基于具有极化和空模自由度的单光子的量子加密量子对话

叶天语^{*}, 耿茂洁, 徐天婕, 陈颖

浙江工商大学信息与电子工程学院, 杭州 310018

*联系人, E-mail: happyty@aliyun.com

收稿日期: 2021-07-03; 接受日期: 2021-08-06; 网络出版日期: 2021-09-15

国家自然科学基金(编号: 62071430)、浙江省新型网络标准及应用技术重点实验室开放课题(编号: 2013E10012)和浙江省属高校基本业务费专项(编号: JRK21002)资助项目

摘要 本文提出一种新颖的基于具有极化和空模自由度的单光子的抗信息泄露量子对话(Quantum Dialogue, QD)协议, 利用量子加密技术克服信息泄露问题. 本文协议利用量子加密技术和诱骗光子技术对用于编码两个通信者隐秘经典比特的双自由度单光子进行双重保护. 为了避免信息泄露问题, 用于编码的双自由度单光子的初始态通过量子密钥加密和解密被两个通信者共享. 本文协议的信息论效率为40%.

关键词 量子对话, 量子加密, 极化自由度, 空模自由度, 信息泄露

PACS: 03.67.Dd, 03.65.Ud, 03.67.Hk

1 引言

众所周知, 量子密码诞生于1984年Bennett和Brassard^[1]提出的BB84量子密钥分配(Quantum Key Distribution, QKD)协议. 目前, 量子密码已经发展出多个分支, 如QKD^[1-4]、量子隐私比较(Quantum Private Comparison, QPC)^[5-9]、量子安全直接通信(Quantum Secure Direct Communication, QSDC)^[10-14]等. 自然而然地, 不同分支具有不同的功能. QKD的目标是借助于量子信号的传输在两个远距离通信者之间建立一个随机原始密钥. QPC的目标是判断两个用户的隐秘输入是否相等. QSDC致力于实现将隐秘消息从一个用户

直接传送给另一个用户而无需事先产生一个随机原始密钥对它进行加密.

事实上, 许多早期的QSDC协议仅能实现隐秘消息从发送者到接收者的单向传送, 但无法实现两个通信者隐秘消息的相互传送. 幸运的是, 在2004年, Zhang和Man^[15,16]以及Nguyen^[17]分别独立提出量子对话(Quantum Dialogue, QD)这一全新概念解决这个问题. 此后, 许多学者投入到QD的研究中, 构建了许多QD协议^[18-24]. 随后, Tan和Cai^[25]以及Gao等人^[26,27]分别独立发现一种特殊的称为信息泄露的安全漏洞, 它意味着一个外在攻击者Eve能轻易地从公开宣布中推断出关于通信者隐秘消息的部分信息而无需发起任何主

引用格式: 叶天语, 耿茂洁, 徐天婕, 等. 基于具有极化和空模自由度的单光子的量子加密量子对话. 中国科学: 物理学 力学 天文学, 2021, 51: 100311
Ye T Y, Geng M J, Xu T J, et al. Quantum dialogue based on quantum encryption with single photons in both polarization and spatial-mode degrees of freedom (in Chinese). Sci Sin-Phys Mech Astron, 2021, 51: 100311, doi: 10.1360/SSPMA-2021-0188

动攻击. 因此, 有效解决信息泄露问题对于QD是至关重要的. 2009年, Shi等人^[28]利用从一个通信者向另一个通信者直接传送共享的隐秘Bell态克服信息泄露问题. 2010年, Shi等人^[29,30]构建了利用直接传送共享的隐秘单光子克服信息泄露问题的QD协议以及基于Bell态相关提取性和辅助单光子的QD协议; Gao^[31]利用两个Bell态之间纠缠交换后的测量相关性来抵抗信息泄露问题. 2013年, Ye^[32]提出一个基于任意两个GHZ态之间纠缠交换和辅助GHZ态的大容量无信息泄露QD协议. 2014年, Ye^[33]设计了一个无信息泄露量子加密QD协议. 2015年, Huang和Ye^[34]利用辅助量子操作来解决信息泄露问题. 2020年, Gao^[35]指出文献^[36]的QD协议存在信息泄露, 并提出一个相应的改进方案.

最近, 许多学者采用具有极化和空模自由度的单光子设计不同类型的量子密码协议^[37-40]. 如果一个量子密码协议采用具有极化和空模自由度的单光子而非单自由度单光子作为量子资源, 它的量子通信容量通常会被极大提高.

基于以上分析, 在本文中, 我们采用具有极化和空模自由度的单光子作为量子资源提出一个新颖的无信息泄露QD协议, 利用量子加密技术克服信息泄露问题. 在所提出的QD协议中, 一个双自由度单光子总共能携带4个经典比特, 意味着本文协议具有较大的量子通信容量.

