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

量子直接通信

李熙涵

Quantum secure direct communication

Li Xi-Han

引用信息 Citation: Acta Physica Sinica, 64, 160307 (2015) DOI: 10.7498/aps.64.160307
在线阅读 View online: http://dx.doi.org/10.7498/aps.64.160307
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2015/V64/I16

专题: 量子精密计量与操控

量子直接通信*

李熙涵†

(重庆大学物理学院, 重庆 401331)

(Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo N2L3C5, Canada)

(2015 年 5 月 12 日收到; 2015 年 6 月 9 日收到修改稿)

量子直接通信是量子通信中的一个重要分支, 它是一种不需要事先建立密钥而直接传输机密信息的新型通信模式. 本综述将介绍量子直接通信的基本原理, 回顾量子直接通信的发展历程, 从最早的高效量子直接通信协议、两步量子直接通信模型、量子一次一密直接通信模型等, 到抗噪声的量子直接通信模型以及基于单光子多自由度量子态及超纠缠态的量子直接通信模型, 最后介绍量子直接通信的研究现状并展望其发展未来.

关键词: 量子通信, 量子直接通信, 量子直接通信网络

PACS: 03.67.Hk, 03.65.Ud, 03.67.Dd **DOI:** 10.7498/aps.64.160307

1 引 言

量子通信是近三十年发展起来的新兴学科, 它以量子态为信息载体, 利用量子力学的基本原理进行信息编码与传输. 与经典通信安全性依赖于计算复杂度的特点不同, 量子通信的安全性建立在物理原理上, 被证明是绝对安全的保密通信方法. 第一个量子通信方案是1984年Bennett和Brassard提出的量子密钥分配方案[1], 简称为BB84协议. 随后的三十年, 量子通信在理论和实验上都有了长足发展. 我们可以根据量子通信的任务性质来将量子通信划分为几个模式或者方向, 如量子密钥分配[1−24]、量子秘密共享[25−28]、量子直接通信[29−47]、量子隐形传态[48−50]、量子密集编码[51,52]等. 每一个模式又包含了若干个不同的代表性协议, BB84协议是量子密钥分配的一个代表性协议. 而量子密钥分配、量子直接通信、量子秘密共享等以信息安全为主要目的, 又称为量子密码学. 除了点对点的量子通信外, 人们还讨论了利用服务器来完成制备和测量等操作的量子通信网络方案[53−56]. 实验上, 量子通信的距离不断刷新记录, 2013年纠缠分发距离达到300 km[57], 2014年远程量子密钥分配的安全距离已扩展至200 km[58].

所谓通信, 指的是双方或多方之间交换有意义的信息. 机密通信的首要任务是保障信息安全. 经典一次性便签 (one-time pad) 加密体系是惟一被证明安全的经典通信模式. 它要求密码是完全随机的0, 1组合, 密码的长度与明文一致, 且密码只能使用一次. 这种加密通信的安全性完全建立在密码的安全性上, 因此在通信之前双方需要共享大量的安全密钥用于后续的加密通信, 而这在经典物理的环境下是很难做到的. 密钥一旦被截获复制, 则机密信息暴露无遗. 量子密钥分配 (quantum key distribution, QKD) 就是为了解决远距离通信各方共享安全密钥的问题而提出的, 密钥的安全性由量子力学的基本原理保证. 这里的安全不是指密钥分配过程不会被截获或者窃听, 而是指一旦窃听者采取行动扰动密钥分配就会被合法的通信者发现. 这时通信者们抛弃已经传输的数据, 在检查信道安全之后重新开始密钥分发过程, 直到确保安全为止.

* 国家自然科学基金 (批准号: 11004258) 和中央高校基本科研业务费 (批准号: CQDXWL-2012-014) 资助的课题.

† 通信作者. E-mail: xihanlicqu@gmail.com

随后他们用安全的密钥利用一次性便签加密的方式进行机密通信. 严格意义上来讲, 量子密钥分配只是用于建立安全密钥的方法, 并不能用于传递机密信息. 不过由于其最终目的是服务于通信, 量子密钥分配被归类为量子通信的一个重要分支, 代表基于量子密钥分配和经典一次性便签加密相结合的安全通信模式.

安全的直接通信无论在理论上还是实际应用上都是非常重要的. 研究基于量子系统的直接通信首先是科学探索的需要, 这可以帮助人们认识量子通信的能力极限; 第二, 直接通信是一些密码任务的需求, 例如在投票、竞标等方面, 需要传输确定的信息, 在量子通信中完成这些任务需要使用量子直接通信; 第三, 在某些紧急情况下, 如电网攻击中, 不仅需要安全而且时间迫切, 直接通信十分适合于这一类通信的需求[59]. 随着量子技术的发展和普及, 直接通信的需求会越来越多, 它的应用也会越来越广泛. 既然量子力学原理为我们提供了安全保障, 我们能否利用量子信道直接传递机密信息呢? 答案是肯定的, 但这也需要更高级别的安全保障. 量子密钥分配具有"赞歌" 能力, 即在线探测窃听者 (on-site-detection of eve, ODE) 能力[60]. 在量子密钥分配中利用抽样检测发现窃听, 一旦发现窃听就意味着之前传输的数据已经泄露, 即信息前泄露 (information leakage before eve detection, ILBED)[60,61]. 因此量子密钥分配只能传输随机数据, 一旦发现有窃听, 即可抛弃之前已经传输的随机数据. 而如果确认没有窃听, 则可将传输的数据留下作密钥使用. 而传输机密信息时就不能这样处理, 一旦泄露则无法挽回. 这种直接传输机密信息的通信方式称为量子安全直接通信 (quantum secure direct communication, QSDC). 由于安全性是量子通信的基本要求, 因此本文中我们将QSDC简称为量子直接通信. QSDC采用了块传输技术, 消除了信息前泄露, 即不但具有"赞歌"能力, 而且还有"油床" (obliteration of information leakage before eve detection, OILBED) 能力, 因此可以直接传输机密信息. 在这类方案中, 接收者可以通过测量量子态直接读取机密信息.

值得注意的是, 早期曾经将量子直接通信和确定的量子密钥分配 (deterministic quantum key distribution, DQKD) 相混淆. 确定的量子密钥分配有时候也被称为确定安全量子通信 (deterministic secure quantum communication), 为了避免混淆, 最近人们更多地将其称为确定的量子密钥分配. 在DQKD中, 通信双方协调地选用测量基矢, 双方确定性地传输数据. 而且利用DQKD进行通信的时候还可以进行一些变样. QKD是先通过量子信道分发密钥, 再利用密钥加密信息, 通过经典通信传输加密后的密文来达到传输秘密信息的目的. 而在DQKD中, 我们可以首先选择密钥, 利用密钥将秘密信息加密, 通过量子信道传输加密后的密文, 在确定没有窃听后再通过经典信道将密钥公布. 如果发现有窃听, 则放弃传输. 由于通信双方是在确保窃听者Eve没有截获密文的情况下才公布密钥, 因此保证了信息的安全. 表面上看, DQKD与量子直接通信一样, 都可以确定地传输事先确定的数据, 但是两者的根本却别在于是否具有"油床" 能力, 即能否消除信息前泄露. DQKD无法保证消除信息前泄露, 因此不能进行直接通信. 不能保证安全的DQKD在直接通信上与经典通信是一样无能为力的, 经典通信也能做到百分之百地传输数据, 但不能保证信息安全. 虽然DQKD不能直接通信, 但是DQKD具有"赞歌" 能力, 可以传输随机数据, 可以用来高效地进行密钥分配, 因此还是十分重要的. 我们还可以从另一个方面区别DQKD与QSDC. 在QSDC中, 信息接收方可以通过测量量子态"直接" 读取机密信息 (如发送者制备的一组正交量子态[29], 或发送者对量子系统进行的不同量子操作[30−33]); 而在DQKD中还需要额外的经典信息来读出信息, 因此是否需要额外的经典信息是区分QSDC和DQKD的另一个关键. 此外, 从技术层面上看, 是否使用块传输技术是一个判断标准, 如果没有使用块传输技术一般不是QSDC. 在本文中, 我们将回顾量子直接通信这一重要量子通信分支的发展历程, 并重点介绍其中的一些代表性方案, 希望能让读者对这一领域的发展有一个较全面的了解和认识.

2 量子直接通信

2.1 发展历程

最早的安全的QSDC方案可追溯到2000年龙桂鲁和刘晓曙[29]提出的高效量子通信方案 (arXiv:quant-ph/0012056 V1, 2000年12月13日公布). 他们针对量子通信不能直接传输机密信息的

问题, 将大数中心分布定理推广到量子体系, 发明了量子数据块传输与分步传输方法, 解决了信息前泄露难题, 为量子直接通信的发展扫除了物理原理上的障碍. 他们明确提及到传输所有用户在传输前就已生成的共同密钥 (common key), 即确定信息的直接传输, 是第一个量子直接通信协议. 由于其具有效率高的优点, 我们称之为高效 QSDC 协议. 2002 年, Beige 等 [7] 提出了一个基于单光子两自由度两比特量子态的 DQKD 方案, 但是随后作者自己认识到这一方案存在信息泄露的危险, 只能完成两自由度单光子量子态的 BB84 协议. 同年, Boström 和 Felbinger [62] 提出了一个准安全的确定通信方案, 称为 ping-pong 协议. 此方案原理上虽然是一个量子直接通信方案, 但随后多个研究组明确指出 ping-pong 协议的安全漏洞 [63,64], 不是一个真正的量子直接通信协议, 本文就不将它归为 QSDC 方案加以介绍. 2003 年, 邓富国、龙桂鲁和刘晓曙三人 [30] 提出了基于纠缠光子 Einstein-Podolsky-Rosen (EPR) 对的两步量子直接通信方案; 同年, 邓富国和龙桂鲁 [31] 提出了基于单光子量子态序列的量子一次一密直接通信方案. 在这两个方案中, 作者首次提出了 QSDC 需要满足的条件, 阐明了 QSDC 的物理机理, 给出了 QSDC 的构造原理和安全判据 [30,31], 为后续 QSDC 方案的设计提供了理论依据, 极大地推动了 QSDC 的发展. 随后, 人们根据各种不同的量子信号源, 借助数据块传输方法与两步方案给出的构造原理, 提出了多种优美的 QSDC 方案. 譬如, 王川等在 2005 年分别建立了基于高维系统超密集编码的量子直接通信方案 [32] 和基于多粒子系统的多步量子直接通信模型 [33]. 2005 年, Lucamarini 与 Mancini [65] 采用与量子一次一密 QSDC 方案 [31] 相同的物理原理, 构建了一个基于单个光子量子态的确定通信方案, 并讨论了窃听以及环境噪声对通信的影响. 由于它的物理原理与量子一次一密 QSDC 方案完全一样 (即它是后者量子数据块中光子数为 1 的情形), 但又由于没有使用量子数据块传输而失去了直接通信的安全性, 本文就不将它归为 QSDC 方案加以介绍. 它与邓富国和龙桂鲁于 2004 年提出的四态 two-way 量子密钥分配方案 [5] 一样, 只可用于产生密钥. 2007 年, 李熙涵等 [34] 提出了基于量子加密的 QSDC 方案. 2008 年, 林崧等 [35] 提出了基于 χ 型纠缠态的 QSDC 方案. 2011 年, 顾斌等 [36] 首次研究了噪声条件下的量子直接通信. 同年, 王铁军等 [37] 首次提出了基于光子对两自由度超纠缠 Bell 态的高容量 QSDC 方案. 此后, 研究者们还提出了一些基于不同量子信道的量子直接通信方案 [38−44]. 除了基于光量子态的 QSDC 外, 研究者们还提出了基于连续变量 [45] 和基于相干态的 QSDC 方案 [46].

