基于信任评估的量子区块链网络匿名选举协议*

郑 涛，昌 燕，张仕斌†
（成都信息工程大学 网络空间安全学院，成都 610225）

摘 要：为了在量子通信网络中实现效率更高且具备信任评估功能的匿名选举协议，引入了区块链技术与节点信任评估模型。区块链技术架构具有去中心化、去信任、匿名性、防窜改等优势，节点信任评估模型在选举协议开始前完成任意两节点间的身份可信评估，使选举协议更加高效且可信。协议安全模型分析与对比结果表明，与现有协议相比该协议安全性能更好，且具有更好的匿名性、不可窜改性、可验证性等优点，在现有的技术条件下也更容易实现。

关键词：区块链；量子通信网络；匿名选举；信任评估
中图分类号：TP393.04 **文献标志码**：A **文章编号**：1001-3695(2020)12-037-3708-04
doi:10.19734/j.issn.1001-3695.2019.08.0564

Quantum blockchain network anonymous election protocol based on trust evaluation

Zheng Tao, Chang Yan, Zhang Shibin†
(*School of Cybersecurity, Chengdu University of Information Technology, Chengdu* 610225, *China*)

Abstract: In order to implement an anonymous voting protocol with higher efficiency and trust evaluation function in quantum communication network, this paper introduced block chain technology and node trust evaluation model. Blockchain technology architecture had the advantages of de-centralization, de-trust, anonymity and tamper-proof. Node trust evaluation model completed the identity trustworthiness evaluation between any two nodes before the election protocol starts, which made the election protocol more efficient and credible. The analysis and comparison of protocol security model show that the proposed protocol has better security performance, better anonymity, non-tamper modification, verifiability than the existing protocols, and it is easier to be implemented under the existing technical conditions.

Key words: blockchain; quantum communication network; anonymous election; trust evaluation

0 引言

近年来，以比特币为代表的数字加密货币体系发展十分迅速[1]，作为数字加密货币的核心支撑技术，区块链技术[2,3]被学者们广泛关注。区块链技术可以有效解决传统数字货币面临的拜占庭将军问题和双重支付问题两大难题。区块链技术运用数据加密和时间戳技术，严格保证数据安全，同时创造性地加入了分布式共识和经济激励等手段，在节点无须互相信任的分布式网络中实现了去中心化信用的点对点交易、协调和协作，从而能有效解决中心化机构存在的高成本、低效率，以及数据安全性低等问题。自 2008 年中本聪(Satoshi Nakamoto)[4]发表的奠基性论文以来，学者们开始研究将区块链技术应用在电子商务、计算机科学、数字医疗、环境科学、数据存储等领域[5~7]。可以预见，区块链作为一种解决实体间信任问题的技术，未来将会被应用到各行各业中。

随着量子制备技术的发展，学者们开始研究使用量子技术构建一个可以使通信方安全地完成信息交换、信息传输、直接对话等操作的量子通信网络(quantum communication network, QCN)。1984 年，Bennett 等人[8]提出了第一个量子密钥分发协议(quantum key distribution, QKD)，即 BB84 协议。科研工作者们提出了大量基于 QKD 的量子密码应用协议，如量子安全直接通信协议(quantum secure direct communication, QSDC)[9,10]、量子隐私查询协议(quantum private query, QPQ)[11,12]、量子签名协议(quantum signature, QS)[13,14]等，这些应用于各种实际场景的量子协议将成为量子通信网络的重要组成部分。随着对量子通信网络构建研究的深入，如何在网络中实现节点的信任评估成为了研究热点[15]。现有的区块链技术使用了基于数字签名技术，其安全保障大多基于经典数学难题的计算复杂度。随着量子计算机的快速发展，其强大的计算能力也将使得现有的区块链技术变得不再安全。2017 年，俄罗斯学者提出了一种基于量子密钥技术的区块链网络[16]，通过利用具有绝对安全特性的量子密钥取代现有区块链技术中的数字签名，构建了一种具有绝对安全的分布式区块链网络。随后出现了基于量子区块链网络的各类应用方案，其中匿名投票方案是研究热点。匿名投票方案应该满足如下特点：a)匿名性，只有投票者本人知道他作出的投票选择；b)不可窜改性，投票提交后，任何人都不能修改投票信息；c)可验证性，每个投票人可以验证自己的选票是否被正确统计。传统的匿名投票方案很难实现全部的要求，2015 年，Zhao 等人[17]提出了第一个基于区块链的匿名投票方案，该方案引入零知识证明和比特承诺协议，实现了 n 位投票人对两个候选者匿名投票情况的统计。2018 年，Tian 等人[18]在此基础上进行了扩展，将候选者人数拓展到了(key_{min}, key_{max})，并给出了更为简单高效的投票统计策略。2019 年，Sun 等人[19,20]提出了基于量子区块链的匿名投票方

