基于单光子双量子态的确定性的安全量子通信*

危语嫣 [1)] 高子凯 [1)] 王思颖 [1)] 朱雅静 [1)] 李涛 [1)2)] †

1) (南京理工大学理学院，南京 210094)

2) (半导体微纳结构与量子信息感知工业和信息化部重点实验室，南京理工大学，南京 210094)

摘 要

量子通信是量子科学技术的一个重要研究领域,是一种利用量子力学原理,能够在合法各方之间安全地传输私密信息的通信方式.基于单光子的确定性安全量子通信通常需要在发送方和接收方之间来回两次传输单光子态,并利用局域幺正变换加载信息.本文提出了一种单向传输单光子态的确定性安全量子通信方案.发送方利用单光子的极化和 time-bin 两自由度构成的两组共轭基矢量来编码经典逻辑比特.接收方通过设计合适的测量装置可以在发送方辅助下确定性地获取比特信息并感知窃听,从而实现信息的确定性安全传输.另外,我们的协议使用线性光学元件和单光子探测器,可以在当前的量子通信装置上实现.

关键词: 量子通信，确定性的，单光子，两自由度

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

1 引 言

近年来，量子信息科学领域的研究发展已经取得了显著的成就，有望改变信息处理世界的未来[1].量子密码学也已逐渐成为量子信息最具成效、用途最广的应用之一.对于经典加密而言，原则上只要有足够强大的计算机系统，基于数学问题计算复杂度的现代密码学公钥秘密体系就可能被破译;而对于量子加密而言，任何形式的窃听都将会被合法用户检测到.因此，量子通信成为量子信息研究的一个主要内容，具有很好的应用前景.目前已有的量子保密通信方案主要有三类: (1)量子密钥分发(quantum

* 江苏省自然科学基金 (批准号: BK20180461) 和国家自然科学基金 (批准号: 11914171) 资助的课题.

† 通信作者. E-mail: tao.li@njust.edu.cn

key distribution, QKD)[2-6]; (2)量子安全直接通信(quantum secure direct communication, QSDC)[7-14]; (3)量子机密共享(quantum secret sharing, QSS)[15-18].

QKD 方案中使用量子信道生成量子密钥, 利用经典信道传输用于基矢比对、窃听检测的辅助信息, 最终通信双方可以成功获得共享的随机密钥[2-6].QSDC 使用量子态加载信息, 它能借助量子信道安全无泄漏地直接传输机密信息[7-14].为此, 与 QKD 不同, QSDC 不需要提前生成密钥, 是直接利用量子信道进行通信的.QSS 方案是一种利用量子信道实现多方之间秘密共享的通信方法[15-18], 能够加强对信息的保密强度, 是一种多方之间的通信.

对于不同的量子通信方案, 各有各的特点, 它们可能在使用的光子状态、量子信道类型或协议安全性方面有所不同.1984 年, Bennett 和 Brassard[2]提出了利用单光子的两组非正交极化状态进行编码通信的量子密钥分发方案(BB84);随后, 人们提出了基于量子纠缠以及一些考虑实际噪声的量子密钥分发方案[3-6].在这些方案中, 发送方和接收方之间往往涉及两组共轭基矢, 他们随机选取一组基矢进行量子态的制备或测量, 只有当他们使用相同基矢时, 二者之间可以形成一种关联, 从而用于安全检测和密钥生成.由于二者只有1/2 的概率使用相同的基矢, 为此, 这类量子密钥分发是概率性的. 2000 年, 清华大学的龙桂鲁和刘晓曙提出了一种基于 EPR 纠缠光子对的确定性量子密钥分发方案[7].与前面的量子密钥分发不同, 该方案能够直接利用量子信道传输经典信息, 而且是确定性的.因此, 该方案也是第一个 QSDC 方案.2003 年, 邓富国等人提出了两步量子安全直接通信方案, 他们使用 EPR 纠缠光子对并利用两次单向量子信道来传递信息[8];2004 年, 邓富国和龙桂鲁[9]提出了第一个基于单光子的一次一密 DL04 方案, 在他们的方案中单光子通过双向量子信道传输经典信息.

1999 年, Shimizu 和 Imoto 借鉴 BB84 方案单光子共轭编码的思路, 提出了一个利用 EPR 纠缠光子对加载共轭编码从而分发确定性密钥的方案[19].在此方案中, 发送方利用两组共轭的基矢将密钥加载在纠缠光子对上并将其作为整体发送给接收方.利用完全贝尔态测量和发送方的基矢信息, 接收

方可以确定性的读出所接收到的密钥，可以用于实现确定性安全量子通信(deterministic secure quantum communication, DSQC). 2002 年, Boström 和 Felbinger 使用线性光学元件可区分的两个贝尔态和双向传输量子信道，提出了一个准安全的确定性量子通信方案 (记为 ping-pong 协议)[20]. 随后多个研究组进一步研究并发展了 ping-pong 协议[21, 22]. 起初，因为 QSDC 和 DSQC 都可以确定性的实现信息的传输，人们并没有特别区分这两类方案[23]. QSDC 与 DSQC 最大的区别在于除窃听检测外是否需要交换其它经典信息: QSDC 无需交换其它经典信息便可直接读出发送方发送的机密信息，而 DSQC 则需要交换其它经典信息才可以读出发送方发送的机密信息. 此外, QSDC 在量子存储的辅助下消除了所有与密钥相关的安全漏洞，成为量子通信的一个重要分支，在理论和实验上都取得了很多突破[14,24,25].

