DOI:10.11918/j.issn.0367-6234.201709076

一种新的双模态光源诱骗态量子密钥分配方案

王 澈, 周媛媛, 周学军, 陈 霄, 张 政

(中国人民解放军 海军工程大学电子工程学院, 武汉 430000)

摘 要: 提出了一种新的基于双模态光源的被动诱骗态量子密钥分配通用方案. 作为双模态之一的标记态,在发端经过分束和检测后获得 4 类探测结果,据此,将作为信号态的另一模式分成 4 个非空脉冲集合,从而利用这 4 类脉冲进行参数估计和密钥提取. 同时,基于预报单光子源和标记配对相干态光源对此方案展开了性能分析,讨论了发端探测器不同探测效率对系统性能的影响,并对实际系统进行了统计波动分析. 仿真结果表明:方案性能在误码率和安全传输距离(可达 198.6 km)方面都优于现有基于不同光源的 3 强度诱骗态量子密钥分配方案;采用标记配对相干态光源的各方面性能均优于采用预报单光子源;密钥生成率随发端探测效率的增大而增大;考虑统计波动时,标记配对相干态光源的有效性也要优于预报单光子源,且其数据长度为 10^9 时,此方案最大安全距离达到 164 km;此方案仅需使用单一强度脉冲,在降低调制光源实现难度的同时又提升了系统性能,对 QKD 系统的工程实现具有一定的参考价值.

关键词: 量子密钥分配;无条件安全性;被动诱骗态;双模态光源;统计波动

中图分类号: TN918 **文献标志码**: A **文章编号**: 0367-6234(2018)11-0074-09

New scheme for decoy state quantum key distribution with the two-mode state source

WANG Lian, ZHOU Yuanyuan, ZHOU Xuejun, CHEN Xiao, ZHANG Zheng

(School of Electronic Engineering, Naval University of Engineering, Wuhan 430000, China)

Abstract: A new and universal scheme for passive decoy-state quantum key distribution (QKD) with the two-mode state source is proposed. As one of the two-mode, the trigger state can obtain four types of detection events after splitting and detecting at the transmitter. Based on those events, the other mode as the signal state is divided into four sets of pulses which can be used to estimate parameters and extract key. Besides, the performance analysis is carried out on the scheme with the heralded single-photon source (HSPS) and the heralded pair coherent state (HPCS). The impact of different detection efficiency is discussed. Moreover, the statistical fluctuation in the practical system is numerically studied. Our simulation results show that the performance of our scheme is superior to the existing three-intensity decoy-state QKD schemes with different sources in terms of bit error rate and secure transmission distance (up to 198.6 km). The performance of using HPCS is better than that of using HSPS, and the key generation rate increases with the rising of detection efficiency at the transmitter. Considering the statistical fluctuation, the efficiency of HPCS is also better than HSPS, and the maximum secure distance of our scheme can reach 164 km when the data length is 10^9. Furthermore, our scheme only needs to use a single intensity pulse, which reduces the difficulty of the system implementation while improving the system performance. It has certain reference value to the implementation of QKD system.

Keywords: quantum key distribution; unconditional security; passive decoy-state; two-mode state source; statistical fluctuation

量子密钥分配[1](quantum key distribution, QKD)允许合法用户 Alice 和 Bob 之间共享绝对安全的密钥,已成为近年来的研究热点[2-6]. 基于量子力学基本原理,QKD 具有传统密码学所无法企及的完美安全性,并早已得到理论上的严格证明[7-9]. 然而,实际 QKD 系统中使用的各类仪器设备存在非完美性,导致系统出现很多安全漏洞[10-13]. 例如,实际系统常采用衰减的激光脉冲来替代理想的单光子光源,这必然会使发送脉冲中含有多个光子,从而引起光子数分离攻击[13](photon number splitting, PNS),使窃听者得到合法用户的共享信息而不被发现. 为了有效克服 PNS,Hwang[14] 提出了诱骗态方案,该方案通过发送端 Alice 随机调制光脉冲到不同强度来制备诱骗态,并随信号态一同发送给接收端 Bob,双方利用检测到的诱骗态来估计系统的单光子计数率

收稿日期: 2017-09-13
基金项目: 国家自然科学基金(61302099)
作者简介: 王 澈(1992—),女,博士研究生;
周学军(1962—),男,教授,博士生导师
通信作者: 周媛媛,15623529329@163.com

下界和误码率上界，以此来判定此次通信是否安全. 此方案不仅现实可行，而且能显著提高实际 QKD 系统的安全性能[15-16].

目前，研究者们[16-23]提出许多不同的方案来实现诱骗态 QKD. 其中大多数使用的是 3 强度诱骗态[16-19]，也有一些采用 2 强度[20-21]或被动诱骗态[22]（单一强度），虽然它们实现起来较为简单，但其性能却远不如无穷诱骗态. 为获得更好的性能，Zhou 等[23]提出了一种 4 强度诱骗态方案，该方案虽然原则上能显著提高系统密钥率和安全传输距离，但在实际实现中却面临着许多技术困难，并且会造成强度调制过程中的不确定性，带来更多的光源误码.

为避免上述问题，在降低系统实现难度的同时优化系统性能，本文提出一种新的基于双模态光源的被动诱骗态（BB84）量子密钥分配方案，给出改进后双模态光源对应的光子数分布通用公式. 并结合预报单光子源（heralded single-photon source，HSPS）和标记配对相干态光源（heralded pair coherent state，HPCS）对此方案进行了详细地性能分析，讨论了发端不同探测效率的影响. 同时考虑到实际码长有限，对本方案进行了统计波动分析.

1　理论与模型

1.1　基于双模态光源的 QKD 改进方案

提出新的 QKD 方案是在传统 BB84 协议的基础上对发送端（Alice）进行了相应的改造. 由于双模态光源制备纠缠光子对来得到双模光场，两者具有相同的特性，在光子数上是完全关联的. 所以将其中之一作为信号态来进行密钥分配，另一模式作为标记态，由发送端（Alice）的探测器探测吸收，以此来预报信号态中光子数分布. 该方案利用这一优点，在发送端采用双模态光源，由信号态（S 模态）来完成编码传输，标记态（T 模态）则对信号态进行预报探测，标记态被 Alice 端的分束器分离成两态，再分别经过各自路径上的衰减器后被 Alice 端的探测器检测，由此获得 4 类探测结果. 据此可将信号态分成 4 个非空集合，从而利用这 4 类非零脉冲来实现系统的参数估计和密钥提取. 由此可知，本方案无需改变光强，只需采用单一强度的信号态就能以 4 强度诱骗态的形式实现有效且更精确的参数估计.

QKD 改进方案模型见图 1. Alice 端发射光脉冲产生双模态，其中 T 模态由 Alice 进行分束和探测，S 模态则发送给 Bob. Alice 端改造的具体过程：

1）生成双模态后，T 模态经由分束器（beam splitter，BS）分离，直接通过透射和反射得到频率相同的两束出射光，将其记为 a_1 和 a_2 态.

