基于预报单光子源和探测器诱骗态的循环差分相移量子密钥分发协议

胡 康, 毛钱萍, 赵生妹

南京邮电大学通信与信息工程学院信号处理与传输研究院, 江苏 南京 210003

摘要 提出一种基于预报单光子源和探测器诱骗态的循环差分相移量子密钥分发协议,简称 HSPS-DD-RRDPS-QKD 协议。在详细推导协议密钥生成率的基础上,给出了相关数值仿真,并分别与基于弱相干光源和探测器诱骗态的循环差分相移量子密钥分发(WCS-DD-RRDPS-QKD)协议和诱骗态的 BB84 协议进行了性能比较。结果表明,随着脉冲序列长度 L 的增大,其密钥生成率和最远传输距离都相应减小;当脉冲序列长度 $L=16$ 时,HSPS-DD-RRDPS-QKD 协议较 WCS-DD-RRDPS-QKD 协议,安全通信距离提高了约 100 km,密钥生成率提升了近一个数量级;当系统错误率为 9.5%时,HSPS-DD-RRDPS-QKD 协议的密钥生成率较诱骗态的 BB84 协议的提升了近两个数量级。

关键词 量子光学; 量子密钥分发; 循环差分相移量子密钥分发; 预报单光子源; 探测器诱骗态

中图分类号 O431 **文献标识码** A

doi: 10.3788/AOS201737.0527002

Round Robin Differential Phase Shift Quantum Key Distribution Protocol Based on Heralded Single Photon Source and Detector Decoy State

Hu Kang, Mao Qianping, Zhao Shengmei

Institute of Signal Processing and Transmission, College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecomunications, Nanjing, Jiangsu 210003, *China*

Abstract A novel round robin differential phase shift quantum key distribution protocol based on heralded single photon source and detector decoy state is proposed, which is named as HSPS-DD-RRDPS-QKD protocol. The key generation rate of the proposed protocol is derived in detail, and the relevant numerical simulation is presented. The performance of the proposed protocol is compared with that of the round robin differential phase shift quantum key distribution based on weak coherent source and detector decoy state (named WCS-DD-RRDPS-QKD) protocol and that of the decoy state BB84 protocol, respectively. The results show that the key generation rate and the farthest transmission distance decrease with the increase of the pulse sequence length L. When the pulse sequence length $L=16$, the security communication distance of the HSPS-DD-RRDPS-QKD protocol increases by nearly 100 km and the key generation rate increases by one order of magnitude compared with those of the WCS-DD-RRDPS-QKD protocol. When the system error rate is 9.5%, the key generation rate of the HSPS-DD-RRDPS-QKD protocol is nearly two orders of magnitude higher than that of the decoy state BB84 protocol.

Key words quantum optics; quantum key distribution; round robin differential phase shift quantum key distribution; heralded single photon source; detector decoy state

OCIS codes 270.5568; 200.3050; 060.4370

收稿日期: 2017-01-05; **收到修改稿日期**: 2017-01-20

基金项目: 国家自然科学基金(61475075,61271238)、江苏省普通高校研究生科研创新计划项目(KYLX15_0832)、南京邮电大学宽带无线通信与传感网技术教育部重点实验室开放研究基金(NYKL2015011)

作者简介: 胡 康(1993—),男,硕士研究生,主要从事量子信息技术、无线通信与信号处理技术等方面的研究。E-mail: 2353414268@qq.com

导师简介: 赵生妹(1968—),女,博士,教授,主要从事量子信息技术、无线通信与信号处理技术等方面的研究。E-mail: zhaosm@njupt.edu.cn

