基于指示单光子源和量子存储的量子密钥分配

何业锋[1,2], 王登[1,2*], 杨红娟[2], 宋畅[2], 李东琪[2]

[1]西安邮电大学无线网络安全技术国家工程实验室, 陕西 西安 710121;

[2]西安邮电大学通信与信息工程学院, 陕西 西安 710121

摘要 提出一种基于指示单光子源和量子存储的量子密钥分配方案。分析了其密钥生成率与安全传输距离和量子存储时间的关系,以及量子存储的退相干效应对最终密钥生成率的影响。研究了量子存储对基于指示单光子源的测量设备无关量子密钥分配方案的影响。仿真结果表明,在指示单光子源下,量子存储的实际相干时间增加,使得系统的安全传输距离增大,且量子退相干效应对最终的密钥生成率的影响微弱。

关键词 量子光学; 量子密钥分配; 测量设备无关; 指示单光子源; 量子存储

中图分类号 TN918 **文献标识码** A **doi**: 10.3788/CJL201946.0412001

Quantum Key Distribution Based on Heralded Single Photon Sources and Quantum Memory

He Yefeng[1,2], Wang Deng[1,2*], Yang Hongjuan[2], Song Chang[2], Li Dongqi[2]

[1]*National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi* 710121, *China*;

[2]*School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi* 710121, *China*

Abstract A quantum key distribution scheme based on heralded single photon sources and quantum memory is studied. The relationship between key generation rate and safe transmission distance and storage time is analyzed, and the effect of decoherence effect of quantum memory on the final key generation rate is analyzed. The influence of quantum memory on measurement-device-independent quantum key distribution scheme based on heralded single photon sources is studied. The simulation results show that under heralded single photon sources, the increase of the actual coherence time of the quantum memory makes the safe transmission distance of the system increase, and the quantum decoherence effect has a weak influence on the final key generation rate.

Key words quantum optics; quantum key distribution; measurement-device-independent; heralded single photon sources; quantum memory

OCIS codes 270.5565; 270.5568; 270.3430; 270.1670

1 引 言

量子密钥分配(QKD)可以实现无条件安全的量子密钥分发,在量子通信领域具有重要作用。1984 年,Bennett 等[1]提出了著名的量子密钥分配协议"BB84 协议",之后在理论研究和实验探索方面,都取得了一系列丰硕的量子密钥分配相关成果[2-4]。然而在实际系统中,光源和探测设备的不完善性,使得量子密钥分配存在一些安全漏洞,从而招致多种类型的攻击:部分随机相位攻击[5]、光子数分离攻击[6]、时移攻击[7]、探测器控制攻击[8-9]和探测器致盲攻击[10]等。为解决探测器的不完善性问题,2012 年,Lo 等[11]提出了一种测量设备无关量子密钥分配(MDI-QKD)协议,该方案的优点是可以解决探测器漏洞问题。正是因为拥有如此良好的性能,MDI-QKD 协议成为后来的热门研究[12-17]。然而,在 MDI-QKD 系统中,单边信道传输损耗会限制安全传输距离,为满足长距离量子密钥分配的需求,添

收稿日期: 2018-11-20; **修回日期**: 2018-12-05; **录用日期**: 2018-12-21

基金项目: 国家自然科学基金(61802302,61472472,61772418)、陕西省自然科学基础研究计划(2017JM6037)

* **E-mail**: 1325703108@qq.com

加量子存储器(QM)成为很好的选择。2013 年,Abruzzo 等[18]探讨了在无纠缠光源的情况下实现长距离量子密钥分配的可能性,提出的 MDI-QKD 方案使用了量子存储方案和诱骗态协议,安全传输距离可达 500 km 以上。2016 年,孙颖等[19]提出一种基于量子存储和纠缠光源(EPS)的 MDI-QKD 方案,仿真结果显示安全传输距离约为 520 km。

