科学通报 2024 年 第 69 卷 第 11 期: 1491 ~ 1500
论 文
《中国科学》杂志社
SCIENCE CHINA PRESS

基于多光子纠缠的具有身份认证功能的多方量子安全直接通信

刘成[1], 杜明明[2], 钟伟[3], 盛宇波[2,3], 周澜[1*]

1. 南京邮电大学理学院, 南京 210023;
2. 南京邮电大学电子与光学工程学院, 柔性电子(未来技术)学院, 南京 210023;
3. 南京邮电大学量子信息与技术研究所, 南京 210003
* 联系人, E-mail: zhoul@njupt.edu.cn

2023-11-09 收稿, 2024-01-09 修回, 2024-01-10 接受, 2024-01-12 网络版发表
国家自然科学基金(12175106, 92365110)和广东省重点领域研发计划(2018B030325002)资助

摘要 多方量子安全直接通信(multi-party quantum secure direct communication, MQSDC)可使多个信息发送方通过量子信道同时向一个信息接收方传递秘密信息, 并从理论上保证传递信息的绝对安全性. 已有的MQSDC方案均默认所有通信方为合法通信方, 这在实际实验条件下难以保证, 为窃听者冒充合法通信方窃取信息或扰乱通信提供了可能. 本文提出了基于Greenberger-Horne-Zeilinger(GHZ)态的具有身份认证功能的三方量子安全直接通信方案. 信息接收方可同时认证两个实际信息发送方的身份, 确认身份合法后, 再接收其发送的秘密信息, 理论上可保证合法通信方身份认证码以及传输信息的安全. 本方案使用单光子测量代替GHZ态测量, 操作简单且成功率高. 本文对方案在实际实验条件下的安全信息容量进行了数值模拟. 本方案在未来量子网络领域具有重要的应用.

关键词 多方量子安全直接通信, 身份认证, Greenberger-Horne-Zeilinger态, 安全信息容量

量子通信是指利用量子力学的基本原理实现信息的传输. 与经典通信相比, 量子通信具有绝对安全性这一重要优势, 吸引了大量研究人员的关注. 量子通信包括量子密钥分发(quantum key distribution, QKD)[1~4]、量子秘密共享(quantum secret sharing, QSS)[5~10]、量子安全直接通信(quantum secure direct communication, QSDC)[11~13]等重要分支. QKD和QSS分别用于在远距离的两个通信方及多个通信方之间传递密钥. 与QKD和QSS不同, QSDC无需密钥, 通信双方可直接通过量子信道传输秘密信息.

首个QSDC方案由清华大学龙桂鲁课题组[9]提出. 随后, 该课题组又提出了基于纠缠的QSDC方案(两步方案)[12]和基于单光子的QSDC方案(DL04方案)[13], 并阐明了QSDC需要满足的条件及物理机制[12]. 2020年, 设备无关(device-independent, DI)和测量设备无关(measurement-device-independent, MDI)QSDC方案被提出[14,15], 可有效增强QSDC在实际实验条件下的安全性. 2022年, 本课题组[16]提出了一步QSDC方案, 将光子在信道中的传输次数由2次降低为1次, 可有效化简QSDC的实验操作, 降低信息丢失. 紧接着, DI一步QSDC协议以及MDI一步QSDC协议也被提出, 从理论上增强了一步QSDC方案在实际实验条件下的安全性[17,18]. 近期, QSDC在实验方面也取得了重大突破. 2021年, 首个包含15个用户的QSDC网络实验演示成功[19]. 2022年, 北京量子信息科学研究院通过实验实现了100 km通信距离的QSDC[20]. 同年, 龙桂鲁团队[21]将

引用格式: 刘成, 杜明明, 钟伟, 等. 基于多光子纠缠的具有身份认证功能的多方量子安全直接通信. 科学通报, 2024, 69: 1491–1500
Liu C, Du M M, Zhong W, et al. Multi-party quantum secure direct communication protocol with identity authentication based on multi-photon entanglement (in Chinese). Chin Sci Bull, 2024, 69: 1491–1500, doi: 10.1360/TB-2023-1150

QSDC引入到基于经典中继的量子网络中, 提出了量子安全中继概念并完成了实验演示.

多方量子安全直接通信(multi-party quantum secure direct communication, MQSDC)是QSDC的一个重要分支[22~28]. MQSDC可使多个信息发送方同时向一个信息接收方传递秘密信息, 在经济、军事等众多领域具有重要的应用价值. 2006年, 首个基于Greenberger-Horne-Zeilinger(GHZ)态的三方QSDC方案被提出, 并且被推广到了MQSDC方案[22]. 2007年, 满忠晓课题组[23]对上述方案进行了改进. 同年, 基于EPR(Einstein-Podolsky-Rosen)对的三方QSDC方案被提出[24]. 2011年, Hwang课题组[25]提出了可并行的MQSDC方案. 近年来, 本课题组[26]将超纠缠引入到三方QSDC以及MDI三方QSDC中, 提出基于超纠缠的高效三方QSDC方案和MDI三方QSDC方案. 2019年, 一种对抵御集体噪声的MQSDC方案被提出[28]. 虽然MQSDC已被广泛研究, 然而已有的MQSDC方案均建立在所有通信方均是合法通信方的基础上, 这个假设在实际通信过程中很难实现, 窃听者Eve可能冒充某个合法通信方与其他通信方进行通信(扮演攻击), 从而给通信带来严重的安全性漏洞.

量子身份认证(quantum identity authentication, QIA)允许实际通信方利用量子力学的基本原理来证明自己的合法身份. 1995年, 首个QIA方案被提出[29]. 1999年, Dusek课题组[30]结合QKD和经典的身份认证, 提出两个双向QIA方案. 2000年, 为抵御窃听者的扮演攻击, 首个具有身份认证功能的QKD方案被提出[31]. 2006年, Lee课题组[32]利用GHZ态, 设计了两个具有身份认证功能的量子直接通信方案. 同年, 研究人员又提出了基于纠缠交换的多方QIA方案[33]. 近期, QIA也被引入到QSDC方案中以增强QSDC在实际应用中的安全性[34~36]. 然而, 现有的具有身份认证功能的QSDC方案均无法推广到MQSDC中.

为抵御窃听者的扮演攻击, 增强MQSDC在实际应用中的安全性, 本文提出了基于GHZ态的具有身份认证功能的三方QSDC方案. 本方案中, 信息接收方可同时认证两个实际信息发送方的身份, 确认身份合法后再接收其发送的秘密信息, 理论上可保证合法通信方身份认证码以及传输信息的安全. 本方案只需单光子测量, 实验操作简单, 测量成功率高, 在未来量子网络领域具有重要的应用.

