量子信令交换机模型设计及性能分析*

朱伟† 聂敏

(西安邮电大学, 通信与信息工程学院, 西安 710061)

(2013 年 1 月 21 日收到; 2013 年 2 月 26 日收到修改稿)

本文提出了量子信令交换机的模型, 该交换机由经典信息控制模块、交换控制模块和量子交换模块三部分组成. 经典控制模块负责将纠缠初态信息传送给纠缠测量及交换单元并更新路由信息. 交换控制模块实现通路选择, 为纠缠对的分发提供通路. 量子交换模块制备纠缠对, 进行 Bell 态的测量, 完成纠缠交换. 量子信令交换机可以实现多用户间的信令传输及局域网通信. 通过对交换机的性能分析与仿真, 结果表明该交换机结构简单、安全保密、便于扩展、时延小, 对于构建量子通信网有很好的支撑作用.

关键词: 量子通信, 量子信令网, 量子信令交换机, 纠缠交换

PACS: 03.67.Hk, 42.50.Dv, 89.70.−a **DOI:** 10.7498/aps.62.130304

1 引 言

量子通信以量子力学为基础, 根据量子态叠加原理 [1] 与量子不可克隆定理 [2], 使其具有绝对的安全保密性和高效性 [3], 已经成为各国研究的热点. 而以量子效应为基础的新信息手段初现端倪, 并正成为国际社会激烈竞争的焦点. Gobby 等 [4] 在 2004 年实现 122 km 光纤量子通信实验, 自由空间量子通信已经可达 23.4 km[5]. 我国的许多科技工作者也对量子通信进行了研究 [6−12], 中国科学技术大学教授潘建伟等组成的联合团队, 于 2011 年 10 月在青海湖成功实现了百公里的自由空间量子隐形传态和纠缠分发. 这些研究都为量子通信网的建立奠定了基础.

目前主要的量子通信方案是以 BB84 协议为基础的量子保密通信, 误码较大. 相关的研究主要集中在纠缠光子制备、量子信号的传输与检测技术、密钥分发协议、纠错编码、信道特性分析等方面. 基于隐形传态和纠缠交换的量子通信网络还处在实验阶段, 随着量子通信技术的进一步发展, 点对点的量子通信将趋于多用户、广域的量子通信网络, 而对量子通信网起关键作用的量子信令网 [13−18] 的研究还处在探索阶段. 为了构建量子通信网络, 本文设计了量子信令交换机的模型, 并对其性能进行了仿真分析.

2 量子信令网

图 1 为量子信令网信令传输模型, 与量子信令交换机 A 连接的用户 A_1 的量子态为 $|\phi\rangle = a|H\rangle + b|V\rangle$, 其中 $|H\rangle$, $|V\rangle$ 分别为水平极化与垂直极化, $|a^2| + |b^2| = 1$, a, b 为系数, a, b 的多种组合代表各种信令. 经过量子信令交换机及量子路由器交换, 可以实现 A_1 与 B_2 建立量子信道, 通过对 A_1 进行量子操作, 对 B_2 进行幺正变换, 实现信令传递至 B_2. 由量子信令交换机、量子路由器、量子卫星控制中心及通信终端等设备, 可以构建量子信令网. 量子信令控制着用户间, 交换机间和用户与交换机间的通信, 以及整个量子通信网的正常运行与维护. 用不同的量子态表示各种信令, 量子交换机根据信令指示, 可实现交换、选择链路、建立信道以及拆线、资费管理等功能.

* 国家自然科学基金 (批准号: 61172071, 61201194)、陕西省自然科学基础研究计划 (批准号: 2010JM8021)、陕西省教育厅自然科学研究项目 (批准号: 2010JK834) 和西安邮电学院青年教师科研基金 (批准号: ZL2010-05) 资助的课题.

