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

基于量子存储的长距离测量设备无关量子密钥分配研究

孙颖　赵尚弘　东晨

Long distance measurement device independent quantum key distribution with quantum memories

Sun Ying　Zhao Shang-Hong　Dong Chen

引用信息 Citation: Acta Physica Sinica, 64, 140304 (2015)　DOI: 10.7498/aps.64.140304
在线阅读 View online: http://dx.doi.org/10.7498/aps.64.140304
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2015/V64/I14

基于量子存储的长距离测量设备无关量子密钥分配研究*

孙颖[1)†] 赵尚弘[1)] 东晨[1)2)]

1) (空军工程大学信息与导航学院, 西安 710077)

2) (西安通信学院信息安全系, 西安 710006)

(2014 年 12 月 10 日收到; 2015 年 3 月 20 日收到修改稿)

针对量子中继器短时间内难以应用于长距离量子密钥分配系统的问题, 提出了基于量子存储的长距离测量设备无关量子密钥分配协议, 分析了其密钥生成率与存储效率、信道传输效率和安全传输距离等参数间的关系, 研究了该协议中量子存储单元的退相干效应对最终密钥生成率的影响, 比较了经典测量设备无关量子密钥分配协议和基于量子存储的测量设备无关量子密钥分配协议的密钥生成率与安全传输距离的关系. 仿真结果表明, 添加量子存储单元后, 协议的安全传输距离由无量子存储的 216 km 增加至 500 km, 且量子存储退相干效应带来的误码对最终的密钥生成率影响较小. 实验中可以采取调节信号光强度的方式提高测量设备无关量子密钥分配系统的密钥生成率, 为实用量子密钥分配实验提供了重要的理论参数.

关键词: 量子存储, 测量设备无关量子密钥分配, 诱骗态

PACS: 03.67.Dd **DOI:** 10.7498/aps.64.140304

1 引 言

量子密钥分配[1] (quantum key distribution, QKD) 是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[5−9]. 然而, 量子信道对光子的指数衰减作用 (光纤信道损耗 0.2 dB/km) 限制了 QKD 系统的安全密钥传输距离[10]. 为了实现长距离的 QKD, 人们提出了量子中继方案[11], 即通过 n 级纠缠交换使得距离为 L 的两个节点内的光子对产生纠缠, 将量子态在光纤信道中的传输损耗形式从指数衰减变为多项式衰减[12], 有效增加 QKD 的安全密钥传输距离. 但是, 量子中继方案要求量子存储单元[13] 具有较长的退相干时间和较高的存储效率[14], 目前的量子存储技术很难实现, 量子态存储时间和纠缠保真度距离实际应用也还存在较大的差距[15].

最近, Lo 等[16] 提出了测量设备无关量子密钥分配方案 (measurement device independent QKD, MDI-QKD). 在该方案中, Alice 和 Bob 将光脉冲发送至非可信任的第三方进行 Bell 态测量 (Bell state measurement, BSM)[17] 并公布测量结果, Alice 和 Bob 根据基比对结果提取出原始安全密钥, 由于该方案的测量过程允许在非可信任第三方进行, 故其可以移除所有的探测器侧信道漏洞[18,19]. 但是在该系统中, Alice 和 Bob 发送的光脉冲在到达第三方进行 BSM 前, 要承受单边信道传输损耗, 降低了 BSM 成功的概率, 限制了安全传输距离.

事实上, 结合量子中继的思想将量子存储单元引入 MDI-QKD 系统, 不仅可以增加 QKD 系统的安全密钥传输距离, 也可以降低信道传输损耗对 BSM 的影响, 且其对量子存储器退相干时间的要求相对较短, 这样就使得在实际中实现长距离

* 国家自然科学基金 (批准号: 61106068) 资助的课题.