在实际应用中,理想单光子源的制备十分困难,可以用来替代的有弱相干态(WCS)光源和奇相干态(OCS)光源等。事实上,采用弱相干光源时,空脉冲和多光子脉冲的存在会减小密钥生成率。与弱相干光源相比,奇相干态光源的光子数分布服从亚泊松分布,单光子脉冲的比率增大,最大安全传输距离得以提升。何业锋等[20]研究了基于奇相干光源和轨道角动量的量子密钥分配协议,进一步提高了密钥生成率。之后,文献[21-22]提出的 MDI-QKD 方案使用了指示单光子源(HSPS)。文献[23]分析了基于指示单光子源的 MDI-QKD 协议,得到了密钥生成率与安全传输距离之间的关系。何业锋等[24]研究了非对称信道下基于指示单光子源的 MDI-QKD 协议的密钥生成率。周媛媛等[25]研究了指示单光子源条件下的 MDI-QKD 方案,结合三强度诱骗态理论,通过数值模拟,推导出了密钥生成率下限和误码率上限,并对其性能进行了分析。

本文在基于指示单光子源的 MDI-QKD 方案基础上添加了量子存储单元,通过脉冲转发来实现长距离的安全传输。通过仿真模拟有关密钥生成率的曲线,分析其与量子存储时间及安全传输距离之间的关系,并对其性能参数进行评估。

2　基本原理

2.1　指示单光子源

指示单光子源一共产生两种模式的光子:休闲光子和信号光子。指示单光子源的光子数分布为 $P_n=[1-(1-P_d)(1-\eta_d)^n]\cdot[I^n/(1+I)^{n+1}]$,式中:$P_d$ 和 η_d 分别表示探测器的探测效率和暗计数率,I 表示信号态的光强,n 为光子数。在同一光强下,弱相干光源和指示单光子源的光子数分布如表 1 所示[26],光源的平均光子数为 0.5。

表 1　不同光源的光子数比较

Table 1　Comparison of photon numbers of different light sources

Source	Single photon	Multi-photon
WCS	0.3033	0.0902
HSPS	0.7274	0.2726

2.2　基于量子存储和指示单光子源的 MID-QKD 方案模型

基于量子存储的 HSPS-MID-QKD 结构图如图 1 所示,其中,Alice 和 Bob 为通信双方,Charlie 为可以不受信任的第三方,PBS 为偏振分束器,BS 为 50∶50 分束器,Pol-M 为偏振调制器,IM 为强度调制器,QM-A、QM-B 分别为 A、B 两个量子存储器,1H、2H、1V 和 2V 分别为单光子探测器的编号,a 和 b 分别为 Alice 端和 Bob 端的触发探测器编号。引入量子存储的 HSPS-MDI-QKD 系统建立密钥的过程如下。

1) Alice 和 Bob 分别独立地制备自己的纠缠光子对,纠缠光子对首先通过偏振分束器,探测器探测纠缠光子对中的休闲光子,并根据探测结果,每探测到一个休闲光子,就发射一个信号光子给 Charlie,用来预测休闲光子的到达时间;另一方面将每个信号光子作为指示信号,随后被独立随机地编码在两组基(x 基或 z 基,x 基是作为估计信道参数的测试基,z 基则用来产生安全密钥)组成的 4 个偏振态($|\leftrightarrow\rangle$、$|\updownarrow\rangle$、$|\nearrow\rangle$、$|\nwarrow\rangle$)其中的一个态上,然后发送给 Charlie。

