第 58 卷 第 23 期/2021 年 12 月/激光与光电子学进展 研究论文

激光与光电子学进展

基于标记配对相干态光源的发送或不发送量子密钥分发

徐瑞，赵生妹*

南京邮电大学信号处理与传输研究院，江苏 南京 210003

摘要 为了提高发送或不发送量子密钥分发(SNS-QKD)的性能，提出了基于标记配对相干态光源(HPCS)的SNS-QKD协议，即HPCS-SNS-QKD协议。该协议中使用HPCS代替弱相干态光源(WCS)。与WCS相比，HPCS所发射的真空态脉冲比例更低，因此HPCS-SNS-QKD协议可有效降低单光子误码率。推导了密钥生成率与安全传输距离之间的关系，并进一步给出在脉冲总数有限条件下的密钥生成率表达形式。仿真结果表明：HPCS-SNS-QKD协议可以突破单光子密钥传输距离上界，且相比于WCS-SNS-QKD协议，HPCS-SNS-QKD协议的安全传输距离更远、密钥生成率更高，且能容忍更大的失调误差。在有限脉冲数下，HPCS-SNS-QKD获得更高的密钥生成率。

关键词 量子光学；量子密钥分发；发送或不发送量子密钥协议；标记配对相干态；弱相干光源

中图分类号 O436 **文献标志码** A **doi**：10.3788/LOP202158.2327001

Sending or Not Sending Quantum Key Distribution Based on Heralded Pair-Coherent Source

Xu Rui, Zhao Shengmei*

Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu 210003, *China*

Abstract In order to improve the performance of sending or not sending quantum key distribution (SNS-QKD), an SNS-QKD protocol based on a heralded pair-coherent source (HPCS) is proposed, named HPCS-SNS-QKD protocol. In the protocol, a weak coherent source (WCS) is replaced by HPCS. HPCS has lower ratio of vacuum state pulse than WCS. Hence the single photon error bit rate can be effectively reduced in HPCS-SNS-QKD. The relationship between the key generation rate and secure transmission distance is derived, and the expression of the key generation rate under limited pulses is given. The numerical simulation results show that the proposed HPCS-SNS-QKD protocol can exceed the upper limit of single-photon key transmission distance. Compared with WCS-SNS-QKD protocol, HPCS-SNS-QKD protocol has longer transmission distance and higher key generation rate and can endure larger misalignment error. For limited pulses in practical experiment, HPCS-SNS-QKD always has a higher key generation rate.

Key words quantum optics; quantum key distribution; sending or not sending quantum key protocol; heralded pair-coherent state; weak coherent source

OCIS codes 270.5568; 270.5565; 010.1330

收稿日期：2021-01-04；**修回日期**：2021-01-18；**录用日期**：2021-03-26

基金项目：国家自然科学基金(61871234)、江苏省研究生科研与实践创新计划项目(SJCX19_0251)

通信作者：*zhaosm@njupt.edu.cn

1 引　　言

量子密钥分发(QKD)[1-3]提供了一种基于量子力学的密钥共享方法,可以实现无条件的安全通信。在实际量子密钥分发实验中,光源和探测器的不完美导致了量子密钥分发存在安全漏洞。为了消除不完美设备引起的安全问题,众多应对方法被提出。例如,诱骗态方法[4-5]被提出,用于解决光子数分离攻击[6];测量设备无关量子密钥分发协议(MDI-QKD)[7]被提出,用于解决针对测量设备的攻击。虽然这些方法和协议具有很高的安全性,但是其最大密钥速率 $O(\eta)$ 与信道损耗 η 呈线性关系[8-10],因此,在不使用量子中继器时,量子密钥分发只能传输有限的距离。

2018年,Lucamarini等[11]提出了一种可以克服受密钥生成率与信道损耗呈线性关系限制的双场量子密钥分发协议(TF-QKD),其密钥速率 $O(\sqrt{\eta})$ 与信道损耗的平方根呈线性关系,并且该协议也与测量设备无关,可以抵御针对测量设备的攻击。不久后,一些更进一步的工作相继出现[12-16],其中清华大学王向斌教授研究小组提出的发送或不发送量子密钥分发协议(SNS-QKD)[13]可以容忍较大的非对准误差,更加适合实际应用。因此,SNS-QKD受到极大关注[17-20],例如Minder等[19]通过实验对SNS-QKD进行了验证,Liu等[20]考虑了统计涨落影响的SNS-QKD的实际性能。但是这些研究通常使用弱相干态光源(WCS),弱相干态光源的空脉冲成分多,导致密钥生成率低。而标记配对相干态光源(HPCS)[21-29]具有空脉冲成分少的特点,能够提升量子密钥分发的性能。