1 引　言

量子密钥分发(QKD)协议是以量子态为信息载体,通过量子信道传输,在合法通信用户间建立安全密钥的过程。自 1984 年 Bennett 等[1]提出第一个量子密钥分发协议(BB84 协议)以来,各种离散变量[2-5]和连续变量[6-9]的 QKD 协议被相继提出。量子力学基本原理保证了这些协议的安全性,且合法通信双方通过监控干扰量大小来估算泄漏信息,确定窃听者 Eve 的存在;若泄漏信息在限定范围内,可通过错误协商和私密放大等技术获得安全密钥,否则将放弃该次密钥分发过程。2014 年,日本学者 Sasaki 等[10]提出了更为实用的 QKD 协议,即循环差分相移量子密钥分发(RRDPS-QKD)协议,之后在理论[11-15]和实验[16-19]两方面进行了深入的研究。该协议在不需要监控 Eve 干扰的情形下保证了密钥的安全。理论上,即使 Eve 引起的误码率高达 50%,Alice 和 Bob 也可获取安全的密钥。在实际中,弱相干光源(WCS)常被用来代替理想单光子源,由于 WCS 所含的空脉冲比例很高,因此原始 RRDPS-QKD 协议[10]的传输距离较短、密钥产生率较低。而预报单光子源[20](HSPS)利用自发参量下转换产生光子对,使用其中一个光子的探测结果来预报另一个光子的到达,从而大大减小了空脉冲的比例,这样可获得较高的密钥生成率和较远的安全传输距离。另一方面,原始 RRDPS-QKD 协议[10]需要使用光子数目解析(PNR)探测器,由于 PNR 探测器尚未成熟,对实验环境要求很高,因此目前大多数 RRDPS-QKD 协议的实验都使用阈值探测器(TD),但是其探测效率并不高。探测器诱骗态[21](DD)方法,可通过调节强度大小来估算单光子的统计特性,从而实现与 PNR 探测器相似的性能。

基于以上分析,本文将 HSPS 和 DD 方法应用于 RRDPS-QKD 协议,提出 HSPS-DD-RRDPS-QKD 新协议。在该协议中,Alice 先制备 1 串长为 L、经相位编码的 HSPS 脉冲序列,然后通过量子信道传输给 Bob,Bob 用 DD 方法对传输过来的脉冲序列进行调制,然后通过不等臂的马赫-曾德尔干涉仪(MZI)进行测量,并将结果发送给 Alice,这样 Alice 和 Bob 共享安全密钥。预报单光子源和探测器诱骗态方法特性优良,因此,HSPS-DD-RRDPS-QKD 协议将在密钥生成率和安全传输距离方面具有更好的性能。

2 协议模型

2.1 基于 HSPS 和 DD 的 RRDPS-QKD 协议

HSPS-DD-RRDPS-QKD 协议如图 1 所示,其中 PDC 代表非线性晶体,PM 代表相位调节器,BS 代表分束器,D_1、D_2、D_3 代表探测器,IM 代表光强调节器,S 代表 Alice 的筛选密钥,$r'=rT$ 代表随机的延迟时长($1\leqslant r\leqslant L-1$,$L$ 为脉冲序列长度,T 为相邻脉冲间的时隙)。根据图 1,由 Alice 端发送过来的 HSPS 脉冲序列先经过透射率为 η 的 IM,经过 BS 分成两路,其中一路经过随机延迟后与另一路进行叠加,Bob 若恰好探测到一个光子,则记录下是哪两个脉冲叠加的,并将其相对应的下标(i,j)发送给 Alice,随后通信双方通过后处理过程来获得安全密钥。

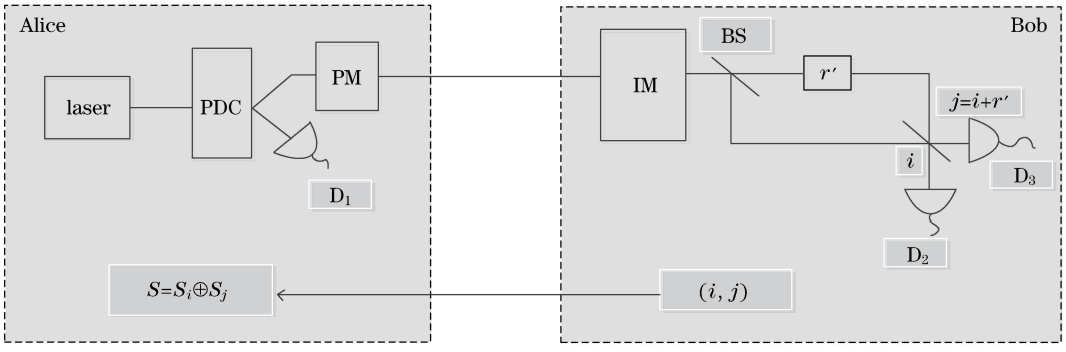

图 1　HSPS-DD-RRDPS-QKD 协议示意图

Fig. 1　Schematic diagram of HSPS-DD-RRDPS-QKD protocol

该协议的具体流程如下:

1) HSPS 脉冲序列的制备。Alice 制备 L 个纠缠光子对(即休闲光子和信号光子)组成一个脉冲序列,同时产生随机比特序列$(S_1,S_2,\cdots,S_L)$。一方面,Alice 利用探测器 D_1 探测纠缠对中的休闲光子,每探测到

一个休闲光子，就发射一个指示信号给 Bob；另一方面，Alice 根据随机比特序列(S_1，S_2，…，S_L)对每个信号光子(无论其对应的休闲光子有没有被探测到)进行相位调制(0→0，π→1)，然后发送给 Bob。

2) 测量。Bob 方的探测器根据 Alice 是否发来指示信号来调整其开关门时间和频率。Bob 先对 Alice 发送过来的信号进行 DD 调制，即通过一个透射率为 η 的 IM (其中，$\eta=\{\eta_1,\eta_2,\cdots,\eta_i\}$，Alice 每发送过来一个长为 L 的脉冲序列，就改变一下 η 的值)；然后将接收到的脉冲序列分成两路，送入不等臂的 MZI，并对其中一路的脉冲序列进行时长为 r'的延迟，将这两路脉冲序列进行干涉；最后通过探测器 D_2、D_3 来测量。如果在整个测量过程中恰好有一个光子被探测到，并且这个光子来源于没有进行任何操作的脉冲序列第 i 个脉冲与进行了 r'延迟的脉冲序列第 j 个脉冲的叠加，其中 $j-i=\pm r'$，则称此为一个成功探测事件，记录下此叠加脉冲所对应的(i，j)，并将其发送给 Alice。而 Bob 则根据探测到信号的那个探测器来获得筛选密钥，若是 D_2，Bob 获得的筛选密钥为 0；若是 D_3，Bob 获得的筛选密钥为 1。

3) Alice 根据 $S=S_i\oplus S_j$ 获得筛选密钥。

4) 重复步骤 1)～3)多次，直至获得足够多的筛选密钥，最后通过私密放大和错误协商来获得最终的安全密钥。

2.2　密钥生成率分析

对于 HSPS，信号光子的模式基本满足热光场分布[20]，即

$$\rho_\mu=\frac{1}{P_{\text{post}}(\mu)}\left\{\frac{d_{\text{A}}}{1+\mu}\,|0\rangle\langle 0|+\sum_{n=1}^{\infty}[1-(1-\eta_{\text{A}})^n]\times\frac{\mu^n}{(1+\mu)^{n+1}}\,|n\rangle\langle n|\right\},\tag{1}$$

式中 μ 表示信号光脉冲的平均强度，d_{A} 和 η_{A} 分别为 Alice 方探测器的暗计数率和探测效率，$P_{\text{post}}(\mu)=\frac{d_{\text{A}}}{1+\mu}+\frac{\mu\eta_{\text{A}}}{1+\mu\eta_{\text{A}}}$为后选择概率，$|0\rangle\langle 0|$表示真空态，$|n\rangle\langle n|$表示 n 光子态。

参考诱骗态 QKD 的方法[22]，对于平均强度为 μ 的弱相干光源，其增益 Q_μ 和量子比特误码率 E_μ 分别为

$$Q_\mu=\sum_{n=0}^{\infty}P_\mu(n)\cdot Y_n,\tag{2}$$

$$E_\mu=\sum_{n=0}^{\infty}(e_n\cdot Y_n)P_\mu(n)/Q_\mu,\tag{3}$$

式中 $P_\mu(n)=\frac{\mu^n}{n!}\cdot\exp(-\mu)$为平均强度为 μ 的弱相干光源脉冲中含有 n 个光子的概率，$Y_n=Y_0+\eta_n-Y_0\eta_n$为含有 n 个光子脉冲的增益，e_n 为含有 n 个光子脉冲的错误概率，Y_0为探测器暗计数与信道杂散光等造成的系统背景噪声，η_n 为 Alice 发出的包含 n 个光子的脉冲被探测到的概率。

