doi:10.3788/gzxb20124104.0501

受第三方控制的量子安全对话方案

邹昕，叶志清

（江西师范大学 物理与通信电子学院；江西省光电子与通信重点实验室，南昌 330022）

摘　要：通过量子隐形传态只能单向传递信息，从某种意义上说，并不是真正的“通信”，本文提出一个由第三方控制的量子双向通信方案：通信双方经过幺正变换实现信息编码，然后分别对自己拥有的粒子进行贝尔基联合测量，公布测量结果，在控制方同意的情况下，实现量子安全对话，而控制方并不知道对话内容. 由于控制方的加入，大大增强了量子对话的安全性，使得这一方案更趋完美. 通过量子信道实现了经典信息的安全双向通信，它在未来量子安全对话、量子保密通信的实际应用中能起到重要的参考作用.

关键词：量子对话；幺正变换；Bell 基联合测量；安全性

中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1004-4213(2012)04-0501-4

0 引言

量子通信(Quantum Communication)是指利用量子纠缠效应传递信息的一种新型的通讯方式. 量子通信是近二十年发展起来的新型交叉学科，是量子论和信息论相结合的新的研究领域. 量子通信主要涉及：量子密码通信、量子远程传态和量子密集编码等，基于量子力学的基本原理，如未知量子态不可克隆、非正交量子态不可识别、量子态测量无法不扰动系统状态等[1]，量子通信具有高效率和绝对安全等特点，因此成为国际上量子物理和信息科学的研究热点. 自 1984 年第一个 BB84 量子密钥分发协议(Quantum Key Distribution，QKD)[2-6] 以及 1993 年量子态隐形传输方案[7-10] 提出以来，量子通信在理论研究和实践应用方面都取得了重大突破，如实现安全量子通信距离超过百公里量级、成功实现长距离量子通信中的量子中继器以及成功实现具有存储和读出功能的纠缠交换[11-12]. 高效安全的信息传输日益受到人们的关注.

本文提出受第三方控制的量子安全对话方案，是相对于单向量子通信，如量子隐形传态、量子直接通信而言又进了一步. 为实现双向通信，通信双方需将经典信息通过幺正变换实现信息编码，然后分别对自己拥有的粒子作 Bell 基联合测量(Bell State Measurement，BSM)，并公布测量结果. 若控制方同意通信双方进行量子对话(Quantum Dialogue)，只要对自己拥有的粒子作单粒子态测量，并公布测量结果，就可以完成双向通信，实现量子安全对话. 由于控制方的加入，大大增强了量子对话的安全性，使得这一方案更具有实际应用价值.

1 受第三方控制实现安全的量子双向通信方案

通信之前先秘密建立三方量子信道，如图 1，其中通信方之一 Alice 拥有粒子 A_1、A_2，另一通信方 Bob 拥有粒子 B_1、B_2，控制方 Charlie 拥有粒子 C_1、C_2. 假设三对粒子的纠缠态分别为 $|\phi^+\rangle_{A_1C_1}=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$、$|\phi^-\rangle_{C_2B_1}=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)$、$|\varphi^+\rangle_{B_2A_2}=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)$. 通信双方事先约定编码方式通过幺正变换实现.

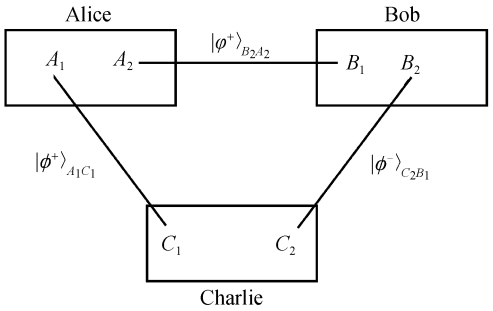

图 1　量子信道的构建

Fig. 1　Construction of quantum channel

基金项目：国家自然科学基金(No. 60967002)、江西省教育厅科研项目(No. GJJ10401)和江西省自然科学基金(No. 20114BAB202003)资助