2) 信号光子经过 IM,将 Alice 和 Bob 的光脉冲随机制备成三种强度的光子 μ_i,ν_j:

$$\begin{cases}\{\mu_i\}_i=0,1,2\\ \{\upsilon_j\}_j=0,1,2\end{cases},\tag{1}$$

式中:$i(j)=0,1,2$,分别对应真空态、诱骗态和信号态,真空态光强为零,信号态光强大于诱骗态光强。

3) 在第三方进行贝尔态测量(BSM)前,Alice 和 Bob 发送的脉冲信号分别送入量子存储器 QM-A 和 QM-B,进行光子偏振态与存储量子比特的转化[27]:$\frac{1}{\sqrt{2}}[|S_H\rangle_{A(B)}|H\rangle_P+|S_V\rangle_{A(B)}|V\rangle_P]$,式中 $|H\rangle_P$、$|V\rangle_P$ 分别为偏振编码中的水平态和垂直态,$|S_H\rangle_{A(B)}[|S_V\rangle_{A(B)}]$为 Alice(Bob)的单模量子存储器 A(B)所对应的量子比特。

4) Charlie 对 Alice 和 Bob 发送的光脉冲进行 BSM,随后公布成功的测量结果:单侧探测器(即 D_{1H} 与 D_{1V},或 D_{2H} 与 D_{2V})同时响应,表明探测到 $|\psi^+\rangle$ 态;双侧探测器(D_{1H} 和 D_{2V},或 D_{2H} 和 D_{1V})同时响应,表明探测到 $|\psi^-\rangle$ 态。其中,$|\psi^\pm\rangle=\frac{1}{\sqrt{2}}(|\updownarrow\rangle|\leftrightarrow\rangle\pm|\leftrightarrow\rangle|\updownarrow\rangle)$,$|\leftrightarrow\rangle$、$|\updownarrow\rangle$分别表示水平和竖直偏振态。

5) 对照表 2,Alice 和 Bob 对探测到的成功结果进行比特翻转操作,再将筛选后的结果进行保密

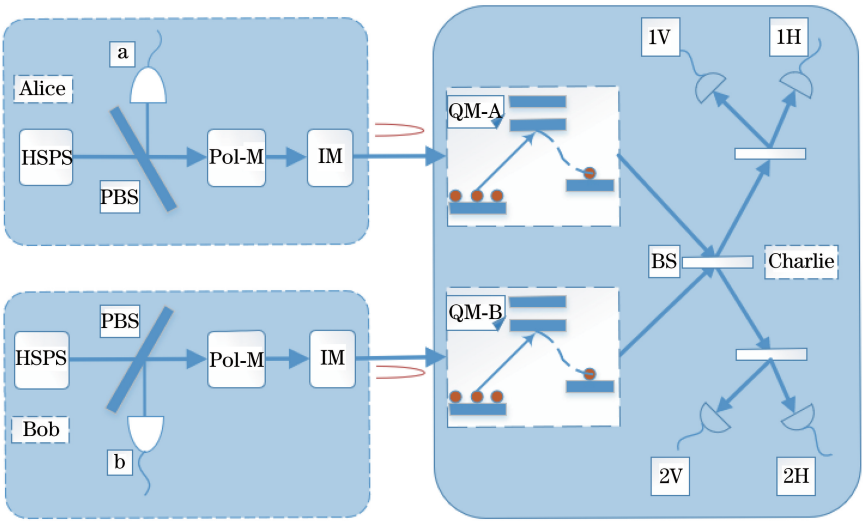

图 1　基于量子存储的 HSPS-MID-QKD 结构图

Fig. 1　HSPS-MID-QKD structure diagram based on quantum memory

表 2　比特翻转操作列表

Table 2　Bit-flip operation list

Base	Project on $\|\psi^+\rangle$	Project on $\|\psi^-\rangle$
z	Bit-flip	Bit-flip
x	No change	Bit-flip

加强处理，由此可获得最终的安全密钥。

2.3　密钥生成率

由文献[18]可知，最终安全密钥生成率可表示为

$$R_{\mathrm{QM}} \geqslant \frac{1}{\langle T\rangle}\{Q_{11}^{\mathrm{QM}}[1-H(e_{11}^{x})]-H(e_{11}^{z})\}, \tag{2}$$

