第 57 卷 第 9 期 2008 年 9 月
1000-3290/2008/57(09)/5600-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.9,September,2008

一种新的预报单光子源诱骗态量子密钥分发方案*

权东晓† 裴昌幸 朱畅华 刘 丹

(西安电子科技大学综合业务网国家重点实验室,西安 710071)

(2007 年 12 月 20 日收到;2008 年 1 月 18 日收到修改稿)

提出一种新的预报单光子源诱骗态量子密钥分发方案.在发端采用参量下变换产生纠缠光子对,其中之一用来进行预报探测,根据探测结果将另一路光脉冲分成两个集合,其中预报探测有响应的脉冲集合用作信号态,无响应的脉冲集合作为诱骗态.由于探测效率的问题,这两个集合都是有光子的,通过这两个集合的通过率和错误率估计出单光子的通过率和错误率.此方法不需要改变光强,简单可行.仿真结果表明:该方法可以达到完美单光子源的安全通信距离;与预报单光子源的量子密钥分发相比,密钥产生率有了很大的提高;和三强度预报单光子源诱骗态量子密钥分发的密钥产生率相差不大.

关键词:量子保密通信,量子密钥分发,诱骗态,预报单光子源

PACC:4250,4230Q,0365

1. 引 言

量子信息科学是量子力学与信息科学相结合的产物,是将对人类社会产生重大影响的新兴前沿科学.量子密钥分发是量子信息科学中的重要分支.自从 1984 年,Bennett-Brassard 提出量子密钥分发的 BB84 协议以来,由于其建立在量子的不确定性原理和不可克隆原理基础上的无条件安全性,而得到了迅速的发展[1,2].2002 年,瑞士日内瓦大学的研究组在 67 km 的光纤中实现了单光子密码通信,实验单脉冲平均光子数目为 0.2,误码率为 5.6%[3].2004 年,文献[4]报道了 122 km 光纤中单向量子密钥分发实验,单脉冲平均光子数目为 0.1,误码率为 8.9%.但是由于目前还没有完美的单光子源,以上实验均是用弱相干光衰减来近似得到单脉冲,其中有些脉冲仍然含有多个光子,对光子数目分割攻击就是不安全的.2003 年,Hwang[5] 提出了基于诱骗态的量子密钥分发的思想,2004 年,Wang[6] 提出了实际可行的诱骗态量子密钥分发方案.2005 年,文献[7]也对诱骗态量子密钥分发进行了研究.2007 年初,文献[8—10]分别用实验实现了诱骗态量子密钥分发.

预报的单光子源是利用自发参量下变换产生纠缠光子对,由于这对光子几乎是同时产生的,所以它们具有相同的特性,可以用其中一束的探测结果来预报另一束光子的数目和到达时间,并控制其探测器的开启时间,这样就可以大大减少长距离量子密钥分发过程中暗计数的影响,从而增大量子密钥分发的安全距离[11—13].文献[13]基于这种光源提出了一种诱骗态量子密钥分发的方案,通过发送空脉冲和另外两束强度不同的脉冲来实现三态诱骗态量子密钥分发.本文基于这种光源提出一种新的诱骗态量子密钥分发方案,发送端只需要发送空脉冲和单一强度的脉冲就可以实现三态诱骗态量子密钥分发.

2. 一种新的诱骗态量子密钥分发方案

本文所提出的新的量子密钥分发方案如图 1 所示,图中实线表示光信号,虚线表示电信号.发送端 Alice 随机的控制是否发送强度为 u 的脉冲.通过不发送时的通过率,可以估计出接收端的暗计数概率.在发送强度为 u 的脉冲时,通过参量下转换产生光子对,其中的一束通过发送端的单光子探测器进行

* 国家自然科学基金(批准号:60572147,60672119)资助的课题.

† 通讯联系人. E-mail:dxquan@xidian.edu.cn

探测，另外一束编码后通过光纤发送.

在 Alice 端探测到光子时，将光纤中对应的脉冲的集合记为 S_1.考虑暗计数的影响，集合 S_1 中的脉冲大部分是单光子和多光子，还有极少的空脉冲，它的平均光子数目比较大，将这个集合用作信号态脉冲.当 Alice 端没有探测到光子时，将光纤中对应的脉冲的集合记为 S_0.由于探测效率的问题，S_0 的脉冲大部分是空脉冲和单光子，还有较少的多光子，平均光子数目比较小，将这个集合用作诱骗态脉冲.这样，我们就利用 Alice 端探测器的探测结果，将光纤中的光脉冲分成信号态和诱骗态两个集合，这两个集合其实都是有光子的.我们利用这两个集合的通过率和错误率来判断是否存在 PNS 攻击，估计出单光子的通过率和错误率.如果不存在攻击，则通过纠错和密性放大得到最终的密钥.这样，发送端只需要随机的控制是否发送强度为 u 的脉冲就可以实现三态诱骗态量子密钥分发.不发送时可以估计出暗计数，在发送强度为 u 的脉冲时，通过预报探测，将一束光被动地分成强度不同的两束光来估计单光子通过率和暗计数.