第一作者：邹昕(1988－)，男，硕士研究生，主要研究方向为光量子通信 Email：zouxin-88@163.com

责任作者/导师(通讯作者)：叶志清(1960－)，男，教授，主要研究方向为光纤光栅传感器、光量子通信. Email：yezhiqing2008@163.com

收稿日期：2011-11-01；**修回日期**：2012-01-18

假设 Alice 想把两比特经典信息“10”传送给 Bob，则她对自己的粒子 A_1 作幺正变换$(\sigma^{(2)})_{A_1}$，即将经典信息编码进量子纠缠态中，则有$(\sigma_x)_{A_1}|\phi^+\rangle_{A_1C_1}\rightarrow|\varphi^+\rangle_{A_1C_1}$，其中 $\sigma^{(i)}\{i=0,1,2,3\}$与各经典信息的对应关系如表 1 所示. 接着，Alice 对自己拥有的粒子 A_1、A_2 作 Bell 基联合测量，得到的测量结果有4种：$|\phi^\pm\rangle_{A_1A_2}=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle)$，$|\varphi^\pm\rangle_{A_1A_2}=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle)$且几率均为 1/4. 假设 Alice 的测量结果为$|\phi^+\rangle_{A_1A_2}$，则子系统塌缩为$|\phi^+\rangle_{C_1B_2}$，然后 Alice 将自己测量结果只告诉 Bob，而对子系统塌缩态保密.

表 1 $\sigma^{(i)}\{i=0,1,2,3\}$及其对应矩阵、对应经典信息

Table 1 $\sigma^{(i)}\{i=0,1,2,3\}$ corresponding matrix, corresponding classic information

$\sigma^{(i)}$	Corresponding matrix	Corresponding classic information
$\sigma^{(0)}$	I	00
$\sigma^{(1)}$	σ_z	01
$\sigma^{(2)}$	σ_x	10
$\sigma^{(3)}$	$\sigma_x\sigma_z$	11

同样的，假设 Bob 想把两比特经典信息“01”传送给 Alice，则他先对自己拥有的粒子 B_1 作幺正变换$(\sigma^{(1)})_{B_1}$，则有$(\sigma_z)_{B_1}|\phi^-\rangle_{C_2B_1}\rightarrow|\phi^+\rangle_{C_2B_1}$，然后对粒子 B_1、B_2 进行一次 Bell 基联合测量，得到的测量结果有4种：$|\phi^\pm\rangle_{B_1B_2}=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle)$，$|\varphi^\pm\rangle_{B_1B_2}=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle)$，且几率均为 1/4. 然后 Bob 把自己的测量结果告诉 Alice.

若控制方 Charlie 同意 Alice 和 Bob 双方进行量子对话，则对自己拥有的粒子 C_1、C_2 作单粒子态测量，得到的测量结果有4种：$|\phi^\pm\rangle_{C_1C_2}=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle)$，$|\varphi^\pm\rangle_{C_1C_2}=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle)$，且几率均为 1/4. 然后公开测量结果.

Bob 和 Alice 是如何根据对方以及 Charlie 公布的测量结果推算对方所传的信息. 首先，Bob 根据 Charlie 公布的测量结果和自己对 B_1 粒子所作的幺正变换才能推知 Alice 测量后子系统塌缩态(见表 2). 而窃听者 Eve 即使从公开信道中获取 Alice、Bob 和 Charlie 公布的测量结果也不能推出 C_1、B_2 粒子的塌缩态. 假设粒子 C_1、B_2 的塌缩态为$(\sigma_m)_{C_1}|\phi^+\rangle_{C_1B_2}$则 Bob 子系统态为

表 2 Alice Bob Charlie 公布测量结果以及 Bob 推知 C_1B_2 塌缩态

Table 2 Alice Bob Charlie announce measured results and deduce C_1B_2 collapsed states

Alice′s measured results	Bob′s measured results	Charlie′s measured results	Bob′s deduced C_1B_2 collapsed states
$\|\phi^+\rangle_{A_1A_2}$	$\|\phi^+\rangle_{B_1B_2}$	$\|\phi^+\rangle_{C_1C_2}$	$\|\phi^+\rangle_{C_1B_2}$
$\|\phi^-\rangle_{A_1A_2}$	$\|\phi^-\rangle_{B_1B_2}$	$\|\phi^-\rangle_{C_1C_2}$	$\|\phi^-\rangle_{C_1B_2}$
$\|\varphi^+\rangle_{A_1A_2}$	$\|\varphi^+\rangle_{B_1B_2}$	$\|\varphi^+\rangle_{C_1C_2}$	$\|\varphi^+\rangle_{C_1B_2}$
$\|\varphi^-\rangle_{A_1A_2}$	$\|\varphi^-\rangle_{B_1B_2}$	$\|\varphi^-\rangle_{C_1C_2}$	$\|\varphi^-\rangle_{C_1B_2}$

