DOI: 10.3969/j.issn.1007-5461.2023.05.013

基于GHZ态的多方半量子安全直接通信

郭 瀚， 李云霞， 魏家华*， 唐 杰， 王俊辉

(空军工程大学信息与导航学院， 陕西 西安 710077)

摘 要: 量子安全直接通信不需要提前准备密钥, 直接通过量子就可以进行秘密信息传递。针对量子通信设备成本较高的问题, 基于 Greenberger-Horne-Zeilinger (GHZ) 态粒子和半量子理论, 提出了一个双向三方的半量子安全直接通信 (SQSDC) 方案。该方案可以实现两个经典方和一个量子方之间的秘密通信, 且通过调整GHZ态粒子的个数，可以将经典方扩展至任意多方, 因此尤其适用于一个上级单位和多个下级单位之间的通信。方案安全性分析表明, 利用GHZ态的纠缠特性进行窃听检测, 可以有效地抵抗窃听者的截获测量重发攻击和纠缠测量攻击。在三方通信时, 该方案的通信效率达17.65%, 具有较高的通信效率。

关 键 词: 量子通信; 半量子安全直接通信; GHZ态; 多方通信

中 图 分 类 号 : O431.2 **文 献 标 识 码 :** A **文章编号:** 1007-5461(2023)05-00738-09

Multi-party semi-quantum secure direct communication based on GHZ states

GUO Han, LI Yunxia, WEI Jiahua, TANG Jie, WANG Junhui*

(School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China)

Abstract: Quantum secure direct communication does not need to prepare the quantum keys in advance, and secret information can be transmitted directly through quantums. In order to solve the problem of high cost of quantum communication equipment, a bidirectional three-party semi-quantum secure direct communication (SQSDC) scheme was proposed based on Greenberger-Horne-Zeilinger (GHZ) state and semi-quantum theory. The scheme can realize the secret communication between two classical parties and a quantum party. By adjusting the number of GHZ particles, the classical party can be extended to any number of parties according to the scheme, making the scheme particularly suitable for the communication between one superior unit and several subordinate units. The security analysis shows that, using the entanglement characteristics of GHZ state for eavesdropping detection can effectively resist the attack of eavesdroppers. In three-party communication, the communication efficiency of the scheme is up to 17.65%, showing a high communication efficiency.

Key words: quantum communication; semi-quantum secure direct communication; Greenberger–Horne–Zeilinger states; multi-party communication

基金项目: 国家自然科学基金 (61971436)

作者简介: 郭 瀚 (1997 -), 女, 陕西西安人, 研究生, 主要从事量子通信方面的研究。E-mail: mimamany@qq.com

导师简介: 李云霞 (1966 -), 女, 陕西西安人, 硕士, 教授, 硕士生导师, 主要从事光通信与量子通信方面的研究。E-mail: yunxial@foxmail.com

收稿日期: 2021-06-17; **修改日期:** 2021-09-03

*通信作者。 E-mail: weijiahua@126.com

0　引　言

量子加密基于量子力学理论来实现无条件的安全性, 目前已有各种量子加密协议应用在不同条件下, 包括量子密钥分发 (QKD)[1−3]、量子秘密共享 (QSS)[4, 5]、量子密钥协商 (QKA)[6, 7]、量子支付协议 (EPP)[8]、量子签名 (QS)[9]等。2002 年, Long 和 Liu[10]提出了一种新的量子加密方式 : 量子安全直接通信 (QSDC), 与 QKD 不同, QSDC 不需要提前准备密钥, 其可以通过量子直接传递秘密信息; 2002 年, Boström 和 Felbinger[11] 基于密集编码提出了一个准安全的 QSDC, 即 Ping-pong 协议, 虽然此协议存在信息泄露的风险, 但它首次明确了 QSDC 的定义, 具有相当的理论价值; 2003、2004 年, Deng 等[12, 13]分别基于 EPR 对和单光子提出了两种 QSDC 方案, 明确了 QSDC 的含义和要求。随后, 研究人员又基于不同的粒子状态和应用条件提出了多种 QSDC 方案[14−18]。