值得一提的是, 2004 年蔡庆宇等 [66] 借鉴两步量子直接通信协议 [30] 中的安全检测方法, 改进了 ping-pong 协议, 但由于没有使用量子态块传输, 无法解决信息前泄露问题, 不能用于安全的量子直接通信, 可用于产生随机密钥. 同一年, 他们提出了一个单个光子态的类 ping-pong 协议 [67], 由于在安全检测模式时信息发送方没有做抽样测量, 而是采用自己制备单光子后随机地替代信息接收者发给她的光子, 且只使用了两个非正交量子态, 在物理原理上留下了安全漏洞, 无法完成安全的量子通信. 当然, 虽然这两个协议在物理原理上存在不足 [66,67], 但在引起了人们对量子直接通信的关注方面也做出了一定贡献.

除点对点的量子直接通信方案外, 人们也讨论了利用服务器完成制备和测量等操作的量子直接通信网络方案 [53−56]. 量子直接通信是近年来量子通信的研究热点之一, 文献 [60, 61, 68] 综述了该领域的一些主要进展. 在本文中, 我们将主要按时间顺序介绍这一领域的代表性方案.

2.2 安全性检测

在详细介绍量子直接通信的代表性方案之前, 我们先介绍量子通信的关键步骤——安全性检测的常见方法. 量子通信相较于经典通信的最大优势在于可以实现绝对安全的通信过程. 这里的“绝对安全” 并不是指没有窃听者监听信道, 而是一旦有窃听就会被发现. 方案的安全性由量子力学的非克隆定理和测不准原理保障, 通过统计抽样分析来判断, 即安全性检测. 具体来说, 安全性检测一般指合法的通信各方随机选取一定数量的量子态样本公布制备基矢、初始态和测量结果用于计算实际出错率, 随后将实际出错率与一个根据传输环境预测的出错率进行比对. 若实际出错率不在安全范围内, 则表明信道被监听. 若实际出错率在安全范围内, 则表明传输安全. 在量子密钥分配方案中, 安全性检测一般在通信结束后进行. 若发现信道被监听, 则抛弃已经建立的随机密钥; 否则, 密钥可作为

裸码 (raw key), 经机密放大等处理后用于加密信息. 然而在量子直接通信过程中, 由于传输的是机密信息而不是随机密钥, 一旦泄露无法挽回. 因此安全性检测需要在传输机密信息之前进行, 确保信道安全后才能进行通信 [29,30].

在安全性检测过程中, 一般需要选取两组或两组以上的相互无偏基矢 (unbiased bases) [69], 最常用的为 X 基矢和 Z 基矢. 对于二维系统, Z 基矢由相互正交的 $|0\rangle$ 和 $|1\rangle$ 构成. X 基矢表示为 $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. 两组基矢相互平分:

$$\begin{aligned} |\langle 0|+\rangle|^2 &= |\langle 1|+\rangle|^2 = |\langle 0|-\rangle|^2 \\ &= |\langle 1|-\rangle|^2 = \frac{1}{2}. \end{aligned} \tag{1}$$

两组基矢的这种关系保证了一旦信道被窃听会引起最大的出错率. 对于 d 维系统, Z 基矢由 d 个相互正交的基构成 $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$. X 基矢可表示为 [18]

$$\begin{aligned} |k\rangle_x = \frac{1}{\sqrt{d}}\Big(&|0\rangle + \mathrm{e}^{\frac{2\pi \mathrm{i}(d-1)}{d}}|1\rangle + \mathrm{e}^{\frac{2\times 2\pi \mathrm{i}(d-1)}{d}}|2\rangle + \cdots \\ &+ \mathrm{e}^{\frac{(d-1)\times 2\pi \mathrm{i}(d-1)}{d}}|d-1\rangle\Big). \end{aligned} \tag{2}$$

这里我们用下标的 "x" 指示 X 基矢 ($k = 0, 1, \cdots, d-1$). d 维系统的这两组基矢同样相互平分,

$$|\langle j|k\rangle_x|^2 = \frac{1}{d} \quad (j, k = 0, 1, \cdots, d-1). \tag{3}$$

若窃听者选错测量基进行截获重发窃听, 将引起 $e = (d-1)/d$ 的出错率. 由此可见, 高维系统比二维系统具有更好的安全保证 [18,32].

在量子通信中, 最常见的信息载体为单粒子态和两粒子最大纠缠态 (贝尔态). 一般来说, 基于单粒子态的量子通信方案中, 量子态都会随机地处于 X 基矢或 Z 基矢, 因此安全性检测只需选取随机位置的样本用相应的基矢测量即可. 而基于贝尔态的通信方案中, 当双方各执纠缠系统的两部分时, 通信双方对随机挑选的纠缠粒子对选取相同的基矢做单粒子测量 [30]. 由于最大纠缠态的粒子在两组基矢下都有完美的对应关系

$$\begin{aligned} |\phi^+\rangle_{\mathrm{AB}} &= \frac{1}{\sqrt{2}}(|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} + |1\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}}) \\ &= \frac{1}{\sqrt{2}}(|+\rangle_{\mathrm{A}}|+\rangle_{\mathrm{B}} + |-\rangle_{\mathrm{A}}|-\rangle_{\mathrm{B}}). \end{aligned} \tag{4}$$

通信双方可由此计算出错率从而判断传输是否安全. 除了两粒子二维纠缠态以外, 两粒子高维最大纠缠态在 X 基矢和 Z 基矢上也都有完美的对应关系 [32], 多粒子最大纠缠态各个粒子之间以及任意两个部分之间同样存在类似的在不同基矢上的对应关系 [33], 均可用于安全性检测.

此外, 还有基于非最大纠缠信道的量子通信方案 [34]. 由于处于非最大纠缠态的粒子只在一个基矢上有对应关系, 在另一个基矢上没有,

$$\begin{aligned} |\phi\rangle_{\mathrm{AB}} &= \alpha|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} + \beta|1\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}} \\ &= \frac{1}{2}[(\alpha+\beta)(|+\rangle_{\mathrm{A}}|+\rangle_{\mathrm{B}} + |-\rangle_{\mathrm{A}}|-\rangle_{\mathrm{B}}) \\ &\quad + (\alpha-\beta)(|+\rangle_{\mathrm{A}}|-\rangle_{\mathrm{B}} + |-\rangle_{\mathrm{A}}|+\rangle_{\mathrm{B}})] \\ &\quad (|\alpha|^2 + |\beta|^2 = 1). \end{aligned} \tag{5}$$

因此, 我们需要在传输的量子态序列中事先插入足够数量的用于安全性检测的诱骗光子 (decoy photon) [70,71]. 这些光子随机地选取 X 基矢或 Z 基矢制备, 并被插入粒子序列中的随机位置. 传输完成后, 发送者告知接收者诱骗光子的位置和量子态, 接收者选择相应基矢进行单粒子测量即可检测传输安全. 采取诱骗光子的安全性检测方法是一种相对普适的做法, 适用于不同的量子系统 [70,71]. 特别地, 如果携带信息的量子态是高维系统, 我们仍可以用二维的诱骗光子做安全性检测 [18,70,71]. 目前, 诱骗光子技术 [70,71] 已经成为量子通信中一种众所周知的实用安全检测方式.

除了传统的纠缠量子态外, 量子通信中还可能用到在两个或两个以上自由度上同时纠缠的超纠缠态 (hyperentangled state). 若使用最大超纠缠态作为量子信道, 安全性检测时需要对各个自由度上的量子态选取两组相互平分的基矢进行测量 [37]. 我们同样可以选择插入诱骗光子的方法进行安全性检测, 不过, 此时诱骗光子需包含各个自由度的信息: 一方面可以制备单光子多自由度的量子态; 另一方面可以随机选择自由度制备诱骗光子, 每个诱骗光子用于检测特定自由度的安全.

我们这里介绍的安全性检测方法不仅适用于量子直接通信方案, 而且在量子通信的其他分支中同样有用 [69]. 虽然每一个方案中具体的安全性检测过程的操作可能不同, 但都需要从大量的量子态中随机选取一定量的样本测量, 用统计分析的方法来判断信道是否安全. 这就要求量子态的传输是块状进行的, 每一次传输有足够多的样本用于挑选和检测. 这也正是量子直接通信对传输方式的要求之一 [30,31].

3 代表性方案

3.1 高效QSDC方案

2000年, 龙桂鲁和刘晓曙[29]提出了一个基于EPR对的高效量子直接通信方案. 一个EPR对可以是四个贝尔态 (Bell state) 之一,

$$|\phi^{\pm}\rangle_{\rm AB}=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle)_{\rm AB},$$
$$|\psi^{\pm}\rangle_{\rm AB}=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle)_{\rm AB}. \quad (6)$$

通信双方Alice和Bob事先约定这四个态分别编码为00, 01, 10, 11. 发送者Alice首先制备N个EPR对组成的序列: $[(P_{\rm A_1},P_{\rm B_1}),(P_{\rm A_2},P_{\rm B_2}),\cdots,(P_{\rm A_i},P_{\rm B_i}),\cdots,(P_{\rm A_N},P_{\rm B_N})]$, 每一个EPR对根据不同的确定信息编码为四个贝尔态之一. 这里的下标A, B代表处于同一个贝尔态的两个粒子, 数字代表不同的纠缠粒子对. Alice将每个EPR对中的B粒子取出构成粒子序列$S_{\rm B}$ $([P_{\rm B_1},P_{\rm B_2},P_{\rm B_3},\cdots,P_{\rm B_N}])$, 并将其传输给远距离的接收方Bob, 她自己手中保留粒子序列$S_{\rm A}$ $([P_{\rm A_1},P_{\rm A_2},P_{\rm A_3},\cdots,P_{\rm A_N}])$. Bob接收到粒子序列$S_{\rm B}$后, 从中随机选取足够数量的样本进行测量并告诉Alice粒子的位置、测量基矢及结果. Alice随后对相应的粒子采用相同的基矢进行测量并记录结果. 随后Alice和Bob通过经典信道比对测量结果从而判断信道是否被窃听, 即进行本方案的第一次安全性检测. 当通信双方确认信道安全时, Alice将手中余下的粒子序列$S_{\rm A}$发送给Bob. Bob收到后对对应的粒子对进行贝尔态分析并记录测量结果. Alice和Bob选择足够多的样本进行第二次安全性检测, 若出错率低于某一确定的阈值, Bob将剩下的测量结果作为裸码保存下来. 随后经过机密放大等一系列处理, 通信双方可建立一组用于机密通信的安全密钥.

