中国科学: 物理学 力学 天文学 2011 年 第 41 卷 第 4 期: 332 ~ 342
SCIENTIA SINICA Phys, Mech & Astron www.scichina.com phys.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS

清华大学百年校庆专刊 · 评述

量子安全直接通信

龙桂鲁[①*], 王川[①], 李岩松[①], 邓富国[②]

① 教育部原子分子纳米科学重点实验室, 清华大学物理系, 北京 100084;
② 北京师范大学物理系, 北京 100875
*E-mail: gllong@tsinghua.edu.cn

收稿日期: 2011-02-18; 接受日期: 2011-02-28
国家自然科学基金(批准号: 10874098)和国家重点基础研究发展计划(编号: 2009CB929402)资助项目

摘要 量子通信利用量子力学原理进行信息传输和处理, 具有高安全、高容量等优点. 量子安全直接通信在量子信道中直接传输秘密信息, 是一种新式的量子通信模式. 自 2000 年提出以来, 量子安全直接通信得到了迅速的发展. 该文综述量子安全直接通信的基本原理, 描述几个典型的量子安全直接通信协议. 最后介绍量子安全直接通信的最新发展动态, 展望量子安全直接通信的未来.

关键词 量子安全直接通信, 量子通信, 两步方案, 量子一次便笺方案, 网络通信, QSDC

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

简单地说, 量子通信就是通过量子信道传递经典或者量子信息的通信. 量子通信的主要优点是能在合法的通信者之间实现绝对安全的通信. 量子通信在过去的 20 多年中成为量子信息研究的一个主要内容, 具有很好的应用前景. 量子密钥分发是量子通信的一个重要研究内容. 1984 年, Bennett 和 Brassard 提出了利用两组正交偏振状态的单光子进行编码通信的量子密钥分发方案(俗称 BB84)[1]. 量子密钥分发的结果是通信双方共享一组由二进制随机序列组成的密钥. 要传递秘密信息, 通信的发送者需要将秘密信息利用密钥加密生成密文, 然后将密文发送给信息接收者. 接收者利用密钥解码密文从而得到传递的秘密信息. 也就是说, 借助于量子密钥分发, 通信双方还要再进行一次经典通信才能完成秘密信息的安全传输.

量子不可克隆原理和量子测不准原理保证了量子通信的安全性. 1992 年, Bennett 提出了一个利用一组非正交态进行量子通信的简化量子密钥分发方案[2]. 量子通信的载体可以是单光子, 也可以是诸如量子纠缠态的其他资源[3,4].

量子安全直接通信(Quantum secure direct communication, QSDC)是一种不同于量子密钥分发的新量子通信形式, 与量子密钥分发根本性区别在于量子安全直接通信在量子信道中直接传递秘密信息. 量子安全直接通信的安全性也是基于量子不可克隆原理、量子测不准原理以及纠缠粒子的关联性和非定域等. 与量子密钥分发的过程不同, 量子安全直接通信过程中, 通信双方不需要事先生成密钥, 而是通过直接建立量子信道的方式进行通信, 从而将一般意义上的量子通信过程简化为一步量子通信过程, 即直接完成秘密信息的安全传输. 既然量子安全直接通信可以传递指定的秘密信息, 当然可以传递完全

引用格式: 龙桂鲁, 王川, 李岩松, 等. 量子安全直接通信. 中国科学: 物理学 力学 天文学, 2011, 41: 332–342
Long G L, Wang C, Li Y S, et al. Quantum secure direct communication (in Chinese). Sci Sin Phys Mech Astron, 2011, 41: 332–342, doi: 10.1360/132011-178

随机的密钥. 由此也经常导致人们将量子安全直接通信和量子密钥分发相混淆. 在实际分析一个量子通信方案是否是量子安全直接通信方案时, 必须看其是否能够安全地直接传递秘密信息, 即是否能防止秘密信息在直接传输过程中发生泄露.

2000 年, 龙桂鲁和刘晓曙提出了第一个量子安全直接通信方案——高效两步量子安全直接通信方案[5]. 2001 年, Beige 等人[6,7]提出了确定的安全通信的概念; Boström 和 Felbinger[8]借鉴了量子密集编码中的思想, 提出了利用量子纠缠态实现近似安全的确定的量子直接通信方案. 2003 年, 邓富国、龙桂鲁和刘晓曙提出了基于密集编码的两步量子安全直接通信方案[9], 并对量子安全直接通信方案的标准进行了讨论.

在量子安全直接通信的发展过程中, 出现了几个与之相关, 但也是容易混淆的概念. 一是确定性量子密钥分发. 它传递的密钥是随机数, 但每次传递的信息可以确定性地读取. 如果发现有人窃听, 则把传递的数据扔掉, 如果没有窃听则可以留下. 特别强调的是, 确定性密钥分发传递的是随机数, 而不是秘密信息. 另一个容易混淆的概念是确定的安全量子通信 (Deterministic Secure Quantum Communication, DSQC), 它也与确定性量子密钥分发紧密相关. 在确定的安全量子通信中, 通信发送者利用密码加密秘密信息后, 通过量子信道发送, 如果确认信道没有被窃听, 则通过经典信道公开密钥. 这实际上是基于量子密钥分发通信的变形. 通常信息发送者使用量子密钥分发通过量子信道产生密码, 然后使用密码将秘密信息加密成密文, 通过经典信道将密文发送给接收者. 而 DSQC 则是将密码通过经典信道发送, 这完全可以被窃听者获得, 而密文是通过量子信道发送的, 可以确定量子信道是否被窃听, 从而保证了通信的安全. 确定的安全量子通信与量子安全直接通信的区别在于通信双方在直接通信的过程中是否需要经典信息的交换. 确定的安全量子通信是通信双方在完成信息直接传递的过程中需要经典信息的通信过程作为辅助, 即经经典信道公开传输密码, 然后才能读出秘密信息; 而量子安全直接通信过程则不需要经典信息的传递, 发送者完成量子比特传输以后, 接收者可以直接读出机密信息.