收稿日期：2019-08-09；**修回日期**：2019-09-22 **基金项目**：国家重点研发计划资助项目(2017YFB0802302)；国家自然科学基金资助项目(61572086,61402058)；四川省高校科研创新团队项目(17TD0009)；四川省学术和技术带头人培养支持经费资助项目(2016120080102643)；四川省应用基础项目(2017JY0168)；四川省重点研发计划项目(2018TJPT0012)；四川省科技支撑计划项目(2016FZ0112,2018GZ0204)；四川省重点研发项目(2018GZ0232)；四川省科技成果转化平台(2018CC0060)

作者简介：郑涛(1994-)，四川达州人，硕士，主要研究方向为量子安全通信；昌燕(1979-)，女(蒙古族)，内蒙古人，教授，博士，主要研究方向为量子密码、信息安全；张仕斌(1971-)，男(通信作者)，重庆丰都人，教授，博士，主要研究方向为网络安全、量子安全通信(cuitzsb@cuit.edu.cn).

案,该方案采用 Tian 等人的基础架构,并加强了对匿名投票方案的匿名性、可追溯性等保障。然而,以上方案都不是在一个量子通信网络体系下应用的方案,即忽略了对投票人身份可信度的检查。再者,区块链发展至今,为了更满足实际需求,去中心化思想已经演变成多中心化思想。多中心化是由多个中心节点组成的平等网络,对节点的参与和退出有一定程度的限制。这就要求在量子通信网络中必须对投票人身份进行验证。

本文提出了一种基于量子区块链网络的匿名投票协议,该协议可以对投票人身份可信度进行评估,在现有条件下易于实现;并且满足匿名投票协议的特点。在现代密码协议中,协议的匿名性在不同的应用场景有不同的含义[21,22],本文对匿名性定义为:a)除了投票人外,任何机构或攻击者都无法通过选票信息倒推判断出这张选票的拥有人;b)选票一经投出,任何人都无法进行修改;c)选票产生后,可以对选票或投票人的合法性进行验证。

1　准备知识

1.1　量子节点的信任评估模型

去中心化量子通信网络中,节点与节点之间的通信必须具备一个用于节点身份可信度的评估机制。量子态可以表述为 $|\phi\rangle=\alpha|0\rangle+\beta|1\rangle$,其中 $|\alpha|^2+|\beta|^2=1$,且 α 和 β 描述了量子态被测量为 $|0\rangle$ 态和 $|1\rangle$ 态的概率值。α 和 β 可以描述单粒子节点的一些不确定性,在可信网络中,本文引入直觉模糊理论中的隶属度与非隶属度来描述这种不确定程度,称为信任因子。每个量子态都具有多位不同的信任因子。由于实际应用场景中,不同的信任因子具有不同程度的重要性,本文引入权重系数 t_j 来定量描述不同信任因子的重要值。对于节点 k,定义其第 j 位信任因子值为 $|T\rangle_k=\sum_{j=1}^{m}t_j(\cos\theta_j|0\rangle+\sin\theta_j|1\rangle)$。其中 $\cos\theta_j$ 描述节点 k 隶属与第 j 位信任因子(隶属度),$\sin\theta_j$ 描述节点 k 非隶属与第 j 位信任因子(非隶属度),且 $\sum_{j=1}^{m}t_j=1$。至此,基于直觉模糊理论的量子节点的信任评估模型已经建立。

