基于指示单光子源的量子密钥分配协议

朱 峰 王 琴

(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 主要介绍了量子光源,尤其是指示单光子源在量子密钥分配(QKD)中的应用,提出了一种新的基于指示单光子源的不依赖于测量装置的量子密钥分配(MDI-QKD)方案。与现有的其他方案,如弱相干态方案相比,该方案具有安全性好,密钥提取率与安全传输距离都显著提高等优点。因而,该方案在未来的量子密钥分配实用化进程中具有广阔的发展前景。

关键词 量子光学;量子密钥分配;密钥提取率;参量下转换

中图分类号 O436 **文献标识码** A **doi**: 10.3788/AOS201434.0627002

Quantum Key Distribution Protocol Based on Heralded Single Photon Source

Zhu Feng Wang Qin

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

Abstract Applications of quantum sources, especially the heralded single photon source in the quantum key distribution (QKD) are introduced, and a new scheme of the measurement-device-independent quantum key distribution (MDI-QKD) based on heralded single photon source is presented. Comparing with existing schemes, such as the scheme of using weak coherent sources, the new scheme has many advantages like a better security, a higher key generation rate and a longer safe transmission distance. Therefore, it seems to be a promising candidate for the implementation for the quantum key distribution in the near future.

Key words quantum optics; quantum key distribution; key generation rate; parametric down-conversion

OCIS codes 270.5568; 200.3050; 190.4410; 060.4370

1 引 言

量子通信具有经典通信所不具有的绝对安全性[1-2],因而在信息与通信领域有着非凡的魅力与巨大的发展潜能。量子通信的核心方向量子密钥分配,自 Bennett 等[3]提出第一个 BB84 方案被以来,至今已有二十多年的发展历史,无论是理论还是实验都发展十分迅猛,日趋成熟,目前正朝着实用性方向发展。但是贯穿着量子密钥整个发展过程中,一直存在着对密钥分发系统的攻击与反攻击策略的斗争,这主要围绕量子密钥安全性证明的完美理论假设与现实密钥系统缺陷之间的矛盾展开。

针对现有密钥系统存在的种种缺陷,人们提出了各种不同攻击手段,比如光子数分束(PNS)攻击[4-6]、移时攻击[7-8]、赝态攻击[9]、相位重投影攻击[10]等。所有这些攻击中,危害最大的为 PNS 攻击。为了解决 PNS 攻击,人们提出诱骗态的方法[11-13]。而为了解决其他诸如移时、相位重投影等攻击,人们又给出了不同的解决方案[14-18],其中不依赖于测量装置的量子密钥分配(MDI-QKD)方案以其卓越的表现脱颖而出。它不仅可以抵御所有针对探测器的攻击,同时还大大提高了密钥的安全传输距离。

收稿日期: 2014-01-10; **收到修改稿日期**: 2014-02-12

基金项目: 国家自然科学基金(11274178,11311140250)

作者简介: 朱 峰(1991—),男,硕士研究生,主要从事量子密钥分配方面的研究。E-mail: 844383041@qq.com

导师简介: 王 琴(1979—),女,博士,教授,主要从事量子光学与量子信息方面的研究。E-mail: qinw@njupt.edu.cn (通信联系人)

本文电子版彩色效果请详见中国光学期刊网 www.opticsjournal.net

迄今为止，在所有的 MDI-QKD 理论与实验方案中，人们使用的光源都是衰减激光光源，也就是大家常说的“赝单光子源”或相干态（WCS）光源。由于 WCS 光源中存在着大量的真空脉冲与相当比例的多光子脉冲，所以它的安全传输距离与密钥提取率受到很大限制。本文提出了一种新的方案，采用具有显著优势的“指示单光子光源”（HSPS）取代了原有的 WCS 光源。HSPS 是指使用纠缠光子对中的一个来指示另外一个的到达时间。由于纠缠光子对之间存在着完美的同时性，人们以此可以预测信号（被指示）光子的精确到达时间，进而可以通过调整探测器的开关门时间与频率来降低真空脉冲与多光子脉冲的比率，从而获得较高的密钥提取率与安全传输距离。