在当前技术水平下，相对于 QSDC, DSQC 在完成安全性检测后无需再次使用量子信道,从而避免了对量子存储的需求[26]，能够直接依托量子密钥分发装置提供更高的通信效率[19-23, 27-32]，国内外大量的学者和公司的科研技术人员都在从事这一方面的研究，相关的实验与理论也取得了很大的进展. 2005 年, Lucamarini 和 Mancini[27]提出了一种无需量子纠缠的确定性通信方案，它利用双向量子信道中的单光子非正交态来获得无条件的安全性和高效率的传输.2010 年, Wang 等[33]人提出一个基于单光子双量子位(两个自由度联合编码)的量子密钥分发方案，该方案使用极化和相位差分来对单光子进行编码，从而提高了密钥的生成效率.随后，多个研究组给出了单光子非正交态编码下 DSQC 的安全性分析[34-36]. 2020 年, Tarek[30]提出了一个基于非纠缠光子对的 DSQC 方案，该方案使用两个光子编码一个经典比特，并且使用一个单向量子信道和一个经典信道实现对经典比特信息的确定性分发.

本文中，我们提出了一种基于单光子双量子位编码的 DSQC 方案.我们的方案使用单个光子的极化和 time-bin 两自由度构成的共轭基矢量来编码经典逻辑比特，最终只需要使用一个单向量子信道和一个经典信道就可以实现确定性的安全量子通信.在理想状态下，我们的方案和 Tarek[30]的方案一样可

以在通信双方之间确定性地生成共享密钥.考虑到光子的传输效率和单光子的实际探测效率，我们的方案相比 Tarek[30]的方案具有更高的效率，从而能够更好地服务于私密信息的传输.

2 单光子双量子态的 DSQC 方案

在第二部分，我们将通过单光子逻辑比特态的制备、单光子逻辑比特态的测量、安全检测和信息收发四个步骤来详细介绍我们的方案.在单光子逻辑比特态的制备中, Alice 可以通过对光学元件的调控,制备出编码经典比特的光量子态.在单光子逻辑比特的测量和安全检测中, Bob 记录下每个光子对应的探测器响应情况. Alice 根据 Bob 随机公布的部分信息判断是否有窃听者的存在.在通过安全检测后, Ailce 和 Bob 进一步进行信息收发.

2.1 单光子逻辑比特态制备

单光子双量子态 DSQC 方案的核心部分是量子态制备和量子态测量.对于逻辑比特 0，采用量子态$|+t_0\rangle$和$|Ht_+\rangle$来编码;对于逻辑比特 1，采用量子态$|-t_1\rangle$和$|Vt_-\rangle$来编码.这里，$|H\rangle$和$|V\rangle$表示水平极化和垂直极化，并且$|\pm\rangle=(|H\rangle\pm|V\rangle)/\sqrt{2}$；$|t_0\rangle$和$|t_1\rangle$表示两个 time-bin 时间状态，并且$|t_\pm\rangle=(|t_0\rangle\pm|t_1\rangle)/\sqrt{2}$.在量子态制备中，发送方 Alice 利用单光子源制备一个单光子序列，其中每个光子均处于量子态$|Ht_0\rangle$.为了简化表述，我们设定每个光子的初始时刻为t_0.利用图 1 光路, Alice 可以确定性地编码逻辑比特 0 ($|+t_0\rangle$和$|Ht_+\rangle$)和逻辑比特 1 ($|-t_1\rangle$和$|Vt_-\rangle$).

在编码逻辑比特 0 时，图1中的*HWP*光轴设置为水平方向θ=0，使得穿过它的光子极化状态保持不变.Alice 通过控制开关*SW*1可以确定性地制备量子态$|+t_0\rangle$和$|Ht_+\rangle$:

(1)当 Alice 控制*SW*1处于透射*T*状态时，光子透过*SW*1，进而透过光轴方向为$\pi/8$的半波片*H*1，光子态$|Ht_0\rangle$变为$|+t_0\rangle$，到达极化分束器*PBS*1(*PBS*1和*PBS*2透射$|+\rangle$，反射$|-\rangle$).经过*PBS*1透射后，光子透过*PBS*2，经*SW*3反射后以量子态$|+t_0\rangle$进入量子信道，发送给接收方 Bob.

(2)当 Alice 控制 $SW1$ 处于反射 R 状态时，光子经过 $SW1$ 反射到达分束器 $BS1$，并由 $BS1$ 的两个输出端口等概率幅的输出.其中，一路直接达到 $SW2$，另一路通过相位调制器 PM （引入相移 $\varphi=0$ ）到达 $SW2$.两路径经 $SW2$ 合束后，光子态变为 $|Ht_+\rangle$，并透过 $SW3$ 进入量子信道发送给 Bob.这样，在编码逻辑比特 0 时，Alice 利用光学元件可以确定性地制备 $|+t_0\rangle$ 或 $|Ht_+\rangle$ 两种量子态，并通过同一量子信道发送给 Bob.

在编码逻辑比特 1 时，图1中半波片 HWP 的光轴设置为水平方向 $\theta=\pi/4$，使得穿过它的光子态 $|Ht_0\rangle$ 变为 $|Vt_0\rangle$.随后，Alice 通过控制 $SW1$ 可以确定性地制备量子态 $|-t_1\rangle$ 或 $|Vt_-\rangle$:

(1)当 Alice 控制 $SW1$ 处于透射 T 状态时，光子透过 $SW1$ 和 $H1$，光子态 $|Vt_0\rangle$ 变为 $|-t_0\rangle$，进而经过 $PBS1$ 反射进入长路径引入 t_1 延迟.此时，光子状态变为 $|-t_1\rangle$，再经过 $PBS2$ 反射、$SW3$ 透射进入量子信道发送给 Bob;

(2)当 Alice 控制 $SW1$ 处于反射 R 状态时，光子经过 $SW1$ 反射到达 $BS1$，并由 $BS1$ 的两个输出端口等概率幅输出.其中，一路直接达到 $SW2$，另一路通过相位调制器 PM （引入相移 $\varphi=\pi$ ）到达 $SW2$.两路径经 $SW2$ 合束，光子状态变为 $|Vt_-\rangle$，并透过 $SW3$ 进入量子信道传输给 Bob.这样，在编码逻辑比特 1 时，Alice 利用光学元件可以确定性地制备 $|-t_1\rangle$ 或 $|Vt_-\rangle$ 两种量子态，并通过同一量子信道发送给 Bob.