1.2　量子比特承诺

密码学中的比特承诺问题可简单描述为:A 想说服 B 完成某件事情,由于特殊原因 A 不能告诉这件事情的具体信息,B 在做此事前想要确保事件的真实性,且不会受到 A 的欺骗,为保证事件的可靠性和公平性,可以使用密码算法的方式实现。密码学语言描述为:比特承诺方案允许 Alice 向 Bob 发送一个证据表明她拥有一个秘密比特 $x\in\{0,1\}$,Bob 收到的证据不能获得 x 的具体信息,这个过程称为承诺阶段;必要时,Bob 请求 Alice 公示 x 的值,但是在身份检测没通过的情况下,不会公开 $1-x$ 的信息。此阶段称为公示阶段。以量子态实现的比特承诺称为量子比特承诺协议,并且已经被证明不可能具有绝对的安全性,但是学者们研究出了很多在一定条件下安全的量子比特承诺协议:将消息量子化,并在测量基、线性码等的选择上做了一定限制,使得发送者 Alice 不能完成通用量子测量,这样的方案称为有条件安全量子比特承诺协议。

1.3　量子拜占庭协议

在分布式计算中,即使有些进程已经失败,整体的计算流程依然可以进行下去。这就要求所有正常节点在遭遇干扰时能快速达成一个一致性协议。这种解决容错问题的一致性协议称为拜占庭将军协议。在经典的拜占庭问题中,能达成协议的前提是要求故障节点(叛徒数量)最大值为 $t=\lfloor(n-1)/3\rfloor$(n 为节点总数)。研究表明,解决拜占庭问题可以简化为解决生成和安全分发数字列表的问题。而生成和安全分发正是以量子态为载体的量子密码学最具有核心优势的特点。区块链技术要求系统采用时效性强,安全性高的一致性算法,基于量子密钥分发的量子拜占庭协议(quantum Byzantine agreement,QBA)能满足上述所有要求。迄今为止,学者们提出了许多高效实用的 QBA 协议。在本文中采用 Sun 等人[20]提出的诚实量子拜占庭协议,该协议表明当诚实节点数量范围在 $0<p<(m-2)/m$(m 是节点总数)范围时,区块链系统仍能达成一致性协议。传统的诚实拜占庭算法的有效范围是 $0<p<1$,因此 Sun 等人的协议效率更好。

2　协议描述

假设有 n 位投票人 P_i($i=1,\cdots,n$)需要对两位候选者 Alice和 Bob 进行投票。每个投票人 P_i 都有选票 O_i,其中 $O_i=0$ 代表支持 Alice,$O_i=1$ 代表支持 Bob。本协议过程基于文献[17~19]的基本框架,同样分为投票承诺和选票统计两个阶段。本文加入了节点间身份评估过程,使得投票方案更加贴近现实应用场景。

2.1　投票承诺

a)建立 $n\times n$ 矩阵。投票人 P_i 生成 n 位正整数 $X_{i,1},\cdots,X_{i,n}$ 作为矩阵的第 i 行数据。根据文献[17],生成的数据应当满足如下关系:$\sum_{j=1}^{n}X_{i,j}\equiv0(\bmod n+1)$。

b)完成身份评估。在多中心化节点下的区块链网络中,节点间需要完成身份评估。基于笔者团队的前期研究成果[15],借助量子隐形传输技术(quantum teleportation,QT)可以完成评估。具体流程为

