奇相干光源的测量设备无关量子密钥分配研究*

东晨[1)2)†] 赵尚弘[1)] 张宁[3)] 董毅[1)] 赵卫虎[1)] 刘韵[1)]

1) (空军工程大学信息与导航学院, 西安 710077)

2) (西安通信学院信息安全系, 西安 710006)

3) (61711 部队, 喀什 844000)

(2014 年 3 月 16 日收到; 2014 年 6 月 5 日收到修改稿)

刻画了奇相干光源的光子数分布特征, 研究了奇相干光源下诱骗态测量设备无关量子密钥分配系统的密钥生成率与安全传输距离的关系, 推导了奇相干光源下的计数率下界和误码率上界. 仿真结果表明, 奇相干光源光子数分布中多光子脉冲的比例低于弱相干光, 可以有效提高诱骗态测量设备无关密钥分配系统的最大安全通信距离, 为实用的量子密钥分配实验提供了重要的理论参数.

关键词: 奇相干态, 测量设备无关量子密钥分配, 统计波动

PACS: 03.67.Dd **DOI:** 10.7498/aps.63.200304

1 引 言

量子密钥分配[1]以其建立在量子力学和信息论框架下的无条件安全性特点[2−4], 近年来已成为国内外的研究热点[5−9]. 然而在建立实际的量子密钥分配系统时, 由于所采用的光学和电学设备存在各种非完美性, 使得系统存在安全漏洞, 如针对非理想光源提出的光子数分流攻击[10]、相位部分随机化攻击[11]等; 针对非理想探测器提出的伪态攻击[12]、时移攻击[13]、致盲攻击[14]等. 为了克服上述实际光源和探测设备非完美性问题, Lo等[15]提出了测量设备无关量子密钥分配方案 (measurement-device-independent QKD, MDI-QKD). 在该方案中, Alice 和 Bob 将光脉冲发送至非可信任的第三方进行 Bell 态测量, 根据第三方公布的 Bell 态结果采用 BB84 协议进行比特反转操作得到安全密钥. 由于该方案的测量过程在第三方进行, 故其可以移除所有的探测器侧信道漏洞. 在实际的 MDI-QKD 系统中, Alice 和 Bob 通常使用弱相干光源代替单光子光源, 故实验中可结合诱骗态方法[16]有效地估计密钥生成率. 理论方面, 文献 [17—19] 分析了 MDI-QKD 的统计波动问题; 实验方面, Liu 等[20]和 Tang 等[21]分别实现了相位编码和偏振编码的 MDI-QKD.

在诱骗态 MDI-QKD 中, 实验一般采用的弱相干光源光子数服从泊松分布. 事实上, 在诱骗态方法中可以通过减少多光子脉冲比例有效地估计计数率下界和误码率上界, 从而得到更高的密钥生成率[22]. 本文研究了奇相干光源诱骗态 MDI-QKD 系统的密钥生成率与安全传输距离的关系, 并与理想单光子源和弱相干光源情形进行了比较, 同时采用标准误差方法分析了统计波动对量子密钥生成率的影响.

2 理论与计算公式

测量设备无关量子密钥分配系统模型如图 1 所示. Alice 和 Bob 发送的相干光脉冲先经过偏振调制器 (PM) 进行偏振编码 (选取 x 基 z 基),

* 国家自然科学基金 (批准号: 61106068) 资助的课题.

† 通讯作者. E-mail: dongchengfkd@163.com

再经过强度调制器 (IM) 调制为3强度 μ_i, v_j:

$$\begin{cases} \{\mu_i\} & (i=1,2,3), \\ \{v_j\} & (j=1,2,3), \end{cases} \tag{1}$$

分别对应真空态、诱骗态和信号态, 第三方通过分束器 (BS)、偏振分束器 (PBS) 和探测器对接收到的相干光脉冲进行 Bell 态测量并公布测量结果, Alice 和 Bob 根据基比对过程提取出安全密钥生成率公式 [15]:

$$R = P_{\mu_2}(1)P_{\nu_2}(1)Y_{11}^z\left[1-H_2(e_{11}^x)\right] - Q_{\mu_2\nu_2}^z f(E_{\mu_2\nu_2}^z)H_2(E_{\mu_2\nu_2}^z), \tag{2}$$

