物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于高维单粒子态的双向半量子安全直接通信协议

龚黎华　陈振泳　徐良超　周南润

Bi-directional semi-quantum secure direct communication protocol based on high-dimensional single-particle states

Gong Li-Hua　Chen Zhen-Yong　Xu Liang-Chao　Zhou Nan-Run

引用信息 Citation: Acta Physica Sinica, 71, 130304 (2022)　DOI: 10.7498/aps.71.20211702
在线阅读 View online: https://doi.org/10.7498/aps.71.20211702
当期内容 View table of contents: http://wulixb.iphy.ac.cn

基于高维单粒子态的双向半量子安全直接通信协议*

龚黎华 陈振泳 徐良超 周南润†

(南昌大学电子信息工程系, 南昌 330031)

(2021 年 9 月 12 日收到; 2022 年 3 月 14 日收到修改稿)

本文设计了一个基于高维单粒子态的双向半量子安全直接通信协议, 该协议包括量子方 Alice 和经典方 Bob, 每个参与方可以同时接收和发送秘密信息. 协议中的经典方 Bob 无需具备量子态检测能力, 因此该协议在现有技术条件下更易实现. 安全性分析表明: 在不被合法通信者发现的情况下, 截获重发、测量重发、篡改攻击以及纠缠攻击等常见攻击手段均无法获取秘密信息. 此外, 该协议利用高维单粒子态作为信息传输的载体, 这有效提高了秘密信息的传输效率.

关键词: 半量子安全直接通信, 高维单粒子态, 双向通信, 安全性分析

PACS: 03.67.–a, 03.67.HK **DOI:** 10.7498/aps.71.20211702

1 引 言

量子通信协议主要包括量子隐形传态 (quantum teleportation)[1–3]、量子密钥分配 (quantum key distribution, QKD)[4–6]、量子签名[7,8]、量子身份认证 (quantum identity authentication, QIA)[9]、量子秘密比较 (quantum private comparison, QPC)[10,11] 以及量子安全直接通信 (quantum secure direct communication, QSDC) 等. 近年量子芯片[12,13] 的快速发展, 有助于降低量子通信的成本.

量子安全直接通信在量子信息技术中扮演着重要的角色. 不同于量子密钥分配传输随机数, 量子安全直接通信无需密钥, 可以利用量子信道直接传输秘密信息. 2002 年, Long 和 Liu[14] 利用 Einstein-Podolsky-Rosen (EPR) 态的纠缠特性, 设计了第一个量子安全直接通信协议, Boström 和 Felbinger[15] 基于 EPR 对的纠缠特性提出了著名的乒乓协议 (ping-pong protocol, PPP). 2003 年, 以 EPR 对为信息载体, Deng 等[16] 提出了一个“两步”QSDC 协议. 2004 年, Deng 和 Long[17] 基于量子一次一密技术设计了一个 QSDC 协议. 2005 年, Wang 等[18] 基于高维量子超密编码构建了一个 QSDC 协议. 2011 年, Shi 等[19] 利用三维超纠缠性质设计了一个 QSDC 协议. 2017 年, Zheng 和 Long[20] 基于 Cluster 态提出了一个信道容量可控的 QSDC 方案. 2018 年, Chen 等[21] 利用 Bell 态的超纠缠特性构建了一个“三步”三方 QSDC 协议. 2019 年, Gao 等[22] 提出了测量设备无关的远程 QSDC 协议. 2020 年, Zhou 等[23] 提出了与设备无关的 QSDC 协议. 2022 年, 利用 Bell 态的超纠缠特性, Sheng 等[24] 构建了一个“一步”QSDC 协议. QSDC 的物理可实现性逐渐被实验所验证. 2016 年, Hu 等[25] 实现了基于单光子的 QSDC 实验. 2017 年, Zhang 等[26] 借助量子寄存器实验实现了“两步”QSDC 协议, 同年, Zhu 等[27] 实现了长距离 QSDC 实验. 2021 年, Qi 等[28]

* 国家自然科学基金 (批准号: 61871205) 资助的课题.

† 通信作者. E-mail: znr21@163.com

实现了 15 个用户之间的 QSDC 网络.

通常, 量子通信协议要求每一位参与者都具备完整的量子能力, 即参与者具备在量子比特或量子系统上进行量子操作的全部能力. 然而, 并不是每位参与者都能负担的起昂贵的量子设备. Boyer 等[29]最早提出了半量子的概念, 半量子意味着量子方拥有完整的量子能力, 而经典方不需具备完整的量子能力, 或者说经典方只能用一组固定的基 $\{|0\rangle, |1\rangle\}$ 处理量子信息. Zhou 等[30]指出半量子也可以保证量子中心与无量子能力的用户之间的通信安全. 半量子技术在量子通信的各个方向上都得到了应用, 例如: 半量子密钥分配 (semi-quantum key distribution, SQKD)[31,32]、半量子身份认证 (semi-quantum identity authentication, SQIA)[33]、半量子秘密比较 (semi-quantum private comparison, SQPC)[34,35] 以及半量子安全直接通信 (semi-quantum secure direct communication, SQSDC) 等.

半量子安全直接通信结合量子安全直接通信和半量子的思想, 为资源受限的经典方和具备完整量子能力的量子方之间提供了直接传输秘密信息的可靠方式. SQSDC 的提出不仅有利于提高量子通信协议的可实现性, 而且有利于减少量子通信中设备资源的消耗.