式中：Q_{11}^{QM} 表示全局单光子增益；e_{11}^{x} 和 e_{11}^{z} 分别表示 x 基和 z 基下的单光子误码率；$H(\cdot)$ 表示二进制香农函数，$H(y)=-y\log_2(y)-(1-y)\log_2(1-y)$；$1/\langle T\rangle$ 为未进行筛选的原始安全密钥生成率：

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

式中：R_{s} 为脉冲发送的频率；P_0 为光子成功存储的概率，$P_0=\sum_{n=1}^{\infty}P_n[1-(1-\eta_{\mathrm{T}})^n]$，$\eta_{\mathrm{T}}=10^{-\frac{\alpha L}{2.10}}$，$L$ 为传输距离，α 为光纤耗损率；P_{BSM} 为第三方进行成功 BSM 的概率[18]：

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

式中：$\eta_{\mathrm{MD}}=\eta_{\mathrm{M}}\eta_{\mathrm{D}}$，$\eta_{\mathrm{M}}$ 为量子存储效率，η_{D} 为探测器效率，P_{D} 为探测器探测成功的概率。

假设 Alice 和 Bob 发送光强分别为 μ 和 v 的光脉冲，其总增益 $Q_{\mu\nu}$ 和和量子误码率 $E_{\mu\nu}$ 则可分别表示为

$$Q_{\mu\nu}^{w}=\sum_{n,m=0}^{\infty}\frac{\mu^n v^m}{(1+\mu)^{n+1}(1+v)^{m+1}}\eta_{r_{\mathrm{A}}}\eta_{r_{\mathrm{B}}}Y_{nm}^{w}, \tag{5}$$

$$E_{\mu\nu}^{w}Q_{\mu\nu}^{w}=\sum_{n,m=0}^{\infty}\frac{\mu^n v^m}{(1+\mu)^{n+1}(1+v)^{m+1}}\eta_{r_{\mathrm{A}}}\eta_{r_{\mathrm{B}}}e_{nm}^{w}Y_{nm}^{w}, \tag{6}$$

式中：$w=x,z$ 表示采用 x 基或 z 基进行编码；Y_{nm}^{w} 为 Alice 发送 n 个光子脉冲，Bob 发送 m 个光子脉冲时 BSM 获得成功的概率；e_{nm}^{w} 为相应的误码率；$Q_{\mu\nu}^{11}$ 为探测器 a 和 b 全都响应时的增益；$E_{\mu\nu}^{11}Q_{\mu\nu}^{11}$ 为相应的误码率；r_{A} 和 r_{B} 为 Alice 和 Bob 的探测结果。

只考虑对称信道的情况，在指示单光子源的条件下，由(5)式可得到全局单光子增益：

$$Q_{11}^{\mathrm{QM}}=\frac{\mu v}{(1+\mu)^2(1+v)^2}Y_{11}^{w}, \tag{7}$$

式中：Y_{11}^{w} 表示单光子增益下界[25]，满足

$$Y_{11}^{w}\geqslant\frac{g_1+g_2+g_3-(1+\mu_2)(1+v_2)Q_{\mu_2v_2}^{1,1}+(1+\mu_1)(1+v_1)Q_{\mu_1v_1}^{1,1}}{\frac{\kappa\mu_2v_1\eta_{\mathrm{d}}^2}{(1+\mu_2)(1+v_1)}+\frac{\kappa\mu_1v_2\eta_{\mathrm{d}}^2}{(1+\mu_1)(1+v_2)}-\frac{\kappa\mu_2v_2\eta_{\mathrm{d}}^2}{(1+\mu_2)(1+v_2)}+\frac{\kappa\mu_1v_1\eta_{\mathrm{d}}^2}{(1+\mu_1)(1+v_1)}}, \tag{8}$$