以上方案都假设参与方有充分的量子设备和量子资源, 可以做各种量子操作。然而, 量子设备目前仍然较昂贵, 从实用化角度而言, 对半量子安全直接通信 (SQSDC) 进行研究十分必要。半量子密钥协商由 Boyer 等[19] 于 2007 年提出, 该协议基于 BB84 弱化通信参与方其中一方的处理量子的能力, 实现了量子方 Alice 与经典方 Bob 安全共享密钥, 随后研究人员在不同协议中展开了半量子的研究 [20, 21]。2014 年, Zou 和 Qiu[22] 基于单光子提出了三步 SQSDC 方案, 实现了经典方到量子方的 QSDC; 2017 年, Zhang 等[23]提出了基于 EPR 对以及诱骗单光子的 SQSDC 方案; 2018 年, Xie 等[24]提出了可以由量子方发送信息给经典方的 SQSDC 方案; 2019 年, Yang 和 Tsai[25] 基于 Zhang 的协议提出了改进方案, 从而进一步抵抗窃听者的攻击; 2020 年, Rong 等[26]基于单光子提出一个 SQSDC 方案, 该方案不需要使用量子寄存器, 降低了设备成本; 同年, Xu 等[27]利用四粒子簇态提出了一个多方 SQSDC 方案; 2021 年, Rong 等[28] 提出了存在中介第三方的 SQSDC 方案, 该方案可以在通信双方都是经典方的条件下通过一个不可信的量子方中介实现安全通信。

与上述研究不同, 本文基于 GHZ 态提出一个可以实现双向通信的三方 SQSDC 方案, 并且此协议可以将经典方扩展至多方。所提出协议可以减少经典信息的传输, 同时利用 GHZ 态的纠缠特性进行窃听检测, 提高了通信效率, 尤其适用于上级单位与多个下级单位进行秘密通信的情况。

1　方案描述

1.1　预备知识

假设上级单位 Alice 为量子方, 下级单位 Bob 和 Charlie 为经典方, 其中量子方具有制备量子态和执行各种量子操作的能力, 而经典方只具有弱化的量子操作能力。由文献 [29, 30] 可知, 经典方能够执行的操作如下: 1) 不进行任何干扰, 发送或返回所收到的量子比特; 2) 在经典测量基 $\left\{|0\rangle,|1\rangle\right\}$ 上测量量子比特; 3) 制备量子比特 $|0\rangle$ 和 $|1\rangle$; 4) 对量子比特进行顺序打乱或重新排序。

1.2　方案具体过程

Step 1 准备阶段: 一个三粒子 GHZ 态可表示为

$$\left|\Psi(i,j,k)\right\rangle_{\mathrm{ABC}}=\frac{1}{\sqrt{2}}\left(|0\rangle_{\mathrm{A}}\left|j\right\rangle_{\mathrm{B}}\left|k\right\rangle_{\mathrm{C}}+(-1)^{i}|1\rangle_{\mathrm{A}}\left|\bar{j}\right\rangle_{\mathrm{B}}\left|\bar{k}\right\rangle_{\mathrm{C}}\right),\ (i,j,k=0,1),\tag{1}$$

此处用到的粒子为$i=j=k=0$的状态, 即$\left|\Psi_{000}\right\rangle_{\mathrm{ABC}}=\frac{1}{\sqrt{2}}\left(\left|000\right\rangle_{\mathrm{ABC}}+\left|111\right\rangle_{\mathrm{ABC}}\right)$。Alice首先制备$N=4n(1+\delta)$个状态为$\left|\Psi_{000}\right\rangle_{\mathrm{ABC}}$的粒子, 此处$n$表示所要传输的密信比特串的长度, $\delta>0$是一个固定的参数。Alice分别取其中所有的第一个粒子组成量子比特序列$S_{\mathrm{A}}=\{P_1(A),P_2(A)...P_k(A)...P_N(A)\}$, 取所有的第二个粒子组成序列$S_{\mathrm{B}}=\{P_1(B),P_2(B)...P_k(B)...P_N(B)\}$, 所有的第三个粒子组成序列$S_{\mathrm{C}}=\{P_1(C),P_2(C)...P_k(C)...P_N(C)\}$, 然后Alice分别将序列$S_{\mathrm{B}}$与$S_{\mathrm{C}}$发送给Bob和Charlie。

Step 2 编码阶段: 为了抵抗特洛伊木马攻击, 需要在经典方Bob和Charlie接收机前插入一个波长滤波器和光子数分裂器 (PNS)。Bob和Charlie随机选择返回 (CTRL) 或者投影测量 (SIFT), 如果返回, 则将粒子直接进行返回而不进行任何干扰; 如果测量, 则选择用Z基$\{|0\rangle,\ |1\rangle\}$进行投影测量, Bob和Charlie记录测量的量子比特的状态, 之后制备编码的量子态发送给Alice。编码规则如下: 以Bob为例, 假设Bob要传递的信息序列为$M_{\mathrm{B}}=\{m_1(B),m_2(B),...m_k(B)...m_n(B)\}$, 那么经典信息编码为1时, 则反转对应位置的量子比特, 生成一个新的相反的量子比特; 经典信息编码为0时, 则保持该位置的量子比特状态不变, 直到全部编码完成, 通过量子延迟线路调整编码量子比特的顺序得到序列S'_{B}, 并将序列发给Alice。Charlie同理将S'_{C}发送给Alice。

