基于 Cayley 图上量子漫步的匿名通信方案*

贺振兴 范兴奎 初鹏程 马鸿洋†

(青岛理工大学理学院, 青岛 266033)

(2020 年 3 月 4 日收到; 2020 年 5 月 1 日收到修改稿)

信息安全是信息化社会国家安全的基石与命脉, 而匿名量子通信是保护信息安全的重要通信方式之一. 利用量子漫步随机性有效解决身份信息泄露等敏感问题, 本文提出一种基于 Cayley 图上量子漫步的匿名通信方案. 首先, 通信双方隐藏自身身份信息, 发送方 Alice 通过逻辑或操作匿名选择接收方 Bob. 其次, 可信第三方与通信双方利用 BB84 协议生成和分发安全密钥, Alice 根据安全密钥对信息序列进行加密, 获得盲化信息; Bob 利用联合 Bell 态测量和安全密钥进行签名, 可信第三方验证签名信息. 再次, 可信第三方依据傅里叶变换计算 Bob 量子漫步的位置概率分布函数, 将概率最大值对应的位置信息转换为确认帧发送给 Alice; Alice 利用量子降维压缩算法减少传输信息比特数, 并利用安全密钥完成信息加密后将信息传输至确认帧表示的位置, Bob 利用量子漫步搜索位置节点获取传输信息, 完成匿名量子通信. 最后, 对方案进行安全分析, 并给出 200 个节点 Cayley 图的数值仿真结果, 漫步 10 步时, 第 6 个节点的概率最大为 45.31%. 根据仿真结果, 本方案通信过程中 Bob 漫步 10 步时被窃听到具体位置的概率近似为 6×10^{-7}%.

关键词: 匿名量子通信, 量子网络, 量子漫步

PACS: 03.67.Ac, 03.67.Hk **DOI:** 10.7498/aps.69.20200333

1 引 言

近年来, 量子通信是通信技术重要研究方向之一, 包括量子秘密共享和隐形传态等领域[1−3]. 而隐私和匿名是量子通信过程中保护信息安全的重要方法, 隐私意味着传输消息不能公开, 匿名意味着隐藏发送方和接收方的身份信息, 而两者在匿名量子通信、匿名量子投票等方面有着举足轻重的作用[4,5].

众多学者在量子通信理论方案和实验实现方面有深入的研究[6−11], 并且在匿名通信协议设计及量子信息比特匿名传输等方面硕果累累[12−18]. 1988 年, Chaum[9] 提出一种经典的匿名通信方案, 方案中根据无条件保密信道, 构造出无条件发送不可跟踪信道, 实现匿名通信; 2002 年, 薛鹏和郭光灿[13] 在物理期刊中综述了量子通信领域发展, 并介绍了量子通信的基本理论框架和研究进展, 其团队后期的研究成果为本文提供了研究方向; 2002 年, Boykin[14] 提出利用量子密钥编码经典比特信息的匿名通信协议, 协议中通信方共享量子纠缠对获取安全密钥, 并对噪声攻击具有较高的抗性; 2005 年, Christandl 和 Wehner[15] 提出一种匿名传输经典比特的量子协议, 该协议主要讨论传输量子态时的安全问题, 并利用纠缠量子态扩展协议使得通信双方能够匿名发送和接收量子位; 2007 年, Bouda 和 Sprojcar[16] 提出了一种量子信息比特的匿名分发协议, 该协议在公共接收方 (发送方) 的通信模型下, 可用于接收方 (发送方) 匿名信道构建和无条件信息保密; 2007 年, Brassard 等[5] 提出

* 国家自然科学基金 (批准号: 11975132, 61772295)、山东省自然科学基金 (批准号: ZR2019YQ01) 和山东省高等教育科技计划 (批准号: J18KZ012) 资助的课题.

† 通信作者. E-mail: hongyang_ma@aliyun.com

匿名量子通信协议模型, 并在理论上证明该模型受到攻击时只能以指数级的小概率破坏通信双方的匿名性以及量子态的隐私性, 该模型提升了整个通信协议的安全性; 2012 年, Jiang 等[17] 提出了以连续变量纠缠量子态作为信息载体的匿名量子投票系统. 与上述成果不同, 本方案利用量子漫步作为搜索算法进行量子信息搜索, 并且量子漫步算法本身可以模拟多体物理体系的量子行为适用于多种网络结构.

经典随机行走算法是对粒子在底层图结构内随机移动的模拟算法[19], 量子漫步算法则是模拟粒子在图上移动的量子相干性演化. 深入研究文献 [20—30], 很多学者发现量子漫步算法相较于经典随机算法的优点主要有两个: 寻找目标节点时间更少和从源顶点分散到所有顶点的时间更少. 2002 年, Travaglione 和 Milburn[21] 提出在离子阱量子计算机上实现量子漫步的方案, 方案展示了量子漫步直线方差和混合时间增强的特征, 实验结果显示在强退相干限制下量子漫步算法逐渐趋于经典算法; 在 2004 年, Childs 和 Goldstone[22] 提出利用图上连续时间量子漫步来求解 Grover 问题的一般方法, 并证明了如果图结构是一个高维度的晶格可以实现算法的二次加速; 2009 年, Childs[25] 提出利用散射过程构造量子算符, 将量子漫步作为计算基在基层图中进行量子计算; 2019 年, Zhan[26] 从图谱的角度解释离散量子漫步肯顿模型的完全态转移, 并构造了一个允许完全态转移的无限族的四正则循环图; 2019 年, Costa 等[27] 根据气体 HPP 模型提出多粒子量子漫步算法, 通过 HPP 模型模拟量子态碰撞后的运动方向, 并构造出粒子碰撞的演化算符. 而量子各个领域在不断交叉情况下出现非常多的研究成果, 尤其是近年来将量子漫步算法与量子通信相结合的通信方案不断涌现[31—38], 例如在 2017 年, 薛鹏团队[31] 提出基于两个硬币态量子漫步的广义隐形传态, 与现有的 d 维量子态隐形传态相比不需要预先制备纠缠态, 这是第一个利用量子漫步实现通信协议的方案; 2019 年, 冯艳艳等[32] 提出基于量子漫步-隐形传态的仲裁量子签名方案, 方案通过量子漫步产生纠缠态进行隐形传态, 并利用随机数和公共板验证量子签名正确性; 2019, Li 等[33] 提出基于多硬币态量子漫步的量子信息分割方案, 该方案不需要预先准备纠缠态, 也不需要测量纠缠度, 降低量子网络通信资源消耗.