式中 $w=x$, z 分别代表 x 基和 z 基, 其中 x 基作为测试集用来估计信道参数, z 基用来产生安全密钥; Alice 脉冲强度为 μ_i 且 Bob 脉冲强度为 ν_j 时的增益 $Q_{\mu_i\nu_j}$ 和误码率 $E_{\mu_i\nu_j}$:

$$Q_{\mu_i\nu_j}^w = \sum_{n,m=0}^{\infty} P_{\mu_i}(n)P_{\nu_j}(m)Y_{nm}^w, \tag{3}$$

$$E_{\mu_i\nu_j}^w Q_{\mu_i\nu_j}^w = \sum_{n,m=0}^{\infty} P_{\mu_i}(n)P_{\nu_j}(m)e_{nm}^w Y_{nm}^w. \tag{4}$$

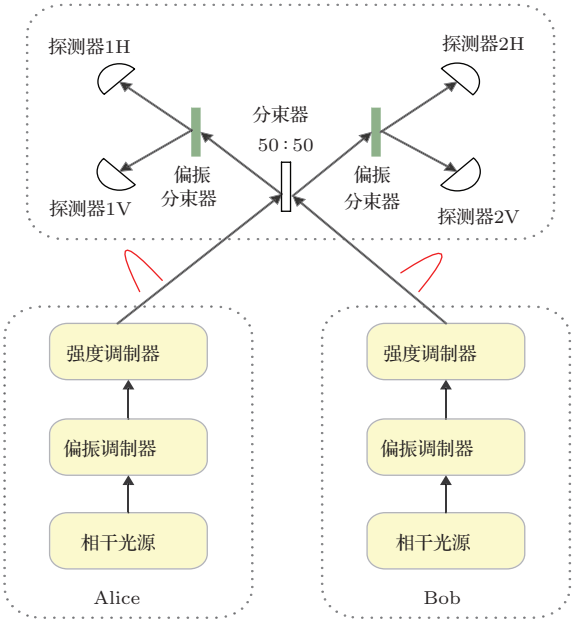

图 1 测量设备无关量子密钥分配系统结构 [15]

在密钥生成率估计 (2) 式中, $Q_{\mu\nu}^z$ 和 $E_{\mu\nu}^z$ 可直接由实验测得 [17], 在理论上只需要估计单光子计数率 Y_{11}^z 下界和单光子误码率上界 e_{11}^x, 可以得到最终的密钥生成率. 本文采用奇相干光源代替弱相干光源对 Y_{11}^z 下界和 e_{11}^x 上界进行估计. 奇相干态光源就是没有偶数光子脉冲的相干光状态, 首先可以利用光参量振荡器产生压缩真空场, 并通过反射分束器和压缩真空场消除特定的光子态, 奇相干态光源由相位相反的相干态 $|\alpha\rangle$, $|-\alpha\rangle$ 组成:

$$|\alpha\rangle_{\rm ocs} = N(|\alpha\rangle - |-\alpha\rangle). \tag{5}$$

在实验中可以通过控制线性光学器件利用非线性过程产生奇相干态 [23,24]:

$$\boldsymbol{U}|0\rangle = \exp\frac{1}{2}(\zeta^*\boldsymbol{a}^2 - \zeta\boldsymbol{a}^{+2})|0\rangle \xrightarrow{\rm BS} |\alpha\rangle_{\rm ocs}, \tag{6}$$

式中 $\boldsymbol{U}$ 为幺正压缩算符, ζ 为抽运场的幅度值, 产生的奇相干态可以表示为

$$|\alpha\rangle_{\rm ocs} = \frac{1}{\sinh|\alpha|^2}\sum_{n=0}^{\infty}\frac{\alpha^{2n+1}}{\sqrt{(2n+1)!}}|2n+1\rangle, \tag{7}$$