2014 年, Zou 等[36]讨论了半量子安全直接通信, 结合一次一密技术提出了一个基于单光子的“三步”SQSDC 协议. 随后, Gu 等[37]对该“三步”SQSDC 协议进行改进, 设计了一个可以抵御双重 C-NOT 攻击的 SQSDC 协议. 2017 年, Zhang 等[38]利用 EPR 对的纠缠特性和诱骗态思想, 提出了一个全新的 SQSDC 协议. 2018 年, Xie 等[39]将量子方和经典方的职责互换, 以 Bell 态为信息载体设计了一个信息发送者为量子方的 SQSDC 协议. 2019 年, Sun 等[40]通过引入新的编码手段提出了两个基于 Bell 态的高效 SQSDC 协议. 2020 年, Rong 等[41]利用 Bell 态纠缠特性, 设计了一种多参与方的 SQSDC 协议.

然而, 现有的半量子安全直接通信协议只使用二维量子态作为信息的载体, 并要求经典方具备量子态测量能力. 为了突破低维量子态的限制, 提高信息传输效率、减少量子资源的消耗和降低协议的实现难度, 本文基于高维单粒子态设计了一个双向 SQSDC 协议.

2 高维单粒子态

d 维量子系统中的 Z 基和 X 基的定义 $\overline{Z}$ 和 $\overline{X}$ 分别为

$$\overline{Z} = \{|k\rangle \,|k = 0, 1, \cdots, d-1.\}, \tag{1}$$

$$\overline{X} = \{F\,|k\rangle \,|k = 0, 1, \cdots, d-1.\}, \tag{2}$$

其中 $F\,|k\rangle = |F_k\rangle = \dfrac{1}{\sqrt{d}} \sum_{j=0}^{d-1} w^{jk}\,|j\rangle$, $w = \mathrm{e}^{\frac{2\pi \mathrm{i}}{d}}$, F 为量子傅里叶变换. 在本协议中, 经典方 Bob 以 d 维单粒子态作为传输秘密信息的载体, 被限制只能对粒子执行以下几种操作: 1) 不做任何操作 CTRL; 2) 进行幺正操作 U_m; 3) 进行重新排序. Bob 执行的幺正操作为

$$U_m = \sum_{r=0}^{d-1} |r \oplus m\rangle \langle r|, m = 0, 1, \cdots, d-1, \tag{3}$$

其中 $\oplus$ 为模 d 加. Ye 等[42]指出当对 $\overline{Z}$ 基粒子 $|k\rangle$ 执行幺正操作 U_m 时, 它的量子态将会变成 $|k \oplus m\rangle$, 而当对 $\overline{X}$ 基粒子进行幺正操作 U_m 时其状态不会改变.

3 协议描述

在无噪声、无失真的理想环境中, 拥有完整量子能力的量子方 Alice 和能力受限的经典方 Bob (无需具备量子态测量能力) 之间基于高维单粒子态的双向半量子安全直接通信协议的具体步骤如下:

步骤 1 Alice 随机制备 $4n$ 个 $\overline{Z}$ 基粒子和 n 个 $\overline{X}$ 基粒子, n 为 Alice 和 Bob 在一次通信过程中需传输的秘密信息长度. Alice 将 $\overline{X}$ 基粒子随机插入 $\overline{Z}$ 基粒子序列中得到序列 S_T, 并将其发送给 Bob.

步骤 2 Bob 收到序列 S_T 后, 对粒子随机执行 CTRL 或幺正操作 U_m 并记录 m 的值得到序列 S_{T_1}. Bob 通过不同的延时线对所有粒子进行重新排序得到序列 S'_{T_1}, 并将其返还 Alice. 根据粒子的原始状态和 Bob 的操作, 可将所得的粒子归为四类, 如表 1 所列.

步骤 3 Alice 收到序列 S'_{T_1} 后, 公布原始序列中 $\overline{Z}$ 基粒子的位置. Bob 公布序列 S'_{T_1} 的正确顺序和对每个粒子执行的操作, 并随机公布一半对 $\overline{Z}$ 基粒子执行的幺正操作信息. Alice 恢复粒子序列的

正确顺序, 并按照粒子发送时的基测量粒子, 结果如表 2 所列. Alice 比对每个收到粒子的测量结果和预期结果, 计算误码率. 若误码率高于预设的阈值, 则说明窃听存在, 终止本次协议, 否则 Alice 将剩余未公布幺正操作的 $\overline{Z}-U$ 粒子作为媒介粒子(媒介粒子组成的序列记为 S_m), 并通过比对测量结果读出媒介粒子 S_m 的幺正操作信息 m.

表 1 操作后粒子的分类

Table 1. Classification of the particles after operation.

原始状态所属基	Bob的操作	标记为
$\overline{Z}$	CTRL	$\overline{Z}-$CTRL
$\overline{Z}$	U_m	$\overline{Z}-U$
$\overline{X}$	CTRL	$\overline{X}-$CTRL
$\overline{X}$	U_m	$\overline{X}-U$

表 2 Alice 的窃听检测策略

Table 2. Eavesdropping detection strategy for Alice.

原始状态	Bob的操作	Alice的操作	预期结果
$\|k\rangle$	CTRL	$\overline{Z}$ 基测量	$\|k\rangle$
$\|k\rangle$	U_m	$\overline{Z}$ 基测量	$\|k\oplus m\rangle$
$F\|k\rangle$	CTRL	$\overline{X}$ 基测量	$F\|k\rangle$
$F\|k\rangle$	U_m	$\overline{X}$ 基测量	$F\|k\rangle$

步骤 4 根据自己的秘密信息 $m_{\rm a}$ 和 Bob 的幺正操作信息 m, Alice 计算 $M_{\rm a}=m\oplus m_{\rm a}$. Alice 根据 $M_{\rm a}$ 制备 n 个 $\overline{Z}$ 基粒子得到序列 S_C, 并将之发送给 Bob.