1 基于GHZ态的具有身份认证功能的三方量子安全直接通信方案

本节详细介绍基于3光子极化GHZ态的具有身份认证功能的三方QSDC方案. 本方案的原理图如图1所示. 在通信之前, 信息发送者Alice先与2个合法通信方Bob1′和Bob2′分别共享一组由n个随机密钥(0或1)组成的密钥串K_1和K_2(n为大数), 作为识别每个合法通信方的身份识别码, 可描述为

$$\begin{aligned} K_1 &= (K_{11}, K_{12}, K_{13}, \cdots, K_{1n}), \\ K_2 &= (K_{21}, K_{22}, K_{23}, \cdots, K_{2n}). \end{aligned} \tag{1}$$

步骤1: Alice随机制备N个任意的3光子极化GHZ态(N为大数, 且$N \gg n$), 将所有GHZ态中对应的光子组成序列S_1、S_2、S_3. 符合条件的3光子极化GHZ态共有8个, 可分别描述为

$$\begin{aligned}
|\psi_1\rangle &= \frac{1}{\sqrt{2}}\left(|\mathrm{HHH}\rangle + |\mathrm{VVV}\rangle\right)_{S_1S_2S_3} = \frac{1}{2}\left(|{+_x}{+_x}{+_x}\rangle + |{+_x}{-_x}{-_x}\rangle + |{-_x}{+_x}{-_x}\rangle + |{-_x}{-_x}{+_x}\rangle\right)_{S_1S_2S_3}, \\
|\psi_2\rangle &= \frac{1}{\sqrt{2}}\left(|\mathrm{HHH}\rangle - |\mathrm{VVV}\rangle\right)_{S_1S_2S_3} = \frac{1}{2}\left(|{-_x}{-_x}{-_x}\rangle + |{-_x}{+_x}{+_x}\rangle + |{+_x}{-_x}{+_x}\rangle + |{+_x}{+_x}{-_x}\rangle\right)_{S_1S_2S_3}, \\
|\psi_3\rangle &= \frac{1}{\sqrt{2}}\left(|\mathrm{HHV}\rangle + |\mathrm{VVH}\rangle\right)_{S_1S_2S_3} = \frac{1}{2}\left(|{+_x}{+_x}{+_x}\rangle - |{+_x}{-_x}{-_x}\rangle - |{-_x}{+_x}{-_x}\rangle + |{-_x}{-_x}{+_x}\rangle\right)_{S_1S_2S_3}, \\
|\psi_4\rangle &= \frac{1}{\sqrt{2}}\left(|\mathrm{HHV}\rangle - |\mathrm{VVH}\rangle\right)_{S_1S_2S_3} = \frac{1}{2}\left(|{-_x}{+_x}{+_x}\rangle + |{+_x}{-_x}{+_x}\rangle - |{+_x}{+_x}{-_x}\rangle - |{-_x}{-_x}{-_x}\rangle\right)_{S_1S_2S_3}, \\
|\psi_5\rangle &= \frac{1}{\sqrt{2}}\left(|\mathrm{HVV}\rangle + |\mathrm{VHH}\rangle\right)_{S_1S_2S_3} = \frac{1}{2}\left(|{+_x}{+_x}{+_x}\rangle + |{+_x}{-_x}{-_x}\rangle - |{-_x}{+_x}{-_x}\rangle - |{-_x}{-_x}{+_x}\rangle\right)_{S_1S_2S_3}, \\
|\psi_6\rangle &= \frac{1}{\sqrt{2}}\left(|\mathrm{HVV}\rangle - |\mathrm{VHH}\rangle\right)_{S_1S_2S_3} = \frac{1}{2}\left(|{-_x}{+_x}{+_x}\rangle - |{+_x}{-_x}{+_x}\rangle - |{+_x}{+_x}{-_x}\rangle + |{-_x}{-_x}{-_x}\rangle\right)_{S_1S_2S_3}, \\
|\psi_7\rangle &= \frac{1}{\sqrt{2}}\left(|\mathrm{HVH}\rangle + |\mathrm{VHV}\rangle\right)_{S_1S_2S_3} = \frac{1}{2}\left(|{+_x}{+_x}{+_x}\rangle - |{+_x}{-_x}{-_x}\rangle + |{-_x}{+_x}{-_x}\rangle - |{-_x}{-_x}{+_x}\rangle\right)_{S_1S_2S_3}, \\
|\psi_8\rangle &= \frac{1}{\sqrt{2}}\left(|\mathrm{HVH}\rangle - |\mathrm{VHV}\rangle\right)_{S_1S_2S_3} = \frac{1}{2}\left(|{+_x}{+_x}{-_x}\rangle + |{-_x}{+_x}{+_x}\rangle + |{+_x}{-_x}{+_x}\rangle + |{-_x}{-_x}{-_x}\rangle\right)_{S_1S_2S_3},
\end{aligned} \tag{2}$$

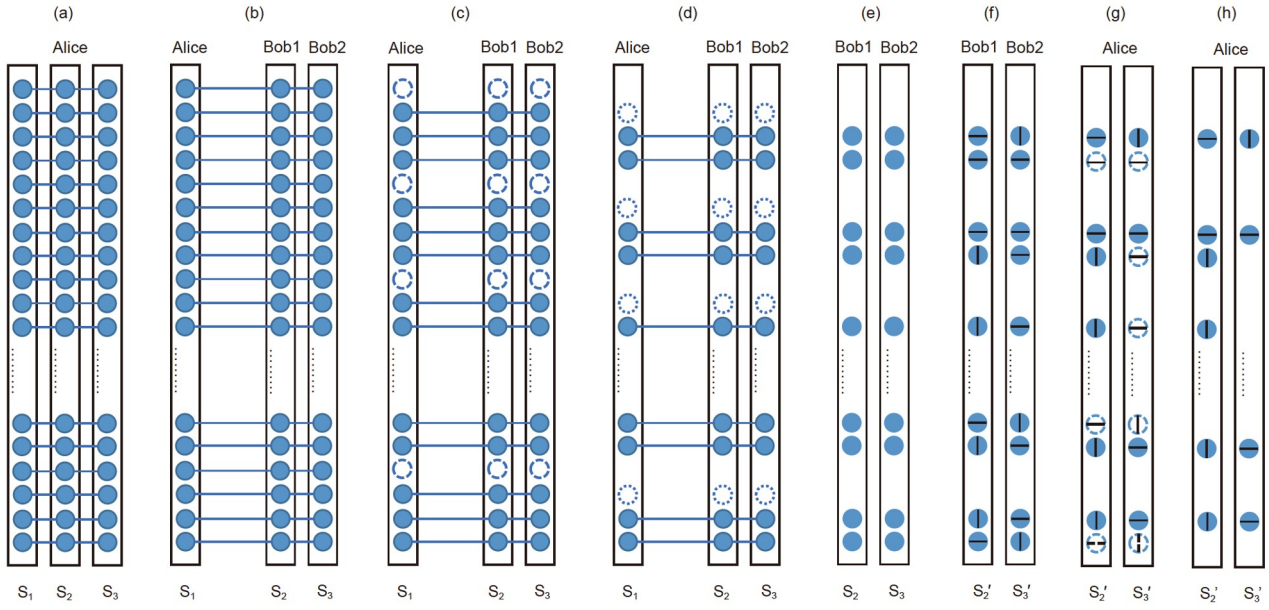

图 1 (网络版彩色)具有身份认证功能的三方量子安全直接通信方案示意图. (a) Alice随机制备大量三光子-GHZ态; (b) Alice向Bob1、Bob2分发GHZ态; (c) 第一轮安全性检测; (d) 身份认证; (e) Alice解除纠缠; (f) Bob1、Bob2编码信息; (g) 第二轮安全性检测; (h) Alice解码信息. 由实线连接的圆圈代表处于GHZ态的纠缠光子. (c), (g) 虚线圆圈代表安全性检测光子; (d) 点线圆圈代表身份认证光子. (f)~(h) 带横线和竖线的圆圈分别表示经过U_0和U_1操作后的光子

