• 量子信息专栏 •

# 区块链环境下用户身份匿名的量子委托计算协议

王育齐[1,2*]，陈 庚[1,2]，钱伟中[3]

(1. 闽南师范大学计算机学院 福建 漳州 363000；2. 数据科学与智能应用福建省高等学校重点实验室 福建 漳州 363000；
3. 电子科技大学信息与软件工程学院 成都 610054)

【摘要】在大数据背景下，数据安全与身份安全同等重要。其中，身份的盲性值得特别关注。为满足量子委托计算对数据与身份盲性的需求，提出一个在区块链环境下进行，能兼顾数据安全与身份安全的匿名量子委托计算协议。协议不依赖可信的第三方，用户能够匿名地参与委托计算协议，无需展示身份信息就可以完成委托的发送与结果的接收。在发送计算委托时，Alice 使用环形网络对身份进行混淆以隐藏发送方。Bob 使用受控量子隐形传态安全且匿名地反馈委托计算结果。另外，协议引入区块链技术协助第三方 Charlie 对用户的支付进行匿名审批。协议使用到的区块链与量子技术基本已实现，因此协议具有较高的可行性。进一步提出了改进协议，用户可以通过比对多委托方的计算结果来实现委托计算结果的可验证。该文提出的协议是一个面向大数据环境的实用协议框架，具有很好的迁移性。

**关 键 词** 区块链； 身份安全； 量子委托计算； 量子隐形传态

**中图分类号** TN918.91 **文献标志码** A doi:10.12178/1001-0548.2022178

# Quantum Delegate Computing Protocol with Anonymous User Identity in Blockchain Scenario

WANG Yuqi[1,2*], CHEN Geng[1,2], and QIAN Weizhong[3]

(1. School of Computer, Minnan Normal University Zhangzhou Fujian 363000;
2. Key Laboratory of Data Science and Intelligence Application, Fujian Province University Zhangzhou Fujian 363000;
3. School of Information and Software Engineering, Universtity of Electronic Science and Technology of China Chengdu 610054)

**Abstract** In the big data scenario, data security is as important as identity security. The identity blindness deserves additional attention. In order to meet the needs of quantum entrusted computing in the blockchain scenario, this paper proposes an anonymous quantum entrusted computing protocol which considering both data security and identity security. In our protocol, the user participates in the delegated computing protocol anonymously, and can send the delegation and receive the results without displaying the identity information. The protocol can achieve the above objectives without a trusted third party. When sending the calculation delegation, Alice uses the ring network to confuse the identity to hide the specific sender. Bob uses controlled quantum teleportation to transmit quantum states safely and anonymously in the process of feeding back the entrusted calculation results. The protocol introduces blockchain technology for Charlie, the third party, to anonymous payment and anonymous approval. The blockchain and quantum technology used in the protocol have been basically realized, so the protocol has high feasibility. Furthermore, we propose an improved protocol for users to verify the results of delegated calculations by comparing the results of multiple principals. The protocol proposed is a practical protocol framework for big data environment and has good portability

**Key words** blockchain; identity security; quantum entrusted computing; quantum teleportation

随着大数据应用的发展，以云端计算为代表的委托计算成为了一个研究热点。委托计算中有两个关键的安全性问题：数据隐私安全与身份隐私安全性[1-2]。

收稿日期：2022－07－21；修回日期：2022－10－15
基金项目：福建省自然科学基金面上项目 (2020J01812)； 四川省 2022 年重点研发计划 (2022YFG0315)；行业职业教育教学指导委员会 2021 科创融教项目 (HBKC217177)
作者简介：王育齐 (1976－)，男，博士，副教授，主要从事量子信息、量子密码和量子机器学习方面的研究.
*通信作者：王育齐，E-mail：wyq1141@mnnu.edu.cn

数据安全是通信范围内的一个核心问题，范围从情报信息与算法到私人通讯和元数据。在经典计算机领域中，可以使用同态加密等方式来保证委托计算中数据的安全性[3-4]。与之相对应的是密码学场景中身份隐私的安全。以移动互联网为例，定位数据，包括物理定位数据与 IP 定位数据等，都是富有特点与价值的信息。尤其是在对敏感数据的委托计算中，仅仅猜测委托方的身份就能够对用户的隐私产生威胁，如关键科研实验中的实验数据或远程医疗中患者的健康参数。已经有一些成熟的经典方法来保护身份安全性，但是仍存在因为所有权和控制权相互分离导致难以进行审计、难以在数据拓展与通信效率之间找到平衡等问题。除此之外，另一个重要问题是，大部分经典的身份保护方法必须依赖一个可信的第三方[5-6]，这在现实大数据场景中是一个极其苛刻的假设。

区块链技术与量子技术的发展，为大数据环境下的数据与身份隐私安全提供了新的解决思路。量子同态加密[7-9](quantum homomorphic encryption, QHE) 能在保证完成计算的基础上，保护数据的安全性；去中心化的区块链机制与配套协议能够摆脱第三方进行安全的匿名交易，其不可篡改性也保证了仲裁机制发挥作用。基于区块链的支付机制已经较为成熟，能够完成支付方与收款方都保持匿名的支付[10-12]。对使用量子技术在区块链中的应用协议，已有较多探索。2019 年，文献 [13] 提出使用量子签名来增强传统区块链的安全性进而实现安全支付，但未能充分应用区块链的特殊性质与功能。文献 [14] 于 2020 年提出量子隐形传态可以实现区块链节点之间的通信，并以此设计出量子区块链模型，但是对区块链的其他功能并未有充分讨论。文献 [15] 在文献 [13] 的工作上展开，于 2021 年提出了一个基于区块链的量子电子支付协议，购物信息与支付信息能够依靠量子技术进行安全传输，协议在效率上有着良好表现。但是，文献 [13] 的协议依赖半可信的第三方。量子技术与区块链技术的优缺点有互补之处[16]，二者的结合能很好解决缺乏可信第三方问题。

本文提出一个基于区块链与量子受控隐形传态的委托计算协议，能够实现委托计算中的匿名支付，兼顾身份安全与数据安全。进一步，改进协议实现了在保持匿名的情况下，通过多方验算对委托计算结果进行正确性验证。协议存在一个第三方协助审批以保证委托的公平与可追溯，但其可以是不可信的。除此之外，协议讨论的是一种面向现实场景中用户与委托方需求的委托计算框架，具有很高的可移植性，并不依赖于某一种特定的量子协议，可以根据具体需求替换协议模块。