2 预备知识

具有极化和空模自由度的单光子态可被描述为^[37]

$$|\phi\rangle = |\phi\rangle_p \otimes |\phi\rangle_s, \quad (1)$$

式中, $|\phi\rangle_p$ 和 $|\phi\rangle_s$ 分别是具有极化自由度的单光子态和具有空模自由度的单光子态. $Z_p = \{|H\rangle, |V\rangle\}$ 和 $X_p = \{|R\rangle, |A\rangle\}$ 分别是极化自由度下的两组非正交测量基, 而 $Z_s = \{|b_1\rangle, |b_2\rangle\}$ 和 $X_s = \{|s\rangle, |a\rangle\}$ 是空模自由度下的两组非正交测量基. 这里,

$$\begin{aligned} |R\rangle &= \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \\ |A\rangle &= \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle), \\ |s\rangle &= \frac{1}{\sqrt{2}}(|b_1\rangle + |b_2\rangle), \\ |a\rangle &= \frac{1}{\sqrt{2}}(|b_1\rangle - |b_2\rangle), \end{aligned} \quad (2)$$

式中, $|H\rangle$ 和 $|V\rangle$ 分别是光子的水平极化态和垂直极化态, 而 $|b_1\rangle$ 和 $|b_2\rangle$ 分别是光子的上空模和下空模.

定义极化自由度下的两个酉操作为

$$\begin{aligned} I_p &= |H\rangle\langle H| + |V\rangle\langle V|, \\ U_p &= |V\rangle\langle H| - |H\rangle\langle V|. \end{aligned} \quad (3)$$

因此,

$$\begin{aligned} I_p|H\rangle &= |H\rangle, \quad I_p|V\rangle = |V\rangle, \\ I_p|R\rangle &= |R\rangle, \quad I_p|A\rangle = |A\rangle, \end{aligned} \quad (4)$$

$$\begin{aligned} U_p|H\rangle &= |V\rangle, \quad U_p|V\rangle = -|H\rangle, \\ U_p|R\rangle &= -|A\rangle, \quad U_p|A\rangle = |R\rangle. \end{aligned} \quad (5)$$

显然, U_p 只在基内翻转光子的量子态. 同样地, 定义空模自由度下的两个有趣酉操作为

$$\begin{aligned} I_s &= |b_1\rangle\langle b_1| + |b_2\rangle\langle b_2|, \\ U_s &= |b_2\rangle\langle b_1| - |b_1\rangle\langle b_2|, \end{aligned} \quad (6)$$

因此,

$$\begin{aligned} I_s|b_1\rangle &= |b_1\rangle, \quad I_s|b_2\rangle = |b_2\rangle, \\ I_s|s\rangle &= |s\rangle, \quad I_s|a\rangle = |a\rangle, \end{aligned} \quad (7)$$

$$\begin{aligned} U_s|b_1\rangle &= |b_2\rangle, \quad U_s|b_2\rangle = -|b_1\rangle, \\ U_s|s\rangle &= -|a\rangle, \quad U_s|a\rangle = |s\rangle. \end{aligned} \quad (8)$$

显然, U_s 只在基内翻转光子的量子态.

3 QD协议描述

两个通信者, Alice和Bob, 想交换他们的隐秘经典比特. 假设Alice的 $2N$ 隐秘经典比特为

$$\{(t_1, j_1), (t_2, j_2), \dots, (t_N, j_N)\}; \quad (9)$$

而Bob的 $2N$ 隐秘经典比特为

$$\{(k_1, l_1), (k_2, l_2), \dots, (k_i, l_i), \dots, (k_N, l_N)\}, \quad (10)$$

其中, $t_i, j_i, k_i, l_i \in \{0, 1\}$, $i \in \{1, 2, \dots, N\}$. 他们事先商定, 每个复合酉操作以如下规则对应两个经典比特:

$$\begin{aligned} C_{00} &= I_P \otimes I_S \rightarrow 00, \\ C_{01} &= I_P \otimes U_S \rightarrow 01, \\ C_{10} &= U_P \otimes I_S \rightarrow 10, \\ C_{11} &= U_P \otimes U_S \rightarrow 11. \end{aligned} \quad (11)$$

所提出的QD协议可描述如下.

步骤1: 量子密钥产生和传输. Alice制备 N 个四粒子纠缠态 $\{A_1^1 A_2^1 B_1^1 B_2^1, A_1^2 A_2^2 B_1^2 B_2^2, \dots, A_1^N A_2^N B_1^N B_2^N\}$ 都处于量子态

$$\begin{aligned} |\psi\rangle &= \frac{1}{2}(|H\rangle|H\rangle|H\rangle|H\rangle + |H\rangle|V\rangle|H\rangle|V\rangle \\ &\quad + |V\rangle|H\rangle|V\rangle|H\rangle + |V\rangle|V\rangle|V\rangle|V\rangle), \end{aligned} \quad (12)$$

其中, 上标1, 2, ..., N 代表这些四粒子纠缠态的顺序. Alice将这些四粒子纠缠态分别分割成4个粒子序列 $S_{A_1}, S_{A_2}, S_{B_1}, S_{B_2}$, 即

$$\begin{aligned} S_{A_1} &= \{A_1^1, A_1^2, \dots, A_1^N\}, S_{A_2} = \{A_2^1, A_2^2, \dots, A_2^N\}, \\ S_{B_1} &= \{B_1^1, B_1^2, \dots, B_1^N\} \text{ 和 } S_{B_2} = \{B_2^1, B_2^2, \dots, B_2^N\}. \end{aligned}$$

为了进行安全检测, Alice制备两组诱骗光子, 它们的每个粒子都随机处于4个量子态 $\{|H\rangle, |V\rangle, |R\rangle, |A\rangle\}$ 中的一个. 然后, Alice将一组诱骗光子随机插入 S_{B_1} 以组成粒子序列 S'_{B_1} , 并以块传输的方式^[10]将它发送给Bob. 同样地, Alice将另一组诱骗光子随机插入 S_{B_2} 以组成粒子序列 S'_{B_2} , 并以块传输的方式将它发送给Bob.