在高效QSDC方案中[29], 除用于检测的样本外, 每一个EPR对可携带两比特的信息, 信道容量高, 是其他利用EPR对的量子密钥分配方案的两倍 (如Ekert91协议[2]和BBM92协议[3]). 除检测外, 每一个粒子都可以用于传输信息, 通信效率比BB84协议高一倍. 此外, 方案中载有信息的纠缠粒子对是分两步传输的, 窃听者每次只能窃取纠缠粒子对的一部分, 得不到纠缠体系的全部信息, 从而保障了共同密钥的安全. 此方案虽然是为共同密钥分发设计的, 但其发明的块状传输与分步传输的特点正好满足了量子直接通信的必要条件[30,31], 且明确提到传输所有用户在传输前就已生成的共同密码 (a common key), 即确定信息的直接传输, 是第一个QSDC方案. 它解决了信息前泄露难题, 为量子直接通信的发展扫除了物理原理上的障碍.

3.2 两步QSDC方案

2003年, 邓富国等[30]基于量子密集编码 (quantum dense coding) 提出了一个安全的量子直接通信方案, 由于方案由两个主要的步骤构成, 一般称为"两步方案" (two-step QSDC protocol), 其原理如图1所示. 该方案同样基于EPR纠缠粒子对, 理论上每一个光子可以携带一个比特的信息, 具有高的信道容量. 方案中即使窃听者截获量子态也不能获取任何有用的信息.

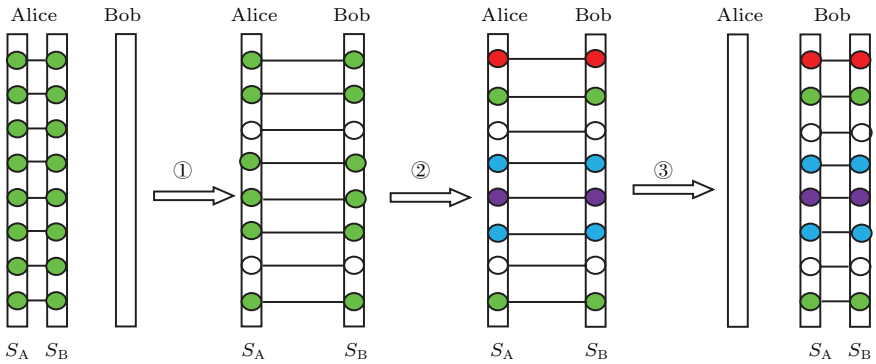

图1 两步QSDC方案原理图

Fig. 1. Schematic demonstration of the two-step QSDC protocol.

在两步方案中, 信息发送者Alice制备N个相同的EPR对$|\phi^+\rangle_{\rm AB}$. Alice将每一个纠缠对中的A粒子挑出, 构成信息序列$S_{\rm A}$, 用于编码信息; 剩下的粒子构成检测序列$S_{\rm B}$. Alice首先将检测序列$S_{\rm B}$发送给Bob, 两人检测传输的安全性. 若出错率高于某一阈值, 则表明$S_{\rm B}$序列的传输是不安全的, Alice和Bob放弃已有的传输结果. 由于$S_{\rm B}$序列并未编码信息, 因此即便$S_{\rm B}$序列的传输不安全也不会泄露机密信息. 如果Alice确认信道安全, 她将根据自己要传输的机密信息"00", "01", "10"和"11"对应地对$S_{\rm A}$序列进行四个单粒子幺正操作U_i $(i=0,1,2,3)$中的一个.

$$\begin{aligned} U_0 &= I = |0\rangle\langle 0| + |1\rangle\langle 1|, \\ U_1 &= \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \\ U_2 &= \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, \\ U_3 &= -{\rm i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|. \end{aligned} \tag{7}$$

在编码过程中, Alice随机选取一些位置的粒子加载用于下一次安全检测的随机编码, 这相当于在携带信息的量子态序列中插入用于安全性检测的诱骗光子. Alice完成信息序列的编码后将该序列发送给Bob. Bob对对应的纠缠对进行联合贝尔基测量读取Alice加载的机密信息. Bob通过比对Alice的随机编码分析出错率, 判断第二次传输的安全性以确定是否需要进行纠错等后续处理.

在两步方案中, 安全性检测的过程需要对粒子序列进行存储, 这对实验技术的要求较高. 正如两步方案描述那样, 在实际应用过程中可以采取光学延迟的办法来替代存储, 降低实验成本. 在两步方案中, 信道是否被窃听由两次安全性检测判断, 每一次传输需要一次安全性检测. 机密信息的安全由分步传输来保障, 检测序列的安全传输保证了机密信息传输的安全, 窃听者不能同时拥有携带信息的两个部分, 因而即使窃听也不能获得任何有意义的信息. 两步方案还明确指出了量子数据块传输的好处: 可以检查检测序列的安全, 一旦它安全了, 机密信息就不可能泄露给窃听者. 在有噪声的环境下, 两步方案可以利用纠缠纯化与冗余编码的方式完成机密信息的直接传输, 因此从理论上讲, 这是一个完美的QSDC方案.

2008年, 林崧等[35]基于两步QSDC方案的原理提出了利用χ型纠缠态作为量子信道的QSDC方案, 虽然每一个粒子理论上也可以携带1 bit的信息, 但由于使用了四粒子纠缠系统, 增加了量子态实验制备与测量的难度, 与两步QSDC方案相比并没有优势.

3.3 量子一次一密QSDC方案

前述的两个方案都基于纠缠系统, 它们利用分步传输和块传输的方式使窃听者无法同时获得完整的纠缠态, 从而保证了机密信息的安全. 2003年, 邓富国和龙桂鲁[31]首次将非正交量子态块传输和经典一次一密这一著名加密体系的思想结合起来, 提出了一个基于单光子量子态序列的一次一密量子直接通信方案 (部分学者称之为DL04方案), 原理如图2所示. 与基于纠缠粒子对的方案相比, 单光子态在实验上更容易获得且更容易测量, 这使得方案具有更好的实用价值. 2006年, 意大利实验组对它的原理进行了实验验证[72]. 2015年, 山西大学[73]在实验上进一步验证了基于量子数据块传输的量子一次一密QSDC方案[31].

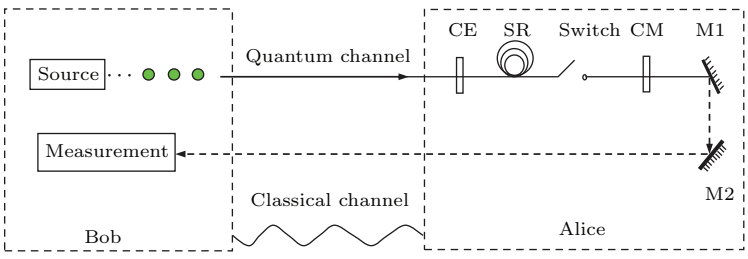

图2 量子一次一密QSDC方案原理图

Fig. 2. Schematic demonstration of the quantum one-time pad QSDC protocol.

在量子一次一密QSDC方案中[31], 信息的接收方Bob首先制备N个单光子态构成序列S. 这些量子态随机地处于四个量子态之一$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Bob将$S$序列发送给Alice之后, 通信双方随机抽取一定数量的样本进行安全性检测. 若传输安全, Alice根据自己所需传送的

机密信息“0”, “1” 分别选取U_0, U_3对量子态进行操作. U_0为恒等操作, 量子态保持不变. U_3操作只会在一组正交基矢内部翻转量子态, 即

$$U_3|0\rangle=-|1\rangle,\quad U_3|1\rangle=|0\rangle,$$
$$U_3|+\rangle=|-\rangle,\quad U_3|-\rangle=|+\rangle. \tag{8}$$

Alice在编码机密信息的过程中也随机选取一些位置的光子加载用于安全性检测的随机编码. 随后Alice将编码操作后的序列发回给Bob. 由于Alice用于编码机密信息的量子幺正操作并不会改变量子态的基矢, Bob可根据制备时的信息选择正确的基矢进行单粒子测量从而读取Alice传输的机密信息. Alice随后公布随机编码的位置和信息, Bob通过比对分析出错率以判断第二次传输是否安全.

在量子一次一密QSDC方案中, 虽然窃听者可以在第二次传输中截获携带信息的量子态, 但由于缺乏量子态初始状态的信息, 窃听者即使测量也只能得到无意义的随机结果. 这一方案同样使用了块状传输数据的方法便于安全性检测, 同时分步传输先确保信道安全后再传输携带机密信息的量子态. 量子一次一密QSDC方案还明确给出了基于单光子的QSDC的要求: 1) 信息加载传输前必须进行窃听检测; 2) 窃听检测基于抽样的概率统计, 要求进行块状的量子态传输.

量子一次一密方案给出了基于光学延迟的实验方案[31]. 在实际噪声下, 邓富国和龙桂鲁[74]还首次给出了对单光子量子态进行量子秘密放大的处理方法, 使得基于单光子量子态的量子直接通信在理论上可以做得非常完美.

2005年, Lucamarini与Mancini[31]采用量子一次一密QSDC方案的物理原理, 提出了一个基于单个光子态的确定量子通信方案[65], 并进一步讨论了环境噪声对通信的影响. 由于它没有使用量子数据块传输, 与邓富国和龙桂鲁[5]于2004年提出的四态two-way量子密钥分配方案一样, 只可用于量子密钥分配.

3.4 高维QSDC方案

在基于二维量子系统的量子通信方案中, 每一个粒子可携带$\log_2 2=1$ bit的经典信息. 2005年, 王川等[32]利用量子超密集编码 (quantum superdense coding) 的思想提出了基于高维系统的量子直接通信方案, 我们称为高维QSDC方案. 由于方案以d维系统为信息载体, 每个粒子可携带$\log_2 d$比特的经典信息. 高维两粒子贝尔态表示为

$$|\psi_{nm}\rangle_{\rm AB}=\sum_j {\rm e}^{2\pi {\rm i}jn/d}|j\rangle\otimes|j+m \bmod d\rangle/\sqrt{d}, \tag{9}$$

d为系统的维度, $n,m=0,1,\cdots,d-1$. d维系统的幺正操作可统一描述为

$$U_{nm}=\sum_j {\rm e}^{2\pi {\rm i}jn/d}|j+m \bmod d\rangle\langle j|. \tag{10}$$

此幺正操作可在这一组高维两粒子纠缠基中变换量子态

$$(U_{nm})_{\rm B}|\psi_{00}\rangle_{\rm AB}=|\psi_{nm}\rangle_{\rm AB}. \tag{11}$$

在高维QSDC方案中[32], 信息接收方Bob制备高维纠缠粒子对序列, 其中所有的纠缠对初态均为$|\psi_{00}\rangle_{\rm AB}$. Bob将每一个纠缠对中的A粒子取出构成$S_{\rm A}$序列, 对应的粒子构成$S_{\rm B}$序列. Bob将$S_{\rm A}$序列发送给信息的发送方Alice, 随后双方随机选取一定数量的样本用相同的测量基矢做单光子测量, 从而判断传输是否安全. 若传输安全, Alice根据机密信息“nm” $(n,m=0,1,2,\cdots,d-1)$选择相应的幺正操作U_{nm}对手中粒子进行编码. 编码过程中Alice随机插入用于下一次安全性检测的随机编码. 随后Alice将$S_{\rm A}$发还给Bob. Bob对对应的粒子对进行高维Bell态分析, 根据结果便能推测出Alice加载的信息. 通信双方用插入的随机编码进行第二次安全性检测以判断传输的安全性.