可以得到奇相干光源光子数的分布为

$$P(2n+1) = \frac{|\alpha|^{2(2n+1)}}{\sinh(|\alpha|^2)(2n+1)!}. \tag{8}$$

表 1 弱相干光源和奇相干光源的多光子数与单光子数比较 (平均光强为 0.6)

光源	单光子数	多光子数
WCS	0.3293	0.1219
OCS	0.9424	0.0576

如表 1 所示, 相同光强下奇相干光源多光子脉冲概率小于弱相干光源多光子脉冲概率. 对于奇相干态光源下诱骗态 MDI-QKD, 由 (3) 和 (8) 式可以推出单光子增益 $Q_{\mu_i\nu_j}$:

$$Q_{\mu_2\nu_2} = \sum_{n,m=0}^{\infty} P_{\mu_2}(2n+1)P_{\nu_2}(2m+1) \times Y_{(2n+1)(2m+1)}, \tag{9}$$

$$Q_{\mu_1\nu_1} = \sum_{n,m=0}^{\infty} P_{\mu_1}(2n+1)P_{\nu_1}(2m+1) \times Y_{(2n+1)(2m+1)}, \tag{10}$$

利用文献 [25] 中关于诱骗态量子密钥分配的一元不等式证明:

$$\frac{P_{\mu_2}(3)}{P_{\mu_2}(2n+1)} - \frac{P_{\mu_1}(3)}{P_{\mu_1}(2n+1)} = \frac{(2n+1)!}{3!}\left(\frac{1}{\mu_2^{2n-2}} - \frac{1}{\mu_1^{2n-2}}\right) \leqslant 0, \tag{11}$$

可以得到固定的 m:

$$Q_{\mu_2} = P_{\mu_2}(1)Y_1 + \sum_{n=1}^{\infty} P_{\mu_2}(2n+1)Y_{2n+1} \geqslant P_{\mu_2}(1)Y_1$$

$$+\sum_{n=1}^{\infty}\frac{P_{\mu_2}(3)}{P_{\mu_1}(3)}P_{\mu_1}(2n+1)Y_{2n+1}$$
$$=P_{\mu_2}(1)Y_1+\frac{P_{\mu_2}(3)}{P_{\mu_1}(3)}\times(Q_{\mu_1}-P_{\mu_1}(1)Y_1), \tag{12}$$

由 n, m 的对称性得到关于 n 的类似结果. 由 (3) 和 (10) 式可以推出单光子增益的下界 Y_{11}^w:

$$Y_{11}\geqslant\frac{P_{\mu_1}(3)P_{v_1}(3)Q_{\mu_2\nu_2}-P_{\mu_2}(3)P_{v_2}(3)Q_{\mu_1\nu_1}}{P_{\mu_2}(1)P_{v_2}(1)P_{\mu_1}(3)P_{v_1}(3)-P_{\mu_2}(3)P_{v_2}(3)P_{\mu_1}(1)P_{v_1}(1)}. \tag{13}$$

类似地由 (10) 和 (13) 式可以推出单光子误码率的上界 e_{11}^w:

$$e_{11}\leqslant\frac{Q_{\mu_2\nu_2}E_{\mu_2\nu_2}}{P_{\mu_2}(1)P_{\nu_2}(1)Y_{11}}. \tag{14}$$

在实际的 MDI-QKD 系统中, 有限长度密钥会带来参数估计的统计波动问题, 利用文献 [17] 提出的标准误差方法对奇相干光源的统计波动问题进行分析. 单光子增益与单光子误码率的统计波动表示为

$$\begin{aligned}\underline{Q_{\mu_i\nu_j}^w}&\approx Q_{\mu_i\nu_j}^w(1-\beta_q)\leqslant Q_{\mu_i\nu_j}^w\\&\leqslant Q_{\mu_i\nu_j}^w(1+\beta_q)\\&\approx\overline{Q_{\mu_i\nu_j}^w},\end{aligned} \tag{15}$$