在Bob证实已经接收到 $S'_{B_1}(S'_{B_2})$ 后, Alice告诉Bob诱骗光子的位置和制备基. 然后, Bob利用正确的测量基测量相应的诱骗光子并告诉Alice他的测量结果. Alice通过对比Bob的测量结果和诱骗光子的初态来计算错误率. 如果 $S'_{B_1}(S'_{B_2})$ 的传输是安全的, 他们将继续执行下一步; 否则, 他们将终止通信.

步骤2: Alice的加密. Alice制备由 N 个具有极化和空模自由度的单光子态构成的序列, 即

$$S_T = \{|\phi\rangle_1, |\phi\rangle_2, \dots, |\phi\rangle_N\},$$

其中, 下标1, 2, ..., N 代表 S_T 中这些单光子态的顺序,

$$|\phi\rangle = |\phi\rangle_P \otimes |\phi\rangle_S, \quad |\phi\rangle_P \in \{|H\rangle, |V\rangle\} \text{ 和 } |\phi\rangle_S \in \{|b_1\rangle, |b_2\rangle\}.$$

Alice利用 Z_P 基分别测量粒子 A_1^i 和 A_2^i , 其中 $i=1, 2, \dots, N$. 为了加密 S_T 中的单光子态, Alice根据以下规则对它们施加复合酉操作: 如果粒子 A_1^i 和 A_2^i 的测量结果分别是 $|H\rangle$ 和 $|H\rangle$, Alice对 $|\phi\rangle_i$ 施加复合酉操作 C_{00} ; 如果粒子 A_1^i 和 A_2^i 的测量结果分别是 $|H\rangle$ 和 $|V\rangle$, Alice对 $|\phi\rangle_i$ 施加复合酉操作 C_{01} ; 如果粒子 A_1^i 和 A_2^i 的测量结果分别是 $|V\rangle$ 和 $|H\rangle$, Alice对 $|\phi\rangle_i$ 施加复合酉操作 C_{10} ; 如果粒子 A_1^i 和 A_2^i 的测量结果分别是 $|V\rangle$ 和 $|V\rangle$, Alice对 $|\phi\rangle_i$ 施加复合酉操作 C_{11} . 然后, Alice制备足够多的具有极化和空模自由度的诱骗单光子, 其中每个诱骗单光子随机处于16个量子态 $\{|H\rangle \otimes |b_1\rangle, |V\rangle \otimes |b_1\rangle, |R\rangle \otimes |b_1\rangle, |A\rangle \otimes |b_1\rangle, |H\rangle \otimes |b_2\rangle, |V\rangle \otimes |b_2\rangle, |R\rangle \otimes |b_2\rangle, |A\rangle \otimes |b_2\rangle, |H\rangle \otimes |s\rangle, |V\rangle \otimes |s\rangle, |R\rangle \otimes |s\rangle, |A\rangle \otimes |s\rangle, |H\rangle \otimes |a\rangle, |V\rangle \otimes |a\rangle, |R\rangle \otimes |a\rangle, |A\rangle \otimes |a\rangle\}$ 中的一个, 并将它们随机插入自己加密后的 S_T 以组成序列 S'_T . 最后, Alice以块传输的方式将 S'_T 发送给Bob.

在Bob证实接收到 S'_T 后, Alice和Bob一起执行与步骤1类似的安全检测过程. 如果 S'_T 的传送是安全的, 他们将继续执行下一步; 否则, 他们将终止通信.

步骤3: Bob的解密和编码. Bob丢弃 S'_T 中的诱骗单光子恢复Alice加密后的 S_T . 然后, Bob利用 Z_P 基分别测量粒子 B_1^i 和 B_2^i , 其中 $i=1, 2, \dots, N$. 接着, Bob解密Alice加密后的 S_T 中的单光子态. 即, 如果粒子 B_1^i 和 B_2^i 的测量结果分别是 $|H\rangle$ 和 $|H\rangle$, Bob对Alice加密后的 S_T 中的第 i 个单光子态施加复合酉操作 C_{00} ; 如果粒子 B_1^i 和 B_2^i 的测量结果分别是 $|H\rangle$ 和 $|V\rangle$, Bob对Alice加密后的 S_T 中的第 i 个单光子态施加复合酉操作 C_{01} ; 如果粒子 B_1^i 和 B_2^i 的测量结果分别是 $|V\rangle$ 和 $|H\rangle$, Bob对Alice加密后的 S_T 中的第 i 个单光子态施加复合酉操作 C_{10} ; 如果粒子 B_1^i 和 B_2^i 的测量结果分别是 $|V\rangle$ 和 $|V\rangle$, Bob对Alice加密后的 S_T 中的第 i 个单光子态施加复合酉操作 C_{11} . 显然, 在Bob的解密后, S_T 被恢复成 $\{|\phi\rangle_1, |\phi\rangle_2, \dots, |\phi\rangle_N\}$. 然后, Bob利