本文基于HPCS,结合SNS-QKD协议,提出基于HPCS的SNS-QKD协议,即HPCS-SNS-QKD协议,该协议中使用HPCS替代弱相干态光源,有效减少了空脉冲成分;推导了HPCS-SNS-QKD协议的安全密钥生成率公式,讨论并分析HPCS-SNS-QKD协议在传输距离、失调误差以及有限脉冲数方面的性能。

2 协议及安全密钥生成率分析

标记配对相干态是将光子标记技术应用于配对相干态[21]光源,HPCS包含两种模式(空闲模式和信号模式)的光子。空闲模式的光子被发送到触发探测器,用于预测信号模式的光子数以及到达第三方的时间。信号模式光子经编码后被发送给第三方进行测量。将HPCS应用在SNS-QKD中,当空闲模式光子使触发探测器产生响应时保留此次事件,当触发探测器未产生响应时,以概率 p 保留此次事件结果,此时,HPCS的光子数分布为

$$P_n(\mu)=\frac{1}{P_{\mathrm{post}}(\mu)}\left\{\frac{1}{\mathrm{I}_0(2\mu)}\frac{\mu^{2n}}{(n!)^2}\left[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})^n\right]+\frac{1}{\mathrm{I}_0(2\mu)}\frac{\mu^{2n}}{(n!)^2}p(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})^n\right\},\tag{1}$$

式中:μ 为脉冲的平均强度;n 为光子数;$\mathrm{I}_0(x)$ 为第一类修正贝塞尔函数;η_{A} 和 d_{A} 分别是单光子探测器的探测效率及暗计数率;p 为探测器无响应时保留该次结果的概率;$P_{\mathrm{post}}(\mu)$ 是后选择的概率,$P_{\mathrm{post}}(\mu)=1-(1-p)(1-d_{\mathrm{A}})\dfrac{\mathrm{I}_0(2\mu\sqrt{1-\eta_{\mathrm{A}}})}{\mathrm{I}_0(2\mu)}$。

基于HPCS的SNS-QKD协议的示意图如图1所示,SNS-QKD主要包含以下几个步骤[13]:

1) 在信号传输之前,Alice和Bob向不可信接收端Charlie发送参考脉冲用于相位补偿。

2) Alice和Bob发送的脉冲通过非线性晶体产生空闲模式的光子和信号模式的光子,经过偏振分束器(PBS)分束后进入不同光路。空闲模式的光子被发送到触发探测器(Da、Db),用来预报信号模式的光子数和光子到达时间;对信号模式的光子进行调制后将其发送给第三方进行测量。在所有时间窗口中,Alice(Bob)独立随机地以概率 P_{X} 选择诱骗态窗口(X窗口),以概率 $1-P_{\mathrm{X}}$ 选择信号态窗口(Z

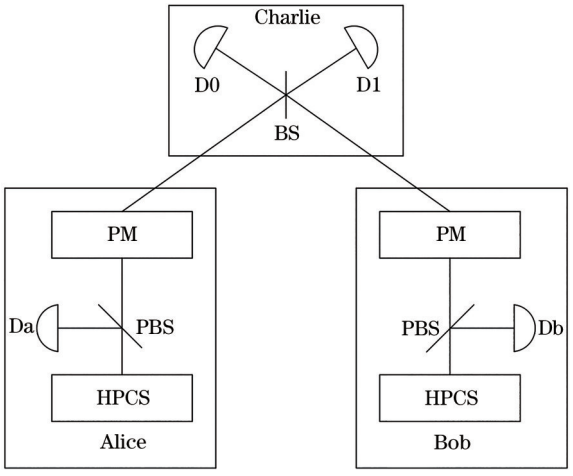

图1　基于HPCS的SNS-QKD协议示意图

Fig. 1　Schematic of SNS-QKD protocol based on HPCS

窗口),此时信号模式光子被调制为诱骗态脉冲或信号态脉冲。在诱骗态窗口中,以概率p_i选择诱骗态脉冲(i为0,1,2对应的强度分别为0、μ_1和μ_2,其中$\mu_2>\mu_1>0$),并将通过相位调制器(PM)附加随机相移θ_A(θ_B)的诱骗态脉冲发送给Charlie;在信号态窗口中,Alice(Bob)以概率ε向Charlie发送信号态脉冲(强度为μ),以概率$1-\varepsilon$不发送脉冲。