Step 3 窃听检测阶段: Alice全部接收Bob和Charlie的量子比特后告知Bob和Charlie, 此时Bob和Charlie公布自己选择测量和返回的量子比特的具体位置。Bob和Charlie同时选择测量的量子比特称为SIFT-SIFT比特, Bob和Charlie同时选择返回的量子比特称为CTRL-CTRL比特, Bob和Charlie一个选择返回一个选择测量的量子比特称为SIFT-CTRL比特。当n足够大时, 期望CTRL-CTRL和SIFT-SIFT的比特不少于n, 否则就中止通信重新回到Step 1。Alice就CTRL-CTRL的粒子进行GHZ基测量, 并根据GHZ基的测量结果进行窃听检测, 如果检测的错误率高于阈值则放弃通信, 否则继续下一步。

Step 4 译码阶段: Alice告知Bob和Charlie未发现窃听, 而后, Bob和Charlie宣布自己编码序列的顺序, Alice利用Z基对Bob和Charlie编码的量子比特进行测量, 同时测量对应位置S_{A}的量子状态, 二者进行比较就可以分别得到Bob和Charlie的信息。如果结果相同则编码为0, 结果相反则编码为1, 具体编码如表1所示。

表1 编码表

Table 1 Coding schedule

Classical message	Initial qubit	Encoding qubit
0	$\|0\rangle$	$\|0\rangle$
	$\|1\rangle$	$\|1\rangle$
1	$\|0\rangle$	$\|1\rangle$
	$\|1\rangle$	$\|0\rangle$

Step 5 Alice编码阶段: Alice编码存在两种情况, 即Alice发送给Bob和Charlie一样的信息以及Alice发送给Bob和Charlie不同的信息。

Case 1: Alice同时发送信息给Bob和Charlie。Alice挑选出SIFT-SIFT模式的前n个粒子进行编码, 如果此位置编码为0则保持量子比特状态不变; 如果编码为1, 则翻转量子比特的状态, 粒子A重新组成量子比特序列S_{A}', 而后公布序列S_{A}'以及对应的SIFT-SIFT量子比特的位置。Bob和Charlie根据对应位置的量子比特

进行译码, 并根据 $S_A'\oplus S_B''(S_C'')$ 得到Alice的信息, 此处 $S_B''(S_C'')$ 表示SIFT-SIFT比特在Bob和Charlie处的量子比特序列。

Case 2: Alice想要发送信息给其中一个, 或者发送给双方的密信不同。比如Alice要给Bob发送信息 M_1, 要给Charlie发送信息 M_2, 则分别选择Bob和Charlie选择测量的前 n 个量子比特对应的A粒子进行编码。如果此位置编码为0, 则保持量子比特状态不变;如果编码为1, 则翻转量子比特的状态, 分别形成新的量子比特序列 S_{A1}'、S_{A2}'。而后将序列 S_{A1}'、S_{A2}' 分别发送给Bob和Charlie, Bob和Charlie根据自己手中记录的测量结果进行译码, 并根据 $S_{A1}'(S_{A2}')\oplus S_{EB}'(S_{EC}')$ 得到Alice的信息, 此处 $S_{EB}'(S_{EC}')$ 表示Bob (Charlie) 执行测量操作的前 n 个量子比特。