与基于二维量子系统的QSDC方案相比, 高维QSDC方案具有更高的安全性, 且每一个纠缠粒子对可以携带$\log_2 d^2$比特的信息, 大大地提高了信道容量.

3.5 多步QSDC方案

随着人们对量子纠缠的深入研究, 多粒子纠缠系统也被广泛应用于量子通信. 2005年, 王川等[33]提出了基于三粒子Greenberger-Horne-Zeilinger (GHZ) 态的多步量子直接通信方案. 三粒子GHZ态构成的8个正交基矢可表示为

$$|\varphi^{\pm}\rangle_0=\frac{1}{\sqrt{2}}(|000\rangle\pm|111\rangle)_{\rm ABC}, \tag{12}$$
$$|\varphi^{\pm}\rangle_1=\frac{1}{\sqrt{2}}(|001\rangle\pm|110\rangle)_{\rm ABC}, \tag{13}$$
$$|\varphi^{\pm}\rangle_2=\frac{1}{\sqrt{2}}(|010\rangle\pm|101\rangle)_{\rm ABC}, \tag{14}$$

$$|\varphi^{\pm}\rangle_3 = \frac{1}{\sqrt{2}}(|100\rangle \pm |011\rangle)_{\rm ABC}. \quad (15)$$

下标 A, B, C 对应处于 GHZ 态的三个粒子. 通过对其中两个粒子进行单粒子幺正操作可在 8 个 GHZ 态之间变换. 在量子直接通信方案中, 通信双方事先约定 8 个量子态分别对应一个三比特编码: 000, 001, ⋯, 111. 信息发送方 Alice 先制备一个 GHZ 态序列, 每一个 GHZ 态均处于 $|\varphi^+\rangle_0$. 随后 Alice 将每一个 GHZ 态的三个粒子分别纳入三个粒子序列 $S_{\rm A}$, $S_{\rm B}$ 和 $S_{\rm C}$. Alice 首先将 $S_{\rm C}$ 发送给接收方 Bob, 双方进行安全性检测以判断传输是否安全. 当他们确定 $S_{\rm C}$ 的传输安全后, Alice 根据要传输的机密信息选择合适的幺正操作作用到 $S_{\rm A}$ 和 $S_{\rm B}$ 序列上, 在此过程中 Alice 同样随机地插入用于安全性检测的随机编码. 随后 Alice 分两步将 $S_{\rm B}$ 和 $S_{\rm A}$ 序列发送给 Bob, 每一次传输完成后, 双方都进行安全性检测. 全部传输完成后, Bob 对每一组构成 GHZ 态的三个粒子进行三粒子联合测量从而读取 Alice 的机密信息. 在多步 QSDC 方案中, 由于窃听者不能同时拥有载有机密信息的三个粒子, 因此无法获得有用的信息, 保证了机密信息的安全.

2012 年, Banerjee 和 Pathak [44] 基于三粒子类 GHZ 态也提出了一个多步 QSDC 方案, 方案利用三比特的量子态可传输三比特的机密信息, 实现最大效率的通信. 该方案使用的 8 个正交量子态可表示为

$$\left\{\frac{|\phi^+\rangle|0\rangle+|\psi^+\rangle|1\rangle}{\sqrt{2}}, \frac{|\phi^+\rangle|0\rangle-|\psi^+\rangle|1\rangle}{\sqrt{2}}, \frac{|\psi^+\rangle|0\rangle+|\phi^+\rangle|1\rangle}{\sqrt{2}}, \frac{|\psi^+\rangle|0\rangle-|\phi^+\rangle|1\rangle}{\sqrt{2}}, \frac{|\phi^-\rangle|0\rangle+|\psi^-\rangle|1\rangle}{\sqrt{2}}, \frac{|\phi^-\rangle|0\rangle-|\psi^-\rangle|1\rangle}{\sqrt{2}}, \frac{|\psi^-\rangle|0\rangle+|\phi^-\rangle|1\rangle}{\sqrt{2}}, \frac{|\psi^-\rangle|0\rangle-|\phi^-\rangle|1\rangle}{\sqrt{2}}\right\}. \quad (16)$$

信息发送者可以选择相应的幺正操作作用于其中的两个粒子在 8 个态之间变换. 该方案的通信过程与基于 GHZ 态的多步 QSDC 方案 [33] 类似, 三个粒子分三步传送给接收者, 接收者通过测量可直接读取机密信息. 值得一提的是, 虽然该方案使用三粒子纠缠信道, 但是接收者可以通过对其中两个粒子进行联合贝尔基测量同时对剩下的粒子做单粒子测量来读取信息, 不需要做三个粒子的联合测量. 不过相比于王川等 [33] 的多方 QSDC 方案, 此方案需要制备更复杂的量子态作为纠缠信道.

3.6 基于量子加密的 QSDC 方案

2007 年, 李熙涵等 [34] 提出了基于量子加密的 QSDC 方案, 它利用控制非门 (controlled-NOT gate) 实现机密信息的编码和解码过程, 原理如图 3 所示. 不同于已有的那些需要最大纠缠信道的量子直接通信方案, 此方案仅需处于纯纠缠态的非最大纠缠信道作为量子密钥, 而且安全的量子信道一经建立可反复使用. 它是第一个量子通信与量子计算相结合的 QSDC 协议.

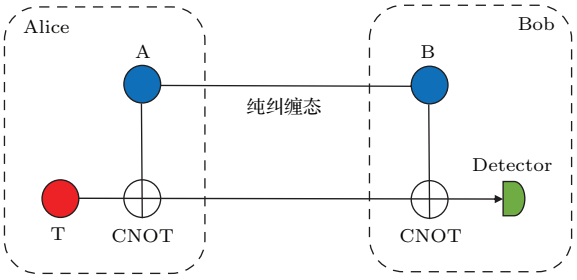

图 3 基于量子加密的 QSDC 方案原理图

Fig. 3. Principle of QSDC scheme based on quantum encryption.

通信双方 Alice 和 Bob 事先共享一组两粒子纯纠缠态, 它们随机地处于以下两个量子态之一:

$$|\phi\rangle_1 = \alpha|00\rangle_{\rm AB} + \beta|11\rangle_{\rm AB}, \quad (17)$$

$$|\phi\rangle_2 = \beta|00\rangle_{\rm AB} + \alpha|11\rangle_{\rm AB}. \quad (18)$$

这里参数 α 和 β 满足归一化条件 $|\alpha|^2 + |\beta|^2 = 1$. Alice 将每一个纠缠对中的 B 粒子挑出组成序列 $S_{\rm B}$ 发送给 Bob. Alice 手中保留每一个纠缠对中 A 粒子构成的 $S_{\rm A}$ 序列. 由于此方案采用非最大纠缠态作为量子信道, Alice 选择使用诱骗光子检测安全 [70,71]. 通信双方确认纯纠缠信道安全后, Alice 根据要传送的机密信息制备处于 $\{|0\rangle, |1\rangle\}$ 的单光子序列 $S_{\rm T}$. 在信息序列中, Alice 同样随机插入处于上述四个量子态 ($|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$) 的诱骗光子用于后续的安全性检测. 随后, Alice 用 $S_{\rm A}$ 序列对信息序列 $S_{\rm T}$ 进行量子加密: 以 $S_{\rm A}$ 为控制位, $S_{\rm T}$ 为目标位进行控制非门操作. 操作完成后, $S_{\rm T}$ 序列中的粒子与预先建立的纯纠缠信道处于纠缠态. 随后 Alice 将 $S_{\rm T}$ 序列发送给 Bob. Bob 以手中的 $S_{\rm B}$ 序列为控制位, $S_{\rm T}$ 为目标位进行控制非门操作, 从而将载有信息的粒子从纯纠缠信道中解纠缠. Bob 对信息序列用 Z 基矢进行单光子测量即可读取机密信息. 通信双方利用诱骗光子进行安全性检测,

若确定传输安全, 通信双方可重复使用已经建立的纯纠缠信道进行下一轮的机密信息传输. 由于 $S_{\rm T}$ 序列在传输过程中与纯纠缠信道处于纠缠, 其量子态为最大混合态, 因此窃听者即使截获携带信息的量子态也无法获得任何有用的信息. 此方案的最大优点在于量子信道可以重复使用, 大大地节省了量子资源. 不过实际操作过程中需要量子态存储以及两比特门操作, 这在现有的实验条件下还不易实现, 有待于实验技术条件的提高.

3.7 抗噪声的QSDC方案

早期的量子直接通信方案都基于理想环境, 偏重于物理原理上对量子通信绝对安全的设计, 即解决量子直接通信的物理原理问题, 认为量子态的传输过程是完美保真的. 2011 年, 顾斌等[36]提出了两个考虑实际信道噪声的QSDC方案. 两个方案分别针对联合退相位噪声 (collective-dephasing noise) 和联合旋转噪声 (collective-rotation noise), 用两个物理比特编码一个逻辑比特 [6], 利用逻辑比特在相应噪声下的不变性使整个通信方案免受噪声的影响.

首先, 在对抗联合退相位噪声的方案中, 由两个物理比特构成的两个逻辑比特正交基为[6]

$$|0\rangle_{\rm L}\equiv|H\rangle_{\rm A}|V\rangle_{\rm B},\ \ |1\rangle_{\rm L}\equiv|V\rangle_{\rm A}|H\rangle_{\rm B}. \tag{19}$$

这里 H 和 V 代表光子的水平和竖直偏振状态, 下标L代表逻辑比特. 这两个态在退相位噪声 ($U_{\rm dp}|H\rangle=|H\rangle$, $U_{\rm dp}|V\rangle=e^{i\phi}|V\rangle$) 的作用下保持不变, 因此以它们为基矢的任意叠加态都不会受到噪声的影响.

$$U_{\rm dp}|0\rangle_{\rm L}=|0\rangle_{\rm L},\ \ U_{\rm dp}|1\rangle_{\rm L}=|1\rangle_{\rm L}. \tag{20}$$

这里 ϕ 是信道噪声带来的相位移动, 它随作用时间的长短变化. 在量子直接通信中, 通信双方选择 $|0\rangle_{\rm L}/|1\rangle_{\rm L}$ 和 $|\pm x\rangle_{\rm L}\equiv\dfrac{1}{\sqrt{2}}(|0\rangle_{\rm L}\pm|1\rangle_{\rm L})=\dfrac{1}{\sqrt{2}}(|HV\rangle_{\rm AB}\pm|VH\rangle_{\rm AB})$ 两组基矢制备和测量量子态. 同时他们选择两个作用在逻辑比特上的幺正操作加载机密信息

$$\begin{aligned}U_0^{\rm dp}&=I_{\rm A}\otimes I_{\rm B},\\ U_1^{\rm dp}&=(-{\rm i}\sigma_y)_{\rm A}\otimes(\sigma_x)_{\rm B}.\end{aligned} \tag{21}$$

这两个操作只在基矢内部交换量子态, 并不改变量子态的基矢.