用 $Z_P \otimes Z_S$ 基测量 $|\phi\rangle_i$ 以知道它的初态. 根据他的测量结果, Bob 重新制备一个没有被测量过的新的 $|\phi\rangle_i$. 为了编码他的两个隐秘经典比特 (k_i, l_i) , Bob 对新的 $|\phi\rangle_i$ 施加复合酉操作 $C_{k_i l_i}$. 相应地, 新的 $|\phi\rangle_i$ 转变成 $C_{k_i l_i}|\phi\rangle_i$ 从而得到 $S_T'' = \{C_{k_1 l_1}|\phi\rangle_1, C_{k_2 l_2}|\phi\rangle_2, \dots, C_{k_N l_N}|\phi\rangle_N\}$. 为了安全检测, Bob 制备足够多的具有极化和空模自由度的诱骗单光子, 其中每个诱骗单光子随机处于 16 个量子态 $\{|H\rangle \otimes |b_1\rangle, |V\rangle \otimes |b_1\rangle, |R\rangle \otimes |b_1\rangle, |A\rangle \otimes |b_1\rangle, |H\rangle \otimes |b_2\rangle, |V\rangle \otimes |b_2\rangle, |R\rangle \otimes |b_2\rangle, |A\rangle \otimes |b_2\rangle, |H\rangle \otimes |s\rangle, |V\rangle \otimes |s\rangle, |R\rangle \otimes |s\rangle, |A\rangle \otimes |s\rangle, |H\rangle \otimes |a\rangle, |V\rangle \otimes |a\rangle, |R\rangle \otimes |a\rangle, |A\rangle \otimes |a\rangle\}$ 中的一个, 并将它们随机插入 S_T'' 以组成序列 S_T'' . 最后, Bob 以块传输的方式将 S_T'' 传送给 Alice.

在 Alice 证实已经接收到 S_T'' 后, Alice 和 Bob 一起执行与步骤 1 类似的安全检测过程. 如果 S_T'' 的传送是安全的, 他们将继续执行下一步; 否则, 他们将终止通信.

步骤 4: Alice 的编码和双向通信. Alice 丢弃 S_T'' 中的诱骗单光子恢复 S_T'' . 然后, 为了编码她的两个隐秘经典比特 (t_i, j_i) , Alice 对 $C_{k_i l_i}|\phi\rangle_i$ 施加复合酉操作 $C_{t_i j_i}$. 相应地, $C_{k_i l_i}|\phi\rangle_i$ 转变成 $C_{t_i j_i} C_{k_i l_i}|\phi\rangle_i$. 然后, Alice 利用 $Z_P \otimes Z_S$ 基测量 $C_{t_i j_i} C_{k_i l_i}|\phi\rangle_i$. 为了实现双向通信, Alice 公开宣布 $C_{t_i j_i} C_{k_i l_i}|\phi\rangle_i$ 的测量结果. 根据 $|\phi\rangle_i$ 的初态、她自己的复合酉操作 $C_{t_i j_i}$ 以及 $C_{t_i j_i} C_{k_i l_i}|\phi\rangle_i$ 的测量结果, Alice 能读出 Bob 的两个隐秘经典比特 (k_i, l_i) . 同样地, 根据他知道的 $|\phi\rangle_i$ 的初态、他自己的复合酉操作 $C_{k_i l_i}$ 以及 Alice 对 $C_{t_i j_i} C_{k_i l_i}|\phi\rangle_i$ 的测量结果的宣布, Bob 也能读出 Alice 的两个隐秘经典比特 (t_i, j_i) .

现在我们用一个例子来进一步解释双向通信过程. 假设 (t_1, j_1) , (k_1, l_1) 和 $|\phi\rangle_1$ 分别是 $(0, 0)$, $(0, 1)$ 和 $|H\rangle \otimes |b_1\rangle$. Alice 制备一个四粒子量子态 $A_1^1 A_2^1 B_1^1 B_2^1$ 处于 $|\psi\rangle$ 并将粒子 B_1^1 和 B_2^1 传送给 Bob. 然后, Alice 利用 Z_P 基测量粒子 A_1^1 和 A_2^1 . 不失一般性, 假设 Alice 对粒子 A_1^1 和 A_2^1 的测量结果分别为 $|V\rangle$ 和 $|H\rangle$. 相应地, Alice 对 $|\phi\rangle_1$

施加复合酉操作 C_{10} 进行加密从而得到加密后的 $|\phi\rangle_1$ (即 $|V\rangle \otimes |b_1\rangle$). 然后, Alice 将加密后的 $|\phi\rangle_1$ 传送给 Bob. Bob 利用 Z_P 基测量粒子 B_1^1 和 B_2^1 分别得到测量结果 $|V\rangle$ 和 $|H\rangle$, 并对 Alice 加密后的 $|\phi\rangle_1$ 施加复合酉操作 C_{10} 解密出 $|\phi\rangle_1$. 然后, Bob 利用 $Z_P \otimes Z_S$ 基测量 $|\phi\rangle_1$ 以知道它的初态. 根据他的测量结果, Bob 重新制备一个没有被测量过的新的 $|\phi\rangle_1$. 因此, 新的 $|\phi\rangle_1$ 按照以下过程演化:

$$\begin{aligned} |\phi\rangle_1 &= |H\rangle \otimes |b_1\rangle \Rightarrow C_{01}|\phi\rangle_1 \\ &= (I_P \otimes U_S)(|H\rangle \otimes |b_1\rangle) \\ &= |H\rangle \otimes |b_2\rangle \Rightarrow C_{00}C_{01}|\phi\rangle_1 \\ &= (I_P \otimes I_S)(|H\rangle \otimes |b_2\rangle) \\ &= |H\rangle \otimes |b_2\rangle. \end{aligned} \quad (13)$$