本方案依据量子漫步的随机特性设计匿名量子通信方案[39—41]. 本方案在量子 Cayley 网络上进行通信[42—44], Alice 通过文献 [4] 中的逻辑或操作匿名选择 Bob 实现量子网络匿名协议, 从而保护通信双方身份信息; 可信第三方根据量子盲签名方法检测 Alice 和 Bob 身份信息是否泄露或被窃听; 可信第三方根据群上傅里叶变换计算 Bob 量子漫步位置概率分布函数, 并将概率最大值对应的位置信息作为确认帧发送给 Alice; Alice 获取位置信息后利用量子保密一次通信建立信道[45,46], 将制备的量子信息传输至 Bob 量子漫步时出现概率最大的位置[22,47,48], 利用量子压缩对信息进行预处理, 减少信息的比特长度, 最多减少 37.5% 的比特长度[49—51]; Bob 通过 Cayley 图上离散时间量子漫步算法在网络中搜索 Alice 传输的信息. 在通信双方遵循量子网络匿名协议的前提下, 本方案根据量子漫步的随机特性, 使得接收方能够以极大的概率避免被窃听者获得身份信息, 并且没有破坏量子网络匿名协议.

本文具体内容如下: 第 2 节介绍 Cayley 图上量子漫步和量子压缩; 第 3 节讨论匿名通信方案和离散量子漫步概率解析解; 第 4 节分析方案的安全性, 并计算 Cayley 中环的概率分布; 第 5 节, 对方案进行总结和简要概述.

2 相关工作

2.1 Cayley 图上量子漫步

假设群 G 是有限群, S 是该群的生成集合, Cayley 图和群 G 存在一一对应关系, 若节点 g 和 g' 满足 $g'=gh$, 则存在一条边 (g,g'), 其中 $g\in G$, $h\in S$. 将 Cayley 图中元素量子化:

$$h\in S\rightarrow|h\rangle\in H_S, g\in G\rightarrow|g\rangle\in H_G, \tag{1}$$

其中, H_S 为硬币算符所在的 Hilbert 空间, H_G 为量子漫步所处的位置空间. Cayley 图上量子漫步的演化算符为 $E=T(C\otimes I)$, I 为位置空间的单位算符, C 为硬币算符, T 为转移算符, 具体定义如下:

$$C=\sum_{h_1h_2\in H_S}|h_1\rangle\langle h_2|, \tag{2}$$

$$T=\left[|h_1\rangle\langle h_1|\otimes\sum_{g\in G}|gh_1\rangle\langle g|+|h_2\rangle\langle h_2|\otimes\sum_{g\in G}|gh_2\rangle\langle g|\right]. \tag{3}$$

2.2 量子信息降维压缩算法

量子降维压缩算法中 3 维张量信息可以表示为

$$|M\rangle=|aaa\rangle,|aab\rangle,|aba\rangle,|abb\rangle,|baa\rangle,|bab\rangle,|bba\rangle,|bbb\rangle, \tag{4}$$

其中 $|a\rangle=|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$; $|b\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$. 令 $|\phi\rangle=|\lambda_i\lambda_j\lambda_k\rangle$, 其中 $\lambda_i,\lambda_j,\lambda_k\in\{\lambda_a,\lambda_b\}$,

$$|\lambda_a\rangle=\begin{pmatrix}\cos\left(\frac{\pi}{8}\right)\\ \sin\left(\frac{\pi}{8}\right)\end{pmatrix},\ |\lambda_b\rangle=\begin{pmatrix}\sin\left(\frac{\pi}{8}\right)\\ -\cos\left(\frac{\pi}{8}\right)\end{pmatrix}. \tag{5}$$

Alice 根据幺正变换进行典型态转化, $|xy0\rangle=|xy\rangle\otimes|0\rangle$, 令 $|\phi_1\rangle=|xy\rangle$, 映射到典型子空间; 非典型态转化为, $|mn1\rangle=|mn\rangle\otimes|1\rangle$, 令 $|\phi_2\rangle=|mn\rangle$, 映射到非典型子空间; 将压缩后的 $|\phi_1\rangle$, $|\phi_2\rangle$ 作为传输信息, 最后利用逆幺正变换解压缩还原压缩信息.

3 通信方案

通信双方在超立方体量子 Cayley 网络上进行量子通信. 初始化阶段: 发送方利用文献 [4] 中逻辑或操作匿名选择接收方. 假设网络中存在 $m+1$ 个通信节点, 可信第三方选择发送方为 Alice, 并设置安全参数 Z; Alice 根据比特分布 D 选取随机比特 $x_i=0$ 或 1 ($x_i\in D$), 其他 m 个节点选择 $x_i=0$; Alice 根据 $\{x_i\}_{i=1}^m$ 的取值 (不包含发送方选择的比特数) 进行逻辑或操作匿名选择接收方, 即设 i 为其他 m 个节点中的一个节点, 根据安全参数 Z 重复选择比特数 x_i, 做模 2 加运算, 令 $y_i=\oplus_{j=1}^{Z}x_i^{(j)}$ (j 表示选择 x_i 的次数), 若 $y_i=1$, 则选择节点 i 为接收方 Bob, 否则重新执行逻辑或操作选择接收方, 接收方将模 2 加运算结果发送给可信第三方. 图 1 为匿名量子通信流程,