本文详细介绍了具体的理论方案与公式推导过程，同时给出相应的数值模拟，通过与现有的其他方案作比较，证明了使用指示单光子源的新方案具有显著的优点，在以后的量子密钥分配的实用化进程中具有重要的应用与推广价值。

2　不依赖于测量装置的量子密钥分配协议

2.1　指示单光子源

通常，人们利用参量下转换的过程来制备纠缠光子对，比如，通过合适的相位匹配条件，可以得到以下双模光场[19]：

$$|\zeta\rangle = \cosh^{-1}\chi \sum_{n=0}^{\infty} \exp(in\theta)\tanh^{n}\chi \,|\, n,n\rangle, \quad (1)$$

式中 $|\, n\rangle$ 代表 n 光子态，θ 代表相位角，$\exp(in\theta)$ 代表各个光子态之间的相对相位，而 $\sin^2\chi$ 代表其中一个模式的平均光子数（或光脉冲的平均强度），为方便起见，使用 x 来标记信号光脉冲的平均强度。

把纠缠光子对中的一个用探测器探测吸收后作为指示信号，另外一个光子的模式在一定实验条件下可以满足热光场分布[20]，即

$$\rho_x = \sum_{n=0}^{\infty} [1-(1-d_i)\,(1-\eta_i)^n] \times \frac{x^n}{(1+x)^{n+1}} \,|\, n\rangle\langle n \,|\,, \quad (2)$$

式中 η_i 和 d_i 分别代表对指示光子探测时的探测效率和暗计数率。

2.2　MDI-QKD 理论方案

实验方案示意图如图 1 所示，其中 MD 代表强度调节器，PDC 代表非线性晶体，PR 代表偏振旋转片，BS 代表分束器，PBS 代表偏振分束器，D1～D4 代表 4 个单光子探测器。由 Alice 和 Bob 端发送过来的单光子源同时到达 BS 以后，以 50% 的概率透射或反射，被分成两条路径穿过 PBS，最后分别进入单光子探测器 D1～D4。为方便起见，以偏振编码的 BB84 协议为例来进行说明（注：本方案同样适用于其他协议）。把需要建立密钥的通信双方分别称为 Alice 和 Bob，把位于两者之间的第三方称为 Charlie，Charlie 可以是不受信任的第三方，甚至可以是窃听者。建立密钥的过程可以分为以下 4 个步骤：

1）Alice（A）和 Bob（B）分别独立制备自己的纠缠光子对，一方面探测吸收其中一个（休闲）光子，并根据探测结果，每探测到一个休闲光子，就发射出

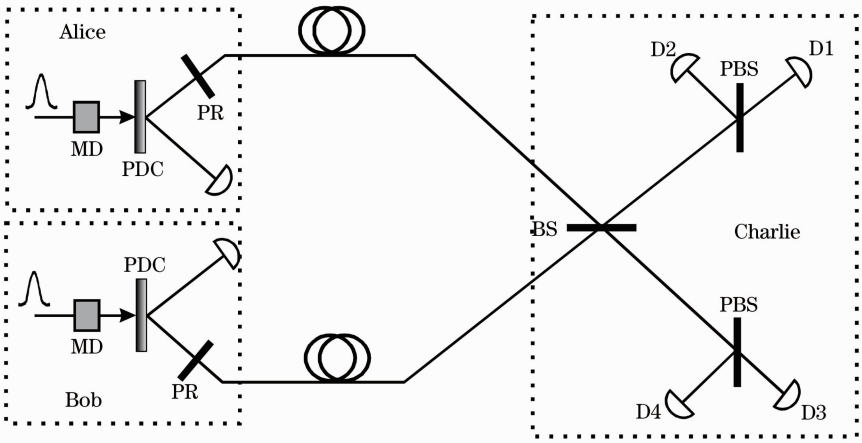

图 1　实验装置示意图

Fig. 1　Schematic of experimental setup

一个指示信号给 Charlie；另一方面，它们把每个信号光子任意编码在两组基（水平、竖直基，即“H/V”，记为 Z 基或±45°基，即“+/−”，记为 X 基）组成的 4 个偏振态中的其中一个态上，随即发送给 Charlie。

