物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于相干叠加态的非正交编码诱骗态量子密钥分发

孙伟　尹华磊　孙祥祥　陈腾云

Nonorthogonal decoy-state quantum key distribution based on coherent-state superpositions

Sun Wei　Yin Hua-Lei　Sun Xiang-Xiang　Chen Teng-Yun

引用信息 Citation: Acta Physica Sinica, 65, 080301 (2016)　DOI: 10.7498/aps.65.080301
在线阅读 View online: http://dx.doi.org/10.7498/aps.65.080301
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2016/V65/I8

基于相干叠加态的非正交编码诱骗态量子密钥分发*

孙伟[1)†] 尹华磊[2)] 孙祥祥[1)] 陈腾云[2)]

1) (中国科学技术大学近代物理系, 合肥 230026)

2) (中国科学技术大学, 微尺度物质科学国家实验室, 合肥 230026)

(2015 年 12 月 10 日收到; 2016 年 1 月 11 日收到修改稿)

非正交编码协议和诱骗态方法可以有效地抵御光子数分离攻击. 由于相干叠加态中单光子成分高达90%, 常作为单光子量子比特的替代出现, 用于量子信息过程处理和计算. 本文结合非正交编码协议和诱骗态方法提出一种新的量子密钥分发方案, 光源采用相干叠加态, 推导了单光子的密钥生成速率、计数率下限和误码率的上限, 利用 Matlab 模拟了无限多诱骗态情况下和有限多诱骗态情况下密钥生成速率和传输距离的关系, 得出该方案可以提升密钥生成速率并且提高安全传输距离, 验证了该方案可以进一步提高量子密钥分发系统的性能.

关键词: 相干叠加态, 密钥生成速率, 计数率, 误码率

PACS: 03.65.–w, 03.67.–a, 42.50.–p **DOI:** 10.7498/aps.65.080301

1 引 言

量子密钥分发(quautum key distribution, QKD)[1,2]为通信双方在即使有窃听者存在的前提下也能享有安全密钥提供了基于量子力学[3]的信息理论安全保证. 但是, 实际QKD 系统并不完美, 不能完全满足QKD的理论安全证明前提. 例如, 实际光源采用的都是强衰减的弱相干态激光脉冲(weak coherent pulse, WCP), 并非严格意义上的单光子源, 以致窃听者Eve可以实施光子数分离攻击(photon number splitting, PNS)[4].

幸运的是, 诱骗态方法和非正交编码协议可以有效地抵御PNS. 文献[5]提出了可以抵抗PNS的诱骗态方案, 其基本思想为: Alice在发送光脉冲给Bob时, 在信号态中随机加入不同强度的诱骗态. 通信结束后, Alice和Bob利用检测到的诱骗态脉冲结果来估计信号态计数率的下限和误码率的上限, 如果得到的结果与理论安全值相差太大, 则认为有Eve存在. 2004年, Scarani等[6]提出了SARG04协议, 该协议采用与BB84协议[1]相同的两组共轭基中的四个量子态进行量子密钥分发, 采用相同的实验测量设备, 他们的区别仅在于经典的编码方式上, SARG04协议采用四态非正交的编码方式, Alice发送双光子也可以安全成码.

诱骗态方法和SARG04协议相结合的理论即SARG04协议诱骗态QKD方案[7–9]随后被提出, 基于参量下转换光子对的一些诱骗态方案[10–14]相继被提出, 基于条件下转换光子对的一些诱骗态方案[15]也相继被提出. 这些方案中光源采用弱相干态或者自发参量下转化光子对.

相干叠加态(coherent-state superpositions, CSS)[16]通常被称为薛定谔猫态, 定义是经典可区分态的量子相干叠加. 由于CSS中单光子成分高达90%, 常作为单光子量子比特的替代出现, 用于量子信息过程处理和计算, 例如容错的线性光学

* 安徽省自然科学基金(批准号: 1508085J02)资助的课题.

† 通信作者. E-mail: sunwei85@mail.ustc.edu.cn

量子计算[17]、测量设备无关的量子密钥分发、量子隐形传态[18−20]、量子中继器[21]、长距离纠缠分发[22]和量子精密测量[23]. 小振幅的近似CSS可以由压缩真空态的减光子操作产生[24], 大振幅的近似CSS可以由Fock态产生, 用单零差检测探测[25].

近来, 随着CSS制备技术的发展, 人们开始从理论上利用CSS来进行QKD.