根据 $|H\rangle \otimes |b_2\rangle$ 被宣布的测量结果、 $|H\rangle \otimes |b_1\rangle$ 的初始制备态以及她的复合酉操作 C_{00} 这三种已知信息, Alice 能读出 (k_1, l_1) 为 $(0, 1)$. 类似地, 根据 $|H\rangle \otimes |b_2\rangle$ 被宣布的测量结果、 $|H\rangle \otimes |b_1\rangle$ 的初始制备态以及他的复合酉操作 C_{01} , Bob 能读出 (t_1, j_1) 为 $(0, 0)$.

4 安全性分析

(1) 外在攻击者的主动攻击

我们根据所提出的 QD 协议的每个步骤对外在攻击者的主动攻击进行安全性分析.

量子密钥产生和传输. 在这步中, Alice 制备 N 个四粒子纠缠态都处于 $|\psi\rangle$ 作为量子私钥, 并将 S_{B_1}' 和 S_{B_2}' 传送给 Bob. Eve 会尽其所能去得到 S_{B_1} 和 S_{B_2} , 并利用它们去解密 Alice 随后传送给 Bob 的密文. 如果 Eve 能成功地做到这点, 她将能知道 $|\phi\rangle_i$ 的初态, 从而导致 Eve 在 Alice 宣布 $C_{t_i j_i} C_{k_i l_i}|\phi\rangle_i$ 的测量结果后能合法地知道 Alice 的两个隐秘经典比特 (t_i, j_i) 和 Bob 的两个隐秘经典比特 (k_i, l_i) 之间的经典相关性^[25]. 幸运的是, Eve 无法实现这个目标, 其原因在于: 由于 Eve 无法知道诱骗光子的真正位置, 她对 S_{B_1}' 和 S_{B_2}' 的攻击将不可避免地在诱骗光子上留有痕迹从而被 Alice 和 Bob 检测到. 值得强调的是, 诱

骗光子技术^[41,42]可被视为BB84 QKD协议^[1]的安全检测方法的一个变种, 这种安全检测方法已被证实是无条件安全的^[43].

Alice的加密. 在这步中, Alice加密 $|\phi\rangle_i$ 并将密文传送给Bob. 如果Eve想解密出 $|\phi\rangle_i$ 的初态, 她首先需要在量子私钥的传输过程中知道粒子 B_1^i 和 B_2^i 的状态. 然而, 正如以上所分析的, 诱骗光子技术的应用能阻止Eve达到这一目标. 事实上, 由于这步采用了诱骗光子技术, Eve无法截获密文而不被发现. 文献^[44]已经证实, 这步采用的诱骗光子技术能有效防止Eve发起的截获-重发攻击、测量-重发攻击和纠缠-测量攻击. 例如, 根据文献^[44], 由于Bob对假诱骗单光子的测量结果并不总是与对真实诱骗单光子的测量结果一致, Eve的截获-重发攻击能以 $1 - \left(\frac{1}{4}\right)^{\delta_1}$ 的概率被安全检测过程发现; 由于Eve对诱骗单光子的测量基并不总是与Alice的制备基相同, Eve的测量-重发攻击能以 $1 - \left(\frac{9}{16}\right)^{\delta_1}$ 的概率被安全检测过程发现. 这里, δ_1 是诱骗光子的数量.

Bob的解密和编码. 在这步中, Bob解密出 $|\phi\rangle_i$ 的初态, 对其编码自己的两个隐秘经典比特 (k_i, l_i) , 并将粒子 $C_{k_i l_i}|\phi\rangle_i$ 传送给Alice. 即使截获粒子 $C_{k_i l_i}|\phi\rangle_i$, 由于Eve不知道 $|\phi\rangle_i$ 的初态, 她仍然无法从 $C_{k_i l_i}|\phi\rangle_i$ 中提取出 (k_i, l_i) . 事实上, 因为这步采用了诱骗光子技术, Eve无法截获 $C_{k_i l_i}|\phi\rangle_i$ 而不被检测到.

Alice的编码和双向通信. 在这步中, Alice对 $C_{k_i l_i}|\phi\rangle_i$ 编码她的两个隐秘经典比特 (t_i, j_i) , 并与Bob完成双向通信过程. 显然, 这步不存在量子态传输, 从而导致Eve没有机会在这步发起攻击.

(2) 信息泄露问题

不失一般性, 这里以第3节的例子为例来分析信息泄露问题.