$$|\psi^s\rangle_{\text{Bob}}=(\sigma_m)_{C_1}|\phi^+\rangle_{C_1B_2}\otimes|\phi^+\rangle_{C_2B_1}=\frac{1}{2}(\sigma_m)_{C_1}\cdot(|\phi^+\rangle_{C_1C_2}\otimes|\phi^+\rangle_{B_1B_2}+|\phi^-\rangle_{C_1C_2}\otimes|\phi^-\rangle_{B_1B_2}+|\varphi^+\rangle_{C_1C_2}\otimes|\varphi^+\rangle_{B_1B_2}+|\varphi^-\rangle_{C_1C_2}\otimes|\varphi^-\rangle_{B_1B_2})\quad(1)$$

Bob 根据 Charlie 公布的自测结果$|\phi^+\rangle_{C_1C_2}$和自己对应的测量结果$|\phi^+\rangle_{B_1B_2}$，可知$(\sigma_m)_{C_1}|\phi^+\rangle_{C_1C_2}=|\phi^+\rangle_{C_1C_2}$，得$(\sigma_m)_{C_1}=(\sigma^{(0)})_{C_1}=(I)_{C_1}$，由此 Bob 可推出：$(\sigma_m)_{C_1}|\phi^+\rangle_{C_1B_2}=|\phi^+\rangle_{C_1B_2}$. 其次，Bob 假设 Alice 所作幺正变换为 $\sigma^{\text{a}}_{A_1}$，加上 Bob 知道事先秘密共享的量子信道，则可以写出 Alice 子系综态为

$$|\psi^s\rangle_{\text{Alice}}=\sigma^{\text{a}}_{A_1}|\phi^+\rangle_{A_1C_1}\otimes|\varphi^+\rangle_{B_2A_2}=\frac{\sigma^{\text{a}}_{A_1}}{2}(|\phi^+\rangle_{A_1A_2}\otimes|\varphi^+\rangle_{C_1B_2}+|\phi^-\rangle_{A_1A_2}\otimes|\varphi^-\rangle_{C_1B_2}+|\varphi^+\rangle_{A_1A_2}\otimes|\phi^+\rangle_{C_1B_2}+|\varphi^-\rangle_{A_1A_2}\otimes|\phi^-\rangle_{C_1B_2})\quad(2)$$

根据 Alice 告诉的测量结果$|\phi^+\rangle_{A_1A_2}$，即可推知 Alice 所作的幺正变换为

$$\sigma^{\text{a}}_{A_1}|\varphi^+\rangle_{A_1A_2}=|\phi^+\rangle_{A_1A_2}\quad\sigma^{\text{a}}_{A_1}=\sigma_x\quad(3)$$

故得知其要传递的经典信息为“10”. 同理，Alice 若要推算 Bob 要传递的经典信息，首先应假设 Bob 对粒子 B_1 所作的幺正变换 $\sigma^{\text{b}}_{B_1}|\phi^-\rangle_{C_2B_1}$ 以及 Alice 没有公开的 C_1、B_2 塌缩态，才可写出 Bob 子系综态为

$$|\psi^s\rangle_{\text{Bob}}=\sigma^{\text{b}}_{B_1}|\phi^-\rangle_{C_2B_1}\otimes|\phi^+\rangle_{C_1B_2}=\frac{1}{2}\sigma^{\text{b}}_{B_1}(|\phi^-\rangle_{C_1C_2}\otimes|\phi^+\rangle_{B_1B_2}+|\phi^+\rangle_{C_1C_2}\otimes|\phi^-\rangle_{B_1B_2}+|\varphi^-\rangle_{C_1C_2}\otimes|\varphi^+\rangle_{B_1B_2}+|\varphi^+\rangle_{C_1C_2}\otimes|\varphi^-\rangle_{B_1B_2})\quad(4)$$

由 Charlie 公布的测量结果$|\phi^+\rangle_{C_1C_2}$和 Bob 告诉的测量结果为$|\phi^+\rangle_{B_1B_2}$得

$$\sigma^{\text{b}}_{B_1}|\phi^-\rangle_{B_1B_2}=|\phi^+\rangle_{B_1B_2}\quad\sigma^{\text{b}}_{B_1}=\sigma_z\quad(5)$$

故得知 Bob 要传送的秘密信息为“01”. 至此，双方只对自己拥有的粒子做幺正变换和 BSM 就实现了量子安全对话.