图1描述了基于GHZ的三方双向SQSDC方案过程。

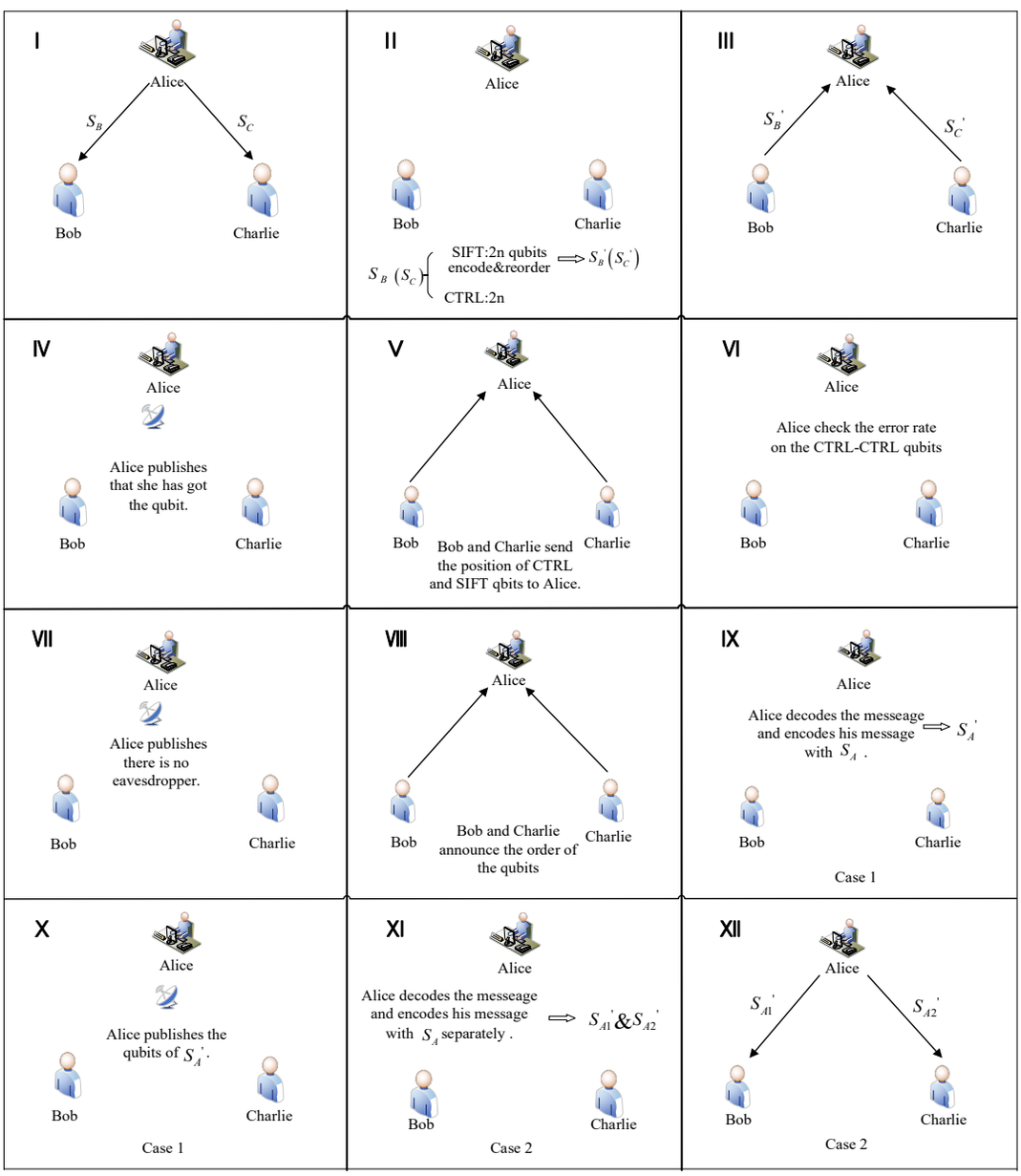

图1　基于GHZ的三方双向SQSDC方案过程

Fig.1　Process of the proposed three-party bidirectional SQSDC based on GHZ

1.3 协议扩展

通过将方案中的三粒子GHZ态换为k粒子GHZ态, 可以实现1个量子方和$k-1$个经典方之间的双向通信。

Step1 准备阶段: 假设Alice为量子方, Bob_1、Bob_2……$Bob_{k\text{-}1}$为$k-1$个经典方, Alice首先制备$N=2^{k-1}n(1+\delta)$个k粒子GHZ态

$$|\Psi\rangle_{AB_1B_2...B_{k-1}}=\frac{1}{\sqrt{2}}\left(\underbrace{|0\rangle|0\rangle...|0\rangle}_{k}+\underbrace{|1\rangle|1\rangle...|1\rangle}_{k}\right), \tag{2}$$

分别将第一个、第二个、第三个、……、第k个粒子组成的序列称为S_A、S_{B_1}、S_{B_2}、……、$S_{B_{k-1}}$, 分别将S_{B_1}、S_{B_2}、……、$S_{B_{k-1}}$发送给Bob_1、Bob_2、……、$Bob_{k\text{-}1}$。

Step 2 编码阶段: 在所有的经典方前都要插入波长滤波器和PNS。同样, Bob_1、Bob_2、……、$Bob_{k\text{-}1}$随机选择返回或者测量, 把Bob_1、Bob_2、……、$Bob_{k\text{-}1}$全部返回的量子比特称为All-CTRL[31], Bob_1、Bob_2、……、$Bob_{k\text{-}1}$全部选择测量的量子比特称为All-SIFT比特。编码方案与上述过程相同。

