量子-经典混合光网络的密钥分配协议研究

东 晨[1,2] 赵尚弘[1] 董 毅[1] 赵顾颢[1] 赵 静[1]

[1]空军工程大学信息与导航学院,陕西 西安 710077

[2]西安通信学院信息安全系,陕西 西安 710006

摘要 分析了点对点量子密钥分配协议的特点,在此基础上仿真研究了不同用户数量下量子-经典混合光网络量子密钥分配协议的网络性能,同时对比了三类协议的网络部署成本。仿真结果表明,对于中小型接入网(仿真用户数为32),制备-测量协议密钥生成率最高,安全传输距离最短,纠缠光协议密钥生成率最低,安全传输距离最长;对于较大规模网络,测量设备无关协议的网络部署成本最小,是建立混合光网络的最优选择。

关键词 量子光学;量子密钥分配;制备-测量分配协议;纠缠光分配协议;测量设备无关分配协议

中图分类号 O431.2 **文献标识码** A **doi**: 10.3788/LOP51.112701

Analysis of Quantum Key Distribution Protocols in Hybrid Quantum-Classical Optical Network

Dong Chen[1,2] Zhao Shanghong[1] Dong Yi[1] Zhao Guhao[1] Zhao Jing[1]

[1]*School of Information and Navigation, Air Force Engineering University, Xi'an, Shaanxi* 710077, *China*

[2]*Department of Information Security, Xi'an Communication College, Xi'an, Shaanxi* 710006, *China*

Abstract Quantum key distribution (QKD) networks are designed to allow multi-users for a dynamically any-to- any security communication. In this paper, three quantum key distribution schemes, compatible with classical optical networks, for future HQC networks are proposed and compared. For small-to-moderate size network, the highest secret key generation rate is supported by the prepare-measure scheme and the longest security distance is offered by entanglement- based scheme. For large networks, measurement- device-independent QKD, which is less demanding end-user technology and offers the best key rate, is the most proper solution for a cost-effective and reliable network deployment.

Key words quantum optics; quantum key distribution (QKD); prepare-measure QKD; entanglement-based QKD; measurement device independent QKD

OCIS codes 270.5565;010.1330;270.5568

1 引 言

量子密钥分配[1](QKD)作为量子信息科学的重要分支,以其建立在量子力学和信息论框架下的无条件安全性特点[2-4],近年来已成为国内外的研究热点之一[5-9]。在理论方面人们提出了制备-测量分配协议、基于纠缠光分配协议和测量设备无关分配协议并且通过实验进行了验证[10-12],点对点量子密钥分配协议已经进入了实用化阶段,但是点对点量子密钥分配协议使密钥只能在节点与节点之间分发,无法满足多个用户之间建立保密链路的实际需求,为了以有限的资源给更多的用户提供安全通信服务,在经典光网络上集成量子密钥分配网络,建立量子-经典混合光网络成为一种经济实用的可行方案。

在建立实际的量子-经典混合光网络时,如何选择量子密钥分配协议为多用户提供安全通信的链路成为网络部署的核心问题。本文在分析点对点量子密钥分配协议特点的基础上,仿真研究了不同用户数量对

收稿日期: 2014-05-04; **收到修改稿日期**: 2014-06-05; **网络出版日期**: 2014-10-21

基金项目: 国家自然科学基金(61106068)

作者简介: 东 晨(1985—),男,博士研究生,主要从事量子信息处理及量子密钥分配方面的研究。E-mail: dongchengfkd@sina.com

导师简介: 赵尚弘(1960—),男,教授,博士生导师,主要从事卫星光网络方面的研究。E-mail: zhaoshangh@aliyun.com

混合光网络量子密钥分配协议的性能影响，同时分析了三类方案的网络部署成本，为建立实际的量子-经典混合光网络提供了有益的理论参考。

2 理论与模型

2.1 量子密钥分配协议

量子密钥分配是利用量子比特携带一定的信息，在Alice和Bob之间进行传输，最后通过两人数据协调和隐私放大等数据后处理得到最终的安全比特。为实用起见，本文考虑的量子密钥分配协议是经过实验验证并在目前技术下可行的方案。主要分为三类:制备-测量协议，包括BB84、B92、SARG04等，其安全性证明等价于纠缠提纯的方法[13]；基于纠缠的协议，包括E91等，其安全性证明由量子比特的纠缠特性保证；测量设备无关协议，其安全性证明等价于纠缠证明的可逆过程。三种协议的基本结构如图1所示。