本文介绍了协议使用到的相关量子技术与经典技术，并进行了数学描述，提出对协议环境的一些基本假设；正式提出了委托计算协议，并分为 5 个步骤说明协议的详细运行过程；提出一个可验证委托计算结果正确性的改进协议；讨论了委托计算协议的优势、安全性并进行了效率分析；探讨了协议在未来进一步拓展的可能性。

## 1　预备知识

本章将介绍委托协议中使用到的量子技术与经典技术，并且对这些技术进行密码学的描述。另外，将说明对协议使用场景的一些基本假设与技术要求。

### 1.1　量子同态加密

同态加密是现代密码学中的一项关键技术，能够使得 Bob 在无需解密 Alice 数据的情况下，完成对 Alice 数据的特定计算。随着量子技术的发展，研究者也提出了使用于量子计算领域中的同态加密，即为量子同态加密 (quantum homomorphic encryption, QHE)。与经典的同态方案相比，QHE 方案具有完美的安全性[17]。

根据文献 [18-19] 提出的 QHE 定义与框架，QHE 方案可分为两类，即为对称密钥方案与公钥方案，不同之处在于加解密过程中使用的密钥是否相同。QHE 协议包含以下 4 种算法，这里以一$n$位长密文为输入的公钥 QHE 为例进行展示。

1) 密钥生成算法$\mathrm{KeyGen}(1^n)\to(p_k,s_k)$，该算法可以生成两个密钥，公钥$p_k$与私钥$s_k$。

2) 加密算法$\mathrm{Encrypt}_\Delta$，用于计算量子态密文$\rho=\mathrm{Encrypt}_\Delta(p_k,\sigma)$，该算法能够使用公钥加密量子明文$\sigma$。

3) 解密算法$\mathrm{Decrypt}_\Delta$，即$\sigma=\mathrm{Decrypt}_\Delta(sk,\rho)$，该算法使用私钥解密量子密文$\rho$。

4) 同态算法$\mathrm{Evaluate}_\Delta$，即$\widehat{\rho}=\mathrm{Evaluate}_\Delta(T,\rho)$，使得特定算法能够在不解密量子态密文$\rho$的前提下等价于直接作用在量子态明文$\sigma$上，即$T(\sigma)=\mathrm{Decrypt}_\Delta(sk,\widehat{\rho})$。特定算法与一组允许的量子门$\mathcal{F}_\Delta$相关，特定算法只能从该组量子门中进行选择，即$T\in\mathcal{F}_\Delta$。

实现 QHE 的方式有很多，从利用特定酉算子的性质[20]，到使用量子通用电路、量子隐形传态

等[21-24]。本文协议中使用的安全的 QHE 协议需要满足以下要求：1) 是一个公钥方案；2) 协议过程中不需要 Alice 与 Bob 就同态算法进行实时交互；3) 同态加密后的输出与同态过程的输出均是一个完全混合态，方案是计算安全的。

### 1.2 量子隐形传态

作为量子纠缠的一种具体应用，量子隐形传态 (quantum teleportation, QT) 可以实现在不传输真实粒子的情况下重建任意未知量子态[25]。QT 过程中的粒子信息与信道信息被隐藏在粒子的纠缠关系中，量子力学基本原理保证了这些信息的安全性。这一特性能让 Alice 和 Bob 不依赖公钥基础设施而完成未知量子态的传输，这使得真正意义上的匿名传输信息成为可能。量子受控隐形传态 (controlled quantum teleportation, CQT) 指传输双方在第三方的批准与帮助下，完成 QT 的过程。

受控量子隐形传态需要使用一组三量子纠缠态，量子系统状态为：

$$|\xi\rangle=\frac{1}{2}(|000\rangle+|011\rangle+|110\rangle+|101\rangle)$$

对 3 个粒子中的任一个，如果测量结果为$|0\rangle$，则可以推知另外两个粒子测量结果相同；为$|1\rangle$则可以推知另外两个粒子测量结果不同。但是，通过测量单一粒子均无法决定另外两个粒子的准确测量结果。只有至少测量两个粒子，才可以确定量子系统的状态。这种特性实现了一个量子门限函数，可以用于设计第三方受控量子协议。CQT 与 QT 可以传输 $d$ 维量子态，本节中以二值量子态为例来展示 CQT 的完整过程。

为了表示方便，将发送者 Bob 持有的需要发送的粒子记作$|M\rangle=a|0\rangle+b|1\rangle$，目的是实现 Bob 在 Charlie 帮助下将$|M\rangle$传送给 Alice。三方按照以下步骤操作。

1) 将要纠缠的三量子分发至 Alice、Bob 与 Charlie 三方，并分别记作$|\xi\rangle_{\mathrm{A}}$，$|\xi\rangle_{\mathrm{B}}$和$|\xi\rangle_{\mathrm{C}}$。

2) Bob 对粒子 $M$ 与$|\xi\rangle_{\mathrm{B}}$进行一次 Bell 态测量，并将测量结果发送至 Alice 与 Charlie。

3) 如果 Charlie 允许 Bob 完成对 Alice 的传输，则对持有的单粒子$|\xi\rangle_{\mathrm{C}}$进行测量，并将测量结果发送给 Alice。

4) Alice 根据 Bob 与 Charlie 的测量结果，对持有的单粒子$|\xi\rangle_{\mathrm{A}}$作用适当的酉算子$U$，还原未知的量子态$|M\rangle$。其中，酉算子$U$的选择展示在表 1 中，酉算子的推导过程参照文献 [25]。

**表 1 Bob 与 Charlie 测量结果与 Alice 作用酉算子的关系**

| Bob测量结果 | Charlie测量结果 | Alice作用的酉算子 |
|---|---|---|
| $\|\Phi^+\rangle$ | $\|0\rangle$ | $I$ |
| $\|\Phi^+\rangle$ | $\|1\rangle$ | $\sigma_x$ |
| $\|\Phi^+\rangle$ | $\|0\rangle$ | $\sigma_z$ |
| $\|\Phi^+\rangle$ | $\|1\rangle$ | $-\sigma_y$ |
| $\|\Psi^+\rangle$ | $\|0\rangle$ | $\sigma_x$ |
| $\|\Psi^+\rangle$ | $\|1\rangle$ | $I$ |
| $\|\Psi^+\rangle$ | $\|0\rangle$ | $\sigma_y$ |
| $\|\Psi^+\rangle$ | $\|1\rangle$ | $-\sigma_z$ |