量子安全直接通信不但可以使用 Bell 态, 而且可以使用单光子和其他的量子载体. 量子一次便笺方案采用单光子作为信息载体[10], 在这里单光子成块地每次以 N 个为单位进行传输. 这个方案的 N=1 特例就是 Lucamarini 等人[11]提出了 LM05 方案. 蔡庆宇等人提出了用极化单光子来替代纠缠粒子对完成 Boström 和 Felbinger 的确定性量子密钥分发方案[12]. 2004 年, 闫凤利等人[13]提出了利用量子远程传态进行量子直接通信的方案. 2005 年, 王川等人提出了高维超密集编码的量子安全直接通信模型[14]和一个多步量子安全直接通信模型[15]. 随后, 满忠晓和张战军等人提出了利用量子纠缠交换和局域幺正操作进行确定的安全直接通信方案[16], 朱爱东等人提出了利用粒子重排方法进行安全量子直接通信的方案[17], 李熙涵等人提出了基于量子加密的量子安全直接通信方案[18]和基于单光子及其非最大纠缠态的确定的安全量子通信方案[19]. 在利用多粒子纠缠提高通信容量方面, 曹海静等人提出了一个利用三粒子 W 态的量子安全直接通信方案[20]. 王剑等人提出了利用三粒子 GHZ 态进行多方控制量子安全直接通信的方案[21]. 在 QSDC 的安全性研究中, 蔡庆宇提出了不可见光子攻击方法[22]; 邓富国等人研究了多光子特洛伊木马攻击及其防御方法[23];李熙涵等人提出了多光子和延迟光子攻击方法及其预防措施, 给出了安全检测的一般原理[24]; 杨宇光等人[25]推广了认证的量子安全直接通信方案模型; 高飞等人[26]在论文中对不同攻击策略下 QSDC 的安全性进行了一些分析. 顾斌等人[27]研究了在噪声下的量子安全直接通信. 量子安全直接通信的研究成为近年来研究热点之一, 文献[28]综述了量子安全直接通信的一些主要进展.

1 窃听探测前信息泄露和量子通信安全

量子通信的最大优点之一是其安全性. 而量子通信的安全性是通过合法的通信双方依靠量子力学原理能探测到窃听者的存在来保证的. 传统意义上的量子通信方式, 即量子密钥分发的安全性来源于窃听者对于量子通信的任何窃听行为都能被合法的通信双方发现, 然后通信双方可以抛弃已有的通信结果, 并重新开始传输量子比特, 从而保证密钥分发的安全. 量子安全直接通信传输的是机密信息本身, 因而对于安全性的要求更高, 不能简单地通过抛弃传输结果的方法来保证机密信息不会泄露给窃听者. 通信者必须在传输机密信息之前就要确定窃听者是

否监听了量子信道. 因此在量子密钥分发的过程中就会存在信息泄露的问题, 即随机密钥会被窃听者得到. 由于随机密钥不携带任何信息, 故不会对通信的安全性产生影响. 窃听探测之前的信息泄露(Information Leakage Before Eavesdropper Detection——ILBED)是量子通信的一个重要概念, 也是区分量子安全直接通信和其他量子通信的关键之一.

为了说明量子通信的安全和量子密钥分发与量子安全直接通信的区别, 我们这里先介绍ILBED. 一般而言, 在量子通信中, 合法通信的参加者要挑选出一部分信息载体进行测量, 并通过公开比对测量结果确认误码率, 根据误码率的大小确认信道的安全程度. 也就是说, 在确认误码率之前传输的信息, 都不能认为是安全的. 例如在量子密钥分发中, 误码率的大小是在整个通信过程完成之后才能确定, 如果发现有窃听, 只能将已传输的结果抛弃.

量子信道的安全性在量子通信的过程中要始终进行确认. 在BB84中, Alice制备一系列的单光子态, 每个单光子随机地处在$|0\rangle$, $|1\rangle$, $|0\rangle+|1\rangle$和$|0\rangle-|1\rangle$态上. Alice将这些单光子发送给Bob. Bob在接收到单光子之后, 随机地选取{$|0\rangle$,$|1\rangle$}基底或者{$|0\rangle+|1\rangle$, $|0\rangle-|1\rangle$}基底进行测量. 然后, 他们公开他们对每个单光子制备或者测量时所用的基底, 并保留使用相同基底的那些结果. 为了检验窃听, 他们从留下的相同测量基底的结果中再随机地选取部分结果进行比对, 从而得到误码率, 判断通信的安全. 因此直到通信的最后, 合法的通信双方才能确认信道的安全性. 在BB84中, 所有的传输都存在窃听探测前的信息泄露威胁.

无论是非确定的量子密钥分发方案, 如BB84方案, 还是确定性的量子密钥分发方案, 如乒乓协议, 是否保留所传输的数据, 要在通信完成之后才能确定. 对于这一问题, 量子密钥分发的解决方案是在通信结束后, 确认是否有信息泄露. 如果有则放弃所传输的结果, 否则保留结果, 再进行下一步的后处理过程. 在确定性量子通信(DSQC)中, 这一困难是通过公开还是不公开密钥来解决的. 如果确认量子信道安全, 则通信双方可以确认窃听者没有得到通过量子信道传输的密文, 然后再经过经典信道公开密钥. 它等同于量子密钥分发. 这样, 在探测到窃听之前的信息泄露, 就可以通过抛弃传输结果而避免. 但是在量子安全直接通信中, 这样的处理则是不允许的. 因为这时候量子信道中传输的是秘密信息, 如果采用类似于量子密钥分发的处理方法, 在我们发现窃听者之前就已经泄露了. 这就是为什么乒乓协议实际上只是一个量子密钥分发协议, 而不是量子安全直接通信的根本原因. 在乒乓协议中, 对每个粒子或者进行检测或者进行编码, 然后经过一系列的传输后确认误码率, 确定是否存在窃听, 在这之前的所有传输都存在信息泄露, 无法进行量子安全直接通信.

量子安全直接通信的要求要比量子密钥分发高, 它要求通信双方必须在机密信息加载于量子态上之前就能判断窃听者Eve是否监听了量子信道. 而量子通信的安全性都是基于抽样统计分析, 因此在安全分析前Alice和Bob需要有一批随机抽样数据. 这就要求QSDC中的量子数据必需以块的方式进行传输[5]. 只有这样, Alice和Bob才能从块传输的量子数据中做抽样分析. 而量子密钥分发没有这样的要求, 因为它只要求Alice和Bob在最后能判断Eve是否监听了量子信道, 从而判断传输的结果是否可用, 而且这种判断是量子密码通信的一种后处理过程.