3) Charlie在接收端使用分束器(BS)和两个探测器(D0、D1)对Alice和Bob的脉冲进行双场测量,并且记录探测器的响应结果。当量子通信结束后,Charlie公开宣布所有探测结果,定义Z窗口和X窗口的有效事件如下:当Alice和Bob选择信号态窗口并且Charlie端仅有一个探测器响应或者当Alice和Bob选择的诱骗态窗口且所选脉冲强度相同,随机相位满足$\left|\theta_A-\theta_B-m\pi\right|\leqslant\frac{2\pi}{M}$时Charlie端仅有一个探测器产生响应,这里的$m$为0,1时分别表示$\theta_A$和$\theta_B$同相、反相,$M$表示Alice和Bob可选的相位片总数,$\frac{2\pi}{M}$表示每个相位片的大小。

4) Alice和Bob公开宣布诱骗态窗口和信号态窗口的顺序,以及每个诱骗态窗口脉冲强度及详细相位值θ_A和θ_B。这里将位于Z窗口的量子态命名为Z基下的态,将X窗口下脉冲强度相同且随机相位满足$\left|\theta_A-\theta_B-m\pi\right|\leqslant\frac{2\pi}{M}$的量子态命名为X基下的态。

5) 通过随机选择Z基上的比特进行错误测试,并计算比特错误率E_Z。对于Z基上的有效事件:如果Alice(Bob)选择发送一个信号态脉冲,记录一个比特值1(0);如果Alice(Bob)选择不发送,记录一个比特值0(1)。如果发生有效事件时,Alice和Bob同时选择发送或者不发送,将会产生一个错误比特。

6) 获得X基上的测量结果后可通过以下标准判断响应是X基上的一个正确比特还是一个错误比特。当左(右)探测器产生响应时有$\cos(\theta_A-\theta_B)>0$,表示一个正确的X基比特;当右(左)探测器产生响应时有$\cos(\theta_A-\theta_B)>0$,表示一个错误的X基比特。通过X基上的数据可以计算单光子计数率和相位翻转错误率。

7) 通过错误纠正及隐私放大后可得到最终密钥。

下面对SNS-QKD进行详细的理论分析,为了简单起见,假设Alice与Charlie、Bob与Charlie之间的信道是对称的。

在X基中有效事件的计数率可表示为

$$S_\xi^{m,D}=\frac{M^2}{4\pi^2}\int_{\delta_0}^{\delta_0+\frac{2\pi}{M}}\int_0^{\frac{2\pi}{M}}S_{\xi,\theta_A,\theta_B}^{m,D}\,\mathrm{d}\theta_A\,\mathrm{d}\theta_B,\tag{2}$$

$$S_{\xi,\theta_A,\theta_B}^{m,D}=\sum_{j,k}P_j(\xi)P_k(\xi)\times$$
$$\sum_{t=0}^{j+k}C_{j+k}^t\left(\left|\left\langle X_A|X_B\right\rangle_D^m\right|^2\right)^t\left(1-\left|\left\langle X_A|X_B\right\rangle_D^m\right|^2\right)^{j+k-t}Y_t,\tag{3}$$