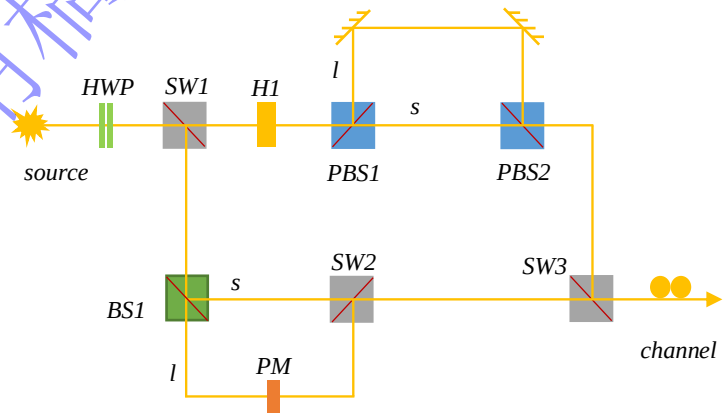

图 1 量子逻辑比特制备示意图. HWP :半波片,光轴与水平方向的夹角 $\theta=0$，穿过它的光子极化状态保持不变，$\theta=\pi/4$，对穿过它的光子执行以下操作: $|H\rangle\rightarrow|V\rangle$、$|V\rangle\rightarrow|H\rangle$; $SWi\ (i=1,2,3)$:开关，处于 T 状态时，光子直

接透过器件，处于 R 状态时，光子将被反射；$H1$:光轴角度为 $\pi/8$ 的半波片，对经过的光子进行以下操作：$|H\rangle \to |+\rangle$、$|V\rangle \to |-\rangle$；$PBS1$、$PBS2$:极化分束器，将透射 $|+\rangle$ 光子，反射 $|-\rangle$ 光子；PM:相位调制器，产生 $\varphi = 0$ 或 $\varphi = \pi$ 的相位差；$BS1$:50:50 分束器.

Fig.1 Schematics of quantum logic qubit preparation. HWP: half wave plate with its axis aligned at $\theta = 0$ ($\theta = \pi/4$) completes the transformations $|H\rangle \to |H\rangle, |V\rangle \to |V\rangle$ ($|H\rangle \to |V\rangle, |V\rangle \to |H\rangle$); $SWi\ (i = 1,2,3)$: optical switch transmits (reflects) photons when it is set to mode T (R); $H1$ with its axis aligned at $\pi/8$ completes the following transmissions: $|H\rangle \to |+\rangle, |V\rangle \to |-\rangle$; $PBS1$ and $PBS2$ are polarizing beam splitters that transmit (reflect) photons in state $|+\rangle (|-\rangle)$; PM is a phase modulator which introduces a phase $\varphi=0$ or $\varphi=\pi$; $BS1$ is a 50:50 beam splitter.

2.2 单光子逻辑比特态测量

Bob 接收到 Alice 发送的光子后，将其输入图2所示的测量光路进行测量.此时,不同光子量子态将会触发不同的探测器.光子经 $BS2$ 后将随机地进入两个测量路径:下路径的测量单元可以确定性地区分基矢 $\{|Ht_0\rangle, |Ht_1\rangle, |Vt_0\rangle, |Vt_1\rangle\}$；而右路径的测量单元可以确定性地区分基矢 $\{|+t_+\rangle, |+t_-\rangle, |-t_+\rangle, |-t_-\rangle\}$.Alice 发送的逻辑比特 0 和 1 是加载在上述两组基矢的叠加态上的(逻辑比特 0 对应 $|+t_0\rangle$ 或 $|Ht_+\rangle$；逻辑比特 1 对应 $|-t_1\rangle$ 或 $|Vt_-\rangle$).注意，在图 2 所示的测量光路中 $PBS3$ 和 $PBS4$ 透射 $|H\rangle$ 光子，反射 $|V\rangle$ 光子，$PBS5$ 和 $PBS6$ 透射 $|+\rangle$ 光子，反射 $|-\rangle$ 光子.下面我们将详细分析这四个叠加态在这两组基矢下的测量结果.

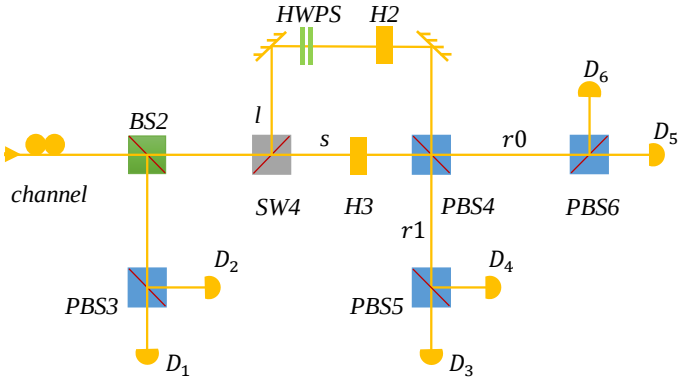

图 2 量子逻辑比特解码示意图. $BS2$:50:50 分束器; $SW4$:开关，透射 t_1 模式的光子，反射 t_0 模式的光子; $PBS3$、$PBS4$、$PBS5$、$PBS6$:极化分束器($PBS3$、$PBS4$ 透射 $|H\rangle$ 光子，反射 $|V\rangle$ 光子，$PBS5$、$PBS6$ 透射 $|+\rangle$ 光子，反射 $|-\rangle$ 光子); $HWPS$:半波片，将对光子进行如下操作: $|H\rangle\rightarrow|V\rangle$，$|V\rangle\rightarrow-|H\rangle$，$|+\rangle\rightarrow|-\rangle$，$|-\rangle\rightarrow-|+\rangle$; $H2$、$H3$:光轴角度为 $\pi/8$ 的半波片，对经过的光子进行以下操作: $|H\rangle\rightarrow|+\rangle$、$|V\rangle\rightarrow|-\rangle$; $D_i(i=1,...,6)$:单光子探测器.