$$\begin{aligned}\underline{E_{\mu_i\nu_j}^wQ_{\mu_i\nu_j}^w}&\approx E_{\mu_i\nu_j}^wQ_{\mu_i\nu_j}^w(1-\beta_{eq})\leqslant E_{\mu_i\nu_j}^wQ_{\mu_i\nu_j}^w\\&\leqslant E_{\mu_i\nu_j}^wQ_{\mu_i\nu_j}^w(1+\beta_{eq})\\&\approx\overline{E_{\mu_i\nu_j}^wQ_{\mu_i\nu_j}^w},\end{aligned} \tag{16}$$

其中

$$\beta_q=\frac{n_\alpha}{\sqrt{N_{\mu_i\nu_j}^wQ_{\mu_i\nu_j}^w}},$$
$$\beta_{eq}=\frac{n_\alpha}{\sqrt{N_{\mu_i\nu_j}^wE_{\mu_i\nu_j}^wQ_{\mu_i\nu_j}^w}}$$

分别刻画单光子增益与单光子误码率的波动强度; $N_{\mu_i\nu_j}^w$ 为 w 基下的脉冲个数; n_α 为统计波动的标准方差. 在统计波动下重新得到单光子增益的下界 $\underline{Y_{11}}$ 和单光子误码率上界 $\overline{e_{11}}$:

$$\underline{Y_{11}}\geqslant\frac{P_{\mu_1}(3)P_{v_1}(3)\underline{Q_{\mu_2\nu_2}}-P_{\mu_2}(3)P_{v_2}(3)\overline{Q_{\mu_1\nu_1}}}{P_{\mu_2}(1)P_{v_2}(1)P_{\mu_1}(3)P_{v_1}(3)-P_{\mu_2}(3)P_{v_2}(3)P_{\mu_1}(1)P_{v_1}(1)}, \tag{17}$$

$$\overline{e_{11}}\leqslant\frac{\overline{Q_{\mu_2\nu_2}E_{\mu_2\nu_2}}}{P_{\mu_2}(1)P_{\nu_2}(1)\underline{Y_{11}}}. \tag{18}$$

3 仿真结果与分析

在奇相干光源 MDI-QKD 的参数估计中, 可以看到奇相干光源光子数服从亚泊松分布, 随着 n, m 的增加, 展开 (7) 式的系数逐渐减小, 即可以通过截断 n, m 值较大的展开项简化参数估计. 定义截断项求和上界为

$$\begin{aligned}&\tau(\mu,\nu,k)\\&=1-\left(\sum\nolimits_{n=0}^{k-1}\frac{\mu^{2n+1}}{\sinh(\mu)\sqrt{(2n+1)!}}\right)\\&\quad\times\left(\sum\nolimits_{m=0}^{k-1}\frac{v^{2m+1}}{\sinh(v)\sqrt{(2m+1)!}}\right).\end{aligned} \tag{19}$$

如图 2 所示, 当截断项数 k 超过 6 时, 截断项求和上界为 10^{-15} 量级左右, 对最终估计密钥生成率的影响可以忽略.

根据 (13) 和 (14) 式可以估计出单光子计数率的下限和单光子误码率的上限, 代入 (2) 式可以得到最终的安全密钥生成率与安全传输距离之间的关系. 在计算过程中, 诱骗态和信号态的光强分别为 0.1 和 0.5, 其余主要参数 [17] 为 $e_{\rm d}=1.5\%$, $P_{\rm d}=3\times10^{-6}$, $f=1.16$, $N_{\rm data}=10^{12}$.

如图 3 所示, 对于理想单光子源, 最大的安全传输距离可以达到 392 km, 对于弱相干光源, 由于多光子脉冲的影响, 最大的安全传输距离缩短至 245 km, 而本文采用的奇相干光源通过减少多光子脉冲的概率可以增加最大安全传输距离至 309 km. 如图 4 所示, 对于奇相干光源的统计波动问题, 随着脉冲长度的减少, 最大安全距离也相应从无波动时的 309 km 逐步减少至 270 (脉冲个数 10^{12}) 和 211 km (脉冲个数 10^{10}).

