第 58 卷 第 4 期 2009 年 4 月
1000-3290/2009/58(04)/2189-04

物 理 学 报
ACTA PHYSICA SINICA

Vol.58,No.4,April,2009


# 基于伪态协议的量子密钥分配系统研究*

焦荣珍† 张文翰

(北京邮电大学理学院,北京 100876)

(2008 年 8 月 3 日收到;2008 年 9 月 10 日收到修改稿)

采用包含两个伪态和一个信号态的双伪态协议分析了量子密钥分配系统的性能,比较了双伪态(真空态—弱伪态)和单伪态协议条件下密钥生成率与通信距离的关系,分析了信号态的强度、量子比特误码率、单光子的增益和单光子的误码率对系统密钥生成率的影响,得出密钥生成率的最优化条件,为实现实用安全的量子密钥分配系统奠定理论基础.

关键词:伪态协议,量子密钥生成率,量子比特误码率

PACC:0367,4250

## 1. 引 言

量子保密通信是量子信息科学中的重要分支,量子保密通信以其优越的先天特点有可能改变未来的保密通信方式,近年来已成为国内外的热门研究领域[1—3].量子保密通信的关键在于量子密钥分配(QKD),QKD 能让通信双方(Alice 和 Bob)共享一个无条件安全密钥,因为量子机制就能保证安全,密钥能被用来一次性的加密和解密消息.当前,量子密码研究的核心内容,是如何利用量子技术在量子信道上安全可靠地分配密钥,利用各种协议来抵御外界的攻击,实现系统的绝对安全.因此,研究低误码率和长距离安全的 QKD 系统已成为量子保密通信走向实用化的关键.2004 年,世界上第一个量子密码通信网络在美国剑桥城正式投入运行;2006 年,多个研究小组合作实现了在自由空间 144 km 的 QKD 实验.在国内,中国科学院和华东师范大学等单位也相继实现了远距离的 QKD 实验[4,5].针对实用的 QKD 系统一般是基于弱相干光源,这给了窃听者 Eve 进攻的机会,因此提供安全的 QKD 已成为物理学界和密码学界关注的一个热点.本文利用两个伪态和一个信号态来分析一般情况下双伪态协议的安全性,比较了双伪态协议和单伪态协议条件下,量子密钥生成率和通信距离的关系,分析了信号态强度、量子比特误码率和单光子的增益及误码率对量子密钥生成率的影响.

## 2. 理论和计算公式

在量子保密通信中,最常见的 QKD 协议有:BB84,BBM92 和相关粒子协议[6—8].伪态协议[9]是以 BB84 协议为基础,针对窃听者的光子数分裂攻击的协议:发送方 Alice 准备一系列附加的伪态脉冲,这些伪态用来检测 Eve 的攻击;当 Alice 和 Bob 在量子通信阶段结束后,通过利用检测到的伪态脉冲结果来估算信号光中单光子计数率的下限和单光子所引起误码率的上限,来判断通信的安全性.在基于光纤的 QKD 系统中,设激光源发出弱相干光脉冲,每个脉冲的相位是随机的,且其光子由 Alice 发出,光子数目 $\mu$ 符合泊松分布;量子信道的损耗可以通过损耗系数 $\alpha$(单位为 dB/km)和光纤长度 $l$(单位为 km)得到.信道传输系数 $t_{AB}$ 可由下式表示:

$$t_{AB} = 10^{-\alpha l/10}. \tag{1}$$

Alice 与 Bob 之间的总传输和检测效率 $\eta$ 为

$$\eta = t_{AB} t_B \eta_D, \tag{2}$$

其中 $t_B$ 和 $\eta_D$ 分别为 Bob 端的光组件的内部传输系数和检测器效率.

在 Bob 端设置一个阈值检测器,假定此检测器可以从非真空态中识别出真空态,则在此阈值检测

* 北京市共建基金(批准号:XK100130837)资助的课题.

† E-mail:jrz218@163.com

器下光子 $i$ 的传输系数 $\eta_i$ 为：

$$\eta_i = 1 - (1 - \eta)^i \quad (i = 0,1,2,\cdots). \tag{3}$$

光子 $i$ 由 Alice 发送并被 Bob 接收到这一检测事件的计数率 $Y_i$ 为：

$$Y_i = Y_0 + \eta_i, \tag{4}$$

其中 $Y_0$ 为背景比.光子 $i$ 的增益 $Q_i$ 为：

$$Q_i = Y_i \frac{\mu^i}{i!}e^{-\mu}. \tag{5}$$

总增益 $Q_\mu$ 为

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!}e^{-\mu}. \tag{6}$$

光子 $i$ 的误码率 $e_i$ 为

$$e_i = \frac{e_0 Y_0 + e_d \eta_i}{Y_i}. \tag{7}$$

则总的量子比特误码率(QBER)为

$$E_\mu = \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!}e^{-\mu}, \tag{8}$$

其中 $e_d$ 为光子误击中检测器的概率，$e_0 = 1/2$ 为背景的误码率.