Figure 1 (Color online) Schematic diagram of the three-party QSDC protocol with identity authentication. (a) Alice randomly generates a large number of three-photon GHZ states; (b) Alice distributes the GHZ state to Bob1 and Bob2; (c) the first round of security checking; (d) the identity authentication; (e) Alice releases the entanglement; (f) Bob1 and Bob2 encode messages; (g) the second round of security checking; (h) Alice decodes the messages. The circles connected by the real line represent the entangled photons in the GHZ state. (c), (g) The dashed circles represent the security checking photons. (d) The dotted circles represent the identity authentication photons. (f)–(h) The circles with horizontal and vertical lines represent the photons operated by U_0 and U_1, respectively

其中, $|\mathrm{H}\rangle$和$|\mathrm{V}\rangle$分别代表光子的水平极化和垂直极化, $|+_{\mathrm{x}}\rangle=\frac{1}{\sqrt{2}}(|\mathrm{H}\rangle+|\mathrm{V}\rangle)$, $|-_{\mathrm{x}}\rangle=\frac{1}{\sqrt{2}}(|\mathrm{H}\rangle-|\mathrm{V}\rangle)$, 下标$S_1$、$S_2$、$S_3$代表光子所在序列号.

步骤2: Alice将序列S_1的光子存储到量子存储器中, 将序列S_2、S_3的光子分别通过量子信道发送给实际通信方Bob1和Bob2. Bob1和Bob2在接收完光子后, 将光子存储在量子存储器中. 随后, Alice随机选择t组3光子GHZ态作为安全性检测光子(t为大数). Alice从序列S_1中提取所有安全性检测光子, 随机选择Z基或X基进行测量. Alice通过经典信道公布序列S_1中安全性检测光子的位置以及测量基. Bob1和Bob2分别从量子存储器中提取出对应的安全性检测光子. 按照公布的测量基对光子进行测量并公布测量结果. Alice根据式(2)以及自己制备的初始GHZ态, 将上述测量结果与自己的测量结果进行对比, 进行安全性检测. 若三方的测量结果与式(2)中的可能结果不符, 则判断有错误发生. 安全性检测完成后, Alice估算错误率e_1. 若e_1高于事先设定的阈值, 则认为光子传输过程不安全, 通信取消. 若e_1低于事先设定的阈值, 则安全性检测通过, 进行下一步.

步骤3: Alice在剩余的三光子GHZ态中随机选择n组作为身份认证光子. Alice根据合法通信方Bob1′和Bob2′的身份识别码K_{1i}和K_{2i}(i=1, 2, ⋯, n)生成一组新的密钥串$K_{\mathrm{A}}=(K_{\mathrm{A}1}, K_{\mathrm{A}2}, \cdots, K_{\mathrm{A}n})$, 其中, $K_{\mathrm{A}i}=K_{1i}\oplus K_{2i}$($\oplus$代表模二加). Alice根据$K_{\mathrm{A}}$选择测量基对$S_1$序列的身份认证光子进行测量. 测量基选择规则为: 若$K_{\mathrm{A}i}$=0, Alice选择X基对光子进行测量, 若$K_{\mathrm{A}i}$=1, Alice选择Y基$\left\{|+_{\mathrm{y}}\rangle=\frac{1}{\sqrt{2}}(|\mathrm{H}\rangle+\mathrm{i}|\mathrm{V}\rangle),\ |-_{\mathrm{y}}\rangle=\frac{1}{\sqrt{2}}(|\mathrm{H}\rangle-\mathrm{i}|\mathrm{V}\rangle)\right\}$对光子进行测量. 测量结束后, Alice公布身份认证光子的位置, 实际通信方Bob1和Bob2从量子存储器中提取出对应的身份认证光子, 根据自己的身份认证码进行选基测量并公布测量结果, 选基规则与Alice的选基规则相同. 任意一方若测量结果为$|+_{\mathrm{x(y)}}\rangle$, 则公布结果$k_{ji}$=0($j$=A, 1, 2; i=1, 2, ⋯, n), 若测量结果

为$|-_{x(y)}\rangle$, 则公布结果k_{ji}=1(j=A, 1, 2; i=1, 2, ⋯, n). 因此, 当Bob1和Bob2为合法通信方时, 有以下几种情况[35]:

(1) 若K_{1i}=K_{2i}=0, 则K_{Ai}=0, 三方都选择X基对光子进行测量. 若初始GHZ态为$|\psi_1\rangle$, $|\psi_3\rangle$, $|\psi_5\rangle$或$|\psi_7\rangle$, 有k_{Ai}=$k_{1i}\oplus k_{2i}$; 若初始GHZ态为$|\psi_2\rangle$, $|\psi_4\rangle$, $|\psi_6\rangle$或$|\psi_8\rangle$, 有$k_{Ai}\oplus 1$=$k_{1i}\oplus k_{2i}$.

(2) 若K_{1i}=0, K_{2i}=1, 则K_{Ai}=1, Bob2和Alice选择Y基对光子进行测量, Bob1选择X基对光子进行测量. 若初始GHZ态为$|\psi_2\rangle$, $|\psi_4\rangle$, $|\psi_5\rangle$或$|\psi_8\rangle$, 有k_{Ai}=$k_{1i}\oplus k_{2i}$; 若初始GHZ态为$|\psi_1\rangle$, $|\psi_3\rangle$, $|\psi_6\rangle$或$|\psi_7\rangle$, 有$k_{Ai}\oplus 1$=$k_{1i}\oplus k_{2i}$.

(3) 若K_{1i}=1, K_{2i}=0, 则K_{Ai}=1, Bob1和Alice选择Y基对光子进行测量, Bob2选择X基对光子进行测量. 若初始GHZ态为$|\psi_2\rangle$, $|\psi_4\rangle$, $|\psi_5\rangle$或$|\psi_7\rangle$, 有k_{Ai}=$k_{1i}\oplus k_{2i}$; 若初始GHZ态为$|\psi_1\rangle$, $|\psi_3\rangle$, $|\psi_6\rangle$或$|\psi_8\rangle$, 有$k_{Ai}\oplus 1$=$k_{1i}\oplus k_{2i}$.

