基于量子存储和纠缠光源的测量设备无关量子密钥分配网络

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, 陕西 西安 710077

[2]西安通信学院信息安全系, 陕西 西安 710006

摘要 针对传统量子密钥分配协议安全密钥传输距离较短,难以实现长距离量子保密网的问题,提出了基于量子存储和纠缠光源(EPS)的测量设备无关量子密钥分配协议及其网络模型。比较了直接预报量子存储、非直接预报量子存储与基于EPS的量子存储的优劣,分析了基于量子存储和EPS的测量设备无关量子密钥分配系统中密钥生成率与安全传输距离、存储器量子态保持时间的关系。仿真结果表明,基于EPS的量子存储方案弥补了直接预报量子存储方案需要预报存储器的不足,安全传输距离远高于非直接预报量子存储方案,且当存储器的量子态保持时间 T_1 大于1 ms时,量子密钥生成率基本不再随 T_1 增大而增大。实验中采用双信道两用户网络模型,实际中可通过时分复用器和快速光开关实现单信道多用户的量子密钥分配网络。

关键词 量子光学; 测量设备无关; 量子密钥分配网络; 量子存储; 纠缠光源

中图分类号 O431; TN918 **文献标识码** A

doi: 10.3788/AOS201636.0327001

Measurement Device Independent Quantum Key Distribution Network Based on Quantum Memory and Entangled Photon Sources

Sun Ying[1] Zhao Shanghong[1] Dong Chen[1,2]

[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 The long-distance quantum key distribution network is difficult, since the secure transmission distance of traditional quantum key distribution (QKD) is not long enough. To overcome this problem, A measurement device independent (MDI) QKD protocol based on quantum memories(QM) and entangled photon sources(EPS) is proposed, as well as its network model. And indirectly heralding QM scheme and directly heralding QM with QM scheme based on EPS are compared. The relationships of the key generation rate, secure transmission distance, and hold time of quantum state about MDI-QKD protocol based on QM and EPS are also analyzed. The simulation results show that MDI-QKD based on QM and EPS compensate for the lack of MDI-QKD based on directly heralding QM, which is necessary for heralding QM, and the secure transmission distance is far higher than traditional MDI-QKD and general MDI-QKD based on indirectly heralding QM. Furthermore, once the hold time of quantum state is greater than 1 ms, the key generation rate will be almost invariable. The double-channel and two-user network model are employed. The single-channel and multi-user QKD network can be implemented with time division multiplexer and fast optical switch.

Key words quantum optics; measurement device independent; quantum key distribution network; quantum

收稿日期: 2015-08-28; **收到修改稿日期**: 2015-09-21

基金项目: 国家自然科学基金(61106068)

作者简介: 孙 颖(1991—),男,硕士研究生,主要从事量子信息科学和量子密钥分配等方面的研究。

E-mail: sunyingkgd@163.com

导师简介: 赵尚弘(1964—),男,博士,教授,主要从事空间信息技术和量子信息等方面的研究。

E-mail: zhaoshanghong@aliyun.com(通信联系人)

memory; entangled photon sources

OCIS codes　270.5565; 270.5568; 210.4680; 230.6080

1　引　　言

量子密钥分配[1](QKD)能在通信双方之间实现无条件安全的密钥共享，任何攻击都会因为引入新的误码而被发现[2-3]。基于“点到点”的QKD技术飞速发展，各国的研究小组分别实现了稳定的QKD实验[4-6]，美国的Magi Q公司和瑞士的Id Q公司还分别于2000年和2001年推出了商用化产品。目前，人们开始研究QKD的网络化，已经实现了多个通信节点、多个控制中心环境下的密钥共享网络[7-9]。1995年，Townsend[10]实现了无源光网络上的QKD实验。2004年，波斯顿大学和BBN公司利用标准电信光缆进行通信，实现了6节点的QKD网络[11]。2010年，东京建成了世界上速度最快的QKD网络[12]。2011年，瑞士建成了长期稳定的QKD网络，并成功运行了一年半[13]。2012年，我国建成世界上规模最大的46节点QKD实验网[14]。