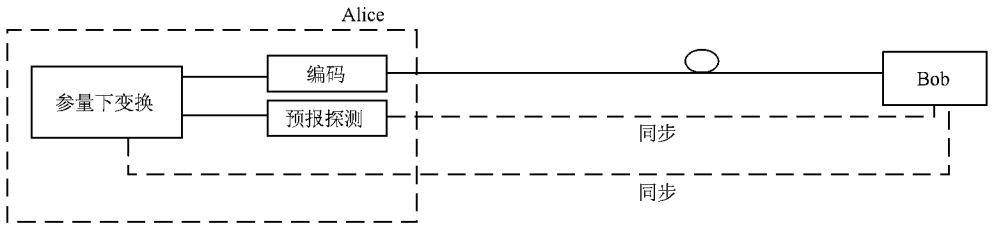

图 1　单一强度的预报单光子源诱骗态量子密钥分发

3. 密钥产生率计算

自发参量下变换的光子数目概率分布为[12]

$$p_n(u) = \frac{u^n}{(1+u)^{n+1}}. \tag{1}$$

假设 Alice 端探测器的效率是 η_A，暗计数为 d_A，用 Y_n 表示 Alice 发送 n 光子脉冲时 Bob 的探测概率，e_n 表示 Alice 发送 n 光子脉冲时 Bob 的错误探测概率.设信道的总的传输率为 η，它可以表示为 Alice 到 Bob 之间的传输率和 Bob 端探测率的乘积，即 $\eta = 10^{-\alpha L/10}\cdot\eta_B$.那么当 Alice 发送 n 光子脉冲时，Bob 端至少可收到一个光子的概率为 $\eta_n = 1-(1-\eta)^n$. Y_n 和 e_n 分别可表示为

$$Y_n = \eta_n + Y_0 - \eta_n Y_0 \approx \eta_n + Y_0, \tag{2}$$

$$e_n = \left(e_d\eta_n + \frac{1}{2}Y_0\right)/Y_n, \tag{3}$$

其中 Y_0 是 Bob 端探测器的暗计数概率，e_d 是光子到达错误探测器的概率.将 Alice 端探测器探测结果为空的集合记为 S_0，则其通过率和错误率分别为

$$Q' = P_0(1-d_A)Y_0 + \sum_{n=1}^{\infty}P_n(1-\eta_A)^nY_n, \tag{4}$$

$$Q'E' = P_0(1-d_A)Y_0e_0 + \sum_{n=1}^{\infty}P_n(1-\eta_A)^nY_ne_n. \tag{5}$$

将 Alice 端探测器探测结果非空的集合记为 S_1，则其通过率和错误率分别为

$$Q = P_0d_AY_0 + \sum_{n=1}^{\infty}P_n[1-(1-\eta_A)^n]Y_n, \tag{6}$$

$$QE = P_0d_AY_0e_0 + \sum_{n=1}^{\infty}P_n[1-(1-\eta_A)^n]Y_ne_n. \tag{7}$$

我们用探测结果非空的光作为信号态，探测结果为空的光作为诱骗态，则

$$\begin{aligned}
&(1-d_A)Q - d_AQ'\\
&= (\eta_A-d_A)Y_1P_1 + \sum_{n=2}^{\infty}[1-d_A-(1-\eta_A)^n]Y_nP_n\\
&> (\eta_A-d_A)Y_1P_1 + \left(1-\frac{d_A}{1-(1-\eta_A)^2}\right)\\
&\quad\times\sum_{n=2}^{\infty}[1-(1-\eta_A)^n]Y_nP_n\\
&= (\eta_A-d_A)Y_1P_1 + \left(1-\frac{d_A}{2\eta_A-\eta_A^2}\right)\\
&\quad\times[Q - P_0d_AY_0 - P_1\eta_AY_1].
\end{aligned} \tag{8}$$