本文在这些理论的基础上, 提出了一种基于CSS的SARG04协议诱骗态QKD新方案, 该方案采用诱骗态方法和SARG04协议相结合的方式, 但是光源采用CSS.

2 基于CSS的SARG04协议诱骗态QKD方案

2.1 无限多诱骗态QKD方案

文献[16]给出了CSS下光子数分布$P_n(u)$为

$$P_n(u)=\frac{1}{\sinh u}\sum_{n=0}^{\infty}\frac{u^{2n+1}}{(2n+1)!},\tag{1}$$

式中n表示光子数, u表示平均强度, 需要注意的是, 这里仅考虑光子数为奇数的光脉冲.

文献[7]给出了SARG04协议下相关参数的计算公式. 具体如下: 设量子信道的衰减率为α, 量子信道距离为L, 则通信双方Alice和Bob间的传输效率为$\eta_{\rm AB}=10^{-\alpha L/10}$, Bob端探测器的探测效率为$\eta_{\rm Bob}$, 则信道总的传输效率为$\eta=\eta_{\rm AB}\cdot\eta_{\rm Bob}=10^{-\alpha L/10}\cdot\eta_{\rm Bob}$, 用$Y_{n,\rm SARG04}$表示Alice发送$n$光子脉冲时引起Bob端探测器计数率,

$$\begin{aligned}&Y_{n,\rm SARG04}\\=&\eta_n\left(\frac{e_{\rm detector}}{2}+\frac{1}{4}\right)+(1-\eta_n)p_{\rm dark}\frac{1}{2},\end{aligned}\tag{2}$$

式中$e_{\rm detector}$为信道中的噪声、脉冲的后向反射和探测器本身的缺陷等因素所引起的Bob端探测器的错误响应概率, $p_{\rm dark}$为背景噪声引起的暗计数, η_n为n光子脉冲引起的计数率, $\eta_n=1-(1-\eta)^n$.

Alice发送n光子脉冲时引起Bob端探测器错误探测概率(误码率)$e_{n,\rm SARG04}$为

$$e_{n,\rm SARG04}=\frac{\eta_n\dfrac{e_{\rm detector}}{2}+(1-\eta_n)p_{\rm dark}\dfrac{1}{4}}{Y_{n,\rm SARG04}},\tag{3}$$

信号态的计数率$Q_{u,\rm SARG04}$为

$$\begin{aligned}&Q_{u,\rm SARG04}\\=&\sum_{n=0}^{\infty}Y_{n,\rm SARG04}P_n(u)\\=&\frac{1}{4}\big\{1+2e_{\rm d}\\&+\operatorname{csch}(u)\sinh[(-1+\eta)u]\\&+2e_{\rm d}\operatorname{csch}(u)\sinh[(-1+\eta)u]\\&-2p_{\rm d}\operatorname{csch}(u)\sinh[(-1+\eta)u]\big\},\end{aligned}\tag{4}$$

信号态的误码率$E_{u,\rm SARG04}$为

$$\begin{aligned}&E_{u,\rm SARG04}\\=&\frac{\displaystyle\sum_{n=0}^{\infty}e_{n,\rm SARG04}Y_{n,\rm SARG04}P_n(u)}{Q_{u,\rm SARG04}}\\=&\frac{1}{4}\big\{2e_{\rm d}+2e_{\rm d}\operatorname{csch}(u)\sinh[(-1+\eta)u]\\&-p_{\rm d}\operatorname{csch}(u)\sinh[(-1+\eta)u]\big\}\\&\times Q_{u,\rm SARG04}^{-1}.\end{aligned}\tag{5}$$

用$e_{\rm p}$表示相位错误率, $e_{\rm b}$表示比特错误率, e_1表示单光子比特错误率, 文献[7]推导出在SARG04协议下, 三者有如下关系:

$$\begin{aligned}e_{\rm p}&=\frac{3}{2}e_{\rm b},\\a&=\frac{1}{2}e_1,\\e_{\rm b}&=e_1.\end{aligned}\tag{6}$$

文献[26]给出$H_2(Z_1/X_1)$的计算公式, 具体如下:

$$\begin{aligned}&H_2(Z_1/X_1)\\=&-[1-(e_{\rm p}+e_{\rm b})+a]\log_2\frac{1-(e_{\rm p}+e_{\rm b})+a}{1-e_{\rm b}}\\&-(e_{\rm p}-a)\log_2\frac{e_{\rm p}-a}{1-e_{\rm b}}-(e_{\rm b}-a)\log_2\frac{e_{\rm b}-a}{1-e_{\rm p}}\\&-a\log_2\frac{a}{e_{\rm b}}.\end{aligned}\tag{7}$$