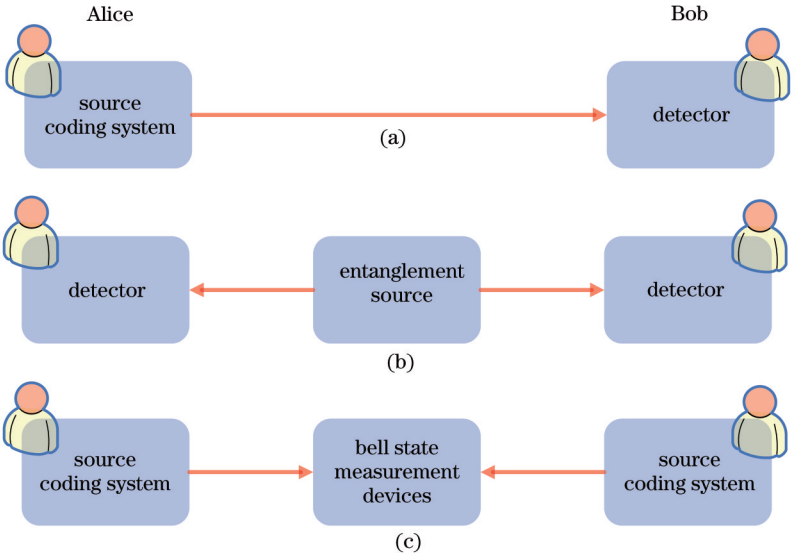

图1 三种量子密钥分配协议 (a)制备-测量协议 (b)纠缠光协议 (c)测量设备无关协议

Fig.1 Three different QKD schemes. (a) Prepare-measure QKD; (b) entanglement-based QKD; (c) measurement device independent QKD

1) 制备-测量分发协议：

如图1(a)所示，Alice从x基和z基中随机选取一组进行信息编码并将光脉冲发送给Bob，Bob随机地选择两组基进行测量，测量结束后公开选取的测量基，双方保留选择了相同基的量子比特，通过数据协调和隐私放大，产生安全密钥序列公式：

$$R_{\mathrm{BB84}} \geqslant q\left\{Q_1\left[1-H\left(e_1\right)\right]-fQ_\mu H\left(E_\mu\right)\right\}, \tag{1}$$

式中R_{BB84}为BB84协议的密钥生成率，$q=1/2$为BB84协议的效率，Q_μ为发送光脉冲强度为μ时的增益，E_μ为发送光脉冲强度为μ时的误码，Q_1为单光子增益，e_1为单光子误码率，$H(x)$为二元熵函数，f为误差校正系数，利用文献[12]的公式可以得到：

$$Q_\mu = 1-(1-Y_0)\exp(-\eta\mu), \tag{2}$$

$$E_\mu Q_\mu = e_0 Y_0 - e_{\mathrm{d}}[1-\exp(-\eta\mu)], \tag{3}$$

$$Q_1 = Y_1 \mu \exp(-\mu), \tag{4}$$

$$e_1 = (Y_0/2 - e_{\mathrm{d}}\eta)/Y_1, \tag{5}$$

其中η为信道传输效率，Y_0为暗记数噪声，Y_1为单光子计数率，e_0为背景噪声误码，e_{d}为探测器误码。

2) 基于纠缠光的分发协议：

如图1(b)所示，Alice与Bob共享一对纠缠光子对，双方对接收到的单光子随机地选择x基与z基进行分别测量，测量结束后通过公开信道对比两人所选择的基，双方保留选择了相同基的量子比特，并进行比特反

转等操作得到安全密钥序列公式：

$$R_{\mathrm{ent}} \geqslant qQ_e\left[1-H\left(e_Q\right)-fH\left(e_Q\right)\right], \tag{6}$$

