r$ 作为私钥生成交易公钥;

6) $C(u, l)$, 信誉反馈的佩德森承诺, 其中致盲因子 $u=H_n(\text{“}t_rep\text{”}, rF_i)$;

7) $C(x, l')$, 下界佩德森承诺, 其中下界 $l'=\tau-s_i+\delta$, 致盲因子 $x'=H_n(\text{“}level_rep\text{”}, rF_i)$;

8) $C(x, l'')$, 上界佩德森承诺, 其中上界 $l''=\delta+s_i-\tau$;

9) $ZKP$, 工人提供的 Bulletproofs 范围证明.

评定过程是由工人在链下计算完成的, 为了防止工人的恶意报复行为, 验证评分过程的正确性, 实现信誉反馈计算的透明性, 工人需向外提供式(4)中的不等式与等式验证以供其他参与者在密文状态下验证其信誉反馈过程的正确性. 具体而言, 首先利用 Bulletproofs 轻量级零知识证明提供范围证明, 然后提供 Schnnor 签名以验证评分的正确性. 其中考虑到普通范围证明只能验证式(4)中 $\tau-s_i$ 是否是正数, 因此需要对绝对值不等式进行转换. 评分正向的特殊范围约束可转换为如式(5)两个不等式约束.

$$\begin{cases}\tau-s_i+\delta\geqslant 0,\\ \delta+s_i-\tau>0.\end{cases} \tag{5}$$

特别地, 在范围证明中, 因上界与下界均为工人链下计算, 工人需向外提供证明以验证上下界计算过程的正确性, 同理 3.4.1 节, 利用上下界承诺的同态加法表示为:

$$\begin{aligned}&C(y,\tau)-C(x,s_i)+C(\delta)-C(x',l')=z_1G,\\ &C(\delta)+C(x,s_i)-C(y,\tau)-C(x',l'')=z_2G.\end{aligned} \tag{6}$$

同理, 我们使用 CLSAG 环形签名实现输入任务评分交易与工人身份的不可链接性. 设 $\pi$ 表示环中真正签名者的索引, 签名者拥有私钥集合 $\{z_1, z_2, k_1, k_2\}$, 其中 $k_1, k_2$ 为交易地址的私钥.

由于所有的信誉反馈交易只有请求者才能链接, 故信誉更新过程由请求者自动执行. 请求者检查信誉反馈数是否达到系统预设的数量 $m$, 若达到阈值使用表 5 所示的事务发布交易进行信誉更新.

请求者利用 $\alpha$-$\beta$ 贝叶斯分布[32] 更新信誉, 如式(7)表示:

$$\begin{aligned}&\alpha=\alpha'+\sum_{i=1}^{m}l_i,\\ &T=T+m,\\ &w=\frac{\alpha}{T}.\end{aligned} \tag{7}$$

考虑到信誉计算是请求者在链下完成的, 为了验证请求者信誉计算的正确性, 实现信誉计算的透

**Table 5 Structure of a Requester Reputation Update Transaction**

**表 5 请求者信誉更新交易结构**

| 类型 | 项目 | 描述 |
|---|---|---|
| Input | $A_0$ | 信誉交易环 |
| | $A_1$ | 反馈交易环 |
| | ⋮ | ⋮ |
| | $A_m$ | 反馈交易环 |
| Token | $Q=qG$ | 交易公钥 |
| | $s_i=\tau\oplus H_n(\text{“}r_rep\text{”}, qE)$ | 加密评分 |
| | $C(x, \alpha)=xG+\alpha H$ | 正向因子承诺 |
| | $C(y, w)=yG+wH$ | 信誉承诺 |
| | $T=T+m$ | 反馈总次数 |
| Extra | $\sigma_r=(ms, c_0, s_0, \cdots, s_{n-1}, \cdots)$ | CLSAG 签名 |

明性, 请求者需向外提供等式证明, 即:

$$\begin{aligned} &C(x',a')+\sum_{i=1}^{m}C(u,l)-C(x,a)=z_1G,\\ &\frac{1}{T}C(x,a)-C(y,w)=z_2G. \end{aligned} \tag{8}$$

上述信誉反馈交易同样需要使用 CLSAG 环形签名实现其信誉更新输入的不可链接性. 签名者拥有私钥集合$\{z_1, z_2, k_1, k_2, \cdots, k_m\}$, 若签名验证成功, 信誉更新交易发布到信誉链中, 记为 $h_{dr}$.