Step 3 窃听检测阶段: Alice针对All-CTRL粒子进行k粒子的GHZ基测量, 用于窃听检测, 确认安全后通过公共信道告知所有经典方进行下一步, 编码方法与上述步骤相同。

Step 4 译码阶段: 各经典方公布编码顺序, Alice首先测量S_A中量子比特的状态, 然后用Z基测量各经典方发送的编码量子比特, 最后进行对比解码。

Step 5 Alice编码阶段: Alice要发送给各经典方的信息相同时, 利用All-SIFT的前n比特进行编码; 要发送给各经典方信息不同时, 利用各经典方测量的前n比特分别进行编码, 编码方法与上文相同。

2 性能分析

2.1 安全性分析

2.1.1 特洛伊木马攻击

所提出方案是双向传输的, 因此可能存在特洛伊木马攻击。实际上, 有两种特洛伊木马攻击策略需要解决: 不可见光子木马攻击 (IPE) [32, 33]和时间延迟攻击[33, 34]。在经典方Bob和Charlie的接收机前安装隔离器和波长滤波器[35, 36], 隔离器可以在一定波长范围内使光信号单向通过, 反向的光会被阻挡, 因此可以极大削弱反射或者散射回来的光信号, 有效避免特洛伊木马攻击。然而, 隔离器只在所设计波长附近很窄的带宽内有效, 如果Eve使用隔离器消光水平较低的波长, 隔离器将会失效。因此需要加一个滤波器, 滤去波长不合法的光信号, 只允许波长合法的光信号通过, 同时又可以利用隔离器阻挡相同波长光信号的反射和折射, 有效地阻止IPE攻击。PNS则可以有效地检测是否有多量子信号的存在, 从而抵抗时间延迟攻击。

2.1.2 截获测量重发攻击

测量重发攻击是指在Alice发送序列给Bob的过程中, 窃听者Eve俘获 Alice的发送序列, 然后随机选取测量基Z基$\{|0\rangle,|1\rangle\}$或X基$\{|+\rangle,|-\rangle\}$进行单光子测量, 并将测量后的序列发给Bob或Charlie。

在1.2节的Step3中, 通过对CTRL-CTRL粒子执行GHZ基可以防止截获量重发攻击, 如果听者Eve将序列截获并执行Z基测量, GHZ态就会坍缩到$\{|000\rangle, |111\rangle\}$中的一个状态上, 而此时如果Bob和Charlie同时

执行返回操作, 那么Alice利用GHZ基进行测量时就会出现错误, 从而发现窃听。Eve随机选择Z基或X基的可能性均为1/2, Bob和Charlie同时至少有一方执行测量操作的可能性为3/4, 同时选择反射的概率为1/4, 则窃听检测不被检测到的概率为$\frac{1}{2}\times\frac{1}{4}+\frac{1}{2}\times\frac{3}{4}=\frac{1}{2}$。因此对于截获测量重发攻击, 其能够被检测出来的概率为

$$p_{\text{int}-\text{mea}-\text{res}}=1-\left(\frac{1}{2}\right)^{n}, \tag{3}$$

当n足够大时, 这个结果趋近于1。

2.1.3　纠缠测量攻击

窃听者Eve提前制备好辅助粒子, 然后截获Alice发给Bob (Charlie) 的粒子。接着用辅助粒子$|\varepsilon\rangle_{\text{E}}$对截获粒子进行纠缠测量攻击, 则她需要对截获的量子态执行幺正操作U_{E}, 从而使之与辅助光子产生纠缠。具体分析可表示为[37]

$$\begin{cases}U_{\text{E}}|0\rangle|\varepsilon\rangle_{\text{E}}=a|0\rangle|\varepsilon_{00}\rangle_{\text{E}}+b|1\rangle|\varepsilon_{01}\rangle_{\text{E}}\\ U_{\text{E}}|1\rangle|\varepsilon\rangle_{\text{E}}=c|0\rangle|\varepsilon_{10}\rangle_{\text{E}}+d|1\rangle|\varepsilon_{11}\rangle_{\text{E}}\end{cases}, \tag{4}$$

$$\begin{aligned}U_{\text{E}}\left(|+\rangle|\varepsilon\rangle_{\text{E}}\right)=&\frac{1}{2}\left[|+\rangle\left(a|\varepsilon_{00}\rangle_{\text{E}}+b|\varepsilon_{01}\rangle_{\text{E}}+c|\varepsilon_{10}\rangle_{\text{E}}+d|\varepsilon_{11}\rangle_{\text{E}}\right)\right]+\\ &\frac{1}{2}\left[|-\rangle\left(a|\varepsilon_{00}\rangle_{\text{E}}-b|\varepsilon_{01}\rangle_{\text{E}}+c|\varepsilon_{10}\rangle_{\text{E}}-d|\varepsilon_{11}\rangle_{\text{E}}\right)\right],\end{aligned} \tag{5}$$