2）a_1 和 a_2 分别通过衰减器 A_1 和 A_2 后被发送到单光子探测器 $D_j(j=1,2)$；此处的衰减器实际上分别表示 a_1 和 a_2 态所在路径上的总的传输、探测和耦合效率 η_1、η_2，且其也可用分束器模型来表示，将其称为虚拟分束器，具体如图 1 中的放大图所示. 所以，衰减器 A_1 和 A_2 分别等效为透射率为 η_1 和 η_2 的虚拟分束器，此后，a_1 和 a_2 的反射光被丢弃，透射光则被发送到 Alice 端的单光子探测器 D_1 和 D_2 中进行检测.

3）记录 T 模态的探测器 D_1 和 D_2 所有响应结果（4 种），并可将其分成 4 类探测事件，分别记为 $X_i(i=1,2,3,4)$，即 X_1：两个探测器 D_1、D_2 都不响应，X_2：D_1 响应但 D_2 不响应，X_3：D_2 响应但 D_1 不响应，X_4：D_1 和 D_2 都响应. 由此，标记态可依据这 4 类探测事件分成 4 个脉冲集合. 同时由双模态光源的特性可知，两个模式在光子数上完全关联，则 S 模态同样被分成了 4 个不同的光脉冲集合，再经过极化旋转器（polarization rotator，PR）完成极化编码后，发送至 Bob 处进行测量. 最后双方根据 Bob 公布的测量基执行基对比等操作以提取安全密钥.

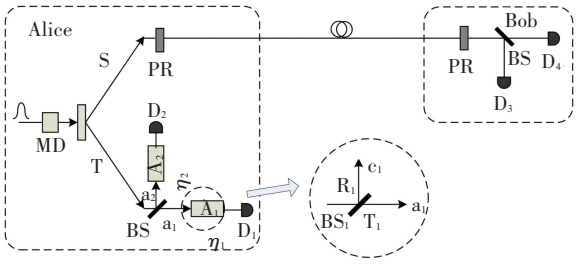


图 1　基于单一强度双模态光源的 QKD 改进方案模型

Fig.1　The model of modified QKD scheme with single-intensity two-mode state source

由于探测器 $D_1(D_2)$ 的探测效率被考虑到衰减器 $A_1(A_2)$ 中，故此处的 $D_1(D_2)$ 可看成是一个探测效率为 100% 的探测器. 所以，在 Alice 置信区域内如果探测器的入射脉冲为非真空态即含有光子，那么探测器 D_j 必定响应；反之，若其投影到真空态，D_j 的响应概率为 d_j（即该探测器的暗计数率），不响应概率则为 $(1-d_j)$. 参考文献[24]给出的被动 HSPS 光源概率公式，可得到本方案的光子数分布通用式（1）~（6）.

假设探测器的入射脉冲为 $|r_1r_2\rangle$，则此时事件 X_i 发生的概率 $P_{X_i|r_1r_2}$ 为

$$P_{X_1|r_1r_2}=\begin{cases}(1-d_1)(1-d_2)\ ;\ \exists r_1=0,r_2=0,\\ 0\ ;\ \exists r_1\neq 0 \text{ or } r_2\neq 0,\end{cases}$$

$$P_{X_2|r_1r_2}=\begin{cases}d_1(1-d_2)\ ;\ \exists r_1=0,r_2=0,\\ (1-d_2)\ ;\ \exists r_1\neq 0,r_2=0,\\ 0\ ;\ \exists r_1r_2\neq 0,\end{cases}$$

$$P_{X_3|r_1r_2}=\begin{cases}d_2(1-d_1)\ ;\ \exists r_1=0,r_2=0,\\(1-d_1)\ ;\ \exists r_1=0,r_2\neq 0,\\0;\ \exists r_1r_2\neq 0,\end{cases}$$

$$P_{X_4|r_1r_2}=\begin{cases}d_1d_2;\ \exists r_1=0,r_2=0,\\d_1;\ \exists r_1=0,r_2\neq 0,\\d_2;\ \exists r_1\neq 0,r_2=0,\\0;\ \exists r_1r_2\neq 0.\end{cases}\tag{1}$$

假设 T 模态下的任意 n 光子态(即 Alice 的发射脉冲)均以 $P_{X_i|n}$ 概率获得事件 X_i,且当 X_i 发生时,S 模态将被投影到 $\rho=\sum P_nP_{X_i|n}|n\rangle\langle n|$,其中 P_n 表示原始 S 模态的光子数分布. 将 n 光子态投影到 $|r_1r_2\rangle$ 态的概率记为 $P_{r_1r_2|n}$,则有

$$P_{X_i|n}=\sum_{r_1,r_2}P_{X_i|r_1r_2}P_{r_1r_2|n}.\tag{2}$$

事件 X_i 对应的信号态为

$$\rho=\sum_{n,r_1,r_2}P_nP_{X_i|r_1r_2}P_{r_1r_2|n}|n\rangle\langle n|,\tag{3}$$

式中 $P_{X_i|r_1r_2}$ 已由式(1)给出,下面对 $P_{r_1r_2|n}$ 进行计算.

T 模态下的 n 光子态在经过 Alice 端的 BS 后将转变为

$$\frac{1}{\sqrt{n!}}(Ta_1^{\dagger}+Ra_2^{\dagger})^n|0\rangle=\frac{1}{\sqrt{n!}}\sum_{k=0}^{n}C_n^kR^{n-k}T^ka_1^{\dagger k}a_2^{\dagger n-k}|0\rangle.\tag{4}$$

式中:$T^2=t$ 为 BS 的传输率,$R^2=1-t$ 为 BS 的反射率,$t\in[0,1/2]$.

为便于计算,用 $\eta_i(i=1,2)$ 表示衰减器 A_1、A_2 内部虚构的 BS 的总传输效率(如图 1 所示),且经过该 BS 后,只有部分透射光 $a_1(a_2)$ 被发送至探测器 $D_1(D_2)$. 因此,通过 A_1 和 A_2 后上述光子态转变为

$$|\Phi\rangle=\frac{1}{\sqrt{n!}}\sum_{k=0}^{n}\sum_{r_2=0}^{n-k}\sum_{r_1=0}^{k}C_n^kT^kR^{n-k}C_k^{r_1}T_1^{r_1}R_1^{k-r_1}\times C_{n-k}^{r_2}T_2^{r_2}R_2^{n-k-r_2}a_1^{\dagger r_1}a_2^{\dagger r_2}c_1^{\dagger k-r_1}c_2^{\dagger n-k-r_2}|0\rangle.\tag{5}$$

式中 $|T_i|^2=\eta_i$,$|R_i|^2=1-\eta_i$.