2) Charlie 对 Alice 和 Bob 发送过来的光脉冲做 Bell 基投影测量操作（此方案只需要区分出 4 个 Bell 态中的两个即可，因而，实际上所进行的是部分 Bell 基投影测量），并把测量结果为 Ψ^+（探测器 1，2 或 3，4 同时响应）和 Ψ^-（探测器 1，4 或 2，3 同时响应）的符合事件记录为成功事件，其余均为非成功事件，待所有信号传输完毕以后公布他的测量结果。

3) Alice 和 Bob 根据 Charlie 公布的测量结果，它们中的一个把对应于成功事件的编码进行相应的比特翻转操作，具体如表 1 所示，得到筛选码。

4) Alice 和 Bob 把筛选码进行纠错和保密放大等操作，获得最终码，即安全密钥。

表 1　Alice 与 Bob 对于成功事件采取的比特翻转操作列表

Table 1　List of either Alice or Bob appling bit-flip operation on their bits corresponding to the successful events

Alice and Bob	Project on $\|\Psi^-\rangle$	Project on $\|\Psi^+\rangle$
H/V base	Bit-flip	Bit-flip
+/− base	Bit-flip	No change

值得注意的是，以上步骤仅仅是针对理想纠缠光源的方案，但是在实际的 HSPS 光源中还存在着相当比率的真空脉冲与多光子脉冲，且无法直接测得其中单光子脉冲比率的大小。针对非理想的 HSPS 光源，可以使用诱骗态的方法估计出所有成功事件中由单光子脉冲引起的比率大小，进而可以得到由单光子脉冲产生的误码率的大小。具体做法如下：Alice 和 Bob 在制备 HSPS 光源时，分别使用三种不同强度的抽运光，对应产生被指示信号光脉冲的强度分别是 0，μ 和 μ'，其中 $0<\mu<\mu'$。需要强调的是，不同强度的抽运光的选取顺序是随机的。

实验中使用了 Z 和 X 两组基，定义：Y_{mn}^{W} 为在 W（W = Z 或 X）基上，当 Alice 发射一个包含 m 个光子的脉冲，同时 Bob 发射一个包含 n 个光子的脉冲时，成功符合事件的产生率，e_{mn}^{W} 为对应的误码率；$S_{xy}^{\mathrm{W}}(E_{xy}^{\mathrm{W}})$ 代表 Alice、Bob 分别发射强度为 x，y 脉冲的成功符合事件的计数率（误码率）大小。假设这两组基是分别独立完成的，则在后面的公式推导中，可以略去上角标 W。

2.3　公式推导

对于 Alice 和 Bob 端发射的强度分别为 x，y 的被指示双脉冲信号，它们的密度矩阵可记为

$$\rho_{xy}=\left[\sum_{n=0}^{\infty}q_n^{\mathrm{A}}\frac{x^n}{(1+x)^{n+1}}\mid n\rangle\langle n\mid\right]\otimes\left[\sum_{n=0}^{\infty}q_n^{\mathrm{B}}\frac{y^n}{(1+y)^{n+1}}\mid n\rangle\langle n\mid\right],\tag{3}$$