$$\begin{aligned}U_{\text{E}}\left(|-\rangle|\varepsilon\rangle_{\text{E}}\right)=&\frac{1}{2}\left[|+\rangle\left(a|\varepsilon_{00}\rangle_{\text{E}}+b|\varepsilon_{01}\rangle_{\text{E}}-c|\varepsilon_{10}\rangle_{\text{E}}-d|\varepsilon_{11}\rangle_{\text{E}}\right)\right]+\\ &\frac{1}{2}\left[|-\rangle\left(a|\varepsilon_{00}\rangle_{\text{E}}-b|\varepsilon_{01}\rangle_{\text{E}}-c|\varepsilon_{10}\rangle_{\text{E}}+d|\varepsilon_{11}\rangle_{\text{E}}\right)\right],\end{aligned} \tag{6}$$

式中$\{\varepsilon_{00},\varepsilon_{01},\varepsilon_{10},\varepsilon_{11}\}$为算符$U_{\text{E}}$所决定的四个纯态, 满足归一化条件

$$\sum_{p,q\in\{0,1\}}\langle\varepsilon_{p,q}|\varepsilon_{p,q}\rangle=1. \tag{7}$$

Eve的幺正操作$U_{\text{E}}U_{\text{E}}^{*}=I$可用矩阵形式表示为

$$U_{\text{E}}=\begin{bmatrix}a & c\\ b & d\end{bmatrix}, \tag{8}$$

式中参数a,b,c,d满足

$$\begin{cases}|a|^2+|b|^2=1\\ |c|^2+|d|^2=1\end{cases}. \tag{9}$$

Eve如果想要避免引入错误, 则必须要满足

$$\begin{cases}a|\varepsilon_{00}\rangle_{\text{E}}+c|\varepsilon_{10}\rangle_{\text{E}}=b|\varepsilon_{01}\rangle_{\text{E}}+d|\varepsilon_{11}\rangle_{\text{E}}\\ a|\varepsilon_{00}\rangle_{\text{E}}-c|\varepsilon_{10}\rangle_{\text{E}}=b|\varepsilon_{01}\rangle_{\text{E}}+d|\varepsilon_{11}\rangle_{\text{E}}\end{cases}. \tag{10}$$

由此可知 (10) 式必须满足三个条件 : $a=d=1$, $b=c=0$,$\left|\varepsilon_{00}\right\rangle_{\mathrm{E}}=\left|\varepsilon_{11}\right\rangle_{\mathrm{E}}$, 则 (4) 式可以写为

$$\begin{cases}U_{\mathrm{E}}|0\rangle|\varepsilon\rangle_{\mathrm{E}}=|0\rangle\left|\varepsilon_{00}\right\rangle_{\mathrm{E}}\\ U_{\mathrm{E}}|1\rangle|\varepsilon\rangle_{\mathrm{E}}=|1\rangle\left|\varepsilon_{11}\right\rangle_{\mathrm{E}}\end{cases}. \tag{11}$$

显然, 当且仅当辅助状态和目标粒子$\{|0\rangle,\ |1\rangle\}$是直积状态时, Eve 不会引入任何错误。因此, 该协议可以抵抗外部攻击。

2.2 效率分析

通常, QSDC 协议的效率可以定义为

$$\eta=\frac{b_{\mathrm{s}}}{q_{\mathrm{t}}+q_{\mathrm{s}}}, \tag{12}$$

式中: b_{s}表示实际接收信息的比特数, q_{t}表示需要传送的量子比特, q_{s}表示需要传送的经典信息比特。在所提出协议中, Alice 制备了 $N=4n(1+\delta)$个 GHZ 态, 此处δ很小, 在计算效率时可以忽略, 共需要 12 n bits, 之后 Bob 和 Charlie 会随机进行测量或者返回, 每个 SIFT 的量子比特都需要制备一个新的量子比特, Bob 和 Charlie 测量的量子比特各为$2n$, 之后 Alice 编码需要制备 n 量子比特, 而需要的经典信息q_{s}为0。