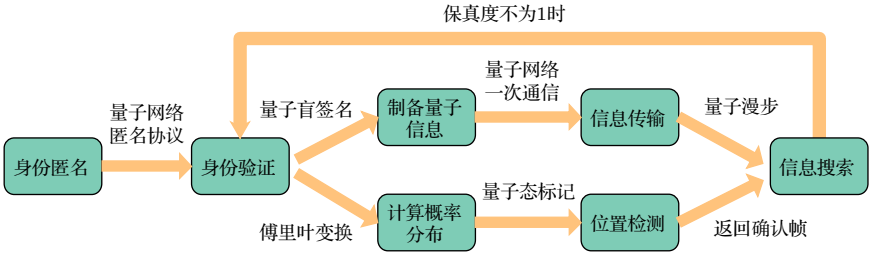

图 1 匿名量子通信方案流程图

Fig. 1. Flow chart of anonymous quantum communication scheme.

3.1 身份验证阶段

协议 1 可信第三方利用量子盲签名验证通信双方身份信息. 可信第三方与 Alice 和 Bob 通过量子密钥分发生成和分发安全密钥 K_{3A} 和 K_{3B}, Bob 作为签名者, 可信第三方作为仲裁者判断签名的有效性. Bob 制备 EPR 对序列,

$$|\Phi\rangle_{AB}=\{|\Phi_1\rangle_{AB},|\Phi_2\rangle_{AB},\cdots,|\Phi_n\rangle_{AB}\}, \tag{6}$$

这些 EPR 对处于相同状态, Bob 通过可信第三方将 A 粒子发送给 Alice. 身份验证过程如下:

Alice 盲化信息. Alice 制备量子比特信息序列 A, 并利用量子投影测量方法对序列 A 进行测量, 测量后序列 A 中量子比特不发生变化, 且得到相对应的经典二进制信息序列 $n=\{n_1,n_2,\cdots,n_n\}$; 依据经典比特信息测量量子比特序列 A, 当 $n_i=0$ 时, Alice 将 Pauli-Z 作为测量基, 当 $n_j=1$ 时, Alice 选择 Pauli-X 作为测量基, 得到的测量结果记为 $M=\{m_1,m_2,\cdots,m_n\}$, 测量后的量子比特序列记为 A'; Alice 将序列 n 和 M 组合成新的信息序列 $N=\{n_1\|m_1,n_2\|m_2,\cdots,n_n\|m_n\}$, Alice利用安全密钥 K_{3A} 对信息序列 N 加密得到盲化信息 $N'=E_{K_{3,4}}(N)$; Alice 将序列 N 和盲化信息 N' 同时传输给可信第三方.

Bob 进行签名. 可信第三方将序列 A' 发送给 Bob, Bob 对量子态序列 A' 和 B 粒子进行可观测量 C 上的联合测量, C 有非简并本征态, 并且符合

$$|\psi_1\rangle=\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{2}\left(\mathrm{e}^{\frac{\mathrm{i}\pi}{4}}|01\rangle+\mathrm{e}^{-\frac{\mathrm{i}\pi}{4}}|10\rangle\right),$$
$$|\psi_2\rangle=\frac{1}{\sqrt{2}}|00\rangle-\frac{1}{2}\left(\mathrm{e}^{\frac{\mathrm{i}\pi}{4}}|01\rangle+\mathrm{e}^{-\frac{\mathrm{i}\pi}{4}}|10\rangle\right),$$
$$|\psi_3\rangle=\frac{1}{\sqrt{2}}|11\rangle+\frac{1}{2}\left(\mathrm{e}^{\frac{\mathrm{i}\pi}{4}}|10\rangle+\mathrm{e}^{-\frac{\mathrm{i}\pi}{4}}|01\rangle\right),$$
$$|\psi_4\rangle=\frac{1}{\sqrt{2}}|11\rangle-\frac{1}{2}\left(\mathrm{e}^{\frac{\mathrm{i}\pi}{4}}|10\rangle+\mathrm{e}^{-\frac{\mathrm{i}\pi}{4}}|01\rangle\right);\quad(7)$$

联合测量结果为 $Sor=\{Sor_1,Sor_2,\cdots,Sor_n\}$, Sor_j 表示两个比特, 且测量结果为$|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$, $|\psi_4\rangle$时, 序列 Sor_j 对应 00, 10, 01, 11; Bob 利用密钥 K_{3B} 对序列 Sor 加密获得签名序列 $Sor'=E_{K_{3B}}(Sor)$, 并将签名序列 Sor' 发送给可信第三方.

可信第三方验证签名信息. 可信第三方对 N' 和 Sor' 解密获得序列 N 和 Sor, 若序列 N 与对应位置的元素都匹配, 则认定签名有效, 否则签名无效并终止通信. 对应关系如表 1 所示.

表 1 信息 N 和签名 Sor 的对应关系

Table 1. Correspondence between information N and Sor signature.

Alice信息序列 N_j	Bob签名序列 Sor_j
00	00 或 01
01	10 或 11
10	00 或 11
11	01 或 11

3.2 信息传输阶段

协议 2 完成协议 1 后, 可信第三方计算 Bob 从当前位置进行量子漫步, 概率最大值对应的位置信息为 $LocB$, 将其转化为量子态 $LocB\rightarrow|LocB\rangle$, 并将$|LocB\rangle$作为确认帧通过信道传输给 Alice. 协议中的具体操作如下:

1) 可信第三方对 Alice 返回确认帧 ACK, $ACK\rightarrow|ACK\rangle$, 且$|ACK\rangle=|LocB\rangle$.