借助于量子私钥 $|\psi\rangle$, Bob能确切地知道 $|\phi\rangle_1$ 的初态, 因此Alice没有必要对它进行公开的宣布. 在这种情形下, Eve无法知道 $|\phi\rangle_1$ 的初态. 因此, 当Eve从Alice听到 $C_{00}C_{01}|\phi\rangle_1$ 的测量结果, 她不得不随机猜测 $|\phi\rangle_1$ 的初态.

如果她猜测 $|\phi\rangle_1$ 的初态为 $|H\rangle \otimes |b_1\rangle$, 她将会认为 $\{(t_1, j_1), (k_1, l_1)\}$ 是 $\{(0, 0), (0, 1)\}, \{(0, 1), (0, 0)\}, \{(1, 0), (1, 1)\}$ 和 $\{(1, 1), (1, 0)\}$ 中的一个; 如果她猜测 $|\phi\rangle_1$ 的初态为 $|H\rangle \otimes |b_2\rangle$, 她将会认为 $\{(t_1, j_1), (k_1, l_1)\}$ 是 $\{(0, 0), (0, 0)\}, \{(0, 1), (0, 1)\}, \{(1, 0), (1, 0)\}$ 和 $\{(1, 1), (1, 1)\}$ 中的一个; 如果她猜测 $|\phi\rangle_1$ 的初态为 $|V\rangle \otimes |b_1\rangle$, 她将会认为 $\{(t_1, j_1), (k_1, l_1)\}$ 是 $\{(0, 0), (1, 1)\}, \{(0, 1), (1, 0)\}, \{(1, 0), (0, 1)\}$ 和 $\{(1, 1), (0, 0)\}$ 中的一个; 如果她猜测 $|\phi\rangle_1$ 的初态为 $|V\rangle \otimes |b_2\rangle$, 她将会认为 $\{(t_1, j_1), (k_1, l_1)\}$ 是 $\{(0, 0), (1, 0)\}, \{(0, 1), (1, 1)\}, \{(1, 0), (0, 0)\}$ 和 $\{(1, 1), (0, 1)\}$ 中的一个. 因此, 对于Eve而言, $\{(t_1, j_1), (k_1, l_1)\}$ 总共有16种可能性. 根据Shannon^[45]的信息论, 这16种可能性共包含了 $-\sum_{i=1}^{16} p_i \log_2 p_i = -\sum_{i=1}^{16} \frac{1}{16} \times \log_2 \frac{1}{16} = 4$ 比特信息, 正好等于 (t_1, j_1) 和 (k_1, l_1) 的总比特数. 因此, (t_1, j_1) 和 (k_1, l_1) 都没有被泄露给Eve. 可以得出结论, 所提出的QD协议能避免信息泄露问题.

5 讨论与结论

(1) 信息论效率

信息论效率^[3]被定义为

$$\gamma = \frac{b_s}{q_t + b_t} \times 100\%, \quad (14)$$

其中, b_s , q_t 和 b_t 分别是期望接收到的隐秘经典比特, 所消耗的量子比特和所消耗的用于Alice和Bob之间通信的经典比特. 在所提出的QD协议中, 若不考虑安全检测过程, $|\phi\rangle_i$ 可被用于交换Alice的两个隐秘经典比特 (t_i, j_i) 和Bob的两个隐秘经典比特 (k_i, l_i) , 与此同时, 两个经典比特被消耗于Alice对 $C_{t_i j_i} C_{k_i l_i} |\phi\rangle_i$ 的测量结果的宣布中. 另外, 一个四粒子量子纠缠态 $|\psi\rangle$ 被用于加密 $|\phi\rangle_i$, 而且Bob需重新制备一个没有被测量过的新 $|\phi\rangle_i$. 因此, 所提出的QD协议的信息论效率为

$$\gamma = \frac{2+2}{2+4+2+2} \times 100\% = 40\%.$$

(2) 与之前基于具有极化和空模自由度的单光子的QD协议的对比

最近, Wang等人^[38]也提出一个基于具有极化和空模自由度的单光子的QD协议. 随后, Zhang和Situ^[39]发现, 文献[38]的QD协议具有信息泄露这一安全漏洞, 并提出通过修改Alice和Bob的编码规则避免这个问题. 在文献[39]中, 不考虑安全检测过程, 一个具有极化和空模自由度的单光子能被用于交换Alice的1个经典比特和Bob的1个经典比特, 与此同时, 2个经典比特被消耗于Alice对R的值的宣布. 因此, 文献[39]的信息论效率为 $\gamma = \frac{1+1}{2+2} \times 100\% = 50\%$. 然而, 在文献[39]中, 一个具有极化和空模自由度的单光子总共只能携带2个经典比特. 在所提出的QD协议中, 一个具有极化和空模自由度的单光子总共能携带4个经典比特. 因此, 尽管所提出的QD协议的信息论效率比文献[39]小一点, 但它的量子通信容量是文献[39]的2倍.

另外, 我们最近在文献[44]中提出了一个基于具有极化和空模自由度的单光子的抗信息泄露QD协议. 在文献[44]中, 不考虑安全检测过程, 两个相邻的单光子能被用于交换Alice的2个经典比特和Bob的2个经典比特, 与此同时, 4个经典比特被消耗于Bob对单光子编码后的最终量子态的测量结果的宣布. 因此, 文献[44]的信息论效率为 $\gamma = \frac{2+2}{2+2+4} \times 100\% = 50\%$. 然而, 文献[44]需要制备两个相邻的具有极化和空模自由度的单光子处于相同的量子态, 这在现实中会较难实现. 尽管所提出的QD协议的信息论效率比文献[44]小一点, 它不存在“制备两个相邻的具有极化和空模自由度的单光子处于相同的量子态”这个麻烦.