式中 R_{ent} 为纠缠协议的密钥生成率，Q_e 为双边探测器同时相应的概率，e_Q 为纠缠协议的误码率：

$$Q_e=\eta_{\mathrm{a}}\eta_{\mathrm{b}}+\left(\eta_{\mathrm{a}}+\eta_{\mathrm{b}}-2\eta_{\mathrm{a}}\eta_{\mathrm{b}}\right)Y_0+(1-\eta_{\mathrm{a}}\eta_{\mathrm{b}})Y_{\mathrm{o}}^2, \tag{7}$$

$$e_Q=e_{\mathrm{d}}\eta_{\mathrm{a}}\eta_{\mathrm{b}}+\frac{1}{2}\left[\left(\eta_{\mathrm{a}}+\eta_{\mathrm{b}}-2\eta_{\mathrm{a}}\eta_{\mathrm{b}}\right)Y_0+(1-\eta_{\mathrm{a}}\eta_{\mathrm{b}})Y_{\mathrm{o}}^2\right], \tag{8}$$

其中 η_{a}，η_{b} 分别为Alice和Bob的单边传输效率。

3) 测量设备无关分发协议：

如图1(c)所示，Alice和Bob发送的相干光脉冲经过偏振调制器进行偏振编码(选取 x 基 z 基)后将光脉冲发送至第三方，第三方通过分束器、偏振分束器和探测器对接收到的光脉冲进行Bell态测量并公布测量结果，Alice和Bob根据基比对过程提取出安全密钥生成率的公式：

$$R_{\mathrm{MDI}} \geqslant \left\{Q_{11}\left[1-H\left(e_{11}^x\right)\right]-Q_{\mu\nu}^z fH\left(E_{\mu\nu}^z\right)\right\}, \tag{9}$$

其中 R_{MDI} 为测量设备无关协议的密钥生成率，$Q_{\mu\nu}$、$E_{\mu\nu}$ 分别为Alice发送光强度为 μ 且Bob发送光强度为 ν 时的增益和误码，Q_{11}、e_{11} 分别为单光子增益和单光子误码率，利用文献[14]的实验结果可以得到：

$$Q_{\mu\nu}^z=Q_C+Q_E, \tag{10}$$

$$E_{\mu\nu}^z Q_{\mu\nu}^z=e_{\mathrm{d}}Q_C+(1-e_{\mathrm{d}})Q_E, \tag{11}$$

为简化表达，式中：

$$Q_C=2(1-Y_0)^2\exp[-(\eta_{\mathrm{a}}\mu+\eta_{\mathrm{b}}\nu)/2]\left[1-(1-Y_0)\exp(-\eta_{\mathrm{a}}\mu/2)\right]\left[1-(1-Y_0)\exp(-\eta_{\mathrm{b}}\nu/2)\right], \tag{12}$$

$$Q_E=2Y_0(1-Y_0)^2\exp[-(\eta_{\mathrm{a}}\mu+\eta_{\mathrm{b}}\nu)/2]\left[\mathrm{I}_0(2s)-(1-Y_0)\exp[-(\eta_{\mathrm{a}}\mu+\eta_{\mathrm{b}}\nu)/2]\right], \tag{13}$$

式中 $\mathrm{I}_0(x)$ 表示第一类修正贝塞尔函数，然后利用文献[15]的方法估计得到单光子增益与单光子误码率：

$$Q_{11}=\mu\nu\exp(-\mu-\nu)Y_{11}, \tag{14}$$

$$e_{11}^x Y_{11}=\frac{Y_{11}}{2}-\left(\frac{1}{2}-e_{\mathrm{d}}\right)\frac{(1-Y_0)^2\eta_{\mathrm{a}}\eta_{\mathrm{b}}}{2}, \tag{15}$$

式中 Y_{11} 表示单光子计数率。

2.2 混合光网络量子密钥分配协议的网络部署

量子密钥分配网络是未来密钥分发向多用户、高速率、长距离发展的必然趋势，通过扩展点对点密钥分发协议实现多用户的保密通信并且降低了互联成本，从而提高保密通信的可靠性和安全性，通常根据量子密钥分配网络的不同部署方案分为可信任中继密钥分配网络[16]、无源光器件密钥分配网络[17]和量子纠缠密钥分配网络[18]，其中采用波分复用技术集成于无源光网络(WDM-PON)[19]组成量子-经典混合光网络是目前技术条件下最为可行的方案。本文在光纤中采用波分复用技术实现经典信号(1550 nm)与量子信号(1310 nm)的传输，为了重点研究不同协议对网络性能的影响，本文将经典信号对量子信号的串扰噪声定义为常数，同时假设接入网的用户数为 N，量子密钥分配网络部署拓扑如图2所示。