式中 $q_n^{\mathrm{i}}=1-(1-d_i)(1-\eta_i)^n$，i=A，B。由此，把 Charlie 的测量结果中对应于成功事件的符合计数率记为

$$\begin{aligned}S_{xy}=&\widetilde{S}_{00}+\eta_{\mathrm{A}}\eta_{\mathrm{B}}\frac{x}{(1+x)^2}\frac{y}{(1+y)^2}Y_{11}+\eta_{\mathrm{A}}\frac{x}{(1+x)^2}\sum_{n=2}^{\infty}[1-(1-\eta_{\mathrm{B}})^n]\frac{y^n}{(1+y)^{n+1}}Y_{1n}+\\&\eta_{\mathrm{B}}\frac{y}{(1+y)^2}\sum_{n=2}^{\infty}[1-(1-\eta_{\mathrm{A}})^n]\frac{x^n}{(1+x)^{n+1}}Y_{n1}+\sum_{m=2,n=2}^{\infty}[1-(1-\eta_{\mathrm{A}})^m][1-(1-\eta_{\mathrm{B}})^n]\times\\&\frac{x^m}{(1+x)^{m+1}}\frac{y^n}{(1+y)^{n+1}}Y_{mn},\end{aligned}\tag{4}$$

式中 $\widetilde{S}_{00}=S_{x0}+S_{0y}-S_{00}$，$S_{x0}=\dfrac{d_{\mathrm{B}}}{1+x}\sum_{n=0}^{\infty}[1-(1-d_{\mathrm{A}})(1-\eta_{\mathrm{A}})^n]Y_{n0}$，$S_{0y}=\dfrac{d_{\mathrm{A}}}{1+y}\sum_{n=0}^{\infty}[1-(1-d_{\mathrm{B}})\times(1-\eta_{\mathrm{B}})^n]Y_{0n}$，$S_{00}=\dfrac{d_{\mathrm{A}}}{1+x}\dfrac{d_{\mathrm{B}}}{1+y}Y_{00}$（注：$S_{x0}$，$S_{0y}$ 和 S_{00} 的数值在实验中可以直接测得，因而 $\widetilde{S}_{00}$ 的大小也可以视为已知）。

根据(4)式，当 Alice 和 Bob 同时发送强度为 μ 或是 μ' 的脉冲时，得到

$$\begin{aligned}S_{\mu\mu}=&\widetilde{S}_{00}+\eta_{\mathrm{A}}\eta_{\mathrm{B}}\frac{\mu}{(1+\mu)^2}\frac{\mu}{(1+\mu)^2}Y_{11}+\eta_{\mathrm{A}}\frac{\mu}{(1+\mu)^2}\sum_{n=2}^{\infty}[1-(1-\eta_{\mathrm{B}})^n]\frac{\mu^n}{(1+\mu)^{n+1}}Y_{1n}+\\&\eta_{\mathrm{B}}\frac{\mu}{(1+\mu)^2}\sum_{n=2}^{\infty}[1-(1-\eta_{\mathrm{A}})^n]\frac{\mu^n}{(1+\mu)^{n+1}}Y_{n1}+\sum_{m=2,n=2}^{\infty}[1-(1-\eta_{\mathrm{A}})^m][1-(1-\eta_{\mathrm{B}})^n]\frac{\mu^m}{(1+\mu)^{m+1}}\frac{\mu^n}{(1+\mu)^{n+1}}Y_{mn},\end{aligned}\tag{5}$$

$$S_{\mu'\mu'}=\widetilde{S}'_{00}+\eta_A\eta_B\frac{\mu'}{(1+\mu')^2}\frac{\mu'}{(1+\mu')^2}Y_{11}+\eta_A\frac{\mu'}{(1+\mu')^2}\sum_{n=2}^{\infty}[1-(1-\eta_B)^n]\frac{\mu'^n}{(1+\mu')^{n+1}}Y_{1n}+$$
$$\eta_B\frac{\mu'}{(1+\mu')^2}\sum_{n=2}^{\infty}[1-(1-\eta_A)^n]\frac{\mu'^n}{(1+\mu')^{n+1}}Y_{n1}+\sum_{m=2,n=2}^{\infty}[1-(1-\eta_A)^m][1-(1-\eta_B)^n]\times$$
$$\frac{\mu'^m}{(1+\mu')^{m+1}}\frac{\mu'^n}{(1+\mu')^{n+1}}Y_{mn}. \tag{6}$$