传统QKD网络中普遍使用BB84协议，要求用户提供光源、编码器以及高成本的单光子探测器等，非常不利于QKD网络的推广。然而，Lo等[15]在2012年提出的测量设备无关量子密钥分配(MDI-QKD)协议恰好能解决这个问题，并且能移除测量端的所有侧信道漏洞[16-17]。在MDI-QKD系统中，Alice和Bob将光脉冲发送至非可信任第三方进行Bell态测量(BSM)并公布测量结果[18]，Alice和Bob根据基比对结果提取出原始安全密钥。高精度、高成本的单光子探测器和量子存储器都集中在网络的中心节点，用户只需要光源和编码器，极大地降低了用户的成本。MDI-QKD系统的安全密钥传输距离约250 km，高于传统的QKD系统，但仍然难以实现长距离量子保密网。

2013年，Panayi等[19]结合量子中继思想提出在传统MDI-QKD系统的两条信道上各添加一个量子存储器(QM)可以极大地提高安全密钥传输距离，实验仿真表明添加写入时间低于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 μm的量子存储器，安全传输距离超过300 km。在文献[19]的基础上，本文比较了基于直接预报量子存储的MDI-QKD协议与基于非直接预报量子存储的MDI-QKD协议的优劣，提出了基于量子存储和纠缠光源的MDI-QKD协议，分析了其密钥生成率与安全传输距离、量子态保持时间的关系。最后，给出了基于量子存储和纠缠光源的MDI-QKD网络模型，并分析了网络中三次Bell态测量的响应结果与原始密钥提取操作的关系。

2　理论与模型

2.1　基于量子存储的测量设备无关量子密钥分配协议

直接预报量子存储方案如图1所示。

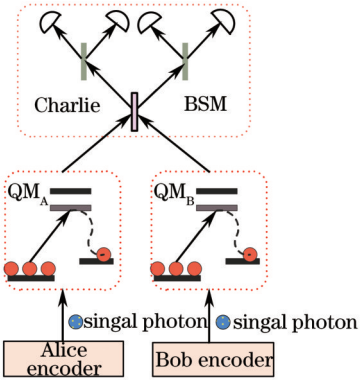

图1　直接预报量子存储方案

Fig.1　Directly heralding QM scheme

Alice和Bob发送的信号光子分别存入量子存储器QM_A和QM_B(存储器均为预报存储器，可预报是否完成存储)，当QM_A与QM_B均完成光子态的写入、存储，第三方Charlie立即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[20]。

$$\begin{cases} R \geqslant \dfrac{1}{<T>}\left\{Q_{11}^{\mathrm{QM}}\left[1-h(e_{11;X}^{\mathrm{QM}})\right]-h(e_{11;Z}^{\mathrm{QM}})\right\} \\ <T> = R_{\mathrm{S}}\dfrac{1}{P_{\mathrm{BSM}}}\dfrac{3-2P_0}{(2-P_0)P_0} \end{cases}, \tag{1}$$

式中 $\frac{1}{<T>}$ 为未进行筛选的原始密钥生成速率。$e_{11;Z}^{\mathrm{QM}}$ 为 Z 基下的单光子误码率，$e_{11;X}^{\mathrm{QM}}$ 为 X 基下的单光子误码率，Q_{11}^{QM} 为单光子增益，$h(x)=x\log(x)-x\log(-x)$ 为二元熵函数。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_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。

直接预报量子存储方案依赖于预报量子存储器，但能预报存储状态的存储器很少，且存储效率普遍非常低[21]。因此，分析了非直接预报存储方案，如图2所示，先对量子存储器 $\mathrm{QM}_{\mathrm{A(B)}}$ 进行抽运，使其产生与存储器产生纠缠的单光子P，然后对单光子P和Alice(Bob)发送来的信号光子进行BSM-1(2)，这样就可以将信号

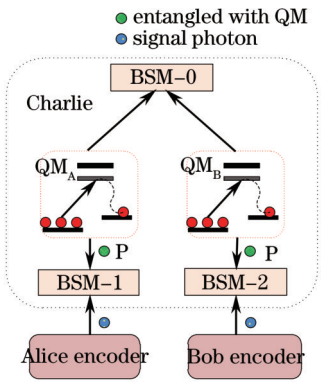

图2 非直接预报量子存储方案

Fig.2 Indirectly heralding QM scheme

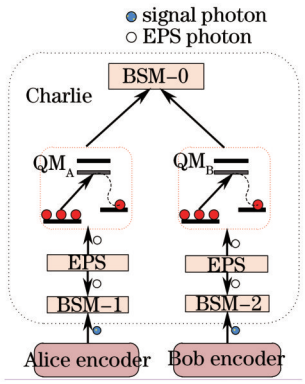

图3 基于EPS的量子存储方案

Fig.3 QM scheme based on EPS

光子的量子态写入 $\mathrm{QM}_{\mathrm{A(B)}}$，且实现了预报功能，克服了需使用预报存储器的不足，之后的密钥提取操作与直接预报量子存储方案相同。