如图2(a)所示，制备-测量密钥分配网络中不同接入网的用户通过光交换中心同时进行信息传输与密钥分配，用户端同时部署发送与接收设备，得到制备-测量密钥分配网络的密钥生成率与网络部署成本为：

$$R_1=R_{\mathrm{BB84}}r_{\mathrm{BB84}}/N, \tag{16}$$

$$C_{\mathrm{BB84}}=NC_{\mathrm{send}}+NC_{\mathrm{receive}}+C_{\mathrm{network}}, \tag{17}$$

其中 r_{BB84} 为BB84协议弱相干光源脉冲发送频率，C_{BB84} 为BB84协议网络部署成本。如图2(b)所示，纠缠光密钥分发网络中，不同接入网的用户接收并测量来自服务中心发送的纠缠光子进行密钥分配同时接收经典信息，服务中心部署纠缠光源发送设备，用户端只需部署接收测量设备，则可以得到纠缠光密钥分配网络的密钥生成率与网络部署成本为：

$$R_2=R_{\mathrm{ent}}r_{\mathrm{ent}}/N, \tag{18}$$

$$C_{\mathrm{ent}}=C_{\mathrm{send}}+NC_{\mathrm{receive}}+C_{\mathrm{network}}, \tag{19}$$

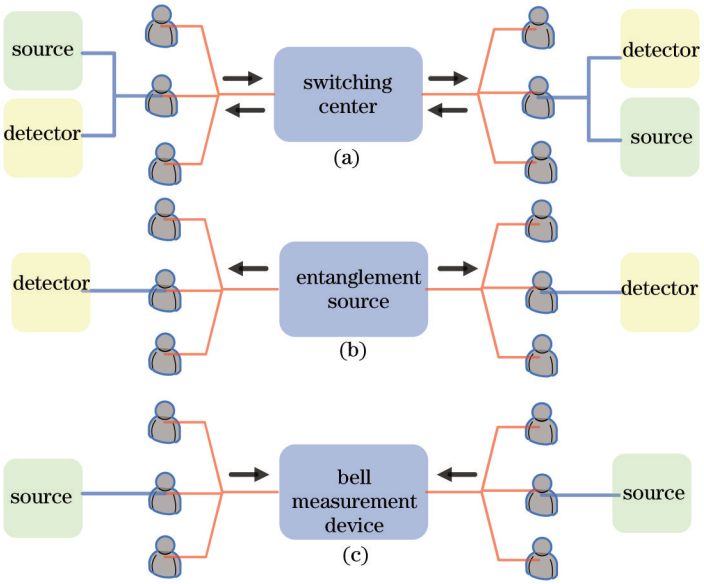

图2 基于三种量子密钥协议的网络结构。(a)制备-测量密钥网络; (b)纠缠光源密钥网络; (c)测量设备无关密钥网络

Fig.2 Three different architectures for QKD networks. (a) Prepare-measure QKD; (b) entanglement-based QKD; (c) measurement device independent QKD

其中 r_{ent} 为纠缠光源脉冲发送频率，C_{ent} 为纠缠网络部署成本。如图2(c)所示，测量设备无关密钥分发网络中，不同接入网的用户只需将量子信息与经典信息发送至服务中心，服务中心部署Bell态测量设备，用户端只需部署相干光发送设备，便可以得到测量设备无关密钥分配网络的密钥生成率与网络部署成本为：

$$R_3 = R_{MDI} r_{MDI} / N, \tag{20}$$

$$C_{MDI} = NC_{send} + C_{receive} + C_{network}, \tag{21}$$

其中 r_{MDI} 为测量设备无关协议弱相干光源脉冲发送频率，C_{MDI} 为测量设备无关协议网络部署成本。。

3 仿真结果与分析

根据(1)、(6)、(9)式可以对点对点量子密钥分配协议的性能进行分析，固定接入网用户数 N=32；利用(16)、(18)、(20)式可以得到三种协议集成于混合光网络的网络性能；根据(17)、(19)、(21)式可以推出三种密钥分配协议的网络部署成本，仿真主要参数如表1所示[15]。