Fig.2 Schematics of quantum logic qubit measurement. $BS2$: 50:50 beam splitter; $SW4$: switch transmits photons in t_1 mode and reflects photons in t_0 mode; $PBS3, PBS4, PBS5$ and $PBS6$: polarizing beam splitters. $PBS3$ and $PBS4$ transmit (reflect) photons in state $|H\rangle$ ($|V\rangle$). $PBS5$ and $PBS6$ transmit (reflect) photons in state $|+\rangle$ ($|-\rangle$). $HWPS$: half wave plate transforms the polarization of a photon passing it as follows: $|H\rangle\rightarrow|V\rangle, |V\rangle\rightarrow-|H\rangle, |+\rangle\rightarrow|-\rangle, |-\rangle\rightarrow-|+\rangle$. $H2$ and $H3$ with their axes aligned at $\pi/8$ complete the following transmissions: $|H\rangle\rightarrow|+\rangle, |V\rangle\rightarrow|-\rangle$. D_i $(i=1,...,6)$: single-photon detectors.

(1)当 Bob 接收到的光子量子态为 $|Ht_+\rangle$ 时，光子经过 $BS2$ 分束后，将随机从一个端口输出.当光子经过 $BS2$ 分束器的下路径输出时，将直接透过 $PBS3$ 从而触发探测器 D_1，使其在 t_0 或 t_1 时刻响应;而当光子经过 $BS2$ 分束器的右路径输出时，光子的 t_1 模式透射 $SW4$，而光子的 t_0 模式被 $SW4$ 反射，则 $|Ht_+\rangle$ 态的光子将会转换为 $\left(|Ht_0\rangle_l+|Ht_1\rangle_s\right)/\sqrt{2}$，这里下标 l 和 s 分别表示 $SW4$ 和 $PBS4$ 之间的长路径和短路径.经长路径 l 传输的光子，将被引入一个延迟 t_1，并透过 $HWPS$ 和 $H2$ 变为 $|-t_1\rangle$ 态，而经短路

径 s 传输的光子，将透过 $H3$ 转换为 $|+t_1\rangle$ 并与长路径模式的光子同时到达极化分束器 $PBS4$.由于 $PBS4$ 透射 $|H\rangle$ 反射 $|V\rangle$，长路径的 $|-t_1\rangle_l$ 态和短路径的 $|+t_1\rangle_s$ 经过 $PBS4$ 后将变成 $\left(|-t_1\rangle_{r0}+|+t_1\rangle_{r1}\right)/\sqrt{2}$，这里的下标 $r0$ 和 $r1$ 分别表示光子在图中传输时的不同路径. 随后，状态为 $|-t_1\rangle_{r0}$ 的光子将经过 $PBS6$ 反射后触发 D_6 探测器在 t_1 时刻响应，而状态为 $|+t_1\rangle_{r1}$ 的光子将经过 $PBS5$ 透射，最终触发 D_3 探测器在 t_1 时刻响应.

(2)当 Bob 接收到的光子量子态为 $|Vt_-\rangle$ 时，光子经过 $BS2$ 分束后，将随机从一个端口输出.当光子经过 BS 分束器下路径输出时，其直接透过 $PBS3$ 触发探测器 D_2，使其在 t_0 或 t_1 时刻响应;而当光子经过 $BS2$ 分束器的右路径输出时，光子的 t_1 模式透射 $SW4$，而光子的 t_0 模式被 $SW4$ 反射，则 $|Vt_-\rangle$ 态的光子将会转换为 $\left(|Vt_0\rangle_l-|Vt_1\rangle_s\right)/\sqrt{2}$.$|Vt_0\rangle$ 将从长路径 l 途经 $HWPS$ 和 $H2$ 变为 $-|+t_1\rangle$ 态到达 $PBS4$;而 $-|Vt_1\rangle$ 将从短路径 s 经 $H3$ 变为 $-|-t_1\rangle$ 到达 $PBS4$.长路径的 $-|+t_1\rangle_l$ 态和短路径的 $-|-t_1\rangle_s$ 经过 $PBS4$ 合束后将变成 $-\left(|+t_1\rangle_{r0}+|-t_1\rangle_{r1}\right)/\sqrt{2}$.随后，处于 $-|+t_1\rangle_{r0}$ 态的光子将透过 $PBS6$ 后触发 D_5 探测器，使其在 t_1 时刻响应，而处于 $-|-t_1\rangle_{r1}$ 态的光子将被 $PBS5$ 反射，最终触发 D_4 探测器在 t_1 时刻响应.

(3)当 Bob 接收到的光子量子态为 $|+t_0\rangle$ 时，光子经过 $BS2$ 分束后，将随机从一个端口输出.当光子经过 $BS2$ 分束器的下路径输出时，将直接透过 $PBS3$ 触发探测器 D_1 或探测器 D_2，使其在 t_0 时刻响应;而当光子经过 $BS2$ 分束器的右路径输出时，则被 $SW4$ 输入到长路径 l，并经过 $HWPS$ 和 $H2$ 变为 $|Vt_1\rangle$，经 $PBS4$ 反射进入 $r0$ 路径，并由 $PBS6$ 分束触发探测器 D_5 或 D_6 在 t_1 时刻响应.