假设 Alice 和 Bob 根据所需要的光子数选择出两个伪态 $v_1$ 和 $v_2$，并满足：$0 \leqslant v_2 \leqslant v_1$，$v_1 + v_2 < \mu$ 则有 $Y_1$ 的下限

$$Y_1 \geqslant Y_1^{L,v_1,v_2} = \frac{\mu}{\mu v_1 - \mu v_2 - v_1^2 + v_2^2} \times \left(Q_{v_1}e^{v_1} - Q_{v_2}e^{v_2} - \frac{v_1^2 - v_2^2}{\mu^2}(Q_\mu e^\mu - Y_0^L)\right).$$

$$Y_0^L = \mathrm{Max}\left\{\frac{v_1 Q_{v_2} e^{v_2} - v_2 Q_{v_1} e^{v_1}}{v_1 - v_2}, 0\right\}. \tag{9}$$

单光子增益 $Q_1$ 为

$$Q_1 \geqslant Q_1^{L,v_1,v_2} = \mu e^{-\mu} Y_1^{L,v_1,v_2}. \tag{10}$$

$e_1$ 的上限为

$$e_1 \leqslant e_1^{U,v_1,v_2} = \frac{E_{v_1} Q_{v_1} e^{v_1} - E_{v_2} Q_{v_2} e^{v_2}}{(v_1 - v_2) Y_1^{L,v_1,v_2}}. \tag{11}$$

双伪态协议的密钥生成率为

$$R = \frac{1}{2}\{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - H_2(e_1)]\} \tag{12}$$

在双伪态的特例：在真空-弱伪态中，Alice 切断光子源来形成真空伪态，对于这一双伪态的特例 $Q_v = Y_0$.

由于暗计数是随机形成的，所以有 $E_v = e_0 = \frac{1}{2}$.

对于弱伪态，即 Alice 和 Bob 选择一个与所需光子数目 $v < \mu$ 相关的弱光强态.

$$Y_1 \geqslant Y_1^{L,v,0} = \frac{\mu}{\mu v - v^2}\left(Q_v e^v - Q_\mu e^\mu \frac{v^2}{\mu^2} - \frac{\mu^2 - v^2}{\mu^2} Y_0\right), \tag{13}$$

$e_1$ 上限为

$$e_1 \leqslant e_1^{U,v,0} = \frac{E_v Q_v e^v - e_0 Y_0}{Y_1^{L,v,0} v} \tag{14}$$

对于单伪态，$Y_1$ 的下限为

$$Y_1 \geqslant Y_1^{L,v} = \frac{\mu}{\mu v - v^2}\left(Q_v e^v - Q_\mu e^\mu \frac{v^2}{\mu^2} - E_\mu Q_\mu e^\mu \frac{\mu^2 - v^2}{e_0 \mu^2}\right), \tag{15}$$

$e_1$ 的上限为

$$e_1 \leqslant e_1^{U,v} = \frac{E_\mu Q_\mu e^\mu}{Y_1^{L,\mu,0}\mu}. \tag{16}$$

## 3. 结果与讨论

通过计算双伪态和单伪态协议中量子比特误码率、单光子的增益、单光子计数率 $Y_1$ 的下限和单光子所引起误码率 $e_1$ 的上限，得出量子密钥生成率随安全通信距离的变化关系如图 1(a)和(b)所示：在图 1(a)中比较了真空-弱伪态和 Wang[10] 等人采用 GLLP 协议计算的结果，同时我们考虑了在双伪态一般条件下，当 $v_1 \to 0$，$v_2 \to 0$ 条件下的渐近结果.在图 1(b)中比较双伪态当 $v_1 \to 0$，$v_2 \to 0$ 条件下的渐近情况、真空-弱伪态和单伪态的量子密钥生成率随安全通信距离的变化关系.

在计算过程中，量子信道的损耗系数 $\alpha = 0.21$ dB/km，$\mu = 0.48$，同时假定背景计数与信号光子检测器无关，且 $Y_0$ 和 $\eta$ 都很小；从理论推导可得出，在相同条件下，$(v_1 + v_2)$ 越小，量子密钥生成率越高，所以当 $v_1 < \mu$，取 $v_2 = 0$ 将使密钥生成率最优.