可得出 $P_{r_1r_2|n}$ 的表达式为

$$P_{r_1r_2|n}=\frac{1}{n!}\sum_{k=0}^{n}\sum_{r_2=0}^{n-k}\sum_{r_1=0}^{k}|C_n^kC_k^{r_1}C_{n-k}^{r_2}T^kR^{n-k}T_1^{r_1}R_1^{k-r_1}\times T_2^{r_2}R_2^{n-k-r_2}|^2r_1!\ r_2!\ (k-r_1)!\ (n-k-r_2)!=\sum_{k=0}^{n}\sum_{r_2=0}^{n-k}\sum_{r_1=0}^{k}\frac{n!}{r_1!\ r_2!\ (k-r_1)!\ (n-k-r_2)!}t^k\times(1-t)^{n-k}\eta_1^{r_1}\eta_2^{r_2}(1-\eta_1)^{k-r_1}(1-\eta_2)^{n-k-r_2}!.\tag{6}$$

根据式(1)~(6),若已知原始双模态光源的光子数分布 P_n,则可得到探测事件 X_i 对应的信号态(S 模态)光子数分布的具体表达式.

1.2 基于 HSPS 和 HPCS 的 QKD 改进方案

实际上,本方案只要求光源能产生光子数分布概率相关的两路信号,并未规定其具体形式,因此后续将结合常见的 HSPS 和 HPCS 光源,对方案性能进行详细分析.

HSPS 是指光脉冲经过非退化的参量下转换过程[25](parametric down-conversion, PDC),同时生成一个特性相同的双模态[26],用其中一个模式进行编码,作为信号态来传输,另一模式则由发送端的探测器探测来预报信号态的到达,即

$$|\Psi\rangle_{TS}=\sum_{n=0}^{\infty}\sqrt{P_n}|n\rangle_T|n\rangle_S,\tag{7}$$

其中,

$$P_n(\mu)=\frac{\mu^n}{n!}e^{-\mu}(\Delta t_c\ll\Delta t),\tag{8}$$

或

$$P_n(\mu)=\frac{\mu^n}{(1+\mu)^{n+1}}(\Delta t_c\gg\Delta t).\tag{9}$$

式中:$|n\rangle$ 为 n 光子态,P_n 为其对应的光子数分布概率,μ 为平均光强,Δt_c 为发射的相干时间,Δt 则为泵浦脉冲的持续时间. 通过改变文献[27-28]中所述的实验条件(如改变 Δt)可得到两种分布类型,即式(8)的泊松分布和式(9)的热分布.

HPCS 则是指由激光源产生配对相干态[29](pair coherent state, PCS),生成两个相互对称的模式,与 HSPS 光源类似,模式之一作为信号态,另一则为标记态,且两者的光子数分布都服从亚泊松分布

$$P_n(\mu)=\frac{1}{I_0(2\mu)}\frac{\mu^{2n}}{(n!)^2}.\tag{10}$$

式中 $I_0(x)$ 为修正的第一类贝塞尔函数.

在利用上述两类光源分析本方案的性能之前,必须要先估算出其单光子计数率 Y_1 下界和单光子误码率 e_1 上界. 传统 QKD 方案通常是随机改变光强制备诱骗态来估计参数,而本方案仅需 Alice 发射一个平均光强为 μ 的光脉冲,再利用 Alice 端得到的 4 类探测事件 $X_i(i=1,2,3,4)$ 就可完成相对精确的参数估计. 由于文献[23]中推导的 Y_1 和 e_1 的界限是目前常用且较精确的,其中使用了 3 个非零强度的光源进行估算,因此本文选取 3 个事件 X_i(如 X_1、X_2、X_3,概率分布为 $P_{X_1|n}$、$P_{X_2|n}$、$P_{X_3|n}$)对应的信号脉冲来估计参数,并将其分别记为 x、y 和 z 态. 假设 Alice 端量子态为 $\rho_l=\sum_n f_n^l|n\rangle\langle n|$ $(l=x,y,z)$,则光子数分布为 $f_n^x=P_{X_1|n}P_n(\mu)$ $f_n^y=P_{X_2|n}P_n(\mu)$ $f_n^z=P_{X_3|n}P_n(\mu)$.

式(8)~(10)给出原始 HSPS 和 HPCS 光源光

子数分布 $P_n(\mu)$ 的 3 种形式，结合 2.1 节的式(1)~(6)，可求出改进后本方案采用 HSPS 或 HPCS 光源所对应的光子数分布表达式 $f_n^l(f=a,b,c,\ l=x,y,z)$，具体如下.

1)采用泊松分布的 HSPS 光源时，光子数分布 $a_n^l(l=x,y,z)$ 为

$$\begin{aligned}
a_n^x &= (1-d_A)^2(1-\eta_A)^n\frac{\mu^n}{n!}e^{-\mu},\\
a_n^y &= (1-d_A)(1-\eta_A)^n\left[\left(1-\frac{t\eta_A}{1-\eta_A}\right)^n+d_A-1\right]\frac{\mu^n}{n!}e^{-\mu},\\
a_n^z &= (1-d_A)(1-\eta_A)^n\left[\left(\frac{1-t\eta_A}{1-\eta_A}\right)^n+d_A-1\right]\frac{\mu^n}{n!}e^{-\mu}.
\end{aligned}\tag{11}$$

式中：$t\in[0,1/2]$，Alice 端探测器的探测效率 $\eta_A\in[0,1]$，暗计数率 $d_A\ll 1$.

2)采用热分布的 HSPS 光源时，光子数分布 $b_n^l(l=x,y,z)$ 为

$$\begin{aligned}
b_n^x &= (1-d_A)^2(1-\eta_A)^n\frac{\mu^n}{(1+\mu)^{n+1}},\\
b_n^y &= (1-d_A)(1-\eta_A)^n\left[\left(1-\frac{t\eta_A}{1-\eta_A}\right)^n+\right.\\
&\quad \left.d_A-1\right]\frac{\mu^n}{(1+\mu)^{n+1}},\\
b_n^z &= (1-d_A)(1-\eta_A)^n\left[\left(\frac{1-t\eta_A}{1-\eta_A}\right)^n+\right.\\
&\quad \left.d_A-1\right]\frac{\mu^n}{(1+\mu)^{n+1}}.
\end{aligned}\tag{12}$$

3)采用亚泊松分布的 HPCS 光源时，光子数分布 $c_n^l(l=x,y,z)$ 为

$$\begin{aligned}
c_n^x &= (1-d_A)^2(1-\eta_A)^n\frac{1}{I_0(2\mu)}\frac{\mu^{2n}}{(n!)^2},\\
c_n^y &= (1-d_A)(1-\eta_A)^n\left[\left(1-\frac{t\eta_A}{1-\eta_A}\right)^n+\right.\\
&\quad \left.d_A-1\right]\frac{1}{I_0(2\mu)}\frac{\mu^{2n}}{(n!)^2},\\
c_n^z &= (1-d_A)(1-\eta_A)^n\left[\left(\frac{1-t\eta_A}{1-\eta_A}\right)^n+\right.\\
&\quad \left.d_A-1\right]\frac{1}{I_0(2\mu)}\frac{\mu^{2n}}{(n!)^2}.
\end{aligned}\tag{13}$$

1.3　密钥生成率计算

当 Alice 发送 ρ_l 量子态脉冲时，系统的总计数率和误码可表示为

$$S_l=\sum_{k\geqslant 0}f_k^lY_k,\ (l=x,y,z),\tag{14}$$

$$T_l=\sum_{k\geqslant 0}f_k^lt_k,(l=x,y,z).\tag{15}$$

式中：$T_l=E_lS_l,t_k=e_kY_k$，E_l 为总误码率，e_k 为 k 光子对应的误码率.