表 1 中酉算子结构与 Bell 测量结果表示为：

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

$$\sigma_y=\begin{pmatrix}0&-i\\i&0\end{pmatrix},\ \sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

$$|\Phi^{\pm}\rangle=\frac{i}{\sqrt{2}}(|00\rangle\pm|11\rangle)$$

$$|\Psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|01\rangle|10\rangle)$$

上述过程中粒子与信息的传输展示在图 1 中。

在实际的量子电路中，酉算子体现为量子门，每个有效的量子门由一个单一酉矩阵定义。与之相对的，量子隐形传态则没有 Charlie 的第三方审批过程。2021 年，文献 [26] 完成了高维度 QT 协议的物理实验，验证了 QT 应用于现实场景的可行性。

### 1.3 区块链技术

区块链于 2008 年提出，本质上是一种被称为分布式账本的数据库机制，是互联网与密码学领域中具有广阔应用前景的一项重要技术[27-28]。区块链以其去中心化的管理方式与基于网络节点共识机制的运营方式而享有盛誉。区块链建立在公钥密码系统的基础上，其中公钥及其拓展协议作为身份标识，持有的私钥签名为实体权鉴。本质上，区块链是一个分布式共识存储系统，节点之间通过共识协议就存储的内容达成一致，且每个节点都具有判断新加入的内容是否符合共识的能力。这样的共识机制可以保证分布式网络中的每个节点存储的账本是一致的，只有符合大多数节点共识的内容才被认定是正确的信息，因此区块链能很好地防止内部或外部的攻击者篡改共识内容。

区块链的一个重要应用是智能合约。现代的智能合约是区块链上的一种能够自动执行的协议[29-31]，在满足一定条件时不需要第三方的启动与操作就可

以完成一定任务。智能合约内容及其执行过程对区块链上的所有节点均是透明可见的，每个节点能够观察、记录、验证合约状态。

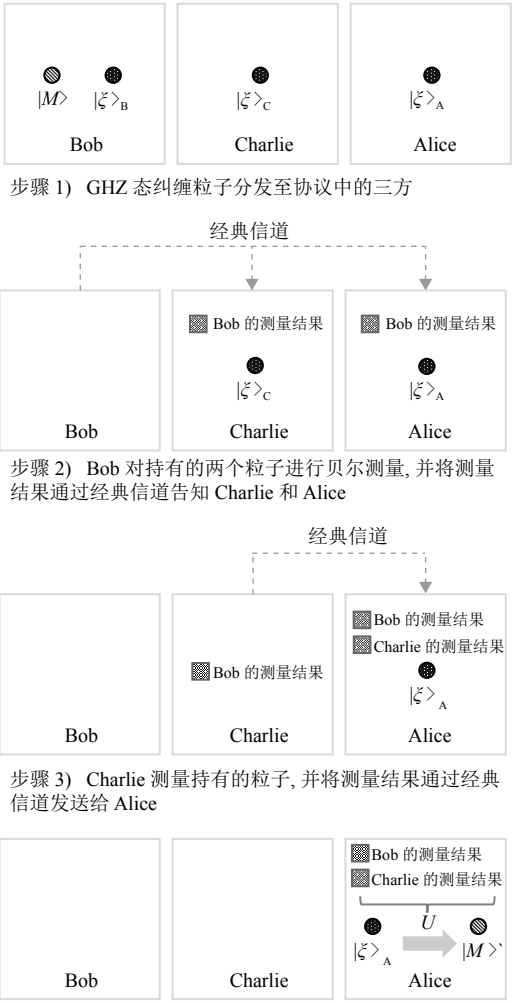


图 1　量子受控隐形传态中粒子与信息的传输过程

共识机制让区块链能够解决密码学场景中的一些关键问题，已有许多研究者为此做出了探索。2016 年，文献 [32] 在区块链上实现了链上和链下的匿名交易，使用了一不受信任的第三方发行匿名代金券，供用户安全兑换比特币。两年后，文献 [33] 将区块链的匿名支付协议引入车联网中，利用区块链在注册与数据维护中的特性，在保护敏感用户信息的同时实现数据共享。该方案是区块链应用于现实场景的一个成功案例。2020 年，文献 [34] 进一步丰富了区块链上的匿名支付协议并进行了详尽的安全性分析。

### 1.4　环签名与地址混淆

环签名是一种面向组的签名，用于隐藏来自组内用户的信息的具体来源[35-37]。本质上，环签名是一个匿名签名系统，能够实现在多个公钥中隐藏用户拥有私钥对应的公钥，进而达到摆脱用户地址与信息之间的一对一关系。作为环签名的一个实际应用，门罗币网络具有类似区块链的网络结构[38-39]。不同之处在于，发件人要进行一笔转账时，该笔资产不会定向的立即打进收款方地址，而是转入一个环状网络上临时设置的安全地址，利用环状路径对发件人的物理地址进行混淆。相对于设置可信第三方的代理支付机制，依靠地址混淆来保护身份隐私更加安全，因为现实场景中不可信的第三方经常与攻击者进行联合攻击来窃取用户的信息。

在环签名机制中，用户数量越多，环形网络越复杂，地址混淆的程度越高，用户身份也就越安全。但同时，随之带来的延误也越严重。混淆过程在提高安全性的同时，也降低了通信过程中的效率。

