简单的非正交诱惑态量子密钥分配方案

周媛媛，周学军，李晓强，高 俊

(海军工程大学电子工程学院 武汉 430033)

【摘要】基于预报单光子光源，提出了一种实现简单的非正交一诱惑态方案。由于非正交编码协议需要估计参量的项数是BB 84协议的两倍，所以无法完全采用被动诱惑态方案来降低实现的难度。并考虑到实际应用中，激光器不能做到完全消光而无法制备真正的真空态。因此，将主动诱惑态思想和被动诱惑态思想相结合，把所需诱惑态减少为一个弱光强态。数值仿真表明，由于被动诱惑态思想的加入，非正交一诱惑态方案可以获得较高的密钥生成效率，安全传输距离较理论极限安全传输距离只少2.2 km；且相比于已经提出的非正交诱惑态方案，因为诱惑态数量的减少而更容易实现。

关 键 词 诱惑态； 非正交编码协议； 量子密钥分配； 密钥生成效率； 安全传输距离

中图分类号 TN918 **文献标识码** A doi:10.3969/j.issn.1001-0548.2011.02.007

Simple Non-Orthogonal Decoy State Protocol in Quantum Key Distribution

ZHOU Yuan-yuan, ZHOU Xue-jun, LI Xiao-qiang, and GAO Jun

(Electronic Engineering College, Naval University of Engineering Wuhan 430033)

Abstract A simple non-orthogonal decoy state protocol with one weak decoy state is presented with a heralded single photon source (HSPS). Because the number of estimation terms in non-orthogonal encoding protocol is double of that in the Bennett-Brassard 1984 (BB 84) protocol, the passive decoy state method is unsuitable for non-orthogonal encoding protocol to decrease the implementation difficulty. Considering the imperfect extinction ratio of the practical laser, vacuum states are not prepared easily. Therefore, this paper combines passive decoy state method with active decoy state method to decrease the number of decoy state to one weak decoy state. The simulation results show that the protocol with one weak decoy state can obtain good key generation rate by the passive decoy idea and the secure transmission distance is only 2.2 km less than that of the theoretical limit of an infinite decoy state protocol. Compared with the existing non-orthogonal decoy state protocols, the proposed protocol is easier to implement.

Key words decoy state; non-orthogonal encoding protocol; quantum key distribution; secure key generation rate; secure transmission distance

目前量子密钥分配(quantum key distribution，QKD)[1]系统没有严格的单光子光源，而是用强衰减的弱相干态脉冲(weak coherent pulse，WCP)来代替。因此光源输出的脉冲会有一部分含有多个光子，使得QKD系统受到光子数分离(photon number splitting，PNS)[2]攻击的威胁。幸运的是，文献[3]提出可以抵抗PNS攻击的诱惑态方案，该方案由于需要发送方Alice主动产生诱惑态，被称为主动诱惑态方案[4]。但基于WCP光源的主动诱惑态方案有两个缺点：1) 当传输距离超过100 km后，系统的暗计数成为影响密钥生成效率的主要因素；2) Alice需要额外产生诱惑信号，从而增加了实际系统实现的难度，且诱惑态数量越多实现难度越大，引入的不稳定因素也越多。文献[5-8]提出的预报单光子光源(HSPS)在QKD系统中的应用为解决以上问题带来希望。HSPS能产生两个相同的特性模式，不但可以有效抑制暗计数的影响，也为文献[8]提出基于门限探测器的被动诱惑态方案(AYKI)奠定了基础。由于只需产生一个强度的信号，所以AYKI方案实现非常容易，无需对标准QKD系统的硬件做任何改动。

以上研究都基于BB 84协议。文献[9]提出的非正交编码协议(SARG 04)从BB 84协议发展而来，只是编码部分有所不同，两个协议完全可在相同的实验设备上实现，因此研究SARG 04诱惑态方案的性

收稿日期：2009－09－15； 修回日期：2010－01－18
基金项目：国家863计划(2009AAJ128)
作者简介：周媛媛(1979－)，女，博士生，主要从事量子信息、光纤量子密码通信方面的研究.