2 安全性分析

该方案中，若不加第三方控制也可完成双向通信，即基于量子安全直接通信(Quantum Secure

Direct Communication，QSDC）协议的所谓量子对话[13]. 在这种协议里，秘密消息可以沿着正反两个方向同时传输，即 Alice 到 Bob 和 Bob 到 Alice. 本文不致力于寻找巧妙的攻击策略，而是从一个不同的角度来分析量子对话的安全性，即信息泄露[14]. 也就是说，该协议中传输的信息将会被部分地泄露出去，窃听者不需要进行任何主动攻击，仅从合法通信者的公开声明中就能提取到部分秘密信息，因此，窃听者不会被任何检测窃听过程发现，这无疑会给量子安全通信带来威胁. 以一种量子对话协议为例，Alice、Bob 秘密共享 2 个 EPR（Einstein-Podolsky-Rosen）对 $|\phi^+\rangle_{A_1B_1}=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$、$|\phi^-\rangle_{A_2B_2}=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)$ 作为信息载体，Alice 拥有粒子 A_1、A_2，Bob 拥有粒子 B_1、B_2. 假设 Alice 想把两比特经典信息传送给 Bob，由表 1 知，他需对自己拥有的其中一个粒子作一种幺正变换来完成编码；同理，Bob 也可用相同的方式对自己拥有的其中一个粒子进行编码，然后 Alice 对自己的两个粒子进行 BSM，并公布测量结果；Bob 对自己的粒子作单粒子态测量，并公布自己粒子所处的纠缠态. 通信双方根据对方公布的测量结果，就能推断出对方想要传送的经典信息. 举例来说，Alice 对粒子 A_1 作幺正变换 σ_x，则有 $(\sigma_x)_{A_1}|\phi^+\rangle_{A_1B_1}\rightarrow|\varphi^+\rangle_{A_1B_1}$；然后 Bob 对粒子 B_2 作幺正变换 σ_z，有 $(\sigma_z)_{B_2}|\phi^-\rangle_{A_2B_2}\rightarrow|\phi^+\rangle_{A_2B_2}$. 接着，Alice 对粒子 A_1、A_2 作 BSM，并将测量结果告诉 Bob，此时量子系统的系综态为

$$|\psi^s\rangle=|\varphi^+\rangle_{A_1B_1}\otimes|\phi^+\rangle_{A_2B_2}=\frac{1}{2}(|\varphi^+\rangle_{A_1A_2}\otimes|\phi^+\rangle_{B_1B_2}-|\varphi^-\rangle_{A_1A_2}\otimes|\phi^-\rangle_{B_1B_2}+|\phi^+\rangle_{A_1A_2}\otimes|\varphi^+\rangle_{B_1B_2}-|\phi^-\rangle_{A_1A_2}\otimes|\varphi^-\rangle_{B_1B_2}) \tag{6}$$

Alice 假设 Bob 所作的编码操作为 $\sigma^i_{B_2}$，则有子系统态

$$|\psi^s\rangle_1=|\varphi^+\rangle_{A_1B_1}\otimes(\sigma^i_{B_2}|\phi^-\rangle_{A_2B_2})=\frac{1}{2}\sigma^i_{B_2}(-|\varphi^-\rangle_{A_1A_2}\otimes|\phi^+\rangle_{B_1B_2}+|\varphi^+\rangle_{A_1A_2}\otimes|\phi^-\rangle_{B_1B_2}+|\phi^-\rangle_{A_1A_2}\otimes|\varphi^+\rangle_{B_1B_2}-|\phi^+\rangle_{A_1A_2}\otimes|\varphi^-\rangle_{B_1B_2}) \tag{7}$$