(4)当 Bob 接收到的光子量子态为 $|-t_1\rangle$ 时，光子经过 $BS2$ 分束后，将随机从一个端口输出.当光子经过 BS 分束器的下路径输出时，将直接透过 $PBS3$ 触发探测器 D_1 或探测器 D_2，使其在 t_1 时刻响应;而当光子经过 $BS2$ 分束器的右路径输出时，将透过 $SW4$，由短路径 s 上的 $H3$ 变为 $|Vt_1\rangle$，并在 $PBS4$ 处产生反射进入 $r1$ 路径，并由 $PBS5$ 分束后触发探测器 D_3 或 D_4 在 t_1 时刻响应.

上述四种光子态 $|Ht_+\rangle$，$|Vt_-\rangle$，$|+t_0\rangle$，$|-t_1\rangle$ 经过测量光路后所触发的单光子探测器的响应情况可

以整理为表格，如表 1 所示.不难发现，当 Bob 的测量结果是$D_1(t_0)$或$D_6(t_1)$时，Bob 可以确定性的获知 Alice 发送的单光子态处于量子态$|Ht_+\rangle$或$|+t_0\rangle$，即 Alice 发送的逻辑比特是 0;当 Bob 的测量结果是$D_2(t_1)$或$D_4(t_1)$时，Bob 可以确定性的获知 Alice 发送的单光子量子态是$|Vt_-\rangle$或$|-t_1\rangle$，即 Alice 发送的逻辑比特是 1.对于探测器的其他相应情况，Bob 将无法直接获知 Alice 的逻辑比特，该部分逻辑信息可以在获知 Alice 制备基矢的情况下获知，该过程可以由一个经典信道完成.

表 1 四种单光子态对应的探测器响应情况

Table1. Clicks of detectors for four different single-photon states.

量子态	下路径	右路径
$\|Ht_+\rangle$	$D_1(t_0)/D_1(t_1)$	$D_3(t_1)/D_6(t_1)$
$\|Vt_-\rangle$	$D_2(t_0)/D_2(t_1)$	$D_4(t_1)/D_5(t_1)$
$\|+t_0\rangle$	$D_1(t_0)/D_2(t_0)$	$D_5(t_1)/D_6(t_1)$
$\|-t_0\rangle$	$D_1(t_1)/D_2(t_1)$	$D_3(t_1)/D_4(t_1)$

2.3 安全检测

在 Bob 接收完一个序列的光子后，Bob 按顺序记录下对应探测器响应情况和响应时间，不同量子态的响应结果对应表1.随后，Bob 随机选取一部分测量结果，并通过经典信道发送给 Alice.她通过 Bob 所给的信息计算误码率，从而判断是否有窃听者 Eve 存在.在第三部分，我们针对通信过程进行了安全性分析.当 Eve 存在时，她对 Alice 发送的所有光子在两组基矢下随机测量，并重新制备与测量结果相同的光子态发送给 Bob，其引起的平均误码率为 0.25.当误码率低于这一值时，Alice 和 Bob 认为信道是安全的，Alice 再将编码时的基矢信息发送给 Bob，Bob 即可知道所有的逻辑编码比特信息.否则，他们将从头开始，重复单光子逻辑态的制备、分发和测量过程.

2.4 信息收发

去除上一步骤中用于安全检测的光子，Alice 和 Bob 可以从余下的光子中生成共享的密钥.此时，

所有的光子都可以用于生成密钥，无需进行基矢比对，这表明我们的方案是确定性通信的.利用这样一组密钥, Alice 对需要发送的明文进行加密，随后将加密后的密文采用与上文相同的编码方式加载在一个单光子序列上并随机插入一组编码逻辑比特 0 和 1 的检测单光子.将修改后的光子序列发送给 Bob.

在确定 Bob 完成单光子测量过程以后, Alice 公布随机插入的检测单光子的位置和基矢信息, Bob 利用表 1 检测密文传输过程的可靠性，即检测有无窃听者存在.此时分为两种情况:(1)若窃听者存在，则 Alice 不公布单光子态的制备基矢,窃听者只能获取部分密文信息，在没有密钥信息的情况下，窃听者是无法窃取 Alice 发送的私密信息的;(2)若窃听者不存在，则 Alice 公布单光子态的制备基矢, Bob 可以利用与上文相同的方式确定性地获取 Alice 发送的私密信息，完成通信过程.

3 安全性分析

在上述单光子 DSQC 方案中，单光子量子态$|Ht_+\rangle$和$|+t_0\rangle$编码逻辑比特 0;单光子量子态$|Vt_-\rangle$和$|-t_1\rangle$编码逻辑比特 1. 量子态$|Ht_+\rangle$和$|Vt_-\rangle$是正交归一化的且可以视为算符$\hat{\sigma}_z^p \otimes \hat{\sigma}_x^t = \left(|H\rangle\langle H| - |V\rangle\langle V|\right) \otimes \left(|t_+\rangle\langle t_+| - |t_-\rangle\langle t_-|\right)$的两个本征态；$|+t_0\rangle$和$|-t_1\rangle$同样是正交归一化的,是算符$\hat{\sigma}_x^p \otimes \hat{\sigma}_z^t = \left(|+\rangle\langle +| - |-\rangle\langle -|\right) \otimes \left(|t_0\rangle\langle t_0| - |t_1\rangle\langle t_1|\right)$的两个本征态. 每个单光子的极化和 time-bin 自由度上的量子态始终在不同基矢下制备.为此,窃听者在未获知单光子态制备基矢的情况下,对光子的测量(包括破坏性测量和非破坏性测量)均会干扰单光子的状态,从而影响接收方的单光子测量结果[6].由于和 BB84 使用的单光子态类似,单光子 DSQC 的安全性可以归约到原始 BB84 方案的安全性. 为了获取经典比特信息，窃听者可以采用个体攻击(individual attack)和集体攻击(collective attack)等方式来获取单光子的量子态. 从理论上来说,这些攻击方式都会影响光子的量子态,进而影响接收方的测量结果[6].其中，测量重发的个体攻击分析过程较为简单,我们下面以测量重发的个体攻击为例来分析单光子

DSQC 的安全性.