能有着重要的现实意义。由于SARG 04协议允许2-光子态进行安全传输，需要估计的参量项数比BB 84协议多一倍，所以设计简单的SARG 04诱惑态方案难度更大。另外，由于在实验中，激光器存在自发辐射，不能做到完全消光，无法制备真正的真空态，本文提出了实现简单的SARG 04一诱惑态方案(一个弱光强态)，以解决以上两个问题。

1 基于HSPS的SARG 04诱惑态方案

1.1 HSPS QKD系统模型

HSPS光源所产生的双模态为：

$$|\psi\rangle_{\mathrm{TS}}=\sum_{n=0}^{\infty}\sqrt{P_n}\,|n\rangle_{\mathrm{T}}\,|n\rangle_{\mathrm{S}} \tag{1}$$

式中，$|n\rangle$ 为n-光子态；$P_n=x^n/(1+x)^{n+1}$为光源产生n-光子态的概率，x为一个模式的信号强度。HSPS光源利用未退化参数转换产生纠缠光子对，由于该光子对几乎是同时产生，所以该两个模式具有完全相同的特性。其中，模式S作为信号模式被发送给接收方Bob，而模式T被Alice端探测器检测，预报模式S的光子数和到达时间，可大大减少长距离量子密钥分配过程中暗计数的影响。

Y_n为n-光子态的计数率，即Alice发送一个n-光子态，Bob端探测器响应的概率。G_n为n-光子态的全局计数率。根据Alice端探测器是否响应，G_n可以分为响应集合$G_n^{(t)}$和未响应集合$G_n^{(nt)}$：

$$G_n^{(t)}=Y_n[1-(1-\eta_{\mathrm{A}})^n]\frac{x^n}{(1+x)^{n+1}} \tag{2}$$

$$G_n^{(nt)}=Y_n(1-\eta_{\mathrm{A}})^n\frac{x^n}{(1+x)^{n+1}} \tag{3}$$

式中，η_{A}为Alice端探测器探测效率。

Q_x为信号强度为x的光子源的总计数率，其同样可分为$Q_x^{(t)}$和$Q_x^{(nt)}$两部分：

$$Q_x^{(t)}=\frac{d_{\mathrm{A}}Y_0}{1+x}+\sum_{n=1}^{\infty}G_n^{(t)} \tag{4}$$

$$Q_x^{(nt)}=\frac{(1-d_{\mathrm{A}})Y_0}{1+x}+\sum_{n=1}^{\infty}G_n^{(nt)} \tag{5}$$

式中，d_{A}为Alice端探测器的暗计数率。

与以上相同，信号强度为x的光子源的量子比特误码率(quantum bit error Rate，QBER)可写为：

$$E_x^{(t)}Q_x^{(t)}=\frac{d_{\mathrm{A}}Y_0e_0}{1+x}+\sum_{n=1}^{\infty}G_n^{(t)}e_n \tag{6}$$

$$E_x^{(nt)}Q_x^{(nt)}=\frac{(1-d_{\mathrm{A}})Y_0e_0}{1+x}+\sum_{n=1}^{\infty}G_n^{(nt)}e_n \tag{7}$$

式中，e_n为n-光子态的误码率；e_0=1/2，为随机背景噪声产生的误码率。

Bob探测到的所有信号都可以根据Alice的探测情况被分到不同的集合，那么每个集合都可用GLLP (Gottesman-Lo-Lütkenhaus-Preskill)[10]的思想进行分析，则最终密钥生成效率可以看成是响应集合和未响应集合各自密钥生成效率的总和，即$R^{(\mathrm{both})}=R^{(t)}+R^{(nt)}$，其中：

$$R^{(t)}\geqslant\frac{1}{4}\{-Q_u^{(t)}f(E_u^{(t)})H_2(E_u^{(t)})+G_0^{(t)}+G_1^{(t)}[1-H_2(e_1)]+G_2^{(t)}[1-H_2(e_2)]\} \tag{8}$$

$$R^{(nt)}\geqslant\frac{1}{4}\{-Q_u^{(nt)}f(E_u^{(nt)})H_2(E_u^{(nt)})+G_0^{(nt)}+G_1^{(nt)}[1-H_2(e_1)]+G_2^{(nt)}[1-H_2(e_2)]\} \tag{9}$$

式中，1/4为SARG 04协议的筛选效率；下标u为信号态强度；$f(x)$为以误码率为变量的双向纠错效率函数；$H_2(x)=-x\log_2(x)-(1-x)\log_2(1-x)$；$Q_u^{(t)}$、$Q_u^{(nt)}$、$E_u^{(t)}$和$E_u^{(nt)}$可在诱惑态方案实验中直接观测得到(当有真空诱惑态时，$G_0^{(t)}$、$G_0^{(nt)}$也可由观测得到)。为了对现实QKD系统的密钥生成效率进行估算，需求得Y_1和Y_2的下限及e_1和e_2的上限。