联合旋转噪声作用如下:

$$\begin{aligned}U_{\rm r}|H\rangle&=\cos\theta|H\rangle+\sin\theta|V\rangle,\\ U_{\rm r}|V\rangle&=-\sin\theta|H\rangle+\cos\theta|V\rangle.\end{aligned} \tag{22}$$

在对抗联合旋转噪声的方案中, 逻辑比特选为[6]

$$\begin{aligned}|0\rangle_{\rm L}&=\frac{1}{\sqrt{2}}(|H\rangle_{\rm A}|H\rangle_{\rm B}+|V\rangle_{\rm A}|V\rangle_{\rm B}),\\ |1\rangle_{\rm L}&=\frac{1}{\sqrt{2}}(|H\rangle_{\rm A}|V\rangle_{\rm B}-|V\rangle_{\rm A}|H\rangle_{\rm B}).\end{aligned} \tag{23}$$

两个逻辑比特以及它们的任意叠加态在联合旋转噪声中保持不变. 通信过程中, 双方仍旧选择 $|0\rangle_{\rm L}/|1\rangle_{\rm L}$ 和 $|\pm x\rangle_{\rm L}$ 两组基矢制备和测量. 用于加载机密信息的幺正操作为

$$\begin{aligned}U_0^{\rm r}&=I_{\rm A}\otimes I_{\rm B},\\ U_1^{\rm r}&=I_{\rm A}\otimes(-{\rm i}\sigma_y)_{\rm B}.\end{aligned} \tag{24}$$

两个操作同样只在基矢内部变换量子态, 并不改变基矢.

这两个对抗噪声的量子直接通信方案的具体通信过程类似于量子一次一密QSDC方案 [31], 此处不再赘述. 值得一提的是, 虽然方案利用两个物理比特编码一个逻辑比特, 但在读取信息时只需两个单粒子测量而不需要复杂的联合测量, 这使方案更具可操作性.

3.8 多自由度QSDC方案

2011年, 王铁军等[37]提出了基于两自由度超纠缠态的高容量量子直接通信方案, 是第一个基于光子多自由度的QSDC方案, 我们不妨称之为多自由度QSDC方案. 方案中使用了极化路径两自由度的两粒子超纠缠态

$$\begin{aligned}|\Phi_{\rm AB}^{+}\rangle_{\rm PS}=&\frac{1}{2}(|HH\rangle+|VV\rangle)_{\rm AB}\\ &\otimes(|a_1b_1\rangle+|a_2b_2\rangle)_{\rm AB}.\end{aligned} \tag{25}$$

这里 $a_1(b_1)$ 和 $a_2(b_2)$ 分别表示A(B)粒子两个可能的路径模式. 下标P和S分别代表极化和路径自由度. 两粒子超纠缠态共有16个正交态, 可统一表示为

$$|\xi_{\rm AB}\rangle_{\rm PS}=|\Theta\rangle_{\rm P}\otimes|\Xi\rangle_{\rm S}. \tag{26}$$

这里 $|\Theta\rangle_{\rm P}$ 可处于四个极化贝尔态之一. 而 $|\Xi\rangle_{\rm S}$ 为以下四个路径贝尔态之一:

$$|\phi^{\pm}\rangle_{\rm S}=\frac{1}{\sqrt{2}}(|a_1b_1\rangle\pm|a_2b_2\rangle)_{\rm AB},$$

$$|\psi^{\pm}\rangle_{\rm S}=\frac{1}{\sqrt{2}}(|a_1b_2\rangle\pm|a_2b_1\rangle)_{\rm AB}. \tag{27}$$

类似于极化自由度上的四个单粒子幺正操作, 路径自由度上也有四个对应的操作可以在四个路径贝尔态之间变换.

$$\begin{aligned}U_0^{\rm S}&=|a_1\rangle\langle a_1|+|a_2\rangle\langle a_2|,\\ U_1^{\rm S}&=|a_1\rangle\langle a_1|-|a_2\rangle\langle a_2|,\\ U_2^{\rm S}&=|a_2\rangle\langle a_1|+|a_1\rangle\langle a_2|,\\ U_3^{\rm S}&=|a_2\rangle\langle a_1|-|a_1\rangle\langle a_2|.\end{aligned} \tag{28}$$

理论上, 这16个正交的超纠缠态可以被完备区分. 在通信过程中, Alice和Bob首先约定16个同时作用在两自由度上的幺正操作$U_{ij}=U_i^{\rm P}\otimes U_j^{\rm S}(i,j=0,1,2,3)$代表16个不同的二进制串. Bob首先制备一个超纠缠光子对序列, 其中每个态均处于$|\Phi_{\rm AB}^{+}\rangle_{\rm PS}$. Bob将每一个A粒子挑出构成序列$S_{\rm A}$, 剩下的B粒子构成序列$S_{\rm B}$. 随后Bob将$S_{\rm A}$发送给Alice, 双方随机选取一定数量的样本进行安全性检测. 确定传输安全后, Alice根据要发送的具体信息选取相应的幺正操作U_{ij}对A粒子作用. 同样地, Alice在加载机密信息的过程中随机选取一定数量的粒子进行随机编码, 用于后续的安全性检测. 随后Alice将$S_{\rm A}$发还给Bob. Bob可以通过对相应的粒子对进行联合超纠缠态分析读取Alice加载的机密信息. 双方利用随机插入的编码比对出错率从而决定是否需要机密放大等后续操作. 在这个基于超纠缠态的量子直接通信方案中, 信息编码在幺正操作上, 相当于编码在超纠缠态上. 由于窃听者只能截获粒子对的一部分, 因此即使测量也不能得到任何有用的信息, 保障了通信的安全性. 而且由于一个光子同时携带了两自由度的信息, 每一个超纠缠粒子对可携带4 bit的量子信息, 方案的信道容量是两步方案的两倍. 值得一提的是, 虽然选择四维系统也可以用超密集编码的方式传输相同的信息量[32], 但是相对于高维系统来说, 超纠缠态在现有的技术条件下更容易操控, 此方案具有更好的实用价值. 同年, 顾斌等[38]也基于相同的超纠缠信道提出了两步实现的QSDC方案.

3.9 基于三维超纠缠态的QSDC方案

2011年, 施锦等[39]提出了两个利用两粒子两自由度超纠缠态的量子通信方案. 与前述利用极化路径超纠缠态的方案不同, 这两个方案中处于纠缠的两个自由度都是三维的,

$$\begin{aligned}|\Psi^{00}\rangle_{\rm AB}&=|\phi^{00}\rangle_{\rm AB}^{aa}\otimes|\phi^{00}\rangle_{\rm AB}^{bb}\\ &=\frac{1}{\sqrt{3}}(|00\rangle+|11\rangle+|22\rangle)_{\rm AB}^{aa}\\ &\quad\otimes\frac{1}{\sqrt{3}}(|00\rangle+|11\rangle+|22\rangle)_{\rm AB}^{bb}.\end{aligned} \tag{29}$$

这里上标"a", "b"代表两个不同的自由度, 下标"A", "B"代表处于纠缠的两个粒子. 推广的贝尔基可表示为

$$|\phi^{nm}\rangle^{k_1k_2}=\sum_j\frac{1}{\sqrt{3}}{\rm e}^{\frac{2\pi{\rm i}nj}{3}}|j\rangle^{k_1}|j+m\bmod 3\rangle^{k_2}. \tag{30}$$

类似于我们在二维系统中常用的X和Z方向基矢, 这里也定义了两组基矢

$$\begin{aligned}|X^{nm}\rangle^{k_1k_2}=\frac{1}{\sqrt{3}}\Bigg({\rm e}^{\frac{2\pi{\rm i}}{3}}|0\rangle|m\rangle+\sum_{j=1}^{2}{\rm e}^{\frac{2\pi{\rm i}nj}{3}}\\ \times|j\rangle|j+m\bmod 3\rangle\Bigg)^{k_1k_2},\end{aligned} \tag{31}$$

$$|Z^{nm}\rangle^{k_1k_2}=|nm\rangle^{k_1k_2}. \tag{32}$$

$n,m,j=0,1,2$. 如果k_1,k_2代表不同的自由度, 这两个基矢对应的是单粒子的两自由度基矢; 如果二者对应同一个自由度, 则两个基矢是两粒子在该自由度上的基矢. 对某一特定自由度的幺正操作表示为

$$U_0^{nm}=\sum_{j=0}^{2}{\rm e}^{\frac{2\pi{\rm i}jn}{3}}|j+m\bmod 3\rangle\langle j|, \tag{33}$$

$$\begin{aligned}U_1^{nm}=&{\rm e}^{\frac{2\pi{\rm i}}{3}}|m\rangle\langle 0|\\ &+\sum_{j=0}^{2}{\rm e}^{\frac{2\pi{\rm i}jn}{3}}|j+m\bmod 3\rangle\langle j|.\end{aligned} \tag{34}$$

它们的作用分别为

$$(U_0^{nm})_{\rm B}|\phi^{00}\rangle_{\rm AB}^{k_1k_1}=|\phi^{nm}\rangle_{\rm AB}^{k_1k_1}, \tag{35}$$

$$(U_1^{nm})_{\rm B}|\phi^{00}\rangle_{\rm AB}^{k_1k_1}=|X^{nm}\rangle_{\rm AB}^{k_1k_1}. \tag{36}$$

若对B粒子的a自由度施加U_0^{nm}操作, 整个纠缠系统可表示为

$$\begin{aligned}&(U_0^{nm})_{\rm B}^{a}|\Psi^{00}\rangle_{\rm AB}\\ &=|\Psi^{nm}\rangle_{\rm AB}=|\phi^{nm}\rangle_{\rm AB}^{aa}\otimes|\phi^{00}\rangle_{\rm AB}^{bb}\\ &=\frac{1}{3}\sum_{j,j'}|\phi^{j,j'}\rangle_{\rm A}^{ab}\end{aligned}$$

$$\otimes\,|\phi^{(3+n-j)\bmod 3,(3-m+j')\bmod 3}\rangle_{\mathrm{B}}^{ab}. \tag{37}$$

这里 $n,m,j,j'=0,1,2$. 在通信过程中, 信息的发送方 Bob 首先制备 N 个超纠缠对 $|\Psi^{00}\rangle_{\mathrm{AB}}$, 然后将对应的 A, B 粒子分成 S_{A} 和 S_{B} 两个序列. Bob 将 S_{A} 序列发送给 Alice, 随后双方随机地选取一定数量的样本进行安全性检测. 若判断信道安全, Bob 根据要传输的机密信息选择相应的 9 个幺正操作 U_0^{nm} $(n,m=0,1,2)$ 之一作用在 S_{B} 序列中粒子的 a 自由度上. 随后 Bob 用 $|\phi^{nm}\rangle^{ab}$ 基矢对 B 粒子做单粒子贝尔基测量并公布测量结果. Alice 对手中对应的 S_{A} 序列做相同的单粒子贝尔基分析, 根据自己的测量结果和 Bob 公布的结果, Alice 就能推测出 Bob 的机密信息. 在这个方案中, 每一个纠缠粒子对携带的信息量为 $\log_2 9$ bit. 不过根据定义, 这个方案并不是一个量子直接通信方案, 而是一个确定的量子密钥分配方案. 因为 Alice 需要得到 Bob 的测量结果才能推测出机密信息.