定义 $k=\frac{\mu'^3(1+\mu)^5}{\mu^3(1+\mu')^5}$，联合(5)、(6)式，可得

$$Y_{11}=\frac{k(S_{\mu\mu}-\widetilde{S}_{00})-(S_{\mu'\mu'}-\widetilde{S}'_{00})+\Gamma}{\eta_A\eta_B\left[k\frac{\mu^2}{(1+\mu)^4}-\frac{\mu'^2}{(1+\mu')^4}\right]}, \tag{7}$$

式中

$$\Gamma=\sum_{n=2}^{\infty}\eta_A[1-(1-\eta_B)^n]\left(\frac{\mu'^{n+1}}{(1+\mu')^{n+3}}-\frac{k\mu^{n+1}}{(1+\mu)^{n+3}}\right]Y_{1n}+$$
$$\sum_{n=2}^{\infty}\eta_B[1-(1-\eta_A)^n]\left[\frac{\mu'^{n+1}}{(1+\mu')^{n+3}}-\frac{k\mu^{n+1}}{(1+\mu)^{n+3}}\right]Y_{n1}+$$
$$\sum_{m=2,n=2}^{\infty}[1-(1-\eta_A)^m][1-(1-\eta_B)^n]\left[\frac{\mu'^{m+n}}{(1+\mu')^{m+n+2}}-\frac{k\mu^{m+n}}{(1+\mu)^{m+n+2}}\right]Y_{mn}. \tag{8}$$

由 $\mu'\geqslant\mu$ 可得到 $\Gamma\geqslant0$，所以(7)式可以简化为

$$Y_{11}\geqslant\frac{k(S_{\mu\mu}-\widetilde{S}_{00})-(S_{\mu'\mu'}-\widetilde{S}'_{00})}{\eta_A\eta_B\left[k\frac{\mu^2}{(1+\mu)^4}-\frac{\mu'^2}{(1+\mu')^4}\right]}. \tag{9}$$

进而可以得到成功事件中由单光子脉冲产生的符合计数率为

$$S_{11}=\eta_A\eta_B\frac{\mu'^2}{(1+\mu')^4}Y_{11}. \tag{10}$$

在信号光的制备、传输、测量过程中一共使用了两组基：Z 基与 X 基，前者一般用来作密钥提取使用，而后者一般用来作误码估计使用。在实验中，可以通过牺牲筛选码中的一部分代码做误码率测量工作，得到筛选码中比特翻转错误率 $E_{\mu'\mu'}$ 的大小。但是为了计算最终成码率，需要知道 Z 基上由单光子脉冲引起的相位翻转错误率的大小。它的值是无法直接测量的，但当代码足够长的时候，它在 Z 基上的相位翻转错误率与在 X 基上的比特翻转错误率大小相等。X 基上单光子脉冲引起的比特翻转错误率为

$$e_{11}^{X}\leqslant\frac{E_{\mu\mu}^{X}S_{\mu\mu}^{X}-E_{\mu0}^{X}S_{\mu0}^{X}-E_{0\mu}^{X}S_{0\mu}^{X}+E_{00}^{X}S_{00}^{X}}{S_{11}^{X}}. \tag{11}$$

因而，可以通过著名的 GLLP 公式来计算最终的密钥提取率[21]：

$$R\geqslant\eta_A\eta_B\frac{\mu'^2}{(1+\mu')^4}Y_{11}^{Z}[1-H_2(e_{11}^{X})]-$$
$$S_{\mu'\mu'}^{Z}f(E_{\mu'\mu'}^{Z})H_2(E_{\mu'\mu'}^{Z}), \tag{12}$$