(a)投票人 P_i 借助量子安全直接通信技术,发送通信请求给多中心节点 TP,该请求的内容包含 P_i 的信任因子,请求建立评估对象 P_j 的信息等。

(b)TP 将 P_i 发来的信任因子与 TP 存储的 P_i 原始信任因子对比,通过检测后 TP 通知 P_j 做好通信准备并制备 P_i 的信任因子量子态 $|T\rangle_{P_i}=\sum_{j=1}^{m}t_j(\cos\theta_j|0\rangle+\sin\theta_j|1\rangle)=\cos\gamma_i|0\rangle+\sin\gamma_i|1\rangle$。$TP$ 制备一对 Bell 纠缠态粒子 $|\psi\rangle_{TA}=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{TA}$ 并将 A 粒子发给 P_j,保留 T 粒子。

(c)此时 $|T\rangle_{P_i}$ 和 $|\psi\rangle_{TA}$ 形成三粒子张量空间,即有:

$$|\psi\rangle_{P_iTA}=|T\rangle_{P_i}\otimes|\psi\rangle_{TA}=(\cos\gamma_i|0\rangle+\sin\gamma_i|1\rangle)\otimes\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{TA}=\frac{1}{2}\begin{bmatrix}|\phi^+\rangle_{TA}(\cos\gamma_i|0\rangle+\sin\gamma_i|1\rangle)+\\|\phi^-\rangle_{TA}(\cos\gamma_i|0\rangle+\sin\gamma_i|1\rangle)+\\|\psi^+\rangle_{TA}(\cos\gamma_i|1\rangle+\sin\gamma_i|0\rangle)+\\|\psi^-\rangle_{TA}(\cos\gamma_i|1\rangle+\sin\gamma_i|0\rangle)\end{bmatrix}$$

其中:$|\phi^+\rangle_{TA}$、$|\phi^-\rangle_{TA}$、$|\psi^+\rangle_{TA}$、$|\psi^-\rangle_{TA}$ 是四种 Bell 纠缠态。TP 对复合空间中的 TA 二粒子做 Bell 测量,并将测量结果编码后发送给 P_j。编码规则为 00,01,10,11 分别代表 TA 粒子的测量结果为 $|\phi^+\rangle_{TA}$,$|\phi^-\rangle_{TA}$,$|\psi^+\rangle_{TA}$,$|\psi^-\rangle_{TA}$。

(d)P_j 根据 TP 发送的编码信息,对手中的 A 粒子执行对应的 Pauli 变换,即可恢复出代表 P_i 信任因子的量子态 $|T\rangle_{P_i}$。具体的转换规则如表 1 所示。P_j 计算此量子态装载的信任因子值,就可以判断通信请求方是否为 P_i,完成身份评估。多次执行就可以完成所有节点间的信任评估流程。

c)获取矩阵的第 i 列的值。经过 a)和 b),每个投票人 P_i 完成了对其他投票人的身份信任评估,并得知 $n\times n$ 矩阵中第 i 行数据 $X_{i,1},\cdots,X_{i,n}$。P_i 借助量子安全直接通信技术将每个 $X_{i,j}$ 发送给 P_j。P_i 此时得知 $n\times n$ 矩阵中第 i 列数据 $X_{1,i},\cdots,X_{n,i}$。每个投票人 P_i 计算投票的承诺值:$O_i^c\equiv O_i+\sum_{j=1}^{n}X_{j,i}(\bmod n+1)$,$P_i$ 通过量子比特承诺协议将 O_i^c 承诺给区块链中每个矿工节点。

表 1 节点 P_j 的转换规则

Tab. 1 Operation rules of node P_j

TP 测量结果	*A* 粒子塌缩结果	P_j 执行的泡利变换
$\|\phi^+\rangle_{TA}$	$\cos\gamma_i\|0\rangle+\sin\gamma_i\|1\rangle$	$\boldsymbol{I}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$
$\|\phi^-\rangle_{TA}$	$\cos\gamma_i\|0\rangle+\sin\gamma_i\|1\rangle$	$\boldsymbol{Z}=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$
$\|\psi^+\rangle_{TA}$	$\cos\gamma_i\|1\rangle+\sin\gamma_i\|0\rangle$	$\boldsymbol{X}=\begin{pmatrix}0&1\\1&0\end{pmatrix}$
$\|\psi^-\rangle_{TA}$	$\cos\gamma_i\|1\rangle+\sin\gamma_i\|0\rangle$	$\boldsymbol{U}=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$