(4) 若K_{1i}=K_{2i}=1, 则K_{Ai}=0, Bob1和Bob2选择Y基对光子进行测量, Alice选择X基对光子进行测量. 若初始GHZ态为$|\psi_2\rangle$, $|\psi_3\rangle$, $|\psi_6\rangle$或$|\psi_7\rangle$, 有k_{Ai}=$k_{1i}\oplus k_{2i}$; 若初始GHZ态为$|\psi_1\rangle$, $|\psi_4\rangle$, $|\psi_5\rangle$或$|\psi_8\rangle$, 有$k_{Ai}\oplus 1$=$k_{1i}\oplus k_{2i}$.

上述4种情况中, 若三方得到的测量结果不满足对应的规律, 则判断有错误发生. 当所有身份认证光子测量完成后, 三方估算总错误率. 若总错误率大于事先设定的阈值, 则说明存在不合法通信方, 通信取消; 若错误率小于事先设定的阈值, 则判定Bob1和Bob2均为合法通信方, 通信继续.

步骤4: Alice提取出存储器中存储的S_1序列的剩余光子, 选取Z基对所有光子进行测量. 根据式(2), Alice根据自己的测量结果以及制备的初始GHZ态可判断两个合法通信方处光子的量子态. 例如, 假设初始态为$|\psi\rangle_1=\frac{1}{\sqrt{2}}(|\mathrm{HHH}\rangle+|\mathrm{VVV}\rangle)_{123}$, Alice对光子1在Z基下的测量, 当Alice的测量结果为$|\mathrm{H}\rangle$时, 可以推断出发送到Bob1和Bob2手中S_2和S_3序列的光子状态均塌缩成了$|\mathrm{H}\rangle$. 当Alice的测量结果为$|\mathrm{V}\rangle$时, 可以推断出发送到Bob1和Bob2手中S_2和S_3序列的光子状态均塌缩成了$|\mathrm{V}\rangle$. 由于初始的GHZ态只有Alice知道, 因此Alice对手中光子测量后, Bob1和Bob2手中光子的量子态也只有Alice知道.

步骤5: Bob1和Bob2分别在序列S_2、S_3中随机选取1/3的光子通过45°玻片进行Hadamard(H)操作, H操作的功能为将Z基下的光子转换为X基下的光子:

$$|\mathrm{H}\rangle\rightarrow\frac{1}{\sqrt{2}}(|\mathrm{H}\rangle+|\mathrm{V}\rangle)=|+_{\mathrm{x}}\rangle,|\mathrm{V}\rangle\rightarrow\frac{1}{\sqrt{2}}(|\mathrm{H}\rangle-|\mathrm{V}\rangle)=|-_{\mathrm{x}}\rangle. \tag{3}$$

随后, Bob1和Bob2分别选择X基的光子以及一半Z基下的光子作为第二轮安全性检测光子, 剩余的一半Z基下的光子作为信息传输光子.

Bob1和Bob2各自根据需要传递的信息使用两种幺正操作U_0和U_1对S_2和S_3中的信息传输光子进行编码. 用于编码的两个幺正算符U_0和U_1形式为

$$\mathrm{U}_0=\mathrm{I}=\begin{bmatrix}1&0\\0&1\end{bmatrix},\mathrm{U}_1=\mathrm{i}\sigma_{\mathrm{y}}=\begin{bmatrix}0&1\\-1&0\end{bmatrix}, \tag{4}$$

其中, U_0和U_1分别代表经典信息0和1. 进行U_0和U_1操作后, 光子的量子态演化结果为

$$\begin{aligned}&\mathrm{U}_0|\mathrm{H}\rangle=|\mathrm{H}\rangle,\mathrm{U}_0|\mathrm{V}\rangle=|\mathrm{V}\rangle,\\&\mathrm{U}_0|+_{\mathrm{x}}\rangle=|+_{\mathrm{x}}\rangle,\mathrm{U}_0|-_{\mathrm{x}}\rangle=|-_{\mathrm{x}}\rangle,\\&\mathrm{U}_1|\mathrm{H}\rangle=-|\mathrm{V}\rangle,\mathrm{U}_1|\mathrm{V}\rangle=|\mathrm{H}\rangle,\\&\mathrm{U}_1|+_{\mathrm{x}}\rangle=|-_{\mathrm{x}}\rangle,\mathrm{U}_1|-_{\mathrm{x}}\rangle=-|+_{\mathrm{x}}\rangle.\end{aligned} \tag{5}$$

同时, Bob1和Bob2随机使用U_0和U_1对第二轮安全性检测光子进行编码. 定义编码完成后的序列为S_2'和S_3', Bob1和Bob2分别将序列S_2'和S_3'的光子通过量子信道依次发回给Alice.

步骤6: Alice接收到所有的光子后, 先将光子存储在量子存储器中. Bob1和Bob2公布序列S_2'和S_3'中安全性检测光子的位置、制备基及随机操作. Alice提取出每个序列中的安全性检测光子进行第二轮安全性检测. Alice使用公布的测量基对其进行测量, 再结合Bob1和Bob2公布的随机操作比较测量结果, 分别估算两条信道的错误率e_{21}和e_{22}. 若e_{21}或e_{22}超过了事先设定的阈值, 说明光子在对应信道中的传输不安全, Alice取消与此信道对应通信方的通信. 若e_{21}和e_{22}均低于事先设定的阈值, 则说明光子在此信道中的传输安全, 进行下一步.

步骤7: Alice提取出所有编码光子, 使用Z基对所有编码光子进行测量, 并将测量结果与步骤4结束后Bob1和Bob2手中光子的量子态相比对. 若光子的测量结果与Bob1(Bob2)手中光子的初始态相同, 则说明Bob1(Bob2)进行的是U_0操作, 传递了经典信息0. 反之, 若光子的测量结果与Bob1(Bob2)手中光子的初始态不同, 则说明Bob1(Bob2)进行的是U_1操作, 传递了经典信息1.

2 安全性分析

传递信息的安全性是评估QSDC方案性能的重要指标. 在下面的分析中, 我们对窃听者Eve的能力不做限制, Eve只需遵循量子力学的基本原理即可. 本节重点分析光子传输过程和身份验证过程的安全性.

2.1 光子传输过程的安全性

这里我们考虑最常见的攻击方式: 截获-测量-重发攻击.

本协议中, Eve能获取信息的关键是在第一轮光子传输过程中截获光子. 如果Eve只在第二轮光子传输过程中截取到光子, 由于不知道光子的初始态, 也无法得到光子中传输的信息. 然而, 第二轮光子传输过程中Eve的截获-测量-重发攻击可能改变光子的量子态, 从而干扰Alice的信息读取.

本方案通过安全性检测可有效抵御Eve的截获-测量-重发攻击. 在每一轮光子传输之前, 通信方均会随机选择大量的光子作为安全性检测光子. 因此, 在两轮光子传输过程中, Eve都不可避免地会截获到部分安全性检测光子. 由于Eve不知道截取到的光子的测量基, 因此有50%的概率会猜错测量基. 假设Alice使用Z基测量光子, 而Eve采用X基测量截获的光子. 在第一轮光子传输过程中, 分两种情况讨论.