步骤 5 根据自己的秘密信息 $m_{\rm b}$ 和幺正操作信息 m, Bob 计算 $M_{\rm b}=m\oplus m_{\rm b}$. 在收到序列 S_C 后, Bob 根据 $M_{\rm b}$ 对粒子执行幺正操作 $U_{M_{\rm b}}$ 得到序列 S_{C1}, 并将其返还 Alice.

步骤 6 Alice 收到序列 S_{C_1} 后, 用 $\overline{Z}$ 基对其进行测量, 并公布测量结果 $M=M_{\rm a}\oplus M_{\rm b}$.

步骤 7 根据测量结果 $M=M_{\rm a}\oplus m_{\rm b}\oplus m$ $(M=M_{\rm b}\oplus m_{\rm a}\oplus m)$, Alice (Bob) 获得 Bob (Alice) 的秘密信息 $m_{\rm b}=M\ominus M_{\rm a}\ominus m\,(m_{\rm a}=M\ominus M_{\rm b}\ominus m)$, 其中 $\ominus$ 为模 d 减.

步骤 8 Alice(Bob) 利用哈希函数 $h()$ 分别计算出秘密信息 $m_{\rm a}\,(m_{\rm b})$ 的哈希值 $h(m_{\rm a})\,(h(m_{\rm b}))$ 和收到秘密信息 $m'_{\rm b}\,(m'_{\rm a})$ 的哈希值 $h(m'_{\rm b})\,(h(m'_{\rm a}))$. Alice 和 Bob 分别公布自己秘密信息的哈希值. 如果 $h(m'_{\rm b})=h(m_{\rm b})$ $(h(m'_{\rm a})=h(m_{\rm a}))$, 则 Alice(Bob) 收到的秘密信息准确无误. 否则, 收到的秘密信息有误, Alice 和 Bob 将丢弃收到的秘密信息并重新执行协议.

4 安全性分析

4.1 截获重发攻击

Eve 截获并用提前制备的欺诈粒子替换 Alice 发送给 Bob 的每个粒子, 并在 Bob 将粒子返回给 Alice 时再次截获粒子. 通过测量欺诈粒子并比对测量结果与欺诈粒子的原始状态, Eve 试图获取 Bob 的操作信息, 并通过执行与 Bob 相同的操作以窃听秘密信息. 在截获重发攻击中, Eve 可以选择 $\overline{Z}$ 基粒子或 $\overline{X}$ 基粒子作为欺诈粒子, 具体情况如下:

1) Eve 选择 $\overline{Z}$ 基粒子作为欺诈粒子

在截获 Alice 传来的粒子后, Eve 将提前制备的 $\overline{Z}$ 基粒子发送给 Bob. Bob 只能对收到的粒子执行 CTRL 或幺正操作 U_m. CTRL 和幺正操作 U_0 不会改变 $\overline{Z}$ 基粒子的状态, 其他幺正操作会改变 $\overline{Z}$ 基粒子的状态. Eve 对返回的 $\overline{Z}$ 基粒子进行 $\overline{Z}$ 基测量, 当 $\overline{Z}$ 基粒子的状态不变时, Eve 对截获的相应粒子执行 CTRL. 当 $\overline{Z}$ 基粒子的状态改变时, Eve 对截获的粒子执行对应的幺正操作 U_m. Eve 将操作后的粒子序列 S_T 返回给 Alice. Alice 收到返回的粒子后, 根据 Bob 公布的信息进行窃听检测. Bob 在完成对粒子的操作后对所有的粒子进行重新排序, Eve 通过测量欺诈粒子获取的操作信息将无法与 S_T 中的粒子相对应, 即 Eve 必然会对截获的粒子进行错误操作. 根据表 2 中的窃听检测规则, Eve的窃听行为将以大概率被 Alice 发现, 如表 3 所列.

2) Eve 选择 $\overline{X}$ 基粒子作为欺诈粒子

在截获 Alice 传来的粒子后, Eve 将提前制备的 $\overline{X}$ 基粒子发送给 Bob. Bob 对收到的粒子只能执行 CTRL 或幺正操作 U_m. 这两种操作都无法改变 $\overline{X}$ 基粒子的状态. 当 Eve 对返回的 $\overline{X}$ 基粒子进行 $\overline{X}$ 基测量时, 所有 $\overline{X}$ 基粒子都维持原始状态. Eve 无法从中获得 Bob 的操作信息, 只能对截获的粒子进行随机操作并将其返还 Alice. 这会增大误码率进而被 Alice 发现.

无论是选择 $\overline{X}$ 基粒子或 $\overline{Z}$ 基粒子作为欺诈粒子, Eve 的截获重发攻击都无法在不被发现的情况下成功窃取秘密信息. 因此, 本协议可以抵御截获重发攻击.

表 3 Eve 的截获重发攻击

Table 3. Intercept-resend attack by Eve.