2.2 选票统计

a)一致性计算。P_i 将 O_i^c 的一些信息公布给区块链中所有矿工节点。所有矿工节点运行一个量子诚实拜占庭协议[20]将所有的投票承诺完成一致性计算。

b)选票计算。通过计算 $\sum_{i=1}^{n}O_i^c=\sum_{i=1}^{n}(O_i+\sum_{j=1}^{n}X_{j,i})=\sum_{i=1}^{n}O_i \pmod{n+1}$ 可以计算出所有得票为 1(候选者 Bob 的得票总数)。例如:三个投票人的匿名投票内容为 $O_1=1,O_2=1,O_3=0$。三人共享的 3×3 矩阵表示为 $\begin{pmatrix}2&0&2\\1&1&2\\3&0&1\end{pmatrix}$,分别计算三人投票的承诺值为 $O_1^c=1+(2+1+3)=7\equiv3\pmod4$ $O_2^c=1+(0+1+0)=2\equiv2\pmod4$ $O_3^c=0+(2+2+1)=5\equiv1\pmod4$;则 $O_1^c+O_2^c+O_3^c=3+2+1\equiv2\pmod4$,且 $O_1+O_2+O_3=2$,即候选人 Bob 得票数为 2,可推知 Alice 得票数为 1。

3 协议安全模型建立与分析

分析协议过程,经过投票承诺和选票统计两个阶段后,通过简单计算可以得到 Alice 和 Bob 两位候选人的得票总数。在投票承诺阶段,投票人完成了矩阵建立、节点的身份评估和承诺选票给区块链节点的过程。分析可知,身份评估步骤的安全性主要由量子隐形传态(quantum teleportation)技术保障。选票承诺步骤的安全性由量子比特承诺协议保障。在选票统计阶段,一致性计算步骤的安全性由量子拜占庭协议保障。

综上所述,本协议的安全模型主要讨论攻击者能否通过某些非法操作来破坏协议的匿名性;攻击者或者投票人能否在选票产生后对选票信息作出修改;选票产生后,如果发生纠纷,能否对选票信息和投票人身份作出可信的验证。针对上述安全问题下面给出详细的分析过程。

3.1 匿名性

根据协议过程可知,投票人通过量子安全通信技术将每个 $X_{i,j}$ 发送给 P_j。点对点的两方量子安全直接通信技术保证了每个投票人 P_i 只知道 $n\times n$ 矩阵中第 i 行的全部数据(P_i 生成的 $X_{i,1},\cdots,X_{i,n}$)以及矩阵的第 i 列的值 $X_{1,i},\cdots,X_{n,i}$。这便严格保证了 $n\times n$ 矩阵只有部分信息对 P_i 可见。且所有投票人发送给矿工节点的都是投票的承诺值 O_i^c,原始的选举内容严格保密。

3.2 不可窜改性

量子区块链网络的建立需要对每个节点进行身份认证,基于量子密钥分发技术的认证过程具有绝对安全性。本文中,投票人在发送矩阵数据前,需要完成节点间的身份信任评估,这进一步保证了投票信息的不可窜改性。根据量子比特承诺协议,投票人 P_i 一旦计算并公布了投票的承诺值 O_i^c,P_i 就不得对其进行修改,否则所有矿工节点无法达成一致性,协议随即中止。