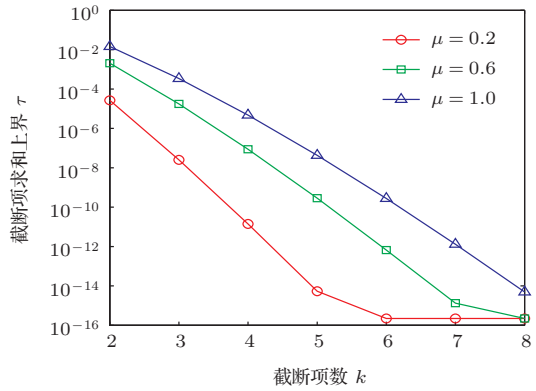

图 2 截断项数与截断项求和上界的关系

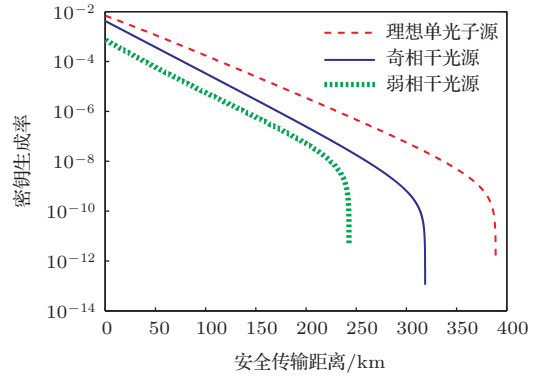

图 3 不同光源下密钥生成率与安全传输距离的关系

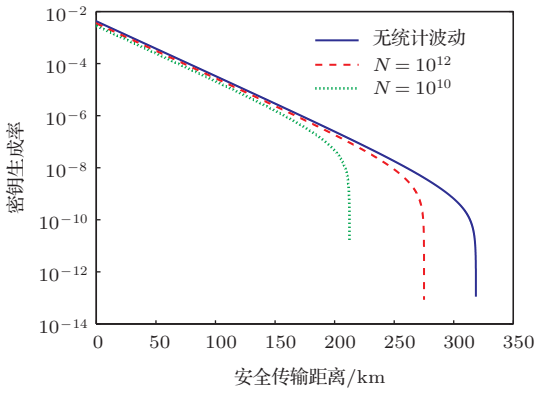

图 4 不同统计波动下密钥生成率的变化

4 结 论

本文研究了奇相干光源MDI-QKD系统的密钥生成率与安全传输距离的关系, 推导了奇相干光源光子数分布下的计数率下界和误码率上界, 并与理想单光子源和弱相干光源情形进行了比较, 同时采用标准误差方法分析了有限长度密钥下统计波动对参数估计的影响. 与弱相干光源相比, 奇相干光源的光子数分布服从亚泊松分布, 可以有效减少多光子脉冲的概率, 提高密钥传输的最大安全传输距离. 仿真结果表明, 采用奇相干光源代替弱相干光源可以增加传输距离64 km; 统计波动在传输距离较短时对密钥生成率影响较小, 随着传输距离逐步增大至200 km后, 光脉冲衰减逐步增大, 密钥生成率对于统计波动的敏感程度也随之增大. 在实验中, 可以通过调整光强度寻找最优的密钥生成率.