综合QSDC的基本要求[5,9,10], 量子安全直接通信的标准[28~30]可以概括为

(ⅰ) 机密信息应该直接由信息的接收者读出, 通信过程除了安全性检测步骤外, 不需要附加的经典信息交换;

(ⅱ) 窃听者无论采取何种方法都不能获得机密信息, 窃听者得到的只能是一个随机的结果;

(ⅲ) 通信双方通过检测可以在机密信息泄露之前检测到窃听者的存在;

(ⅳ) 携带机密信息的量子态必需以量子数据块的形式传输.

第一个原则是区别量子安全直接通信和其他量子通信方案的关键. 有些量子通信方案虽然是确定性的, 但是它们传输的不是机密信息, 而是不含有机密信息的随机数序列, 经过检验后确认信道的安全性之后才能使用. 而另外一类确定性的量子通信中, 虽然传输的是机密信息, 但是需要额外的经典通信才能读出机密信息. 第二个原则在要求机密信息在传输中不能泄露, 即使在安全检验之前也不能泄露. 这就意味着量子安全直接通信的安全性要求更高. 第三个原则与量子密钥分发类似, 但是更加苛刻, 因为QSDC要求在信息泄露之前要检测到窃听者. 第

四个原则实际上是量子安全直接通信方案的构造方法, 如果不采用块传输的方法, 就会发生 ILBED, 即窃听检测前的信息泄露. 量子安全直接通信的相关协议研究中, 都需要遵守这些基本要求.

2 高效两步方案、块传输、分步传输和顺序重排

2000 年, 龙桂鲁和刘晓曙提出了高效两步方案[5], 简称两步方案. 该方案利用两粒子最大量子纠缠态(Bell 态)进行编码和解码. Bell 态的形式可写为

$$|\psi^-\rangle=\sqrt{\frac{1}{2}}\left(|0\rangle_A|1\rangle_B-|1\rangle_A|0\rangle_B\right), \quad (1)$$

$$|\psi^+\rangle=\sqrt{\frac{1}{2}}\left(|0\rangle_A|1\rangle_B+|1\rangle_A|0\rangle_B\right), \quad (2)$$

$$|\phi^-\rangle=\sqrt{\frac{1}{2}}\left(|0\rangle_A|0\rangle_B-|1\rangle_A|1\rangle_B\right), \quad (3)$$

$$|\phi^+\rangle=\sqrt{\frac{1}{2}}\left(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B\right), \quad (4)$$

这里的 A 和 B 分别标记纠缠态中的两个粒子, $|0\rangle$ 和 $|1\rangle$ 表示某个自由度上的两个不同的状态, 如光子的水平和垂直的偏振状态.

在高效两步方案中[5], Alice 随机制备 N 个处在某一个 Bell 态上的纠缠光子对, 并将这 N 个纠缠光子对分成两个序列, 即从每一纠缠光子对中挑出一个光子 A, 再将所有挑出来的光子组成一个光子序列 S_A, 而上述每一纠缠光子对中的另一个光子就可以组成另一个光子序列 S_B. Alice 先将量子数据块 S_B 发给信息接收者 Bob. Bob 接收到这个粒子序列后, 随机地选择部分粒子进行安全性检测, 与 Alice 进行安全分析. 在确保第一步通信安全以后, 通信双方就建立了一个安全的量子纠缠信道. Alice 将量子数据块 S_A 发送给 Bob. 这样, Bob 就得到了 Alice 的编码纠缠态. 对这些纠缠态进行联合的纠缠态测量就可以读出态的信息, 从而获取 Alice 加载的信息. 通信双方就以安全的方式传输了信息.

这个方案可以在通信双方之间直接传输机密信息, 实现量子安全直接通信. 有学者指出, 高效两步方案的优点是容量增大[31]、效率高, 它的效率比 Ekert 的协议高一倍[32].

值得指出, 这里首次使用了块传输和分步传输的方法. 量子信息载体不是一个个地传输, 而是以一定数量构成的块为单位来进行. 这种块传输的方法是构造量子安全直接通信的关键之一. 此外, 纠缠粒子对被分成两步来分别进行传输, 而量子通信的安全则由量子纠缠的性质得以保证. 窃听者每次只能窃取纠缠粒子体系的一部分, 得不到纠缠量子对的整体状态, 从而保证了信息不泄露. 在量子通信的构造中, 可以利用量子体系的性质, 特意将粒子的序列顺序打乱, 从而起到保护信息不被窃听的目的, 这就是顺序重排方法[33]. 分步传输、块传输方法以及粒子顺序重排方法[33] 是构造量子通信的通用方法, 至今已经被广泛地应用于包括量子安全直接通信、量子秘密共享、量子密钥分发、量子对话等量子通信协议的构造.

高效两步方案中的 ILBED 是通过对分步传输的量子数据块进行抽样测量来得以避免的. 对由 EPR 对中的第一个粒子组成的块进行随机抽样测量后, 可以确定该粒子块的安全性, 而这些粒子只是纠缠对中的一个粒子组成的, 因此不携带粒子对的整体状态, 窃听者虽然可以窃听, 但是得不到粒子对的状态信息, 而窃听者的窃听则造成误码检测中的误码率升高, 从而被合法通信双方探测. 如果发现窃听, 则将终止通信, 而此时窃听者由于没有得到整个的粒子对, 得不到任何秘密信息, 从而就避免了 ILBED.

3 两步方案

2003 年, 邓富国、龙桂鲁和刘晓曙提出了利用量子密集编码(DC)的两步量子安全直接通信方案(Two-Step QSDC)[9], 即人们经常提到的两步方案. 在两步方案中[9], 编码态选用 Bell 态形式的量子纠缠态. 我们可以用图 1 来描述两步量子安全直接通信的过程.