在第二个通信方案中, 81 个作用于单粒子两自由度的三维幺正操作被用于编码机密信息. 这些操作可表示为

$$\begin{aligned}&U^{n'm'n''m''}\\ &\equiv (U^{n'm'})\otimes(U^{n''m''})\\ &=\sum_j \mathrm{e}^{\frac{2\pi \mathrm{i} jn'}{3}}|j+m' \bmod 3\rangle^a\langle j|^a\\ &\quad\otimes\sum_{j'}\mathrm{e}^{\frac{2\pi \mathrm{i} j'n''}{3}}|j'+m'' \bmod 3\rangle^b\langle j'|^b.\end{aligned} \tag{38}$$

具体的通信过程类似于基于密集编码的量子直接通信 [30,32,37]. 在这个方案中每一个纠缠粒子对可携带 $\log_2 81$ bit 的信息. 与第一个方案相比, 第二个方案的信息量翻倍, 不过这需要两次传输粒子序列, 而且需要在两个自由度上分别做两粒子联合测量, 大大增加了实验难度. 总的来说, 这篇文章不仅利用超纠缠态, 还把每一个自由度的维度提高到了三维, 这不仅可以增加信道容量, 同时还提高了方案的安全性.

3.10 基于多自由度单光子态的 QSDC 方案

2012 年, 刘丹等 [40] 提出了基于单光子多自由度量子态的量子直接通信方案. 方案利用光子的极化和路径自由度编码信息. 极化自由度上的四个量子态分别为 $|H\rangle_{\mathrm{P}}$, $|V\rangle_{\mathrm{P}}$, $|S\rangle_{\mathrm{P}}=\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$, $|A\rangle_{\mathrm{P}}=\frac{1}{\sqrt{2}}(|H\rangle-|V\rangle)$. 而路径自由度对应的四个态为 $|b_1\rangle_{\mathrm{S}}$, $|b_2\rangle_{\mathrm{S}}$, $|s\rangle_{\mathrm{S}}=\frac{1}{\sqrt{2}}(|b_1\rangle+|b_2\rangle)$, $|a\rangle_{\mathrm{S}}=\frac{1}{\sqrt{2}}(|b_1\rangle-|b_2\rangle)$. 这里 b_1 和 b_2 代表光子的上下两条路径. 由于同时考虑光子的两个自由度, 一个光子可以处于 16 个不同的量子态 $|\varphi\rangle=|\varphi\rangle_{\mathrm{P}}\otimes|\varphi\rangle_{\mathrm{S}}$. 具体的通信过程类似于量子一次一密 QSDC 方案 [31]. Alice 可选择四个幺正操作加密两比特的机密信息.

$$U_{ij}=U_{\mathrm{P}}^i\otimes U_{\mathrm{S}}^j, \tag{39}$$

$$U_{\mathrm{P}}^i\in\{I_{\mathrm{P}},U_{\mathrm{P}}\},U_{\mathrm{S}}^j\in\{I_{\mathrm{S}},U_{\mathrm{S}}\}, \tag{40}$$

这里 I_{P} 和 I_{S} 是两个自由度上的恒等操作, U_{P} 和 U_{S} 是两个自由度上的比特和相位同时翻转的操作. 可以看出, Alice 选择的四个操作并不会改变两个自由度上量子态的基矢, 只会在同一个基矢的内部变换量子态. 因此 Bob 可以根据自己制备时的基矢信息选择正确的测量基矢直接读取机密信息. 在这个方案中, 由于同时使用光子的两个自由度, 每个光子可携带两比特的机密信息, 相较于量子一次一密 QSDC 方案 [31] 信道容量翻倍. 而且此方案不需要制备和测量纠缠态, 大大降低了实验难度.

3.11 基于两光子四比特团簇态的 QSDC 方案

从前述的一些方案中我们看到, 使用光子的多个自由度加载信息可以提高信道容量. 不过前面的方案中光子不同自由度之间处于直积关系. 2012 年, Sun 等 [41] 提出了基于两光子四比特图簇态的量子直接通信方案, 方案中光子的极化和路径自由度处于纠缠的团簇态

$$\begin{aligned}|C_4\rangle=\frac{1}{2}(&|HL\rangle_{\mathrm{A}}|HL\rangle_{\mathrm{B}}+|VL\rangle_{\mathrm{A}}|VL\rangle_{\mathrm{B}}\\ &+|HR\rangle_{\mathrm{A}}|HR\rangle_{\mathrm{B}}-|VR\rangle_{\mathrm{A}}|VR\rangle_{\mathrm{B}}),\end{aligned} \tag{41}$$

这里 L 和 R 代表光子的左侧和右侧的路径. 若将 A 粒子的极化和路径自由度编码为 2, 3 bit, B 粒子的极化和路径自由度编码为 1, 4 bit:

$$\begin{aligned}&|H\rangle\leftrightarrow|0\rangle,\quad |V\rangle\leftrightarrow|1\rangle,\\ &|L\rangle\leftrightarrow|0\rangle,\quad |R\rangle\leftrightarrow|1\rangle.\end{aligned} \tag{42}$$

量子态可改写为

$$|C_4\rangle = \frac{1}{2}(|00\rangle_{23}|00\rangle_{14} + |10\rangle_{23}|10\rangle_{14} + |01\rangle_{23}|01\rangle_{14} - |11\rangle_{23}|11\rangle_{14}). \quad (43)$$

通过对 A 粒子两个自由度的幺正变换, 可以得到一组正交基矢

$$|C^{ij}\rangle_{2314} = U_2^i U_3^j \otimes I_{14}|C_4\rangle_{2314}. \quad (44)$$

这里 $i,j = 0,1,2,3$ 对应四个单比特幺正操作. 此外, 四比特团簇态还可表示为

$$\begin{aligned}|C_4\rangle &= \frac{1}{2}(|0+0+\rangle + |0-0-\rangle + |1-1+\rangle \\ &\quad + |1+1-\rangle)_{2314} \\ &= \frac{1}{2}(|+0+0\rangle + |-0-0\rangle + |+1-1\rangle \\ &\quad + |-1+1\rangle)_{2314}. \end{aligned} \quad (45)$$

各比特在不同测量基矢下的对应关系可用于安全性检测. 通信双方事先约定四个单比特幺正操作代表两比特的信息. 首先 Alice 制备 N 个两光子四比特团簇态, 并把 A, B 两个对应的粒子分别挑出构成 $S_{\rm A}$ 和 $S_{\rm B}$ 序列. Alice 将 $S_{\rm B}$ 序列发送给 Bob. 通信双方先随机选取一些样本做安全性检测, 确认安全后 Alice 根据机密信息选取相应的幺正操作加载在 $S_{\rm A}$ 序列上, 并将携带信息的 $S_{\rm A}$ 序列发送给 Bob. Bob 对两粒子态进行联合测量即可读取 Alice 的机密信息. 此方案中单个光子同样可携带两比特的信息, 不过需要制备四比特纠缠态并完成两粒子联合测量, 在现有的实验条件下尚存在困难.

3.12 基于路径纠缠态的两步 QSDC 方案

2013 年, 任宝藏等 [42] 提出了完备区分路径贝尔态的方案, 并在此基础上提出了基于路径纠缠态的两步 QSDC 方案. 方案以路径贝尔态为量子信道

$$|\phi^+\rangle_{\rm S} = \frac{1}{\sqrt{2}}(|a_1 b_2\rangle + |a_2 b_2\rangle)_{\rm AB}. \quad (46)$$

通信双方用单光子路径态的四个幺正操作 ((28) 式) 编码两比特信息, 通信的具体过程与两步 QSDC 模型类似 [30]. 这里 Bob 通过对路径纠缠进行完备区分可完全读取这两比特的信息. 此方案利用比极化自由度鲁棒性更好的路径自由度作为信息载体, 提高了方案整体的鲁棒性.

同年, 顾斌等 [43] 也提出了基于单光子路径自由度的量子直接通信方案. 方案仅选用光子具有鲁棒性的路径自由度加载信息, 不需联合测量, 降低了实验难度.

3.13 基于相干态的 QSDC 方案

2013 年, Meslouhi 和 Hassouni [46] 提出了基于相干态 (coherent state) 的 QSDC 方案. 该方案的基本原理与基于分离变量的两步 QSDC 方案 [30] 一致, 但量子信道由纠缠相干态构成

$$\begin{aligned}|\phi_{\rm c}^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|\alpha,\alpha\rangle \pm |-\alpha,-\alpha\rangle), \\ |\psi_{\rm c}^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|\alpha,-\alpha\rangle \pm |-\alpha,\alpha\rangle). \end{aligned} \quad (47)$$

下标 c 代表相干态. 其中

$$|\alpha\rangle = \exp\left(\frac{-|\alpha|^2}{2}\right)\left(\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\right). \quad (48)$$

四个变换相干态的近似幺正操作表示为

$$\begin{aligned}U_0^{\rm c} &= |\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|, \\ U_1^{\rm c} &= |\alpha\rangle\langle\alpha| - |-\alpha\rangle\langle-\alpha|, \\ U_2^{\rm c} &= |\alpha\rangle\langle-\alpha| + |-\alpha\rangle\langle\alpha|, \\ U_3^{\rm c} &= |\alpha\rangle\langle-\alpha| - |-\alpha\rangle\langle\alpha|. \end{aligned} \quad (49)$$

通信过程中双方使用块状传输数据以及插入诱骗光子的方法保障通信安全. 作者还讨论了实际操作中使用改良的自旋相干态 (modified spin coherent state) 作为物理实体与普通相干态的差异, 给出了实验实现 QSDC 的一种可行途径. 其实, 基于最早的几个经典 QSDC 方案的原理, 我们可以选择不同的物理实体实现量子直接通信过程.