从(8)式可以得到

$$\begin{aligned}
Y_1 > \frac{1}{\left(1-\frac{1}{2-\eta_A}\right)P_1}\Bigg\{&\left(1-\frac{1}{2\eta_A-\eta_A^2}\right)Q\\
&+ Q' - \left(1-\frac{d_A}{2\eta_A-\eta_A^2}\right)\frac{1}{1+u}Y_0\Bigg\},
\end{aligned} \tag{9}$$

则

$$Q_1 = P_1\eta_A Y_1 > \frac{\eta_A}{\left(1-\frac{1}{2-\eta_A}\right)}\left\{\left(1-\frac{1}{2\eta_A-\eta_A^2}\right)Q + Q' - \left(1-\frac{d_A}{2\eta_A-\eta_A^2}\right)\frac{1}{1+u}Y_0\right\}. \quad (10)$$

又因为

$$\begin{aligned}&(1-d_A)QE - d_A Q'E'\\ &= (\eta_A - d_A)Y_1 P_1 e_1 + \sum_{n=2}^{\infty}[1-d_A-(1-\eta_A)^n]Y_n P_n e_n\\ &> (\eta_A - d_A)Y_1 P_1 e_1,\end{aligned} \quad (11)$$

所以

$$e_1 < \frac{(1-d_A)QE - d_A Q'E'}{(\eta_A - d_A)Y_1\dfrac{u}{(1+u)^2}}. \quad (12)$$

然后将 Q, E, Q_1 和 e_1 带入 GLLP (Gottesman-Lo-Lütkenhaus-Preskill)公式[4]

$$R \geqslant q\{-Qf(E)H_2(E) + Q_1[1-H_2(e_1)]\}, \quad (13)$$

就可以计算出密钥产生率. 其中 $q=\frac{1}{2}$, $H_2(x) = -x\log_2(x)-(1-x)\log_2(1-x)$是二元熵; $f(x)$是双向纠错的效率. 文献[14]给出了 $f(x)$的取值,如表 1 所示.

表 1 双向纠错效率表(x 是误码率)

x	0.01	0.05	0.1	0.15
$f(x)$	1.16	1.16	1.22	1.35

4. 性能仿真

我们利用 GYS[4] 的实验结果作为参数来进行性能仿真,参数如表 2 所示, $f(x)=1.22$. 则集合 S_1 的通过率和错误率分别为

$$\begin{aligned}Q &= P_0 d_A Y_0 + \sum_{i=1}^{\infty} P_i[1-(1-\eta_A)^i]Y_i\\ &= Y_0 d_A\frac{1}{1+u} + \sum_{i=1}^{\infty}\frac{u^i}{(1+u)^i}\times[1-(1-\eta_A)^i][Y_0+1-(1-\eta)^i]\\ &= Y_0 d_A\frac{1}{1+u} + \frac{(Y_0+1)u\eta_A}{1+u\eta_A} - \frac{1}{1+u\eta} + \frac{1}{1+u\eta_A+u\eta-u\eta\eta_A}.\end{aligned} \quad (14)$$

$$\begin{aligned}EQ &= \sum_{i=1}^{\infty} e_i Y_i[1-(1-\eta_A)^i]\frac{u^i}{(1+u)^i} + \frac{1}{2}Y_0 d_A\frac{1}{1+u}\\ &= \sum_{i=1}^{\infty}\{e_0 Y_0 + e_d[1-(1-\eta)^i]\}\times[1-(1-\eta_A)^i]\frac{u^i}{(1+u)^i} + \frac{1}{2}Y_0 d_A\frac{1}{1+u}\\ &= \frac{(e_0 Y_0 + e_d)u\eta_A}{1+u\eta_A} - \frac{e_d}{1+u\eta} + \frac{e_d}{1+u\eta_A+u\eta-u\eta\eta_A} + \frac{1}{2}Y_0 d_A\frac{1}{1+u}.\end{aligned} \quad (15)$$

集合 S_0 的通过率和错误率分别为

$$\begin{aligned}Q' &= \sum_{i=0}^{\infty} P_i Y_i - Q\\ &= 1 + Y_0 - \frac{1}{1+u\eta} - Q,\end{aligned} \quad (16)$$

$$\begin{aligned}Q'E' &= \sum_{i=0}^{\infty} P_i Y_i e_i - QE\\ &= \frac{1}{2}Y_0 + e_d - \frac{e_d}{1+u\eta} - QE.\end{aligned} \quad (17)$$

表 2 量子密钥分发性能仿真参数

实验	波长 λ/nm	衰减 α/(dB/km)	检测错误率	检测效率	暗计数率	频率/MHz
GYS	1550	0.2	0.033	0.045	1.7×10^{-6}	2

4.1. 密钥产生率与发送端探测效率的关系

预报单光子源 Alice 端的暗计数率 $d_A = 5\times10^{-8}$,我们依次取 Alice 端的探测效率为 0.6, 0.8, 0.99 来进行密钥产生率的计算. 对于每一个探测效率,将(14),(15),(10),(12)式代入(13)式,利用 Matlab 计算,求出使得 R 取得最大值的强度,它们与通信距离的关系分别如图 2 中曲线所示,再将最优强度代入(13)式可得 R 与通信距离的关系如图 3 中曲线所示.