2)Alice 获得位置信息$|LocB\rangle$后, 利用量子降维压缩对制备的传输信息进行预处理; Alice 利用 BB84 协议获取安全密钥完成传输信息加密, 将确认帧$|ACK\rangle$作为信息比特串的第一个字符添加到要传输信息中.

对 10 维传输信息进行压缩, 则信息码元为

$$|M\rangle=|aaaaaaaaaa\rangle,|aaaaaaaaab\rangle,|aaaaaaaaba\rangle$$
$$|aaaaaaaaab\rangle,|aaaaaaaabab\rangle,|aaaaaaaabaa\rangle$$
$$|aaaaaaaabba\rangle,|aaaaaaabbb|,|bbbbbbbbbb\rangle.\quad(8)$$

令任意测量态$|\varphi\rangle=|\lambda_1\lambda_j\lambda_k\lambda_1\lambda_m\lambda_n\lambda_0\lambda_p\lambda_q\lambda_r\rangle$, 其中

$$\lambda_i,\lambda_j,\lambda_k,\lambda_1,\lambda_m,\lambda_n,\lambda_o,\lambda_p,\lambda_q,\lambda_r=\lambda_a,\lambda_b.\quad(9)$$

对 10 维量子信息进行压缩, 后 3 个比特为$|0\rangle$, 传输信息为典型信息, Alice 通过幺正变换 U 将典型态转化, $|tuvwxyz000\rangle=|tuvwxyz\rangle\otimes|000\rangle$, 前 7 个比特为典型子空间信息; 后 3 个比特为$|1\rangle$, 则为非典型信息, Alice 将非典型态转化$|hijklmn111\rangle=|higklmn\rangle\otimes|111\rangle$, 前 7 个比特为非典型子空间信息. 实现量子信息压缩后 Alice 只需传输 7 个比特, 就能够完成信息传输. 压缩过程如图 2 所示,

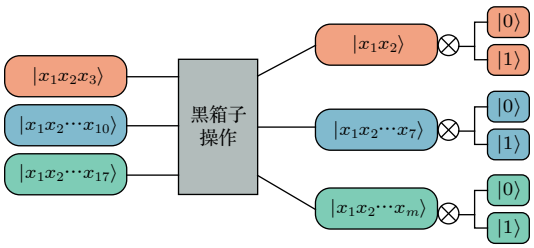

图 2 量子压缩过程

Fig. 2. Quantum compression process.

3)Alice 利用量子保密一次通信, 将压缩后的比特串添加确认帧进行传输, $|ACK,turwxyz\rangle$, 传输到第三方计算出的网络节点位置 $LocB$.

3.3 量子漫步搜索传输信息

在信息传输完成后, Bob 进行量子漫步搜索信息位置, 得到节点存留的信息. 通信协议在量子 Cayley 网络上进行, Bob 以 Cayley 图上量子漫步的演化算符作为量子动力在网络中移动. 但是, 在 Bob 搜索信息前第三方需要对位置进行安全检测, 如下所述:

协议 3 第三方对信息比特串$|ACK,turwxyz\rangle$中的确认帧$|ACK\rangle$作保真度测量. 首先, 对信息比特串作幺正变换提取确认帧的量子态,

$$U|ACK,turwxyz\rangle=|ACK\rangle\otimes|turwxyz\rangle\quad(10)$$

然后, 计算确认帧的保真度判断存储信息的位置是否被窃听,

$$\langle ACK'|ACK\rangle=\begin{cases}1,\\ \alpha,\end{cases}\quad(11)$$

其中, $0\leqslant\alpha<1$. 对信息比特串作做内积, 保真度若为 1, 则表明该位置未被窃听; 若为 α, 在不考虑噪声影响的情况下认为该位置被窃听.

协议 4 在第三方确定信息位置安全的前提下, Bob 在 Cayley 网络中进行量子漫步搜索目标节点, 获得传输信息. 具体步骤如下:

1) 完成协议 3 后, 第三方对 Bob 返回确认帧 $|ACK'\rangle$;

2) Bob 接受确认帧后, 进行 Cayley 图上量子漫步搜索信息; 以 Bob 位置 g 为起点开始搜索,

$$\begin{aligned}|h_1\rangle\otimes|g\rangle &\xrightarrow{C\otimes I}(|h_1\rangle+|h_2\rangle)\otimes|g\rangle\\ &\xrightarrow{T}(|h_1\rangle\otimes|gh_1\rangle+|h_2\rangle\otimes|gh_2\rangle),\end{aligned}\tag{12}$$

上述过程重复 10 次后, 获得 $t=10$ 时 Bob 的量子漫步状态,

$$|\Psi(10)\rangle=\sum_{h\in S}\sum_{g\in G}\psi_{h,g}(10)|h\rangle\,|g\rangle\,.\tag{13}$$

Bob 漫步 10 步的过程中将会搜索到信息位置 $|LocB\rangle$, 但是为了隐藏自身身份信息, Bob 即使在第一步就搜索到传输的信息, 也必须完成 10 步量子漫步. 图 3 为发送方进行量子漫步搜索传输信息的过程演示图.

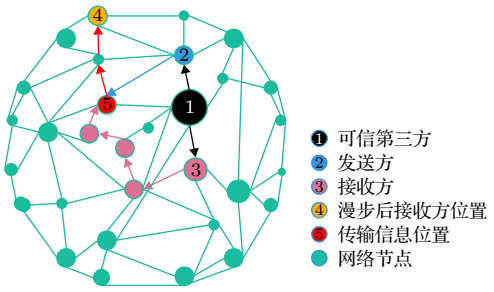

图 3 匿名量子通信过程

Fig. 3. Anonymous quantum communication process.