3.3 可验证性

协议的可验证性分为选举信息可验证性和选举人身份可验证性。由于 $n\times n$ 矩阵每一行的数据分别由 n 位选举人生成,且计算投票承诺的数据包含对应列的值,每个投票人在统计时都可以计算自己的投票承诺 O_i^c 的真实性和有效性,从而完成选举信息的验证。分析协议身份评估过程,P_j 计算 P_i 的信任因子值的过程中完成了对其他选举人身份的验证。根据表 1 中可知,当 *TP* 发送的测量结果为 01 时,P_j 对手中的 *A* 粒子执行 *Z* 门变换,过程如下:

$$Z\cdot(\cos\gamma_i|0\rangle-\sin\gamma_i|1\rangle)=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\cdot\begin{pmatrix}\cos\gamma_i\\0\end{pmatrix}-\begin{pmatrix}1&0\\0&-1\end{pmatrix}\cdot\begin{pmatrix}0\\\sin\gamma_i\end{pmatrix}=$$

$$\begin{pmatrix}1&0\\0&-1\end{pmatrix}\cdot\begin{pmatrix}\cos\gamma_i\\-\sin\gamma_i\end{pmatrix}=\begin{pmatrix}\cos\gamma_i\\\sin\gamma_i\end{pmatrix}=\cos\gamma_i|1\rangle+\sin\gamma_i|1\rangle=|T\rangle_{P_i}$$

P_j 计算出 P_i 的信任因子值 $|T\rangle_{P_i}$,再将其进行与 *TP* 中存储的值对比,就能完成 P_i 的身份验证过程。

3.4 协议比较与分析

在文献[23]中提出了一个基于格的且不使用 NIZK(non-interactive zero-knowledge)证明的两轮 PAKE(password based authenticated key exchange)协议,该协议构建了两个新的基于格的 SPHF(smooth projective hash function),并通过一定程度减少协议的前向安全假设,克服了现有方案的局限性。该协议满足 Abdalla 等人的框架,且具备后量子安全性,表 2 给出了本协议与文献[19,23]协议的比较。

表 2 三个协议的比较

Tab. 2 Comparison of three protocols

比较项	文献[19]协议	文献[23]协议	本文协议
协议安全性能	较差	较强	较强
后量子安全性	差	强	较强
协议实现难度	难	容易	较易

4 结束语

本文提出了一种基于信任评估的量子区块链网络下的匿名选举方案。借助量子安全直接通信技术完成节点间的身份信任评估后,投票人使用量子比特承诺协议,计算其选举内容的承诺值,并广播给区块链中所有的矿工节点。矿工节点结合量子诚实拜占庭协议完成投票统计。本文应用方案在现有技术条件下容易实现,协议中使用的量子技术与区块链方案均已在实验或文献中得以验证。协议的安全模型分析部分证明了协议具有匿名性、不可窜改性、可验证性等优点。

格密码是一种备受关注的抗量子计算攻击的公钥密码体制,其研究的核心问题是如何确定一个给定几何体的最大格堆积密度和最小格覆盖密度。格密码的发展主要分为两个方向:a)高维格困难问题的求解算法及其计算复杂性理论研究;b)基于格困难问题的密码体制设计。在文献[24]中,作者提出了一种自适应平滑的基于格的 SPHF(smooth projective hash function),并将提出的 SPHF 集成到 TCC11 提出的一轮框架中,得到了一个具有严格安全性的格上 PAKE(password based authenticated key exchange)协议,作者还探讨了提出的协议在物联网中的潜在应用,该协议具有很强的现实应用价值。由于本文协议基于量子区块链网络,投票过程中产生的密钥和通信信息等都是通过量子隐形传输技术(quantum teleportation,QT)传输,基于量子原理的通信过程,在实验和理论上都已证明了其可以抵御量子计算攻击。与此同时,本文协议也存在量子资源开销较大的问题,笔者将进一步研究格密码理论,设计安全性能高,资源开销少的密码协议。

参考文献:

[1] 蔡维德,郁莲,王荣,等. 基于区块链的应用系统开发方法研究[J]. 软件学报,2017,28(6):1474-1487. (Cai Weide, Yu Lian, Wang Rong, *et al*. Blockchain application development techniques [J]. Journal of Software,2017,28(6):1474-1487.)

[2] 邵奇峰,金澈清,张召,等. 区块链技术:架构及进展[J]. 计算机学

报,2018,41(5):969-988. (Shao Qifeng, Jin Cheqing, Zhang Zhao, *et al*. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.)