3.14 量子直接通信网络方案

前面我们介绍的都是点对点的量子通信方案, 方案中量子态的制备和测量都由信息的发送者或接收者完成. 这样的通信模式对每个通信参与者的能力要求较高. 借鉴经典通信的经验, 利用安全可靠的服务器来制备和测量量子信号的网络通信模式是量子通信的发展趋势. 不过到目前为止, 量子网络通信的模型并不多. 这是因为虽然服务器的出现可以简化对用户设备的要求, 但是服务器比外界窃听者能接触到更多有用的信息, 因此网络通信模式对方案的安全性提出了更高的要求.

2006 年, 李熙涵等 [53] 提出了一个基于两步 QSDC 模型的量子直接通信网络模型. 这个网络方

案是环形拓扑结构的, 原理如图4所示. 模型中每一个子系统由服务器Alice、信息发送者Bob和接收者Charlie构成. 通信三方事先约定四个单比特幺正操作分别代表相应的两比特信息. 首先服务器Alice制备N个EPR对序列$|\psi^+\rangle_{\rm CM}$. 她将对应的纠缠粒子分别构成$S_{\rm C}$和$S_{\rm M}$两个序列, 分别用于安全性检测和加载信息. 随后, Alice利用两步通信的方法先后将两个粒子序列分两步发送给Bob. Bob收到后先将$S_{\rm C}$序列中的一些粒子用随机处于$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$的诱骗光子替代, 随后发送给Charlie. Bob和Charlie先利用诱骗光子判断传输是否安全, 确认安全后Bob根据要传输的机密信息对$S_{\rm M}$序列进行相应的幺正操作, 同时Bob在机密信息中插入一定量的随机编码. 随机编码分成两份, 用于后续的两次安全性检测. 编码完成后Bob将$S_{\rm M}$序列发送给Charlie. Charlie和Bob首先利用第一组随机编码检测传输安全. 随后Charlie随机选取四个幺正操作中的一个对每一个纠缠对中的一个粒子进行操作. 随后Charlie用两步传输的办法将两个序列发还给服务器Alice. Alice对相应的纠缠粒子进行联合贝尔基测量并公布测量结果. Bob和Charlie使用Bob的第二组随机编码检测安全. Charlie可根据Alice的测量结果及自己的幺正操作推断出Bob的机密信息. 方案中纠缠粒子对在三方之间的传输都遵循两步传输的方式, 避免了外界窃听者同时拥有纠缠的两个部分. 同年, 邓富国等[54]基于两粒子纠缠态还提出了直线型拓扑结构的量子直接通信网络方案. 该方案基于纠缠转移的原理, 避免了服务器二次接触到携带信息的纠缠粒子对, 能保障网络通信的安全. 2007年, 邓富国等[55]基于d维两粒子最大纠缠态提出了环形拓扑结构的量子直接通信网络模型. 由于使用了高维系统, 信道的容量随之增大.

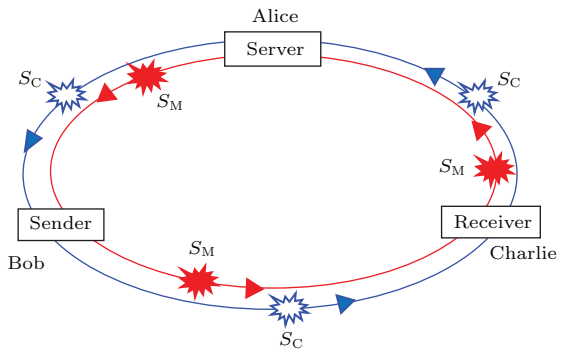

图4 量子直接通信环形网络示意图

Fig. 4. The subsystem of the QSDC network.

2007年, 邓富国等[56]还提出了基于单光子态的量子直接通信网络模型. 服务器首先制备单光子态$|0\rangle$序列S_0, 随后将其发送给信息的接收者Charlie. Charlie首先随机选取一定量的样本做单光子测量并检测是否有多光子态. 确定安全后他随机地选取I或σ_x操作对粒子序列进行操作, 同时Charlie随机选取一些位置加载Hadamard操作制备处于$|\pm\rangle$态的诱骗光子. 随后Charlie将单光子序列发送给信息发送方Bob. Bob首先对诱骗光子及随机另选的一些单光子态做测量进行安全性检测. 他同时用极化分束器检测序列中是否含有多光子信号. 确认安全后, Bob根据自己的机密信息对光子加载I或σ_x操作. 在加载信息的过程中, Bob插入一些随机编码用于后续的安全性检测. 随后Bob将序列发还给服务器Alice. Alice对粒子序列进行单光子测量后公布结果. Bob公布随机编码供Charlie检测最后一次传输的安全. Charlie根据自己加载的随机信息及Alice公布的测量结果即可读取Bob的机密信息. 在这个方案中, 由于参与者只需具备单粒子操作和测量的能力, 对实验技术的要求较低, 容易推广.

4 总 结

在本文的调研过程中, 我们发现部分学者混淆了确定的量子密钥分配(DQKD)与量子直接通信(QSDC)的概念[14−16,19−22]. 前面我们已经提到, 虽然二者都可以用于通信双方协调地得到信息(确定的密钥、机密信息或随机信息), 但接收者是否需要额外的经典信息来读取信息是区分QSDC和DQKD的关键之一. 在DQKD中[14−16,19−21], 通信双方借助测量结果的一一对应关系来获得协调的信息, 但在测量前他们的结果都是随机的, 这相当于量子密钥. 这些方案与基于非最大纠缠信道的DQKD方案[18]类似, 由于测量结果的随机性, 接收者势必需要发送者的测量结果才能读取信息, 因此这些方案都是典型的DQKD方案. 而在文献[22]中携带信息的光子态只需传输一次, 这样接收者势必需要发送者告知正确的测量基矢才能读取信息, 因此该方案也是典型的DQKD方案.

量子通信的优势体现在安全性上, 量子直接通信由于直接传递机密信息而对安全性提出了更高的要求——确保信道安全后才能传输信息[30,31]; 窃听者即使窃听也只能得到随机的结果而非有用

的信息[54]. 在量子直接通信过程中, 除了针对截获重发的安全性检测之外, 还需要考虑特洛伊木马攻击, 即窃听者在合法的信号中混入窃听信号, 用于读取幺正操作编码的机密信息. 这一方面需要我们利用光子数分束器检测多光子信号[75], 另一方面必须保证"一传一测"——每一批量子态传输后都需要进行安全性检测[69].

量子通信由于其不可比拟的安全性而备受关注, 而量子直接通信可利用量子信道直接传输机密信息, 是未来量子通信发展的重要方向. 在物理原理上, 量子直接通信利用块状传输和分步传输保障了机密信息直接传输的安全[29−31]. 在一定噪声环境下, 可以利用机密放大、纠错、冗余编码等方法保障机密信息安全保真的传输[74,76,77]. 如果环境噪声较强, 量子直接通信可以退化到量子密钥分配, 即传输随机的密钥, 其效率比传统量子密钥分配方案高很多. 回顾量子直接通信的发展历程, 研究者们从理想条件到噪声环境、从二维系统到高维系统在QSDC领域进行了一系列的探索. 量子直接通信对安全性的较高要求使其发展落后于相对简单的量子密钥分配分支, 不过其发展轨迹也将遵循量子通信的发展历程——从理论研究过渡到实验研究从而最终走向实用化进程. 在实际应用中, 一方面量子信号的传输距离会受到实验条件的限制, 可以通过量子中继器[78−82]来完成量子信号的远距离传输; 另一方面, 量子信号的保真度会受到环境噪声的影响, 对于单光子态系统我们可以采用量子态避错传输[83−86]等办法避免噪声的影响, 对于纠缠系统我们可以采取纠缠浓缩[87−93]、概率渐进式纠缠纯化[94−98]、确定式纠缠纯化[99−102]等技术压制信道噪声与环境噪声对光量子信号的影响, 最终实现远程化与网络化的量子直接通信.

回顾量子直接通信的发展历程, 我们不难发现, 国内学者在这一量子通信重要方向的发展中做出了突出贡献, 不仅提出了原创的模型, 发明了量子数据块传输与分步传输方法, 给出了QSDC的安全判据和构造原理, 还提出了高效协议、两步协议、量子一次一密协议、高维协议等一批有代表性的协议, 主导了这一方向的发展. 目前, 国内外学者积极开展各种情形下的QSDC理论与实验研究, 并应用于其他一些量子通信任务, 如量子签名[103]、量子对话[104]、量子广播[105]、量子水印[106]、量子匿名排序[107]等需要传输确定信息的量子通信任务. 如今, 量子直接通信已经成为了量子信息研究中的一个持续研究热点.

参考文献

[1] Bennett C H, Brassard G 1984 *Proceedings of IEEE International Conference on Computers, System and Signal Processing* (Bangalore: IEEE) p175

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

[3] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[4] Deng F G, Long G L 2003 *Phys. Rev. A* **68** 042315

[5] Deng F G, Long G L 2004 *Phys. Rev. A* **70** 012311

[6] Li X H, Deng F G, Zhou H Y 2008 *Phys. Rev. A* **78** 022321

[7] Beige A, Englert B G, Kurtsiefer C, Weinfurter H 2002 *Acta Phys. Pol. A* **101** 357

[8] Yan F L, Zhang X 2004 *Eur. Phys. J. B* **41** 75

[9] Gao T, Fan F L, Wang Z X 2005 *J. Phys. A* **38** 5761

[10] Man Z X, Zhang Z J, Li Y 2005 *Chin. Phys. Lett.* **22** 18

[11] Man Z X, Zhang Z J, Li Y 2005 *Chin. Phys. Lett.* **22** 22

[12] Zhu A D, Xia Y, Fan Q B, Zhang S 2006 *Phys. Rev. A* **73** 022338

[13] Lee H, Lim J, Yang H 2006 *Phys. Rev. A* **73** 042305

[14] Wang J, Zhang Q, Tang C J 2006 *Int. J. Quantum Inf.* **4** 925

[15] Wang J, Zhang Q, Tang C J 2006 *Int. J. Mod. Phys. C* **17** 685

[16] Wang H F, Zhang S, Yeon K H, Um C I 2006 *J. Korean Phys. Soc.* **49** 459

[17] Chang Y, Zhang S B, Yan L L, Li J 2014 *Chin. Sci. Bull.* **59** 2835

[18] Li X H, Deng F G, Li C Y, Liang Y J, Zhou P, Zhou H Y 2006 *J. Korean Phys. Soc.* **49** 1354

[19] Gao G, Fang M, Yang R M 2011 *Int. J. Theor. Phys.* **50** 882

[20] Wu Y H, Zhai W D, Cao W Z, Li C 2011 *Int. J. Theor. Phys.* **50** 325

[21] Zhang Q N, Li C C, Li Y H, Nie Y Y 2013 *Int. J. Theor. Phys.* **52** 22

[22] Chang Y, Xu C X, Zhang S B, Yan L L 2013 *Chin. Sci. Bull.* **58** 4571

[23] Quan D X, Pei C X, Liu D, Zhao N 2010 *Acta Phys. Sin.* **59** 2493 (in Chinese) [权东晓, 裴昌幸, 刘丹, 赵楠 2010 物理学报 **59** 2493]