因为只有在传输距离不是很远时(距离界限因不同协议、不同参数而不同)，$R^{(nt)}$才对密钥生成有积极的贡献[8]，所以为了得到传输全程每点距离的最佳密钥生成效率，取$R=\max\{R^{(t)},R^{(\mathrm{both})}\}$。

1.2 一诱惑态方案(一个弱光强态)

在主动诱惑态方案中，当Alice端探测器没有响应时，Bob端探测器可以不工作，即完全舍弃未响应集合的数据，只用响应集合来估计参量和生成密钥。本文将主动诱惑态方案和被动诱惑态方案相结合，把响应集合和未响应集合都应用到参量估计和密钥产生中。因此不管Alice端探测器是否响应，Bob端探测器都要进行检测。

在实际应用中，激光器的调制电压设为零时，由于激光器固有的自发辐射，因此所制备的态并不完全是真空态。在此情况下，再也不能利用真空态精确估算系统的暗计数率，于是以真空态和弱光强态作为诱惑态的方案就相当于只使用了弱光强态。本文设Alice和Bob只采用一个弱光强态作为诱惑态，其平均光子数为v，信号态的平均光子数为u。相对于已提出的三诱惑态和二诱惑态方案[5]，本文方案减少了诱惑态的数量，也就降低了实际系统操作上的难度。下面将讨论在此情况下的诱惑态方案。

由于没有真空诱惑态，无法直接对暗计数率进行观测，所以需要对Y_0的值进行估计。根据式(7)可

以简单估计Y_0的上限为：

$$Y_0 \leqslant \frac{(1+u)E_u^{(nt)}Q_u^{(nt)}}{e_0(1-d_{\mathrm{A}})} \tag{10}$$

利用 $\dfrac{(1+v)\left(\dfrac{u}{1+u}\right)^2 Q_v^{(t)}}{1-(1-\eta_{\mathrm{A}})^2} - \dfrac{(1+u)\left(\dfrac{v}{1+v}\right)^2 Q_u^{(nt)}}{(1-\eta_{\mathrm{A}})^2}$ 可以推导Y_1的下限为：

$$Y_1 \geqslant \frac{(1+v)Q_v^{(t)} - d_{\mathrm{A}}Y_0^v}{\dfrac{\eta_{\mathrm{A}}v}{1+v} - \dfrac{2\eta_{\mathrm{A}}-\eta_{\mathrm{A}}^2}{1-\eta_{\mathrm{A}}}\dfrac{1+u}{u}\left(\dfrac{v}{1+v}\right)^2} - \frac{(1+u)Q_u^{(nt)} - (1-d_{\mathrm{A}})Y_0^v}{\dfrac{(1-\eta_{\mathrm{A}})^2}{2-\eta_{\mathrm{A}}}\dfrac{1+v}{v}\left(\dfrac{u}{1+u}\right)^2 - \dfrac{(1-\eta_{\mathrm{A}})u}{1+u}} \tag{11}$$

满足式(11)的条件为$v \leqslant au/(1+u-au)$，其中$a = \{[(1-\eta_{\mathrm{A}})^{n-2} - (1-\eta_{\mathrm{A}})^n]/[1-(1-\eta_{\mathrm{A}})^n]\}^{1/(n-2)}$。

同理，由 $\dfrac{(1+v)\left(\dfrac{u}{1+u}\right)Q_v^{(t)}}{\eta_{\mathrm{A}}} - \dfrac{(1+u)\left(\dfrac{v}{1+v}\right)Q_u^{(nt)}}{1-\eta_{\mathrm{A}}}$ 可得Y_2的下限为：

$$Y_2 \geqslant \frac{Q_v^{(t)}(1+v) - Y_0^v d_{\mathrm{A}}}{\eta_{\mathrm{A}}(2-\eta_{\mathrm{A}})\left(\dfrac{v}{1+v}\right)^2 - \dfrac{v\eta_{\mathrm{A}}(1-\eta_{\mathrm{A}})}{1+v}\left(\dfrac{u}{1+u}\right)} - \frac{(1+u)Q_u^{(nt)} + Y_0^v(1-d_{\mathrm{A}})}{\dfrac{u\left(\eta_{\mathrm{A}}^2-3\eta_{\mathrm{A}}+2\right)}{1+u}\left(\dfrac{v}{1+v}\right) - (1-\eta_{\mathrm{A}})^2\left(\dfrac{u}{1+u}\right)^2} \tag{12}$$