4.2. 与其他量子密钥分发方法的性能比较

在此过程中我们取 $\eta_A = 0.6$,暗计数率 $d_A = 5\times10^{-8}$. 本文所提出的方法的最优强度与通信距离的关系如图 4 中 MDHSPS 曲线所示, R 与通信距离的关系如图 5 中 MDHSPS 曲线所示.

如果不采用诱骗态,只是利用预报单光子源来进行密钥分发,则其最优强度与通信距离的关系如

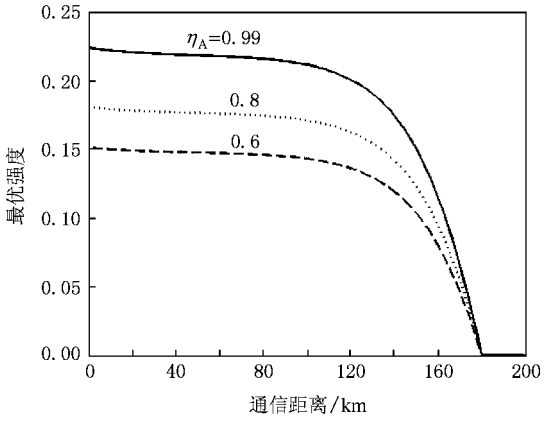

图 2　最优强度与通信距离的关系

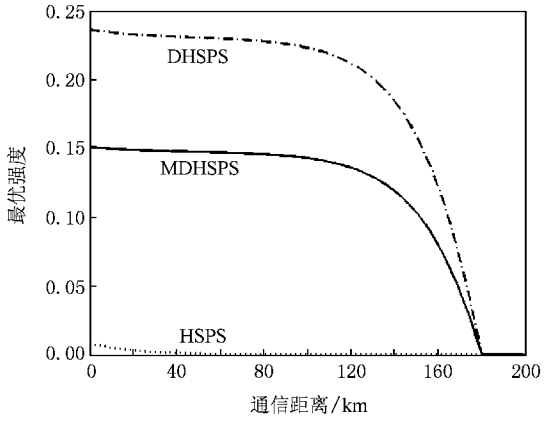

图 4　不同协议最优强度与通信距离的关系

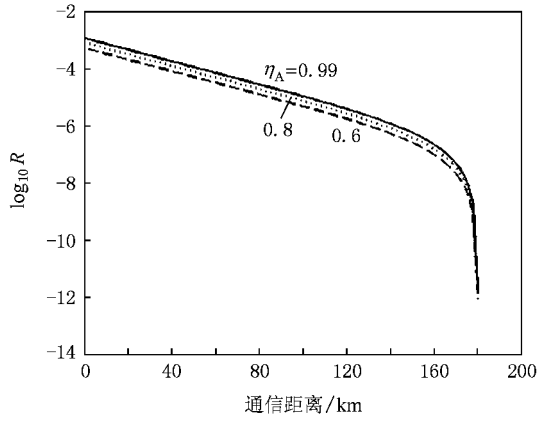

图 3　量子密钥产生率与通信距离的关系

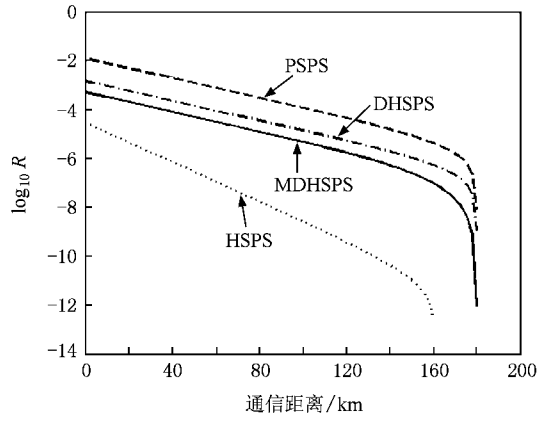

图 5　不同协议量子密钥产生率与通信距离的关系

图 4 中 HSPS 曲线所示，最优强度的取值很小；R 与通信距离的关系如图 5 中 HSPS 曲线所示，安全通信距离达到 161 km.