易证明上述所用的 HSPS 和 HPCS 改进光源满足如下条件

$$\frac{f_n^z}{f_n^y}\geqslant\frac{f_2^z}{f_2^y}\geqslant\frac{f_1^z}{f_1^y},\frac{f_n^y}{f_n^x}\geqslant\frac{f_2^y}{f_2^x}\geqslant\frac{f_1^y}{f_1^x},\ (n\geqslant 2,f=a,b,c).\tag{16}$$

故参考文献[23]可得出单光子计数率 Y_1 下界的通用公式为

$$\bar{Y}_1(x,y)=\frac{f_2^yS_x-f_2^xS_y+(f_2^xf_0^y-f_2^yf_0^x)Y_0}{f_1^xf_2^y-f_1^yf_2^x}.\tag{17}$$

估算出单光子误码率 e_1 上界. 为简化计算，先定义如下表达式

$$\begin{aligned}
G(i,j,k)&=(g_i^x-g_j^x)(g_j^y-g_k^y)-\\
&\quad (g_i^y-g_j^y)(g_j^x-g_k^x),
\end{aligned}\tag{18}$$

其中，

$$g_m^l=\frac{f_m^l}{f_m^z},\ (m\geqslant 1,\ l=x,y,z,f=a,b,c).\tag{19}$$

由于本方案的 HSPS 和 HPCS 改进光源已满足条件(16)，故易证明只要 $k-j\geqslant j-i\geqslant 0$，则有

$$G(i,j,k)\geqslant 0.\tag{20}$$

对于单光子误码率 e_1 来说，以往的估计中，基本是将所有误码都简单看成由单光子脉冲造成，从而得到一个比较粗略的 e_1 上界. 而本方案使用的原始双模态光源虽只产生一个强度的光脉冲，但经改造后得到了 4 个非零量子态，所以根据文献[23]，利用其中 3 个态(x、y、z 态) 就能推导出更精确的 e_1 上界.

首先，利用式(15)消除变量可得

$$t_1=\bar{t}_1+\sum_{k\geqslant 4}h_{t_1}(k)t_k,\tag{21}$$

其中，

$$\begin{aligned}
\bar{t}_1&=\frac{(f_2^yf_3^z-f_2^zf_3^y)T_x-(f_2^xf_3^z-f_2^zf_3^x)T_y}{f_1^zf_2^zf_3^zG(1,2,3)}+\\
&\quad \frac{(f_2^xf_3^y-f_2^yf_3^x)T_z+(f_2^xf_3^z-f_2^zf_3^x)f_0^yY_0e_0}{f_1^zf_2^zf_3^zG(1,2,3)}+\\
&\quad \frac{(f_2^zf_3^y-f_2^yf_3^z)f_0^x+(f_2^xf_3^y-f_2^yf_3^x)}{f_1^zf_2^zf_3^zG(1,2,3)}Y_0e_0,
\end{aligned}\tag{22}$$

$$h_{t_1}(k)=-\frac{G(2,3,k)}{G(1,2,3)},\ (k\geqslant 4).\tag{23}$$

结合式(20)可知，对于所有 $k\geqslant 4$，均满足 $h_{t_1}(k)\leqslant 0$，由此可得式(22)即为 t_1 的上界，故 e_1 上界可表示为

$$\bar{e}_1 = \frac{\bar{t}_1}{\bar{Y}_1}. \tag{24}$$

最后,由文献[22]的密钥生成率公式计算出该系统的最终密钥生成率为

$$R \geqslant a_1^z \bar{Y}_1^Z [1 - H(\bar{e}_1^X)] - S^z f H(E^z). \tag{25}$$

式中:上标 $\bar{Z}$、X 分别表示 Z 基和 X 基,由于它们是相互独立的,因此在前文推导过程中并未额外标明. S^z 和 E^z 为 Alice 端选择 z 态时对应的总计数率和总误码率,均可由实验测得[30]. f 表示实际纠错算法效率, $H_2(x)$ 表示二进制香农熵函数,且 $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$. 为简化运算,此处仅用 z 态来提取密钥,但事实上所有探测事件 $X_i(i = 1,2,3,4)$ 对应的信号脉冲都可用来提取密钥,从而使系统性能得到更大程度地提升.

2 仿真结果与分析

对最终密钥生成率进行数值计算,并通过数值仿真比较分析本文方案与已有的传统诱骗态 QKD 方案性能,同时讨论本方案密钥率与发送端探测器效率之间的关系.

参考文献[20,24]中的线性模型,可估算出观测到的系统计数率和误码率:

$$Y_n = 1 - (1 - Y_0)(1 - \eta)^n, \tag{26}$$

$$e_n = \frac{e_0 Y_0 (1-\eta)^n + e_d[1 - (1-\eta)^n]}{1 - (1 - Y_0)(1 - \eta)^n}. \tag{27}$$

式中:$\eta = \eta_B \times 10^{-\alpha L/10}$ 为全局传输效率, η_B 为 Bob 端的探测效率, α 为信道的损耗系数,设为 0.2 dB/km, L 为传输距离. 据此可得出不同量子态的总计数率 S^l 和总误码率 $E^l(l = x,y,z)$. 主要仿真参数[23-24]见表 1,信号态则根据传输距离选用最优信号态强度.

表 1 主要仿真参数设置

Tab.1 Main parameters set in numerical simulations

参量	e_d	η_A	d_A	η_B	d_B
取值	1.5%	0.75	1.0×10^{-6}	0.145	3.0×10^{-6}

2.1 与其他 QKD 方案的性能比较

为便于比较,传统 QKD 方案的诱骗态依次设为 0、$\mu_1 = 0.1$. 仿真结果如图 2~4 所示,图中各曲线分别表示的是:1)本文方案——基于泊松分布的 HSPS 光源、基于热分布的 HSPS 光源以及基于 HPCS 光源的单强度 QKD 改进方案;2)基于 WCS 光源的 3 强度 QKD 方案[23];3)基于 HSPS 光源的 3 强度 QKD 方案[23].

从图 2 可看出:1)不论采用哪种双模态光源,本文方案的 e_1 上界都明显小于 WCS 或 HSPS 3 强度传统 QKD 方案. 这是因为本方案虽只产生单一强度的光脉冲,但经改造发送端后,获得了 4 个可参与系统参数估计的脉冲集合,从而能得到更加精确的 e_1 上界. 2)对于本文方案来说,采用 HPCS 的 e_1 上界要略优于 HSPS,而采用泊松分布的 HSPS 则要优于热分布的 HSPS,但三者都比较相近.