式中 $f(\cdot)$ 指使用现有的纠错系统产生的纠错损耗因子，经验值为 1.16[17]，$H_2(\cdot)$ 为二进制香农熵，$H_2(x)=x\mathrm{lb}x-(1-x)\mathrm{lb}(1-x)$。

3　数值模拟

在实际的实验中，可以直接测得 $S_{\mu\mu}$、$S_{\mu'\mu'}$ 与 $E_{\mu\mu}$、$E_{\mu\mu}$ 的大小，同时根据(9)式与(11)式可以估算出 Y_{11} 的下限值与 e_{11} 的上限值，进而可以通过(12)式计算密钥提取率的大小。

这里只在理论上比较本文的方案与现有的其他方案的效率，即通过使用适当的信道模型，数值模拟出在没有窃听者的情况下，使用不同的方案得到的密钥提取率随信道损耗的变化。为方便起见，假设第三方 Charlie 位于 Alice 和 Bob 中间，另外假定 Charlie 使用的相同的探测器，即所有探测器的探测效率、暗计数都相同，并且探测效率与探测信号的大小无关。

如参考文献[22－23]所示，通过使用线性模型通道，可以估计出成功事件的计数率以及误码率的大小[17,22]。比如对于 Alice 端发射的任意光子态 $|n\rangle\langle n|$，当它到达 Charlie 端进行 Bell 基投影之前，经过信道损耗后变为 $\sum_{k=0}^{\infty}C_n^k\eta^k(1-\eta)^{n-k}|k\rangle\langle k|$，其中 η 代表从 Alice 到 Charlie 的信道穿透率。通过使用此线性通道模型，可以通过数值模拟给出，当没有窃听者的情况下，$S_{\mu\mu}$、$S_{\mu'\mu'}$ 与 $E_{\mu\mu}$、$E_{\mu\mu}$ 的大小，进而可以计算最终成码率的大小。

在以下的数值模拟中，采用与参考文献[17，22－23]中相同的实验参数，如表 2 所示，其中 α 代表信道损耗率，e_d 代表系统的调节误差，d_C 代表 Charlie 端探测器的暗计数率。除此之外，假设 Alice 和 Bob 使用的指示探测器的探测效率相同，例如，$\eta_A=\eta_B=0.9$（或0.6），并且它们的暗计数率相同，例如$d_A=d_B=10^{-6}$/pulse。具体的数值模拟结果如图 2 和图 3所示。图中曲线 W_0 和 W_1 代表使用 WCS 光源的数值模拟结果，曲线 H_0 和 H_1 代表使用 HSPS 的结果，曲线 W_0、H_0 和曲线 W_1、H_1 分别代表理想情况下使用无穷多个强度诱骗态与使用三密度诱骗态方案的结果。

表 2　数值模拟使用参数

Table 2　Parameters used in numerical simulation

α /(dB/km)	e_d/%	d_C/pulse^{-1}
0.2	1.5	3×10^{-6}

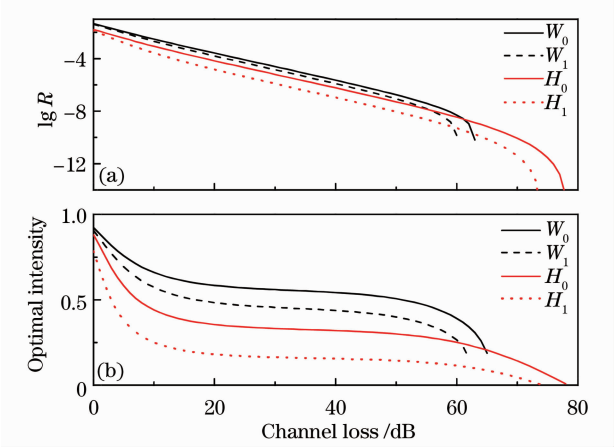

图 2　(a) 量子密钥提取率随信道损耗的变化；(b)对应图(a)中每条曲线的最优强度 μ' 的值($\eta_A=\eta_B=0.9$，$\mu=0.05$)