得出SARG04协议下, $H_2(Z_1/X_1)$与比特错误率e_1的关系式:

$$\begin{aligned}&H_2(Z_1/X_1)\\=&-[1-2e_1]\log_2\frac{1-2e_1}{1-e_1}-e_1\log_2\frac{e_1}{1-e_1}\\&-\frac{1}{2}e_1\log_2\frac{e_1}{2-3e_1}+\frac{1}{2}e_1.\end{aligned}\tag{8}$$

文献 [7] 给出了 SARG04 协议的安全密钥生成速率,

$$\begin{aligned} R_{\mathrm{SARG04}} =& -Q_u f(E_u) H_2(E_u) \\ &+ Q_1[1 - H_2(Z_1/X_1)] \\ &+ Q_2[1 - H_2(Z_2/X_2)], \end{aligned} \tag{9}$$

式中 $f(E_u)$ 为纠错效率, $H_2(x) = x\log_2 x - (1-x)\dfrac{1}{2}\log_2(1-x)$ 是二元熵.

依据 (1)—(9) 式, 可以得出基于 CSS 的 SARG04 协议, 无限多诱骗态情况下单光子的密钥生成速率 R_{SARG04}.

2.2 有限诱骗态 QKD 方案

Alice 发出强度为 u 的信号态光, 发出强度为 v 的诱骗态光, 强度满足 $u > v > 0$, Alice 和 Bob 进行非正交编码和解码实现 QKD, QKD 完成后, Alice 告诉 Bob 信号态和诱骗态的分布情况, 由 Bob 端探测结果计算出 Q_u, Q_v, E_u, E_v.

下面来计算单光子的计数率和量子误码率, 具体推导过程如下:

信号态的计数率为

$$\begin{aligned} Q_u =& \sum_{n=0}^{\infty} Y_n P_n(u) \\ =& \frac{1}{\sinh u} \sum_{n=0}^{\infty} \frac{u^{2n+1}}{(2n+1)!} Y_{2n+1}, \end{aligned} \tag{10}$$

诱骗态的计数率为

$$\begin{aligned} Q_v =& \sum_{n=0}^{\infty} Y_n P_n(v) \\ =& \frac{1}{\sinh v} \sum_{n=0}^{\infty} \frac{v^{2n+1}}{(2n+1)!} Y_{2n+1}. \end{aligned} \tag{11}$$

对 (11), (12) 式进行数学运算, 得出:

$$\sinh u \cdot Q_u = \sum_{n=0}^{\infty} \frac{u^{2n+1}}{(2n+1)!} Y_{2n+1}, \tag{12}$$

$$\sinh v \cdot Q_v = \sum_{n=0}^{\infty} \frac{v^{2n+1}}{(2n+1)!} Y_{2n+1}, \tag{13}$$

$$\begin{aligned} & v^3 \cdot \sinh u \cdot Q_u \\ =& uv^3 Y_1 + \frac{u^3 v^3}{6} Y_3 + \sum_{n=2}^{\infty} \frac{v^3 u^{2n+1}}{(2n+1)!} Y_{2n+1}, \end{aligned} \tag{14}$$

$$\begin{aligned} & u^3 \cdot \sinh v \cdot Q_v \\ =& vu^3 Y_1 + \frac{u^3 v^3}{6} Y_3 + \sum_{n=2}^{\infty} \frac{u^3 v^{2n+1}}{(2n+1)!} Y_{2n+1}. \end{aligned} \tag{15}$$

(15)−(14) 式:

$$\begin{aligned} & u^3 \cdot \sinh v \cdot Q_v - v^3 \cdot \sinh u \cdot Q_u \\ =& (vu^3 - uv^3) Y_1 \\ &+ \sum_{n=2}^{\infty} \frac{u^3 v^{2n+1} - v^3 u^{2n+1}}{(2n+1)!} Y_{2n+1}. \end{aligned} \tag{16}$$

又 $u > v > 0$, 对于 $n \geqslant 2$, 有

$$\sum_{n=2}^{\infty} \frac{u^3 v^{2n+1} - v^3 u^{2n+1}}{(2n+1)!} Y_{2n+1} \leqslant 0, \tag{17}$$

进而有

$$\begin{aligned} & u^3 \cdot \sinh v \cdot Q_v - v^3 \cdot \sinh u \cdot Q_u \\ \leqslant& (vu^3 - uv^3) Y_1, \end{aligned} \tag{18}$$