3) Bob 搜索得到信息后通过逆幺正变换 U^{-1} 对压缩信息解码:

$$\begin{aligned}|\varphi_i\rangle &= U^{-1}\left(|\varphi_1\rangle\otimes|000\rangle\right)\\ &= U^{-1}U|tuvwxyz\rangle=|\varphi_{\mathrm{op}}\rangle\,,\\ |\varphi_j\rangle &= U^{-1}\left(|\varphi_2\rangle\otimes|000\rangle\right)\\ &= |\lambda_a\lambda_a\lambda_a\lambda_a\lambda_a\lambda_a\lambda_a\lambda_a\lambda_a\lambda_a\lambda_a\lambda_a\rangle\,,\end{aligned}\tag{14}$$

其中, $|\varphi_{\mathrm{op}}\rangle=|M\rangle=\{|aaa\rangle,|aab\rangle,|aba\rangle,|baa\rangle\}$.

上述协议 1—4 中, 任何一步的检验出现错误都会终止通信方案, 并且 Alice 在传输完信息后就将量子保密一次通信的信道舍弃, 然后重新选择通信双方, 从协议 1 开始新一轮通信.

3.4 Cayley 图上量子漫步概率计算

协议 4 中, 利用量子漫步算法作为搜索算法搜索传输信息位置, 因此在计算位置概率时需要对 t 时刻量子漫步状态 $|\Psi(t)\rangle$ 进行群上的傅里叶变换, 将离散变量转换为连续变量, 进而得到量子漫步位置概率分布函数的解析解. 假设群 G 为 Abelian 群, 其同构于多个 Z_N 群的直积, $G\cong Z_{N_1}\times\cdots\times Z_{N_s}$, Z_N 为模 N 的加法群, 则群 G 中每个元素 g 都有一个 n 元组 $(g_1,\cdots,g_n)$ 一一对应.

对群元素进行傅里叶变换[35], 算子的形式如下:

$$F=\frac{1}{\sqrt{G}}\sum_{k,g\in G}\chi_g(k)|g\rangle\langle k|,\tag{15}$$

其中, χ_g 为群的特征标, $\chi_s=\prod_{j=1}^{n}\omega_{N_j}^{\varepsilon,k_j}$, $\omega_{N_j}=\mathrm{e}^{\frac{2\pi}{N_j}}$.

将位置空间的基态转换为傅里叶基态: $|\widetilde{\chi}_k\rangle=\dfrac{1}{\sqrt{G}}\sum_{k,s\in G}\chi_s\left(k^{-1}\right)|g\rangle$, 则在 t 时刻量子漫步的状态用傅里叶变换后的基态表示为

$$|\Psi(t)\rangle=\sum_{h\in S}\sum_{k,s\in G}\tilde{\psi}_{h,s}(t)|h\rangle\,|\tilde{\chi}_k\rangle\,,\tag{16}$$

其中, 转移算符对傅里叶基态作用后的形式为

$$T|h\rangle\,|\widetilde{\chi}_g\rangle=\chi_h(g)|h\rangle\,|\widetilde{\chi}_g\rangle\,.\tag{17}$$

可以证明傅里叶基态下, 转移算符只改变基态的振幅.

最后, 得到傅里叶基态下 t 时刻的振幅为 $\tilde{\psi}_{h,g}(t)$, 通过逆傅里叶变换求解离散时间的振幅:

$$\psi_{h,g}(t)=\sum_{g\in G}\frac{\chi_g\left(g^{-1}\right)}{\sqrt{|G|}}\tilde{\psi}_{h,g}(t).\tag{18}$$

得到离散时间量子态的振幅后, 通过模方运算计算位置概率分布函数, $\rho_g(t)=|\psi_{h,g}(t)|^2$.

根据协议 2 中描述, 第三方计算出 Bob 量子漫步的概率分布函数, 即 $\rho_g(t)=|\psi_{h,g}(t)|^2$ 的数值分布情况, 并将出现概率最大的位置以确认帧的形式发送给 Alice, Alice 将信息传输到该位置.

4 协议分析和数值仿真

4.1 协议分析

目前, 存在很多量子漫步实现量子通信的研究, 如文献 [42] 中提出离散时间量子漫步算法实现量子通信的方案, 并且方案拥有通信网络限制少, 实现状态转移保真度为 1 和步骤少等优势; 文献 [43] 利用量子漫步进行量子隐形传态实现 N 比特量子信息传输, 并且实现过程只应用但量子比特门能够简化实验过程. 这些研究成果多是将量子漫步算法应用于信息比特传输或隐形传态编码中, 而本方案

利用量子漫步算法的随机特性进行匿名量子通信, 能够以极大的概率规避窃听. 本节针对常见的通信攻击方式和窃听者进一步对方案进行分析.

1) 在 4.2 节中 $t=10$ 和传输信息节点位置为 6 时符合文献 [42] 中所提出的理论公式 $((n-x)/2)\in Z$ (n 为漫步步数, x 为节点位置, Z 为整数集合), 因此本方案能够利用离散时间量子漫步算法进行匿名通信, 且在量子态转移时能够保证保真度为 1.

2) 假设 Alice 在进行通信之前被恶意替换身份, 在协议 1 中采用量子盲签名方法验证身份信息时, 能够检测出恶意替换身份者为不诚实通信方, 从而第三方终止匿名通信; 假设传输信息位置被窃听者获取, 在协议 3 中对标记状态 $|ACK'\rangle$ 进行保真度测量, 若保真度不为 1 则检测出传输位置被窃听, 可信第三方终止通信防止通信双方身份信息泄露; 假设存在文献 [18] 中提到的虚假粒子纠缠攻击和解纠缠攻击, 由于通信过程中无需纠缠态进行信息传输, 并且只在量子漫步算法的初始态 $|\Psi(0)\rangle=\sum_{h\in S}\sum_{g\in G}\psi_{h,g}(0)|h\rangle\,|g_0\rangle$ 中出现纠缠态, 则通信过程中受到虚假粒子纠缠攻击或解纠缠攻击时, 将会出现纠缠攻击无效或无法进行量子漫步的情况, 但不会泄露通信双方身份信息.