情况1. Eve截获到一组GHZ态中的两个光子, 此时序列S_2和S_3中安全性检测光子的量子态会等概率地随机塌缩到$|++\rangle$、$|+-\rangle$、$|-+\rangle$或$|--\rangle$, 随后Eve根据测量结果制备新的光子发送给Bob1和Bob2. Bob1和Bob2根据Alice公布的Z基对光子进行测量会等概率地得到$|HH\rangle$、$|HV\rangle$、$|VH\rangle$或$|VV\rangle$. 因此, 在与Alice的结果进行对比时, 只有25%的概率导致对比结果正确. 因此, 情况1中, 设Eve截取到的安全性检测光子数量为t', 则Eve不被发现的概率为$(5/8)^{t'}$.

情况2. Eve截获一组GHZ态中的一个光子, 此时序列S_2或S_3中安全性检测光子的量子态就会等概率地随机塌缩到$|+\rangle$或$|-\rangle$, 随后Eve根据测量结果制备新的光子到达实际通信方手中, 实际通信方根据Alice公布的Z基对该光子进行测量会等概率地得到$|H\rangle$或$|V\rangle$. 在与Alice的结果进行对比时, 有50%的概率出错. 设Eve截取到的安全性检测光子数量为t', 则Eve不被发现的概率为$(3/4)^{t'}$. 由此可得, 两种情况下, 当t'为大数时, Eve不被发现的概率均趋向于0. 如果在第一轮光子传输后发现了窃听, 后面的通信步骤均被取消, 保障了传输信息的安全性. 在第一轮光子传输过程中, 由于光子并未编码信息, 因此, 即使窃听者窃取到了部分光子, 也无法得到有用的信息.

第二轮光子传输过程中, 由于光子对间的纠缠已经解除, 各光子序列独立地传输. 由于各光子序列中均包含大量安全性检测光子, 也能有效地抵御Eve的截获-测量-重发攻击, 因此, 传输信息的正确性也能得到保证.

2.2 身份认证过程的安全性

在确定光子传输过程安全的前提下, Alice进一步需要确定信息发送方Bob1和Bob2的身份. Alice知道所有合法通信方的身份识别码. 若通信方Bob1(Bob2)不是合法通信方, 则他不知道合法通信方的身份识别码. 因此, 无法按照步骤3的约定选择正确测量基对身份认证光子进行测量. 若Bob1(Bob2)选择的测量基错误, 则三方的测量结果无法满足步骤3的规律, 因此容易导致错误的出现. 例如, 若用于身份认证的GHZ态为$|\psi_1\rangle$, 当Alice与合法通信方Bob1和Bob2共享的两组身份识别码分别为1和0时, 此时Alice根据模二加得出的密钥为1. Alice对手中的身份认证光子依次进行Y基测量, 若Bob1和Bob2是合法通信方, Bob1和Bob2根据身份识别码应分别选择Y基和X基对手中对应的光子进行测量, 得到的测量结果应满足$k_A\oplus 1=k_1\oplus k_2$. 若Bob1不是合法通信方, 他有50%的概率错选X基对手中光子进行测量. 此时, 三方的测量结果为

$$\begin{aligned}|\psi_1\rangle &= \frac{1}{\sqrt{2}}\left(|HHH\rangle + |VVV\rangle\right)_{123}\\ &= \frac{1}{2}\left(\left|+_y+_x+_x\right\rangle + \left|+_y-_x-_x\right\rangle + \left|-_y+_x-_x\right\rangle + \left|-_y-_x+_x\right\rangle\right)_{A12}.\end{aligned} \tag{6}$$

因此, 三方公布的测量结果满足$k_A=k_1\oplus k_2$, 导致错误的产生.

当所有的身份认证光子测量结果比对结束后, 若错误率超过了能容忍的阈值, Alice判定一定存在不合法的通信方, 则终止通信. 因此, 通过身份认证过程, 本方案可有效地抵御不合法通信方的扮演攻击, 保证通信的安全性和正确性. 同时, 由于各方的身份识别码编码在测量基, 而三方公布的是测量结果0或1, 窃听者

或非法的通信方也无法通过其他方公布的测量结果推导出任意通信方的身份认证码，保证了各个通信方身份认证码的安全.

3 安全信息容量

为评估本方案的性能，定义方案的安全信息容量(C_S)为传输的正确且安全的信息比特数除以编码GHZ态的总数. 在理想的量子信道条件下, 第一轮和第二轮光子传输过程中，分发的GHZ态和单光子都能完美地到达通信方处. 一组编码三光子GHZ态可使得合法通信方Bob1和Bob2共向Alice传输2个比特的信息，因此, 有C_S=2. 然而, 实际实验条件下GHZ态制备的不完美以及量子信道中存在环境噪声等因素均会影响通信，从而缩短安全通信距离, 降低本方案的安全信道容量. 根据Wyner[37]提出的窃听信道理论，本三方QSDC方案的安全信道容量为

$$C_S = I(B1:A) + I(B2:A) - I(B1:E) - I(B2:E), \quad (7)$$

其中, I(B1:A)、I(B2:A)分别代表Bob1和Alice的互信息以及Bob2和Alice的互信息，I(B1:E)、I(B2:E)分别代表Eve与Bob1以及Eve与Bob2间的互信息.

I(B1:A)、I(B2:A)的表达式为[37]

$$\begin{aligned} I(B1:A) &= Q_{t1}[1-h(E_{Bob1})], \\ I(B2:A) &= Q_{t2}[1-h(E_{Bob2})], \end{aligned} \quad (8)$$

其中，Q_{t1}(Q_{t2})代表Alice处探测到Bob1(Bob2)发送的光子的总增益, 具体含义为: 经过两轮光子传输后，Alice处来自Bob1(Bob2)发回光子引起的有意义的探测器响应的概率. E_{Bob1}(E_{Bob2})代表Alice处读出Bob1(Bob2)传递信息的总错误率, $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$代表二进制香农熵.

首先计算Q_{t1}(Q_{t2}). 考虑Alice和Bob1及Bob2的距离都是L, 制备的初始目标GHZ态为$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|\mathrm{HHH}\rangle + |\mathrm{VVV}\rangle)_{123}$. 假设GHZ态制备的成功概率为100%[38], 其保真度为P_1, 考虑白噪声模型, 则制备的实际初始量子态为

$$\begin{aligned} \rho_{in1} &= P_1 |\psi_1\rangle\langle\psi_1| + \frac{1-P_1}{7} \\ &\times\left(|\psi_2\rangle\langle\psi_2| + |\psi_3\rangle\langle\psi_3| + \ldots + |\psi_8\rangle\langle\psi_8|\right). \end{aligned} \quad (9)$$

设光子与光纤的耦合系数为η_c, 光子在信道中传输时, 传输效率为$\eta_t = -10^{-\alpha L/10}$($L$为光子传输距离, a = 0.2 dB/kM). 量子存储器的存储效率为η_m, 光子探测器的探测效率为η_d. 若第一轮光子传输过程中存在光子丢失, 将导致其他光子间失去关联性. 此时，Alice在对手中光子进行测量解除纠缠时，无法根据自己的测量结果推断出合法通信方手中光子的量子态，所以本方案要求第一轮光子传输中不能有光子丢失.