参考文献

[1] Bennet C H, Brassard G 1984 *Proc. IEEE International Conference Computers, Systems, and Signal Processing* Bangalore, India, December 9–12, 1984 pp175–179

[2] Shor P W, Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[3] Mayers D 2001 *J. ACM* **48** 351

[4] Gottesman D, Lo H K, Lutkenhaus N, Preskill J 2004 *Quantum Infor. Comput.* **4** 325

[5] Zhou Y Y, Zhou X T, Tian P G, Wang Y J 2013 *Chin. Phys. B* **22** 010305

[6] Sheng Y B, Zhou L, Cheng W W, Gong L Y, Wang L, Zhan S M 2013 *Chin. Phys. B* **22** 030314

[7] Jiao R Z, Zhang W H 2009 *Acta Phys. Sin.* **58** 2189 (in Chinese) [焦荣珍, 张文瀚 2009 物理学报 **58** 2189]

[8] Dong C, Zhao S H, Zhao W H, Shi L, Dong Y 2014 *Acta Phys. Sin.* **63** 030302 (in Chinese) [东晨, 赵尚弘, 赵卫虎, 石磊, 董毅 2014 物理学报 **63** 030302]

[9] Wang J D, Qin X J, Wei Z J, Liu X B, Liao C J, Liu S H 2010 *Acta Phys. Sin.* **59** 281 (in Chinese) [王金东, 秦晓娟, 魏正军, 刘小宝, 廖常俊, 刘颂豪 2010 物理学报 **59** 281]

[10] Brassard G, Lutkenhaus N, Mor T, Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330

[11] Sun S H, Liang L M 2012 *Appl. Phys. Lett.* **101** 071107

[12] Makarov V, Skaar J 2008 *Quantum Infor. Comput.* **86** 622

[13] Zhao Y, Fung C H F, Qi B, Chen C, Lo H K 2008 *Phys. Rev. A* **78** 042333

[14] Makarov V 2009 *New J. Modern Opt.* **11** 065003

[15] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503

[16] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

[17] Ma X F, Fung C H F, Razavi M 2012 *Phys. Rev. A* **86** 052305

[18] Wang X B 2013 *Phys. Rev. A* **87** 012320

[19] Sun S H, Gao M, Li C Y, Liang L M 2013 *Phys. Rev. A* **87** 052329

[20] Liu Y, Chen T Y, Wang L J, Lao H, Shentu G L, Wian J, Cui K, Yin H L, Liu N L, Li L, Ma X F, Pele J S, Fejer M M, Zhang Q, Pan J W 2013 *Phys. Rev. Lett.* **111** 130502

[21] Tang Z, Liao Z, Xu F, Qi B, Qian L, Lo H K 2013 arXiv: 13066134

[22] Pironio S, Acín A, Brunner N, Gisin N, Massar S, Scarani V 2009 *New J. Phys.* **11** 045021

[23] Sasaki M, Suzuki S 2006 *Phys. Rev. A.* **73** 043807

[24] Wenger J, Tuall-Brouri R, Grangie P 2004 *Phys. Rev. Lett.* **92** 153601

[25] Sun S H, Gao M, Dai H Y, Chen P X, Li C Z 2008 *Chin. Phys. Lett.* **25** 2358

Measurement-device-independent quantum key distribution with odd coherent state*

Dong Chen[1)2)†] Zhao Shang-Hong[1)] Zhang Ning[3)] Dong Yi[1)]
Zhao Wei-Hu[1)] Liu Yun[1)]

1) (*School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China*)

2) (*Department of Information Security, Xi'an Communication College, Xi'an 710006, China*)

3) (*61711 Department, Kashi 844000, China*)

(Received 16 March 2014; revised manuscript received 5 June 2014)

Abstract

Measurement-device-independent quantum key distribution (MDI-QKD) is immune to all the detection attacks, thus when it is combined with the decoy state method, the final key is unconditionally safe. In this paper, we propose to perform MDI-QKD with odd coherent state (OCS) and compare the results with weak coherent source scenario. Our simulation indicates that both the secure key rate and transmission distance can be improved evidently with OCS owing to the lower probability of multi-photon events of the OCS. Furthermore, we apply the finite key analysis to the decoy state MDI-QKD with OCS and obtain a practical key rate.

Keywords: odd coherent state, measurement-device-independent quantum key distribution, statistical fluctuation

PACS: 03.67.Dd **DOI:** 10.7498/aps.63.200304

* Project supported by the National Natural Science Foundation of China (Grant No. 61106068).

† Corresponding author. E-mail: dongchengfkd@163.com