本文定义的身份安全需要满足以下条件：

1) 任一攻击者无法根据信道上的信息确认当前信息的准确来源，即发送者的准确身份；

2) 任一攻击者无法分辨信道上的两个信息是否来自同一个发送者。

## 2　用户身份匿名的量子委托计算协议

本章将正式提出量子委托计算协议，并提出了协议的一个改进版本。图 2 为协议的完整运行步骤。

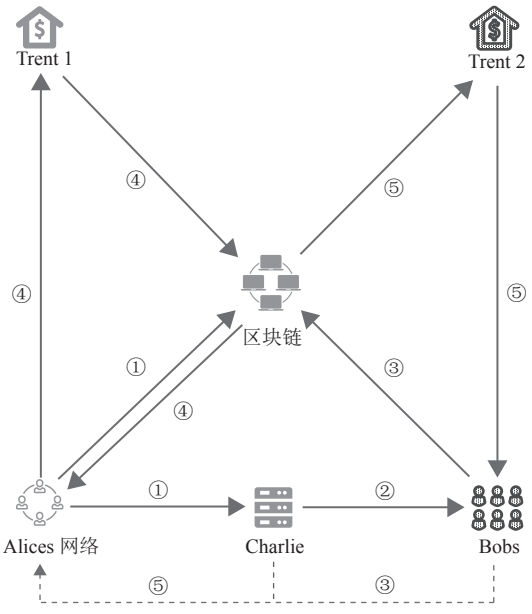


图 2　用户身份匿名的量子委托计算协议

首先说明协议的 5 个参与者。Alice 为委托计

算协议的委托方，一个网络中存在多个 Alice，这些委托方组成一个环形网络。为了简便性，将多个可能参与协议的 Alice 记作 Alices。Bob 为接受委托的一方，现实场景中可能出现多个可承接委托的运营商，与 Alices 类似，将多个 Bob 记作 Bobs。Charlie 是参与协议的不可信第三方，可以试图窥探信道上信息的内容与来源，但是不能够篡改信道上的信息。Trent1 与 Trent2 分别是 Alice 与 Bob 的代理银行。协议的每个参与者都在区块链中注册有账号，分别记作 Account_A，Account_B，Account_C，Account_T1 和 Account_T2。其中，Account_A，Account_B，Account_T1 有在区块链写入信息的权限；Account_C，Account_T2 有在区块链中进行查询检索的权限。

当 Alice 通过协议发布委托时，在 Charlie 的审批下，完成对 Bob 的支付，并获取委托计算的结果。

### 2.1 初始化阶段

协议假设 Alices 网络中用户的数量在一安全区间内浮动，Alice 的数量影响身份混淆的效果，因此直接影响其身份的安全性。全网络内的用户均事先约定好一套量子同态加密算法。本协议是一个面向离散量子位的协议，因此可以选取一位量子位来展示协议运行过程。

1) Alices 事先决定需要哪个 Bobs 来承接自己的委托，并将自己的数据进行同态加密。Alice 执行密钥生成算法$\mathrm{KeyGen}(1)$得到一位公钥$p_k$与私钥$s_k$，并使用$p_k$加密明文量子态数据$|\sigma\rangle$，得到$|\rho\rangle=\mathrm{Encrypt}_{\Delta}(p_k,|\sigma\rangle)$。将委托算法与委托对象等必要信息记作经典信息$\Theta$。

2) Alices 生成三量子纠缠态，记作：

$$|\xi\rangle_{\mathrm{ABC}}=\frac{1}{2}(|000\rangle_{\mathrm{ABC}}+|011\rangle_{\mathrm{ABC}}+|110\rangle_{\mathrm{ABC}}+|101\rangle_{\mathrm{ABC}})$$

3) Alices 生成一个个人信息无关的经典数字假名$\mathrm{Sig}_{\mathrm{A}}$。数字假名可以使用一个含参数的无碰撞哈希函数生成。Alices 每次交易都需要使用不同的数字假名以确保协议的安全性。

初始化结束后，Alices 保有纠缠粒子中的$|\xi\rangle_{\mathrm{A}}$，将量子态信息$\{|\rho\rangle,|\xi\rangle_{\mathrm{BC}}\}$与经典信息$\{\mathrm{Sig}_{\mathrm{A}},\Theta\}$一起作为委托内容打包为$\widehat{\Lambda}$。在现实环境中，存在着保真度降低、信道噪声、测量误差等客观因素，因此在该信息包中还含有纠错码等辅助信息，便于接收方判断信息包的完整程度并进行纠错操作。

### 2.2 发布阶段

1) Alices 将预支付信息$M_{\mathrm{A}}$写入区块链。预支付信息包含许诺支付的酬劳与对象。

2) Alices 将含有委托内容并使用$\mathrm{Sig}_{\mathrm{A}}$签名的信息包通过环形网络进行身份混淆后，上传至 Charlie。

3) Charlie 检查委托信息包$\widehat{\Lambda}$的完整性，并保存其中的纠缠粒子$|\xi\rangle_{\mathrm{C}}$。之后，中间人 Charlie 将$\widehat{\Lambda}$内除该纠缠粒子以外的其他内容发送至对应的 Bobs。

根据安全的 QHE 算法，此时委托的数据对 Charlie 是盲的，由于环形网络的身份混淆，委托包的具体身份也是盲的。在无碰撞哈希函数的保证下，Charlie 也无法从假名中判断多个委托是否来自同一个发送方。

### 2.3 同态加密计算阶段

1) 该阶段主要由 Bobs 内部进行。对应 Bob 接受到信息包后，根据辅助信息先行判断信息包完整程度，并根据纠错码进行纠错。之后，Bob 根据委托信息中的委托算法$\Theta$，以及事先约定好的同态加密算法，开始构造同态算子，即从一组允许的量子门$\mathcal{F}_{\Delta}$中选取$T\in\mathcal{F}_{\Delta}$并拟合出同态算子。之后，Bobs 对$|\rho\rangle$执行算法$\mathrm{Evaluate}_{\Delta}$，可得$|\widehat{\rho}\rangle=\mathrm{Evaluate}_{\Delta}(T,|\rho\rangle)$，即为此次委托计算的结果。

2) Bobs 向区块链写入委托完成信息$M_{\mathrm{B}}$，包含完成委托的时间点与完成声明。

该阶段中，Bobs 与 Alices 在通信上隔离，这要求选用的 QHE 算法不需要双方实时通信。另外，该过程是协议中对效率影响最高的一部分，因此需要选用高效的 QHE 算法。

### 2.4 反馈与支付阶段

1) Bobs 通过受控量子隐形传态将委托计算结果回传给 Alices。Bobs 对$|\widehat{\rho}\rangle$与$|\xi\rangle_{\mathrm{B}}$进行 Bell 测量获得测量结果$|\Phi^{\pm}\rangle$或者$|\Psi^{\pm}\rangle$，并将测量结果使用$\mathrm{Sig}_{\mathrm{A}}$进行签名并发送给 Charlie，Charlie 暂时保留这些信息等待核验与审批。