当 Eve 采用测量重发的方式窃听双方之间的信息时， Eve 在拦截单光子后可以遵循的一个典型策略是在相同的基矢上像 Bob 的操作那样测量这些光子，并依据表 1 与测量结果制备相应的单光子态将它们发送给 Bob，这就是所谓的测量重发攻击.下面，我们详细分析 Alice 发送四种光子态时 Eve 测量重发过程产生的影响.

当 Alice 发送量子态为$\left|Ht_{+}\right\rangle$的光子，到达 Bob 端后，相应探测器的响应及其概率如表 2 所示.

表 2 Bob 探测器响应的可能情况

Table 2. Click probability of Bob's detectors

响应	$D_1(t_0)$	$D_1(t_1)$	$D_3(t_1)$	$D_6(t_1)$
概率	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$

若有窃听者 Eve 存在，在拦截测量光子后，她会根据探测器的响应情况制备一个光子重新发送至信道中.根据探测器的响应情况, Eve 可能制备的光子态的情况如表 3 所示.

表 3 Eve 制备的光子态及概率

Table3. State and probability of photons prepared by Eve

光子态	$\left\|Ht_{+}\right\rangle$	$\left\|+t_0\right\rangle$	$\left\|-t_1\right\rangle$
概率	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$

Eve 将自己制备的光子发送给 Bob, Bob 使用相同的测量装置进行测量.最终 Bob 的探测器可能的响应情况如表 4 所示.

表 4 Eve 制备的光子引起的探测器响应的可能情况

Table4. Click and probability of detectors triggered by Eve's photon

探测器响应	$D_1(t_0)$	$D_1(t_1)$	$D_3(t_1)$	$D_6(t_1)$	$D_2(t_0)$	$D_2(t_1)$	$D_4(t_1)$	$D_5(t_1)$
概率	$\frac{3}{16}$	$\frac{3}{16}$	$\frac{3}{16}$	$\frac{3}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$

对比表 2 和表 4，我们可知，此时 Eve 被发现概率为 0.25.

当 Alice 发送量子态为$|Vt_-\rangle$的光子, Bob 接收光子后，探测器的响应及其概率如表 5 所示.

表 5 Bob 探测器响应的可能情况

Table 5. Click probability of Bob's detectors

响应	$D_2(t_0)$	$D_2(t_1)$	$D_4(t_1)$	$D_5(t_1)$
概率	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$

若有窃听者 Eve 存在，在窃听光子后，她会根据探测器的响应情况制备一个光子重新发送至信道中. 根据探测器的响应情况, Eve 可能制备的光子态的情况如表 6 所示.

表 6 Eve 制备的光子态及概率

Table6. State and probability of photons prepared by Eve

光子态	$\|Vt_-\rangle$	$\|+t_0\rangle$	$\|-t_1\rangle$
概率	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$

Eve 将自己制备的光子发送给 Bob, Bob 使用相同的测量光路进行测量.最终 Bob 的探测器可能的响应情况如表 7 所示.

表 7 Eve 制备的光子引起的探测器响应的可能情况

Table7. Click and probability of detectors triggered by Eve's photon

探测器响应	$D_2(t_0)$	$D_2(t_1)$	$D_4(t_1)$	$D_5(t_1)$	$D_1(t_0)$	$D_1(t_1)$	$D_3(t_1)$	$D_6(t_1)$
概率	$\frac{3}{16}$	$\frac{3}{16}$	$\frac{3}{16}$	$\frac{3}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$

对比表 5 和表 7，我们可知，此时 Eve 被发现概率为 0.25.

当 Alice 发送量子态为$|+t_0\rangle$的光子, Bob 接收光子后，探测器的响应及其概率如表 8 所示.

表 8 Bob 探测器响应的可能情况

Table 8. Click probability of Bob's detectors

响应	$D_1(t_0)$	$D_2(t_0)$	$D_5(t_1)$	$D_6(t_1)$
概率	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$

若有窃听者 Eve 存在，在窃听光子后，她会根据探测器的响应情况制备一个光子重新发送至信道中. 根据探测器的响应情况, Eve 可能制备的光子态的情况如表 9 所示.

表 9 Eve 制备的光子态及概率

Table 9. State and probability of photons prepared by Eve

光子态	$\|+t_0\rangle$	$\|Ht_+\rangle$	$\|Vt_-\rangle$
概率	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$

Eve 将自己制备的光子发送给 Bob, Bob 使用相同的测量光路进行测量.最终 Bob 的探测器可能的响应情况如表 10 所示.

表 10 Eve 制备的光子引起的探测器响应的可能情况

Table 10. Click and probability of detectors triggered by Eve's photon

探测器响应	$D_1(t_0)$	$D_2(t_0)$	$D_5(t_1)$	$D_6(t_1)$	$D_1(t_1)$	$D_2(t_1)$	$D_3(t_1)$	$D_4(t_1)$
概率	$\frac{3}{16}$	$\frac{3}{16}$	$\frac{3}{16}$	$\frac{3}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$

对比表 8 和表 10，我们可知，此时 Eve 被发现概率为 0.25.

当 Alice 发送量子态为$|-t_1\rangle$的光子, Bob 接收到光子后，探测器的响应及其概率如表 11 所示.

表 11 Bob 探测器响应的可能情况

Table 11. Click probability of Bob's detectors

响应	$D_1(t_1)$	$D_2(t_1)$	$D_3(t_1)$	$D_4(t_1)$
概率	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$

若有窃听者 Eve 存在，在窃听光子后，她会根据探测器的响应情况制备一个光子重新发送至信道中. 根据探测器的响应情况, Eve 可能制备的光子态的情况如表 12 所示.