式中：$\kappa=\min\{a,b,c\}$，a，b，c 可分别表示为

$$\begin{cases} a=\dfrac{u_2v_2^2(1+u_1)(1+v_1)^2-u_1v_1^2(1+u_2)(1+v_2)^2}{u_2v_1^2(1+u_1)(1+v_2)^2+u_1v_2^2(1+u_2)(1+v_1)^2}\geqslant 0 \\ b=\dfrac{u_2^2v_2(1+u_1)^2(1+v_1)-u_1^2v_1(1+u_2)^2(1+v_2)}{u_2^2v_1(1+u_1)^2(1+v_2)+u_1^2v_2(1+u_2)^2(1+v_1)}\geqslant 0 \\ c=\dfrac{u_2^2v_2^2(1+u_1)^2(1+v_1)^2-u_1^2v_1^2(1+u_2)^2(1+v_2)^2}{u_2^2v_1^2(1+u_1)^2(1+v_2)^2+u_1v_2^2(1+u_2)^2(1+v_1)^2}\geqslant 0 \end{cases}, \tag{9}$$

g_1，g_2，g_3 可表示为

$$\begin{cases} g_1=(1+v_2)Q_{0v_2}^{1,1}-(1+v_1)Q_{0v_1}^{1,1}+(1+u_2)Q_{u_20}^{1,1}-(1+u_1)Q_{u_10}^{1,1}-Q_{00}^{1,1} \\ g_2=\kappa[(1+u_2)(1+v_1)Q_{u_2v_1}^{1,1}-(1+v_1)Q_{0v_1}^{1,1}-(1+u_2)Q_{u_20}^{1,1}+Q_{00}^{1,1}] \\ g_3=\kappa[(1+u_1)(1+v_2)Q_{u_1v_2}^{1,1}-(1+v_2)Q_{0v_2}^{1,1}-(1+u_1)Q_{u_10}^{1,1}+Q_{00}^{1,1}] \end{cases}。 \tag{10}$$

为了更好地描述量子存储器的最小退相干时间与量子密钥分配距离之间的关系，本研究引用了文献[18]的量子退相干模型，该模型中定义了一个时间 τ，存储器可以在 τ 时间内完美地保留量子态，当存储时间 $t>\tau$ 时，量子态就会发生失真。量子存储器中量子态的保真度可以始终保持在一个确定的时间内，而它超过这个时间时，保真度将会急剧下降。这里，τ 描述的是量子存储器的退相干时间，它也是衡量量子存储器性能优劣的一个重要参数。

x 基下单光子误码率 e_{11}^x 可表示为

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

z 基下单光子误码率 e_{11}^z 可表示为

$$e_{11}^z=e_\infty^z+\frac{1}{2}\cdot\frac{(1/2-e_\infty^z)(1-P_0)^{1+\tau}}{2-P_0}。 \tag{12}$$

量子退相干时间趋于无穷时的误码率 e_∞^w 的表示式为

$$e_\infty^w=\frac{2P_D[2(\eta_{MD}-1)^2P_D-(\eta_{MD}-2)\eta_{MD}]}{\eta_{MD}^2+8(\eta_{MD}-1)^2P_D^2+2(4-3\eta_{MD})\eta_{MD}P_D}。 \tag{13}$$

在 HSPS-MDI-QKD 系统中添加量子存储器，相当于在传输信道上设立中继装置，存储再转发的操作，能降低信道传输损耗对 BSM 的影响，增大 BSM 成功的概率，从而可增长系统的安全传输距离。然而，量子退相干效应引起的误码率不可避免，如果量子比特错误率太大，则无法提取量子密钥。对于诱骗态量子密钥分发协议，最大误码率 e^{max} 的常用值为 0.11，根据参考文献[18]可得到该退相干时间的下限 τ_{HSPS}^{min}：

$$\tau_{HSPS}^{min}=\frac{\log_2\left[\dfrac{(P_0-2)(e_\infty^w-e^{max})}{(P_0-1)(2e_\infty^w-1)}\right]}{\log_2(1-P_0)}。 \tag{14}$$