由于 Alice 发送的是长为 L 的脉冲序列，令 $u=L\times\mu$ 为 HSPS 脉冲序列的平均强度，则

$$P_u(n)=\begin{cases}\dfrac{d_{\text{A}}}{1+u}\cdot\dfrac{1}{P_{\text{post}}(u)}, & u=0\\[2ex] [1-(1-\eta_{\text{A}})^n]\cdot\dfrac{u^n}{(1+u)^{1+n}}\cdot\dfrac{1}{P_{\text{post}}(u)}, & u\geqslant 1\end{cases},\tag{4}$$

强度为 u 的 HSPS 脉冲序列在不同透射率 η_i 下的增益 Q_u^i 和量子比特误码率 E_u^i 分别为

$$\begin{aligned}Q_u^i=&\sum_{n=0}^{\infty}Y_nP_u(n)=\\&\frac{1}{P_{\text{post}}(u)}\left\{Y_0L\cdot\frac{d_{\text{A}}}{1+u}+\sum_{n=1}^{\infty}[1-(1-Y_0L)(1-\eta_{\text{AB}})^n]\cdot[1-(1-\eta_{\text{A}})^n]\frac{u^n}{(1+u)^{n+1}}\right\}=\\&\frac{u\eta_{\text{A}}(1+u)+d_{\text{A}}Y_0L(1+u\eta_{\text{A}})}{d_{\text{A}}(1+u\eta_{\text{A}})+u\eta_{\text{A}}(1+u)}-\frac{u(1-Y_0L)(1+u\eta_{\text{A}})(1-\eta_{\text{AB}})}{[d_{\text{A}}(1+u\eta_{\text{A}})+u\eta_{\text{A}}(1+u)](1+u\eta_{\text{AB}})}+\\&\frac{u(1-\eta_{\text{AB}})(1-Y_0L)(1-\eta_{\text{A}})(1+u\eta_{\text{A}})}{[d_{\text{A}}(1+u\eta_{\text{A}})+u\eta_{\text{A}}(1+u)](1+u\eta_{\text{AB}}+u\eta_{\text{A}}-u\eta_{\text{AB}}\eta_{\text{A}})},\end{aligned}\tag{5}$$

$$E_u^i=\sum_{n=0}^{\infty}(e_nY_n)P_u(n)/Q_u^i=$$

$$\frac{1}{P_{\text{post}}(u)Q_u^i}\left\{e_0\cdot Y_0L\cdot\frac{d_{\text{A}}}{1+u}+\sum_{n=1}^{\infty}(e_0Y_0L+e_{\text{opt}}\eta_{\text{AB}}-Y_0Le_{\text{opt}}\eta_{\text{AB}})\cdot[1-(1-\eta_{\text{A}})^n]\frac{u^n}{(1+u)^{n+1}}\right\}=$$

$$\left\{\frac{e_0Y_0Ld_{\text{A}}(1+u\eta_{\text{A}})+u\eta_{\text{A}}(1+u)[e_0Y_0L+e_{\text{opt}}(1-Y_0)]}{d_{\text{A}}(1+u\eta_{\text{A}})+u\eta_{\text{A}}(1+u)}-\frac{ue_{\text{opt}}(1-\eta_{\text{AB}})(1-Y_0L)(1+u\eta_{\text{A}})}{[d_{\text{A}}(1+u\eta_{\text{A}})+u\eta_{\text{A}}(1+u)](1+u\eta_{\text{AB}})}+\right.$$

$$\left.\frac{ue_{\text{opt}}(1+u\eta_{\text{A}})(1-Y_0L)(1-\eta_{\text{A}})(1-\eta_{\text{AB}})}{[d_{\text{A}}(1+u\eta_{\text{A}})+u\eta_{\text{A}}(1+u)](1+u\eta_{\text{AB}}+u\eta_{\text{A}}-u\eta_{\text{AB}}\eta_{\text{A}})}\right\}\Big/Q_u^i,\tag{6}$$