Alice发送的粒子	Bob的操作	Eve的操作	Alice的操作	窃听是否会被发现
$\overline{Z}$	CTRL	CTRL	用 $\overline{Z}$ 基测量	否
$\overline{Z}$	CTRL	U_m	用 $\overline{Z}$ 基测量	是
$\overline{Z}$	U_m	CTRL	用 $\overline{Z}$ 基测量	$\frac{d-1}{2d}$ 的概率被发现
$\overline{Z}$	U_m	U_m	用 $\overline{Z}$ 基测量	$\frac{d-1}{2d}$ 的概率被发现
$\overline{X}$	CTRL	CTRL	用 $\overline{X}$ 基测量	否
$\overline{X}$	CTRL	U_m	用 $\overline{X}$ 基测量	否
$\overline{X}$	U_m	CTRL	用 $\overline{X}$ 基测量	否
$\overline{X}$	U_m	U_m	用 $\overline{X}$ 基测量	否

4.2 测量重发攻击

在测量重发攻击中, Eve 截获并测量每一个由 Alice 发送给 Bob 的粒子, 并制备与测量结果相同状态的新粒子发送给 Bob. 在 Bob 将粒子返回给 Alice 时, Eve 再次截获并用与之前相同的基测量粒子, 试图获取秘密信息. 在发送 $\overline{Z}$ 基粒子时, Alice 在其中混入了 $\overline{X}$ 基粒子作为诱骗态, 因此 Eve 在对截获的粒子进行测量时, 必须使用 $\overline{X}$ 和 $\overline{Z}$ 两种测量基测量粒子. 然而, Eve 无法准确区分每个粒子所属的基, 只能随机选择测量基. 当测量基与 Alice 发送的粒子不匹配时, Eve 的窃听行为将大概率被 Alice 发现. 为了更清晰地展示 Eve 的攻击对整个通信过程的影响, 表 4 列出了窃听者和合法参与者在执行不同操作后产生的结果.

1) Alice 发送的是 $\overline{Z}$ 基粒子而 Eve 选择 $\overline{Z}$ 基进行测量

Eve 选择的测量基与 Alice 发送粒子的基相同, 且 Bob 的操作不会改变粒子的基. 当 Alice 测量返回的粒子时, 无法发现 Eve 的窃听.

2) Alice 发送的是 $\overline{Z}$ 基粒子而 Eve 选择 $\overline{X}$ 基进行测量

Eve 的 $\overline{X}$ 基测量使得 Alice 发送的粒子坍缩为 $\overline{X}$ 基粒子. Bob 的操作不会改变粒子的基, 因此返回给 Alice 的粒子仍然为 $\overline{X}$ 基. 当 Bob 选择执行 CTRL 操作时, Alice 将以概率 $(d-1)/d$ 发现 Eve 的窃听. 当 Bob 选择执行幺正操作 U_m 时, 因为 Bob 只公布一半的 $\overline{Z}-U$ 粒子, Alice 将以概率 $(d-1)/2d$ 发现 Eve 的窃听.

3) Alice 发送的是 $\overline{X}$ 基粒子而 Eve 选择 $\overline{Z}$ 基进行测量

Eve 的 $\overline{Z}$ 基测量使得 Alice 发送的粒子坍缩为 $\overline{Z}$ 基粒子. Bob 的操作不会改变粒子的基, 因此返回给 Alice 的粒子仍然为 $\overline{Z}$ 基. Alice 将以概率 $(d-1)/d$ 发现 Eve 的窃听.

4) Alice 发送的是 $\overline{X}$ 基粒子而 Eve 选择 $\overline{X}$ 基进行测量

表 4 Eve 的测量重发攻击

Table 4. Measurement-resend attack by Eve.

Alice发送的粒子	Eve的测量基	Bob得到的粒子	Bob的操作	Alice的操作	窃听是否被发现
$\overline{Z}$	$\overline{Z}$	$\overline{Z}$	CTRL	$\overline{Z}$ 基测量	否
$\overline{Z}$	$\overline{Z}$	$\overline{Z}$	U_m	$\overline{Z}$ 基测量	否
$\overline{Z}$	$\overline{X}$	$\overline{X}$	CTRL	$\overline{Z}$ 基测量	$\frac{d-1}{d}$ 概率被发现
$\overline{Z}$	$\overline{X}$	$\overline{X}$	U_m	$\overline{Z}$ 基测量	$\frac{d-1}{2d}$ 概率被发现
$\overline{X}$	$\overline{Z}$	$\overline{Z}$	CTRL	$\overline{X}$ 基测量	$\frac{d-1}{d}$ 概率被发现
$\overline{X}$	$\overline{Z}$	$\overline{Z}$	U_m	$\overline{X}$ 基测量	$\frac{d-1}{d}$ 概率被发现
$\overline{X}$	$\overline{X}$	$\overline{X}$	CTRL	$\overline{X}$ 基测量	否
$\overline{X}$	$\overline{X}$	$\overline{X}$	U_m	$\overline{X}$ 基测量	否

Eve 选择的测量基与 Alice 发送粒子的基相同, 且 Bob 的操作不会改变粒子的基. 当 Alice 对返回的粒子进行测量时, 无法发现 Eve 的窃听.

显然, 对于 Eve 的测量重发攻击, 合法通信者将以概率 $p=1-\left(\frac{2}{5d}+\frac{3}{5}\right)^{N_1}$ 检测到 Eve 的窃听行为, 其中 N_1 为粒子总数, d 为粒子所属希尔伯特空间的维数. 如图 1 所示, 随着粒子总数 N_1 以及高维单粒子态维数 d 的逐渐增大, Eve 被发现的概率 p 也将不断增加. 当 N_1 和 d 足够大时, 概率 p 趋近于 1.

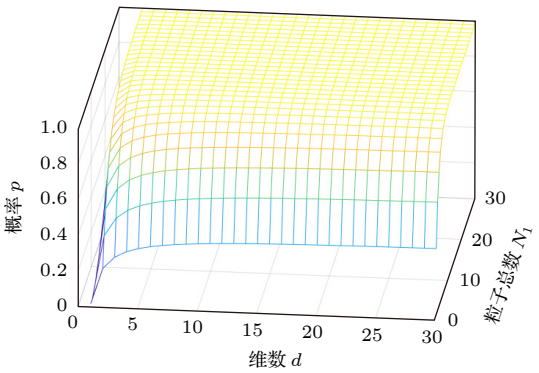

图 1 窃听检测概率

Fig. 1. Eavesdropping detection probability.