在两步方案[9]中, 信息发送者 Alice 制备一组由纠缠光子对组成的量子信号, 即 N 个纠缠光子对, 并使它们都处于相同的量子态, 如量子态 $|\phi^+\rangle$ 上. 然后, Alice 将这 N 个纠缠光子对分成两个序列, 即从每一纠缠光子对中挑出光子 A, 再将所有挑出来的光子组成一个光子序列 S_A, 而上述每一纠缠光子对中的另一个光子就可以组成另一个光子序列 S_B. 如图 1 所示, 用实线连接的两光子表示一纠缠光子对. 我们把 S_B

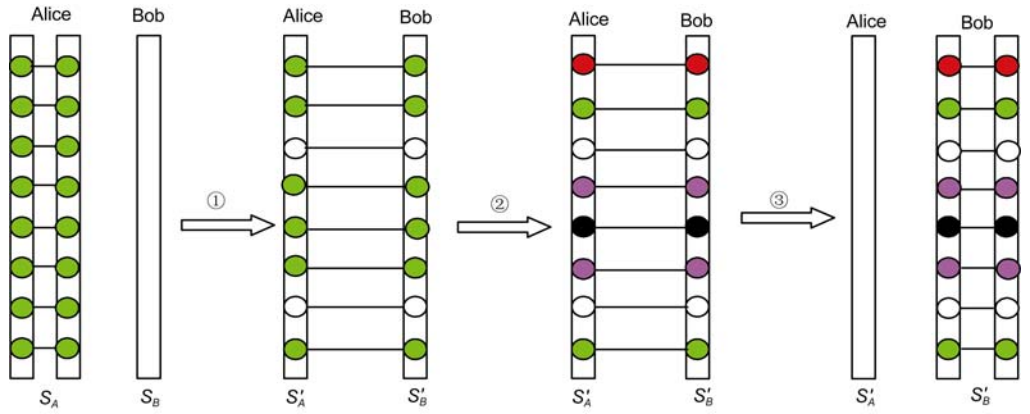

图 1　两步方案的原理图

Figure 1　Principle of the two-step protocol.

序列叫检测序列, 把 S_A 序列叫信息序列[9].

Alice 先将检测序列 S_B 发送给信息接收方 Bob, 但她仍然控制信息序列 S_A. Bob 接收到光子序列 S_B 后, 从中随机地抽取适量的光子, 并对其进行单光子测量. 这里的单光子测量, 原理与 BB84-QKD 方案[1]类似, 即 Bob 随机地选择两组测量基 σ_z 测量基 $\{|0\rangle,|1\rangle\}$ 和 σ_x 测量基 $\{|0\rangle+|1\rangle,|0\rangle-|1\rangle\}$ 中的一组来对每一个抽样光子进行测量并记录测量基信息以及测量结果. 测量完后, Bob 用经典信道(如无线电广播等不能被篡改在其中传输的经典信息的信道)告诉 Alice 他在 S_B 中对哪一些光子进行了单光子测量并告知相应的测量基信息及其测量结果.

Alice 根据 Bob 所告知的所有信息, 在 S_A 中用相同于 Bob 的测量基对与 Bob 的抽样光子相对应的光子(即属于同一纠缠光子对)进行单光子测量, 并记录测量结果. Alice 将自己的测量结果与 Bob 所告知的测量结果进行比对并做出错率分析; 如果出错率比预先设定的安全阈值低很多, 则表明光子序列 S_B 的传输是安全的, 即可以认为没有窃听者监视量子信道; 否则, Alice 和 Bob 放弃已经得到的传输结果. 从而 S_B 序列的传输主要是为了检测纠缠系统的传输安全, 而并没有对 S_B 做信息编码, 即加载机密信息, 这是我们称之为检测序列的主要原因[9].

在确保检测序列 S_B 安全传输的情况下, Alice 根据自己所需传输的信息, 每两比特位来对应地选择四个幺正操作 $U_0=I$, $U_1=\sigma_z$, $U_2=\sigma_x$, $U_3=\sigma_y$ 中的一个来对序列 S'_A (即在 S_A 中扣除用于安全性检测后的所有光子)中的每一个光子依次做相应的幺正操作, 从而完成对量子态的机密信息编码过程. 这也是我们称 S_A 为信息序列的原因. 四个幺正操作 U_0, U_1, U_2, U_3 可以分别代表编码 00, 01, 10 和 11. 当然, 在编码过程中, Alice 需要在随机的位置进行适量的安全检测编码, 即加入一些为下一次安全检测服务的随机编码[9].

随后, Alice 将编码后的 S'_A 序列发送给 Bob. Bob 对 S'_A 序列和与之对应的 S'_B 序列(即在 S_B 中扣除用于安全性检测后的所有光子)中对应的纠缠光子对做贝尔基联合测量, 从而读出 Alice 所做的操作信息, 即 Alice 对光子序列中的每一个光子分别采用了什么局域幺正操作, 也就得到了 Alice 所需传输的机密信息.

为了检查 S'_A 序列的传输安全性, 在量子态传输完后, Alice 告诉 Bob 她对哪一些纠缠粒子对进行了安全检测编码以及编码的数值; Bob 在其测量结果中挑出这一些检测编码数据, 并与 Alice 告知的结果进行比对, 分析出错率. 实际上, 这是 Alice 和 Bob 做第二次安全性分析.

事实上, 在第一次安全分析成功的情况下, 由于 Eve 无法同时得到光子序列 S_A 和 S_B, 因而她已经无法得到机密信息. 这是纠缠系统的量子特性局限了她对机密信息的窃听, 纠缠量子系统的特性要求 Eve 只有对整个纠缠体系做联合测量才能读出 Alice 做的局域幺正操作. 第二次安全性分析主要是为了判断窃听者是否在 S_A 序列传输过程破坏了 S_A 与 S_B 序列的量子关联性, 从而判断是否值得对已经传输的结

果做纠错等数据后处理.

在一定的实际噪声中, 两步方案在 S_B 序列传输完后, Alice 和 Bob 可以先借助纠缠纯化(entanglement purification)来提高信道的纠缠度并进行量子数据块的机密放大处理, 利用纠缠转移(entanglement swapping)来降低损耗对通信安全的影响, 然后再进行类似于理想环境下的两步量子安全直接通信[9].

4 高维两步方案

两步量子安全直接通信方案得到了推广和发展. 2005 年, 王川等人利用量子超密集编码的思想提出了高维两步量子安全直接通信方案, 也叫超密集编码量子安全直接通信方案[14]. 该方案利用高维粒子进行编码, 从而每个粒子可以携带多于一个比特的经典信息. 通信中用到的 d 维希尔伯特空间中的 Bell 态的形式可以写为

$$|\psi_{nm}\rangle=\sum_j e^{2\pi ijn/d}\,|j\rangle\otimes|j+m \bmod d\rangle/\sqrt{d}, \quad (5)$$

这里的 $n, m=0, 1, ..., d-1$. 相应的 d 维希尔伯特空间编码操作形式如下:

$$U_{nm}=\sum_j e^{2\pi ijn/d}\,|j+m \bmod d\rangle\langle j|. \quad (6)$$

该编码操作可以将初始态

$$|\psi_{00}\rangle=\sum_j|j\rangle|j\rangle/\sqrt{d} \quad (7)$$

变换到相应的 Bell 态 $|\psi_{nm}\rangle$.