满足式(12)的条件为$v \leqslant bu/(1+u-bu)$，其中$b = (1-\eta_{\mathrm{A}})\{\eta_{\mathrm{A}}/[1-(1-\eta_{\mathrm{A}})^n]\}^{1/(n-1)}$。综合以上$v$应该满足的两个条件，最终取：

$$v \leqslant \min\{au/(1+u-au); bu/(1+u-bu)\} \tag{13}$$

因为$\eta_{\mathrm{A}} >> d_{\mathrm{A}}$，所以真空态在响应集合的贡献可忽略不计，即$Q_0^{(t)} = 0$。可推导$e_1$和$e_2$的上限分别为：

$$e_1 \leqslant \frac{(1+u)^2 E_u^{(t)}Q_u^{(t)}}{Y_1\eta_{\mathrm{A}}u} \tag{14}$$

$$e_2 \leqslant \frac{(1+u)E_u^{(t)}Q_u^{(t)}}{Y_2[1-(1-\eta_{\mathrm{A}})^2]\left(\dfrac{u}{1+u}\right)^2} \tag{15}$$

2　数值仿真

在实际QKD系统通信中，为方便Alice端的探测，T模式的波长一般选择为800 nm；S模式要在光纤上进行传输，波长一般选择为1 550 nm。

本文设置信道模型如下：光纤传输效率取$t_{\mathrm{AB}}=10^{-\alpha l/10}$；$\alpha$(dB/km)为光纤传输损耗系数；$l$(km)为传输距离；$\eta_{\mathrm{B}}$为Bob探测器的探测效率，则Alice和Bob之间总的传输效率为$\eta=t_{\mathrm{AB}}\eta_{\mathrm{B}}$。$Y_n=d_{\mathrm{B}}+1-(1-\eta)^n$，$d_{\mathrm{B}}$为Bob端探测器的暗计数率。$e_n=\{e_0Y_0+e_d[1-(1-\eta)^n]\}/Y_n$，其中$e_d$是光子击中错误的探测器的概率，一般情况下为常数。本文采用的实验参数主要来自GYS实验[11]：a=0.21dB/km，$d_{\mathrm{A}}=10^{-6}$，η_{A}=0.3，$d_{\mathrm{B}}=1.7\times10^{-6}$，$\eta_{\mathrm{B}}$=0.045，$e_d$=0.033，$f$=1.22。

以下仿真匀根据传输距离选取最优信号态平均光子数u，v = min{au/(1+u–au)，bu/(1+u–bu)}，因为u和v的值匀为独立选取，所以在实验中，以上关系很容易满足。

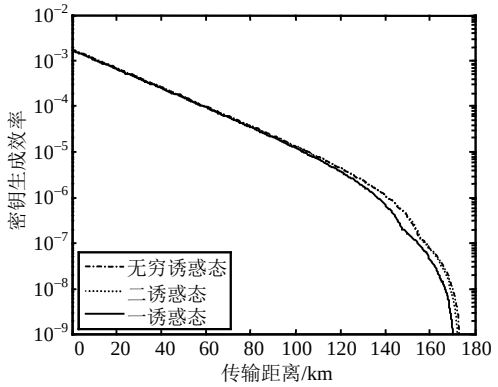

图1　不同诱惑态方案的密钥生成效率比较

从图1可以看出，一诱惑态方案的安全传输距离比无穷诱惑态的理论极限值约小2.2 km，比二诱惑态方案约小1.2 km，差别很小；另一诱惑态方案的密钥生成效率稍低于二诱惑态方案，这是因为一诱惑态方案采用的诱惑态数目比二诱惑态方案少，所以得到的参数估计值没有二诱惑态方案的精确，导致性能的下降，但是一诱惑态方案实现更为容易。图中曲线对于无穷诱惑态方案和二诱惑态方案，大约在156 km处有一个拐点；对于一诱惑态方案，大约在147 km处有一个拐点。这是因为在这之前，未响应集合的参与提高了密钥生成效率。在大于这个距离之后，未响应集合产生密钥的作用消失。

从图2可以看出，当传输距离小于107 km时，一诱惑态方案与二诱惑态方案的密钥生成效率比值达90%以上；当传输距离小于126 km时，密钥生成效率比值达80%以上。所以在近距离传输时，QKD可以选择一诱惑态方案，该方案既可以获得较高的密钥生成效率，又能降低实际实现的难度。在图1中，因为两个诱惑态方案的密钥生成效率曲线的拐点位置不同，所以图2中的比值曲线产生了两个拐点。