量子存储器与单光子P实现纠缠，则两者的联合态为[19]：

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

式中 $\left|H\right\rangle_{\mathrm{P}}$、$\left|V\right\rangle_{\mathrm{P}}$ 分别为偏振编码的水平态和垂直态，$\left|S_H\right\rangle_{\mathrm{A(B)}}$、$\left|S_V\right\rangle_{\mathrm{A(B)}}$ 为 $\mathrm{QM}_{\mathrm{A(B)}}$ 对应的量子比特。

非直接预报量子存储方案要求QM的存取时间短、存储带宽大、纠缠产生时间短，然而这类QM容易出现多激发态效应[19,22]，产生多个光子，导致BSM-1(2)过程中出现伪成功事件，即BSM-1(2)操作的两个光子都来自信道中的QM，导致BSM测量结果与信号光子没有相关性。另外，QM的长抽运时间也会降低密钥生成率，从而造成非直接预报量子存储MDI-QKD方案的密钥生成率达不到预期效果，反而远低于无QM方案。因此，进一步提出了基于QM和纠缠光源(EPS)的MDI-QKD方案，如图3所示，通过EPS来实现信号光子与QM之间的纠缠，之后的密钥提取操作过程也与图1方案相同。

EPS中多光子部分所占比例较小，特别是基于量子点的EPS，多光子部分基本可以忽略[23]，极大地降低了多激发态效应引入的误码率。考虑到无法分辨光子是否已经存入QM，该方案也不能实现存储状态的完全预报，但纠缠光子在本地产生，写入效率较高[24]，最终引入的误码较少。图2和图3方案的最终密钥生成率为：

$$R_{\mathrm{QM}} \geqslant Y_{11}^{\mathrm{QM}}\left[1-h\left(e_{11;X}^{\mathrm{QM}}\right)-h\left(e_{11;Z}^{\mathrm{QM}}\right)\right], \tag{3}$$

式中 $e_{11;X}^{\mathrm{QM}}$ 和 $e_{11;Z}^{\mathrm{QM}}$ 分别表示Alice与Bob之间 X 基与 Z 基的单光子误码率，Y_{11}^{QM} 为 Z 基下 QM_{A} 与 QM_{B} 完成存取且BSM-0成功的概率，$h(x)$ 表示二元熵函数。

2.2 基于量子存储和EPS的测量设备无关量子密钥分配网络

MDI-QKD系统对用户端设备要求低，非可信任测量端可以作为QKD网络的中心节点，再结合基于EPS的量子存储方案就能实现长距离的QKD网络。为便于分析，图4给出的是双信道两用户的网络模型(PBS为偏振分束器，PM为相位编码器)，但实际中可利用时分复用器和快速光开关实现单信道多用户的QKD网络[25]。

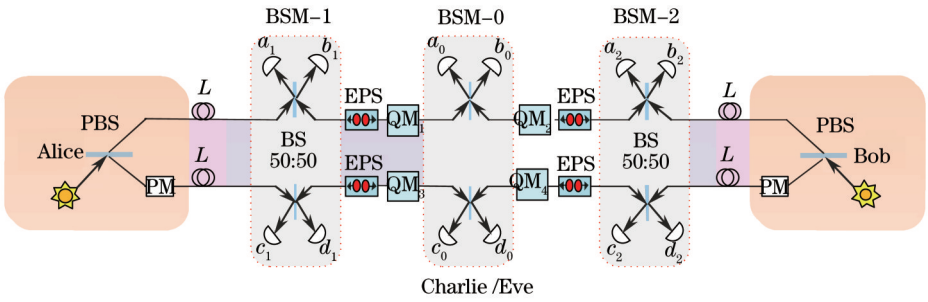

图4 基于量子存储和纠缠光源的测量设备无关量子密钥分配网络

Fig.4 MDI-QKD network based on quantum memories and EPS

如图4所示，高成本的单光子探测器、EPS以及量子存储器都集中在中心节点Charlie(非可信任节点)。Alice和Bob相距 $L=L_{\mathrm{A}}+L_{\mathrm{B}}$，随机的选择编码基 $\{x,z\}$ 和比特 $\{0,1\}$，编码后的信号光子发送至非可信任中心节点，本地EPS产生纠缠光子对，其中一个光子与来自Alice(Bob)的信号光子进行BSM-1(2)，另一个光子写入量子存储器，从而实现信号光子与量子存储器之间的纠缠，然后立即提取量子存储器中的光子进行BSM-0。一旦三次BSM都成功，Alice和Bob就能够提取原始密钥。如表1(Type Ⅰ：a_i 和 c_i 或者 b_i 和 d_i 正常响应，$i=0,1,2$；Type Ⅱ：a_i 和 d_i 或者 b_i 和 c_i 正常响应，$i=0,1,2$。)所示，给出了Charlie/Eve处三次BSM的响应结果与Bob对应的比特反转操作。