Alice 将测量结果 $|\phi^+\rangle_{A_1A_2}$ 告诉 Bob，并根据 Bob 告诉的自测结果（这里假设为 $|\varphi^+\rangle_{B_1B_2}$），可知 $\sigma^i_{B_2}|\varphi^-\rangle_{B_1B_2}=|\varphi^+\rangle_{B_1B_2}$，$\sigma^i_{B_2}=\sigma_z$，由表 1 知 Bob 想要传递的经典信息为“01”；同理，Bob 假设 Alice 所作的编码操作为 $\sigma^j_{A_1}$，则有子系统态

$$|\psi^s\rangle_2=|\phi^+\rangle_{A_2B_2}\otimes(\sigma^j_{A_1}|\phi^+\rangle_{A_1B_1})=\frac{1}{2}\sigma^j_{A_1}(|\phi^+\rangle_{A_1A_2}\otimes|\phi^+\rangle_{B_1B_2}+|\phi^-\rangle_{A_1A_2}\otimes|\phi^-\rangle_{B_1B_2}+|\varphi^+\rangle_{A_1A_2}\otimes|\varphi^+\rangle_{B_1B_2}+|\varphi^-\rangle_{A_1A_2}\otimes|\varphi^-\rangle_{B_1B_2}) \tag{8}$$

Bob 根据自测结果和 Alice 的测量结果 $|\phi^+\rangle_{A_1A_2}$，可知 $\sigma^j_{A_1}|\varphi^+\rangle_{A_1A_2}=|\phi^+\rangle_{A_1A_2}$，$\sigma^j_{A_1}=\sigma_x$，由表 1 知 Alice 想要传递的经典信息为“10”. 但是，通过简单的推导可知，不仅是窃听者 Eve，任何知道这些公开信息，即通信双方测量结果 $|\phi^+\rangle_{A_1A_2}$、$|\varphi^+\rangle_{B_1B_2}$ 的人都可以得到一个结论，那就是 Alice 和 Bob 做完编码操作后，系统的系综态必可以写成 $|\psi^s\rangle=|\varphi^+\rangle_{A_1B_1}\otimes|\phi^+\rangle_{A_2B_2}$ 或 $|\psi^s\rangle=|\varphi^+\rangle_{A_2B_2}\otimes|\phi^+\rangle_{A_1B_1}$ 的形式，而 Alice 和 Bob 的编码操作一定分别为{(σ_x,σ_z)或$(I,\sigma_x\sigma_z)$}这 2 种可能之一，即 Eve 知道 Alice 和 Bob 传输的消息比特定为{(10,01),(00,11)}中的一种，且出现概率相同. 这对 Eve 来说仅包含 $-2\times\frac{1}{2}\log_2\frac{1}{2}=1$ 比特未知信息. 所以，Alice 和 Bob 在该次通信中传输的 4 个经典信息比特中的 3 比特信息在不知不觉中被泄露出去，即在两个 EPR 对所传输的 4 比特经典秘密信息中，只有 1 比特被安全地传送. 当通信双方的测量结果为其他 Bell 态时，这一结论仍然适用. 值得一提的是，虽然 Eve 不能得到任何一个经典信息比特的具体值，但是，在追求无条件安全的量子密码协议中，所有的秘密信息都应该被安全地传送. 当一个协议只能保证部分秘密信息的传输安全时，它就不能被称为一个安全协议. 但是，加入第三方控制后，若没有 Charlie 的同意，即 Charlie 不公布自测结果，Eve 即使知道通信双方公开的信息，也无法准确推算出他们所作的幺正变换；甚至 Eve 知道了三方的测量结果，也同样无法推出通信双方所作的编码；同时控制方 Charlie 也不知道量子对话的内容，这就使双向通信的安全性得到了大幅度提高，使该量子对话方案更具有实用价值.

3　结论

本文提出受第三方控制的量子安全对话方案，是相对于单向量子通信，如量子隐形传态、量子直接通信等而言又进了一步. 即使是保密性好的单向传递信息，从某种意义上说，并不是完美的“通信”，只有通信双方能相互交换信息才能称之为真正意义上的通信. 这里，为实现双向通信，通信双方需将待传的秘密信息通过幺正变换实现编码，然后分别对自己拥有的粒子作 BSM，并且只公布测量结果，在控制方同意的情况下，才能顺利地完成双向通信，实现量子安全对话. 由于控制方的加入，大大增强了量子对话的安全性，使得这一方案更趋完美. 由于该方案

比单向量子通信更进一步，通过量子信道实现了经典信息的安全双向通信，可以预见，它在未来量子安全对话、量子保密通信的实际应用中能起到重要的参考作用.

参考文献

[1] 叶俊. 量子通信中的量子隐形传态技术研究[D]. 武汉：华中科技大学，2007.

[2] BENNETT C H, BRASSARD G, EKERT A K. Quantum cryptography[J]. *Scientific American*, 1992, **267**(4): 26-33.