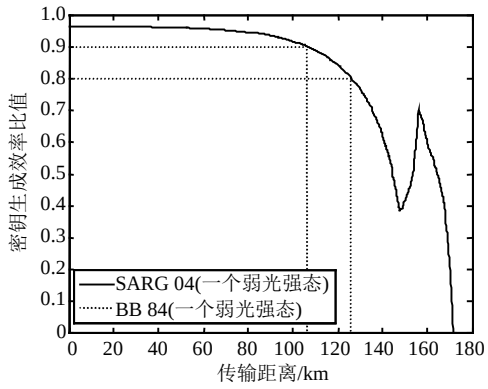

图2 一诱惑态方案与二诱惑态方案的密钥生成效率的比值曲线

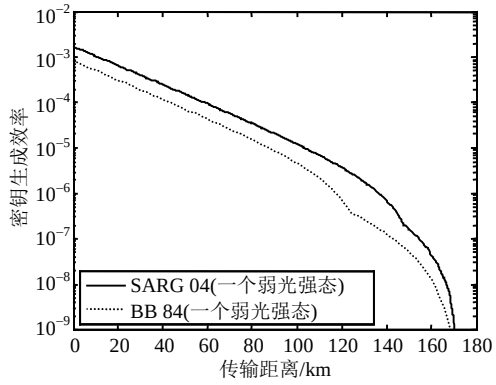

图3 SARG 04诱惑态方案和BB 84诱惑态方案的密钥生成效率比较

图3中SARG 04协议和BB84协议都只采用一个诱惑态，即实际操作难易程度相当。虽然SARG 04一诱惑态方案的性能相比于二诱惑态方案有所下降，但是依然能获得高于BB 84诱惑态方案的密钥生成效率。这是因为虽然HSPS产生的信号中多光子脉冲所占比例要大于WCP光源，会导致密钥生成效率降低，但是SARG 04协议允许2-光子脉冲参与密钥生成，弥补了HSPS的这一缺陷。

3 结 论

为了降低SARG 04诱惑态方案的实现难度，克服激光器不能做到完全消光的问题，本文基于HSPS，将主动诱惑态方案和被动诱惑态相结合，提出只采用一个诱惑态的方案。仿真表明，相比已提出的三诱惑态方案和二诱惑态方案，SARG 04一诱惑态方案虽然性能有所下降，但是依然能获得高于BB 84诱惑态方案的密钥生成效率，因此一诱惑态方案是一种简单有效的量子密钥分配方案。本文的研究为QKD系统选择有效的通信协议和方案提供了理论参考依据。

参 考 文 献

[1] BENNETT C H , BRASSARD G. Quantum cryptography: public key distribution and coin tossing[C]//IEEE Conference on Computers, Systems and Signal Processing. India: IEEE Pree, 1984: 175- 179.

[2] WANG X B. Beating the photon-number-splitting attack in practical quantum cryptography[J]. Phys Rev Lett, 2005, 94: 230503.

[3] HWANG W Y. Quantum key distribution with high loss: toward global secure communication[J]. Phys Rev Lett, 2003, 91: 057901.

[4] MA X F, LO H K. Quantum key distribution with triggering parametric down-conversion sources[J]. New Journal of Physics, 2008, 10: 073018.

[5] MI J L, WANG F Q, LIN Q Q, et al. Practical non-orthogonal decoy state quantum key distribution with heralded single photon source[J]. Chin Phys B, 2008, 17: 1178-1183.

[6] WANG Q, WANG X B, BJÖRK G, et al. Improved practical decoy state method in quantum key distribution with parametric down-conversion source[J]. A Lett Journal Exploring, 2007, 79: 40001.

[7] WANG Q, WEI C, XAVIER G, et al. Experimental decoy-state quantum key distribution with a sub-poissionian heralded single-photon source[J]. Phys Rev Lett, 2008, 100: 090501.

[8] ADACHI Y, YAMAMOTO T, KOASHI M, et al. Simple and efficient quantum key distribution with parametric down-conversion [J]. Phys Rev Lett, 2007, 99: 180503.

[9] SCARANI V, ACIN A, RIBORDY G, et al. Quantum cryptography protocols Robust against photon number splitting attacks for weak laser pulse implementations[J]. Phys Rev Lett, 2004, 92: 057901.

[10] GOTTESMAN D, LO H K, LÜTKENHAUS N, et al. Security of quantum key distribution with imperfect devices[J]. Quantum Inform Comput, 2004, 4: 325-360.

[11] GOBBY C, YUAN Z L, SHIELDS A J. Quantum key distribution over 122 km of standard telecom fiber[J]. Phys Rew Lett , 2004, 84: 3762.

编 辑 张 俊