3) 假设在量子网络中存在窃听者, 则协议 4 中 Bob 搜索传输信息位置时会暴露自身身份信息, 但 Bob 进行量子漫步时具有随机特性, 会不断地改变位置进行信息搜索, 量子漫步的随机特性将会保护 Bob 身份, 即使窃听者获取 Bob 初始位置, 则窃听者获得 Bob 准确身份信息的概率为 $\rho=\prod_{g\in G}\rho_g(t)$, 即漫步 3 步时窃听者获取 Bob 身份信息的概率为 $\rho=0.0929\%$. 除此之外, 窃听者若窃听 Bob 将会改变 Bob 量子漫步时初始态的振幅, 使得 Bob 的概率分布发生变化, 减小搜索到信息位置的概率.

4) 经典网络层轻量级匿名通信协议 [52] 中, Alice 发送空的数据包与 Bob 建立连接后才能进行正式通信, 并且网络节点信息中包含 Bob 位置信息, 网络节点将 Alice 的信息比特转发给 Bob, 最后利用终端加密信息传输路径实现匿名通信, 其他经典协议与文献 [52] 相比也只是身份匿名方式不同; 而匿名量子通信利用量子比特作为信息载体来进行信息交互, 量子比特的测不准原理和不可克隆特性使得传输信息具有较高安全性. 并且经典匿名通信需要安全的两两配对的经典频道, 以及经典的广播频道, 才能实现身份匿名和信息传输; 而匿名量子通信只需要通信双方匿名共享纠缠态即可隐藏身份信息, 传输信息阶段只设计局部操作和经典信道. 本方案中传输信息比特过程与文献 [52]相比步骤更为简便, 只需执行量子漫步算法就能以 45.31% 的概率搜索到传输信息, 并且本方案的量子网络节点只构造量子漫步演化算符不包含 Bob 位置信息, 因此本方案通信过程更为简单, 且支持不同量子网络结构进行匿名量子通信.

4.2 量子漫步概率分布数值仿真

Cayley 图是对环的拓展, 因此本方案对环上量子漫步进行数值仿真, 如图 4 所示, 其生成元集合 $S=\{1,-1\}$, 硬币算符为 Hadamard 算符, $\boldsymbol{C}=\boldsymbol{H}=\dfrac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}$. t 时刻量子漫步的叠加态为

$$|\Psi(t)\rangle=\sum_{n=0}^{N-1}\psi_{0,n}(t)|0,n\rangle+\psi_{1,n}(t)|1,n\rangle, \tag{19}$$

其中, N 为环上节点总数.

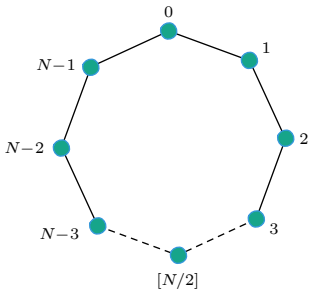

图 4 环形结构

Fig. 4. Ring structure graph.

通过 3.4 节中公式计算离散量子漫步时刻连续叠加态的振幅, t 为偶数:

$$X_k(t)=\cos\theta_k t-\frac{\mathrm{i}\cos\dfrac{2\pi k}{N}\sin\theta_k t}{\sqrt{1+\cos^2\dfrac{2\pi k}{N}}},$$

$$Y_k(t)=-\frac{\mathrm{i}\mathrm{e}^{\mathrm{i}\frac{2\pi}{N}}\sin\theta_k t}{\sqrt{1+\cos^2\dfrac{2\pi k}{N}}}; \tag{20}$$

t 为奇数:

$$X_k(t) = -\mathrm{i}\sin\theta_k t - \frac{\mathrm{i}\cos\dfrac{2\pi k}{N}\sin\theta_k t}{\sqrt{1+\cos^2\dfrac{2\pi k}{N}}},$$

$$Y_k(t) = -\frac{\mathrm{i}\mathrm{e}^{\mathrm{i}\frac{2\pi k}{N}}\sin\theta_k t}{\sqrt{1+\cos^2\dfrac{2\pi k}{N}}}, \tag{21}$$

其中, θ_k满足 $\sin\theta_k = \dfrac{1}{\sqrt{2}}\sin\dfrac{2\pi k}{N}$, k表示环上的位置. 则 t时刻位置 j 的概率为

$$\rho_j(t) = |\psi_{h,j}(t)|^2 = \frac{1}{N^2}\left|\sum_{k=0}^{N-1} X_k(t)\mathrm{e}^{\mathrm{i}jk}\right|^2 + \frac{1}{N^2}\left|\sum_{k=0}^{N-1} Y_k(t)\mathrm{e}^{\mathrm{i}jk}\right|^2. \tag{22}$$

选取节点数 $N = 200$, 0 节点作为初始位置, $t = 10$的概率分布情况如图 5 所示,

Bob 进行量子漫步时搜索环上第 6 个节点的概率最大, 为 45.31%. 其他的数值仿真结果表 2 所列.

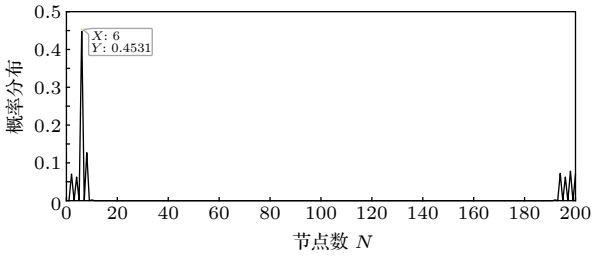

图 5 量子漫步 10 步时概率分布图

Fig. 5. Probability distribution diagram for quantum walk in 10 steps.

表 2 数值仿真结果

Table 2. Numerical simulation results.