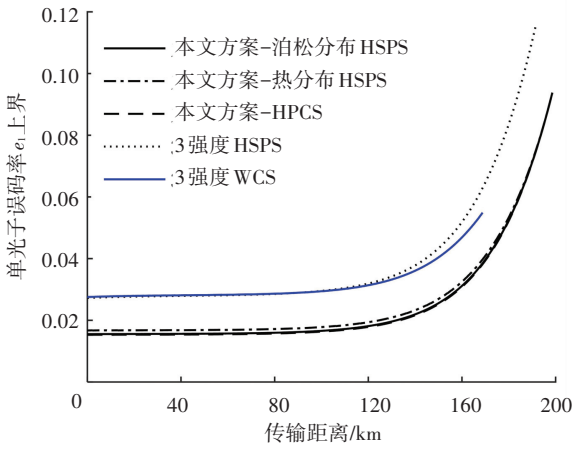


图 2 不同 QKD 方案下的单光子误码率上界

Fig. 2 The upper bound of single photon error rate under different QKD schemes

从图 3 可看出:1)基于泊松分布 HSPS 和 HPCS 的本文方案的最优信号态强度要优于 WCS 和 HSPS 3 强度方案,而基于热分布 HSPS 的本文方案总体要略低于上述两种传统方案. 2)对于采用不同光源的本文方案,最优信号态强度从大到小依次为:HPCS、泊松分布的 HSPS 以及热分布的 HSPS,且 HPCS 的最优信号态强度接近于 1. 而信号态强度越大,可使密钥率在一定范围内得到提高.

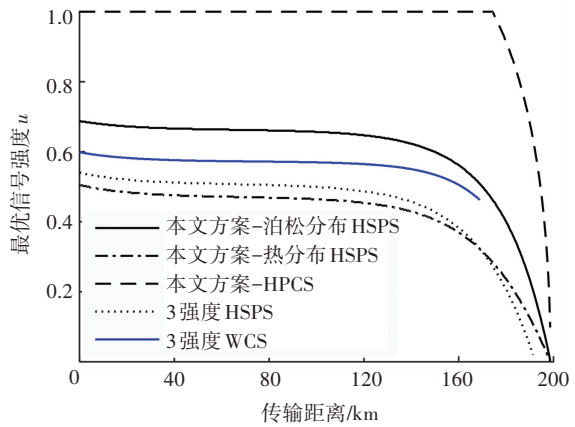


图 3 不同 QKD 方案下的最优信号态强度

Fig.3 The optimal intensity of signal state under different QKD schemes

图 4 表明:1)基于不同光源的本文方案的最大安

全距离都为 198.6 km，这均要高于 WCS 3 强度方案(168 km)和 HSPS 3 强度方案(191 km). 2)基于 HPCS 的本文方案的密钥率最大，均要优于其他 4 种方案. 这主要是因为 HPCS 对应的最优信号态强度最大. 且基于泊松分布 HSPS 的本文方案的密钥率要高于热分布 HSPS. 3)WCS 3 强度方案和其他 3 种 HSPS 方案(包括本文方案)的性能曲线都存在一个交点. 在交点之前，WCS 方案的密钥率要略高于 HSPS 方案，在交点之后则相反. 这一差距主要是由 HSPS 中多光子脉冲比例大于 WCS 所导致，但是 HSPS 可利用标记光子数法来降低暗计数的影响，延长有效传输距离.

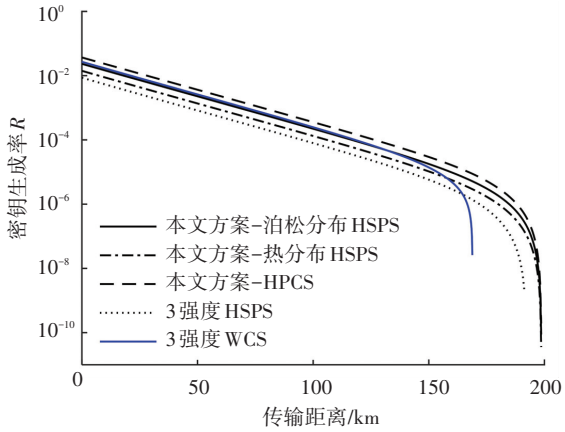


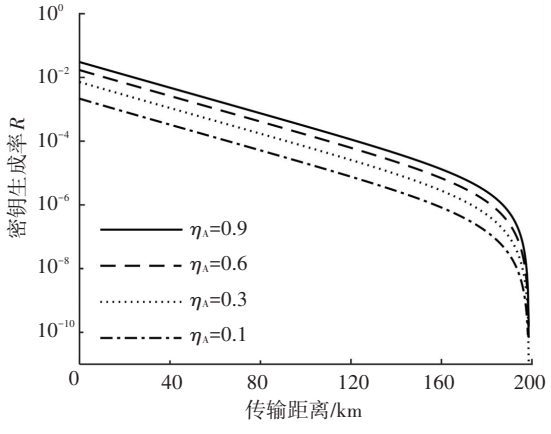
图 4　不同 QKD 方案下的最终密钥生成率

Fig.4　The key generation rate under different QKD schemes

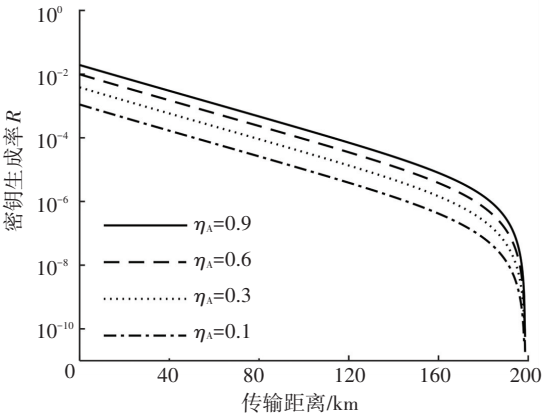
综上所述，本文方案虽只采用单一强度的脉冲，却能使系统性能得到提升. 且若采用 HPCS 光源，此方案可在最大程度上优化系统性能，获得最佳的密钥生成率和最大的安全传输距离.

2.2　QKD 改进方案密钥率与发端探测效率的关系

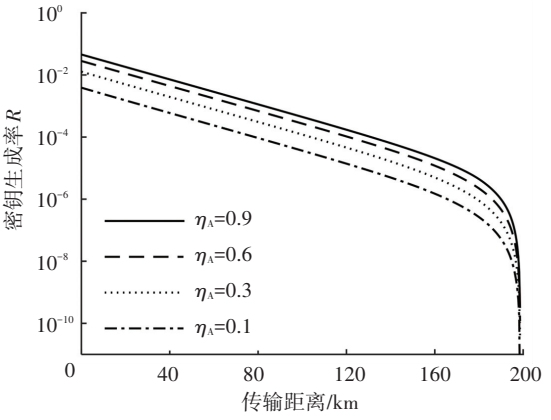
假定 Alice 端的两个探测器完全相同，其探测效率 η_A 依次取为 0.1、0.3、0.6、0.9，其他仿真参数与表 1 一致. 通过对密钥生成率的数值仿真，可得到基于不同光源的本文方案在发送端不同探测效率条件下的性能曲线，见图 5(a)~(c).