上述过程描述了请求者信誉计算的透明性验证, 请求者信誉更新整体流程在算法 2 中被介绍. 算法 2 的行①~⑤为请求者利用本地存储的主公钥、主私钥以及当前的索引生成用于信誉更新的反馈交易地址, 此过程能够得到信誉反馈交易地址集合. 行⑥~⑲为请求者利用信誉反馈进行基于 $\alpha$-$\beta$ 贝叶斯分布的信誉更新. 首先利用交易地址检索并获取区块, 然后验证 CLSAG 签名, 判断工人承诺的上下界计算是否正确. 若验证通过, 进一步联合验证 *ZKP* 零知识证明和 Schnnor 签名. 若验证成功, 则表明其信誉反馈交易符合式(4)评定规则, 将此信誉反馈交易存储到本地, 进行信誉更新计算. 遍历完后, 若发现本地缓存的合法反馈交易数达到系统所设置的阈值, 则通过式(7)计算并返回更新后的信誉值, 否则返回–1, 表示不更新.

**算法 2.** 请求者信誉更新.

输入: 请求者主公钥 $E$, 主私钥 $e$, 当前子公钥集合的索引 $g_r$;

输出: 更新后的信誉值 $w$.

① $K'=\varnothing$, $n=m$; /* 初始化交易地址列表与系统所设阈值*/

② $A=\varnothing$; /* 初始化输入交易列表*/

③ for $i=(g_r-m):g_r$

④ $f_i=H_n(E\|i)+e$, $F_i=f_iG$, $K'\leftarrow H_n(F_i)G$;

⑤ end for

⑥ for each $k'\in K'$

⑦ 检索并获取区块号 $h_{k'}$;

⑧ if CLSAG 签名验证成功 then

⑨ if *ZKP* 零知识证明验证成功 then

⑩ $U'=C(u, l)-C(1)$;

⑪ if $\theta_t(ms, U')$ 验证成功 then

⑫ $A\leftarrow h_{k'}$, $\alpha=\alpha+1$, $n--$;

⑬ end if

⑭ else

⑮ if $\theta_t(ms, C(u, l))$ 验证成功 then

⑯ $A\leftarrow h_{k'}$, $n--$;

⑰ end if

⑱ end if

⑲ end for

⑳ if $n==0$

㉑ $T=T+m$;

㉒ return $w=\alpha/T$;

㉓ end if

㉔ return –1;

## 4 安全性分析

本节将给出基于区块链群智感知的双向信誉评估隐私保护方案的安全性分析. 主要针对 3.3 节中的隐私目标展开详细描述.

1)Proposition 1. 工人和请求者无法窥探其他参与者信誉隐私. 工人集合中的恶意攻击者接收来自请求者的信誉评分交易, 能够获取请求者提供的单个子公钥. 然而请求者每次发起信誉评分交易时均会产生一个新的子公钥. 一方面请求者的子公钥是由其公钥与索引拼接后的哈希组合私钥形成, 工人无法从单个子公钥衍生出子公钥集合, 故无法链接请求者的信誉反馈交易; 另一方面请求者的信誉使用同态加密以密文形式存放在信誉链中, 工人无法对信誉密文解密, 故其无法窥探其他参与者的信誉隐私. 同理, 请求者也无法窥探其他参与者的信誉隐私.

2)Proposition 2. 工人和请求者不能篡改其信誉. 由于信誉更新交易的输入是不可篡改的, 对应的信誉评分承诺无法篡改, 工人若篡改式(1)的计算, 将会导致用于 CLSAG 签名的密钥对不匹配, 进一步导

致 CLSAG 签名验证失败，因此工人无法篡改自身的信誉. 同理，请求者也无法篡改自身信誉.

3）Proposition 3. 工人不能对请求者进行恶意信誉反馈. 若工人对请求者进行恶意信誉反馈，即不满足评分规则(4)，根据 Proposition 2 可得，工人无法篡改其评分上界与评分下界，则工人提供的联合范围证明与 Schnnor 签名将验证失败，因此，工人不能对请求者进行恶意信誉反馈.