式中 $\eta_{\text{AB}}=t_{\text{AB}}\cdot\eta_i\cdot\eta_{\text{B}}$ 为 Alice 与 Bob 之间总的传输率，$t_{\text{AB}}=10^{-\alpha\cdot s/10}$（其中，$\alpha$ 为光纤信道损失率，s 为通信距离），e_0 为背景光引起的错误率，e_{opt} 为系统光学校准（反馈）不完美造成的光学错误率，则 $Q=Q_u$（其中，Q_u 表示 Q_u^i 在透射率为 1 时的值）为 HSPS 脉冲序列的增益，E_u（即 E_u^i 在透射率为 1 的情况下的值）为 HSPS 脉冲序列的量子比特误码率。

Bob 接收到 Alice 发送过来的 HSPS 脉冲序列后，先进行 DD 调制，在不同透射率 η_i 下，Bob 方探测器响应的概率为

$$T_i=1-(1-Y_0L)\sum_{i=0}^{\infty}(1-\eta_i\eta_{\text{B}})^ip_i,\ i=0,1,2,\cdots,\tag{7}$$

式中 η_{B} 为 Bob 端探测器的探测效率，p_i 为 Alice 发送平均强度为 u 的脉冲序列中包含 i 个光子的概率。在这里，假设 Bob 接收到的多光子信号中有且只有一个光子被探测器探测到，这样就可以得到 Bob 接收到的多光子信号中有且只有一个光子被探测器探测到的最小概率：

$$G_{\min}=\sum_{n=0}^{\infty}n\eta_{\text{B}}(1-\eta_{\text{B}})^{n-1}p_n,\quad\text{s.t.}\begin{cases}T_i=Q_u^i,i=0,1,2,\cdots\\\sum_{n=0}^{\infty}p_n=1\\0\leqslant p_n\leqslant1\end{cases}。\tag{8}$$

结合文献[10]和(8)式，HSPS-DD-RRDPS-QKD 协议的密钥生成率为

$$R=\frac{1}{L}\left\{G_{\min}-Q\cdot f\cdot h(E_u)-\left[e_{\text{src}}+(G_{\min}-e_{\text{src}})\cdot h\left(\frac{v_{\text{th}}}{L-1}\right)\right]\right\},\tag{9}$$

式中 Q 为总增益；$h(E_u)=-E_u\text{lb}\ E_u-(1-E_u)\text{lb}\ (1-E_u)$ 为信息熵；f 为纠错效率；$v_{\text{th}}<(L-1)/2$ 且为整数；e_{src} 为一常数，它与每个脉冲序列里的光子数目超过 v_{th} 的概率有关，即

$$e_{\text{src}}=1-\sum_{n=0}^{v_{\text{th}}}p_n=1-\left\{\frac{d_{\text{A}}(1+u\eta_{\text{B}})}{d_{\text{A}}(1+u\eta_{\text{B}})+u\eta_{\text{B}}(1+u)}+\sum_{n=1}^{v_{\text{th}}}\frac{[1-(1-\eta_{\text{B}})^n](1+u\eta_{\text{B}})u^n}{(1+u)^n\cdot[d_{\text{A}}(1+u\eta_{\text{B}})+u\eta_{\text{B}}(1+u)]}\right\}。\tag{10}$$

3　仿真结果与分析

为了方便分析，假定 Bob 接收到的信号中光子数超过 10 个的概率为 0，即(8)式中 n 的取值在 0～10 之间，Bob 方的 IM 透射率为 $\eta=\{1,0.8,0.6\}$。根据以上密钥生成率分析，将本协议性能和文献[14]进行比较，并与经典的诱骗态 BB84 协议[22]在不同系统错误率下的性能进行比较。主要仿真参数如表 1 所示。

表 1　仿真参数

Table 1　Parameters for simulation

Parameter	d_{A} /counts	η_{A}	η_{B}	e_{opt}	f	α /(dB·km^{-1})
Value	10^{-9}	19%	19%	1.5%	1.16	0.2