[3] 袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016,42(4):481-494. (Yuan Yong, Wang Feiyue. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.)

[4] Nakamoto S. Bitcoin: a peer to peer electronic cash system[EB/OL]. (2008). https://bitcoin.org/en/bitcoin-paper.

[5] Miers I, Garman C, Green M, *et al*. Zerocoin: anonymous distributed e-cash from bitcoin[C]//Proc of IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE Press, 2013: 397-411.

[6] Sasson E B, Chiesa A, Garman C, *et al*. Zerocash: decentralized anonymous payments from bitcoin [C]//Proc of IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE Press, 2014: 459-474.

[7] 王文明,施重阳,王英豪,等. 基于区块链技术的交易及其安全性研究[J]. 信息网络安全,2019,19(5):1-9. (Wang Wenming, Shi Chongyang, Wang Yinghao, *et al*. Research on transaction and security based on blockchain technology[J]. Netinfo Security, 2019, 19(5): 1-9.)

[8] Bennett C H, Brassard G. Quantum cryptography: public-key distribution and coin tossing [C]//Proc of IEEE International Conference on Computers, System and Signal Processing. Piscataway, NJ: IEEE Press, 1984: 175-179.

[9] Patwardhan S, Moulick S R, Panigrahi P K. Efficient controlled quantum secure direct communication protocols[J]. International Journal of Theoretical Physics, 2016, 55(7): 3280-3288.

[10] Chang Yan, Xu Chunxiang, Zhang Shibin, *et al*. Quantum secure direct communication and authentication protocol with single photons[J]. Chinese Science Bulletin, 2013, 58(36): 4571-4576.

[11] Jakobi M, Simon C, Gisin N, *et al*. Practical private database queries based on a quantum-key-distribution protocol[J]. Physical Review A, 2011, 83(2): 022301.

[12] Gao Fei, Liu Bin, Wen Qiaoyan. Flexible quantum private queries based on quantum key distribution[J]. Optics Letters, 2012, 20(16): 17411-17420.

[13] Cao Haijing, Huang Jun, Yu Yaofeng, *et al*. A quantum proxy signature scheme based on genuine five-qubit entangled state[J]. International Journal of Theoretical Physics, 2014, 53(9): 3095-3100.

[14] Tian Juanhong, Zhang Jianzhong, Xie Shucui. Quantum multi-proxy blind signature scheme based on genuine four qubit entangled state [J]. International Journal of Theoretical Physics, 2016, 55(2): 809-816.

[15] Zhang Shibin, Xie Zhihai, Yin Yifen, *et al*. Study on quantum trust model based on node trust evaluation[J]. Chinese Journal of Electronics, 2017, 26(3): 608-613.

[16] Kiktenko E O, Pozhar N O, Anufriev M N, *et al*. Quantum-secured blockchain[J]. Quantum Science and Technology, 2018, 3(3): 1-8.

[17] Zhao Zhichao, Chan T H. How to vote privately using bitcoin[C]//Proc of the 17th International Conference on Information and Communications Security. Cham: Springer International Publishing, 2016: 82-96.

[18] Tian Haibo, Fu Liqiang, He Jiejie. A simpler bitcoin voting protocol [C]//Proc of the 13th International Conference on Information Security and Cryptology. Cham: Springer International Publishing, 2018: 81-98.

[19] Sun Xin, Wang Quanlong, Kulicki P, *et al*. A simple voting protocol on quantum blockchain [J]. International Journal of Theoretical Physics, 2019, 58(1): 275-281.

[20] Sun Xin, Wang Quanlong, Kulicki P, *et al*. Quantum-enhanced logic-based Blockchain I: quantum honest-success Byzantine agreement and Qulogicoin[EB/OL]. 2018-05-17. [2018-07-16]. https://arxiv.org/abs/1805.06768.

[21] Wang Ding, Wang Nan, Wang Ping, *et al*. Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity[J]. Information Sciences, 2015, 321(11): 162-178.