得出单光子计数率的下限

$$Y_1 \geqslant \frac{u^3 \cdot \sinh v \cdot Q_v - v^3 \cdot \sinh u \cdot Q_u}{vu^3 - uv^3}. \tag{19}$$

诱骗态的计数率 Q_v 和误码率 E_v 有如下关系:

$$Q_v E_v = \sum_{n=0}^{\infty} e_n Y_n P_n(v) \geqslant e_1 Y_1 P_1(v), \tag{20}$$

得出单光子的误码率上限

$$e_1 \leqslant \frac{E_v Q_v}{Y_1 P_1(v)}. \tag{21}$$

将实验中测算的 Q_u, Q_v, E_u, E_v 代入 (19) 和 (21) 式就可以估算出单光子的计数率及误码率的限值. 最后与理论值比较判断是否正常, 不正常则放弃本次通信, 正常则进一步纠错及保密放大提取密钥.

3 数值模拟

取 $f(E_u) = 1.22$, 利用 Gobby-Yuan-Shields (GYS) 实验 [27] 参数 (波长 1550 nm), 对基于 CSS 的 SARG04 协议诱骗态 QKD 方案进行性能仿真, 各参数如表 1 所列.

表 1 GYS 实验参数

Table 1. Parameters from GYS experiments.

参数类型	数值
衰减率 α	0.21
Bob 端探测器的探测效率 η_{Bob}	0.45%
背景噪声引起的暗计数 p_{dark}	1.7×10^{-6}

根据 (9) 式可知密钥生成速率 R_{SARG04} 是关于平均光强 u 和传输距离 L 的函数, 可以用二元函数简单表示为 $R_{\mathrm{SARG04}}(u, L)$, 利用 Matlab 进行优化处理后可以模拟出 R_{SARG04} 随传输距离 L 的变化曲线, 如图 1 所示.

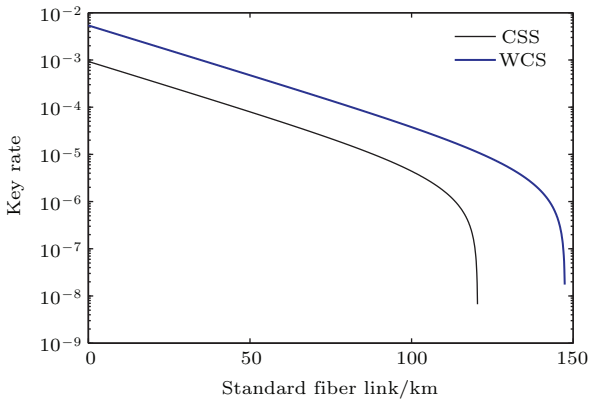

图 1 无限多诱骗态情况下密钥生成率随传输距离变化曲线

Fig. 1. Curves of key generation rate and transmission distance in the case of infinite number of decoy state.

图 1 中的蓝线所示的是采用 CSS 作为光源, 其中光强取 $u = 0.25$, SARG04 协议诱骗态 QKD 方案安全传输距离达到了 147.4 km. 图 1 中的黑线所示的是采用弱相干态 (weak coherent state, WCS) 作为光源, SARG04 协议诱骗态 QKD 方案的密钥生成率随传输距离 L 的变化曲线. 通过图 1 的数据模拟结果可以直观地看出, 采用 CSS 作为光源的 SARG04 协议诱骗态 QKD 方案比采用 WCS 作为光源的 SARG04 协议诱骗态 QKD 方案有更高的安全密钥生成率和更远的安全传输距离; 采用自发参量下转化光子对作为光源的 SARG04 协议诱骗态 QKD 方案, 其安全传输距离为 142.05 km [15], 对比可知, 采用 CSS 作为光源的 SARG04 协议诱骗态 QKD 方案也优于采用自发参量下转化光子对作为光源的 SARG04 协议诱骗态 QKD 方案.

我们还模拟了有限多诱骗态下的非正交编码 QKD 方案成码率随传输距离 L 的变化曲线, 并模拟了统计涨落时成码率随传输距离 L 的变化曲线, 如图 2 所示. 其中信号态光强取 $u = 0.25$, 诱骗态光强取 $v = 0.05$.