在第二轮光子传输前，Alice已经通过对S_1序列的光子在Z基下测量解除了光子间的关联. 因此，第二轮光子传输过程中, 若某条信道的光子发生丢失时, 只会影响到该信道的信息无法传输，另一条信道的信息传输不受影响.

根据上述分析, 本方案的Q_{t1}和Q_{t2}可表示为

$$Q_{t1} = Q_{t2} = (\eta_c\eta_t)^3\eta_m^3\eta_d^2 = \eta_c^3\eta_m^3\eta_d^2 10^{-3\alpha L/10}. \quad (10)$$

在第一轮光子传输过程中同样考虑白噪声模型, 假设目标GHZ态的保真度为P_2. 结合式(9), 可得到第一轮光子传输后三方共享的量子态为

$$\begin{aligned} \rho_{in2} &= \left[P_1P_2 + \frac{(1-P_1)(1-P_2)}{7}\right] |\psi_1\rangle\langle\psi_1| \\ &+ \frac{1-P_1P_2-\frac{(1-P_1)(1-P_2)}{7}}{7} \\ &\times\left(|\psi_2\rangle\langle\psi_2| + |\psi_3\rangle\langle\psi_3| + \cdots + |\psi_8\rangle\langle\psi_8|\right). \end{aligned} \quad (11)$$

结合式(2), 当目标态变为$|\psi_2\rangle$时，不会导致Alice推测Bob1及Bob2的初始态出错；当目标态变为$|\psi_3\rangle$, $|\psi_4\rangle$, $|\psi_5\rangle$或$|\psi_6\rangle$时, 会导致Alice推测Bob2的初始态出错, 当目标态变为$|\psi_5\rangle$, $|\psi_6\rangle$, $|\psi_7\rangle$或$|\psi_8\rangle$时, 会导致Alice推测Bob1的初始态出错. 为计算方便，令$P_{c1} = P_1P_2 + \frac{(1-P_1)(1-P_2)}{7}$, 则$\rho_{in2}$可简化为

$$\begin{aligned} \rho_{in2} &= \left[P_1P_2 + \frac{(1-P_1)(1-P_2)}{7}\right] |\psi_1\rangle\langle\psi_1| \\ &+ \frac{1-P_{c1}}{7}\left(|\psi_2\rangle\langle\psi_2| + |\psi_3\rangle\langle\psi_3| + \cdots + |\psi_8\rangle\langle\psi_8|\right). \end{aligned} \quad (12)$$

假设第二轮光子传输过程中光子发生比特翻转错误的概率为1–P_3, 则经过第二轮光子传输后, Alice能读出Bob1及Bob2传递的正确信息的概率R_{c1}及R_{c2}为

$$R_{c1} = R_{c2} = (P_{c1} + \frac{1-P_{c1}}{7})P_3 + \frac{4(1-P_{c1})(1-P_3)}{7}, \quad (13)$$

所以Alice处读出Bob1和Bob2传递信息的总错误率E_{Bob1}、E_{Bob2}为

$$E_{Bob1} = E_{Bob2} = 1 - R_{c1}. \quad (14)$$

接下来，计算I(B1:E)、I(B2:E). 由第2节安全性分析可知，Eve能获取信息的关键是在第一轮光子传输过程中截获光子. 因此，可以得到[38,39]:

$$I(B1:E)+I(B2:E)\leqslant Q_{\mathrm{Eve}}h(e_1), \tag{15}$$

其中，Q_{Eve}代表Eve在第一轮光子传输过程中窃取到的光子的增益，具体含义为Eve在第一轮光子传输过程中能窃取到的发送给Bob1和Bob2的总光子数比率. e_1代表第一轮光子传输后的错误率. 这里取

$$Q_{\mathrm{Eve}}=(\eta_{\mathrm{c}}\eta_{\mathrm{t}}\eta_{\mathrm{m}})^2\eta_{\mathrm{d}}. \tag{16}$$

根据式(12)可知，

$$e_1=1-P_{c1}=1-P_1P_2-\frac{(1-P_1)(1-P_2)}{7}. \tag{17}$$

结合式(7)~(16)，可得到本方案密钥率的下界，即安全信息容量C_S.

我们对本方案的安全信息容量C_S进行了数值模拟. 设定量子存储器存储效率$\eta_{\mathrm{m}}=0.9$. 根据文献[40~42]的数据，设定光子探测器的探测效率以及光子与光纤的耦合效率满足$\eta_{\mathrm{d}}=\eta_{\mathrm{c}}=0.95$，初始GHZ态的保真度$P_1$=0.95. 如图2所示，调节信道保真度$P_2$=$P_3$=1，0.98，0.96，0.94，绘制$\log_{10}C_S$与光子传输距离$L$的函数曲线图，明显看出，由于信道噪声引起的光子传输丢失，

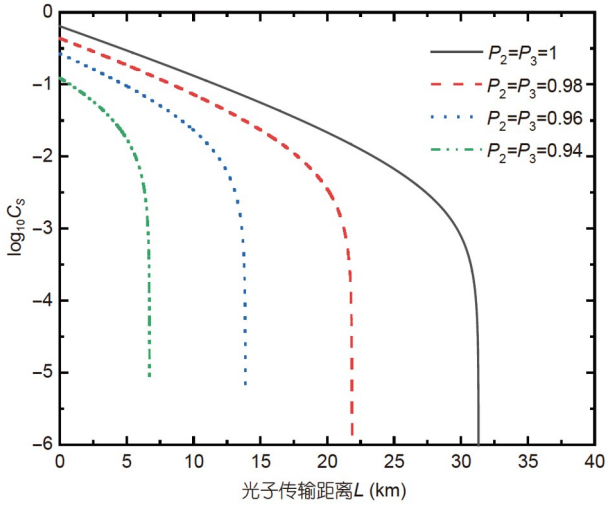

图 2 (网络版彩色)三方QSDC方案的安全信息容量$\log_{10}C_S$与光子传输距离L的函数关系. 假设η_{m}=0.9，$\eta_{\mathrm{d}}=\eta_{\mathrm{c}}$=0.95，$P_1$=0.95，调节$P_2$=$P_3$=1, 0.98, 0.96, 0.94

Figure 2 (Color online) The secret message capacity ($\log_{10}C_S$) of the three-party QSDC protocol as a function of the photon transmission distance L. Here, we set η_{m}=0.9, $\eta_{\mathrm{d}}=\eta_{\mathrm{c}}$=0.95, P_1=0.95 and adjust P_2=P_3=1, 0.98, 0.96, 0.94, respectively

$\log_{10}C_S$随着光子传输距离的增加迅速下降. 同时，信道保真度的降低也会明显降低C_S. 通过计算得出，在初始目标GHZ态的保真度P_1=0.95条件下，本方案能容忍的信道保真度阈值约为0.92，即当P_2=P_3<0.92时，本方案无法得到正的安全信息容量. 在P_2=P_3=1，0.98，0.96，0.94条件下，本三方QSDC方案的最大通信距离分别约为31.3、21.85、13.88、6.71 km.