† 通讯作者. E-mail: zhuwei2008003@163.com

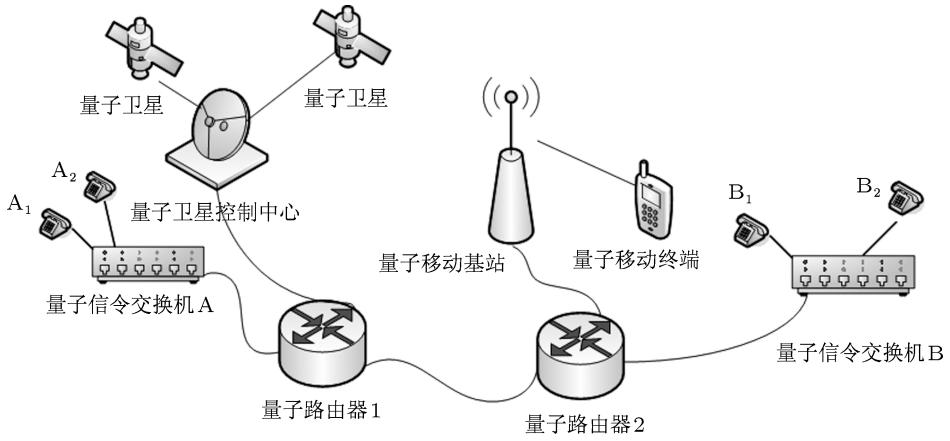

图 1 量子信令网信令传输模型

3 基于密集编码的信令编码

设 AB 的初态为

$$|\varphi^+\rangle_{\mathrm{AB}} = (|0,y\rangle + (-1)^x|0,\bar{y}\rangle)/\sqrt{2}, \qquad (1)$$

其中 x, y 为 0 或 1.

A, B 为具有最大纠缠的光子对, 对 A, B 进行一次局域幺正变换操作, 可编码 2bit 的经典信令信息. 译码时, 通过对纠缠态进行联合 Bell 基测量, 对比初态和测量结果, 便可恢复信息. 具体的编码译码过程如表 1 所示. 表 1 中, 将量子态与信令相对应, 通过对量子态的测量, 便可实现摘、挂机等的识别.

表 1 密集编码表

名称	内容			
AB 初态	$\|\varphi^+\rangle_{\mathrm{AB}}$			
A 发送信息	00	01	10	11
编码规则	$\sigma_0 \to 00$	$\sigma_x \to 01$	$\sigma_y \to 10$	$\sigma_z \to 11$
局域幺正变换	$\sigma_0\|\varphi^+\rangle_{\mathrm{AB}}$	$\sigma_x\|\varphi^+\rangle_{\mathrm{AB}}$	$\sigma_y\|\varphi^+\rangle_{\mathrm{AB}}$	$\sigma_z\|\varphi^+\rangle_{\mathrm{AB}}$
译码规则	$\|\varphi^+\rangle_{\mathrm{AB}} \to 00$	$\|\psi^+\rangle_{\mathrm{AB}} \to 01$	$\|\psi^-\rangle_{\mathrm{AB}} \to 10$	$\|\varphi^-\rangle_{\mathrm{AB}} \to 11$
量子态和信令	$\|\varphi^+\rangle_{\mathrm{AB}}$挂机	$\|\psi^+\rangle_{\mathrm{AB}}$摘机	$\|\psi^-\rangle_{\mathrm{AB}}$忙	$\|\varphi^-\rangle_{\mathrm{AB}}$释放链路

4 量子信令交换机组成及工作原理

量子信令交换机模型如图 2 所示, 由交换控制模块、经典信息控制模块、量子交换模块组成. 量子信令交换机为每个端口分配一个唯一的号码. 交换控制模块依据信令控制光交叉开关, 实现纠缠源与纠缠测量及交换单元、用户之间的连通, 为纠缠对的分发提供通路. 经典控制模块负责将纠缠初态信息传送给纠缠测量及交换单元并更新路由信息, 兼容经典通信系统. 量子交换模块包括纠缠源、纠缠测量及交换单元、光交叉矩阵组成. 量子交换模块进行 Bell 态测量及纠缠源产生并分发光子对. X, Y 端口用于交换机的扩展.

4.1 量子信令交换机信令传输过程

1) Alice (000000) 摘机, 纠缠源产生一对纠缠光子 A 和 B, 初态为 $|\varphi^+\rangle_{\mathrm{AB}}$, 对光子 A 进行幺正 σ_0 操作, A, B 光子均送纠缠测量及交换单元 0 并进行测量, 便可知摘机信令 $|\varphi^+\rangle_{\mathrm{AB}}$.

2) Alice 拨号 111110, 即进行三次局域幺正操作 ($\sigma_z\sigma_z\sigma_y$), Alice 要与 Bob 通话.

3) 量子信令交换机检测 Bob 是否空闲, 若忙则返忙, 若空闲则返回空闲.

4) 交换控制模块依据信令信息, 控制光交叉矩阵, 为 Alice 与 Bob 建立通信链路.