2) 区块链上的智能合约比对$M_{\mathrm{B}}$与$M_{\mathrm{A}}$在时序和身份上是否符合交易情况，相符则通过区块链通知 Alices 进行转账。由于区块链账户的匿名性，该通知过程对除区块链内的其他用户是匿名的。

3) 根据通知，Alices 需要对委托计算进行支付以获取委托计算结果，该过程由 Alices 委托代理银行 Trent1 进行。Trent1 将支付信息$M_{\mathrm{T1}}$写入区块链。智能合约自动比较$M_{\mathrm{T1}}$与$M_{\mathrm{A}}$在支付金额和对象

上是否相同，相同则完成 Tren1 对 Trent2 的转账。与上一步相似，该过程是匿名完成的。

4) Trent2 通知 Bobs 收到转账。Trent1 再次核验$M_{\mathrm{A}}$的目的在于，检测 Alices的转账金额是否符合发布阶段中 Alices 预支付时设定的金额。

### 2.5　审批阶段

1) 区块链内智能合约比较$M_{\mathrm{T1}}$与$M_{\mathrm{A}}$，若二者相符，根据区块链的不可篡改性，就说明转账完成。Charlie 以此作为审批标准，若审批通过，则对持有的粒子$|\xi\rangle_{\mathrm{C}}$进行测量，并将该测量结果与 Bobs 进行 Bell 测量的结果向 Alices 网络进行广播。

2) 对应的 Alices 收到广播后，根据对应法则选择酉算子作用于自己持有的粒子$|\xi\rangle_{\mathrm{A}}$，并将其还原为$|\hat{\rho}\rangle$。之后，Alice 根据$s_k$进行解密获取委托计算结果，即$T(\sigma)=\mathrm{Decrypt}_{\Delta}(sk,|\hat{\rho}\rangle)$。

至此，协议执行结束。上述过程中粒子与信息的传输过程展示在图 3 中。

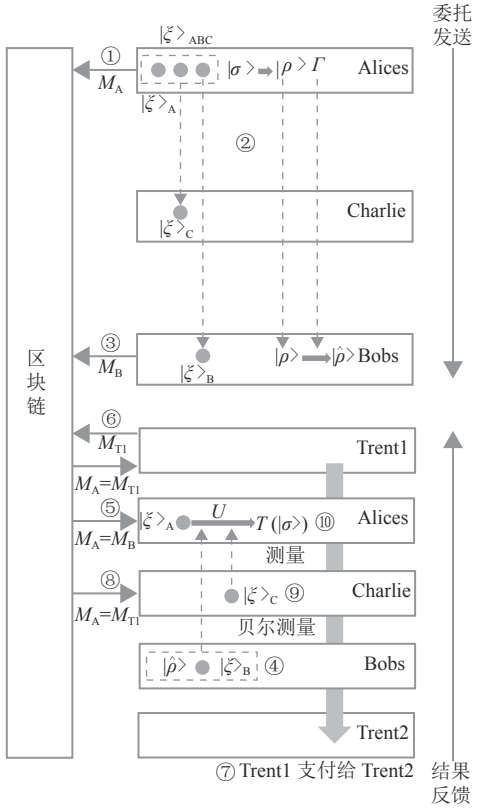


图 3　委托计算协议中粒子与信息的传输过程

### 2.6　协议改进

委托计算的正确性检测是一个尚未解决的问题。已有一些研究尝试对这个问题提出解决方案[40-41]，但存在着算力消耗巨大的问题，短期内无法在现实中实现。与以往跟踪量子计算过程来确保计算的准确性的思路不同，可以将量子计算看作一个黑盒，对量子计算正确性的验证实际上就是对该黑盒输出结果的验证。这为可检验的量子计算提供了新思路。在现实场景中，这种多次计算检验结果可以分摊到多个委托上，即发送多个同样计算内容的委托，并对这些委托计算结果进行比对；当大部分计算方都得到同一结果时，则该结果更可能是正确结果，即区块链中的多数表决机制。反应在数据项上，多个计算结果中的众数 (众数是统计学名词，是一组数据中出现次数最多的数值)，就被用户接受为是正确结果。

该过程类似于区块链中的工作量证明规则，因此改进协议借鉴了相关规则设计出可验证委托结果是否正确的多方委托计算协议。协议认定接受到委托的多个 Bob 中，第一个完成正确结果的节点可以获取报酬。对于一个 Bobs 节点而言，可以作为矿工节点长期在线接受来自网络的委托。与挖矿机制类似，成功处理委托并不意味着一定能取得报酬，还需要经过区块链机制判断是否符合获取报酬的条件。这种抢占式的竞争机制能够促进 Bobs 提升自身算力与计算的准确率，且增加的委托数能够进一步提升 Alices 身份的安全性。

对当前协议进行修改，即可达成上述目的。记 Bobs 中的多个 Bob 为$\mathrm{Bob}_1,\cdots,\mathrm{Bob}_i,\cdots,\mathrm{Bob}_n$。图 4 展示了改进后协议的完整运行过程。

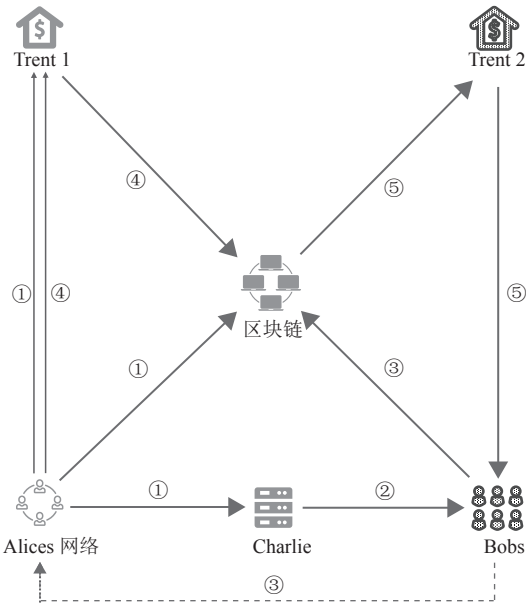


图 4　改进的用户身份匿名的量子委托计算协议

改进协议的完整运行过程如下：

1) Alices 以不同的数字假名$\mathrm{Sig}_{\mathrm{A}_1},\mathrm{Sig}_{\mathrm{A}_2},\cdots,\mathrm{Sig}_{\mathrm{A}_t}$