时间	节点总数	位置	概率/%
3	100	2	72.72
10	500	6	45.31
30	200 或 500	20	25.92
50	200 或 500	34	18.95
100	100	68	12.20
200	200	138	10.81

5 结 论

方案中采用量子压缩对传输信息进行预处理, 减小信息比特长度, 间接提高量子保密一次通信的传输效率; 文献 [49] 针对量子压缩进行研究, 计算 10 维信息解压缩后的保真度为 0.9978, 对传输信息的损耗非常低, 提高匿名量子通信的效率, 并降低通信过程的资源消耗.

本文最后给出 200 个节点的环上量子漫步概率分布, 漫步 10 步时第 6 个节点概率 45.31%, 根据协议 2 和协议 4 第三方将位置节点 6 转化为量子态$|6\rangle$发送给 Alice, 并对 Bob 返回确认帧$|ACK'\rangle$, Bob 进行量子漫步搜索 Alice 传输的信息. 根据漫步 10 步的概率分布规律并舍弃概率趋近于 0 的节点, 窃听者针对 Bob 进行窃听时获取 Bob 具体身份信息的概率近似为 6×10^{-7}%. 因此, 本方案能够更好地保护接收方的身份安全, 防止信息泄露. 若量子网络本身安全性较高, 可以通过减少量子漫步的步数提高搜索概率, 如表 2 中所列, $t = 3$时搜索到第 2 个节点的概率为 72.72%, 并且通过数据可以得出网络性质不变的情况下, 节点总数对概率最大节点位置和概率影响很小.

参考文献

[1] Furusawa A, Sørensen J L, Braunstein S L, Fuchs C A, Kimble H J, Polzik E S 1998 *Science* **282** 706

[2] Hillery M, Bužek V, Berthiaume A 1999 *Phys. Rev. A* **59** 1892

[3] Hu Y A, Ye Z Q 2014 *Acta Photon. Sin.* **43** 827001 (in Chinese) [胡钰安, 叶志清 2014 光子学报 **43** 827001]

[4] Unnikrishnan A, MacFarlane I J, Yi R, Diamanti E, Markham D, Kerenidis I 2019 *Phys. Rev. Lett.* **122** 240510

[5] Brassard G, Broadbent A, Fitzsimons J, Gambs S, Tapp A 2007 *13 th International Conference on the Theory and Application of Cryptology and Information Security* Kuching, Malaysia, December 2–6, 2007 pp460–473

[6] Chen P, Cai Y X, Cai X F, Shi L H, Yu X T 2015 *Acta Phy. Sin.* **64** 040301 (in Chinese) [陈鹏, 蔡有勋, 蔡晓菲, 施丽慧, 余旭涛 2015 物理学报 **64** 040301]

[7] Nie M, Wang L F, Yang G, Zhang M L, Pei C X 2015 *Acta Phy. Sin.* **64** 210303 (in Chinese) [聂敏, 王林飞, 杨光, 张美玲, 裴昌幸 2015 物理学报 **64** 210303]

[8] Wehner S 2004 *Ph. D. Dissertation* (Holland: Universiteit van Amsterdam)

[9] Chaum D 1988 *J. Cryptol.* **1** 1

[10] Chen X B, Sun Y R, Xu G 2019 *Inf. Sci.* **501** 172

[11] Xu G, Xiao K, Li Z P, Niu X X, Ryan M 2019 *CMC-Comput. Mater. Con.* **58** 809

[12] Lipinska V, Murta G, Wehner S 2018 *Phys. Rev. A* **98** 052320

[13] Xue P, Guo G C 2002 *Physics* **31** 385 (in Chinese) [薛鹏, 郭光灿 2002 物理 **31** 385]

[14] Boykin P O 2002 *Ph. D. Dissertation* (Los Angeles: University of California)

[15] Christandl M, Wehner S 2005 *11th International Conference on the Theory and Application of Cryptology and Information* Chennai, India, December 4–8, 2005 pp217–235

[16] Bouda J, Sprojcar J 2007 *First International Conference on Quantum, Nano, and Micro Technologies* Gosier, Guadeloupe, January 2–6, 2007 p12

[17] Jiang L, He G Q, Nie D, Xiong J, Zeng G H 2012 *Phys. Rev. A* **85** 042309

[18] Zhou N R, Gong L H, Liu S Q, Zeng G H 2007 *Acta Phys. Sin.* **56** 5066 (in Chinese) [周南润, 龚黎华, 刘三秋, 曾贵华 2007 物理学报 **56** 5066]

[19] Montanaro A 2016 *NPJ Quantum Inf.* **2** 15023

[20] Yang L, Li K, Dai H Y, Zhang M 2019 *Acta Phys. Sin.* **68** 140301 (in Chinese) [杨乐, 李凯, 戴宏毅, 张明 2019 物理学报 **68** 140301]

[21] Travaglione B C, Milburn G J 2002 *Phys. Rev. A* **65** 032310

[22] Childs A M, Goldstone J 2004 *Phys. Rev. A* **70** 022314

[23] Childs A M, Cleve R, Deotto E, Farhi E, Gutmann S, Spielman D A 2003 *Proceedings of the Thirty-fifth Annual ACM Symposium on Theory of Computing* San Diego, America, June 9–11, 2003 pp59–68

[24] Sansoni L, Sciarrino F, Vallone G, Mataloni P, Crespi A, Ramponi R, Osellame R 2012 *Phys. Rev. Lett.* **108** 010502

[25] Childs A M 2009 *Phys. Rev. Lett.* **102** 180510

[26] Zhan H 2019 *Quantum Inf. Process.* **18** 369

[27] Costa P, de Melo F, Portugal R 2019 *Phys. Rev. A* **100** 042320

[28] Di Molfetta G, Arrighi P 2020 *Quantum Inf. Process.* **19** 47

[29] Wong T G 2019 *Phys. Rev. A* **100** 062325

[30] Szigeti B E, Homa G, Zimborás Z, Barankai N 2019 *Phys. Rev. A* **100** 062320