5) 纠缠源产生两对纠缠光子, 分别为光子 1 和 2、光子 3 和 4.

$$|\varphi\rangle_{12} = [|0\rangle_1|0\rangle_2 + |1\rangle_1|0\rangle_2]/\sqrt{2}, \qquad (2)$$

$$|\varphi\rangle_{34}=[|0\rangle_3|0\rangle_4+|1\rangle_3|0\rangle_4]/\sqrt{2}. \quad (3)$$

光子 2, 3 送纠缠测量及交换单元 0, 光子 1 送 Alice, 光子 4 送 Bob, 由光子 1, 2, 3, 4 组成的系统状态可以表示为

$$\begin{aligned}|\psi\rangle_{1234}=&|\varphi\rangle_{12}\otimes|\varphi\rangle_{34}\\=&[|0\rangle_1|0\rangle_2+|1\rangle_1|0\rangle_2]/\sqrt{2}\\&\otimes[|0\rangle_3|0\rangle_4+|1\rangle_3|0\rangle_4]/\sqrt{2}\\=&\frac{1}{2}[|0\rangle_1|0\rangle_2|0\rangle_3|0\rangle_4+|0\rangle_1|0\rangle_2|1\rangle_3|1\rangle_4]\\&+|1\rangle_1|1\rangle_2|0\rangle_3|0\rangle_4+|1\rangle_1|1\rangle_2|1\rangle_3|1\rangle_4]. \quad (4)\end{aligned}$$

选取的测量 Bell 基为

$$|M\rangle_{23}=[|0\rangle_2|0\rangle_3+|1\rangle_2|0\rangle_3]/\sqrt{2}. \quad (5)$$

纠缠测量及交换单元 0 对光子 2, 3 进行 Bell 态测量, 测量后可得到

$$|M\rangle_{23}|\psi\rangle_{1234}=|M\rangle_{23}[|\varphi\rangle_{12}\otimes|\varphi\rangle_{34}]=|\psi\rangle_{14}. \quad (6)$$

由上式可知, 通过选取适当的 Bell 基对光子 2, 3 进行 Bell 态测量, 就可以实现光子 1, 4 的纠缠, 实现纠缠交换, 从而建立量子通信信道.

6) 当交换机检测到摘机 (on-hook), 立刻终止通信, 释放链路.

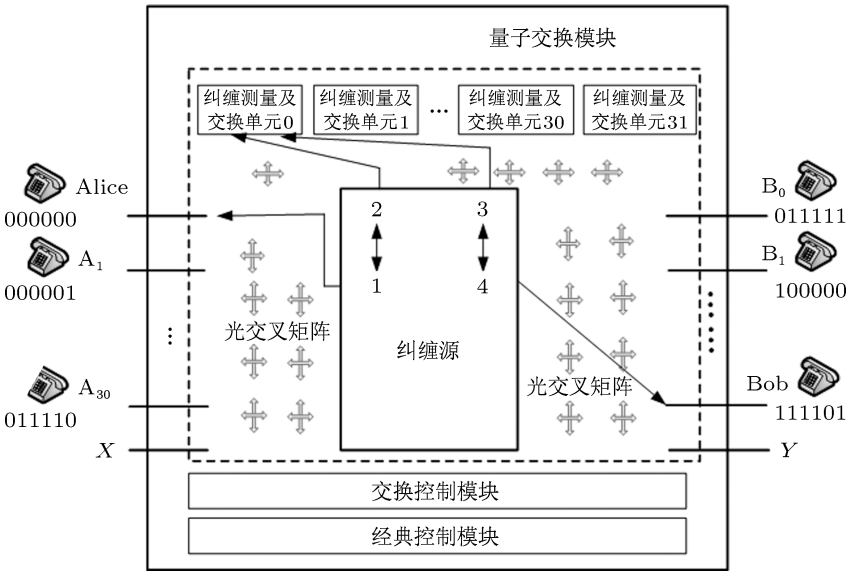

图 2 量子信令交换机模型

4.2 局域网量子信令传输过程

Alice 与 Bob 通信, 需要经过 $n-1$ 个交换机. 通信的具体过程如下:

1) Alice 拨号, 根据 Bob 的号码, 纠缠测量及交换单元 0 判决为非局域网通信. 纠缠源产生两对纠缠光子分别为 1, 2 和 3, 4; 将光子 1 送 Alice, 光子 4 送交换机 1 的扩展端口 Y; 将光子 2, 3 送纠缠测量及交换单元 0.