## 5 性能分析

本节首先从计算开销和通信开销对 BREPP 方案进行评估. 将所提出的信誉管理方案与文献 [25] 中提出的基于随机地址、MLSAG 环形签名方案（ARMS-MCS 方案）以及文献 [26] 中提出的基于智能合约的信誉管理方案（BCDToken 方案）进行了比较. 然后，将双向信誉评估与 ARMS-MCS 方案中采用的单向信誉评估以及 BCDToken 方案中采用的基于质量验证的信誉评估进行了比较.

### 5.1 计算和通信开销分析

计算和通信开销主要考虑哈希生成、公钥操作、验证 Schnnor 签名、数据传输以及交易达成共识的开销. 我们定义一次哈希生成操作的时延为 $T_g$，一次公钥操作的时延为 $T_k$，验证一个 Schnnor 签名的时延为 $T_s$，传输一个 256 b 的时延为 $T_m$，交易达成共识的时延为 $T_c$. 在工人信誉更新过程中，我们所提出的 BREPP 方案与 ARMS-MCS 方案主要分为 2 个阶段，分别为信誉评分交易验证阶段和信誉更新阶段，而 BCDToken 方案则分为质量验证阶段和信誉更新阶段. 在验证阶段，BREPP 方案需要在信誉链中检索最近发布的 $m$ 个交易. 根据 3.4 节中子公钥的计算描述，仅需要根据本地存储的索引计算出最近的子地址集合，并在信誉链中通过子地址进行检索比对找到对应的区块，而检索比对的时间可近似视为 0 ms. 因此，验证 $m$ 个交易的总计算开销为 $(2T_g+2T_k+T_s)m$. 而 ARMS-MCS 方案需要逐个检索，考虑到信誉链中产生的区块数与工人的数量成正比，则验证 $m$ 个交易的总计算开销为 $(T_g+T_k+T_s)m\times k\times n$，其中 $k\times n$ 表示工人距离上一次信誉更新的时间点所产生的区块数. 对于 BCDToken 方案，在质量验证阶段，需要计算同态加密下感知数据与估计真值之间的绝对值，并与请求者进行一次交互，其质量验证开销为 $(N+1)T_k+T_m+T_c$，其中 $N$ 为任务招募的工人数. 在信誉更新阶段，BREPP 方案对交易进行 CLSAG 签名，其计算、验证、传输以及达成共识的总开销为 $(3m+6n+5)T_g+2nT_k+(m+n+2)T_m+T_c$，而 ARMS-MCS 方案的总开销为 $(2m+2mn)T_g+2mnT_k+(mn+1+m)T_m+T_c$. 对于 BCDToken 方案，在信誉更新阶段，需要判断交互值是否相等，其计算以及达成共识的总开销为 $2T_k+T_c$. 综上可知，由于交易达成共识的开销远高于其他开销，因此我们提出的方案在工人信誉管理过程中的总开销较低.

如图 2 所示，BREPP 方案和 BCDToken 方案在区块链上能够稳定地进行验证，而 ARMS-MCS 方案在区块链上检索、验证的执行时延与工人的数量成正比，当参与任务的工人数量从 10 增加到 100 时，BREPP 方案执行时延降低了 6.30%~92.41%. 评估信誉更新阶段的性能如图 3 和图 4 所示. 图 3 记录了随签名总公钥数量变化的信誉更新阶段的总时延，其中 BREPP 方案与 ARMS-MCS 方案的总时延与签名总公钥数量呈正比，这是因为随着总公钥数量的增加，环形签名的验证和传输时延均会增加，而 BCDToken 方案的总时延与签名总公钥数量无关，当签名总公钥数量达到最大值 640 时，BREPP 方案的总时延与 BCDToken 方案相比仅增加了 286 ms. 图 4