图 2 所示为 HSPS-DD-RRDPS-QKD 协议在不同 L 下的密钥生成率随传输距离变化的曲线。由图 2 可以看出，随着 L 的增大，其密钥生成率和最远传输距离都相应减小。当 $L=16$ 时，该协议的最远传输距离达 304 km；而当 $L=128$ 时，该协议的最远传输距离仅为 284 km。当传输距离大于 50 km 后，$L=16$ 时该协议的密钥生成率是 $L=128$ 时的 3 倍以上。图 3 是当 L 分别为 16、64、128 时，HSPS-DD-RRDPS-

QKD 协议和 WCS-DD-RRDPS-QKD 协议[14]的密钥生成率随传输距离变化的曲线。由图 3 可知，当 $L=16$时，HSPS-DD-RRDPS-QKD 协议的性能远比 WCS-DD-RRDPS-QKD 协议的好，并且前者的最远传输距离比后者的多了 96 km；在 $L=64$ 的条件下，当传输距离小于 100 km 时，HSPS-DD-RRDPS-QKD 协议的性能与 WCS-DD-RRDPS-QKD 协议的相近，但当传输距离大于 100 km 时，HSPS-DD-RRDPS-QKD 协议的性能要远比 WCS-DD-RRDPS-QKD 协议的好；当 $L=128$ 时，WCS-DD-RRDPS-QKD 协议的性能比 HSPS-DD-RRDPS-QKD 协议的好。图 4 是当 e_{opt}分别为 1.5%和 9.5%时，HSPS-DD-RRDPS-QKD 协议和诱骗态 BB84 协议的密钥生成率随传输距离变化的曲线。由图 4 可知，当 e_{opt}较小时，诱骗态 BB84 协议的性能优于 HSPS-DD-RRDPS-QKD 协议的；但是当 e_{opt}较大时，HSPS-DD-RRDPS-QKD 协议的性能远远好于诱骗态 BB84 协议的，且前者的密钥生成率比后者的高一个数量级以上。

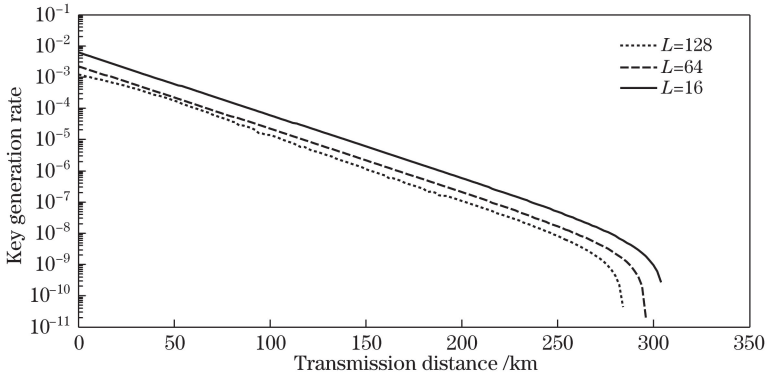

图 2　L 不同时 HSPS-DD-RRDPS-QKD 协议的性能比较

Fig. 2　Performance comparison of HSPS-DD-RRDPS-QKDRRDPS protocol under different L

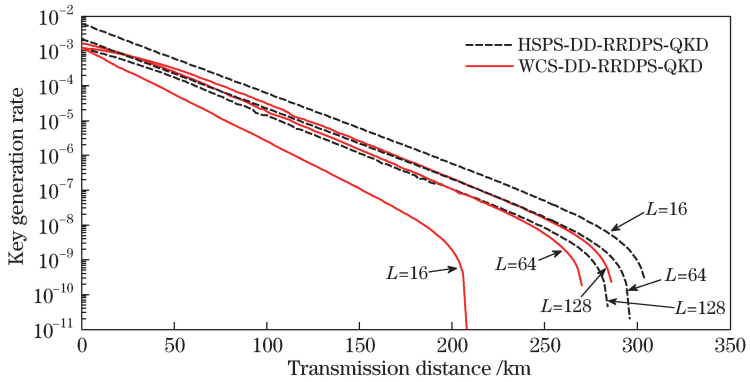

图 3　L 不同时 HSPS-DD-RRDPS-QKD 协议和 WCS-DD-RRDPS-QKD 协议的性能比较

Fig. 3　Performance comparison between HSPS-DD-RRDPS-QKD protocol and WCS-DD-RRDPS-QKD protocol under different L