对于三强度的诱骗态预报单光子源量子密钥分发，其最优强度与通信距离的关系如图 4 中 DHSPS 曲线所示；R 与通信距离的关系如图 5 中 DHSPS 曲线所示.

完美单光子源的密钥产生率与通信距离的关系如图 5 中的 PSPS 曲线所示.

5. 结　论

本文提出了利用单一强度的预报单光子源和空脉冲来进行诱骗态量子密钥分发的方法，推导了密钥产生率的计算公式，仿真了最优强度和密钥产生率与发送端探测效率的关系，并且和非诱骗态、三强度诱骗态、以及完美单光子源的密钥分发进行了性能比较，从而得出以下结论：

1. 本文所提出的方法的密钥产生率随着发送端探测效率的增加而增大，安全通信距离均达到了完美单光子源的通信距离.

2. 与非诱骗态相比，诱骗态量子密钥分发更好地估计出了单光子的通过率和错误率，提高了最优强度，从而提高了密钥产生率和安全通信距离.

3. 本文所提出的方法的密钥产生率，约为三强度预报单光子源的密钥产生率的 1/3，如果在三强度预报单光子源诱骗态量子密钥分发的过程中，诱骗源和信号源的比例为 1∶1，则本文所提方法的密钥产生率可以达到其密钥产生率的 2/3. 但是这种方法不需要改变光强，只用单一的光源即可实现. 而且在三强度预报单光子源的方法中，为了达到最优的密钥产生率，诱骗态的强度非常小，很难得到精确的控制.

因此，本文所提出的诱骗态量子密钥分发是一种简单可行的量子密钥分发方案.

[1] Bennett C H, Brassard G 1984 *Int. Conf. Computers Systems and Signal Processing* (Bangalore, New York, IEEE) pp175—179

[2] Wu G, Zhou C Y, Chen X L *et al* 2005 *Acta Phys. Sin.* **54** 3622 (in Chinese) [吴 光、周春源、陈修亮 等 2005 物理学报 **54** 3622]

[3] Stucki D, Gisin N, Guinnard O *et al* 2002 *New J. Phys.* **4** 41

[4] Gobby C, Yuan Z L, Shields A J 2004 *Appl. Phys. Lett.* **84** 3762

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

[6] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[7] Ma X F, Qi B, Zhao Y *et al* 2005 *Phys. Rev.* A **72** 012326

[8] Peng C Z, Zhang J, Y D *et al* 2007 *Phys. Rev. Lett.* **98** 010505

[9] Rosenberg D, Harrington J W, Rice P R *et al* 2007 *Phys. Rev. Lett.* **98** 010503

[10] Schmitt-Manderbach T, Weier H, Furst M *et al* 2007 *Phys. Rev. Lett.* **98** 010504

[11] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304

[12] Horikiri T, Kobayashi T 2006 *Phys. Rev.* A **73** 032331

[13] Wang Q, Wang X B, Guo G C 2007 *Phys. Rev.* A **75** 012312

[14] Brassard G, Salvail L 1994 in Advances in Cryptology-EUROCRYPT '93, Vol. 765 of Lecture Notes in Computer Science. (Springer, Berlin) pp410—423

New method of decoy state quantum key distribution with a heralded single-photon source*

Quan Dong-Xiao† Pei Chang-Xing Zhu Chang-Hua Liu Dan

(*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an* 710071, *China*)

(Received 20 December 2007; revised manuscript received 18 January 2008)

Abstract

We propose a new method of decoy state quantum key distribution with a heralded single-photon source. Alice uses the parametric down-conversion to generate entangled photon-pairs, one of the pair is used as heralding photon. According to the results of the trigger detector the heralded photons are divided into trigger and non-trigger sets. The states of the photons in the trigger set are used as the signal states and the ones in the non-trigger sets are used as the decoy states. Because of the efficiency of the trigger detector, the two sets both have photons. The yield and error rate of the single-photon are estimated through the yield and error rate of the two sets. This method does not need changing the intensity of the photon source, is easy to implement. Analysis results show that this method can reach the same security distance as with a perfect single photon source; the key generation rate is increased a lot compared with the method with a heralded photon source and is approximately two thirds the rate of the three intensities decoy state quantum key distribution with a heralded photon source.

Keywords: quantum cryptography, quantum key distribution, decoy state, heralded single-photon source

PACC: 4250, 4230Q, 0365

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60572147, 60672119).

† Corresponding author. E-mail: dxquan@xidian.edu.cn