表1 主要仿真参数设置

Table 1 Parameters of the experimental setup

Parameter	e_0	e_d	Y_0	f
Value	0.5	1.5%	10^{-6}	1.16

由图3可知，对于点对点量子密钥分发协议，制备-测量分配协议密钥生成率最高，但是其安全传输距离最短，仅为145 km；纠缠光协议安全传输距离最长为312 km，但受限于频率较低的纠缠光源产生光子对脉冲，其密钥生成率最低；测量设备无关协议安全传输距离能够达到207 km，密钥生成率介于两者之间。由图4可知，对于接入网用户为32的混合光网络，制备-测量分配协议安全传输距离降为72 km，纠缠光协议安全传输距离降为152 km，测量设备无关协议安全传输距离降为105 km。由图5可知，随着用户数的不断增加，制备-测量分配协议密钥生成率迅速下降，在用户数为62时无法安全产生密钥，纠缠光协议与测量设备无关协议的密钥生成率在多用户情形下降较为平缓，由(17)、(19)、(21)式可知，制备-测量分配协议的网络部署成本最高，测量设备无关协议网络部署成本最低。

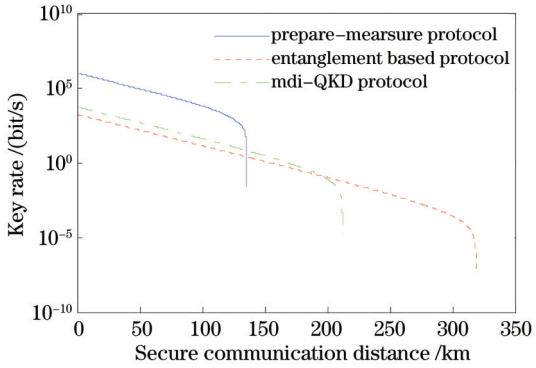

图3 三类协议密钥生成率与安全传输距离

Fig.3 Rate versus distance for three QKD protocols

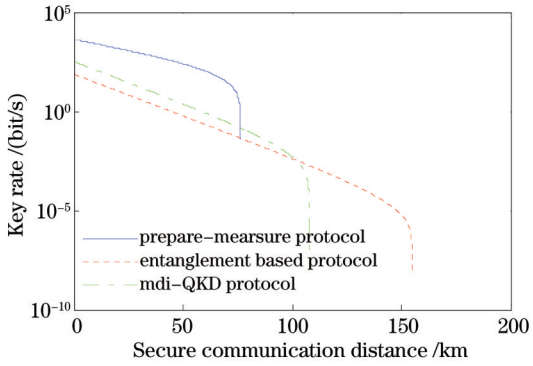

图4 三种网络密钥生成率与安全传输距离的关系(用户数为32)

Fig.4 Rate versus distance for three network architectures at N=32

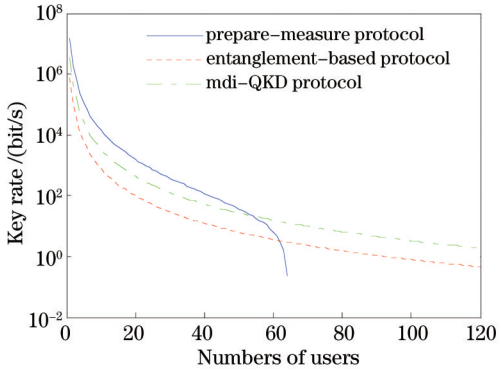

图5 三种网络密钥生成率与用户数的关系

Fig.5 Rate versus number of users for three network architectures

4 结 论

分析了点对点量子密钥分配协议的特点,在此基础上仿真研究了不同用户数量下混合光网络量子密钥分配协议的网络性能,同时对比了三类协议的网络部署成本,仿真结果表明随着用户数量逐渐增加,制备-测量协议密钥生成率下降最快,纠缠光协议和测量设备无关协议能够接入较多的用户,但纠缠光协议密钥生成率小于测量设备无关协议。对于中小型接入网,制备-测量协议密钥生成率最高,安全传输距离最短,纠缠光协议密钥生成率最低,安全传输距离最长;对于大型接入网,测量设备无关协议网络部署成本最低,即使没有纠缠光协议安全传输距离长,在实验中可以通过添加量子存储单元[20]增加其安全传输距离,在实际的网络部署中选择测量设备无关协议作为混合光网络的密钥分配协议是最为可行的方案。

参 考 文 献

1 Bennet C H, Brassard G. Quantum cryptography: public key distribution and coin tossing [C]. IEEE International Conference Computers, Ystems, and Signal Processing Bangalore, India. 1984. 175-179.