式中:$\xi\in\{\mu_1,\mu_2\}$;D表示左探测器(L)或者右探测器(R);$\theta_A\in\left[0,\frac{2\pi}{M}\right)$,$\theta_B\in\left[\delta_0,\delta_0+\frac{2\pi}{M}\right)$,其中$\delta_0$表示全局相位的固定相位差,因此失调误差$e_d=\frac{1-\cos\delta_0}{2}$;$\left|\left\langle X_A|X_B\right\rangle_D^m\right|^2$表示在X基中,从Alice和Bob发送的脉冲到达Charlie端并发生干涉的概率,例如$\left|\left\langle X_A|X_B\right\rangle_L^0\right|^2=\left|\left\langle X_A|X_B\right\rangle_R^1\right|^2=\frac{1+\cos(\theta_A-\theta_B)}{2}$,$\left|\left\langle X_A|X_B\right\rangle_L^1\right|^2=\left|\left\langle X_A|X_B\right\rangle_R^0\right|^2=\frac{1-\cos(\theta_A-\theta_B)}{2}$;$Y_t$表示发送$t$个光子时接收端探测器的响应概率,$Y_t=1-(1-Y_0)(1-\eta)^t$,$Y_0=2P_d(1-P_d)$,$P_d$表示探测器的暗计数率,$\eta$($\eta=\eta_c\eta_d$)表示Alice(Bob)到Charlie的总透射率,η_d表示探测器的探测效率,η_t表示信道传输效率,$\eta_c=10^{\frac{-\alpha_0 l/2}{10}}$,$l$表示Alice与Bob之间的距离,$\alpha_0$为损耗系数,取$\alpha_0=0.2\ \mathrm{dB\cdot km^{-1}}$。

通过X基下比特的判断标准进行判断,可以得到对应的总计数率S_ξ^X及量子比特错误率T_ξ^X分别为

$$S_\xi^X=\frac{1}{2}(S_\xi^{0,L}+S_\xi^{0,R}+S_\xi^{1,L}+S_\xi^{1,R}),\tag{4}$$

$$T_\xi^X=\frac{1}{2}(S_\xi^{0,R}+S_\xi^{1,L})。\tag{5}$$

Z基中只有一端发送相位随机化的信号脉冲,成功事件是在Charlie只有一个探测器响应,所以可以得到Z基下的总计数率S_Z和量子比特错误率T_Z分别为

$$S_Z=(1-\varepsilon)^2Y_0+4\varepsilon(1-\varepsilon)(1-P_d)\sum_{k=0}^{\infty}P_k\left(\frac{\mu}{2}\right)(1-\eta)^k\sum_{k=0}^{\infty}P_k\left(\frac{\mu}{2}\right)\left[1-(1-P_d)(1-\eta)^k\right]+$$
$$2\varepsilon^2(1-P_d)\sum_{m,n=0}P_m\left(\frac{\mu}{2}\right)P_n\left(\frac{\mu}{2}\right)(1-\eta)^{m+n}\sum_{m,n=0}P_m\left(\frac{\mu}{2}\right)P_n\left(\frac{\mu}{2}\right)\left[1-(1-P_d)(1-\eta)^{m+n}\right],\tag{6}$$

$$T_Z=(1-\varepsilon)^2Y_0+2\varepsilon^2(1-P_d)\sum_{m,n=0}P_m\left(\frac{\mu}{2}\right)P_n\left(\frac{\mu}{2}\right)(1-\eta)^{m+n}\sum_{m,n=0}P_m\left(\frac{\mu}{2}\right)P_n\left(\frac{\mu}{2}\right)\left[1-(1-P_d)(1-\eta)^{m+n}\right]。\quad(7)$$

在获得Z基和X基的测量结果之后，可以通过X基的数据计算单光子计数率和相位翻转错误率[13]：

$$s_1\geqslant s_{1,L}=\frac{P_2(\mu_2)\left[S^X_{\mu_1}-P_0(\mu_1)Y_0\right]-P_2(\mu_1)\left[S^X_{\mu_2}-P_0(\mu_2)Y_0\right]}{P_2(\mu_2)P_1(\mu_1)-P_2(\mu_1)P_1(\mu_2)},\quad(8)$$

$$e_1^{ph}\leqslant e_{1,U}^{ph}=\frac{T^X_{\mu_1}-\frac{1}{2}P_0(\mu_1)Y_0}{P_1(\mu_1)s_{1,L}},\quad(9)$$

式中：$s_{1,L}$为s_1的下界；$e_{1,U}^{ph}$是e_1^{ph}的上界。

SNS-QKD的密钥生成率公式[30]为

$$R=(1-P_X)^2\times\left\{2\varepsilon(1-\varepsilon)P_1(\mu)s_1\left[1-H(e_1^{ph})\right]-S_Z fH(E_Z)\right\},\quad(10)$$