发出内容相同但是委托方不同的$t$份委托。需要注意的是，$t$由 Alices 指定，且在协议执行的过程中$t$并不公开。同时，Alices 向 Trent1 申请进行一次带验算的委托计算并说明支付金额，之后 Alices 将每一条预支付信息写入区块链。

2) Charlie 将委托分发给对应的 Bobs。

3) Bobs 对委托计算完成同态计算，执行量子隐形传态中的 Bell 测量部分，将测量结果发送给 Charlie，并把自己完成该委托的时间戳等信息写入区块链。Charlie 根据不同的数字假名对 Alices 网络进行广播，Alices 接收测量结果并将自己持有的纠缠粒子转换为 Bobs 的计算结果。

4) 在接收数量足够的验算结果后，根据多数表决机制，Alices 选取验算结果中的众数作为正确的计算结果，并选定第一个给出正确计算结果的$Bob_i$为委托完成者，并作为支付对象告知 Trent1。Trent1 向区块链内写入支付信息。

5) 区块链内的智能合约比对 Trent1 的支付信息与$Bob_i$的委托完成信息，若相符则完成对 Trent2 的转账，Trent2 通知$Bob_i$已经收到报酬。至此，协议执行完毕。

# 3 分析与讨论

本节将对协议进行先进性、安全性与效率分析。协议实现了用户匿名参与委托计算协议，为将量子委托计算应用于现实场景提供了框架性思路。安全性上，由于协议不依赖于特定的算法，协议的安全性受到具体采用的子协议的影响，因此分析针对理想状态。在实际环境中可能会出现信道噪声与误差的情况，为此可以加入经典和量子纠错码提高协议的鲁棒性，并使用无退相干状态等技术提高纠缠量子的保真度。

## 3.1 协议先进性分析

协议使用经典密码学与区块链技术，解决量子领域现阶段尚不能解决的问题，即计算结果正确性的低成本、高效率可验证问题与面向未来应用场景的量子委托计算可支付问题；同时，使用量子同态加密与量子隐形传态等量子技术解决经典计算领域中用户身份隐私与数据安全依赖第三方的经典问题。协议使用到的经典技术已经得到了诸多实践，如经典的虚拟货币系统，具有良好的现实基础；使用到的量子技术也已在实验室环境进行了初步实践，并取得了积极效果[26]。因此，协议具有较高的可行性。

相较于以往的量子委托计算协议，本协议面向大数据环境中的用户隐私与身份问题，在保证委托计算数据安全的基础上，兼顾了用户身份安全，即攻击者无法确定委托的来源，避免委托计算协议中用户身份隐私的泄露。对用户身份的隐藏，也进一步加强了用户在大数据环境中的数据安全。

协议不依赖于特定算法，局部算法并不会影响协议的执行。本文提供了一个开放性的协议框架，可以进行进一步的推广与移植，这为大数据环境下的用户身份隐私保护提供了解决方案。在现实场景中，可以根据算力需求与限制、同态计算类型、用户数量等条件灵活选取优势算法。

## 3.2 协议安全性分析

本节将从数据盲性与身份盲性、身份的不可伪造性、委托的不可否认性等方面对协议的安全性进行分析。

1) 盲性。本协议的盲性包含身份的盲性与数据的盲性。在大数据背景下，不怀好意的各方会好奇用户的物理身份，只需要知道多个数据来源于同一个 Alice 就有可能造成用户在物理层面上的身份泄露。本文提出的协议能在这种背景下，保护用户 Alice 的身份。

Alices 使用信息脱敏且无碰撞的假名上传委托，结合环形路径实现身份混淆，就能使第三方 Charlie 与 Bobs 无法对委托的来源进行溯源。即使 Alices 网络中存在不可信节点与其他攻击者进行联合攻击，也无法确认接收到的委托是否来自一个可追溯的节点。当 Alices 网络中存在大量不可信节点时，才会对单个用户的身份造成威胁。这与区块链中 51% 攻击类似，即攻击者拥有区块链中过半的算力就可以篡改共识，这样的攻击在现实场景中几乎无法实现。在这一阶段，使用经典方法就能很好的保护 Alice 身份。

在 Bobs 进行同态计算后，需要将计算结果回传给 Alices，这是另一个容易泄露身份信息的环节。为此，协议使用了受控量子隐形传态 (controlled quantum teleportation, CQT) 保护此过程。通过 CQT，协议实现了在不知道目标具体身份的情况下，完成一个未知量子态的传递。同时，交易过程中对 Alices 的支付过程进行审批是必要的，而 CQT 也实现了审批过程中的盲化。在审批过程中，Charlie 将测量结果对 Alices 网络进行广播，对此感兴趣的 Alice 可以在无人察觉的情况下获取

推导酉算子的信息。好奇的窃听者可以很容易推断出应当使用的酉算子，但根据未知量子态不可克隆定理和量子纠缠的原理，窃听者不可能获得对应的纠缠粒子，从而无法进行还原未知量子态的操作。与其他量子密码协议不同，CQT 没有隐藏加密方式，而是隐藏了量子密文本身来应对攻击。

除去同态计算本身的数据保护，协议使用的隐形传态也提高了对数据保护的效果。在 Alices 发出多个内容相同的委托时，多个相同的数据确实可能被发送到网络中，根据协议要求这些数据必须使用不同的假名，在无法区分量子态的情况下，攻击者也不可能确认这些拥有不同署名的量子态是否相同。因此，协议在用户数据和用户身份上具有盲属性。

2) 不可伪造性。考虑一个来自网络内部的节点企图通过伪造身份获取同态计算数据的情况。假设一个攻击者加入到 Alices 网络内并截获了 Alices 委托的签名，在协议其余部分声称自己是 Alices 企图获取任何有用数据。在发布阶段，攻击者可以直接截获 Alice 的委托请求，但是因为同态加密无法获得内部数据，攻击并没有意义。在收取委托结果的阶段，攻击者因为没有办法获取始终由 Alice 持有的纠缠量子，也无法进行任何有意义的攻击，只能够降低 Alice 委托的效率。

在支付阶段，一个不诚实的 Bobs 可以试图通过伪造转账证明来骗取代理银行的转账。在区块链的保护下，这种攻击需要伪造 Bobs 账户并欺骗区块链的共识机制，以现有技术水平是不可能达到的。因此，协议具有不可伪造性。