4.3 纠缠测量攻击

Eve 在 Alice 发送粒子给 Bob 时, 对每一粒子执行幺正操作 $U_{\rm E}$, 将制备的辅助粒子 $|\varepsilon\rangle$ 与 Alice 的粒子纠缠在一起, 测量辅助粒子可以提取有用信息. 当 Eve 对 Z 基粒子执行幺正操作 $U_{\rm E}$ 时可得

$$\begin{aligned} U_{\rm E}|k\rangle|\varepsilon\rangle &= \lambda_{k0}|0\rangle|\varepsilon_{k0}\rangle+\lambda_{k1}|1\rangle|\varepsilon_{k1}\rangle+\cdots \\ &\quad +\lambda_{k,d-1}|d-1\rangle|\varepsilon_{k,d-1}\rangle \\ &= \sum_{t=0}^{d-1}\lambda_{kt}|t\rangle|\varepsilon_{kt}\rangle, \end{aligned} \tag{4}$$

其中 $k=0,1,\cdots,d-1$, $\sum_{t=0}^{d-1}|\lambda_{kt}|^2=1$, 且有 $\langle\varepsilon_m|\varepsilon_n\rangle=\begin{cases}1, m=n,\\ 0, m\neq n.\end{cases}$ 当 Eve 对 X 基粒子执行幺正操作 $U_{\rm E}$ 时可得

$$\begin{aligned} U_{\rm E}|F_k\rangle|\varepsilon\rangle &= U_{\rm E}F|k\rangle|\varepsilon\rangle \\ &= U_{\rm E}\left(\frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}w^{kl}|l\rangle\right)|\varepsilon\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}w^{kl}\left(U_E|l\rangle|\varepsilon\rangle\right) \\ &= \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}w^{kl}\left(\sum_{j=0}^{d-1}\lambda_{lj}|j\rangle|\varepsilon_{lj}\rangle\right) \\ &= \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}w^{kl}\sum_{j=0}^{d-1}\lambda_{lj}\left(\frac{1}{\sqrt{d}}\sum_{\xi=0}^{d-1}w^{-\xi j}|F_\xi\rangle|\varepsilon_{lj}\rangle\right) \\ &= \frac{1}{d}\lambda_{lj}\sum_{l,j,\xi=0}^{d-1}w^{kl-\xi j}|F_\xi\rangle|\varepsilon_{lj}\rangle, \end{aligned} \tag{5}$$

其中 $\sum_{j=0}^{d-1}|\lambda_{lj}|^2=1$, $\langle\varepsilon_m\mid\varepsilon_n\rangle=\begin{cases}1, m=n;\\ 0, m\neq n.\end{cases}$ 无论 Bob 执行 CTRL 或 U_m, 他都无需测量 Alice 发送的粒子, 这意味着不会破坏 (4) 式和 (5) 式中纠缠粒子对的纠缠性. 在 Bob 将粒子返回给 Alice 时, Eve 对返回的粒子执行另一幺正操作 $U_{\rm G}$. 对于 Z 基粒子, 根据 Bob 的操作其状态将分别变为

$$\begin{aligned} & U_{\rm G}U_E|k\rangle|\varepsilon\rangle \\ &= a_{k0}|0\rangle|\varepsilon_{k0}\rangle+a_{k1}|1\rangle|\varepsilon_{k1}\rangle+\cdots \\ &\quad +a_{k,d-1}|d-1\rangle|\varepsilon_{k,d-1}\rangle \\ &= \sum_{t=0}^{d-1}a_{kt}|t\rangle|\varepsilon_{kt}\rangle, \end{aligned} \tag{6}$$

$$\begin{aligned} & U_{\rm G}U_mU_{\rm E}|k\rangle|\varepsilon\rangle \\ &= U_m(a_{k0}|0\rangle|\varepsilon_{k0}\rangle+a_{k1}|1\rangle|\varepsilon_{k1}\rangle+\cdots \\ &\quad +a_{k,d-1}|d-1\rangle|\varepsilon_{k,d-1}\rangle) \\ &= \sum_{t=0}^{d-1}a_{kt}|t\oplus m\rangle|\varepsilon_{kt}\rangle. \end{aligned} \tag{7}$$

其中 $\sum_{t=0}^{d-1}|a_{kt}|^2=1$, $\langle\varepsilon_m|\varepsilon_n\rangle=\begin{cases}1, m=n,\\ 0, m\neq n.\end{cases}$ Eve 必须使得 Alice 的测量结果与预期结果保持一致才能不被 Alice 检测到, 即 $k\neq t$ 时, $a_{kt}=0$, 即必须满足:

$$U_{\rm G}U_mU_{\rm E}|k\rangle|\varepsilon\rangle=a_{kk}|k\oplus m\rangle|\varepsilon_{kk}\rangle, \tag{8}$$

$$U_{\rm G}U_{\rm E}|k\rangle|\varepsilon\rangle=a_{kk}|k\rangle|\varepsilon_{kk}\rangle. \tag{9}$$