图 2 中的绿线所示的是没有波动时, 有限多诱骗态情况下, 密钥生成率随传输距离 L 的变化曲线, 其安全传输距离依然达到了 147.4 km; 图 2 中的红线所示的是 N 取 10^{10}, 有限多诱骗态情况下, 密钥生成率随传输距离 L 的变化曲线, 其安全传输距离达到了 144.0 km; 图 2 中的蓝线所示的是 N 取 10^9, 有限多诱骗态情况下, 密钥生成率随传输距离 L 的变化曲线, 其安全传输距离达到了 139.0 km; 图 2 中的黑线所示的是 N 取 10^8, 有限多诱骗态情况下, 密钥生成率随传输距离 L 的变化曲线, 其安全传输距离达到了 125.9 km.

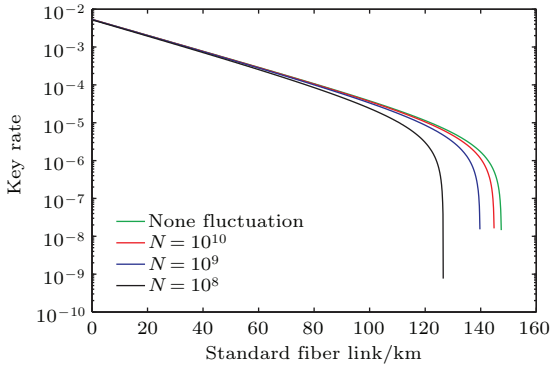

图 2 有限多诱骗态情况下密钥生成率随传输距离变化曲线

Fig. 2. Curves of key generation rate and transmission distance in the case of limited number of decoy state.

4 结 论

本文首次提出利用 CSS 作为光源, 结合 SARG04 协议进行诱骗态 QKD 方案, 推导了单光子安全密钥成码率公式, 该方案有以下优点: 1) 方案结合了 SARG04 协议和诱骗态方法, 可以有效地抵御 PNS; 2) WCS 中单光子成分大约为 30%, 而 CSS 中单光子成分高达 90%, 因此光源采用 CSS 的 SARG04 协议诱骗态 QKD 方案比光源采用 WCS 的 SARG04 协议诱骗态 QKD 方案具有更高的成码率和更远的安全传输距离; 光源采用 CSS 的 SARG04 协议诱骗态 QKD 方案比采用自发参量下转化光子对作为光源的 SARG04 协议诱骗态 QKD 方案也具有更高的成码率和更远的安全传输距离, 光源采用 CSS 的 SARG04 协议诱骗态 QKD 方案提高了 QKD 系统的性能; 3) 光源采用 CSS 的 SARG04 协议诱骗态 QKD 方案, 只需要一种诱骗态, 相比需要几种诱骗态的其他方案, 更加容易制备. 可见本文提出的基于 CSS 的 SARG04 协议诱骗态 QKD 方案是一种很好的量子密钥分发方案, 随着 CSS 制备技术的进一步发展, 必然会有很好的应用.

参考文献

[1] Bennett C H, Brassard 1984 *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (New York: IEEE) p175

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Shor P W, Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[4] Brassard G, Lutkenhaus N, Mor T, Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[5] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[6] Scarani V, Acin A, Ribordy G, Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[7] Fung C H F, Tamaki K, Lo H K 2006 *Phys. Rev. A* **73** 012337
[8] Li J B, Fang X M 2006 *Chin. Phys. Lett.* **23** 1375
[9] Li J B, Fang X M 2006 *Chin. Phys. Lett.* **23** 775
[10] Adachi Y, Yamamoto T, Koashi M, Imoto N 2007 *Phys. Rev. Lett.* **99** 180503
[11] Wang Q, Wang X B, Guo G C 2007 *Phys. Rev. A* **75** 012312
[12] Wang Q, Karlsson A 2007 *Phys. Rev. A* **76** 014309
[13] Zhang S L, Zou X B, Li K, Jin C H, Guo G C 2007 *Phys. Rev. A* **76** 044304
[14] Mi J L, Wang F Q, Lin Q Q, Liang R S, Liu S H 2008 *Acta Phys. Sin.* **57** 678 (in Chinese) [米景隆, 王发强, 林青群, 梁瑞生, 刘颂豪 2008 物理学报 **57** 678]
[15] Hu H P, Wang J D, Huang Y X, Liu S H, Lu W 2010 *Acta Phys. Sin.* **59** 287 (in Chinese) [胡华鹏, 王金东, 黄宇娴, 刘颂豪, 路巍 2010 物理学报 **59** 287]
[16] Yin H L, Cao W F, Fu Y, Tang Y L, Liu Y, Chen T Y, Chen Z B 2014 *Opt. Lett.* **39** 5451
[17] Lund A P, Ralph T C, Haselgrove H L 2008 *Phys. Rev. Lett.* **100** 030503
[18] Andersen U L, Ralph T C 2013 *Phys. Rev. Lett.* **111** 050504
[19] Jeong H, Kim M S, Lee J 2001 *Phys. Rev. A* **64** 052308
[20] van Enk S J, Hirota O 2001 *Phys. Rev. A* **64** 022313
[21] Sangouard N, Gisin N, Laurat J, Tualle Brouri R, Grangier P 2010 *J. Opt. Soc. Am. B* **27** 137
[22] Brask J B, Rigas I, Polzik E S, Andersen U L, Sørensen A S 2010 *Phys. Rev. Lett.* **105** 160501
[23] Munro W J, Nemoto K, Milburn G J, Braunstein S L 2002 *Phys. Rev. A* **66** 023819
[24] Neergaard-Nielsen J S, Nielsen B M, Hettich C, Mølmer K, Polzik E S 2006 *Phys. Rev. Lett.* **97** 083604
[25] Ourjoumtsev A, Jeong H, Tualle-Brouri R, Grangier P 2007 *Nature* **448** 784
[26] Yin H L, Yao F, Chen Z B 2016 *Phys. Rev. A* **93** 032316
[27] Gobby C, Yuan Z L, Shields A J 2004 *Appl. Phys. Lett.* **84** 3762