此处考虑理想状态的情况, 忽略 GHZ 态传输损耗和测量效率的影响。因此, 当 Alice 传输给 Bob 和 Charlie 的信息相同时

$$\eta=\frac{3n}{12n+4n+n}=17.65\%, \tag{13}$$

当 Alice 传输给 Bob 和 Charlie 的信息不同时

$$\eta=\frac{4n}{12n+4n+2n}=22.22\%. \tag{14}$$

表 2 参数对比

Table 2 Comparison of parameters

Protocol	Parties	b_{s}	q_{t}	q_{s}	Efficiency/%
SQSDC 1 [22]	2	n	$5n$	n	16.7
SQSDC 2 [23]	2	n	$10n$	0	10.0
SQSDC 3 [28]	2	$13n$	$48n$	n	2.04
SQSDC 3 [26]	2	n	$6n$	n	14.3
SQSDC 3 [26]	2	n	$12n$	n	7.7
SQSDC 3 [38]	2	n	$13n$	0	7.69
SQSDC 3 [38]	2	$2n$	$14n\sim13n$	0	14.3 ~ 15.4
Proposed protocol	3	$3n$	$17n$	0	17.65

各协议的性能参数对比如表 2 所示, 由表可见本研究所提出 SQSDC 与以往 SQSDC 方案相比效率有所提高, 且能够在一个通信过程中实现量子方和多个经典方之间的双向通信, 对于上级单位量子方而言, 可以进行一次量子制备后与多方进行通信, 通信效率高。

3 结 论

提出了一个基于 GHZ 态的 SQSDC 方案, 该方案实现了一个量子方和两个经典方的双向通信, 并且可以

将经典方扩展至多方。通过利用GHZ态的纠缠特性进行窃听检测, 可以有效克服截获重发攻击、测量重发攻击、纠缠测量攻击等外部攻击, 同时提高了通信效率, 当Alice传输给Bob和Charlie的信息相同时, 效率达17.65%; 当Alice传输给Bob和Charlie的信息不同时, 效率达22.22%。当然, 在实际的量子通信系统中, 量子效率还会受到制备的量子态、信道噪声、非精确测量、通信距离等多方面因素的影响, 将进一步研究SQSDC应用于实际应用系统。

参考文献:

[1] Bennett C H. Quantum cryptography using any two nonorthogonal states [J]. *Physical Review Letters*, 1992, 68(21): 3121-3124.

[2] Grosshans F, Van Assche G, Wenger J, *et al*. Quantum key distribution using Gaussian-modulated coherent states [J]. *Nature*, 2003, 421(6920): 238-241.

[3] Lo H K, Ma X F, Chen K. Decoy state quantum key distribution [J]. *Physical Review Letters*, 2005, 94(23): 230504.

[4] Gottesman D. Theory of quantum secret sharing [J]. *Physical Review A*, 2000, 61(4): 042311.

[5] Shi R H, Zhong H. Multiparty quantum secret sharing with the pure entangled two-photon states [J]. *Quantum Information Processing*, 2012, 11(1): 161-169.

[6] Zhou N, Zeng G, Xiong J. Quantum key agreement protocol [J]. *Electronics Letters*, 2004, 40(18): 1149-1150.

[7] Tang J, Shi L, Wei J H, *et al*. Quantum key agreement protocols immune to collective noise [J]. *Laser & Optoelectronics Progress*, 2020, 57(17): 172703.
唐 杰, 石 磊, 魏家华, 等. 免疫集体噪声的量子密钥协商协议 [J]. 激光与光电子学进展, 2020, 57(17): 172703.

[8] He Y F, Chen S H, Qiang Y W, *et al*. Electronic payment protocol based on quantum dense coding [J]. *Acta Optica Sinica*, 2021, 41(10): 1027001.
何业锋, 陈思昊, 强雨薇, 等. 一种基于量子稠密编码的电子支付协议 [J]. 光学学报, 2021, 41(10): 1027001.

[9] Wang J H, Li Y X, Meng W, *et al*. Protocol of quantum blind signature based on two-qubit and three-qubit maximally entangled states [J]. *Laser & Optoelectronics Progress*, 2021, 58(7): 0727002.
王俊辉, 李云霞, 蒙 文, 等. 基于两粒子和三粒子最大纠缠态的量子盲签名协议 [J]. 激光与光电子学进展, 2021, 58(7): 0727002.

[10] Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme [J]. *Physical Review A*, 2002, 65(3): 032302.

[11] Boström K, Felbinger T. Deterministic secure direct communication using entanglement [J]. *Physical Review Letters*, 2002, 89 (18): 187902.

[12] Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block [J]. *Physical Review A*, 2003, 68(4): 042317.

[13] Deng F G, Long G L. Secure direct communication with a quantum one-time pad [J]. *Physical Review A*, 2004, 69(5): 052319.

[14] Jin X R, Ji X, Zhang Y Q, *et al*. Three-party quantum secure direct communication based on GHZ states [J]. *Physics Letters A*, 2006, 354(1-2): 67-70.