Bob 的两个操作都无法改变 X 基粒子的状态, X 基粒子在 Eve 执行 $U_{\rm E}$ 和 $U_{\rm G}$ 后可以表示为

$$\begin{aligned} & U_{\rm G}U_mU_{\rm E}|F_k\rangle|\varepsilon\rangle \\ &= U_{\rm G}U_{\rm E}|F_k\rangle|\varepsilon\rangle=U_{\rm G}U_{\rm E}F|k\rangle|\varepsilon\rangle \\ &= U_{\rm G}U_{\rm E}\left(\frac{1}{\sqrt{d}}\sum_{r=0}^{d-1}w^{kr}|r\rangle\right)|\varepsilon\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{r=0}^{d-1}w^{kr}U_{\rm G}U_{\rm E}|r\rangle|\varepsilon\rangle, \end{aligned} \tag{10}$$

结合 (9) 式和 (10) 式可得

$$\begin{aligned} & U_{\mathrm{G}}U_mU_{\mathrm{E}}\left|F_k\right\rangle\left|\varepsilon\right\rangle = U_{\mathrm{G}}U_{\mathrm{E}}\left|F_k\right\rangle\left|\varepsilon\right\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{r=0}^{d-1} w^{kr}a_{rr}\left|r\right\rangle\left|\varepsilon_{rr}\right\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{r=0}^{d-1} w^{kr}\left[a_{rr}\left(\frac{1}{\sqrt{d}}F^{-1}\left|F_y\right\rangle\right)\left|\varepsilon_{rr}\right\rangle\right] \\ &= \frac{1}{\sqrt{d}}\sum_{r=0}^{d-1} w^{kr}\left[a_{rr}\left(\frac{1}{\sqrt{d}}\sum_{y=0}^{d-1} w^{-ry}\left|F_y\right\rangle\right)\left|\varepsilon_{rr}\right\rangle\right] \\ &= \frac{1}{d}\sum_{r,y=0}^{d-1} w^{r(k-y)}a_{rr}\left|F_y\right\rangle\left|\varepsilon_{rr}\right\rangle . \end{aligned} \tag{11}$$

F^{-1}为量子傅里叶逆变换. 为了避免被 Alice 发现, Eve 必须使 Alice 的测量结果与发送的粒子态相同, 即$|F_y\rangle$必须等于$|F_k\rangle$. 由此可得

$$\sum_{r,y=0}^{d-1} w^{r(k-y)}a_{rr}\left|F_y\right\rangle\left|\varepsilon_{rr}\right\rangle = 0, k\neq y. \tag{12}$$

由 (11) 式及 (12) 式, 可得

$$a_{00}\left|\varepsilon_{00}\right\rangle = a_{11}\left|\varepsilon_{11}\right\rangle = \cdots = a_{d-1,d-1}\left|\varepsilon_{d-1,d-1}\right\rangle . \tag{13}$$

由 (13) 式可知, Eve 无法区分辅助态$|\varepsilon_{00}\rangle$, $|\varepsilon_{11}\rangle$, $\cdots$, $|\varepsilon_{d-1,d-1}\rangle$, 即无法获得 Alice 和 Bob 的秘密信息. 因此, 本协议可以抵抗纠缠攻击.

4.4 篡改攻击

通过对粒子执行幺正操作$U_n=\sum_{r=0}^{d-1}\left|r\oplus n\right\rangle\left\langle r\right|$, $n=0,1,\cdots,d-1$, Eve 试图篡改 Alice 和 Bob 之间传输的秘密信息, 使合法通信者获得错误的秘密信息. 如果合法通信者无法检测到 Eve 的操作或未检测出秘密信息被篡改, 则攻击成功. 当 Eve 的攻击执行在 $\overline{X}$ 基粒子上时, $\overline{X}$ 基粒子不会发生改变, 因此 Eve 的操作不会篡改秘密信息. 当 Eve 的攻击发生在 $\overline{Z}$ 基粒子上时, 可得

$$U_n\left|k\right\rangle = \left|k\oplus n\right\rangle . \tag{14}$$

显然, 如果 Bob 选择执行 CTRL 操作, Alice 会发现粒子的测量结果与预期结果不同. 如果 Bob 选择执行U_m操作并且公布相应的m值, Alice 的测量结果将为$|k\oplus n\oplus m\rangle$而非预期的$|k\oplus m\rangle$. 如果 Bob 选择执行$U_m$操作而未公布相应的$m$值, 则被篡改的粒子将作为媒介粒子. Alice 获取的媒介粒子信息为$n\oplus m$将不同于 Bob 的m, 当协议进行到差错检测步骤时, Alice 通过哈希函数获得的秘密信息检测值将与 Bob 的不同, 参与者将发现秘密信息被篡改. 因此, 无论 Eve 的篡改攻击发生在协议中的哪一种粒子上, 都无法在不被发现的情况下篡改秘密信息. 因此, 本协议可以抵抗篡改攻击.

5 效率分析

量子通信协议的效率计算式为[43]

$$\eta = \frac{b_{\mathrm{s}}}{q_{\mathrm{t}}+q_{\mathrm{s}}}, \tag{15}$$

其中b_{s}, q_{t}, q_{s}分别表示传递秘密信息的数量, 协议使用的量子比特总数和协议中所需经典比特数量. 本协议中 Alice 共制备了$6n$个d维单粒子态而 Bob 在整个通信进程中未制备任何量子态, 即$q_{\mathrm{t}}=6n$. Alice 和 Bob 在译码阶段共使用了n个经典比特读取彼此的秘密信息, 即$q_{\mathrm{s}}=n$. 在一次通信进程中, Alice 和 Bob 分别向对方传递了n个d维单粒子态的秘密信息, 即$b_{\mathrm{s}}=2n$. 因此本协议的效率为$\frac{2n}{6n+n}\times 100\% = 28.6\%$. 本协议以$d$维单粒子为信息的传输载体, 每一个单粒子可以传输$\log_2 d$比特的秘密信息. 图 2 为维数与单粒子传输秘密信息量的关系, 易知, 随着维数d的不断增加, 单粒子可以传输更多的秘密信息.