高维两步方案的通信过程由 Alice 和 Bob 在两次粒子传输过程完成, 如图 2 所示. 与两步 QSDC 方案类似: 高维方案中信息的接收者 Bob 制备一系列的 d 维 Bell 态 $|\psi_{00}\rangle$. Bob 在每一个 Bell 态中选择一个粒子组成队列, 这里标记为 [P_1 (H), P_2 (H), P_3 (H), ... , P_N (H)]. 其余的粒子组成[P_1 (T), P_2 (T), P_3 (T), ... , P_N (T)]队列. Bob 将标记 T 的光子队列发送给 Alice, 双方进行安全性检测. 在安全的条件下, Alice 对标记为 T 的粒子序列逐一利用幺正操作进行编码, 并将编码后的粒子返回给 Bob. Bob 纠缠粒子对进行 Bell 态测量, 读出 Alice 的信息.

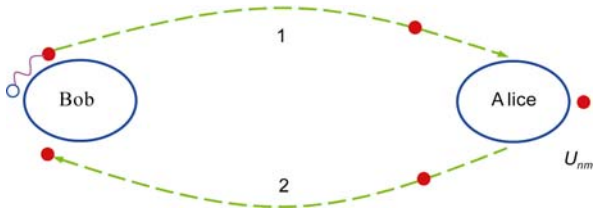

图 2 超密集编码量子安全直接通信方案

Figure 2 Superdense coding QSDC protocol.

在一定的损耗信道中, 高维两步量子安全直接通信方案进一步省略了纠缠转移的步骤, 即不需要借助纠缠转移来判断光子是否存在, 这并不影响光子损耗对通信安全的威胁. 这是一个比两步方案还要好的特点. 另外, 类似于两步方案, 在高维两步量子安全直接通信方案中, 通信双方也可以通过高维系统的纠缠纯化来进行量子机密放大和纠缠保真度的提高, 降低信道噪声对通信安全的影响.

5 多步方案

随着对量子纠缠源的深入研究, 三粒子最大纠缠态(Greenberger-Horne-Zeilinger 态, 简称为 GHZ 态)也被用于量子安全直接通信的研究中[15]. 三粒子 GHZ 态的形式可以写成

$$|\varphi\rangle_{ABC}=\sqrt{\frac{1}{2}}\left(|000\rangle_{ABC}+|111\rangle_{ABC}\right). \quad (8)$$

对于三粒子 GHZ 态中的两个粒子进行单比特的幺正操作 U_i (i=0,1,2,3), 可以将这一量子态变换成以下的任意一个:

$$|\varphi\rangle_0=\sqrt{\frac{1}{2}}\left(|000\rangle_{ABC}+|111\rangle_{ABC}\right), \quad (9)$$

$$|\varphi\rangle_1=\sqrt{\frac{1}{2}}\left(|000\rangle_{ABC}-|111\rangle_{ABC}\right), \quad (10)$$

$$|\varphi\rangle_2=\sqrt{\frac{1}{2}}\left(|100\rangle_{ABC}+|011\rangle_{ABC}\right), \quad (11)$$

$$|\varphi\rangle_3=\sqrt{\frac{1}{2}}\left(|100\rangle_{ABC}-|011\rangle_{ABC}\right), \quad (12)$$

$$|\varphi\rangle_4=\sqrt{\frac{1}{2}}\left(|010\rangle_{ABC}+|101\rangle_{ABC}\right), \quad (13)$$

$$|\varphi\rangle_5=\sqrt{\frac{1}{2}}\left(|010\rangle_{ABC}-|101\rangle_{ABC}\right), \quad (14)$$

$$|\varphi\rangle_6=\sqrt{\frac{1}{2}}\left(|110\rangle_{ABC}+|001\rangle_{ABC}\right), \quad (15)$$

$$|\varphi\rangle_7=\sqrt{\frac{1}{2}}\left(|110\rangle_{ABC}-|001\rangle_{ABC}\right). \quad (16)$$

在通信中, 双方事先约定每一个三粒子纠缠态对应一个三比特经典信息. 由发送者制备同一个 GHZ 态, 这样通信双方可以通过类似于两步量子安全直接通信方案的传输方法, 将每组纠缠态中的粒子组成三个粒子序列, 分三步将三个粒子序列从发送者传输到接收者. 在保证信道安全的前提下, 接收者对三粒子态进行测量, 可以确定的得到态的信息, 从而得到发送者需要传递的秘密信息, 完成量子安全直接通信过程.

6 量子一次便笺方案

以上的量子安全直接方案采用的信息载体是纠缠的光子系统. 单光子是量子通信应用的理想的信息载体之一, 且已经得到了较为广泛的应用. 在量子信道中, 单光子虽然会受到环境的干扰, 克制这种干扰比克制环境对纠缠量子体系的退相干作用要容易. 另外, 在实验上, 单光子测量要比纠缠态的测量容易得多. 因此, 利用单光子作为量子信号来进行量子安全直接通信, 在实验上也更容易实现, 更具有应用前景. 借助于经典密码学中的一次一密方案, 邓富国和龙桂鲁提出了一个基于单光子量子态的一次一密量子安全直接通信方案[10], 也称为量子一次便笺方案. 如果能在通信双方 Alice 和 Bob 之间安全地共享一串量子态, 那么 Alice 就可以在量子态上加载机密信息. 如果对 Eve 而言量子态是完全随机的, 那么这样的机密信息加载从原理上讲具有与一次一密一样的安全性, 即绝对安全.这一方案不需要制备和测量纠缠光子对, 只需要单光子源即可完成量子安全直接通信, 在实验上更容易实现.

一次一密量子安全直接通信方案的原理如图 3 所示. 图 3 中的 SR 表示量子态存储器(或光学延迟装置), CE 表示安全检测过程, Switch 是控制开关, 由 CM, M1, M2 组成的装置完成机密信息加载与量子信号返回量子信道的功能.