† 通信作者. E-mail: sunyingkgd@163.com

QKD 成为可能[20]. Christiana 等[21] 提出在 MDI-QKD 系统的两条信道中各添加一个量子存储器可以极大地增加安全传输距离, 并通过实验仿真验证了添加写入时间低于 10 ns 的快速量子存储器可实现超过 500 km 的 QKD, 添加相干时间高于 1 μs 的量子存储器, 其安全传输距离超过 300 km. 但是达到实用的概率量子中继器的相干时间要达到 1 ms 以上. 2013 年, Silvestre 等[22] 以 Lo 等提出的 MDI-QKD 协议为基础, 在 BSM 设备前添加两个量子存储器, 实现了无纠缠光子对、量子存储器退相干时间较短的基于诱骗态协议[23] 的长距离 QKD, 仿真结果表明该方案可将安全传输距离增加到 500 km 以上. 因此, 在量子中继技术没有突破之前, 结合诱骗态方案的基于量子存储的 MDI-QKD 将是一种折中的易实现的长距离量子密钥分配方案. 本文基于量子存储的 MDI-QKD 协议, 在文献 [21, 22] 的基础上给出了该协议的系统模型和最终密钥生成率公式. 通过实验仿真比较了无量子存储 MDI-QKD 和基于量子存储 MDI-QKD 的量子密钥生成率与安全传输距离的关系, 分析了量子存储退相干效应、信道传输效率以及存储效率对最终密钥生成率的影响.

2 理论与模型

2.1 测量设备无关量子密钥分配协议

测量设备无关量子密钥分配协议模型如图 1 所示.

Alice 和 Bob 发送的相干光脉冲先经过偏振调制器进行偏振编码 (选取 X 基或 Z 基), 再经过强度调制器调制出真空态、诱骗态和信号态后发送至第三方, 第三方通过分束器、偏振分束器和探测器对接收到的相干光脉冲进行 BSM 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[24]:

$$R \geqslant \mu_2\nu_2 \mathrm{e}^{-\mu_2-\nu_2}\check{Y}_{11}^z\left[1-H\left(\hat{e}_{11}^x\right)\right] - Q_{\mu_2\nu_2}^z f H\left(E_{\mu_2\nu_2}^z\right), \quad (1)$$

式中 X, Z 分别代表 X 基和 Z 基, 其中 X 基作为测试基用来估计信道参数, z 基用来产生安全密钥; 利用文献 [24] 可以估计单光子增益的下界 $\check{Y}_{11}^z$ 和单光子误码率的上界 $\hat{e}_{11}^x$; 同时利用文献 [25] 的实验结果可以得到 Z 基下的增益与 QBER, 最终推出 MDI-QKD 协议的密钥生成率.

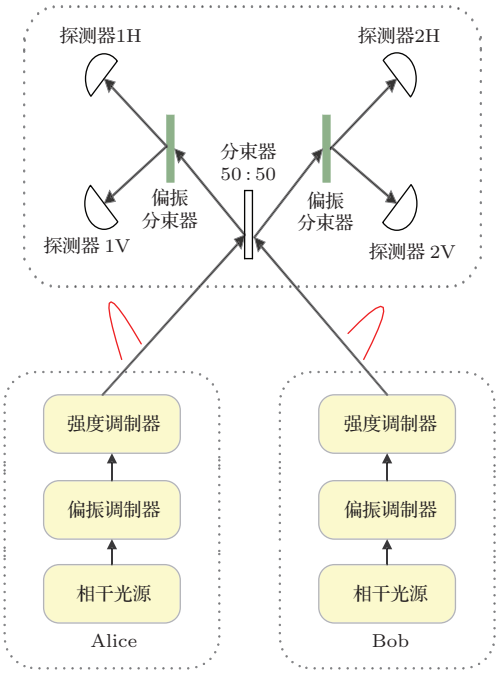

图 1 测量设备无关量子密钥分配系统结构[16]

Fig. 1. The structure of MDI-QKD system.

2.2 基于量子存储的长距离测量设备无关量子密钥分配协议

基于量子存储的长距离 MDI-QKD 系统模型如图 2 所示.