表 12 Eve 制备的光子态及概率

Table 12. State and probability of photons prepared by Eve

光子态	$\left\|-t_1\right\rangle$	$\left\|Ht_+\right\rangle$	$\left\|Vt_-\right\rangle$
概率	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$

Eve 将自己制备的光子发送给 Bob, Bob 使用相同的测量装置进行测量.最终 Bob 的探测器可能的响应情况如表 13 所示.

表 13 Eve 制备的光子引起的探测器响应的可能情况

Table 13. Click and probability of detectors triggered by Eve's photon

探测器响应	$D_1(t_1)$	$D_2(t_1)$	$D_3(t_1)$	$D_4(t_1)$	$D_1(t_0)$	$D_2(t_0)$	$D_5(t_1)$	$D_6(t_1)$
概率	$\frac{3}{16}$	$\frac{3}{16}$	$\frac{3}{16}$	$\frac{3}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$

通过对比表 11 和表 13，我们可知，此时 Eve 被发现概率为 0.25.

综上，我们可以得出，对于任意一个光子而言, Eve 测量重发后引起的误码率均为 0.25.而当 Eve 测量重发 n 个光子时，她的测量重发过程不干扰 Bob 测量结果的概率应为$1-(3/4)^n$，这一结果与先前基于单光子四个非正交态传输的方案相同[6]，其优势在于我们不存在选错基矢的情况，每一个未用于安全检测的单光子都可以生成一个密钥，这表明我们的方案具有确定性的特点.

4 可行性分析与讨论

和其他的量子通信方案相似,单光子源以及光学开关的性能等都会对方案实际的实现产生一定的影响. 目前实际应用中使用的单光子源大致可以分为三类[37, 38]: (1) 确定的单光子(deterministic single-photon source); (2) 预报式单光子源 (heralded single-photon source); (3) 激光衰减的准单光子源 (weak coherent pulse). 确定的单光子源通过单个二能级原子或类原子系统产生单个光子, 由于其产生光子的波长远离通信波段以及单光子源运行的复杂性等往往不直接用于量子通信[38]. 预报式单光子源基于自发参量下转换等非线性过程和单光子探测, 是一种概率性的单光子源被广泛用于研究高性能 QKD. 该类单光子源的预报特性,使得其可以直接用于我们的单光子 DSQC 方案中. 最近, 利用复用技术,该类单光子源的性能得到了大幅提升, 可以近似产生确定性的预报单光子[39], 这更加有利于其在量子通信中的应用. 激光衰减的准单光子源因其高效率等特点是当前 QKD 使用的主要光源,利用诱骗态技术可以探测光子数劈裂攻击,得到高效率的秘钥生成率[37]. 通过引入诱骗态,我们方案中的单光子源同样可以采用这类光源实现,进而完成对经典信息的确定性传输.

在逻辑比特编码过程中, 我们使用光轴可调的 HWP 控制单光子的极化状态来实现不同逻辑比特的切换. 在实际的逻辑比特编码过程中, 往往需要用到高性能的光学开关, 由其带来的延迟响应、插入损耗等将影响量子通信的效率. 2011 年, Hall 等实验实现了高速光学开关[40],并将其用于研究两光子之间的纠缠操控.这类光学开关的切换时间在 10 ps 量级能提供快速的量子态切换,其插入损耗可以被压缩到 0.05 dB,光子极化状态的保真度高达 99%以上.为此,我们忽略了由光学开关引入的影响.电控普克尔盒 (Pockels cell)同样可以实现对单光子极化状态有效调控,输出目标光子极化状态,进而编码逻辑比特信息.目前, 这类普克尔盒已用于 QKD 和玻色取样等量子信息领域[41, 42].

在我们的单光子 DSQC 方案中,我们使用单光子的极化和 time-bin 两自由度构成的两组共轭基矢量来编码一个经典逻辑比特. 与先前的基于双向量子信道的确定性量子密钥分发不同[20-23], 我们使用

一个单向量子信道和一个经典信道就能实现确定性的密钥分发.在考虑光子的丢失和探测器的效率时，我们的方案比先前的双光子逻辑编码 DSQC 方案具有指数倍的增加；在不考虑光子丢失和使用理想探测器的情况下，我们的方案可以直接用于传输私密信息，同时在密文传输过程中，具有与 QSDC[7-11]相同的窃听感知而不泄露私密信息的特点. 尽管我们的方案使用了两个单向量子通道，单个光子传输信息的容量只有 QSDC 的一半，但由于其不需要量子存储[26]，在当前实验条件下更加容易实现.

考虑到光子的多个自由度[43]以及 time-bin 等自由度的高维度内禀特性[44]，对单光子的多重编码已经用于大幅提升加载于单个光子上的信息容量[44, 45],增加单光子的利用率并增加信道的安全性.从理论上来说,通过对单光子的多重编码,有望实现基于单光子多自由度和高维度的 DSQC,即利用一个量子信道和一个经典信道实现单光子确定性传输多比特信息.

5 总结

本文提出了一个基于单光子的 DSQC 方案. 量子通信中的信息发送方和接收方通过对单个光子的极化和 time-bin 两自由度进行逻辑编码和测量，可以利用一个量子信道和一个经典信道实现对经典信息的确定性传输并有效地完成窃听检测. 我们方案的确定性传输特性使其在不需要量子存储的情况下便可以实现 QSDC 利用量子信道直接传输经典信息的功能. 因此，我们的单光子 DSQC 方案综合了先前方案的优势具有非常重要的应用前景.