Fig. 2　(a) Key generation rate verus channel loss; (b) optimal untensity of μ' for each curve in Fig. (a) ($\eta_A=\eta_B=0.9$, $\mu=0.05$)

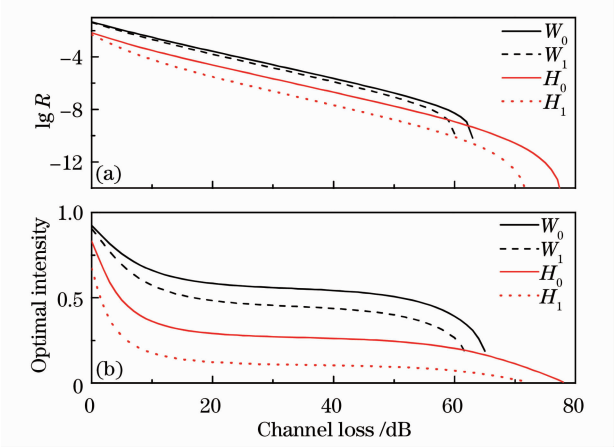

图 3　(a)量子密钥提取率随信道损耗的变化；(b)对应图(a)中每条曲线的最优强度 μ' 的值($\eta_A=\eta_B=0.6$，$\mu=0.05$)

Fig. 3　(a) Key generation rate versus channel loss; (b) optimal intensity of μ' for each curve in Fig. (a) ($\eta_A=\eta_B=0.6$, $\mu=0.05$)

4　分析讨论

从图 2、3 可以看出，本文的实验方案与现有的其他方案(使用 WCS 光源)相比，可以承受更大的信道传输损耗，其理论值大于 15 dB，对应于七十多千米的光纤传输距离。并且当指示探测器的探测效率越高时，可以承受的最大传输损耗越大。这主要由于真空脉冲在 HSPS 光源中所占比例远小于在 WCS 光源中所占比例。但是，当信道损耗较小时(小于 60 dB)，使用 WCS 光源可以获得较高的密钥提取率。这主要由于在数值模拟时，对 HSPS 光源使用了热光场(超泊松)分布，而 WCS 光源则使用了泊松分布。后者与前者相比，显然具有较高的单光子比例，因而可以使用较高的最优信号强度 μ'，则获得的密钥提取率也较高。但是在损耗很大时(大于 60 dB)，HSPS 光源方案则可以使用较高的最优信号强度，则相应的密钥提取率也较高。

根据参考文献[24－25]，新方案理论上也可以使用具有泊松分布或者亚泊松分布的 HSPS 光源。在这些情况下，对应的最优信号强度与密钥提取率都将大大提高，从而可以得到显著优于 WCS 光源方案的结果。

此外，在实际的密钥分配实验中，本文使用 HSPS 光源的方案实际可能测得的 X 基上的误码率远小于使用 WCS 的方案的情况。关键在于，HSPS 光源中的指示信号可以大大降低成功事件(双光子符合)中的两个光子同时来自于 Alice 或同时来自于 Bob 端的比率，因而具有更优的实用性能。

5　结　　论

提出了一种新型的具有安全性好，密钥提取率高以及传输距离远等优点，以指示单光子源为基础的不依赖于测量装置的量子密钥分配方案。与原来的弱相干态方案相比，可以容忍大于 15 dB 的信道损耗，相当于七十多千米的传输距离。此外，三密度诱骗态的实验方案，在现有的实验技术水平下可以很容易实现。该方案在今后量子密钥的实用化发展

中具有重要的应用价值与发展前景。

参 考 文 献

1 D Mayers. Unconditional security in quantum cryptography [J]. J ACM, 2001, 48(3): 351－406.

2 P W Shor, J Preskill. Simple proof of security of the BB84 quantum key distribution protocol [J]. Phys Rev Lett, 2000, 85(2): 441－444.