[24] Tsai C W, Hwang T 2013 *Sci. China Phys. Mech. Astron.* **56** 1903

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

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

[27] Xiao L, Long G L, Deng F G, Pan J W 2004 *Phys. Rev. A* **69** 052307

[28] Deng F G, Zhou H Y, Long G L 2006 *J. Phys. A* **39** 14089

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

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

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

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

[33] Wang C, Deng F G, Long G L 2005 *Opt. Commun.* **253** 15

[34] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J, Zhou H Y 2007 *Chin. Phys.* **16** 2149

[35] Lin S, Wen Q Y, Gao F, Zhu F C 2008 *Phys. Rev. A* **78** 064304

[36] Gu B, Zhang C Y, Cheng G S, Huang Y G 2011 *Sci. China Phys. Mech. Astron.* **54** 942

[37] Wang T J, Li T, Du F F, Deng F G 2011 *Chin. Phys. Lett.* **28** 040305

[38] Gu B, Huang Y G, Fang X, Zhang C Y 2011 *Chin. Phys. B* **20** 100309

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

[40] Liu D, Chen J L, Jiang W 2012 *Int. J. Theor. Phys.* **51** 2923

[41] Sun Z W, Du R G, Long D Y 2012 *Int. J. Theor. Phys.* **51** 1946

[42] Ren B C, Wei H R, Hua M, Li T, Deng F G 2013 *Eur. Phys. J. D* **67** 30

[43] Gu B, Huang Y G, Fang X, Chen Y L 2013 *Int. J. Theor. Phys.* **52** 4461

[44] Banerjee A, Pathak A 2012 *Phys. Lett. A* **376** 2944

[45] Pirandola S, Braunstein S L, Mancini S, Lloyd S 2008 *Eur. Phys. Lett.* **84** 20013

[46] Meslouhi A, Hassouni Y 2013 *Quantum Inf. Process.* **12** 2603

[47] Zheng C, Long G F 2014 *Sci. China Phys. Mech. Astron.* **57** 1238

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

[49] Karlsson A, Bourennane M 1998 *Phys. Rev. A* **58** 4394

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

[51] Bennett C H, Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881

[52] Liu X S, Long G L, Tong D M, Li F 2002 *Phys. Rev. A* **65** 022304

[53] Li X H, Zhou P, Liang Y J, Li C Y, Zhou H Y, Deng F G 2006 *Chin. Phys. Lett.* **23** 1080

[54] Deng F G, Li X H, Li C Y, Zhou P, Zhou H Y 2006 *Phys. Lett. A* **359** 359

[55] Deng F G, Li X H, Li C Y, Zhou P, Zhou H Y 2007 *Phys. Scr.* **76** 25

[56] Deng F G, Li X H, Li C Y, Zhou P, Zhou H Y 2007 *Chin. Phys.* **16** 3553

[57] Inagaki T, Matsuda N, Tadanaga O, Asobe M, Takesue H 2013 *Opt. Express* **21** 23241

[58] Tang Y L, Yin H L, Chen S J, Liu Y, Zhang W J, Jiang X, Zhang L, Wang J, You L X, Guan J Y, Yang D X, Wang Z, Liang H, Zhang Z, Zhou N, Ma X F, Chen T Y, Zhang Q, Pan J W 2014 *Phys. Rev. Lett.* **113** 190501

[59] Lu X, Wang W, Ma J 2013 *IEEE Trans. Smart Grid* **4** 170

[60] Long G L, Wang C, Li Y S, Deng F G 2011 *Sci. China-Phys. Mech. Astron.* **41** 332 (in Chinese) [龙桂鲁, 王川, 李岩松, 邓富国 2011 中国科学: 物理, 力学, 天文学 **41** 332]

[61] Long G L, Qin G Q 2014 *Physics and Engineering* **24** 3 (in Chinese) [龙桂鲁, 秦国卿 2014 物理与工程 **24** 3]

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

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

[64] Deng F G, Li X H, Li C Y, Zhou P, Zhou H Y 2007 *Chin. Phys.* **16** 277

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

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

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

[68] Long G L, Deng F G, Wang C, Li X H 2007 *Front. Phys. China* **2** 251

[69] Li X H, Deng F G, Zhou H Y 2006 *Phys. Rev. A* **74** 054302

[70] Li C Y, Zhou H Y, Wang Y, Deng F G 2005 *Chin. Phys. Lett.* **22** 1049

[71] Li C Y, Li X H, Deng F G, Zhou P, Liang Y J, Zhou H Y 2006 *Chin. Phys. Lett.* **23** 2896

[72] Cerè A, Lucamarini M, Giuseppe G D, Tombesi P 2006 *Phys. Rev. Lett.* **96** 200501

[73] Hu J Y, Yu B, Jing M Y, Xiao L T, Jia S T 2015 arXiv:1503.00451

[74] Deng F G, Long G L 2006 *Commun. Theor. Phys.* **46** 443

[75] Deng F G, Li X H, Zhou H Y, Zhang Z J 2005 *Phys. Rev. A* **72** 044302

[76] Wen K, Long G L 2005 *Phys. Rev. A* **72** 022336

[77] Wen K, Long G L 2010 *Int. J. Quantum Inf.* **8** 697

[78] Briegel H J, Dür W, Cirac J I, Zoller P 1998 *Phys. Rev. Lett.* **81** 5932

[79] Dür W, Briegel H J, Cirac J I, Zoller P 1999 *Phys. Rev. A* **59** 169

[80] Duan L M, Lukin M D, Cirac J I, Zoller P 2001 *Nature* **414** 413

[81] Chen S, Chen Y A, Zhao B, Yuan Z S, Schmiedmayer J, Pan J W 2007 *Phys. Rev. Lett.* **99** 180505

[82] Wang T J, Song S Y, Long G L 2012 *Phys. Rev. A* **85** 062311

[83] Li X H, Deng F G, Zhou H Y 2007 *Appl. Phys. Lett.* **91** 144101

[84] Deng F G, Li X H, Zhou H Y 2011 *Quantum Inf. Comput.* **11** 913

[85] Li X H, Duan X J 2011 *J. Phys. B: At. Mol. Opt. Phys.* **44** 065503

[86] Li X H, Zeng Z, Wang C 2014 *J. Opt. Soc. Am. B* **31** 2334

[87] Bennett C H, Bernstein H J, Popescu S, Schumacher B 1996 *Phys. Rev. A* **53** 2046

[88] Zhao Z, Pan J W, Zhan M S 2001 *Phys. Rev. A* **64** 014301

[89] Yamamoto T, Koashi M, Imoto N 2001 *Phys. Rev. A* **64** 012304

[90] Sheng Y B, Deng F G, Zhou H Y 2008 *Phys. Rev. A* **77** 062325

[91] Ren B C, Du F F, Deng F G 2013 *Phys. Rev. A* **88** 012302

[92] Li X H, Ghose S 2014 *Laser Phys. Lett.* **11** 125201

[93] Li X H, Ghose S 2015 *Opt. Express* **23** 3550

[94] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A, Wootters W K 1996 *Phys. Rev. Lett.* **76** 722

[95] Pan J W, Simon C, Brukner C, Zellinger A 2001 *Nature* **410** 1067

[96] Simon C, Pan J W 2002 *Phys. Rev. Lett.* **89** 257901

[97] Sheng Y B, Deng F G, Zhou H Y 2008 *Phys. Rev. A* **77** 042308

[98] Ren B C, Du F F, Deng F G 2014 *Phys. Rev. A* **90** 052309

[99] Sheng Y B, Deng F G 2010 *Phys. Rev. A* **81** 032307

[100] Li X H 2010 *Phys. Rev. A* **82** 044304

[101] Sheng Y B, Deng F G 2010 *Phys. Rev. A* **82** 044305

[102] Deng F G 2011 *Phys. Rev. A* **83** 062316

[103] Yoon C S, Kang M S, Lim J I, Yang H J 2015 *Phys. Scr.* **90** 015103

[104] Shi G F, Xi X Q, Hu M L, Yue R H 2010 *Opt. Commun.* **283** 1984

[105] Chang Y, Xu C X, Zhang S B, Yan L L 2014 *Chin. Phys. B* **23** 010305

[106] Fatahi N, Naseri M 2012 *Int. J. Theor. Phys.* **51** 2094

[107] Huang W, Wen Q Y, Liu B, Su Q, Qin S J, Gao F 2014 *Phys. Rev. A* **89** 032325

SPECIAL ISSUE — Quantum metrology and control

Quantum secure direct communication*

Li Xi-Han†

(*College of Physics, Chongqing University, Chongqing 401331, China*)

(*Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo N2L3C5, Canada*)

(Received 12 May 2015; revised manuscript received 9 June 2015)

Abstract

Quantum secure direct communication (QSDC) is one of the most important branches of quantum communication. In contrast to the quantum key distribution (QKD) which distributes a secure key between distant parties, QSDC directly transmits secret message instead of sharing key in advance. To establish a secure QSDC protocol, on the one hand, the security of the quantum channel should be confirmed before the exchange of the secret message. On the other hand, the quantum state should be transmitted in a quantum data block since the security of QSDC is based on the error rate analysis in the theories on statistics. Compared with the deterministic quantum key distribution (DQKD) which can also be used to transmit deterministic information, QSDC schemes do not need extra classical bits to read the secret message except for public discussion. In this article, we introduce the basic principles of QSDC and review the development in this field by introducing typical QSDC protocols chronologically. The first QSDC protocol was proposed by Long and Liu, which can be used to establish a common key between distant parties. In their scheme, the method for transmitting quantum states in a block by block way and in multiple steps was proposed and the information leakage before eavesdropping detection was solved. Subsequently, Deng et al. presented two pioneering QSDC schemes, an entangled-state-based two-step QSDC scheme and a single-photon-state-based quantum one-time pad scheme, in which the basic principle and criteria for QSDC were pointed out. From then on, many interesting QSDC schemes have been proposed, including the high-dimension QSDC scheme based on quantum superdense coding, multi-step QSDC scheme based on Greenberger-Horne-Zeilinger states, QSDC scheme based on quantum encryption with practical non-maximally entangled quantum channel, and so on. We also introduce the anti-noise QSDC schemes which were designed for coping with the collective-dephasing noise and the collective-rotation noise, respectively. In 2011, Wang et al. presented the first QSDC which exploited the hyperentangled state as the information carrier and several QSDC schemes based on the spatial degree of freedom (DOF) of photon, single-photon multi-DOF state and hyperentanglement were proposed subsequently. In addition to the point-to-point QSDC schemes, we also review the QSDC networks. Finally, a perspective of QSDC research is given in the last section.

Keywords: quantum communication, quantum secure direct communication, quantum secure direct communication network

PACS: 03.67.Hk, 03.65.Ud, 03.67.Dd **DOI:** 10.7498/aps.64.160307

* Project supported by the National Natural Science Foundation of China (Grant No. 11004258) and the Fundamental Research Funds for the Central Universities, China (Grant No. CQDXWL-2012-014).

† Corresponding author. E-mail: xihanlicqu@gmail.com