方案的具体步骤如下: 首先由 Bob 制备一系列偏振单光子态 S 并将这些光子发送给 Alice. 每个单光子随机地处在 $|H\rangle$ $|V\rangle$ $|L\rangle$ 或 $|R\rangle$. 它们分别是测量基 $\oplus$ 和 $\otimes$ 的本征态,

$$|H\rangle = |0\rangle,$$

$$|V\rangle = |1\rangle,$$

$$|L\rangle = \sqrt{\frac{1}{2}}\left(|0\rangle + |1\rangle\right),$$

$$|R\rangle = \sqrt{\frac{1}{2}}\left(|0\rangle - |1\rangle\right).$$

在接收到光子序列 S 以后, Alice 和 Bob 采用类似于两步安全直接通信的方法检测通信的安全性: Alice 随机地在 S 序列中选择一部分光子作为抽样分析的样品光子, 并告知 Bob 抽样光子的位置. Bob 通过公开信道告诉 Alice 他制备光子时的量子态, Alice 选择对应的测量基测量样品光子, 并分析出错率. 如果通信双方 Alice 和 Bob 能够确定在 S 光子序列传输过程中没有人监听量子信道, 那么他们就共享了一串量子态, 并继续第二步通信, 否则传输中止. 第二步通信过程开始后, Alice 对 S 序列中剩余的光子依次编码信息: 根据需要编码的经典信息是 0 或者 1 选择幺正操作 $U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$ 或者 $U_3 = -\mathrm{i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ 作用到单光子态上. 在编码操作完成以后, Alice 将这些单光子发送给 Bob. Bob 根据原有的制备基信息可以通过相同的测量装置直接读出这些单光子的状态, 从而得到 Alice 传输的经典信息. 为了确

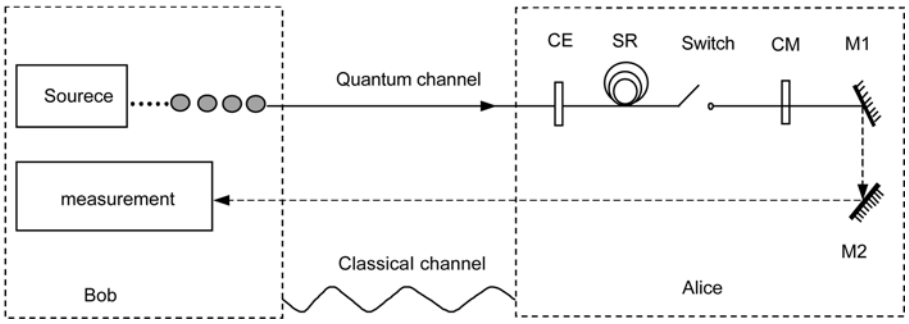

图 3 量子一次一密安全直接通信的原理图

Figure 3 Principle of quantum one time pad QSDC protocol.

保整个通信过程的安全, Alice 在编码队列中随机地选择部分单光子进行安全性检测. Alice 对这些检测单光子随机地选择 U_0 和 U_3 进行操作来加载检测信息. 在 Bob 测量这些光子队列之后, Alice 公布这些检测单光子的位置和所进行的操作. 这样, 尽管这些用于安全检测的单光子无法阻止窃听者对信道的窃听, 但是可以帮助合法的通信者确定窃听者的存在, 并且这样的通信过程使得窃听者无法获得有效的信息.

特别需要强调的地方是, 为了能让 Bob 准确地得到 Alice 加载到光子上的机密信息, Alice 对共享的光子序列 S 的编码不宜改变测量基信息, 详细原理参考文献[10]. 因而 Alice 可以选择两个不改变测量基信息的量子幺正操作 I 和 σ_y 来完成对光子序列的信息编码, 然后将光子序列 S 发回给 Bob, 由他做单光子测量来读出 Alice 的编码信息. 这两个幺正操作可以分别代表编码 0 和 1, 从而与经典的机密信息一一对应.

在一定噪声环境下, 一组单光子极化状态也可以进行量子机密放大处理[34,35], 从而降低噪声对通信安全的影响.

7 量子安全直接通信网络方案

量子安全直接通信的网络化问题也是一个研究热点. 一个安全可靠的量子安全直接通信网络需要可以制备和测量量子信号的服务器. 利用服务器, 在合法的通信者之间进行量子安全直接通信需要防止服务器获得通信方的秘密信息. 基于以上考虑, 邓富国等人[36]将高效方案推广到网络结构.

李熙涵等人[37]提出了一个基于两步量子安全直接通信方案的量子安全直接通信网络模型. 在这个网络协议中, 通信者利用纠缠粒子对进行量子直接通信, 网络组成包括服务器、发送者和接收者三个部分. 在图 4 中给出了这个协议的环状拓扑结构模型.

在通信开始前, 三方事先约定利用幺正操作 $\{U_0,U_1,U_2,U_3\}$ 加载经典信息. 服务器 Alice 一次制备 N 个 Bell 态, 这些态的形式为: $|\psi^+\rangle_{CM}=\sqrt{1/2}(|10\rangle_{CM}+|01\rangle_{CM})$. 她将每个 Bell 态的两个粒子拆开, 第一个粒子组成序列 S_C, 第二个粒子组成序列 S_M. 然后 Alice 采用两步传输的方法将这两个序列发送给 Bob. Bob 将序列 S_C 中的一部分光子替换掉, 所选用的替换光子是他自己制备的单光子. 这些粒子为诱骗光子[38~40]. 诱骗光子被随机地制备在 $|H\rangle,|V\rangle,|L\rangle$ 或 $|R\rangle$ 中的任意一个态上, 然后 Bob 将 S_C 序列发送给 Charlie. 在 Charlie 确认接收到 S_C 光子序列之后, Bob 和 Charlie 检查诱骗光子的状态来确定传输的安全性. 检测过程为 Charlie 随机地选择测量基对诱骗光子进行测量, 而后公布测量基和测量结果. 对于选择了相同测量基的诱骗光子, Bob 和 Charlie 比对他们的结果, 从而分析用于安全检测的粒子的误码率. 如果误码率低于阈值, 那么他们确定信道安全, Bob 将他的信息通过幺正操作编码到 S_M 序列中, 并发送给 Charlie. 在 Charlie 接收到这些光子序列并联合 Bob 完成安全性检测以后, 他可以通过同样的编码方法选择对 S_M 序列中的光子进行信息加密. 这些光子最终全部发送给 Alice, 由 Alice 完成测量并公布测量结果. 这样 Charlie 根据公开的信息就可以读出 Bob 的编码信息, 从而完成这个网络通信过程.