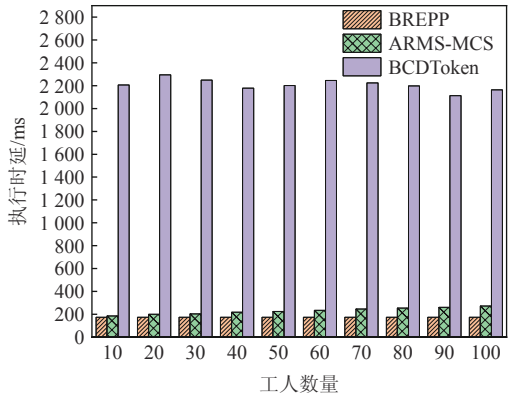



Fig. 2 Total delays in verification phase

图 2 验证阶段总时延

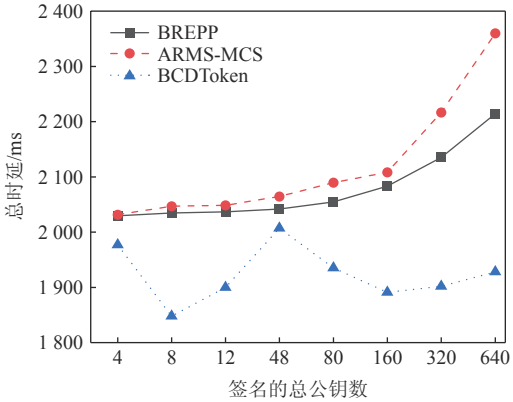



Fig. 3 Total delays in reputation update phase

图 3 信誉更新阶段总时延

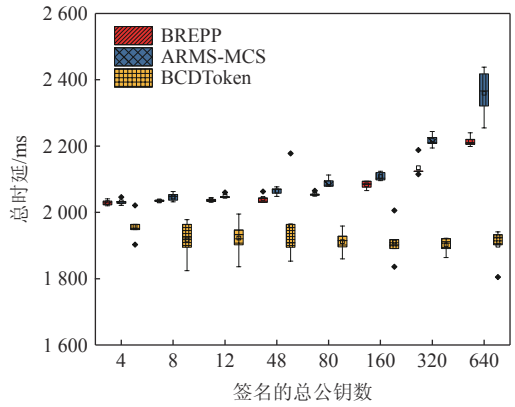



Fig. 4 Total reputation update delays in five experiments

图 4 信誉更新阶段总时延的 5 次实验

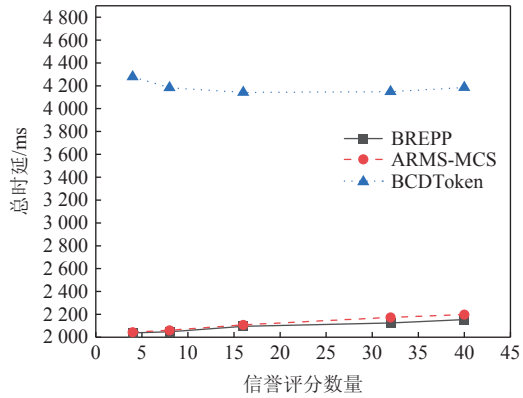



Fig. 5 Total delays in reputation management

图 5 信誉管理总时延

表明 5 次重复实验的偏离值较少, 受网络波动较小, 实验结果是可靠的. 图 5 记录了信誉管理的总执行时间, 其中总时延主要包括验证阶段和信誉更新阶段的总时延. 结果表明与 ARMS-MCS 方案与 BCDToken 方案相比, 总时延分别至少降低了 2.00%, 48.53%.

### 5.2 信誉评估分析

在信誉评估方面, BREPP 方案采用的是基于信誉的加权评估, 而 ARMS-MCS 方案采用的是单向信誉评估, BCDToken 方案采用的是基于质量验证的动态信誉评估. 考虑到请求者具有自私性, 若评分由请求者完成, 会恶意降低可信工人评分以降低成本. 为了真实模拟信誉评估场景, 利用高斯分布生成请求者的真实信誉. 对于请求者的恶意行为, 我们假定其会在 [0.1,0.7] 区间内均匀报告工人的声誉, 其中 0.7 是系统设定的信任上界.

如图 6 所示, 我们测试了真实信誉为 0.9 的工人在信誉评估过程中的表现. 随着诚实请求者的增加, BREPP 方案与 ARMS-MCS 方案中工人的信誉评估值逐步接近于真实值, 而 BCDToken 方案中工人的信誉评估值总是接近真实值, 这是因为其信誉评分是经过验证的且信誉更新是由智能合约自动完成的. 我们计算准确率为(|评估信誉−真实信誉|/真实信誉), 误差率则为(1−准确率). BREPP 方案与 BCDToken 方案相比准确率至多损失 29.75 个百分点. 而与 ARMS-MCS 方案相比, 误差率至少降低了 24.96 个百分点.