表1 三次BSM响应结果与对应的比特反转操作

Table 1 Click result of three BSM and operation of bit flip

Basic	BSM-1	BSM-2	BSM-0	Bit assignment
Z	Type Ⅰ/Ⅱ	Type Ⅰ/Ⅱ	Type Ⅰ/Ⅱ	Bob flips bit
X	Type Ⅰ(Ⅱ)	Type Ⅰ(Ⅱ)	Type Ⅰ	Bob keeps bit
X	Type Ⅰ(Ⅱ)	Type Ⅰ(Ⅱ)	Type Ⅱ	Bob flips bit
X	Type Ⅰ(Ⅱ)	Type Ⅱ(Ⅰ)	Type Ⅰ	Bob flips bit
X	Type Ⅰ(Ⅱ)	Type Ⅱ(Ⅰ)	Type Ⅱ	Bob keeps bit

由于纠缠光子对的产生具有随机性，与Alice(Bob)发送的信号光子的同步要求难以得到保证。因此，如图5所示，考虑在下一步研究中将图4中的纠缠光源与量子存储器重现组合构成一个按需读取的纠缠光源，由协议的第三方Charlie从QM提取光子，与来自Alice和Bob的信号光子进行BSM，从而解决纠缠光子对与Alice和Bob传输的光子无法保持同步的问题。

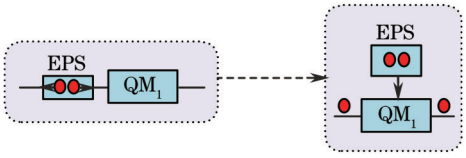

图5 基于量子存储的按需读取纠缠光源

Fig.5 Read-on-demand EPS based on QM

3 仿真结果与分析

结合文献[17]可得到 Z 基单光子计数率 $Y_{11;Z}^{\mathrm{QM}}$，X 基单光子误码率 $e_{11;X}^{\mathrm{QM}}$ 以及原始密钥生成速率 $\frac{1}{<T>}$。Z 基全局计数率 Y_{11}^{QM} 和全局单光子增益 Q_{11}^{QM} 可在实验中测得，再联合(1)式和(3)式可得到基于不同量子存储方案的MDI-QKD系统的密钥生成率 R_{QM} 与安全传输距离 L 的关系以及部分参数对MDI-QKD网络的影响。

表2 主要仿真参数

Table 2 Main simulation parameters

Ref.[19]	T_1	τ_w	P_D	α	η_{r_0}	f
	0.15ms	1ns	10^{-9}	0.17	0.73	1.16

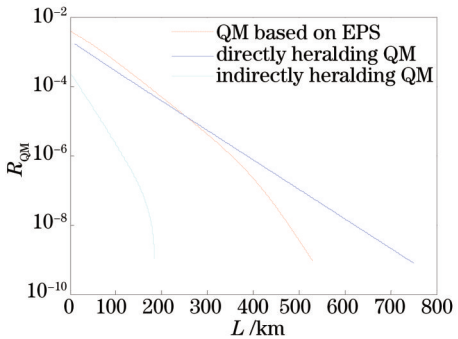

图6 基于不同量子存储方案的密钥生成率与安全传输距离

Fig.6 Key generation rates and secure transmission distances based on different QM schemes

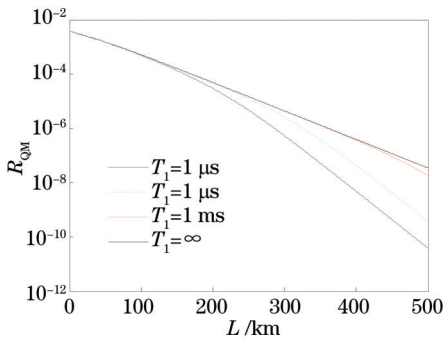

图7 基于不同量子态保持时间的密钥生成率与安全传输距离

Fig.7 Key generation rates and secure transmission distances based on different T_1