[3] EKERT A K. Quantum cryptography based on Bell′s theorem [J]. *Physical Review Letters*, 1991, **67**(6): 661-663.

[4] BENNETT C H. Quantum cryptography using any two nonorthogonal states[J]. *Physical Review Letters*, 1992, **68**(21): 3121-3124.

[5] ZHOU Chun-yuan, WU Guang, CHEN Xiu-liang, *et al*. Quantum cryptography communication in 50 kilometer optical fiber[J]. *Science in China ser G Physics, Mechanics & Astronomy*, 2003, **33**(6): 538-543.
周春源，吴光，陈修亮，等. 50 km 光纤中量子保密通信[J]. 中国科学 G 辑：物理学 力学 天文学，2003，**33**(6)：538-543.

[6] WANG Chuan, ZHANG Jing-fu, WANG Ping-xiao. Experiments on quantum cryptography communication in free space[J]. *Science in China ser. G Physics, Mechanics & Astronomy*, 2005, **35**(2): 149-157.
王川，张竞夫，王平晓. 自由空间中量子密码通讯实验[J]. 中国科学 G 辑：物理学 力学 天文学，2005，**35**(2)：149-157.

[7] BENNETT C H, BRASSARD G, CREPEAU C, *et al*. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rcsen channels [J]. *Physical Review Letters*, 1993, **70**(13): 1895-1899.

[8] XIONG Xue-shi, FU Jie, SHEN Ke. Controlled teleportation of an unknown two-particle partly entangted state[J]. *Acta Photonica Sinica*, 2006, **35**(5): 780-782.
熊学士，付洁，沈柯. 二粒子部分纠缠未知态的量子受控传递[J]. 光子学报，2006，**35**(5)：780-782.

[9] 陈晖，祝世雄，朱甫臣. 量子保密通信引论[M]. 北京：北京理工大学出版社，2010：117-118.

[10] CHEN Xia, WANG Fa-qiang, LU Yi-qun, *et al*. A differential phase shift key distribution QKD system combing with efficient BB84 scheme[J]. *Acta Photonica Sinica*, 2008, **37**(5): 1052-1056.
陈霞，王发强，路轶群，等. 结合高效 BB84 协议的差分密钥分发系统[J]. 光子学报，2008，**37**(5)：1052-1056.

[11] ZHAO Zhi, CHEN Yu-ao, ZHANG An-ning, *et al*. Experimental demonstration of five-photon entanglement and open-destination teleportation[J]. *Nature*, 2004, **430**(6995): 54-58.

[12] CHEN Yu-ao, ZHANG An-ning, ZHAO Zhi, *et al*. Exprimental quantum error rejection for quantum communication[J]. *Physical Review Letters*, 2006, **96**(22): 2205-2209.

[13] NGUYEN B A. Quantum dialogue[J]. *Physics Letters A*, 2004, **328**(1): 6-10.

[14] GAO Fei, GUO Feng-zhuo, WEN Qiao-yan, *et al*. Reexamine the security of quantum dialogue and bidirectional quantum direct communication[J]. *Science in China ser. G Physics, Mechanics & Astronomy*, 2008, **38**(5): 477-484.
高飞，郭奋卓，温巧燕，等. 重新审视量子对话和双向量子安全直接通信的安全性[J]. 中国科学 G 辑：物理学 力学 天文学，2008，**38**(5)477-484.

Controlled by a Third Party to Realize Quantum Secure Dialogue

ZOU Xin, YE Zhi-qing

(*School of Physics Electronics Telecommunication; Key Laboratory of Photoelectronics & Telecommunication of Jiangxi Province, Jiangxi Normal University, Nanchang* 330022, *China*)

Abstract: In a sense, quantum teleportation by which information could only be transferred in one-way is not a perfect mode of communication. Thus, a scheme of two-way quantum communication controlled by a third party is proposed. Firstly, both sides of communication need accomplish information encoding through some unitary transformations. Then they should perform Bell-state measurements(BSMs) to their own qubits respectively, and announce the measured results. With the permission of the controller, two sides of communication could realize the quantum dialogue without divulging information to controller. Because of the join of a third party, safety of quantum dialogue is greatly enhanced, which makes this scheme better. According to the realization of secure two-way quantum communication, the scheme may be a good reference in practical application of quantum secure dialogue and quantum private communication.

Key words: Quantum dialogue; Unitary transformation; Bell-state measurement; Security