式中：E_Z是Z基下的总误码率，$E_Z=T_Z/S_Z$；$H(x)=-x\log_2x-(1-x)\log_2(1-x)$是二进制香农熵；$f$为错误纠正效率。

但是，实际实验中发送的脉冲数目是有限的，假设发送的总脉冲数为N（$N=N_{ZZ}+2N_{XZ}+N_{XX}$，其中N_{ZZ}表示Alice和Bob同时选择Z窗口的脉冲数，N_{XZ}表示Alice和Bob其中一个选择Z窗口、一个选择X窗口的脉冲数，N_{XX}表示Alice和Bob同时选择X窗口的脉冲数）。为了提取最终的安全密钥，必须考虑统计波动的影响。采用文献[31]中所使用的方法，对s_1的下界与e_1^{ph}的上界进行更新，定义$\langle S_{\mu_i}\rangle$和$\langle Y_0\rangle$是$S_{\mu_i}(i=1,2)$和Y_0的期望值，在实验中S_{μ_i}和Y_0是可直接观测的值。对于给定脉冲数和观测值，计算出期望值的上界和下界分别为

$$\begin{cases}\langle X_L\rangle=X/(1+\alpha_X)\\ \langle X_U\rangle=X/(1-\alpha'_X)\end{cases},\quad(11)$$

式中：X代表Y_0，S_{μ_i}和$T_{\mu_1}(i=1,2)$；α_X和α'_X表示起伏比。利用Chernoff界[32]的乘法形式，在一个固定失败概率γ下，可以计算出期望值的上下界区间，其中$\alpha_{Y_0}=f_a(N_{00}Y_0,\gamma)$，$\alpha_{S_{\mu_i}}=f_a\left[(N_{0i}+N_{i0})S_{\mu_i},\gamma\right]$，$\alpha_T=f_a\left[(N^L_{11}+N^R_{11})T_{\mu_1},\gamma\right]$，其中函数$f_a(x,y)$定义为

$$f_a(x,y)=\left\{-\ln(y/2)+\sqrt{\left[\ln(y/2)\right]^2-8\ln(y/2)}\right\}\Big/(2x),\quad(12)$$

式中：N_{jk}（j、k组合的取值为00，01，10，02，20，11）表示Alice发送强度为μ_j的相干态脉冲并且Bob发送强度为μ_k的相干态脉冲的个数，计算可得

$$N_{00}=[P_X^2p_0^2+2P_X(1-P_X)p_0(1-\varepsilon)]N,\quad(13)$$

$$N_{01}=N_{10}=[P_X^2p_0p_1+(1-P_X)P_Xp_1(1-\varepsilon)]N,\quad(14)$$

$$N_{02}=N_{20}=[P_X^2p_0p_2+(1-P_X)P_Xp_2(1-\varepsilon)]N,\quad(15)$$

$$N^L_{11}=N^R_{11}=\frac{2}{M}P_X^2p_1^2N。\quad(16)$$

对于(8)、(9)式中s_1和e_1^{ph}的期望值$\langle s_1\rangle$和$\langle e_1^{ph}\rangle$，分别有如下定义：

$$\langle s_1\rangle\geqslant\langle s_{1,L}\rangle=\frac{P_2(\mu_2)\left[\langle S_{\mu_1,L}\rangle-P_0(\mu_1)\langle Y_{0,U}\rangle\right]-P_2(\mu_1)\left[\langle S_{\mu_2,U}\rangle-P_0(\mu_2)\langle Y_{0,U}\rangle\right]}{P_2(\mu_2)P_1(\mu_1)-P_2(\mu_1)P_1(\mu_2)},\quad(17)$$

$$\langle e_1^{ph}\rangle\leqslant\langle e_{1,U}^{ph}\rangle=\frac{\langle T_{\mu_1,U}\rangle-\frac{1}{2}P_0(\mu_1)\langle Y_{0,L}\rangle}{P_1(\mu_1)\langle s_{1,L}\rangle},\quad(18)$$

式中：$S_{\mu_1,L}$为S_{μ_1}的下界；$S_{\mu_2,U}$为S_{μ_2}的上界；$Y_{0,U}$为Y_0的上界；$T_{\mu_1,U}$为T_{μ_1}的上界；$Y_{0,L}$为Y_0的下界。对应地，实验中可将获得的s_1的下界与e_1^{ph}的上界分别估计为

$$\begin{cases}s_{1,L}=\langle s_{1,L}\rangle(1-\alpha_1)\\ e_{1,U}^{ph}=\langle e_{1,U}^{ph}\rangle(1+\alpha'_1)\end{cases},\quad(19)$$