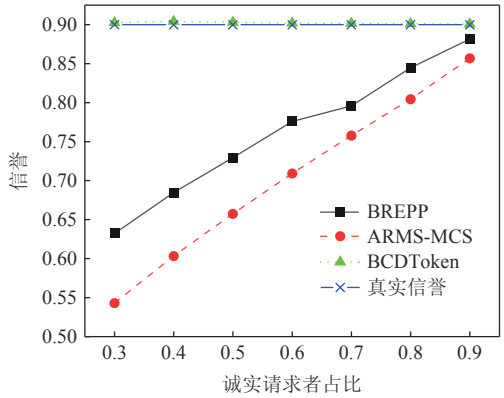



Fig. 6 Workers' reputation evaluation vs proportion of honest requesters

图 6 工人的信任评估 vs 诚实请求者占比

如图 7 所示, 我们测试了 BREPP 方案对真实信誉为 0.8 和 0.9 的工人的信誉评估影响程度, 结果表明对高可信工人的信誉评估准确率较高, 与真实值的绝对误差较小. 而 ARMS-MCS 方案对高可信工人的信誉评估准确率较低, 与真实值的绝对误差较大. 因此, BREPP 方案在高可信工人的信誉评估上展示了较强的优越性.

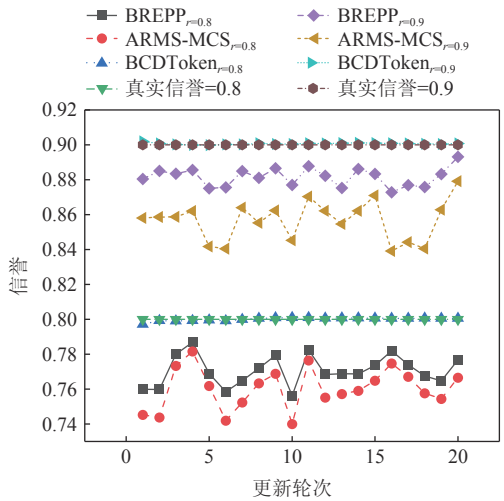



Fig. 7 Workers' reputation evaluation vs the number of update

图 7 工人信誉评估 vs 更新次数

如图 8, 我们研究了 BREPP 方案中请求者信誉更新方法的收敛性. 真实信誉值分别为 0.2, 0.4, 0.6, 0.8 的请求者在多轮实验中信誉逐渐收敛于其真实值, 证明了所提请求者信誉辨识方案的有效性.

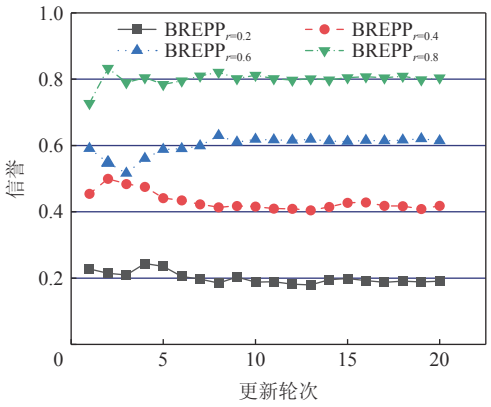



Fig. 8 Requesters' reputation evaluation vs the number of update

图 8 请求者信誉评估 vs 更新次数

## 6 结 论

在基于区块链的群智感知双向信誉评估系统中，我们采用随机干扰、佩德森承诺隐藏工人信誉更新的参数，利用 CLSAG 签名匿名验证了信誉更新过程，联合 Bulletproofs 范围证明与 Schnnor 签名验证了工人的信誉反馈过程. 最后，通过搭建原型测试和评估方案的性能，证实所提方案能有效降低信誉管理过程时延，且在工人信誉评估方面展现出优越性. 未来的工作将研究基于信誉的双边偏好任务匹配方案，并融合公平激励机制，为基于区块链的移动群智感知应用建立分布式的信誉评估框架.