3　仿真结果与分析

测量设备是完全对称的，即有 $e_{11}^x=e_{11}^z$，又因为量子存储过程只进行光子态到量子比特的转化，不会造成新的误码，所以趋于无穷时就有 $e_\infty^x=e_\infty^z=e_\infty^w$。将(13)式代入(11)式或(12)式，可得到单光子误码率 e_{11}^w，再将 e_{11}^w 与(3)式、(7)式一同代入(2)式，便得到最终的密钥生成率 R_{QM}。实验中取光强 $\mu_1=v_1=0.1$，$\mu_2=v_2=0.36$，主要仿真参数如表 3 所示[18]。

表 3　主要仿真参数

Table 3　Main simulation parameters

Parameter	e_0	e_d	P_D	η_M	η_D
Value	0.5	1.5%	10^{-6}	0.6	0.2

系统的安全传输距离与最小退相干时间的关系如图 2 所示，Δt 为最小退相干时间差值。在距离小于 300 km 时，安全传输距离呈现平稳缓慢增长状态，此期间量子存储器的作用体现不明显；但在距离大于 300 km 后，安全传输距离呈迅速增长状态，说明此时经典系统的传输能力受到限制，需要借助量子存储器的存储再转发操作，提升 MDI-QKD 系统的安全传输距离。如果量子存储器能较长时间地存

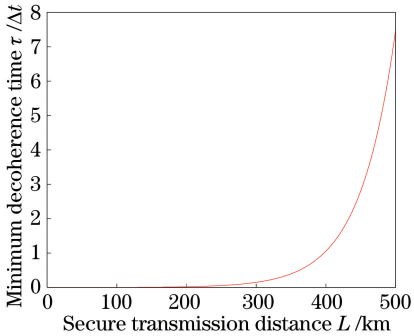

图 2　安全传输距离与最小退相干时间的关系曲线

Fig. 2　Secure transmission distance versus minimum decoherence time

储量子比特，就能达到长距离量子密钥分配的目的。

密钥生成率曲线如图 3 所示，横坐标是实际的量子退相干时间 τ 与最小退相干时间 $\tau^{\min}$ 的比值，纵坐标是密钥生成率，显然这个比值越大，量子退相干过程需要的时间就越久，也就能保证量子存储器更长时间地承载量子态，为存储再转发提供了可能，达到长距离量子密钥分配的目的。由图 3 可知，随着量子退相干时间的不断增加，密钥生成率也在逐渐增加，验证了本研究的预测；然而，当 $\tau \geqslant 6\tau^{\min}$ 时，曲线突然变得平直且无上升趋势，即密钥生成率不再增加，由此可知通过提升量子存储器的存储时间也还是不能无限地增大密钥生成率。

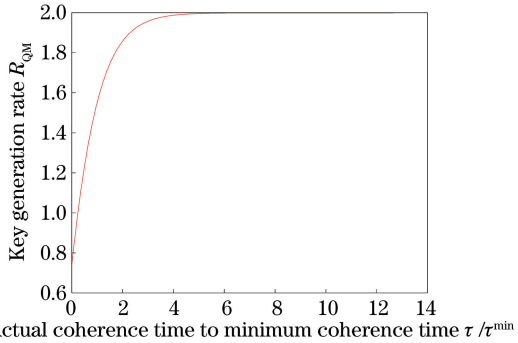

图 3　密钥生成率曲线

Fig. 3　Curve of key generation rate

三种情形下的密钥生成率与安全传输距离的仿真关系曲线如图 4 所示。就基于量子存储的方案和无量子存储的方案来说，无量子存储的 MDI-QKD 系统的安全传输距离仅为 300 km，而在信道上设置量子存储器后，MDI-QKD 系统的安全传输距离可超过400 km；另一方面，在基于量子存储的 MDI-QKD 方案中，量子退相干时间 $\tau=2\tau^{\min}$ 与 $\tau=\infty$ 时，二者的密钥生成率曲线几乎已经重合，说明量子退相干效应对最终的密钥生成率几乎无影响。