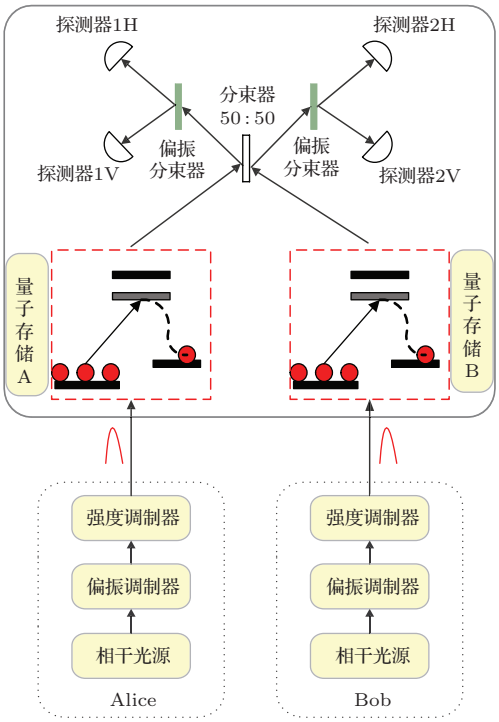

图 2 基于量子存储的长距离测量设备无关量子密钥分配系统

Fig. 2. Long distance MDI-QKD system with quantum memories.

与图1相比, Alice和Bob发送的相干光脉冲在第三方进行BSM前, 分别先与量子存储A、量子存储B进行光子偏振态与存储量子比特的转化:

$$\frac{1}{\sqrt{2}}\left[|S_H\rangle_{\mathrm{A(B)}}|H\rangle_P+|S_V\rangle_{\mathrm{A(B)}}|V\rangle_P\right], \tag{2}$$

其中$|H\rangle_P$, $|V\rangle_P$分别为偏振编码的水平态和垂直态; $|S_H\rangle_{\mathrm{A(B)}}$, $|S_V\rangle_{\mathrm{A(B)}}$为Alice (Bob)的量子存储A(B)对应的量子比特. 本文假设量子存储单元为单模量子存储, 即每个量子存储器只能存储一个光子偏振态或相对应的量子比特, 当量子存储A与量子存储B均完成光子偏振态的写入、转化和存储后, 第三方提取相应的量子比特进行BSM, Alice和Bob根据与MDI-QKD相同的基比对过程提取出未进行筛选的原始安全密钥, 原始密钥经过隐私放大和数据协调过程可以得到最终的密钥生成率:

$$R\geqslant\frac{1}{\langle T\rangle}\left[Q_{11}^{\mathrm{QM}}\left(1-H(e_{11}^x)\right)-H(e_{11}^z)\right]. \tag{3}$$

其中$1/\langle T\rangle$为未进行筛选的原始密钥生成速率:

$$\langle T\rangle=R_{\mathrm{S}}\frac{1}{P_{\mathrm{BSM}}}\frac{3-2P_0}{(2-P_0)P_0}, \tag{4}$$

式中R_{S}为通信双方发射激光脉冲的频率, P_{BSM}为第三方成功进行BSM的概率:

$$P_{\mathrm{BSM}}=\frac{1}{2}(1-P_{\mathrm{D}})^2\left[\eta_{\mathrm{MD}}^2+2(4-3\eta_{\mathrm{MD}})\eta_{\mathrm{MD}}P_{\mathrm{D}}+8(1-\eta_{\mathrm{MD}})^2P_{\mathrm{D}}^2\right], \tag{5}$$

本文将量子存储的写入效率η_{w}、读取效率η_{r}等因素综合考虑为量子存储效率η_{M}; η_{D}为探测器效率, 记$\eta_{\mathrm{MD}}=\eta_{\mathrm{M}}\eta_{\mathrm{D}}$; P_0为A, B发送的光子态能够成功到达第三方并进行量子存储的概率, 与信道传输距离L相关. 本文考虑对称信道传输效率情形, 即Alice和Bob到第三方的距离相等为$L/2$且量子存储A与量子存储B的存储效率相同, 结合文献[26]在理想单光子源情形下对单光子增益及单光子误码率的估计方法, 得到弱相干光源情形下的单光子增益Q_{11}^{QM}:

$$Q_{11}^{\mathrm{QM}}=\frac{\mu\nu\eta_{\mathrm{MD}}^2\eta_{\mathrm{T}}^2\,\mathrm{e}^{\left(\frac{1}{2}\mu\eta_{\mathrm{MD}}\eta_{\mathrm{T}}+\frac{1}{2}\nu\eta_{\mathrm{MD}}\eta_{\mathrm{T}}-\mu-\nu\right)}}{4\left(\mathrm{e}^{\frac{1}{2}(\mu\eta_{\mathrm{MD}}\eta_{\mathrm{T}})}-1\right)\left(\mathrm{e}^{\frac{1}{2}(\nu\eta_{\mathrm{MD}}\eta_{\mathrm{T}})}-1\right)}, \tag{6}$$

z基的单光子误码率e_{11}^z为

$$e_{11}^z=e_\infty^z+\frac{1}{2}\frac{(1/2-e_\infty^z)(1-P_0)^{1+\tau}}{2-P_0}, \tag{7}$$

x基的单光子误码率e_{11}^x为

$$e_{11}^x=e_\infty^x+\frac{1}{2}\frac{(1/2-e_\infty^x)(1-P_0)^{1+\tau}}{2-P_0}, \tag{8}$$

其中τ为量子存储退相干时间, e_∞^z, e_∞^x为z基和x基在量子退相干时间趋于无穷的误码率, 即量子存储过程不引入新的误码:

$$\begin{aligned}e_\infty^z&=e_\infty^x\\&=\frac{2P_{\mathrm{D}}\left[2(\eta_{\mathrm{MD}}-1)^2P_{\mathrm{D}}-(\eta_{\mathrm{MD}}-2)\eta_{\mathrm{MD}}\right]}{\eta_{\mathrm{MD}}^2+8(\eta_{\mathrm{MD}}-1)^2P_{\mathrm{D}}^2+2(4-3\eta_{\mathrm{MD}})\eta_{\mathrm{MD}}P_{\mathrm{D}}}.\end{aligned} \tag{9}$$

与传统的MDI-QKD相比, 通过添加量子存储单元, 使得通信双方中先完成量子存储的一方在进行BSM前能够预报量子态, 等价于在脉冲发送并测量的所有事件中减少了Alice和Bob同时承受单边信道传输损耗的事件, 从而增加单光子进行BSM的成功概率, 但同时因为量子存储单元存在退相干效应, 当存储时间超过退相干时间的阈值时会引入新的误码. 本文采用文献[27]的量子退相干模型, 得到量子存储退相干时间的下限τ^{MIN}:

$$\tau^{\mathrm{MIN}}=\frac{\log_2\left[\frac{(P_0-2)\left(e_\infty^x-e^{\mathrm{MAX}}\right)}{(P_0-1)(2e_\infty^x-1)}\right]}{\log_2(1-P_0)}, \tag{10}$$

对于诱骗态量子密钥分发协议$e^{\mathrm{MAX}}=11\%$.

3 仿真结果与分析

将(9)式代入(7)和(8)式分别得到基于量子存储的MDI-QKD的x基和z基下的单光子误码率, 然后将(6)和(4)式代入(3)式可以得到最终的安全密钥生成率与信道传输损耗之间的关系. 主要仿真参数如表1所列.

表1 主要仿真参数

Table 1. The main simulation parameters.

文献[22]	e_0	e_{d}	P_{D}	η_{M}	η_{D}
	0.5	1.5%	10^{-6}	0.6	0.2

由图3可知, 随着基于量子存储的MDI-QKD安全传输距离的增大, 要求量子存储的最小退相干时间也逐渐增大, 即要求量子存储器能够更长时间地保持所存储量子比特的保真度. 如图4所示, 当安全传输距离为400 km, 随着量子存储能够承受的退相干时间的不断增加, 密钥生成率逐渐增加, 当$\tau\geqslant5\tau^{\mathrm{MIN}}$时密钥生成率曲线逐渐平

坦, 即通过改善量子存储单元的退相干时间不能无限地增大密钥生成率. 如图5所示, 无量子存储的MDI-QKD 能够达到的安全传输距离为216 km, 而添加量子存储单元后, 基于量子存储的MDI-QKD的安全传输距离大于500 km, 同时对于基于量子存储的MDI-QKD, 当退相干时间为$\tau = 2\tau^{\rm MIN}$与$\tau = \infty$时, 密钥生成率的变化不大, 即量子存储退相干效应对最终的密钥生成率影响较小.