(a) 基于泊松分布的 HSPS 光源



(b)基于热分布的 HSPS 光源



(c)基于 HPCS 光源

图 5　发端不同探测效率下密钥生成率的变化

Fig. 5　The change of key generation rate under different detection efficiency at the sender

从图 5 可看出，当 Alice 端探测器的探测效率 η_A 从 0.1 变化到 0.9 时，无论采用哪种双模态光源，本文方案的最大安全距离并未发生变化，但不同光源对应的密钥生成率却得到了逐步提升. 由于探测效率越高，就有越多的非空脉冲被成功探测，这使得在 Alice 端划分信号态的 4 类探测事件对应的概率增大，从而提高了该系统的性能.

3　统计波动分析

在实际 QKD 系统中，生成的量子密钥往往都是有限长的，而密钥有限长效应会引入统计波动问题，从而降低密钥生成率和安全传输距离. 因此，在实际系统的参数估计过程中需要考虑数据有限长效应. 本节将采用文献[30]中的有限密钥分析法对本文方案进行统计波动分析.

根据标准波动理论，可得

$$X = E[X] + \delta, \tag{28}$$

$$\Pr(|X - E[X]| \geqslant \Delta) \leqslant \varepsilon. \tag{29}$$

式中：$X = \frac{1}{n}\sum_{i=1}^{n} X_i$ 为变量 X_i 的经验均值，$E[X]$ 为 X 的期望值，$\delta \in [-\Delta, \hat{\Delta}]$，$\Delta = I(X, \varepsilon^4/16)$，$\hat{\Delta} =$

$I(X,\varepsilon^{3/2})$，其中 $I(a,b)=\sqrt{2a\ln(b^{-1})}$.

若总脉冲数(即数据长度)记为 N，可知 $N\hat{S}_l$ 为实际观测到的事件 $l=x,y,z$ 被 Bob 成功探测的次数，$N\hat{T}_l$ 则为相应的误码数，其与理论估计值间以 $1-2\varepsilon$ 的概率满足如下关系

$$N\hat{S}_l = NS_l + \delta_l, \quad N\hat{T}_l = NT_l + \delta_l'. \tag{30}$$

其中：$\delta_l \in [-\Delta_l,\hat{\Delta}_l]$，$\Delta_l = I(N\hat{S}_l,\varepsilon^4/16)$，$\hat{\Delta} = I(N\hat{S}_l,\varepsilon^{3/2})$，且 $\delta_l' \in [-\Delta_l',\hat{\Delta}_l']$，$\Delta_l' = I(N\hat{T}_l,\varepsilon^4/16)$，$\hat{\Delta}' = I(N\hat{T}_l,\varepsilon^{3/2})$.

为简化计算，式(30)可写为

$$\hat{S}_l - \frac{\hat{\Delta}_l}{N} \leqslant S_l \leqslant \hat{S}_l + \frac{\Delta_l}{N}, \hat{T}_l - \frac{\hat{\Delta}_l'}{N} \leqslant T_l \leqslant \hat{T}_l + \frac{\Delta_l'}{N}. \tag{31}$$

由此，可得到如下不等式：

$$\begin{aligned} &\hat{S}_l(1-\Delta_1^l) \leqslant S_l \leqslant \hat{S}_l(1+\Delta_2^l), \\ &\hat{T}_l(1-\Delta_3^l) \leqslant T_l \leqslant \hat{T}_l(1+\Delta_4^l). \end{aligned} \tag{32}$$

其中：

$$\Delta_1^l = \sqrt{2\ln(\varepsilon^{-3/2})/N\hat{S}_l}, \Delta_2^l = \sqrt{2\ln(16\varepsilon^{-4})/N\hat{S}_l},$$

且

$$\Delta_3^l = \sqrt{2\ln(\varepsilon^{-3/2})/N\hat{T}_l}, \Delta_4^l = \sqrt{2\ln(16\varepsilon^{-4})/N\hat{T}_l}.$$

再结合式(17)、(22)和(24)，可得统计波动下的 Y_1 下界和 e_1 上界：

$$\underline{\underline{Y}}_1 = \frac{f^x_2 S_x(1-\Delta_1^x) - f^x_2 S_y(1+\Delta_2^y) + (f^x_2 f^y_0 - f^y_2 f^x_0)\underline{Y}_0}{f^x_1 f^y_2 - f^y_1 f^x_2}, \tag{33}$$

$$\bar{\bar{e}}_1 = \frac{\bar{\bar{t}}_1}{\underline{\underline{Y}}_1}, \tag{34}$$

其中：

$$\begin{aligned} \bar{\bar{t}}_1 = {} & \frac{(f^y_2 f^z_3 - f^z_2 f^y_3)\hat{T}_x(1+\Delta_4^x)}{f^z_1 f^z_2 f^z_3 G(1,2,3)} - \\ & \frac{(f^x_2 f^z_3 - f^z_2 f^x_3)\hat{T}_y(1-\Delta_3^y)}{f^z_1 f^z_2 f^z_3 G(1,2,3)} + \\ & \frac{(f^x_2 f^y_3 - f^y_2 f^x_3)\hat{T}_z(1+\Delta_4^z)}{f^z_1 f^z_2 f^z_3 G(1,2,3)} + \\ & \frac{(f^x_2 f^z_3 - f^z_2 f^x_3) f^y_0 \bar{Y}_0 e_0}{f^z_1 f^z_2 f^z_3 G(1,2,3)} + \\ & \frac{(f^z_2 f^y_3 - f^y_2 f^z_3) f^x_0 + (f^x_2 f^y_3 - f^y_2 f^x_3)}{f^z_1 f^z_2 f^z_3 G(1,2,3)} \bar{Y}_0 e_0. \end{aligned} \tag{35}$$

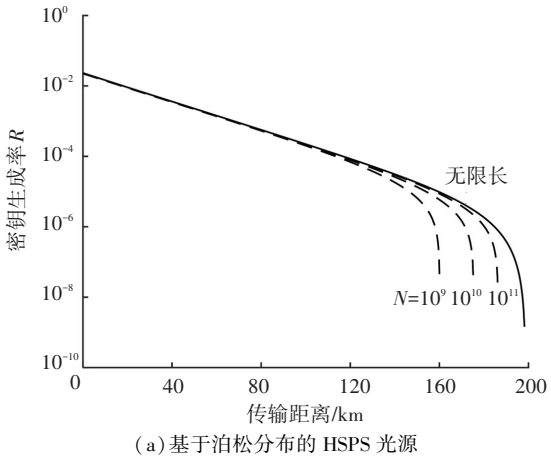
且 $\underline{Y}_0 = Y_0\left(1-\sqrt{2\ln(\varepsilon^{-3/2})/NY_0}\right)$，

$\bar{Y}_0 = Y_0\left(1+\sqrt{2\ln(16\varepsilon^{-4})/NY_0}\right)$.