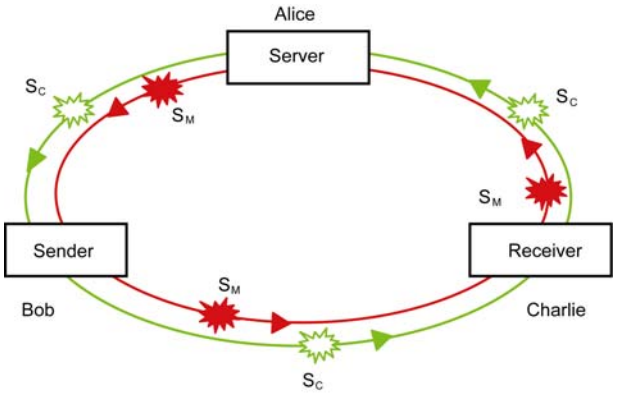

图 4 两步量子安全直接通信网络

Figure 4 Quantum Network based on two-step protocol.

同年, 邓富国等人[29]提出了一个双向量子安全直接通信的网络方案, 方案的模型如图 5 所示.

信息的发送者 Alice 制备一组 N 个 Bell 纠缠态作为信息的载体, 初始状态为 $|\psi^-\rangle_{BC}=\sqrt{1/2}(|01\rangle_{BC}$

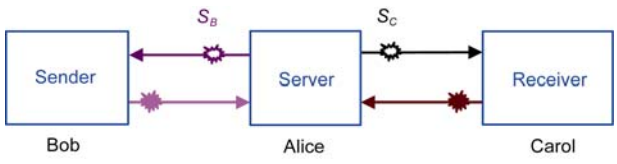

图 5 双向量子安全直接通信网络模型

Figure 5 Bidirectional QSDC Network.

$-|10\rangle_{BC}$), 对于每一个态中的两个光子, 都被分开, 分别组成两个队列 S_B 和 S_C. 这两个队列分别发送给网络用户 Bob 和 Carol. 在双方都接收到光子对序列之后, Bob 和 Carol 在序列中选择一部分光子作为安全检测粒子, 随机地选择测量基进行安全性检测来确定传输的安全性. 在保证安全的前提下, Bob 和 Carol 选择泡利矩阵 $\{U_0,U_1,U_2,U_3\}$ 进行编码操作. 在编码后的粒子序列中, Bob 再次选择部分粒子用于安全性检测, 然后他们将所有粒子发送给 Alice. Alice 作为服务器一方, 对粒子进行 Bell 态测量并公布测量结果. Bob 和 Carol 可以通过第二次选择的安全检测粒子来判断是否存在窃听. 如果通信是安全的, 那么 Carol 可以通过 Alice 公布的结果推出 Bob 所进行的编码操作, 从而得到 Bob 的信息.

最近量子安全直接通信网络的研究引起了人们的广泛关注. 随着量子安全直接通信技术研究的深入, 量子安全直接通信网络的实验研究也逐渐得到重视.

8 结论

相比经典的通信技术, 量子通信由于其安全性高而受到越来越多的关注. 在量子通信中, 任何对于信号的窃听行为都会被发现, 从而保证了通信的安全性. 量子通信的安全性的关键是可以利用量子力学的原理探测窃听者, 从而知道信息是否泄漏. 在量子通信中, 存在 ILBED 问题. 在量子密钥分发中, 在通信结束时根据抽样测量的结果可以确认通信之中是否存在泄漏. 由于加载在载体上的是随机密钥, 在发现信道被窃听之后, 可以放弃通信结果从而避免了 ILBED, 不会对通信安全产生影响. 在 DQSC 中, 可以在通信结束的时候, 通过抽样检测发现窃听行为, 如果发现窃听, 可以通过停止发送经典密钥而阻止 ILBED.

对于量子安全直接通信过程来说, 信号的丢失意味着信息的泄露, 所以必须采取更安全的方式进行信息传输. 量子安全直接通信在方案设计的过程中通过安全性检测可以避免信号丢失而造成的信息泄露, 因而可以提供安全的信息直接传输. 在量子安全直接通信中, 可以利用纠缠量子体系或者单光子量子体系进行通信. 在 QSDC 中, 由于使用了块传输和分步传输的方法, 在确认了量子信道后, 才将整个量子载体发送, 或者进行编码操作, 从而避免了 ILBED. 实现 QSDC 的关键是块传输, 因此量子存储器是实现 QSDC 的关键量子器件之一. 简单的量子存储器是光纤延迟线, 目前的技术已经可以实现.

本文我们介绍了量子安全直接通信的原理和几个常见方案. 量子安全直接通信技术因其不同于量子密钥分发的相对简单的通信步骤而逐渐受到关注. 近年来, 人们开始关注噪声情况下的量子直接安全通信方案的研究[27], 如何进行长距离 QSDC[41], 如何进行量子态的秘密放大[34], 量子纠错[42]. 最近量子态秘密方法已经在实验上进行了原理演示[35]. 高维方案[14]得到实验研究组的关注[43~45], 利用更多自由度产生的高维度超纠缠量子态可以用于高维量子安全直接通信. 随着量子通信实验研究的发展, 量子安全直接通信的实验研究、实用化研究是这一研究方向中的重要课题.