2) 交换机 2 收到光子 4, 并寻找 Bob 的号码, 若未发现 Bob 则将光子 4 送纠缠测量及交换单元 31, 纠缠源产生一对纠缠 5, 6, 将光子 5 送纠缠测量及交换单元 31, 将光子 6 送 B 端口, 传送至下一交换机.

3) 交换机 n 收到光子 $m-2$, 寻找路由信息, 将 $m-2$ 光子送对应的纠缠测量及交换单元. 纠缠源产生纠缠光子对 $m-1$ 与 m, 将 $m-1$ 送与光子 $m-2$ 对应的纠缠测量及交换单元.

设交换机 1 选取的测量基为 $|M\rangle_{23}$, 交换机 2 选取的 Bell 基为 $|M\rangle_{45}$, 交换机 n 选取的 Bell 基为 $|M\rangle_{(m-2)(m-1)}$. 由光子 1, 2, $\cdots$, m 组成的系统的状态为

$$|\psi\rangle_{1\cdots m}=|\varphi\rangle_{12}\otimes|\varphi\rangle_{34}\otimes\cdots|\varphi\rangle_{(m-1)m.} \quad (7)$$

选取测量基

$$|M\rangle=|M\rangle_{23}\otimes|M\rangle_{45}\otimes\cdots|M\rangle_{(m-2)(m-1)}. \quad (8)$$

最终有

$$\begin{aligned}|M\rangle|\psi\rangle_{1\cdots m}=&(|M\rangle_{23}|M\rangle_{45}\cdots|M\rangle_{(m-2)(m-1)})(|\varphi\rangle_{12}\\&\otimes|\varphi\rangle_{34}\otimes\cdots|\varphi\rangle_{(m-1)m})=|\varphi\rangle_{1m}. \quad (9)\end{aligned}$$

5 量子信令交换机性能分析

5.1 量子信令交换机容量

为了简化分析, 文中采用了 6 位二进制码作为用户号码, 实现了 31 对用户通信. 当用户数达到最大容量时, 再有用户通信请求, 信令交换机返回忙, 直到有空闲信道, 才可接入新用户. 根据实际需要, 可以采用 n (为偶数) 位二进制, 可以实现 $2^{n-1}-1$ 对用户建立连接. 用户数量过多用户号码长度也会增加, 将会增加编码译码时延. 用户采用多少位编码将在下一步的研究中给出.