**作者贡献声明**：邓清勇负责研究方案的设计和论文撰写；左清华负责算法分析和实验验证；李哲涛负责初稿审定和修改；王恩、郭斌提出指导意见并修改论文.

## 参 考 文 献

[1] Ganti R, Ye Fan, Lei Hui. Mobile crowdsensing: Current state and future challenges[J]. IEEE Communications Magazine, 2011, 49(11): 32−39

[2] Xu Tiancheng, Qiao Shaojie, Wu Jun, et al. A spatial crowdsourcing task assignment approach based on spatio-temporal location prediction[J]. Journal of Computer Research and Development, 2022, 59(2): 310−328(in Chinese)
(徐天承, 乔少杰, 武俊, 等. 一种基于时空位置预测的空间众包任务分配方法[J]. 计算机研究与发展, 2022, 59(2): 310−328)

[3] Tang Jianheng, Han Feijiang, Fan Kejia, et al. Credit and quality intelligent learning based multi-armed bandit scheme for unknown worker selection in multimedia MCS[J]. Information Sciences, 2023, 647: 119444

[4] Yan Lei, Yang Kan, Yang Shouyi. Reputation-based truth discovery with long-term quality of source in Internet of things[J]. IEEE Internet of Things Journal, 2022, 9(7): 5410−5421

[5] Wang Han, Liu Anfeng, Xiong N N, et al. TVD-RA: A truthful data value discovery-based reverse auction incentive system for mobile crowdsensing[J]. IEEE Internet of Things Journal, 2024, 11(4): 5826−5839

[6] Wang Ping, Li Zhetao, Guo Bin, et al. A UAV-assisted truth discovery approach with incentive mechanism design in mobile crowd sensing[J]. IEEE/ACM Transactions on Networking, 2024, 32(2): 1738−1752

[7] Gao Sheng, Chen Xiuhua, Zhu Jianming, et al. Trustworker: A trustworthy and privacy-preserving worker selection scheme for blockchain-based crowdsensing[J]. IEEE Transactions on Services Computing, 2022, 15(6): 3577−3590

[8] Zhao Junhui, Huang Fanwei, Liao Longxia, et al. Blockchain-based trust management model for vehicular ad hoc networks[J]. IEEE Internet of Things Journal, 2024, 11(5): 8118−8132

[9] Cheng Yudan, Ma Jianfeng, Liu Zhiquan, et al. A privacy-preserving and reputation-based truth discovery framework in mobile crowdsensing[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(6): 5293−5311

[10] Cheng Yudan, Ma Jianfeng, Liu Zhiquan, et al. A lightweight privacy preservation scheme with efficient reputation management for mobile crowdsensing in vehicular networks[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(3): 1771−1788

[11] Li Runchuan, Liu Zhiquan, Ma Yong, et al. RPPM: A reputation-based and privacy-preserving platoon management scheme in vehicular networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(6): 6147−6160

[12] Hui Yilong, Huang Yuanhao, Su Zhou, et al. BCC: Blockchain-based collaborative crowdsensing in autonomous vehicular networks[J]. IEEE Internet of Things Journal, 2022, 9(6): 4518−4532

[13] Wang Weizheng, Zhou Xiaokang, Li Xingwang, et al. BSIF: Blockchain-based secure, interactive, and fair mobile crowdsensing[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(12): 3452−3469

[14] Zhang Long, Qin Shuang, Feng Gang, et al. Integration of blockchain and mobile crowdsensing by trust-preserving mechanism[C]//Proc of IEEE Global Communications Conf. Piscataway, NJ: IEEE, 2022: 3748−3753

[15] Zhang Long, Feng Gang, Qin Shuang, et al. Trust-preserving mechanism for blockchain assisted mobile crowdsensing[J]. IEEE Transactions on Computers, 2023, 72(11): 3113−3126

[16] Wang En, Cai Jiatong, Yang Yongjian, et al. Trustworthy and efficient crowdsensed data trading on sharding blockchain[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(12): 3547−3561

[17] Tang Jianheng, Fan Kejia, Xie Wenxuan, et al. BTV-CMAB: A bi-directional trust verification based combinatorial multi-armed bandit scheme for mobile crowdsourcing[J]. IEEE Internet of Things Journal, 2024, 11(2): 1925−1938

[18] Li Zhetao, Wang Jianhui, Long Saiqin, et al. A trust evaluation joint active detection method in video sharing D2D networks[J]. IEEE Transactions on Mobile Computing, 2024, 23(7): 7739−7752