(3) 四粒子纠缠态 $|\psi\rangle$ 的制备

这里进一步说明如何制备四粒子纠缠态 $|\psi\rangle$. 首先, 产生三粒子GHZ态:

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|H\rangle|H\rangle|H\rangle + |V\rangle|V\rangle|V\rangle)_{123}. \quad (15)$$

然后, 对 $|\phi\rangle$ 的每个粒子施加哈达玛操作得到三粒子类GHZ态:

$$\begin{aligned} |\omega\rangle &= D_1 D_2 D_3 |\phi\rangle \\ &= \frac{1}{2}(|HHH\rangle + |HVV\rangle + |VHH\rangle + |VHV\rangle)_{123}, \end{aligned} \quad (16)$$

其中, 哈达玛操作为

$$D = \frac{1}{\sqrt{2}}[(|H\rangle + |V\rangle)\langle H| + (|H\rangle - |V\rangle)\langle V|]. \quad (17)$$

接着, 制备单粒子 $|H\rangle$, 与 $|\omega\rangle$ 进行张量积得到

$$\begin{aligned} |\chi\rangle &= |\omega\rangle \otimes |H\rangle \\ &= \frac{1}{2}(|HHHH\rangle + |HVVH\rangle + |VHHH\rangle + |VHVH\rangle)_{1234}. \end{aligned} \quad (18)$$

最后, 以第2个粒子为控制量子比特, 第3和第4个粒子分别为目标量子比特对 $|\chi\rangle$ 施加两次控制非操作得到 $|\psi\rangle$.

总之, 在本文中, 我们提出一种新颖的基于具有极化和空模自由度的单光子的抗信息泄露QD协议, 利用量子加密技术克服信息泄露问题. 所提出的QD协议利用量子加密技术和诱骗光子技术对用于编码两个通信者隐秘经典比特的双自由度单光子进行双重保护. 用于编码的双自由度单光子的初始态通过量子密钥加密和解密被两个通信者共享, 从而避免了信息泄露问题. 所提出的QD协议的信息论效率为40%. 所提出的QD协议的量子通信容量为文献[39]协议的2倍, 并且无需制备两个相邻的双自由度单光子处于相同的状态. 在将来, 为了进一步提高信息论效率, 我们将致力于研究如何使量子密钥能被重复使用.

参考文献

- 1 Bennett C H, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. Bangalore: IEEE Press, 1984. 175–179
- 2 Bennett C H, Brassard G, Mermin N D. Quantum cryptography without Bell's theorem. *Phys Rev Lett*, 1992, 68: 557–559
- 3 Cabello A. Quantum key distribution in the Holevo limit. *Phys Rev Lett*, 2000, 85: 5635–5638, arXiv: quant-ph/0007064
- 4 Beige A, Englert B G, Kurtsiefer C, et al. Secure communication with a publicly known key. *Acta Phys Pol A*, 2002, 101: 357–368
- 5 Yang Y G, Wen Q Y. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. *J Phys A-Math Theor*, 2009, 42: 055305