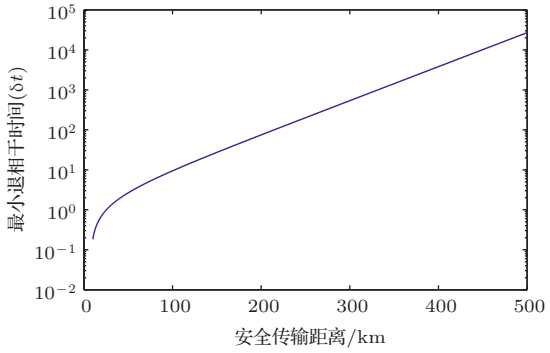

图3 安全传输距离与存储时间

Fig. 3. The secure transmission distance and storage time.

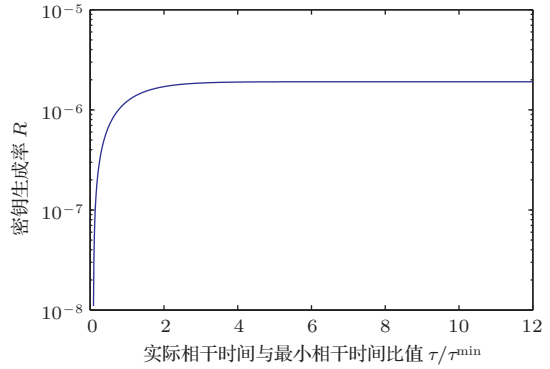

图4 量子存储相干时间与密钥生成率 ($L = 400$ km)

Fig. 4. The quantum storage coherence time and key generation rate ($L = 400$ km).

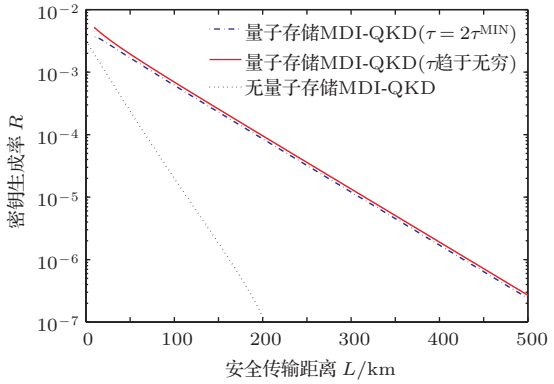

图5 密钥生成率与安全传输距离

Fig. 5. The key generation rate and the secure transmission distance.

4 结 论

本文研究了基于量子存储的MDI-QKD, 结果表明该协议可以实现无量子中继器、仅利用单模量子存储器的长距离QKD, 而且协议中量子存储器要求的相干时间比量子中继协议中要求的短, 极大地降低了对量子存储器的要求, 相比量子中继协议更易实现. 同时, 本文比较了无量子存储MDI-QKD和基于量子存储的MDI-QKD的密钥生成率与安全传输距离的关系, 仿真结果表明添加量子存储单元后, MDI-QKD的安全传输距离大幅增加, 且量子存储退相干效应对最终的密钥生成率影响较小. 但是, 本文没有考虑不对称信道传输率对密钥生成率的影响, 只是理想化假定$e_{\infty}^{z} = e_{\infty}^{x}$以及量子存储A与量子存储B的存储效率相等, 有待进一步研究. 当然, 随着量子存储技术的发展, 我们也可以通过增加量子存储器的级数来提高系统的安全传输距离.