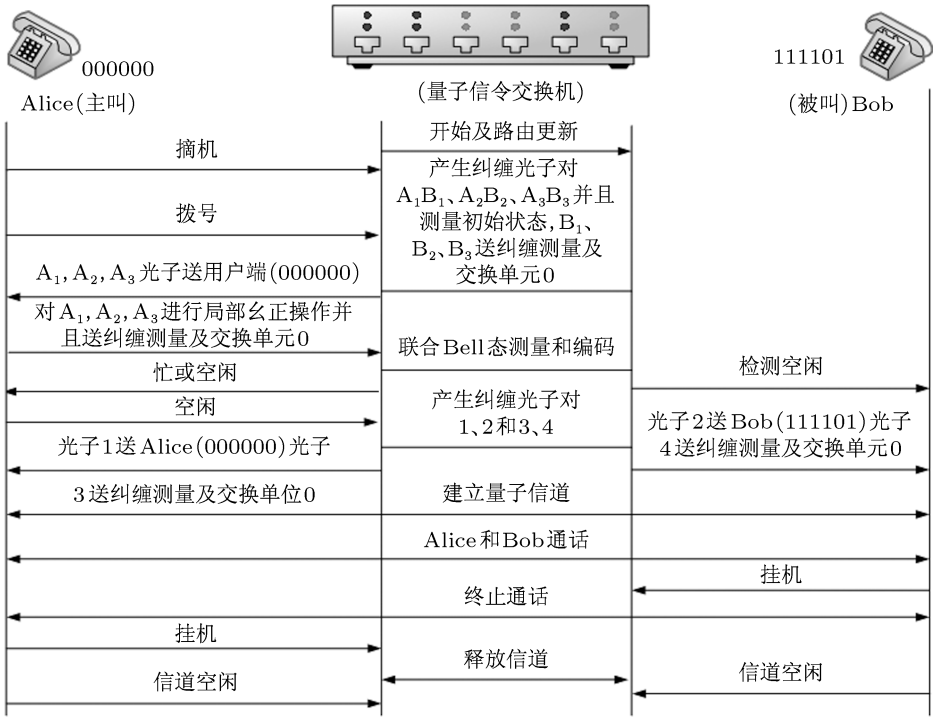

图 3 量子信令交换机信令传输过程

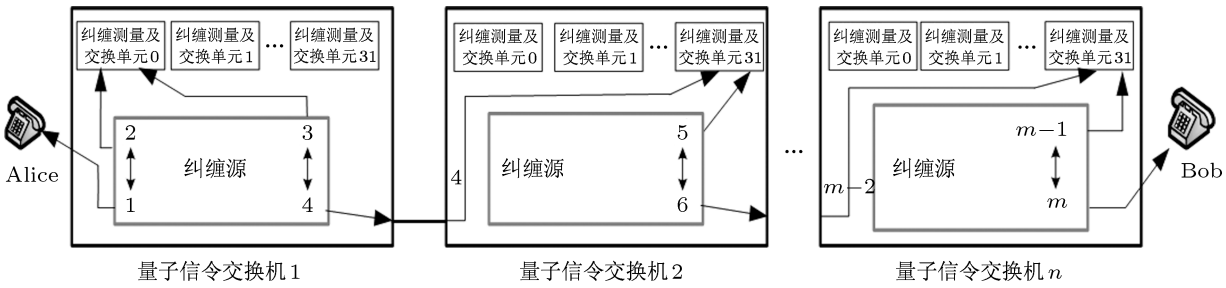

图 4 局域网量子信令传输模型

5.2 量子信令交换机的安全性

量子信令交换机采用密集编码方式, 以 EPR 对为信息载体, 保密性强. 因为传送的量子比特不携带任何信息, 根据纠缠态的信息隐藏特性, 局域的测量是无法提取 EPR 对携带的信息. 即使窃听者截获测量比特, 也无法破解, 所有信息都编码在纠缠粒子对之间的关联中, 局域操作无法提取传送的信息, 只有获得了纠缠粒子对的初态, 通过对比末态, 可知进行了那种局域幺正操作, 从而实现译码. 如果窃听者 Eve 采用最简单的截取重发方式窃听, Eve 虽无法获取任何信息, 但是, Eve 可以破坏所传

递的信息而不被发现, 这种窃听扰乱了正常链路选择. 为此, 选择具有可以进行信息直接传输, 不需要丢弃任何量子位且原理简单等优点的 Ping-Pang QSDC 协议. 量子信令交换机产生纠缠对, 将光子 A 发 Alice, 光子 B 发纠缠测量及交换单元. 如果 Alice 选择控制模式, Alice 则对光子 A 在基 $\{|0\rangle,|1\rangle\}$ 下进行测量, 并通过经典信道告诉纠缠测量及交换单元这次选择的是控制模式和测量结果; 纠缠测量及控制单元在接收到 Alice 的通知后, 对光子 B 也在基 $\{|0\rangle,|1\rangle\}$ 下进行测量, 并记录测量结果; 如果 Alice 和纠缠测量及控制单元的测量结果不相同, 则说明不存在窃听者, 可以继续拨号, 如果 Alice 和纠缠测量及控制单元的测量结果相同, 则说明存在窃听, Alice 将中断拨号.

Alice 和 Bob 建立好信道之后, 量子信令交换机使用 BB84 协议实现通信. Alice 与 Bob 通过与经典信道交换保留序列中的部分数据, 估计通信过程中量子比特的误码率. 依据误码率的门限值, 探测窃听者, 若存在窃听, 终止通信; 若误码率在容许范围之内, 则舍去用于检验误码率而交换的那部分数据, 保留其余的数据. Alice 与 Bob 通过经典信道进行纠错和密钥放大, 从而得到绝对安全的密钥. Eve 可以采用各种方法来进行窃听, 但是由于量子测不准原理和不可克隆定理, Eve 的窃听肯定会带来错误, Alice 和 Bob 通过错误率分析就能够发现窃听者的存在. 使用 BB84 协议通信可以保证量子密钥的安全分发.