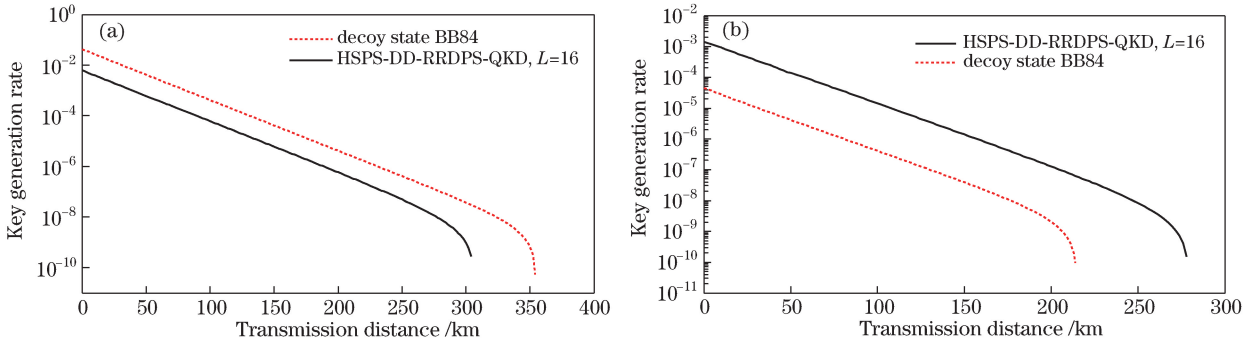

图 4　e_{opt}不同时 HSPS-DD-RRDPS-QKD 协议和诱骗态 BB84 协议的性能比较.(a) $e_{opt}=1.5\%$；(b) $e_{opt}=9.5\%$

Fig. 4　Performance comparison between HSPS-DD-RRDPS-QKD protocol and decoy state BB84 protocol under different e_{opt}. (a) $e_{opt}=1.5\%$; (b) $e_{opt}=9.5\%$

4 结 论

提出了 HSPS-DD-RRDPS-QKD 新协议。L 不同时，HSPS-DD-RRDPS-QKD 协议的性能不相同。当 L 从 16 增大到 128 时，其最远传输距离缩短了 20 km，密钥生成率也相应地降低。与原来的 WCS-DD-RRDPS-QKD 协议相比，HSPS-DD-RRDPS-QKD 协议更适合 L 较小的情况，当 $L=16$ 时，其最远传输距离比 WCS-DD-RRDPS-QKD 协议的长 96 km，相应的密钥生成率提升了近一个数量级。该协议保持了原始 RRDPS-QKD 协议的优势，即具有较大的比特错误容忍度。当 e_{opt} 为 9.5%时，该协议的性能比诱骗态 BB84 协议的好，其密钥生成率较后者提升了近两个数量级，最远传输距离较后者长 64 km。该协议的仿真结果是最优化后的极限数值，在实际实验中要考虑更多的实际问题。考虑到该协议在现有技术下比较容易实现，HSPS-DD-RRDPS-QKD 协议在今后量子密钥的实用中仍具有重要的应用价值与发展前景。

参 考 文 献

[1] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing[C]. Proceeding of IEEE International Conference on Computers, Systems and Signal Processing, 1984: 175-179.

[2] Liu Y, Chen T Y, Wang J, *et al*. Decoy-state quantum key distribution with polarized photons over 200 km[J]. Opt Express, 2010, 18(8): 8587-8594.

[3] Wang L, Zhao S M, Gong L Y, *et al*. Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum[J]. Chin Phys B, 2015, 24(12): 120307.

[4] Yan Long, Sun Hao, Zhao Shengmei. Study on decoyed measurement device independent quantum key distribution protocol using orbital angular momentum[J]. Journal of Signal Processing, 2014, 30(11): 1275-1278.
颜 龙, 孙 豪, 赵生妹. 应用诱骗态的光子轨道角动量测量设备无关量子密钥分发协议的研究[J]. 信号处理, 2014, 30(11): 1275-1278.