式中：$\alpha_1=f_a\left[P_1(\mu)N^c_{ZZ}\langle s_{1,L}\rangle,\gamma\right]$，$\alpha'_1=f_a\left[P_1(\mu)\times N^c_{ZZ}\langle s_{1,L}\rangle\langle e_{1,U}^{ph}\rangle,\gamma\right]$，$N^c_{ZZ}=2\varepsilon(1-\varepsilon)N_{ZZ}$，$N_{ZZ}=(1-P_X^2)N$。

3　分析与讨论

通过数值仿真分析HPCS-SNS-QKD的性能，仿真所使用的参数为：信道衰减为0.2 dB/km，探测器效率$\eta_d=80\%$，暗计数率$P_d=10^{-11}$，错误纠正效率$f=1.10$，失调误差$e_d=5\%$，相位片个数$M=16$，失败概率$\gamma=10^{-10}$。图2中对比了两种光源下密钥生成率与传输距离之间的关系，可以发现相同脉冲数下基于HPCS的SNS-QKD的密钥生成率比基于WCS的SNS-QKD的密钥生成率更高，性能更好。

图3比较了不同光源的e_1^{ph}随传输距离的变

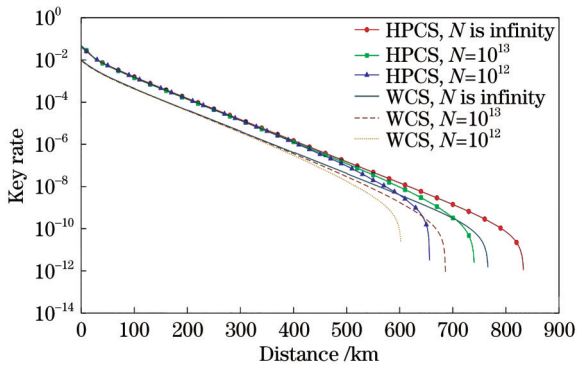

图 2　HPCS-SNS-QKD 的密钥生成率随传输距离的变化

Fig. 2　Key generation rate of HPCS-SNS-QKD varying with transmission distance

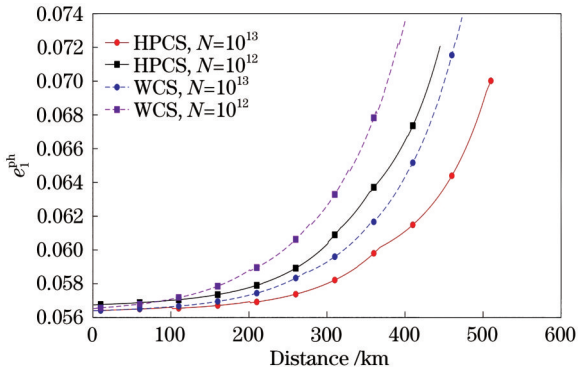

图 3　HPCS-SNS-QKD 的相位翻转错误率随传输距离的变化

Fig. 3　Phase flipping error rate of HPCS-SNS-QKD varying with transmission distance

化，可以看出相同脉冲数下，基于 HPCS 的 SNS-QKD 协议的单光子误码率要低于基于 WCS 的 SNS-QKD 协议。这是因为使用 HPCS 可以优化真空态脉冲与单光子脉冲的比例，并且可以降低多脉冲所占的比例，从而降低相位翻转错误率，因此 HPCS-SNS-QKD 的传输距离增加，密钥生成率也得到了提升。

此外，为了研究该方案在远程传输距离上能容忍的失调误差，绘制了不同光学失调误差下的密钥生成速率的变化，设置脉冲个数为无限个，如图 4 所示。这里将传输距离固定在 500 km，显然，在相同失调误差下，HPCS-SNS-QKD 的密钥生成率更高，并且当失调误差大于 0.35 时，基于 WCS 的 SNS-QKD 只能产生极低的密钥生成率，而 HPCS-SNS-QKD 可以容忍 0.05 左右的失调误差，这在实现远程 QKD 方面展现了更广阔的前景。