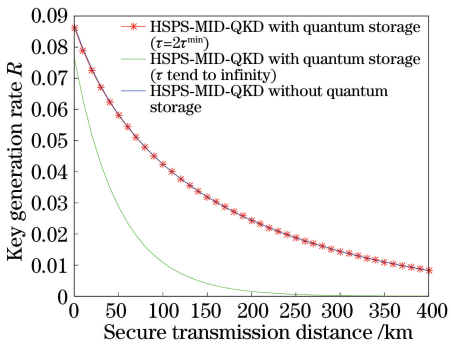

图 4　密钥生成率与安全传输距离关系曲线

Fig. 4　Key generation rate versus secure transmission distance

4　结　　论

将量子存储技术应用于基于指示单光子源的 MDI-QKD 方案中，通过仿真模拟了安全传输距离、量子存储时间与密钥生成率之间的关系。仿真结果表明，若量子存储器能较长时间地保留所存储的量子比特，系统的安全传输距离就会得到一定程度的增大，于是要求量子存储器具有较长的相干时间。同时，与无量子存储的 MDI-QKD 方案进行比较，使用量子存储技术，可以实现较远距离的量子密钥分配，且量子存储退相干效应对最终的密钥生成率的影响微弱。然而在实际通信中，信道往往会存在非对称的情形，对此还有待进一步的研究。

参　考　文　献

[1] Bennett C H, Brassard G. An update on quantum cryptography [M] // Blakley G R, Chaum D. Advances in Cryptology. Berlin, Heidelberg: Springer, 1984: 475-480.

[2] Bennett C H. Quantum cryptography using any two nonorthogonal states [J]. Physical Review Letters, 1992, 68(21): 3121-3134.

[3] Liu Y M, Wang C, Huang D, *et al*. Study of synchronous technology in high-speed continuous variable quantum key distribution system [J]. Acta Optica Sinica, 2015, 35(1): 0106006.
刘友明, 汪超, 黄端, 等. 高速连续变量量子密钥分发系统同步技术研究[J]. 光学学报, 2015, 35(1): 0106006.

[4] Zhu Q L, Shi L, Wei J H, *et al*. Background light suppression in free space quantum key distribution [J]. Laser & Optoelectronics Progress, 2018, 55(6): 060004.
朱秋立, 石磊, 魏家华, 等. 自由空间量子密钥分配的背景光抑制[J]. 激光与光电子学进展, 2018, 55(6): 060004.

[5] Sun S H, Liang L M. Experimental demonstration of an active phase randomization and monitor module for quantum key distribution [J]. Applied Physics Letters, 2012, 101(7): 071107.

[6] Lydersen L, Skaar J, Makarov V. Tailored bright illumination attack on distributed-phase-reference protocols[J]. Journal of Modern Optics, 2011, 58(8): 680-685.

[7] Zhao Y, Fung C H F, Qi B, *et al*. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems [J]. Physical Review A, 2008, 78(4): 042333.

[8] Thomas O, Yuan Z L, Dynes J F, *et al*. Efficient

photon number detection with silicon avalanche photodiodes[J]. Applied Physics Letters, 2010, 97(3): 031102.

[9] Gerhardt I, Liu Q, Lamas-Linares A, *et al*. Full-field implementation of a perfect eavesdropper on a quantum cryptography system [J]. Nature Communications, 2011, 2: 349.

[10] Makarov V, Skaar J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols [J]. Quantum Information & Computation, 2007, 8(6): 622-635.

[11] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution [J]. Physical Review Letters, 2012, 108(13): 130503.

[12] Ma X C, Sun S H, Jiang M S, *et al*. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution [J]. Physical Review A, 2014, 89(4): 042335.

[13] Sun S H, Gao M, Li C Y, *et al*. Practical decoy-state measurement-device-independent quantum key distribution[J]. Physical Review A, 2013, 87(5): 052329.