2 Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol [J]. Phys Rev Lett, 2000, 85 (12): 441-444.

3 Mayers D. Unconditionally secure quantum bit commitment is impossible [J]. Phys Rev Lett, 1997, 78(17): 3414-3417.

4 Gottesman D, Lo H K, Lutkenhaus N, *et al*.. Security of quantum key distribution with imperfect devices [J].Quantum Information Computation, 2004, 4(5): 325-360.

5 Zhao Guhao, Zhao Shanghong, Yao Zhoushi, *et al*.. Effect of the pulse broadening caused by atmosphere on satellite based quantum key distribution [J]. Acta Optica Sinica , 2012, 32(11): 1127001.
赵顾颢, 赵尚弘, 幺周石, 等. 大气导致的脉冲展宽对星载量子密钥分发的影响[J]. 光学学报, 2012, 32(11): 1127001.

6 Lu Daoming. Quantum properties in the system of atoms interacting with weak coherent cavities fields [J]. Acta Optica Sinica, 2012, 32(10): 1027001.
卢道明. 原子与弱相干腔场相互作用系统中的量子特性[J]. 光学学报, 2012, 32(10): 1027001.
7 Lu Daoming, Qiu Changdong. Entanglement properties in the system of atom interacting with two-mode cavity [J]. Acta Optica Sinica, 2013, 33(12): 1227003.
卢道明, 邱昌东. 原子与双模腔相互作用系统中的纠缠特性[J]. 光学学报, 2013, 33(12): 1227003.
8 Wang Fei, Xiao Ming. Output sideband quantum correlation with nonadiabatic elimination [J]. Acta Optica Sinica, 2012, 32(12): 1227001.
王 飞, 肖 明. 非绝热消除条件下输出边频量子关联[J]. 光学学报, 2012, 32(12): 1227001.
9 Guo Xueshi, Gao Kang, Liu Nannan, *et al*.. Differential detection system for measureing the quantum noise of pulsed light [J]. Acta Optica Sinica, 2012, 33(9): 0927002.
郭学石, 高 亢, 刘楠楠, 等. 适用于测量脉冲光量子噪声的差分探测系统[J]. 光学学报, 2013, 33(9): 0927002.
10 Brassard G, Lutkenhaus N, Mor T, *et al*.. Limitations on practical quantum cryptography [J]. Phys Rev Lett, 2000, 85(6): 1330-1333.
11 Bennet t C H, Brassard G, Mermin N D. Quantum cryptography without Bell′s theorem [J]. Phys Rev Lett, 1992, 68(5): 557-559.
12 Lo H K, Curty M, Qi B. Measurement device independent quantum key distribution [J]. Phys Rev Lett, 2012, 108(13): 130503.
13 Lo H K, MA X F, Chen K. Decoy state quantum key distribution [J]. Phys Rev Lett, 2005, 94(23): 230504.
14 Ma X F, Fung C H F, Razavi M. Statistical fluctuation analysis for measurement device independent quantum key distribution [J]. Phys Rev A, 2012, 86(5): 052305.
15 Ma X F, Razavi M. Alternative schemes for measurement device independent quantum key distribution [J]. Phys Rev A, 2012, 86(6): 062319.
16 Elliot C. Building the quantum network [J]. New Journal of Physics. 2002, 4(1): 46.
17 Townsend P D. Quantum cryptography on multiuser optical fiber networks [J]. Nature, 1997, 385(6611): 47-49.
18 Duan L M, Lukin M D, Cirac J I, *et al*.. Long distance quantum communication with atomic ensembles [J]. Nature, 2001, 414(6862): 413-418.
19 Qi B, Zhu W, Qian L, Lo H K. Feasibility of quantum key distribution through a dense wavelength division multiplexing network [J]. New Journal of Physics, 2010, 12(10): 103042.
20 Panayi C, Razavi M, Ma X F, *et al*.. Memory-assisted measurement-device-independent quantum key distribution [J]. New Journal of Physics, 2014, 16(4): 043005.