3) 不可否认性。 Alices 在协议中可以尝试不支付酬劳或者少支付酬劳而获得委托计算结果。在协议的初始化阶段，Alices 就必须在区块链中写入与委托相关的信息，可以看作是 Alices 在一次完整协议过程中进行注册。在此之后，所有交易都以此时写入区块链的$M_{\mathrm{A}}$为准。在原始协议中，Charlie 与代理银行 Trent1 需要就交易细节在区块链中进行两次比对，只有当许诺支付酬劳$M_{\mathrm{A}}$，Bobs 完成任务后的索要的酬劳$M_{\mathrm{B}}$，实际支付酬劳$M_{\mathrm{T1}}$，三者一致时才能完成支付，Alices 才可通过 Charlie 的审批获取委托计算的结果。因为使用了区块链，上述信息均不可否认。

在改进协议中，审批 Alices 的权限被转移到 Alices 的代理银行 Trent1 上。如果 Alices 未按照协议向计算正确的一方支付酬劳，那么 Trent1 可以拒绝 Alices 进行下一次委托计算。因此，本协议具有不可否认性。

### 3.3　协议效率分析

首先分析协议在理想环境下的运行效率。该部分的效率损耗由两方面组成，一个是信道网络的效率，一个是量子同态加密与审批过程的效率。之后，将进一步分析现实场景中各种因素对协议效率的影响。

1) 信道网络效率。信道网络的效率可分为两部分，Alices 在环形网络上进行身份混淆时的效率与信道上传输委托的效率。Alices 网络内较为复杂的传播路径是为了隐藏身份信息的必要操作，传播路径越复杂，混淆效果越好，但是需要找到一个效率与安全的平衡点。为此可以设计一个量子门限算法，在经过特定数量的混淆后就对委托进行上传。

在信道传播上，因为引入了隐形传态，大大降低了信道压力并提升了传播速度。隐形传态是瞬间完成的，在信道上传递的是纠缠量子与经典信息。这样的设置能够提升网络的平均委托交易数量，提升了网络后续的可拓展性。因此，信道网络上唯一延迟来自 Charlie 转发委托的时间。

进一步，在该网络中也可以考虑在委托上传阶段也使用量子隐形传态，从而摆脱第三方 Charlie，进一步减少量子数据在信道上的流动。这样的结果是，所有节点只需要传递纠缠量子和少量经典信息即可。因此，该协议在应用于更加复杂的场景上具有潜力。之外，本协议也可以看作是对文献 [14] 基于量子隐形传态的量子区块链协议的进一步探索。

2) 同态算法与审批效率。量子同态加密的效率取决与所选用的 QHE 算法。为提升效率并满足同态过程无需交互的条件，协议很可能不适用于量子全同态加密算法。如何在保持匿名的情况下，完成同态过程中可能出现的 Alices 与 Bobs 的通信，是协议尚未解决的问题。

审批过程中的主要效率损耗来自 Alices 的支付过程，若用户拖延过长时间才进行支付，Alices 和 Charlie 都需要较长时间存储纠缠量子态。为此，可以设计一个鼓励 Alices 快速支付的机制，如将支付权限交由区块链内智能合约自动快速执行，或设置量子存储时间费用等。

3) 现实环境中的协议效率。现实场景中，量子通信不可避免的存在保真度降低、信道噪声、测量

误差等问题，造成协议失败等后果。本文提出协议的效率在现实环境中必然会有所降低，但并不会影响协议的正常进行。

一方面，协议在 Alice 发出的信息包中附加上了对应的校验码与纠错码，协议中其他方接收到对应信息包后可以根据校验码先行判断信息包的完整程度并根据纠错码对信息进行修正。

另一方面，协议结合了经典区块链技术，协议本身是容错的，对量子错误具有较高的鲁棒性。在一对一 QHE 协议中，量子通信错误往往意味着本轮协议无法获得正确的结果。但是在本协议的一对多委托模式中，若在 Bobs 中有足够多的节点接收委托，在一轮协议中用户可以以高概率获取多个计算结果并经过比对获取正确的计算结果。现实场景中，这些措施会在一定程度上降低协议效率，但是能使协议获得对真实有损有噪信道、非完美操作和测量误差的良好抗性。

## 4 结 束 语

本文针对大数据环境下对身份安全的需求，进行了面向现实场景需求的应用研究，提出了一种量子委托计算的协议。协议兼顾了数据的隐私性与身份的隐私性，且不需要可信的第三方。

协议在委托发出阶段使用了环形路径对委托发出者的身份进行隐藏，确保任一方无法得知发送方的具体物理身份。之后，协议使用受控量子隐形传态实现了委托计算结果的反馈，保持用户身份匿名的同时也提高了信道的效率。这个过程中，第三方可以对传输过程进行盲审批。协议依靠区块链技术实现匿名支付并保证委托报酬的一致性，维护协议的公平性与健壮性。

协议并不限定于某一种量子协议，因此具有很高的可迁移性。结合已较为成熟的经典区块链技术与在实验室环境下现已实现的量子技术，协议具有较高的实用性。协议框架不仅可以拓展到大数据环境中用户隐私数据的保护，还可以拓展到大数据场景下需要用户匿名参与的其他应用，具有良好的应用前景。

## 参 考 文 献

[1] SAGIROGLU S, SINANC D. Big data: A review[C]//2013 International Conference on Collaboration Technologies and Systems (CTS). [S.l.]: IEEE, 2013: 42-47.

[2] FANG W, WEN X Z, ZHENG Y, et al. A survey of big data security and privacy preserving[J]. IETE Technical Review, 2017, 34(5): 544-560.

[3] YI X, PAULET R, BERTINO E. Homomorphic encryption[M]//Homomorphic Encryption and Applications. Cham: Springer, 2014: 27-46.

[4] ACAR A, AKSU H, ULUAGAC A S, et al. A survey on homomorphic encryption schemes: Theory and implementation[J]. ACM Computing Surveys (Csur), 2018, 51(4): 1-35.

[5] THOTA C, MANOGARAN G, LOPEZ D, et al. Big data security framework for distributed cloud data centers[M]// Cybersecurity Breaches and Issues Surrounding Online Threat Protection. [S.l.]: IGI global, 2017: 288-310.