参考文献

[1] Bennet C H, Brassard G 1984 *Proc. IEEE International Conference Computers, Systems, and Signal Processing* Bangalore, India, December 9–12,1984 pp175–179

[2] Shor P W, Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[3] Mayers D 2001 *J. ACM* **48** 351

[4] Gottesman D, Lo H K, Lutkenhaus N, Preskill J 2004 *Quantum Infor. Comput.* **4** 325

[5] Dong C, Zhao S H, Dong Y, Zhao W H, Zhao J 2014 *Acta Phys. Sin.* **63** 170303 (in Chinese) [东晨, 赵尚弘, 董毅, 赵卫虎, 赵静 2014 物理学报 **63** 170303]

[6] Sheng Y B, Zhou L, Cheng W W, Gong L Y, Wang L, Zhan S M 2013 *Chin. Phys. B* **22** 030314

[7] Wang J D, Qin X J, Wei Z J, Liu X B, Liao C J, Liu S H 2010 *Acta Phys. Sin.* **59** 281 (in Chinese) [王金东, 秦晓娟, 魏正军, 刘小宝, 廖常俊, 刘颂豪 2010 物理学报 **59** 281]

[8] Yin Z Q, Han Z F, Chen W, Xu F X, Wu Q L, Guo G 2008 *Chin. Phys. Lett.* **25** 3547

[9] Jiao R Z, Tang S J, Zhang C 2012 *Acta Phys. Sin.* **61** 050302 (in Chinese) [焦荣珍, 唐少杰, 张弼 2012 物理学报 **61** 050302]

[10] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lutkenhaus N, Peev M 2009 *Rev. Mod. Phys.* **81** 1301

[11] Sangouard N, Simon C, Zhao B, Chen Y A, de Riedmateen H, Pan J W, Gisin N 2008 *Phys. Rev. A* **77** 0602301

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

[13] Lloyd S, Shahriar M S, Shapiro J H, Hemmer P R 2001 *Phys. Rev. Lett.* **87** 167903
[14] Razavi M, Shapiro J H 2006 *Phys. Rev. A* **73** 042303
[15] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[16] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[17] Sangouard N, Simon C, de Riedmatten H, Gisin N 2011 *Rev. Modern Phys.* **83** 33
[18] Rubenok A, Slater J A, Chan P, Lucio-Martinez I, Tittle W 2012 arxiv:1204 0738
[19] Liu Y, Chen T Y, Wang L J, Liang H, Shentu G L, Wang J 2012 arXiv:1209 6178
[20] Piparo N L, Razavi M 2012 *The Sixth International Conference on Quantum, Nano and Micro Technologies* Rome, Italy
[21] Panayi C, Razavi M, Ma X F, Norbert L 2013 arXiv:1209 6178
[22] Abruzzo S, Permann H K, Brub D 2013 arXiv:1306 3095v1
[23] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[24] Ma X F, Fung C H F, Razavi M 2012 *Phys. Rev. A* **86** 052305
[25] Ma X F, Razavi M 2012 *Phys. Rev. A* **86** 062319
[26] Abruzzo S, Kampermann H, Brub D 2013 arXiv:1306 3905
[27] Panayi C, Razavi M, Ma X F, Lutkenhaus N 2013 arXiv:1309 3406

Long distance measurement device independent quantum key distribution with quantum memories*

Sun Ying[1)†] Zhao Shang-Hong[1)] Dong Chen[1)2)]

1) (*School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China*)

2) (*Department of Information Security, Xi'an Communication College, Xi'an 710006, China*)

(Received 10 December 2014; revised manuscript received 20 March 2015)

Abstract

We propose a long distance measurement-device-independent (MDI) quantum-key-distribution (QKD) with quantum memory, and analyze the relationship between the key generation rate and the storage efficiency of quantum memory. Our protocol is considered and compared with MDI-QKD without quantum memory. We present general formulas for our protocol with three-intensity decoy states. The simulation results show that the maximum secure distance supported by MDI-QKD with quantum memory is about 500 km, while the maximum secure distance of MDI-QKD without quantum memory is only 216 km. With certain limits, prolonging the time of maintaining the necessary quantum fidelity can increase security key transmission distance. Furthermore, the protocol is robust against device imperfection such as quantum memory decoherence effects, which can be easily applied to practical QKD system.

Keywords: quantum memory, measurement device independent quantum key distribution, decoy state

PACS: 03.67.Dd **DOI:** 10.7498/aps.64.140304

* Project supported by the National Natural Science Foundation of China (Grant No. 61106068).

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