Nonorthogonal decoy-state quantum key distribution based on coherent-state superpositions*

Sun Wei[1)†] Yin Hua-Lei[2)] Sun Xiang-Xiang[1)] Chen Teng-Yun[2)]

1) (*Department of Modern Physics, University of Science and Technology of China, Hefei 230026, China*)

2) (*Hefei National Laboratory for Physical Sciences at Microscale, University of Science and Technology of China, Hefei 230026, China*)

(Received 10 December 2015; revised manuscript received 11 January 2016)

Abstract

Nonorthogonal coded agreements and decoy state method can effectively protect the photon number against splitting attack. Owing to the fact that the component of single-photon in the coherent-state superposition (CSS) is as high as 90%, CSS has recently emerged as an alternative to single-photon qubits for quantum information processing and metrology. The approximate CSS of small amplitudes is generated by the subtraction of photons from a squeezed vacuum state, and the approximate CSS of large amplitude is generated from Fock state by using a single homodyne detection. Here, we combine both of the methods and propose a new protocol by using the CSS as a light source.

We derive the secure key generation rate, the lower bound of count rate and upper bound of error rate of single-photon. We simulate the curves relationship between secure key generation rate and safety transmission distance in the case of an infinite number of decoy states by using matlab. The parameters are given according to the Gobby-Yuan-Shields (GYS) experiment. We infer that the safety transmission distance achieves 147.4 km and the secure key generation rate is much higher than those of other schemes. We also simulate the relationship between key generation rate and safety transmission distance in the case of a limited number of decoy states by using matlab. The parameters are given according to the GYS experiment too. When the N is 10^{10}, the safety transmission distance achieves 144 km; when the N is 10^{9}, the safety transmission distance achieves 139 km; when the N is 10^{8}, the safety transmission distance achieves 125.9 km.

In this paper, we propose the use of CSS as the light source. Combining SARG04 agreements and decoy state, the scheme has the following advantages: first, the scheme which combines SARG04 agreements and decoy state method can effectively resist PNS; second, nonorthogonal decoy-state quantum key distribution based on coherent-state superpositions has a longer safety transmission distance and higher secure key generation rate than nonorthogonal decoy-state quantum key distribution based on weak coherent pulse and nonorthogonal decoy-state quantum key distribution based on conditionally prepared down-conversion source; third, nonorthogonal decoy-state quantum key distribution based on coherent-state superpositions is easier to prepare, which just needs one decoy state, than other schemes that require several decoy states.

Obviously, our scheme can enhance the performance of quantum key distribution. Nonorthogonal decoy-state quantum key distribution based on coherent-state superpositions will have a very good application with the further development of preparation technology of CSS.

Keywords: coherent-state superpositions, key generation rate, count rate, error rate

PACS: 03.65.–w, 03.67.–a, 42.50.–p **DOI:** 10.7498/aps.65.080301

* Project supported by the Natural Science Foundation of Anhui Province, China (Grant No. 1508085J02).

† Corresponding author. E-mail: sunwei85@mail.ustc.edu.cn