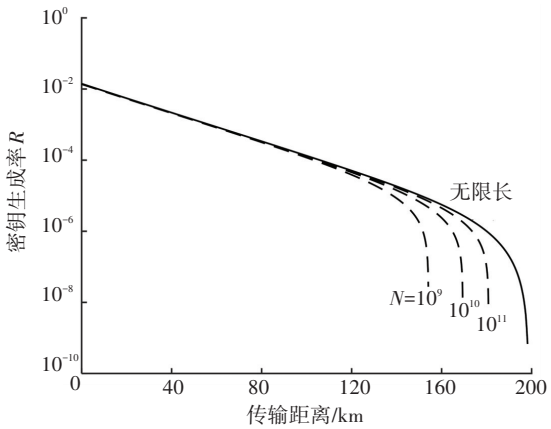
最后将式(33)~(35)代入式(25)中，可得统计波动条件下的最终密钥生成率

$$R \geqslant a_1^z \underline{\underline{Y}}_1^Z [1 - H(\bar{e}_1^X)] - S^z f H(E^z). \tag{36}$$

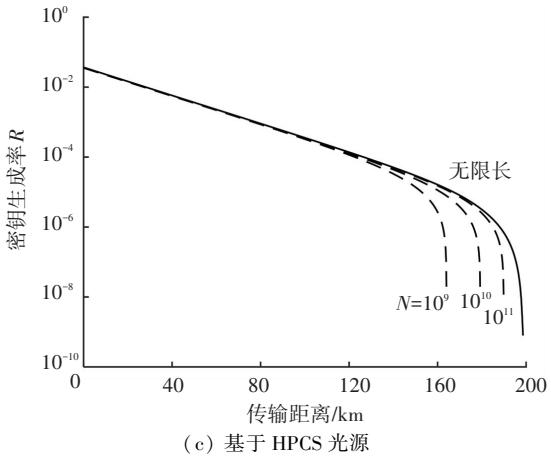
设定系统的不安全系数 $\varepsilon = 10^{-7}$，Alice 发送总脉冲数 $N = 10^9 \sim 10^{11}$. 仿真结果如图 6(a)~(c)所示，分别为本文方案采用不同双模态光源时，不同数据长度对应的密钥生成率的变化曲线，其中实线表示理想情况下即数据无限长时的密钥生成率，虚线则表示数据有限长时对应的密钥生成率.



(a)基于泊松分布的 HSPS 光源



(b)基于热分布的 HSPS 光源



(c) 基于 HPCS 光源

图 6 不同统计波动下密钥生成率的变化

Fig. 6 The change of key generation rate under statistical fluctuation

从图 6 可看出，1）对本文方案来说，不论采用哪种双模态光源，在当前的实验条件下，数据有限长效应并未导致密钥生成率的急剧下滑，且在较远距离处仍能获得较高的密钥生成率. 2）就不同光源而言，对比图 6(a)～(c)可知，统计波动对基于 HPCS 的本文方案的影响要小于 HSPS 的. 对于 HPCS 光源，总脉冲数 $N = 10^9$ 时，本方案的最大安全距离就可达 164 km；总脉冲数 $N = 10^{11}$ 时，最大安全距离达 190 km，且在 182 km 光纤链路上仍具有较大的密钥生成率，其性能比较接近理想情况.

4　结　论

1）基于 BB84 协议，提出一种双模态光源被动诱骗态量子密钥分配改进方案. 该方案无需调制脉冲强度，只需发送单一强度的双模态光源，其中标记态在发端被分束和检测后得到 4 类探测结果，据此将信号态分成 4 个脉冲集合来估计参数，所以本方案能获得更精确的单光子计数率下界和误码率上界.

2）基于 HSPS 光源和 HPCS 光源，在密钥生成率、误码率和最优信号态强度方面对此方案进行了比较分析，讨论了发端不同探测效率对该方案的影响，同时分析了实际系统有限码长效应的影响.

3）仿真结果表明：本方案性能在误码率和安全传输距离方面均优于现有基于 HSPS 和 WCS 的 3 强度 QKD 方案；基于 HPCS 的本文方案可使密钥生成率得到显著提升，其性能不仅优于其他传统方案，总体来说也优于基于 HSPS 的本文方案，但两者的安全传输距离相同，均可达 198.6 km；随着发端探测效率的增大，本方案性能也随之明显提高；在统计波动条件下，本方案在远距离处仍具有较大的密钥生成率，且数据长度达到 10^9 以上即可保证较大的安全传输距离（如 164 km 以上）.

4）与其他多强度 QKD 方案相比，本方案仅需采用单一强度脉冲，从而避免了光强调制误差，降低了系统实现难度，易于工程实现.

参考文献

[1] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing[C]//Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE, New York, 1984, 175

[2] ZHOU Yuanyuan, ZHOU Xuejun, SU Binbin. A measurement-device-independent quantum key distribution protocol with a heralded single photon source[J]. Optoelectron. Lett., 2016, 12(2): 148. DOI: 10.1007/s11801-016-5275-3

[3] BARTKIEWCZ K, CERNOCH A, LEMR K, et al. Temporal steering and security of quantum key distribution with mutually-unbiased bases against individual attacks[J]. Phys. Rev. A, 2016, 93(6): 062345. DOI: 10.1103/PhysRevA.93.062345

[4] 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)：331. DOI：10.3788/aos201737.0527002
HU Kang, MAO Qianping, ZHAO Shengmei. 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): 331. DOI: 10.3788/aos201737.0527002

[5] WANG Le, ZHAO Shengmei. Round-robin differential-phase-shift quantum key distribution with heralded pair-coherent sources[J]. Quantum Inf. Process., 2017, 16(4): 100. DOI: 10.1007/s11128-017-1550-x

[6] 何业锋. 基于四粒子纠缠态的两方量子密钥协商协议[J]. 电子科技大学学报，2017，46(2)：340. DOI：10.3969/j.issn.1001-0548.2017.02.004
HE Yefeng. Two-party quantum key agreement protocols based on four-particle entangled states[J]. Journal of University of Electronic Science and Technology of China, 2017, 46(2): 340. DOI: 10.3969/j.issn.1001-0548.2017.02.004

[7] LO H K, CHAU H F. Unconditional security of quantum key distribution over arbitrarily long distances[J]. Science, 1999, 283(5410): 2050. DOI: 10.1126/science.283.5410.2050

[8] LO H K, CHAU H F, ARDEHALI M. Efficient quantum key distribution scheme and a proof of its unconditional security[J]. Journal of Cryptology, 2005, 18(2): 133. DOI: 10.1007/s00145-004-0142-y

[9] MAYERS D. Unconditional security in quantum cryptography[J]. Journal of the ACM, 2001, 48(3): 351. DOI: 10.1145/382780.382781

[10] HUANG Jingzheng, YIN Zhenqiang, WANG Shuang, et al. Effect of intensity modulator extinction on practical quantum key distribution[J]. Eur. Phys. J. D, 2012, 66(6): 159. DOI: 10.1140/epjd/e2012-20757-5

[11] SUN Shihai, GAO Ming, JIANG Musheng, et al. Partially random phase attack to the practical two-way quantum-key-distribution system[J]. Phys. Rev. A, 2012, 85(3): 032304. DOI: 10.1103/PhysRevA.85.032304

[12] PFISTER C, COLES P J, WEHNER S, et al. Sifting attacks in finite-size quantum key distribution[J]. New J. Phys., 2016, 18(5): 053001. DOI: 10.1088/1367-2630/18/5/053001