5.3 量子信令交换机时延及吞吐量

Alice 与 Bob 成功建立信道的过程中, 设量子信令交换机的纠缠源成功产生纠缠对的概率为 $P_{\rm pro}$, BSM 成功测量 Bell 态的概率为 $P_{\rm mea}$, 交换控制成功完成交换的概率为 $P_{\rm swi}$. 成功建立信道需要的时间包括: 1) $T_{\rm pro}$ 为编码时成功产生纠缠对的平均时间; 2) $T_{\rm mea1}$ 为成功测量纠缠初态的平均时间; 3) $T_{\rm mea2}$ 为成功测量纠缠对编码后 Bell 态的平均时间; 4) $T_{\rm tra}$ 为初态信息传送至 BSM 的时间; 5) $T_{\rm cho}$ 为交换控制光交叉矩阵通路的时间; 6) $T_{\rm pro1}$ 为建立信道时成功产生纠缠对的平均时间; 7) $T_{\rm mea3}$ 为建立信道时成功测量纠缠对编码后 Bell 态的平均时间; 设 $T_{\rm pro}=T_{\rm pro1}$, $T_{\rm mea1}=T_{\rm mea2}=T_{\rm mea3}$; 忽略光子在光纤中的传输时间, 那么成功建立信道的时间T 为

$$T=T_{\rm pro}+T_{\rm mea1}+T_{\rm mea2}+T_{\rm tra}+T_{\rm cho}+T_{\rm pro1}+T_{\rm mea3}$$
$$=2T_{\rm pro}+3T_{\rm mea1}+T_{\rm tra}+T_{\rm cho}. \quad (10)$$

设交换机产生纠缠对的平均次数, BSM 的平均测量次数均服从指数分布. 令成功产生一对纠缠的时间为 $\tau_{\rm pro}=3$ ns, BSM 完成一次检测的时间为 $\tau_{\rm mea}=4$ ns, $T_{\rm tra}=2$ ns, $T_{\rm cho}=3$ ns. 那么有, $T_{\rm pro}=\tau_{\rm pro}/P_{\rm pro}$, $T_{\rm mea1}=\tau_{\rm mea}/P_{\rm mea}$, 那么时延为

$$T=2\tau_{\rm pro}/P_{\rm pro}+3\tau_{\rm mea}/P_{\rm mea}+T_{\rm tra}+T_{\rm cho}. \quad (11)$$

设产生纠缠对的成功率和检测 Bell 态的成功率是相互独立的, $P=P_{\rm mea}P_{\rm pro}$, 则量子通信网传递量子信息的吞吐量 S (单位是 bit/s) 为

$$S=1/(T/P). \quad (12)$$

从图 5 和图 6 中可以看出时延随着成功测量概率及成功产生纠缠对概率的增加而减小. 量子操作的成功率是时延的主要因素, 要减小时延就要提高纠缠源产生纠缠对的成功率, 还要提高 Bell 态检测的准确率.

从图 7 和图 8 可以看出吞吐量随着成功测量概率及成功产生纠缠对概率的增加而增大. 吞吐量随着时延的缩短也显著增加.