- 6 Yang Y G, Cao W F, Wen Q Y. Secure quantum private comparison. *Phys Scr*, 2009, 80: 065002
- 7 Yang Y G, Xia J, Jia X, et al. New quantum private comparison protocol without entanglement. *Int J Quantum Inform*, 2012, 10: 1250065
- 8 Liu B, Gao F, Jia H Y, et al. Efficient quantum private comparison employing single photons and collective detection. *Quantum Inf Process*, 2013, 12: 887–897
- 9 Ye T Y. Quantum private comparison via cavity QED. *Commun Theor Phys*, 2017, 67: 147–156
- 10 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys Rev A*, 2002, 65: 032302, arXiv: [quant-ph/0012056](#)
- 11 Boström K, Felbinger T. Deterministic secure direct communication using entanglement. *Phys Rev Lett*, 2002, 89: 187902, arXiv: [quant-ph/0203064](#)
- 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, arXiv: [quant-ph/0308173](#)
- 13 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. *Phys Rev A*, 2004, 69: 052319, arXiv: [quant-ph/0405177](#)
- 14 Wang C, Deng F G, Li Y S, et al. Quantum secure direct communication with high-dimension quantum superdense coding. *Phys Rev A*, 2005, 71: 044305
- 15 Zhang Z J, Man Z X. Secure direct bidirectional communication protocol using the Einstein-Podolsky-Rosen pair block. arXiv: [0403215](#)
- 16 Zhang Z J, Man Z X. Secure bidirectional quantum communication protocol without quantum channel. arXiv: [0403217](#)
- 17 Nguyen B A. Quantum dialogue. *Phys Lett A*, 2004, 328: 6–10
- 18 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, arXiv: [quant-ph/0601125](#)
- 19 Man Z X, Xia Y J. Controlled bidirectional quantum direct communication by using a GHZ state. *Chin Phys Lett*, 2006, 23: 1680–1682
- 20 Ji X, Zhang S. Secure quantum dialogue based on single-photon. *Chin Phys*, 2006, 15: 1418–1420
- 21 Man Z X, Xia Y J, Nguyen B A. Quantum secure direct communication by using GHZ states and entanglement swapping. *J Phys B-At Mol Opt Phys*, 2006, 39: 3855–3863
- 22 Yang Y G, Wen Q Y. Quasi-secure quantum dialogue using single photons. *Sci China Ser G-Phys Mech Astron*, 2007, 50: 558–562
- 23 Shan C J, Liu J B, Cheng W W, et al. Bidirectional quantum secure direct communication in driven cavity QED. *Mod Phys Lett B*, 2009, 23: 3225–3234
- 24 Ye T Y, Jiang L Z. Improvement of controlled bidirectional quantum direct communication using a GHZ state. *Chin Phys Lett*, 2013, 30: 040305
- 25 Tan Y G, Cai Q Y. Classical correlation in quantum dialogue. *Int J Quantum Inform*, 2008, 6: 325–329
- 26 Gao F, Qin S J, Wen Q Y, et al. Comment on: “Three-party quantum secure direct communication based on GHZ states” [Phys. Lett. A 354 (2006) 67]. *Phys Lett A*, 2008, 372: 3333–3336
- 27 Gao F, Guo F Z, Wen Q Y, et al. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. *Sci China Ser G-Phys Mech Astron*, 2008, 51: 559–566, arXiv: [0801.2420](#)
- 28 Shi G F, Xi X Q, Tian X L, et al. Bidirectional quantum secure communication based on a shared private Bell state. *Opt Commun*, 2009, 282: 2460–2463
- 29 Shi G F, Xi X Q, Hu M L, et al. Quantum secure dialogue by using single photons. *Opt Commun*, 2010, 283: 1984–1986
- 30 Shi G F. Bidirectional quantum secure communication scheme based on Bell states and auxiliary particles. *Opt Commun*, 2010, 283: 5275–5278
- 31 Gao G. Two quantum dialogue protocols without information leakage. *Opt Commun*, 2010, 283: 2288–2293
- 32 Ye T Y. Large payload bidirectional quantum secure direct communication without information leakage. *Int J Quantum Inform*, 2013, 11: 1350051
- 33 Ye T Y. Quantum secure dialogue with quantum encryption. *Commun Theor Phys*, 2014, 62: 338–342
- 34 Huang L Y, Ye T Y. A kind of quantum dialogue protocols without information leakage assisted by auxiliary quantum operation. *Int J Theor Phys*, 2015, 54: 2494–2504
- 35 Gao G. Information leakage in protection of quantum dialogue affected by quantum field. *Quantum Inf Process*, 2020, 19: 300
- 36 Huang Z M, Situ H Z. Protection of quantum dialogue affected by quantum field. *Quantum Inf Process*, 2019, 18: 37
- 37 Liu D, Chen J L, Jiang W. High-capacity quantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys*, 2012, 51: 2923–2929

- 38 Wang L L, Ma W P, Shen D S, et al. Efficient bidirectional quantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys*, 2015, 54: 3443–3453
- 39 Zhang C, Situ H Z. Information leakage in efficient bidirectional quantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys*, 2016, 55: 4702–4708
- 40 Wang L L, Ma W P, Wang M L, et al. Three-party quantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys*, 2016, 55: 2490–2499
- 41 Li C Y, Zhou H Y, Wang Y, et al. Secure quantum key distribution network with Bell states and local unitary operations. *Chin Phys Lett*, 2005, 22: 1049–1052, arXiv: [0705.1746](#)
- 42 Li C Y, Li X H, Deng F G, et al. Efficient quantum cryptography network without entanglement and quantum memory. *Chin Phys Lett*, 2006, 23: 2896–2899, arXiv: [0705.1748](#)
- 43 Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys Rev Lett*, 2000, 85: 441–444, arXiv: [quant-ph/0003004](#)
- 44 Ye T Y, Li H K, Hu J L. Information leakage resistant quantum dialogue with single photons in both polarization and spatial-mode degrees of freedom. *Quantum Inf Process*, 2021, 20: 209
- 45 Shannon C E. Communication theory of secrecy systems. *Bell Syst Technical J*, 1949, 28: 656–715

Quantum dialogue based on quantum encryption with single photons in both polarization and spatial-mode degrees of freedom

YE TianYu^{*}, GENG MaoJie, XU TianJie & CHEN Ying

College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China

In this paper, a novel information-leakage-resistant quantum dialogue (QD) protocol with single photons in both polarization and spatial-mode degrees of freedom is proposed. This protocol utilizes quantum encryption technology to overcome the information leakage problem; the protocol utilizes quantum encryption and decoy photon technologies to dually protect the single photons with two degrees of freedom used for encoding two communicants' private classical bits, and makes the initial states of the single photons with two degrees of freedom for encoding shared between two communicants through quantum key encryption and decryption. The information-theoretical efficiency of this protocol is 40%.

quantum dialogue, quantum encryption, polarization degree, spatial-mode degree, information leakage

PACS: 03.67.Dd, 03.65.Ud, 03.67.Hk

doi: [10.1360/SSPMA-2021-0188](#)