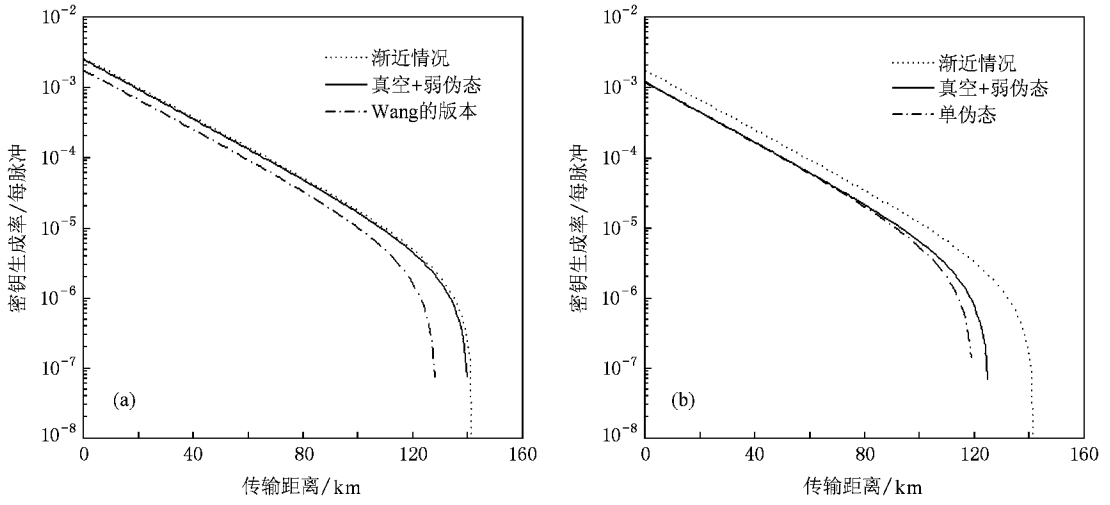


**图 1　量子密钥生成率随安全通信距离的变化关系　(a) Wang 的版本比较结果；(b) 单伪志比较结果**


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

[2] Jiao R Z, Feng C X 2008 *Acta Phys. Sin.* **57** 685 (in Chinese) [焦荣珍、冯晨旭 2008 物理学报 **57** 685]

[3] Liu Y M, Yu Z Y, Yang H B 2006 *Acta Phys. Sin.* **55** 5023 (in Chinese) [刘玉敏、俞重远、杨红波 2006 物理学报 **55** 5023]

[4] Mao E L, Mo X F, Gui Y Z, Han Z F, Guo G C 2004 *Acta Phys. Sin.* **53** 2126 (in Chinese) [苗二龙、莫小范、桂有珍、韩正甫、郭光灿 2004 物理学报 **53** 2126]

[5] Chen J, Li Y, Wu G, Zeng H P 2007 *Acta Phys. Sin.* **56** 5243 (in Chinese) [陈　杰、黎　遥、吴　光、曾和平 2007 物理学报 **56** 5243]

[6] Bennet C H, Brassard G 1984 *Proc. IEEE Int. Conf. Computers, Systems Signal Processing* (Bangalore, New York: IEEE)

[7] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[8] Inoue K, Waks E, Yamamoto Y 2003 *Phys. Rev.* A **68** 022317

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

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

# Analysis of decoy state quantum-key-distribution system *

Jiao Rong-Zhen† Zhang Wen-Han

(*Science School of Beijing University of Post and Telecommunication, Beijing* 100876, *China*)

(Received 3 August 2008; revised manuscript received 10 September 2008)

Abstract

The security of quantum-key-distribution system is analyzed using the decoy state protocol with two weak decoy states and one signal state. The comparison is based on the key generation rate as a function of distance for two types of decoy states: the vacuum and a weak decoy state, asymptotically approaching the theoretical limit of the most general type of decoy protocol, one-decoy-state protocol. We studied the two-decoy-state protocol in connection with the intensity of signal state, and the gain of signal states, the overall quantum bit error rate, the gain of single-photon states and the error rate of single-photon states and arrived at the optimal condition which maximizes the key generation rate.

**Keywords**: decoy state protocol, quantum key generation rate, quantum bit error rate

**PACC**: 0367, 4250

* Project supported by the Corporate Building Project of Beijing Educational Committee, China (Grant No. XK100130837).

† E-mail: jrz218@163.com