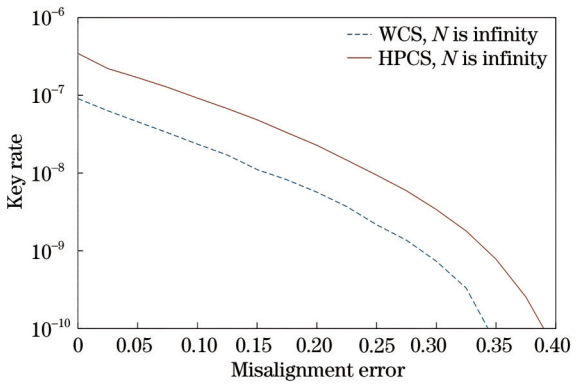

图 4　在 500 km 处 HPCS-SNS-QKD 的密钥生成率随失调误差的变化

Fig. 4　Key generation rate of HPCS-SNS-QKD varying with misalignment error at 500 km

4　结　　论

提出了一种 HPCS-SNS-QKD 协议，研究了该协议的密钥生成率与安全传输距离之间的关系。通过使用 HPCS 对真空态脉冲与单光子脉冲的比例进行优化，可以有效降低单光子误码率，从而增大密钥安全传输距离。数值计算结果表明，相比于基于 WCS 的 SNS-QKD 协议，HPCS-SNS-QKD 在密钥生成率、安全传输距离和失调错误容忍度上都具有更好的性能，且在相同脉冲数下，HPCS-SNS-QKD 的密钥生成率也总是要高于 WCS-SNS-QKD 的密钥生成率。该研究可以为进一步实施 SNS-QKD 协议提供有价值的参考。

参　考　文　献

[1] Zhao S M, Zheng B Y. Quantum information processing technology[M]. Beijing: Beijing University of Posts and Telecommunications Press, 2010.
赵生妹, 郑宝玉. 量子信息处理技术[M]. 北京: 北京邮电大学出版社, 2010.

[2] Hu K, Mao Q P, Zhao S M. Round robin differential phase shift quantum key distribution protocol based on heralded single photon source and detector decoy state[J]. Acta Optica Sinica, 2017, 37(5): 0527002.
胡康, 毛钱萍, 赵生妹. 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[J]. 光学学报, 2017, 37(5): 0527002.

[3] Gottesman D, Lo H K, Lutkenhaus N, et al. Security of quantum key distribution with imperfect devices[C]//International Symposium OnInformation Theory, 2004. ISIT 2004. Proceedings, June 27-

July 2, 2004, Chicago, IL, USA. New York: IEEE Press, 2004: 136.

[4] Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography[J]. Physical Review Letters, 2005, 94(23): 230503.

[5] Lo H K, Ma X F, Chen K. Decoy state quantum key distribution[J]. Physical Review Letters, 2005, 94(23): 230504.

[6] Brassard G, Lutkenhaus N, Mor T, et al. Limitations on practical quantum cryptography[J]. Physical Review Letters, 2000, 85(6): 1330-1333.

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

[8] Curty M, Lewenstein M, Lütkenhaus N. Entanglement as a precondition for secure quantum key distribution [J]. Physical Review Letters, 2004, 92(21): 217903.

[9] Takeoka M, Guha S, Wilde M M. Fundamental rate-loss tradeoff for optical quantum key distribution [J]. Nature Communications, 2014, 5: 5235.

[10] Pirandola S, Laurenza R, Ottaviani C, et al. Fundamental limits of repeaterless quantum communications[J]. Nature Communications, 2017, 8: 15043.

[11] Lucamarini M, Yuan Z L, Dynes J F, et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters[J]. Nature, 2018, 557(7705): 400-403.

[12] Ma X F, Zeng P, Zhou H Y. Phase-matching quantum key distribution[J]. Physical Review X, 2018, 8(3): 031043.

[13] Wang X B, Yu Z W, Hu X L. Twin-field quantum key distribution with large misalignment error[J]. Physical Review A, 2018, 98(6): 062323.

[14] Cui C H, Yin Z Q, Wang R, et al. Twin-field quantum key distribution without phase postselection [J]. Physical Review Applied, 2019, 11(3): 034053.

[15] Curty M, Azuma K, Lo H K. Simple security proof of twin-field type quantum key distribution protocol [J]. Npj Quantum Information, 2019, 5: 64.