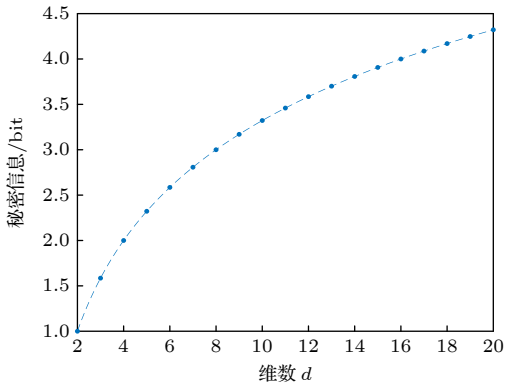

图 2 单粒子传输秘密信息-维数

Fig. 2. Single particle transport secret information - dimension.

现有的 SQSDC 协议通常是基于低维单粒子态或低维纠缠态, 每个粒子只能编码 1 比特的秘密信息, 秘密信息的传输效率不高, 本文首次基于高维量子态实现 SQSDC 协议, 当维数足够大时, 将明显提高秘密信息的传输效率. 现有的 SQSDC 协

表 5 本协议与现有经典 SQSDC 协议的比较

Table 5. Comparison of the proposed protocol with existing classical SQSDC protocols.

协议	文献[36]	文献[38]	协议一[40]	协议二[40]	本文协议
量子载体	二维单粒子态	二维Bell态	二维Bell态	二维Bell态	d 维单粒子态
通信模式	单向	单向	单向	单向	双向
经典方是否需要测量能力	是	是	是	是	否
每粒子传输秘密信息(bit)	1	1	1	1	$\log_2 d$
量子通信协议效率(%)	14.3	19.0	16.7	28.6	28.6

议中一般要求经典方具备量子态测量能力, 本协议中经典方无需具备量子测量能力, 这降低了协议的实现难度. 此外, 本协议是一个双向通信协议, 在一次通信进程中两个参与者都可以同时发送和接收秘密信息. 本协议与一些现有 SQSDC 协议的详细比较如表 5 所列. 与现有的 SQSDC 协议相比, 本文协议具有更高的秘密信息传输效率.

6 总 结

本文提出的基于高维单粒子态的双向半量子安全直接通信协议中的合法参与者为量子方 Alice 和经典方 Bob, 每个参与者既是秘密信息发送方, 又是秘密信息接收方. 本文协议中的经典方 Bob 无需具备量子态测量能力, 这降低了协议对于量子设备的需求. 安全性分析表明, 本文协议可以抵抗测量重发攻击、截获重发攻击和纠缠测量攻击等常见攻击手段. 此外, 每个 d 维粒子可以编码 $\log_2 d$ 比特的秘密信息而每个二维量子比特只能编码 1 比特的秘密信息, 因此, 与基于二维量子比特的单向半量子安全通信协议相比, 当 d 足够大时本协议具有更高的秘密信息传输效率.

参考文献

[1] Bennett C H, Brassard G, Crepeau C, Jozsa R, Peres A, Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895

[2] Li X H, Ghose S 2015 *Phys. Rev. A* **91** 012320

[3] Yang L, Ma H Y, Zheng C, Ding X L, Gao J C, Long G L 2017 *Acta Phys. Sin.* **66** 230303 (in Chinese) [杨璐, 马鸿洋, 郑超, 丁晓兰, 高健存, 龙桂鲁 2017 物理学报 **66** 230303]

[4] Vlachou C, Krawec W, Mateus P, Paunković N, Souto A 2018 *Quantum Inf. Process.* **17** 288

[5] Wu C F, Du Y N, Wang J D, Wei Z J, Qin X J, Zhao F, Zhang Z M 2016 *Acta Phys. Sin.* **65** 100302 (in Chinese) [吴承峰, 杜亚男, 王金东, 魏正军, 秦晓娟, 赵峰, 张智明 2016 物理学报 **65** 100302]

[6] An X B, Yin Z Q, Han Z F 2015 *Acta Phys. Sin.* **64** 140303 (in Chinese) [安雪碧, 银振强, 韩正甫 2015 物理学报 **64** 140303]

[7] Feng Y Y, Shi R H, Shi J J, Guo Y 2019 *Acta Phys. Sin.* **68** 120302 (in Chinese) [冯艳艳, 施荣华, 石金晶, 郭迎 2019 物理学报 **68** 120302]

[8] Rong M X, Xin X J, Li F G 2020 *Acta Phys. Sin.* **69** 190302 (in Chinese) [荣民希, 辛向军, 李发根 2020 物理学报 **69** 190302]

[9] Zhang P, Zhou X Q, Li Z W 2014 *Acta Phys. Sin.* **63** 130301 (in Chinese) [张沛, 周小清, 李智伟 2014 物理学报 **63** 130301]

[10] Chen F L, Zhang H, Chen S G, Cheng W T 2021 *Quantum Inf. Process.* **20** 178

[11] Jiang D H, Tang K K, Xu G B 2021 *Int. J. Theor. Phys.* **60** 4122

[12] Ma Z H, Chen J Y, Li Z, Tang C, Sua Y M, Fan H, Huang Y P 2020 *Phys. Rev. Lett.* **125** 263602

[13] Wang Q Q, Zheng Y, Zhai C H, Li X D, Gong Q H, Wang J W 2021 *J. Semicond.* **42** 091901