参考文献

1 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, System and Signal Processing. Bangalore, India: IEEE, 1984. 175–79

2 Bennett C H. Quantum cryptography using any two nonorthgonal states. Phys Rev Lett, 1992, 68: 3121–3124

3 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67: 661–663

4 Bennett C H, Brassard G, Mermin N D. Quantum cryptography without Bell's theorem. Phys Rev Lett, 1992, 68: 557–669

5 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002, 65: 032302

6 Beige A, Englert B G, Kurtsiefer C, et al. Secure communication with a publicly known key. Acta Phys Pol A, 2002, 101(6): 357–368

7 Beige A, Englert B G, Kurtsiefer C, et al. Secure communication with single-photon two-qubit states. J Phys A-Math Gen, 2002, 35: L407–L413

8 Boström K, Felbinger T. Deterministic secure direct communication using entanglement. Phys Rev Lett, 2002, 89(18): 187902
9 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(4): 042317
10 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69(5): 052319
11 Lucamarini M, Mancini S. Secure deterministic communication without entanglement. Phys Rev Lett, 2005, 94(14): 140501
12 Cai Q Y, Li B W. Deterministic secure communication without using entanglement. Chin Phys Lett, 2004, 21(4): 601–603
13 Yan F L, Zhang X Q. A scheme for secure direct communication using EPR pairs and teleportation. Eur Phys J B, 2004, 41: 75–78
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 Wang C, Deng F G, Long G L. Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. Opt Commun, 2005, 253: 15–20
16 Man Z X, Zhang Z J, Li Y. Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations. Chin Phys Lett, 2005, 22(1): 18–21
17 Zhu A D, Xia Y, Fang Q B, et al. Secure direct communication based on secret transmitting order of particles. Phys Rev A, 2006, 73(2): 022338
18 Li X H, Li C Y, Deng F G, et al. Quantum secure direct communication with quantum encryption based on pure entangled states. Chin Phys, 2007, 16(8): 2149–2153
19 Li X H, Deng F G. Li C Y, et al. Deterministic secure quantum communication without maximally entangled states. J Korean Phys Soc, 2006, 49(4): 1354–1359
20 Cao H J, Song H S. Quantum secure direct communication with W state. Chin Phys Lett, 2006, 23(2): 290–292
21 Wang J, Zhang Q, Tang C J. Multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. Opt Commun, 2006, 266(2): 732–737
22 Cai Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys Lett A, 2006, 351(1-2): 23–25
23 Deng F G, Li X H, Li C Y, et al. Eavesdropping on the 'ping-pong' quantum communication protocol freely in a noise channel. Chin Phys, 2007, 16(2): 277–281
24 Li X H, Deng F G, Zhou H Y. Improving the security of secure direct communication based on the secret transmitting order of particles. Phys Rev A, 2006, 74(5): 054302
25 Yang Y G, Wen Q Y, Zhu F C. An efficient quantum secure direct communication scheme with authentication. Chin Phys, 2007, 16(7): 1838–1842
26 Gao F, Wen Q Y, Zhu F C. Teleportation attack on the QSDC protocol with a random basis and order. Chin Phys B, 2008, 17(9): 3189–3193
27 Gu B, Pei S X, Song B, et al. Deterministic secure quantum communication over a collective-noise channel. Sci China Ser G-Phys Mech Astron, 2009, 52(12): 1913–1918
28 Long G L, Deng F G, Wang C, et al. Quantum secure direct communication and deterministic secure quantum communication. Front Phys China, 2007, 2(3): 251–272
29 Deng F G, Li X H, Li C Y, et al. Quantum secure direct communication network with Einstein-Podolsky-Rosen pairs. Phys Lett A, 2006, 359: 359–365
30 Long G L, Wang C, Deng F G, et al. Quantum Direct Communication, Advances in Lasers and Electro Optics. Nelson Costa, Adolfo Cartaxo, Eds. INTECH, 2010
31 Horodecki R, Horodecki P, Horodecki M, et al. Quantum entanglement. Rev Mod Phys, 2009, 81: 865–942
32 Bovino F A, Degiovanni I P. Quantum correlation bounds for optimization of quantum-information experiments: The Wigner inequality case. Phys Rev A, 2008, 77: 052110
33 Deng F G, Long G L. Controlled order rearrangement encryption for quantum key distribution. Phys Rev A, 2003, 68: 042315
34 Deng F G, Long G L. Quantum privacy amplification for a sequence of single qubits. Commun Theor Phys, 2006, 46(3): 443–446
35 Hao L, Wang C, Long G L. Realization of quantum state privacy amplification in a nuclear magnetic resonance quantum system. J Phys B-At Mol Opt Phys, 2010, 43: 125502
36 Deng F G, Liu X S, Ma Y J, et al. A theoretical scheme for multiuser quantum key distribution with N Einstein- Podolsky- Rosen Pairs in a passive optical network. Chin Phys Lett, 2002, 19: 893–896

37 Li X H, Zhou P, Liang Y J, et al. Quantum secure direct communication network with two-step protocol. Chin Phys Lett, 2006, 23: 1080–1083
38 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(5): 1049–1052
39 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(11): 2896–2899
40 Deng F G, Li X H, Li C Y, et al. Quantum secure direct communication network with superdense coding and decoy photons. Phys Scr, 2007, 76: 25–30
41 Wang W Y, Wang C, Zhang G Y, et al. Arbitrarily long distance quantum communication using inspection and power insertion. Chin Sci Bull, 2009, 54(1): 158–162
42 Wen K, Long G L. One-party quantum error correcting codes or unbalanced errors: Principles and application to quantum dense coding and quantum secure direct communication. Int J Quantum Info, 2010, 8(4): 697–719
43 Barreiro J T, Langford N K, Peters N A, et al. Generation of hyperentangled photon pairs. Phys Rev Lett, 2005, 95: 260501
44 Ramelow S, Ratschbacher L, Fedrizzi A, et al. Discrete tunable color entanglement. Phys Rev Lett, 2009, 103: 253601
45 Yan H, Zhang S C, Chen J F, et al. Generation of narrow-band hyperentangled nondegenerate paired photons. Phys Rev Lett, 2011, 106: 033601

Quantum secure direct communication

LONG GuiLu[1*], WANG Chuan[1], LI YanSong[1] & DENG FuoGuo[2]

[1] *Key Laboratory of Atomic and Molecular Nanosciences and Department of Physics, Tsinghua University, Beijing 100084, China;*
[2] *Department of Physics, Beijing Normal University, Beijing 100875, China*

Quantum communication exploits the principles of quantum mechanics in the transmision and processing of information. It has the advantages of high security and high capacity. Quantum secure direct communication (QSDC) is a new mode of quantum coomunication by Long and Liu in which secret information can be transmitted securely and directly over quantum channels. Since it was first proposed in 2000, QSDC has been developed very fast. In this review, we will explain the basic principles of QSDC and describe some typical QSDC protocols. Toward the end of the review, we will introduce the new trends in the QSDC research and give a perspectiv of QSDC research.

quantum secure direct communication, QSDC, quantum communication, two-step QSDC protocol, efficient QSDC protocol, quantum one-time-pad QSDC protocol, QSDC network

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

doi: 10.1360/132011-178