[19] Huang Mingfeng, Li Zhetao, Xiao Fu, el al. Trust mechanism-based multi-tier computing system for service-oriented edge-cloud networks[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(4): 1639−1651

[20] Li Ming, Weng Jian, Yang Anjia, et al. CrowdBC: A blockchain-based decentralized framework for crowdsourcing[J]. IEEE Transactions on Parallel and Distributed Systems, 2019, 30(6): 1251−1266

[21] Zhang Wenjing, Luo Yuchuan, Fu Shaojing, et al. Privacy-preserving reputation management for blockchain-based mobile crowdsensing[C]//Proc of IEEE Int Conf on Sensing, Communication, and Networking (SECON). Piscataway, NJ: IEEE, 2020: 1−9

[22] Shen Xiaodong, Xu Chang, Zhu Liehuang, et al. Blockchain-based lightweight and privacy-preserving quality assurance framework in crowdsensing systems[J]. IEEE Internet of Things Journal, 2023, 11(1): 974−986

[23] Zhao Ke, Tang Shaohua, Zhao Bowen, et al. Dynamic and privacy-preserving reputation management for blockchain-based mobile crowdsensing[J]. IEEE Access, 2019, 7: 74694−74710

[24] Feng Wei, Yan Zheng, Yang L T, et al. Anonymous authentication on trust in blockchain-based mobile crowdsourcing[J]. IEEE Internet of Things Journal, 2022, 9(16): 14185−14202

[25] Wu Haotian, Zheng Yucong, Zhao Bowen, et al. An anonymous reputation management system for mobile crowdsensing based on dual blockchain[J]. IEEE Internet of Things Journal, 2022, 9(9): 6956−6968

[26] An Baoyi, Xiao Mingjun, Liu An, et al. Secure crowdsensed data trading based on blockchain[J]. IEEE Transactions on Mobile Computing, 2023, 22(3): 1763−1778

[27] Pedersen T P. Non-interactive and Information-theoretic secure verifiable secret sharing[C]//Proc of Annual Int Cryptology Conf. Berlin: Springer, 1991: 129−140

[28] Schnorr C P. Efficient identification and signatures for smart cards[C]//Proc of Int Cryptology Conf. Berlin: Springer, 1989: 239−252

[29] Goodell B, Noether S, Blue A. Concise linkable ring signatures and forgery against adversarial keys[J/OL]. Cryptology ePrint Archive, [2023-10-12 ]. https://eprint.iacr.org/2019/654

[30] Bünz B, Bootle J, Boneh D, et al. Bulletproofs: Short proofs for confidential transactions and more[C]//Proc of 2018 IEEE Symp on Security and Privacy (SP). Piscataway, NJ: IEEE, 2018: 315−334

[31] Ma Lichuan, Liu Xuefeng, Pei Qingqi, et al. Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing[J]. IEEE Transactions on Services Computing, 2019, 12(5): 786−799

[32] Abdelhamid S, Hassanein H S, Takahara G. Reputation-aware, trajectory-based recruitment of smart vehicles for public sensing[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 19(5): 1387−1400



**Deng Qingyong**, born in 1981. PhD, associate professor, master supervisor. Senior member of IEEE and CCF. His main research interests include IoT, AI, and network security.

**邓清勇**, 1981 年生. 博士，副教授，硕士生导师. IEEE 和 CCF 高级会员. 主要研究方向为物联网、人工智能、网络安全.



**Zuo Qinghua**, born in 2001. Master. His main research interests include crowdsensing and blockchain.

**左清华**, 2001 年生. 硕士. 主要研究方向为群智感知、区块链.



**Li Zhetao**, born in 1980. PhD, professor, PhD supervisor. His main research interests include IoT, crowdsensing, and network security.

**李哲涛**, 1980 年生. 博士，教授，博士生导师. 主要研究方向为物联网、群智感知、网络安全.



**Wang En**, born in 1987. PhD, professor. His main research interests include mobile computing, mobile crowdsensing, and delay tolerant network.

**王　恩**, 1987 年生. 博士，教授. 主要研究方向为移动计算、移动群智感知、延迟容忍网络.



**Guo Bin**, born in 1980. PhD, professor. His main research interests include ubiquitous computing, mobile crowdsensing, and HCI.

**郭　斌**, 1980 年生. 博士，教授. 主要研究方向为泛在计算、移动群智感知、人机交互.