[6] KUMAR V, AHMAD M, KUMAR P. An identity-based authentication framework for big data security[C]// Proceedings of 2nd International Conference on Communication, Computing and Networking. Singapore: Springer, 2019: 63-71.

[7] BARZ S, KASHEFI E, BROADBENT A, et al. Demonstration of blind quantum computing[J]. Science, 2012, 335(6066): 303-308.

[8] BROADBENT A, FITZSIMONS J, KASHEFI E. Universal blind quantum computation[C]//2009 50th Annual IEEE Symposium on Foundations of Computer Science. [S.l.]: IEEE, 2009: 517-526.

[9] FITZSIMONS J F. Private quantum computation: An introduction to blind quantum computing and related protocols[J]. NPJ Quantum Information, 2017, 3(1): 1-11.

[10] KHALIL R, GERVAIS A. Revive: Rebalancing off-blockchain payment networks[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. [S.l.]: ACM, 2017: 439-453.

[11] ZHANG Y, DENG R H, LIU X, et al. Blockchain based efficient and robust fair payment for outsourcing services in cloud computing[J]. Information Sciences, 2018, 462: 262-277.

[12] CUI H, WAN Z, WEI X, et al. Pay as you decrypt: Decryption outsourcing for functional encryption using blockchain[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 3227-3238.

[13] ZHANG J L, HU M S, JIA Z J, et al. A novel E-payment protocol implented by blockchain and quantum signature[J]. International Journal of Theoretical Physics, 2019, 58(4): 1315-1325.

[14] SINGH S, RAJPUT N K, RATHI V K, et al. Securing blockchain transactions using quantum teleportation and quantum digital signature [EB/OL]. (2020-06-08). http://doi.org/10.1007/s11063-020-10272-1.

[15] GOU X, SHI R, GAO W, et al. A novel quantum E-payment protocol based on blockchain[J]. Quantum Information Processing, 2021, 20(5): 1-17.

[16] EDWARDS M, MASHATAN A, GHOSE S. A review of quantum and hybrid quantum/classical blockchain protocols[J]. Quantum Information Processing, 2020, 19(6): 1-22.

[17] LIANG M. Symmetric quantum fully homomorphic encryption with perfect security[J]. Quantum Information Processing, 2013, 12(12): 3675-3687.

[18] LIANG M, YANG L. Quantum-message-oriented public-key encryption scheme beyond computational hypothesis[C]//Quantum Optics II. [S.l.]: International Society for Optics and Photonics, 2012: 8440.
[19] LIANG M. Quantum fully homomorphic encryption scheme based on universal quantum circuit[J]. Quantum Information Processing, 2015, 14(8): 2749-2759.
[20] ZHANG Y, SHANG T, LIU J. A multi-valued quantum fully homomorphic encryption scheme[J]. Quantum Information Processing, 2021, 20(3): 1-25.
[21] SUN X, WANG T, SUN Z, et al. An efficient quantum somewhat homomorphic symmetric searchable encryption[J]. International Journal of Theoretical Physics, 2017, 56(4): 1335-1345.
[22] WANG Y, SHE K, LUO Q, et al. Symmetric weak ternary quantum homomorphic encryption schemes[J]. Modern Physics Letters B, 2016, 30(7): 1650076.
[23] LIANG M. Teleportation-based quantum homomorphic encryption scheme with quasi-compactness and perfect security[J]. Quantum Information Processing, 2020, 19(1): 1-32.
[24] CHEN R, SHANG T, LIU J. IND-secure quantum symmetric encryption based on point obfuscation[J]. Quantum Information Processing, 2019, 18(6): 1-16.
[25] TING G, FENG L Y, ZHI X W. Controlled quantum teleportation and secure direct communication[J]. Chinese Physics, 2005, 14(5): 893.
[26] HU X M, ZHANG C, LIU B H, et al. Experimental high-dimensional quantum teleportation[J]. Physical Review Letters, 2020, 125(23): 230501.
[27] NOFER M, GOMBER P, HINZ O, et al. Blockchain[J]. Business & Information Systems Engineering, 2017, 59(3): 183-187.
[28] YLI-HUUMO J, KO D, CHOI S, et al. Where is current research on blockchain technology: A systematic review[J]. PloS One, 2016, 11(10): e0163477.
[29] WANG S, YUAN Y, WANG X, et al. An overview of smart contract: Architecture, applications, and future trends[C]//2018 IEEE Intelligent Vehicles Symposium (IV). [S.l.]: IEEE, 2018: 108-113.
[30] ZOU W, LO D, KOCHHAR P S, et al. Smart contract development: Challenges and opportunities[J]. IEEE Transactions on Software Engineering, 2019, 47(10): 2084-2106.
[31] BODKHE U, TANWAR S, PAREKH K, et al. Blockchain for industry 4.0: A comprehensive review[J]. IEEE Access, 2020, 8: 79764-79800.
[32] HEILMAN E, BALDIMTSI F, GOLDBERG S. Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions[C]//International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2016: 43-60.
[33] GAO F, ZHU L, SHEN M, et al. A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks[J]. IEEE Network, 2018, 32(6): 184-192.
[34] LIN C, HE D, HUANG X, et al. DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 2440-2452.
[35] ZHANG F, KIM K. ID-based blind signature and ring signature from pairings[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Heidelberg: Springer, 2002: 533-547.
[36] CHOW S S M, YIU S M, HUI L C K. Efficient identity based ring signature[C]//International Conference on Applied Cryptography and Network Security. Berlin, Heidelberg: Springer, 2005: 499-512.
[37] AWASTHI A K, LAL S. ID-based ring signature and proxy ring signature schemes from bilinear pairings [EB/OL]. (2005-04-23). https://arxiv.org/abs/cs/0504097.
[38] MöSER M, SOSKA K, HEILMAN E, et al. An empirical analysis of traceability in the monero blockchain[EB/OL]. (2018-04-23). https://arxiv.org/abs/1704.04299.
[39] SUN S F, AU M H, LIU J K, et al. Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero[C]//European Symposium on Research in Computer Security. Cham: Springer, 2017: 456-474.
[40] ALAGIC G, DULEK Y, SCHAFFNER C, et al. Quantum fully homomorphic encryption with verification[C]// International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer, 2017: 438-467.
[41] MAHADEV U. Classical verification of quantum computations[C]//2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS). [S.l.]: IEEE, 2018: 259-267.

编　辑　蒋　晓