[31] Wang Y, Shang Y, Xue P 2017 *Quantum Inf. Process.* **16** 221

[32] Feng Y Y, Shi R H, Shi J J, Zhou J, Guo Y 2019 *Quantum Inf. Process.* **18** 154

[33] Li H J, Li J, Xiang N, Zheng Y, Yang Y G, Naseri M 2019 *Quantum Inf. Process.* **18** 316

[34] Abd-El-Atty B, El-Latif A A A, Venegas-Andraca S E 2019 *Quantum Inf. Process.* **18** 272

[35] Xu P A, He Z X, Qiu T H, Ma H Y 2020 *Opt. Express* **28** 12508

[36] Shi P, Li N C, Wang S M, Liu Z, Ren M R, Ma H Y 2019 *Sensors* **19** 5257

[37] Ma H Y, Teng J K, Hu T, Shi P, Wang S M 2020 *Wireless. Pers. Commun.* https://doi.org/10.1088/1674-1056/ab773 e [quant-ph]

[38] Zhao J B, Zhang W B, Ma Y L, Zhang X H, Ma H Y 2020 *Appl. Sci.* **10** 1935

[39] Ye C Q, Ye T Y 2019 *Int. J. Theor. Phys.* **58** 1282

[40] Qin L G, Wang Z Y, Wu S C, Gong S Q, Ma H Y, Jing J 2018 *Opt. Commun.* **410** 102

[41] Gong L, Qiu K, Deng C, Zhou N 2019 *Opt. Laser Technol.* **115** 257

[42] Chen X B, Wang Y L, Xu G, Yang Y Y 2019 *IEEE Access* **7** 13634

[43] Li H J, Chen X B, Wang Y L, Hou Y Y, Li J 2019 *Quantum Inf. Process.* **18** 16

[44] Facer C, Twamley J, Cresser J 2008 *Phys. Rev. A* **77** 012334

[45] Deng F G, Long G L 2004 *Phys. Rev. A* **69** 052319

[46] Long G L, Wang C, Li Y S, Deng F G 2011 *Sci. Sin. Phys. Mech. Astron.* **41** 332 (in Chinese) [龙桂鲁, 王川, 李岩松, 邓富国 2011 中国科学: 物理学 力学 天文学 **41** 332]

[47] Kempf A, Portugal R 2009 *Phys. Rev. A* **79** 052317

[48] Childs A M 2010 *Commun. Math. Phys.* **294** 281

[49] Liu X, Liang Y X, Nie M, Wei Y Y 2017 *J. Optoelectron. Laser* **11** 7 (in Chinese) [刘欣, 梁燕霞, 聂敏, 魏媛媛 2017 光电子·激光 **11** 7]

[50] Ma H Y, Zhang X, Xu P A, Liu F, Fan X K 2020 *J. Commun.* **41** 190 (in Chinese) [马鸿洋, 张鑫, 徐鹏翱, 刘芬, 范兴奎 2020 通信学报 **41** 190]

[51] Diaconis P, Rockmore D 1990 *J. Am. Math. Soc.* **3** 297

[52] Hsiao H C, Kim T J, Perring A, Yamada A 2012 *IEEE Secur. Privacy* **19** 506

Anonymous communication scheme based on quantum walk on Cayley graph*

He Zhen-Xing Fan Xing-Kui Chu Peng-Cheng Ma Hong-Yang †

(*School of Sciences, Qingdao University of Technology, Qingdao* 266033, *China*)

(Received 4 March 2020; revised manuscript received 1 May 2020)

Abstract

Information security is the cornerstone and lifeblood of national security in the information society, and anonymous quantum communication is one of the important ways to protect information security. Using quantum walk randomness to effectively solve sensitive problems such as leakage of identity information. In this paper, an anonymous communication scheme based on quantum walks on the Cayley graph is proposed. First, both parties in the communication hide their identity information, and the sender Alice anonymously selects the receiver Bob through logic or operation. Secondly, the trusted third party and the communicating parties use the BB84 protocol to generate and distribute the security key. Alice encrypts the information sequence according to the security key to obtain the blind information; Bob uses the joint Bell state measurement and security key to sign and the trusted third party verifies the signature information. Third, the trusted third party calculates the position probability distribution function of Bob's quantum walk via the Fourier transform, converts the position information corresponding to the maximum probability into a confirmation frame and sends it to Alice; Alice uses the quantum compression algorithm by decreasing dimensions to reduce the number of transmitted information bits(the length of the information bit can be reduced by up to 37.5%) and uses the security key to complete the information encryption and then transmit the information to the location indicated by the confirmation frame. Bob uses quantum walks to search the location node to obtain the transmission information and complete the anonymous quantum communication. Finally, the security analysis of the scheme is carried out, and the numerical simulation results of the Cayley graph of 200 nodes are given. At the 10-step walk, the maximal probability of the 6th node is 45.31%. According to the simulation results, the probability that Bob is eavesdropped on the specific location at his 10-step walk during the communication of this scheme is approximately 6×10^{-7}%, so the receiver can avoid the identity information from the eavesdropping with a high probability, and the quantum network anonymity protocol is not broken.

Keywords: anonymous quantum communication, quantum networks, quantum walk

PACS: 03.67.Ac, 03.67.Hk **DOI:** 10.7498/aps.69.20200333

* Project supported by the National Natural Science Foundation of China (Grant Nos. 11975132, 61772295), the Natural Science Foundation of Shandong Province, China (Grant No. ZR2019YQ01), and the Project of Higher Educational Science and Technology Program of Shandong Province, China (Grant No. J18KZ012).

† Corresponding author. E-mail: hongyang_ma@aliyun.com