参考文献

[1] Wehner S, Elkouss D, Hanso R 2018 *Science* **362** eaam9288

[2] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems & Signal Processing Bangalore*, India, December 10–12, 1984 p175

[3] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[4] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[5] Guo P L, Dong C, He Y, Jing F, He W T, Ren B C, Li C Y, Deng F G 2020 *Opt. Express* **28** 4611

[6] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

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

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

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

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

[11] 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

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

[13] Li T, Gao Z K, Li Z H 2020 *EPL* **131** 60001

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

[15] Hillery M, Bužek V, Berthiaume A 1999 *Phys. Rev. A* **59** 1829

[16] Karlsson A, Koashi M, Imoto N 1999 *Phys Rev. A* **59** 162

[17] Deng F G, Li X H, Li T 2018 *Acta Phys. Sin.* **67** 130301 (in Chinese) [邓富国, 李熙涵, 李涛 2018 物理学报 **67** 130301]

[18] Gao Z K, Li T, Li Z H 2020 *Sci. China-Phys. Mech. Astron.* **63** 120311

[19] Shimizu K, Imoto Y 1999 *Phys. Rev. A* **60**, 157

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

[21] Cai Q Y, Li B W 2004 *Chin. Phys. Lett.* **21** 601

[22] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901

[23] Long G L, Deng F G, Wang C, Li X H, Wen K, Wang W Y 2007 *Front. Phys. China* **2** 251

[24] Li T, Long G-L. 2020 *New J. Phys.* **22** 063017

[25] Wang M-Y, Wang X-D, Ruan D, Long G-L 2021 *Acta Phys. Sin.* **70** 190301 (in Chinese) [王明宇, 王馨德, 阮东, 龙桂鲁 2021 物理学报 **70** 190301]

[26] Dou J-P, Li H, Pang X-L, Zhang C-N, Yang T-H, Jin X-M 2019 *Acta Phys. Sin.* **68** 030307 (in Chinese) [窦建鹏, 李航, 庞晓玲, 张超妮, 杨天怀, 金贤敏 2019 物理学报, **68** 030307]

[27] Lucamarini M, Mancini S 2005 *Phys. Rev. Lett.* **94** 140501

[28] Cai Q Y, Li B W 2004 *Phys. Rev. A* **69** 054301

[29] Gao T, Yan F L, Wang Z X 2005 *J. Phys. A: Gen. Phys.* **38** 5761

[30] Elsayed T A. 2020 *Phys. Scr.* **96** 025101

[31]Jeong Y C, Ji S W, Hong C, Park H S, Jang J 2020 *Entropy* **22** 1268

[32] Jiang D, Chen Y, Gu X, Xie L, Chen L 2017 *Sci. Rep.* **7** 44934

[33] Wang J D, Wei Z J, Zhang H, Qin X J, Liu X B, Zhang Z M, Liao C J, Liu S H 2010 *J. Phys. B: At. Mol. Opt. Phys.* **43** 095504

[34] Lu H, Fung C, Ma X, Cai QY 2011 *Phys. Rev. A* **84** 042344

[35] Beaudry N J, Lucamarini M, Mancini S, Renner R 2013 *Phys. Rev. A* **88** 062302

[36] Henao C I, Serra R M 2015 *Phys. Rev. A* **92** 052317

[37] Xu F, Ma X, Zhang Q, Lo H-K, Pan J-W 2020 *Rev. Mod. Phys.* **92** 025002

[38] Meyer-Scott E, Silberhorn C, Migdall A 2020 *Rev. Sci. Instrum.* **91** 041101

[39] Kaneda F. and Kwiat P. G. 2019 *Sci. Adv.* **5** eaaw8586

[40] Hall M A, Altepeter J B, Kumar P 2011 *Phys. Rev. Lett.* **106** 053901

[41] Cao Y, Liang H, Yin J, Yong H-L, Zhou F, Wu Y-P, Ren J-G, Li Y-H, Pan G-S, Yang T, Ma X, Peng

C-Z, Pan J-W 2013 *Opt. Express* **21** 27260

[42] Wang H, Li W, Jiang X, He Y M, Li Y H, Ding X, Chen M C, Qin J, Peng C Z, Schneider C, Kamp M, Zhang W J, Li H, You L X, Wang Z, Dowling J P, Höfling S, Lu C-Y, Pan J-W 2018 *Phys. Rev. Lett.* **120** 230502

[43] Deng F-G, Ren B-C, Li X-H 2017 *Sci. Bull.* **62** 46

[44] Erhard M, Krenn M, Zeilinger A 2020 *Nat. Rev. Phys.* **2** 365

[45] Guo B-H, Yang L, Xiang C, Guan C, Wu L-A, Liu S-H. 2013 *Acta Phys. Sin.* **62** 130303(in Chinese) [郭邦红, 杨理, 向憧, 关翀, 吴令安, 刘颂豪 2013 物理学报 **62** 130303]

Deterministic secure quantum communication with double-encoded single photons‡

Wei Yuyan[1)] Gao Zikai[1)] Wang Siying[1)] Zhu Yajing[1)] Li Tao[1)2)§]

1) (Science of School, Nanjing University of Science and Technology, Nanjing 210094, China)

2) (MIIT Key Laboratory of Semiconductor Microstructure, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract

Quantum communication is an important branch of quantum technology. It can safely transmit private information between legitimate parties and its unconditional security is guaranteed by quantum physics. So far, deterministic secure quantum communication without entanglement usually transmits single photons in two-way quantum channels. We propose a deterministic secure quantum communication proposal, and it requires a one-way quantum channel and a classical channel. In our protocol, a sender encodes logical bits by using two conjugate bases of the polarization and time-bin degrees of freedom of a photon and transmits it to a receiver over a quantum channel. Upon receiving this photon, the receiver measures it randomly in two bases and can decode the bit deterministically with the help of the sender. Any attack from eavesdroppers will be detected by the legitimate parties. Furthermore, this protocol can be implemented with linear-optic elements and single-photon detectors.

‡ Project supported by the Natural Science Foundation of Jiangsu Province (Grant No. BK20180461) and the National Natural and Science Foundation of China (Grant No. 11904171).

§ Corresponding author. E-mail: tao.li@njust.edu.cn

Keywords: quantum communication, deterministic, single photon, two degrees of freedom