[15] Wang T J, Li T, Du F F, *et al*. High-capacity quantum secure direct communication based on quantum hyperdense coding with hyperentanglement [J]. *Chinese Physics Letters*, 2011, 28(4): 040305.

[16] Yang Y Y. A quantum secure direct communication protocol without quantum memories [J]. *International Journal of Theoretical Physics*, 2014, 53(7): 2216-2221.

[17] Li J, Song D J, Li R F, *et al*. A quantum secure direct communication protocol based on four-qubit cluster state [J]. *Security and Communication Networks*, 2015, 8(1): 36-42.

[18] Arunaday G, Bikash K B, Prasanta K P. Measurement-device-independent QSDC protocol using Bell and GHZ states on quantum simulator[J]. *Quantum Physics*, 2020, 57(2): 043520.

[19] Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob [J]. *Physical Review Letters*, 2007, 99(14): 140501.

[20] Zhou N R, Zhu K N, Wang Y Q. Three-party semi-quantum key agreement protocol [J]. *International Journal of Theoretical Physics*, 2020, 59(3): 663-676.

[21] Li Q, Chan W H, Long D Y. Semi-quantum secret sharing using entangled states [J]. *Physical Review A*, 2010, 82(2): 022303.

[22] Zou X F, Qiu D W. Three-step semiquantum secure direct communication protocol [J]. *Science China (Physics*, Mechanics & Astronomy), 2014, 57(9): 1696-1702.

[23] Zhang M H, Li H F, Xia Z Q, *et al*. Semiquantum secure direct communication using EPR pairs [J]. *Quantum Information Processing*, 2017, 16(5): 117.

[24] Xie C, Li L Z, Situ H Z, *et al*. Semi-quantum secure direct communication scheme based on Bell states [J]. *International Journal of Theoretical Physics*, 2018, 57(6): 1881-1887.

[25] Yang C W, Tsai C W. Intercept-and-resend attack and improvement of semiquantum secure direct communication using EPR pairs [J]. *Quantum Information Processing*, 2019, 18(10): 306.

[26] Rong Z B, Qiu D W, Zou X F. Two single-state semi-quantum secure direct communication protocols based on single photons [J]. *International Journal of Modern Physics B*, 2020, 34(11): 2050106.

[27] Xu L C, Chen H Y, Zou N R, *et al*. Multi-party semi-quantum secure direct communication protocol with cluster states [J]. *International Journal of Theoretical Physics*, 2020, 59: 2175-2186.

[28] Rong Z B, Qiu D W, Mateus P, *et al*. Mediated semi-quantum secure direct communication [J]. *Quantum Information Processing*, 2021, 20(2): 58.

[29] Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob [J]. *Physical Review Letters*, 2007, 99(14): 140501.

[30] Tan Y G, Lu H, Cai Q Y. Comment on "Quantum Key Distribution with Classical Bob" Reply [J]. *Physical Review Letters*, 2009, 102(9): 098902.

[31] Rong Z B, Qiu D W, Zou X F. Semi-quantum secure direct communication using entanglement [J]. *International Journal of Theoretical Physics*, 2020, 59(6): 1807-1819.

[32] Cai Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons [J]. *Physics Letters A*, 2006, 351(1/2): 23-25.

[33] Li X H, Deng F G, Zhou H Y. Improving the security of secure direct communication based on the secret transmitting order of particles [J]. *Physical Review A*, 2006, 74(5): 054302.

[34] Deng F G, Li X H, Zhou H Y, *et al*. Improving the security of multiparty quantum secret sharing against Trojan horse attack [J]. *Physical Review A*, 2005, 72(4): 044302.

[35] Jain N, Stiller B, Khan I, *et al*. Attacks on practical quantum key distribution systems (and how to prevent them) [J]. *Contemporary Physics : A Review of Physics and Associated Technologies*, 2016, 57(3): 366-387.

[36] Jain N, Stiller B, Khan I, *et al*. Risk analysis of Trojan-horse attacks on practical quantum key distribution systems [J]. *IEEE Journal of Selected Topics in Quantum Electronics*, 2015, 21(3): 168-177.

[37] Tang J, Shi L, Wei J H, *et al*. Multi-party quantum key agreement based on *d*-dimensional GHZ states [J]. *Acta Physica Sinica*, 2020, 69(20): 200301.
唐 杰, 石 磊, 魏家华, 等. 基于 *d* 维GHZ态的多方量子密钥协商 [J]. 物理学报, 2020, 69(20): 200301.

[38] Sun Y H, Yan L L, Chang Y, *et al*. Two semi-quantum secure direct communication protocols based on Bell states [J]. *Modern Physics Letters A*, 2019, 34(1): 1950004.