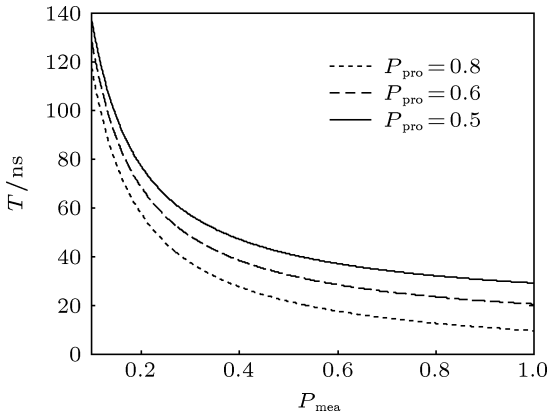

图 5 时延随着 $P_{\rm mea}$ 的变化曲线

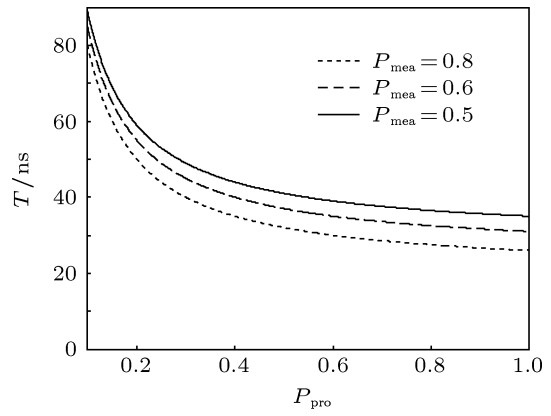

图 6 时延随着 $P_{\rm pro}$ 的变化曲线

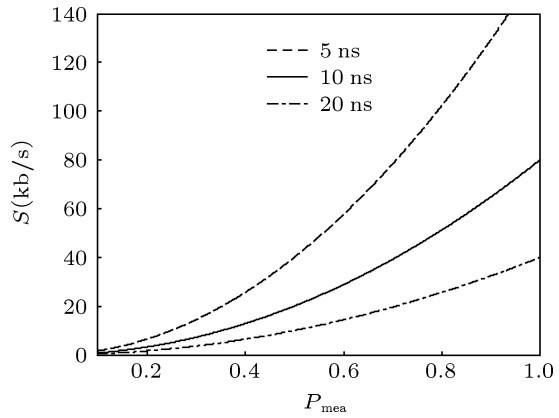

图 7 吞吐量随着 P_{mea} 的变化曲线

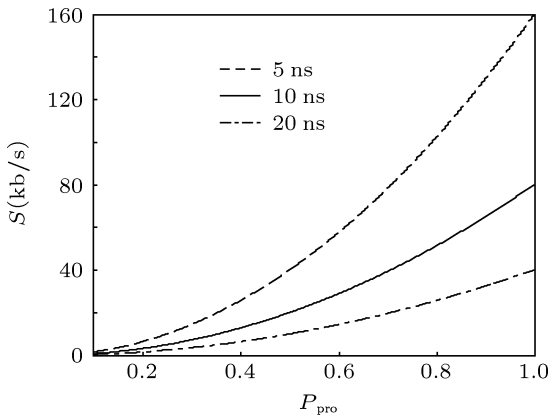

图 8 吞吐量随着 P_{pro} 的变化曲线

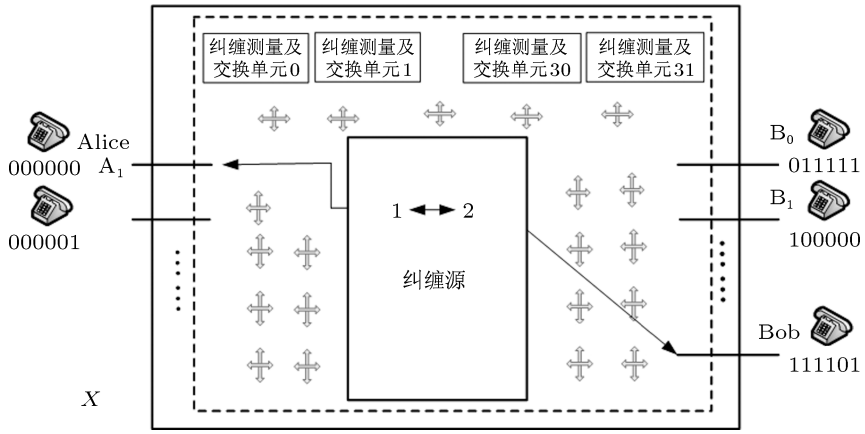

图 9 量子信令交换机局间传输模型

6 单个量子信令交换机局间传输信令的改进方法

局间是指与同一个量子信令交换机相连接的用户之间, 当要进行信令传输时, 可以将纠缠对直接分发至用户, 从而节约资源. 如图 9 所示, 当 Alice 与 Bob 通信时, 直接由纠缠源产生纠缠对 1, 2, 将 1, 2 光子分别分发至 Alice 与 Bob, 无需经过 BSM, 从而减小测量误差, 缩短时延.

7 结 论

本文提出的量子信令交换机模型, 基于纠缠交换实现了局域网用户信令的传输. 通过密集编码实现了路由选择, 保密性强. 仿真分析表明, 通过提高 Bell 态测量成功率和纠缠源产生纠缠对的成功率可以有效减小量子信令交换机的时延, 也可以提高吞吐量. 该量子信令交换机结构简单, 扩展性能强, 对于未来构建量子信令网络有重要的作用.