[13] BRASSARD G, LTTTKENHAUS N, MOR T, et al. Limitations on practical quantum cryptography[J]. Phys. Rev. Lett., 2000, 85(6): 1330. DOI: 10.1103/PhysRevLett.85.1330

[14] HWANG W Y. Quantum key distribution with high loss: toward global secure communication[J]. Phys. Rev. Lett., 2003, 91(5): 057901. DOI: 10.1103/PhysRevLett.91.057901

[15] LO H K, MA X, CHEN K. Decoy state quantum key distribution[J]. Phys. Rev. Lett., 2005, 94(23): 230504. DOI: 10.1103/PhysRevLett.94.230504

[16] PENG Chengzhi, ZHANG Jun, YANG Dong, et al. Experimental long-distance decoy-state quantum key distribution based on polarization encoding[J]. Phys. Rev. Lett., 2007, 98(1): 010505. DOI: 10.1103/PhysRevLett.98.010505

[17] WANG Qin, CHEN W, XAVIER G, et al. Experimental decoy-state quantum key distribution with a sub-poissonian heralded single-photon source[J]. Phys. Rev. Lett., 2008, 100(9): 090501. DOI: 10.1103/PhysRevLett.100.090501

[18] WANG Qin, WANG Xiangbin, GUO Guangcan. Practical decoy-state method in quantum key distribution with a heralded single-photon source[J]. Phys. Rev. A, 2007, 75(1): 012312. DOI: 10.1103/PhysRevA.75.012312

[19] WANG Xiangbin. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors[J]. Phys. Rev. A, 2013, 87(1): 012320. DOI: 10.1103/PhysRevA.87.012320

[20] ZHAO Yi, QI Bing, MA Xiongfeng, et al. Experimental quantum key distribution with decoy states[J]. Phys. Rev. Lett., 2006, 96(7): 070502. DOI: 10.1103/PhysRevLett.96.070502

[21] MA Xiongfeng, QI Bing, ZHAO Yi, et al. Practical decoy state for quantum key distribution [J]. Phys. Rev. A, 2005, 72(1): 012326. DOI: 10.1103/PhysRevA.72.012326

[22] CURTY M, MA Xiongfeng, QI Bing, et al. Passive decoy-state quantum key distribution with practical light sources[J]. Phys. Rev. A, 2010, 81(2): 022310. DOI: 10.1103/PhysRevA.81.022310

[23] ZHOU Yiheng, YU Zongwei, WANG Xiangbin. Tightened estimation can improve the key rate of measurement-device-independent quantum key distribution by more than 100%[J]. Phys. Rev. A, 2014, 89(5): 052325. DOI: 10.1103/PhysRevA.89.052325

[24] WANG Qin, ZHANG Chunhui, WANG Xiangbin. Scheme for realizing passive quantum key distribution with heralded single-photon sources[J]. Phys. Rev. A, 2016, 93(3): 032312. DOI: 10.1103/PhysRevA.93.032312

[25] 周淳. 有限长诱骗态量子密钥分配安全性研究 [D]. 郑州: 解放军信息工程大学, 2014
ZHOU Chun. Research on security of decoy-state quantum key distribution with finite resources[D]. Zhengzhou: PLA Information Engineering University, 2014

[26] LUTKENHAUS N, Security against individual attacks for realistic quantum key distribution [J]. Phys. Rev. A, 2000, 61(5): 052304. DOI: 10.1103/PhysRevA.61.052304

[27] MORI S, SODERHOLM J, NAMEKATA N, et al. On the distribution of 1550-nm photon pairs efficiently generated using a periodically poled lithium niobate waveguide[J]. Opt. Commun., 2006, 264(1):156. DOI: 10.1016/j.optcom.2006.02.010

[28] RIBORDY G, BRENDEL J, GAUTHIER J D, et al. Long-distance entanglement-based quantum key distribution[J]. Phys. Rev. A, 2000, 63(1): 012309. DOI: 10.1103/PhysRevA.63.012309

[29] ZHANG Shengli, ZOU Xubo, LI Chuanfeng, et al. A univeral coherent source for quantum key distribution[J]. Chin. Sci. Bull., 2009, 54(11): 1863. DOI: 10.1007/s11434-009-0330-0

[30] ZHANG Chunhui , LUO Sunlong , GUO Guangcan, et al. Approaching the ideal quantum key distribution with two- intensity decoy states[J]. Phys. Rev. A, 2015, 92(2): 022332. DOI: 10.1103/PhysRevA.92.022332

(编辑 苗秀芝)

(上接第 58 页)

[8] Rehman O U, Yang J, Zhou Q, et al. A modified QPSO algorithm applied to engineering inverse problems in electromagnetics [J]. International Journal of Applied Electromagnetics and Mechanics, 2017, 54(1): 107. DOI: 10.3233/JAE-160114

[9] Nayak R, Patra D. An edge preserving IBP based super resolution image reconstruction using P-spline and MuCSO-QPSO algorithm [J]. Microsystem Technologies, 2017, 23(3): 553. DOI: 10.1007/s00542-016-2972

[10] Xu X, Shan D, Wang G, et al. Multimodal medical image fusion using PCNN optimized by the QPSO algorithm[J]. Applied Soft Computing, 2016, 46: 588. DOI: 10.1016/j.asoc.2016.03.028

[11] 孙俊. 量子行为粒子群优化算法研究[D].无锡:江南大学, 2009. DOI: 10.7666/d.y1585071
Sun Jun. Research on quantum-behaved particle swarm optimization [D]. Wuxi: Jiangnan University, 2009. DOI: 10. 7666/d.y1585071. DOI: 10.7666/d.y1585071

[12] Sun J, Wu X, Palade V, et al. Convergence analysis and improvements of quantum-behaved particle swarm optimization [J]. Information Sciences, 2012, 193: 81. DOI: 10.1016/j.ins.2012.01.005

[13] Li Y, Xiang R, Jiao L, et al. An improved cooperative quantum-behaved particle swarm optimization [J]. Soft Computing, 2012, 16(6): 1061. DOI: 10. 1007/ s005 00 -012-0803-y

[14] Xi M, Sun J, Xu W. An improved quantum-behave particle swarm optimization algorithm with weighted mean best position [J]. Applied Mathematics and Computation, 2008, 205(2): 751. DOI: 10.1016/j.amc.2008.05.135

[15] Suganthan P N. Particle swarm optimizer with neighbourhood operator[C]//Evolutionary Computation, 1999. CEC 99. Proceedings of the 1999 Congress on. IEEE, 1999, 3: 1958. DOI: 10. 11 09 / CEC. 1999.7 85514

[16] Kennedy J. Small worlds and mega-minds: effects of neighborhood topology on particle swarm performance [C] //Evolutionary Computation, 1999. CEC 99. Proceedings of the 1999 Congress on. IEEE, 1999, 3: 1931. DOI: 10.1109/CEC.1999.785509

[17] Mirjalili S, Mirjalili S M, Lewis A. Grey wolf optimizer [J]. Advances in Engineering Software, 2014, 69: 46. DOI: 10.1016/j.advengsoft.2013.12.007

(编辑 苗秀芝)