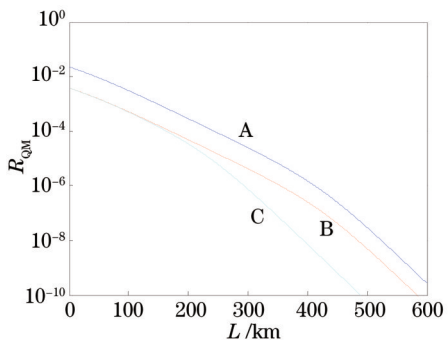

图8 不同参数组合下的密钥生成率与安全传输距离

Fig.8 Key generation rates and secure transmission distances with different parameters

如图6所示，基于直接预报量子存储的MDI-QKD系统的安全传输距离高达750 km，是因为只有一次BSM操作，降低了误码率，但该系统中使用的预报量子存储器种类比极少，且存储效率普遍较低；基于非直接预报量子存储的MDI-QKD系统中存在多激发态效应，会带来较多误码，其系统的安全传输距离仅190 km，远低于无量子存储的传统MDI-QKD系统；基于量子存储和EPS的MDI-QKD系统的安全传输距离约520 km，克服了多激发态效应，无需预报存储器。

如图7所示，在一定范围内，基于量子存储和EPS的MDI-QKD系统的密钥生成率 R_{QM} 与存储器的量子态保持时间 T_1 成正比，T_1 会影响存储器的读取效率，最后影响系统的密钥生成率。但从 $T_1=1$ ms 和 $T_1=\infty$ 两条曲线可以看出，量子态保持时间的增大并不能无限提高系统的密钥生成率，当 $T_1\geqslant 1$ ms，密钥生成率基

本不再变化。

如图8所示，系统采用三组不同的器件参数，其密钥生成率与安全传输距离如曲线A、B、C所示，曲线A：$T_1=150\ \mu s$, $\eta_{r_0}=0.73$ 为存储器的量子态起始读取效率[26]；曲线B：$T_1=150\ \mu s$, $\eta_{r_0}=0.3$；曲线C：$T_1=1.5\ \mu s$, $\eta_{r0}=0.3$ [27]。三种情况都采用效率为12%的EPS[28]，量子存储器写入时间 τ_w 为1ns，光源脉冲频率为1GHz[29]，信道衰耗 α 为0.17 dB/km。说明基于量子存储和EPS的长距离MDI-QKD网络完全可以实现。

4 结 论

研究了基于直接预报量子存储和非直接预报量子存储的MDI-QKD协议，提出了基于量子存储和EPS的MDI-QKD协议及其网络模型，分析了网络中三次Bell态测量的响应结果与原始密钥提取操作的关系。仿真结果表明基于量子存储和EPS的MDI-QKD协议的安全传输距离约520 km，远高于非直接预报存储器方案的190 km，弥补了直接预报存储方案需要预报存储器的不足；当存储器的量子态保持时间 T_1 大于1 ms时，基本不再影响系统的密钥生成率；原子系综存储器[14]和基于量子点的EPS完全可以满足MDI-QKD网络的要求。因此，基于量子存储和EPS的长距离MDI-QKD网络具有很好的发展前景。

参 考 文 献

1 C H Bennett, G Brassard. Quantum cryptography: public key distribution and coin tossing[C]. Theoretical Computer Science, 2014, 560 (1): 7-11.

2 Zhu Feng, Wang Qin. Quantum key distribution protocol based on heralded single photon source[J]. Acta Optica Sinica, 2014, 34(6): 0627002.
朱 峰, 王 琴. 基于指示单光子源的量子密钥分配协议[J]. 光学学报, 2014, 34(6): 0627002.

3 Inamori H, Lütkenhaus N, Mayers D. Unconditional security of practical quantum key distribution[J]. European Physical Journal D, 2007, 41(3): 599-627.

4 Davide B, Matteo C, Nicola L, *et al*.. Experimental quantum key distribution with finite-key security analysis for noisy channels[J]. Nature Communications, 2013, 4(9): 275-289.

5 Sun Q C, Wang W L, Liu Y, *et al*.. Experimental passive decoy-state quantum key distribution[J]. Laser Physics Letters, 2014, 11(8): 085202.

6 Hiskett P A, Rosenberg D, Peterson C G, *et al*.. Long-distance quantum key distribution in optical fibre[J]. New J Phys, 2006, 8(17): 4529-4532.