[5] Xiao Hong, Shi Peng, Zhao Shengmei. A reconciliation protocol with delayed error correction for quantum key distribution[J]. Scientia Sinica: Technologica, 2015, 45(8): 843-848.
肖 红, 施 鹏, 赵生妹. 基于 Polar 码的纠错延后量子协商协议[J]. 中国科学: 技术科学, 2015, 45(8): 843-848.

[6] Wang Yunyan, Guo Dabo, Zhang Yanhuang, *et al*. Algorithm of multidimensional reconciliation for continuous-variable quantum key distribution[J]. Acta Optica Sinica, 2014, 34(8): 0827002.
王云艳, 郭大波, 张彦煌, 等. 连续变量量子密钥分发多维数据协调算法[J]. 光学学报, 2014, 34(8): 0827002.

[7] Chen Yan, Shen Yong, Zou Hongxin. An all-fiber continuous variable quantum key distribution based on multi-bits coding of single pulse[J]. Acta Optica Sinica, 2015, 35(7): 0727001.
陈 岩, 沈 咏, 邹宏新. 基于单脉冲多位编码的全光纤连续变量量子密钥分发[J]. 光学学报, 2015, 35(7): 0727001.

[8] Leverrier A, Grangier P. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation[J]. Phys Rev A, 2011, 83(4): 042312.

[9] Huang P, He G, Fang J, *et al*. Performance improvement of continuous-variable quantum key distribution via photon subtraction[J]. Phys Rev A, 2013, 87(1): 012317.

[10] Sasaki T, Yamamoto Y, Koashi M. Practical quantum key distribution protocol without monitoring signal disturbance[J]. Nature, 2014, 509(7501): 475-478.

[11] Zhang Z, Yuan X, Cao Z, *et al*. Round-robin differential-phase-shift quantum key distribution[EB/OL]. (2015-05-11)[2016-12-20]. https://arxiv.org/abs/1505.02481.

[12] Mizutani A, Imoto N, Tamaki K. Robustness of the round-robin differential-phase-shift quantum-key-distribution protocol against source flaws[J]. Phys Rev A, 2015, 92(6): 060303.

[13] Sasaki T, Koashi M. Round-robin differential phase-shift quantum key distribution protocol with threshold detectors[C]. 5th International Conference on Quantum Cryptography, 2015.

[14] Yin H L, Fu Y, Mao Y, *et al*. Detector-decoy quantum key distribution without monitoring signal disturbance[J]. Phys Rev A, 2016, 93(2): 022330.

[15] Zhang Y Y, Bao W S, Zhou C, *et al*. Practical round-robin differential phase-shift quantum key distribution[J]. Opt Express, 2016, 24(18): 20763-20773.

[16] Takesue H, Sasaki T, Tamaki K, *et al*. Experimental quantum key distribution without monitoring signal disturbance[J]. Nature Photonics, 2015, 9: 827-831.

[17] Wang S, Yin Z Q, Chen W, *et al*. Experimental demonstration of a quantum key distribution without signal disturbance monitoring[J]. Nature Photonics, 2015, 9: 832-836.

[18] Li Y H, Cao Y, Dai H, *et al*. Experimental round-robin differential phase-shift quantum key distribution[J]. Phys Rev A, 2016, 93(3): 030302.

[19] Guan J Y, Cao Z, Liu Y, *et al*. Experimental passive round-robin differential phase-shift quantum key distribution[J]. Phys Rev Lett, 2015, 114(18): 180502.

[20] Lütkenhaus N. Security against individual attacks for realistic quantum key distribution[J]. Phys Rev A, 2000, 61(5): 052304.

[21] Moroder T, Curty M, Lütkenhaus N. Detector decoy quantum key distribution[J]. New J Phys, 2009, 11(4): 045008.

[22] Ma X, Qi B, Zhao Y, *et al*. Practical decoy state for quantum key distribution[J]. Phys Rev A, 2005, 72(1): 012326.