[14] Long G L, Liu X S 2002 *Phys. Rev. A* **65** 032302

[15] Boström K, Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[16] Deng F G, Long G L, Liu X S 2003 *Phys. Rev. A* **68** 042317

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

[18] Wang C, Deng F G, Li Y S, Liu X S, Long G L 2005 *Phys. Rev. A* **71** 044305

[19] Shi J, Gong Y X, Xu P, Zhu S N, Zhan Y B 2011 *Commun. Theor. Phys.* **56** 831

[20] Zheng X Y, Long Y X 2017 *Acta Phys. Sin.* **66** 180303 (in Chinese) [郑晓毅 龙银香 2017 物理学报 **66** 180303]

[21] Chen S S, Zhou L, Zhong W, Sheng Y B 2018 *Sci. Chin. - Phys. Mech. Astron.* **61** 90312

[22] Gao Z K, Li T, Li Z H 2019 *EPL* **125** 40004

[23] Zhou L, Sheng Y B, Long G L 2020 *Sci. Bull.* **65** 12

[24] Sheng Y B, Zhou L, Long G L 2022 *Sci. Bull.* **67** 367

[25] Hu J Y, Yu B, Jing M Y, Xiao L T, Jia S T, Qin G Q, Long G L 2016 *Light Sci. Appl.* **5** e16144

[26] Zhang W, Ding D S, Sheng Y B, Zhou L, Shi B S, Guo G C 2017 *Phys. Rev. Lett.* **118** 220501

[27] Zhu F, Zhang W, Sheng Y B, Huang Y D 2017 *Sci. Bull.* **62** 1519

[28] Qi Z T, Li Y H, Huang Y W, Feng J, Zheng Y L, Chen X F 2021 *Light Sci. Appl.* **10** 183

[29] Boyer M, Kenigsberg D, Mor T 2007 *Phys. Rev. Lett.* **99** 140501

[30] Zhou N R, Zhu K N, Bi W, Gong L H 2019 *Quantum Inf. Process.* **18** 197

[31] Tsai C W, Yang C W 2021 *Sci. Rep.* **11** 23222

[32] Han S Y, Huang Y T, Mi S, Qin X J, Wang J D, Yu Y F, Wei Z J, Zhang Z M 2021 *EPJ Quantum Technol.* **8** 28

[33] Jiang S Q, Zhou R G, Hu W W 2021 *Int. J. Theor. Phys.* **60** 3353

[34] Zhou N R, Xu Q D, Du N S, Gong L H 2021 *Quantum Inf. Process.* **20** 124

[35] Ye C Q, Li J, Chen X B, Yuan T 2021 *Quantum Inf. Process.*

20 262
[36] Zou X F, Qiu D W 2014 *Sci. Chin. -Phys. Mech. Astron.* **57** 1696
[37] Gu J, Lin P H, Hwang T 2018 *Quantum Inf. Process.* **17** 182
[38] Zhang M H, Li H F, Xia Z Q, Feng X Y, Peng J Y 2017 *Quantum Inf. Process.* **16** 117
[39] Xie C, Li L Z, Situ H Z, He J H 2018 *Int. J. Theor. Phys.* **57** 1881
[40] Sun Y H, Yan L L, Chang Y, Zhang S B, Shao T T, Zhang Y 2019 *Mod. Phys. Lett. A* **34** 1950004
[41] Rong Z B, Qiu D W, Zou X F 2020 *Int. J. Theor. Phys.* **59** 1807
[42] Ye C Q, Ye T Y, He D, Gan Z G 2019 *Int. J. Theor. Phys.* **58** 3797
[43] Wen X J, Zhao X Q, Gong L H, Zhou N R 2019 *Laser Phys. Lett.* **16** 075206

Bi-directional semi-quantum secure direct communication protocol based on high-dimensional single-particle states*

Gong Li-Hua Chen Zhen-Yong Xu Liang-Chao Zhou Nan-Run †

(*Department of Electronics Information Engineering, Nanchang University, Nanchang* 330031, *China*)

(Received 12 September 2021; revised manuscript received 14 March 2022)

Abstract

Semi-quantum secure direct communication allows the quantum party and the classical party to transmit secure messages directly, but does not need sharing a secret key in advance. To increase the information transmission efficiency and practicability of semi-quantum secure direct communication, a bidirectional semi-quantum secure direct communication protocol with high-dimensional single-particle states is designed. The proposed protocol involves quantum party Alice and classical party Bob. Each participant can receive a secret message while sending a secret message. Unlike most of existing quantum secure direct communication protocols, it is not necessary for the classical party Bob in the proposed protocol to possess the capability of measuring quantum states, which greatly enhances the feasibility of the protocol. The protocol allows the classical party Bob to implement the unitary operations on particles and reorder the quantum sequence. Furthermore, the quantum party Alice and the classical party Bob can verify the correctness of the received secret message with the Hash function. Security analysis indicates that without being discovered by the legitimate participants, Eve cannot obtain the secret message with common attack, such as intercept-resend attack, measure-resend attack, tampering attack and entanglement-measure attack. Compared with the typical semi-quantum secure direct communication protocols, the proposed protocol has a high qubit efficiency of about 28.6%. In addition, the transmission efficiency of secret message is greatly enhanced, since the proposed protocol utilizes the high-dimensional single-particle states as the carrier of secret message.

Keywords: semi-quantum secure direct communication, high-dimensional single-particle state, bi-directional communication, security analysis

PACS: 03.67.–a, 03.67.HK **DOI:** 10.7498/aps.71.20211702

* Project supported by the National Natural Science Foundation of China (Grant No. 61871205).

† Corresponding author. E-mail: znr21@163.com