[1] Yin H, Ma H X 2003 *Military Quantum Communication Probability* (Beijing: Military Science Press) p61–63 (in Chinese) [尹浩, 马怀新 2006 军事量子通信概论 (北京: 军事科学出版社) 第 61—63 页]

[2] Long G L, Deng F G, Zen J Y 2011 *Recent progress in quantum mechanics fifth volume* (Beijing: Tsinghua University Press), p328–344 (in Chinese) [龙桂鲁, 邓富国, 曾谨言 2011 量子力学新进展 (北京: 清华大学出社) 第 328—344 页]

[3] Wang X B, YIN H, Ma H X, Pen C Z, Yang T, PAN J W 2006 *Physics* **35** 125 (in Chinese) [王向斌, 尹浩, 马怀新, 彭承志, 杨涛, 潘建伟 2006 物理 **35** 125]

[4] Gobby C, Yuan Z L, Shields A J 2004 *Appl. Phys. Lett.* **84** 3762

[5] Kurtsiefer C, Zarda P, Halder M 2002 *Nature* **419** 450

[6] Wu Y W, Hai W H 2006 *Acta Phys. Sin.* **55** 3315 (in Chinese) [邬云文, 海文华 2006 物理学报 **55** 3315]

[7] Zhou N R, Zeng B Y, Wang L J, Cong L H 2010 *Acta Phys. Sin.* **59** 2193 (in Chinese) [周南润, 曾宾阳, 王立军, 龚黎华 2010 物理学报 **59** 2193]

[8] Sun Y, Du J Z, Qin S J, Wen Q Y, Zhu F C 2008 *Acta Phys. Sin.* **57** 4689 (in Chinese) [孙莹, 杜建忠, 秦素娟, 温巧燕, 朱甫臣 2008 物理学报 **57** 4689]

[9] Yang Y G, Cao W F, Wen Q Y 2010 *Chin. Phys.* B **19** 050306

[10] Deng H L, Fang X M 2008 *Chin. Phys.* B **17** 0702

[11] Liu J, Wang Q, Kuang L M, Zeng H S 2010 *Chin. Phys.* B **19** 030313

[12] Zhao Z, Chen Y A, Zhang A N, Yang T, Briegel H J, Pan J W 2004 *Nature* **430** 54

[13] Yi Y H, Nie M, Pei C X 2012 *Journal of Northwest University* (Natural Science Edition) **42** 207 (in Chinese) [易运晖, 聂敏, 裴昌幸 2012 西北大学学报 (自然科学版) **42** 207]

[14] Zhang T P, Nie M, Pei C X 2009 *Acta Photonica Sinica* **38** 987 (in Chinese) [张天鹏, 聂敏, 裴昌幸 2009 光子学报 **38** 987]

[15] Wang Zhi, Nie M 2012 *Acta Photonica Sinica* **41** 1108 (in Chinese) [王志, 聂敏 2012 光子学报 **41** 1108]

[16] Lian T, Nie M 2012 *Acta Photonica Sinica* **41** 1251 (in Chinese) [连涛, 聂敏 2012 光子学报 **41** 125]

[17] Yi Y H, Nie M, Pei C X 2012 *Journal of Xidian University* (Natural Science Edition) **39** 29 (in Chinese) [易运晖, 聂敏, 裴昌幸 2012 西安电子科技大学学报 (自然科学版) **39** 29]

[18] Liu Dan, Pei C X, Quan D X, Zhao N 2010 *Chin. Phys. Lett.* **27** 050306

The model design and performance analysis of quantum signaling switch*

Zhu Wei† Nie Min

(*College of Communication and Information Engineering, Xi'an university of posts and telecommunications, Xi'an* 710061, *China*)

(Received 21 January 2013; revised manuscript received 26 February 2013)

Abstract

This paper puts forward a quantum signaling switch model. The quantum signaling switch consists of a classical information control module, an exchange control module and a quantum exchange module. Classical control module transmits the initial entangled state information to the entanglement measurement and switching unit and updates the routing information. Exchange control module will choose the path, and is ready for the distribution channel of the entanglement photons. The quantum exchange module generates quantum entanglement pairs, measures the Bell state and achieves entanglement swapping. Quantum signaling switches can realize multi-user communication and local area network communication. Through the performance analysis and simulation of the switch, the results show that the switch is simple in structure, secure and easy to expand; also the time delay is small. This will be helpful for the construction of the quantum communication network.

Keywords: quantum communication, quantum signaling network, quantum signaling switch, Entanglement swapping

PACS: 03.67.Hk, 42.50.Dv, 89.70.−a **DOI:** 10.7498/aps.62.130304

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61172071, 61201194), the Natural Science Foundation Research Project of Shanxi Province, China (Grant No. 2010JM8021), the Young Teachers' Scientific Research Fund of Xi'an institute of Posts and Telecommunications, China (Grant No. ZL2010-05), and the Natural Science research project of shaanxi province education department China (Grand No. 2010JK834).

† Corresponding author. E-mail: zhuwei2008003@163.com