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

4 B Huttner, N Imoto, N Gisin, *et al*.. Quantum cryptography with coherent states [J]. Phys Rev A, 1995, 51(3): 1863－1869.

5 G Brassard, N Lutkenhaus, T Mor, *et al*.. Limitations on practical quantum cryptography [J]. Phys Rev Lett, 2000, 85(6): 1330－1333.

6 Chen Yan, Yang Hongyu, Deng Ke. Effects of photon-number-splitting attacks on the security of satellite-to-ground quantum key distribution systems [J]. Acta Optica Sinica, 2009, 29(11): 2989－2993.
陈　彦, 杨红宇, 邓　科. 光子数分束攻击对量地量子密钥分配系统安全的影响[J]. 光学学报, 2009, 29(11): 2989－2993.

7 B Qi, C H F Fung, H K Lo, *et al*.. Time-shift attack in practical quantum cryptosystems [J]. Quantum Inf Comput, 2007, 7: 073－082.

8 Y Zhao, C H F Fung, B Qi, *et al*.. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems [J]. Phys Rev A, 2008, 78(4):042333.

9 V Makarov, A Anisimov, J Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems [J]. Phys Rev A, 2006, 74(2): 022313.

10 C H F Fung, B Qi, K Tamaki, *et al*.. Phase-remapping attack in practical quantum-key-distribution systems [J]. Phys Rev A, 75(3): 032314.

11 W Y Hwang. Quantum key distribution with high loss: toward global secure communication [J]. Phys Rev Lett, 2003, 91(5): 057901.

12 X B Wang. Beating the photon-number-splitting attack in practical quantum cryptography [J]. Phys Rev Lett, 2005, 94(23): 230503.

13 H K Lo, X Ma, K Chen. Decoy state quantum key distribution [J]. Phys Rev Lett, 2005, 94(23): 230504.

14 C H F Fung, K Tamaki, B Qi, *et al*.. Security proof of quantum key distribution with detection efficiency mismatch [J]. Quantum Inf Comput, 2009, 9: 131－165.

15 A Acìn, N Brunner, N Gisin, *et al*.. Device-independent security of quantum cryptography against collective attacks [J]. Phys Rev Lett, 2007, 98(23): 230501.

16 S Pironio, A Acin, N Brunner, *et al*.. Device-independent quantum key distribution secure against collective attacks [J]. New J Phys, 2009, 11(4): 045021.

17 H K Lo, M Curty, B Qi. Measurement-device-independent quantum key distribution [J]. Phys Rev Lett, 2012, 108(13): 130503.

18 S L Braunstein, S Pirandola. Side-channel-free quantum key distribution [J]. Phys Rev Lett, 2012, 108(13): 130502.

19 B Yurke, M Potasek. Obtainment of thermal noise from a pure quantum state [J]. Phys Rev A, 1987, 36(7): 3464－3466.

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

21 D Gottesman, H K Lo, N Lutkenhaus, *et al*.. Security of quantum key distribution with imperfect devices [J]. Quantum Information and Computation, 2004, 4(5): 325－360.

22 Q Wang, X B Wang. Efficient implementation of the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources [J]. Phys Rev A, 2013, 88(5): 052332.

23 X Ma, M Razavi. Alternative schemes for measurement-device-independent quantum key distribution [J]. Phys Rev A, 2012, 86(6): 062319.

24 Q Wang, A Karlsson. Performance enhancement of a decoy-state quantum key distribution using a conditionally prepared down-conversion source in the Poisson distribution [J]. Phys Rev A, 2007, 76(1): 014309.

25 Q Wang, W Chen, G Xavier, *et al*.. Experimental decoy-state quantum key distribution with a sub-Poissonian heralded single-photon source [J]. Phys Rev Lett, 2008, 100(9): 090501.

栏目编辑：史　敏