7 Chapuran T E, Toliver P, Peters N A, *et al*.. Optical networking for quantum key distribution and quantum communications[J]. New J Phys, 2009, 11(11): 105001.

8 Fu Y, Yin H L, Chen T Y, *et al*.. Long-distance measurement-device-independent multiparty quantum communication[J]. Phys Rev Lett, 2015, 114(9): 090501.

9 Chen T Y, Wang J, Liang H, *et al*.. Metropolitan all-pass and inter-city quantum communication network[J]. Opt Express, 2010, 18(26): 27217-27255.

10 Townsend P D. Experimental investigation of the performance limits for first telecommunications-window quantum cryptography systems [J]. IEEE Photonics Technology Letters, 1998, 7(10): 1048-1050.

11 Chip Elliott, Alexander Colvin, Davin Pearson, *et al*.. Current status of the DARPA quantum network[C]. SPIE, 2005, 5815: 138-149.

12 Sasaki M, Fujiwara M, Ishizuka H, *et al*.. Field test of quantum key distribution in the tokyo QKD network[J]. Opt Express, 2011, 19(11): 10387-10409.

13 Stucki D, Legre M, Buntschu F, *et al*.. Long term performance of the Swiss quantum key distribution network in a field environment[J]. New J Phys, 2011, 13(12): 123001.

14 Wang S, Chen W, Yin Z Q, *et al*.. Field and long-term demonstration of a wide area quantum key distribution network[J]. Quantum Physics, 2014, 2(18): 21739-21756.

15 Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution[J]. Phys Rev Lett, 2012, 108(13): 130503.

16 Rubenok A, Slater J A, Chan P, *et al*.. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks[J]. Phys Rev Lett, 2013, 111(13): 130501.

17 Liu Y, Chen T Y, Wang L J, *et al*.. Experimental measurement-device-independent quantum key distribution[J]. Phys Rev Lett, 2013, 111(13): 130502.

18 Liang W Y, Li M, Yin Z Q, *et al*.. Simple implementation of quantum key distribution based on single-photon Bell-state measurement [J]. Phys Rev A, 2015, 92(1): 012319.

19 Panayi C, Razavi M, Ma X, *et al*.. Memory-assisted measurement-device-independent quantum key distribution[J]. New J Phys, 2014, 16(4): 043005.

20 Sun Ying, Zhao Shanghong, Dong Chen. Long distance measurement device independent quantum key distribution based on quantum memories[J]. Acta Physica Sinica, 2015, 64(14): 140304.
孙 颖, 赵尚弘, 东 晨. 基于量子存储的长距离测量设备无关量子密钥分配研究[J]. 物理学报, 2015, 64(14): 140304.

21 Stute A, Casabone B, Schindler P, *et al*.. Tunable ion-photon entanglement in an optical cavity[J]. Nature, 2012, 485(7399): 482-485.

22 Razavi M, Shapiro J H. Long-distance quantum communication with neutral atoms[J]. Phys Rev A, 2006, 73(4): 042303.

23 Muller M, Bounouar S, Jons K D, *et al*.. On demand generation of indistinguishable polarization-entangled photon pairs[J]. Nature Photonics, 2014, 8(3): 224-228.

24 Chen Y H, Lee M J, Wang I C, *et al*.. Coherent optical memory with high storage efficiency and large fractional delay[J]. Phys Rev Lett, 2013, 110(8): 083601.

25 Ma X, Razavi M. Alternative schemes for measurement-device independent quantum key distribution[J]. Phys Rev A, 2012, 86(6): 062319.

26 Dousse A, Suffczynski J, Krebs O, *et al*.. A quantum dot based bright source of entangled photon pairs operating at 53 K[J]. Appl Phys Lett, 2010, 97(8): 081104.

27 Bao X H, Reingruber A, Dietrich P, *et al*.. Efficient and long-lived quantum memory with cold atoms inside a ring cavity[J]. Nat Phys, 2012, 8(7): 517-521.

28 Reim K F, Michelberger P, Lee K C, *et al*.. Single-photon-level quantum memory at room temperature[J]. Phys Rev Lett, 2011, 107(5): 053603.

29 Saglamyurek E, Sinclair N, Slater J A, *et al*.. An integrated processor for photonic quantum states using a broadband light-matter interface [J]. New J Phys, 2014, 16(6): 065019.

栏目编辑：刘丰瑞