[22] Wang Ding, Wang Ping. Two birds with one stone: two-factor authentication with security beyond conventional bound[J]. IEEE Trans on Dependable and Secure Computing, 2018, 15(4): 708-722.

[23] Li Zengpeng, Wang Ding. Two-round PAKE protocol over lattices without NIZK[C]//Proc of the 14th International Conference on Information Security and Cryptology. Cham: Springer International Publishing, 2019: 138-159.

[24] Li Zengpeng, Wang Ding. Achieving one-round password-based authenticated key exchange over lattices[J]. IEEE Trans on Services Computing, 2019(8): 1-14.

(上接第 3707 页)

[5] Yerima S Y, Sezer S. DroidFusion: a novel multilevel classifier fusion approach for Android malware detection[J]. IEEE Trans on Cybernetics, 2019, 49(2): 453-466.

[6] 张玉清,董颖,柳彩云,等. 深度学习应用于网络空间安全的现状、趋势与展望[J]. 计算机研究与发展,2018,55(6):1117-1142. (Zhang Yuqing, Dong Ying, Liu Caiyun, *et al*. Situation, trends and prospects of deep learning applied to cyberspace security[J]. Journal of Computer Research and Development, 2018, 55(6): 1117-1142.)

[7] 蒋晨,胡玉鹏,司凯,等. 基于图像纹理和卷积神经网络的恶意文件检测方法[J]. 计算机应用,2018,38(10):2929-2933. (Jiang Chen, Hu Yupeng, Si Kai, *et al*. Malicious file detection method based on image texture and convolutional neural network[J]. Journal of Computer Applications, 2018, 38(10): 2929-2933.)

[8] Cui Zhihua, Xue Fei, Cai Xingjuan, *et al*. Detection of malicious code variants based on deep learning[J]. IEEE Trans on Industrial Informatics, 2018, 14(7): 3187-3196.

[9] 韩晓光,曲武,姚宣霞,等. 基于纹理指纹的恶意代码变种检测方法研究[J]. 通信学报,2014,35(8):125-136. (Han Xiaoguang, Qu Wu, Yao Xuanxia, *et al*. Research on malicious code variants detection based on texture fingerprint[J]. Journal on Communications, 2014, 35(8): 125-136.)

[10] Kim J Y, Bu S J, Cho S B. Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders [J]. Information Sciences, 2018, 460-461(4): 83-102.

[11] Karbab E B, Debbabi M, Derhab A, *et al*. Android malware detection using deep learning on API method sequences [EB/OL]. (2017-12-25). https://arxiv.org/abs/1712.08996..

[12] Nix R, Zhang J. Classification of android apps and malware using deep neural networks [C]//Proc of International Joint Conference on Neural Networks. Piscataway, NJ: IEEE Press, 2017: 1871-1878.

[13] Kwon I, Im E G. Extracting the representative API call patterns of malware families using recurrent neural network [C]//Proc of International Conference on Research in Adaptive and Convergent Systems. New York: ACM Press, 2017: 202-207.

[14] Alsulami B, Mancoridis S. Behavioral malware classification using convolutional recurrent neural networks [C]//Proc of the 13th International Conference on Malicious and Unwanted Software. Piscataway, NJ: IEEE Press, 2018: 103-111.

[15] Docker. Docker security scanning [EB/OL]. [2019-08-02]. https://docs.docker.com/v17.12/docker-cloud/builds/image-scan/.

[16] CoreOS. Clair [EB/OL]. [2019-08-02]. https://coreos.com/clair/docs/latest/.

[17] Twistlock. Cloud native security for docker, Kubernetes and beyond [EB/OL]. [2019-08-02]. https://www.twistlock.com/.

[18] VirusShare. VirusShare.com [EB/OL]. [2019-08-02]. https://virusshare.com/.

[19] Zaheer M, Ahmed A, Smola A J. Latent LSTM allocation joint clustering and non-linear dynamic modeling of sequential data[C]//Proc of the 34th International Conference on Machine Learning. New York: ACM Press, 2017: 3967-3976.