[16] Lin J, Lütkenhaus N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution[J]. Physical Review A, 2018, 98(4): 042332.

[17] Jiang C, Yu Z W, Hu X L, et al. Sending-or-not-sending twin-field quantum key distribution with discrete-phase-randomized weak coherent states[J]. Physical Review Research, 2020, 2(4): 043304.

[18] Xu H, Yu Z W, Jiang C, et al. Sending-or-not-sending twin-field quantum key distribution: breaking the direct transmission key rate[J]. Physical Review A, 2020, 101(4): 042330.

[19] Minder M, Pittaluga M, Roberts G L, et al. Experimental quantum key distribution beyond the repeaterless secret key capacity[J]. Nature Photonics, 2019, 13(5): 334-338.

[20] Liu Y, Yu Z W, Zhang W J, et al. Experimental twin-field quantum key distribution through sending or not sending[J]. Physical Review Letters, 2019, 123(10): 100505.

[21] Agarwal. Generation of pair coherent states and squeezing via the competition of four-wave mixing and amplified spontaneous emission[J]. Physical Review Letters, 1986, 57(7): 827-830.

[22] Usenko V C, Paris M G A. Multiphoton communication in lossy channels with photon-number entangled states[J]. Physical Review A, 2007, 75(4): 043812.

[23] Zhang S L, Zou X B, Li C F, et al. A universal coherent source for quantum key distribution[J]. Chinese Science Bulletin, 2009, 54(11): 1863-1871.

[24] Wang L, Zhao S M. Round-robin differential-phase-shift quantum key distribution with heralded pair-coherent sources[J]. Quantum Information Processing, 2017, 16(4): 1-15.

[25] He Y F, Zhao Y K, Guo J R, et al. Statistical fluctuation analysis of quantum key distribution protocols based on heralded pair coherent state[J]. Acta Optica Sinica, 2020, 40(7): 0727002.
何业锋, 赵艳坤, 郭佳瑞, 等. 基于标记配对相干态的量子密钥分配协议的统计涨落分析[J]. 光学学报, 2020, 40(7): 0727002.

[26] Shen Z G, Wang L, Mao Q P, et al. Round-robin differential phase shift quantum key distribution protocol based on orbital angular momentum[J]. Acta Optica Sinica, 2019, 39(2): 0227001.
沈志冈, 王乐, 毛钱萍, 等. 基于轨道角动量的循环差分相移量子密钥分发[J]. 光学学报, 2019, 39(2): 0227001.

[27] He Y F, Yang H J, Wang D, et al. Quantum key distribution based on heralded pair coherent state and orbital angular momentum[J]. Acta Optica Sinica, 2019, 39(4): 0427001.
何业锋, 杨红娟, 王登, 等. 基于标记配对相干态和轨道角动量的量子密钥分配[J]. 光学学报, 2019, 39(4): 0427001.

[28] He Y F, Zhao Y K, Li C Y, et al. Measurement-

device-independent quantum key distribution of finite detector's dead time in heralded pair coherent state [J]. Acta Optica Sinica, 2020, 40(24): 2427001.
何业锋, 赵艳坤, 李春雨, 等. 标记配对相干态下有限探测器死时间的测量设备无关量子密钥分配[J]. 光学学报, 2020, 40(24): 2427001.

[29] He Y F, Li C Y, Guo J R, et al. Passive measurement-device-independent quantum key distribution based on heralded pair coherent states [J]. Chinese Journal of Lasers, 2020, 47(9): 0912002.
何业锋, 李春雨, 郭佳瑞, 等. 基于标记配对相干态的被动测量设备无关量子密钥分配[J]. 中国激光, 2020, 47(9): 0912002.

[30] Yu Z W, Hu X L, Jiang C, et al. Sending-or-not-sending twin-field quantum key distribution in practice[J]. Scientific Reports, 2019, 9(1): 3080.

[31] Wang X B, Yang L, Peng C Z, et al. Decoy-state quantum key distribution with both source errors and statistical fluctuations[J]. New Journal of Physics, 2009, 11(7): 075006.

[32] Zhou Y H, Yu Z W, Wang X B. Making the decoy-state measurement-device-independent quantum key distribution practically useful[J]. Physical Review A, 2016, 93(4): 042324.