4 讨论与结论

本文提出了基于三光子极化GHZ态的具有身份认证功能的三方QSDC方案. 与已有的基于GHZ态的三方QSDC方案[22,23]相比，本方案具有两个显著的优点：第一，本方案利用QSS的思想，在三方QSDC中加入了基于GHZ态的身份认证过程. 信息接收方可同时认证两个信息发送方的身份合法性，只要存在一个信息发送方不合法，就会导致身份认证过程不通过，从而终止通信. 同时，本方案还可以严格保护每个合法通信方身份认证码的安全. 因此，本方案可以消除由于实际不合法通信方造成的安全性漏洞(不合法通信方的扮演攻击)，增强方案在实际实验条件下的安全性. 第二，之前基于GHZ态的三方QSDC方案[22,23]需要信息接收方执行完全GHZ态测量，即能完全区分8个三光子极化GHZ态. 然而，在线性光学条件下只能区分8个三光子极化GHZ态中的2个[43]，测量成功概率低，容易导致传递信息的丢失. 本方案用简单的单光子探测代替了GHZ态测量. 单光子探测在当前实验条件下很容易实现，且成功率接近100%. 因此，使用单光子测量可有效化简实验操作，提高测量成功率，减少由于测量引起的信息丢失.

本方案是通信方利用偏振模式自由度进行编码. 当然，也可以采用光子的其他自由度进行编码，如时间片段、空间模式、轨道角动量、频率等，还可以利用多自由度超编码来进行信息传输，以便提高光子的信息容量. 同时，本方案还可以扩展到包含任意N个通信方的MQSDC. 由于本方案只需要执行单光子测量，测量难度不会因为通信方数量的增加而增加. 理论上N–1个信息发送方可利用一个N光子GHZ态向信息接收方共传输N–1个比特的信息.

本方案中，我们假设信息接收方Alice为合法通信方，Alice验证实际信息发送方的身份. 该通信模式在实际军事和国民经济领域具有重要的应用意义. 同理，由信息发送方验证信息接收方的身份在实际应用中也有重要的研究意义. 例如，在军事行动中，信息发送方

有必要先验证信息接收方的身份, 然后再向其发送信息. 实际上, 本方案中的身份认证过程也可以扩展为双向身份认证, 即信息发送方和信息接收方互相认证对方的身份. 具体为合法信息接收方和每个合法信息发送方之间共享2组密钥串, 第一组作为信息发送方的身份码序列, 第二组作为信息接收方的身份码序列. 身份认证过程分为两个步骤. 步骤1: 信息接收方利用第一组身份码序列认证各个信息发送方的身份. 步骤2: 各个信息发送方再根据第二组身份码序列认证信息接收方的身份. 两个步骤中具体的身份认证过程与本文的身份认证过程相同. 只有两个步骤的身份认证过程均通过, 实际通信方才进行信息传输. 这里, 为保证各个通信方的身份安全(通信方的身份不会在以后被人冒充), 我们规定, 每组身份码序列只能使用一次, 即各组身份码序列使用一次后就失效. 因此, 即使有非法通信方获得了其他合法通信方的身份认证码, 他也无法在以后利用此身份码序列冒充对方的身份.

总之, MQSDC可使得多个通信方同时向一个信息接收方传递秘密信息, 并从理论上保证了传递信息的绝对安全性, 在经济、军事等众多领域具有重要的研究价值. 已有的MQSDC方案均默认所有通信方为合法通信方, 这样给了窃听者冒充合法通信方窃取信息或扰乱通信的可能, 威胁MQSDC在实际应用中的安全性和信息传输的正确性. 本文利用量子秘密共享的思想, 提出了基于GHZ态的具有身份认证功能的三方QSDC方案. 信息接收方可在身份认证过程中同时认证两个实际信息发送方的身份, 只要任一方的身份认证不通过, 即刻终止通信, 可有效抵御窃听者的扮演攻击并保护合法通信方身份认证码的安全. 本方案中使用单光子测量代替了复杂的GHZ态测量, 操作简单且成功率高. 理论上一轮通信过程中, 各个合法通信方可分别向信息接收方传递1个比特的秘密信息. 本文对方案在实际实验条件下的安全信息容量进行了数值模拟. 模拟结果显示, 当初始GHZ态保真度为P_1=0.95时, 本方案能容忍的信道保真度阈值约为0.92. 在信道保真度P_2=P_3=0.98的条件下, 本方案的最大通信距离约为21.85 km. 本方案在未来量子网络领域具有重要的应用.

参考文献

1 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proc IEEE International Conference on Computers Systems and Signal Processing, 1984, 560: 175–179
2 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67: 661–663
3 Bennett C H. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett, 1992, 68: 3121–3124
4 Xu F, Ma X, Zhang Q, et al. Secure quantum key distribution with realistic devices. Rev Mod Phys, 2020, 92: 025002
5 Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829–1834
6 Bell B A, Markham D, Herrera-Martí D A, et al. Experimental demonstration of graph-state quantum secret sharing. Nat Commun, 2014, 5: 5480
7 Fu Y, Yin H L, Chen T Y, et al. Long-distance measurement-device-independent multiparty quantum communication. Phys Rev Lett, 2015, 114: 090501
8 Gao Z K, Li T, Li Z H. Deterministic measurement-device-independent quantum secret sharing. Sci China-Phys Mech Astron, 2020, 63: 120311
9 Zhang T, Zhou L, Zhong W, et al. Multiple-participant measurement-device-independent quantum secret sharing protocol based on entanglement swapping. Laser Phys Lett, 2023, 20: 025203
10 Ju X X, Zhong W, Sheng Y B, et al. Measurement-device-independent quantum secret sharing with hyper-encoding. Chin Phys B, 2022, 31: 100302
11 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002, 65: 032302
12 Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68: 042317
13 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319
14 Zhou L, Sheng Y B, Long G L. Device-independent quantum secure direct communication against collective attacks. Sci Bull, 2020, 65: 12–20
15 Zhou Z R, Sheng Y B, Niu P H, et al. Measurement-device-independent quantum secure direct communication. Sci China-Phys Mech Astron, 2020, 63: 230362
16 Sheng Y B, Zhou L, Long G L. One-step quantum secure direct communication. Sci Bull, 2022, 67: 367–374
17 Zhou L, Sheng Y B. One-step device-independent quantum secure direct communication. Sci China-Phys Mech Astron, 2022, 65: 250311
18 Ying J W, Zhou L, Zhong W, et al. Measurement-device-independent one-step quantum secure direct communication. Chin Phys B, 2022, 31:

120303
19 Qi Z, Li Y, Huang Y, et al. A 15-user quantum secure direct communication network. Light Sci Appl, 2021, 10: 183
20 Zhang H, Sun Z, Qi R, et al. Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. Light Sci Appl, 2022, 11: 83
21 Long G L, Pan D, Sheng Y B, et al. An evolutionary pathway for the quantum internet relying on secure classical repeaters. IEEE Network, 2022, 36: 82–88
22 Jin X R, Ji X, Zhang Y Q, et al. Three-party quantum secure direct communication based on GHZ states. Phys Lett A, 2006, 354: 67–70
23 Man Z X, Xia Y J. Improvement of security of three-party quantum secure direct communication based on GHZ states. Chin Phys Lett, 2007, 24: 15–18
24 Wang M Y, Yan F L. Three-party simultaneous quantum secure direct communication scheme with EPR pairs. Chin Phys Lett, 2007, 24: 2486–2488
25 Chong S K, Hwang T. The enhancement of three-party simultaneous quantum secure direct communication scheme with EPR pairs. Opt Commun, 2011, 284: 515–518
26 Chen S S, Zhou L, Zhong W, et al. Three-step three-party quantum secure direct communication. Sci China Phys Mech Astron, 2018, 61: 90312
27 Hong Y P, Zhou L, Zhong W, et al. Measurement-device-independent three-party quantum secure direct communication. Quantum Inf Process, 2023, 22: 111
28 He Y F, Ma W P. Multiparty quantum secure direct communication immune to collective noise. Quantum Inf Process, 2019, 18: 4
29 Crépeau C, Salvail L. Quantum oblivious mutual identification. In: International Conference on the Theory and Applications of Cryptographic Techniques, 1995. 133–146
30 Dušek M, Haderka O, Hendrych M, et al. Quantum identification system. Phys Rev A, 1999, 60: 149–156
31 Zeng G, Zhang W. Identity verification in quantum key distribution. Phys Rev A, 2000, 61: 022303
32 Lee H, Lim J, Yang H J. Quantum direct communication with authentication. Phys Rev A, 2006, 73: 042305
33 Wang J, Zhang Q, Tang C J. Multiparty simultaneous quantum identity authentication based on entanglement swapping. Chin Phys Lett, 2006, 23: 2360–2363
34 Liu D, Pei C X, Quan D X, et al. A new quantum secure direct communication scheme with authentication. Chin Phys Lett, 2010, 27: 050306
35 Das N, Paul G. Measurement device-independent quantum secure direct communication with user authentication. Quantum Inf Process, 2022, 21: 260
36 Das N, Paul G. Cryptanalysis of quantum secure direct communication protocol with mutual authentication based on single photons and Bell states. EPL, 2022, 138: 48001
37 Wyner A D. The wire-tap channel. Bell Syst Tech J, 1975, 54: 1355–1387
38 Qi R, Sun Z, Lin Z, et al. Implementation and security analysis of practical quantum secure direct communication. Light Sci Appl, 2019, 8: 22
39 Pan D, Lin Z, Wu J, et al. Experimental free-space quantum secure direct communication and its security analysis. Photonics Res, 2020, 8: 1522–1531
40 Kaufmann H, Ruster T, Schmiegelow C T, et al. Scalable creation of long-lived multipartite entanglement. Phys Rev Lett, 2017, 119: 150503
41 Zhang W J, You L X, Li H, et al. NbN superconducting nanowire single photon detector with efficiency over 90% at 1550 nm wavelength operational at compact cryocooler temperature. Sci China Phys Mech Astron, 2017, 60: 120314
42 Lu X, Li Q, Westly D A, et al. Chip-integrated visible-telecom entangled photon pair source for quantum communication. Nat Phys, 2019, 15: 373–381
43 Pan J, Zeilinger A. Greenberger-Horne-Zeilinger-state analyzer. Phys Rev A, 1998, 57: 2208–2211

Summary for “基于多光子纠缠的具有身份认证功能的多方量子安全直接通信”

Multi-party quantum secure direct communication protocol with identity authentication based on multi-photon entanglement

Cheng Liu[1], Mingming Du[2], Wei Zhong[3], Yubo Sheng[2,3] & Lan Zhou[1*]

[1] *College of Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China;*
[2] *College of Electronic and Optical Engineering & College of Flexible Electronics (Future Technology), Nanjing University of Posts and Telecommunications, Nanjing 210023, China;*
[3] *Institute of Quantum Information and Technology, Nanjing University of Post and Telecommunications, Nanjing 210003, China*
* Corresponding author, E-mail: zhoul@njupt.edu.cn

Multi-party quantum secure direct communication (MQSDC) enables multiple communication parties to simultaneously transmit secret messages to one message receiver through quantum channels. MQSDC plays an important role in promoting the networking and practicality of QSDC and has wide applications in the economy, commerce, and military fields.

Existing MQSDC schemes all assume that all the communication parties are legitimate parties, which is difficult to guarantee in practical applications. The lack of the identity authentication for the communication parties would seriously increase the security risk. In this way, it is possible for eavesdroppers to impersonate legitimate communicators to steal message or disrupt communication. In this paper, we propose the first three-party QSDC protocol with identity authentication based on the Greenberger-Horne-Zeilinger (GHZ) state. Before the communication, the message receiver Alice and each of the two legal message senders share a sequence of keys as the legal message sender’s identity code sequence in advance. Alice generates a large number of three-photon GHZ states. Then, Alice distributes two photons of each GHZ state to the practical message senders Bob1 and Bob2, respectively. The parties first check the security of the photon transmission process. Only when the security checking is past, Alice and the practical message senders perform the identity authentication. The identity authentication is based on the quantum secret sharing theory. In detail, Alice, Bob1, and Bob2 select measurement bases according to their identity codes and announce their measurement results through a public channel. Based on the announced measurement results, Alice can simultaneously authenticate the identities of two practical message senders and ensure the security of their identity authentication codes. After the identity authentication, Alice first measures her photons to release the entanglement. Then, the legal message senders can encode their messages on the photons and send the encoded photons back to Alice. By measuring each transmitted photon and comparing the measurement result with its initial quantum state, Alice can finally read out the transmitted messages from two message senders.

Our protocol can guarantee the absolute security of each legal message sender’s identity authentication codes and transmitted messages. In theory, each sender can independently send one bit of secret message to Alice. Our protocol replaces the complicated GHZ measurement with the single photon measurement, which can simplify the experimental operation and achieve higher success probability. The security message capacity of the three-party QSDC protocol under practical experimental conditions is numerically simulated. The simulation results indicate that with the initial fidelity of the GHZ state of P_1=0.95, and the channel fidelity of 0.98, the maximal communication distance of our protocol can reach about 21.85 km. Moreover, our protocol can also extend to the MQSDC with arbitrary number of practical message senders, and the identity authentication process can be extended to the bidirectional identity authentication. Based on above feature, our protocol has important applications in the future quantum networks field.

multi-party quantum secure direct communication, identity authentication, Greenberger-Horne-Zeilinger state, security message capacity

doi: 10.1360/TB-2023-1150