[14] Wang Q, Wang X B. Efficient implementation of the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources [J]. Physical Review A, 2013, 88(5): 052332.

[15] Dong C, Zhao S H, Zhao W H, *et al*. Analysis of measurement device independent quantum key distribution with an asymmetric channel transmittance efficiency [J]. Acta Physica Sinica, 2014, 63(3): 030302.
东晨, 赵尚弘, 赵卫虎, 等. 非对称信道传输效率的测量设备无关量子密钥分配研究[J]. 物理学报, 2014, 63(3): 030302.

[16] Kang D N, He Y F. Quantum key distribution protocol based on asymmetric channels of odd coherent sources [J]. Acta Optica Sinica, 2017, 37(6): 0627001.
康丹娜, 何业锋. 基于奇相干光源非对称信道的量子密钥分配协议[J]. 光学学报, 2017, 37(6): 0627001.

[17] Zhu Z D, Zhang X, Zhao S H, *et al*. Measurement-device-independent quantum key distribution protocols for heralded pair coherent state [J]. Laser & Optoelectronics Progress, 2017, 54(12): 122703.
朱卓丹, 张茜, 赵尚弘, 等. 预报相干光子对的测量设备无关量子密钥分发协议[J]. 激光与光电子学进展, 2017, 54(12): 122703.

[18] Abruzzo S, Kampermann H, Bruß D. Measurement-device-independent quantum key distribution with quantum memories [J]. Physical Review A, 2014, 89: 012301.

[19] Sun Y, Zhao S H, Dong C. Measurement device independent quantum key distribution network based on quantum memory and entangled photon sources [J]. Acta Optica Sinica, 2016, 36(3): 0327001.
孙颖, 赵尚弘, 东晨. 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[J]. 光学学报, 2016, 36(3): 0327001.

[20] He Y F, Li D Q, Song C, *et al*. Quantum key distribution protocol based on odd coherent sources and orbital angular momentum [J]. Chinese Journal of Lasers, 2018, 45(7): 0712001.
何业锋, 李东琪, 宋畅, 等. 基于奇相干光源和轨道角动量的量子密钥分配协议[J]. 中国激光, 2018, 45(7): 0412001.

[21] Fasel S, Alibart O, Tanzilli S, *et al*. High-quality asynchronous heralded single-photon source at telecom wavelength [J]. New Journal of Physics, 2004, 6: 163.

[22] Quan D X, Pei C X, Zhu C H, *et al*. New method of decoy state quantum key distribution with a heralded single-photon source[J]. Acta Physica Sinica, 2008, 57(9): 5600-5604.
权东晓, 裴昌幸, 朱畅华, 等. 一种新的预报单光子源诱骗态量子密钥分发方案[J]. 物理学报, 2008, 57(9): 5600-5604.

[23] Zhu F, Wang Q. 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.

[24] He Y F, Song C, Li D Q, *et al*. Asymmetric-channel quantum key distribution based on heralded single-photon sources[J]. Acta Optica Sinica, 2018, 38(3): 0827001.
何业锋, 宋畅, 李东琪, 等. 基于指示单光子源的非对称信道量子密钥分配[J]. 光学学报, 2018, 38(3): 0827001.

[25] Zhou Y Y, Zhang H Q, Zhou X J, *et al*. Performance analysis of decoy-state quantum key distribution with a heralded pair coherent state photon source [J]. Acta Physica Sinica, 2013, 62(20): 200302.
周媛媛, 张合庆, 周学军, 等. 基于标记配对相干态光源的诱骗态量子密钥分配性能分析[J]. 物理学报, 2013, 62(20): 200302.

[26] Dong C, Zhao S H, Shi L. Measurement device-independent quantum key distribution with heralded pair coherent state [J]. Quantum Information Processing, 2016, 15(10): 4253-4263.

[27] 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.