

泊松分布单光子源的光束分离器窃听模型

张成龙¹, 张存华², 姬广举¹, 王振华¹, 李瑞²,
杨玉强¹, 都文和³, 张光宇¹

(1. 哈尔滨理工大学 应用科学学院, 黑龙江 哈尔滨 150080; 2. 齐齐哈尔大学 理学院, 黑龙江 齐齐哈尔 161006;
3. 齐齐哈尔大学 通信与电子工程学院, 黑龙江 齐齐哈尔 161006)

摘要: 针对低轨卫星-地面站间量子密钥分配的光束分离器窃听问题, 分析了泊松分布单光子源, 建立了量子比特率理论模型, 给出了光束分离器窃听中窃听率的表达式. 从而分析了低轨卫星-地面站间量子密钥分配的光束分离器窃听问题. 结果表明, 对于低轨卫星-地面站间链路, 每个脉冲平均光子数可以取最优值, 窃听率在 10^{-4} 量级. 通过数据纠错和保密加强, 可以使得窃听者所获得的密钥信息量降低到1比特以下. 这说明, 在低轨卫星-地面站间进行量子密钥分配是可行的, 在保证系统具有很高量子比特率的同时, 量子密钥分配仍然是安全的.

关键词: 量子密钥分配; 窃听; 泊松分布单光子源; 光束分离器

DOI: 10.15938/j.jhust.2015.01.020

中图分类号: O431.2 文献标志码: A 文章编号: 1007-2683(2015)01-0100-05

Beam Splitter Eavesdropping Model Based on Single-photon Sources with Poisson Distribution

ZHANG Cheng-long¹, ZHANG Cun-hua², JI Guang-ju¹, WANG Zhen-hua¹, LI Rui²,
YANG Yu-qiang¹, DU Wen-he³, ZHANG Guang-yu¹

(1. School of Applied Sciences, Harbin University of Science and Technology, Harbin 150080, China; 2. College of Science, Qiqihar University, Qiqihar 161006, China; 3. Communications and Electronic Engineering Institute, Qiqihar University, Qiqihar 161006, China)

Abstract: In order to avoid beam splitter (BS) eavesdropping problem during quantum key distribution between a ground station and a satellite in a low earth orbit, the single-photon sources with Poisson distribution are analyzed, the theoretical model of quantum bit rate is established and the expression of eavesdropping ratio in BS eavesdropping is given. The BS eavesdropping is analyzed for quantum key distribution between a ground station and a satellite in a low earth orbit. The results show that mean photon number per pulse can be optimized and that eavesdropping ratio is on the order of 10^{-4} , and by error detection and privacy amplification, the information gained by an eavesdropper can be reduced to less than 1 bit. This means that it is feasible to implement quantum key distribution between a ground station and a satellite in a low earth orbit. Security can be guaranteed in a high quantum bit exchanging rate system.

Key words: quantum key distribution; eavesdropping; single-photon sources with Poisson distribution; beam splitter

收稿日期: 2014-03-26

基金项目: 黑龙江省教育厅科学技术研究项目(12511119).

作者简介: 张成龙(1989—), 男, 硕士研究生;

张存华(1969—), 男, 硕士, 副教授.

通讯作者: 张光宇(1971—), 男, 博士, 教授, Email: gyzhang@hrbust.edu.cn.

0 引言

量子密码术,确切地说是量子密钥分配,采用单光子通信技术,通信双方 Alice 和 Bob 通过经典信道和量子信道分配密钥. 根据量子力学的不确定原理和量子不可克隆原理,任何窃听者 Eve 的存在都会被发现,从而保证密钥的绝对安全,也就保证了加密信息的绝对安全. 量子密码术在理论上具有绝对安全性,这是基于理想单光子源和无噪声的量子信道. 但对于实际量子密钥分配系统而言,由于量子信道噪声和窃听者的存在,为了产生安全的量子密钥,需要增加一些非量子过程. 一般来说,量子密钥分配需要完成 5 个过程: 身份认证、单光子传输、数据筛选、数据纠错和保密加强.

目前,空间量子密钥分配研究主要集中在地面点对点大气光路量子密钥分配实验^[1-11]和星地量子密钥分配的可行性分析^[12-18]. 在已经进行的基于偏振编码的自由空间量子密钥分配实验中,单光子源采用具有泊松分布的高度衰减激光脉冲,量子密钥分配协议采用 BB84 协议^[19],量子信息态采用单光子偏振态,链路距离达到 144 km. 由于大气湍流的影响和地球表面的弯曲,100 km 量级的链路距离是地面点对点量子密钥分配的瓶颈. 为了实现全球任意两点间保密通信,需要通过卫星进行量子密钥分配. 目前,卫星量子密钥分配的可行性论证正在进行,一旦实验取得成功,人们就可以通过卫星实现迄今最安全的全球通信. 已有实验表明,目前实验链路距离大气湍流的影响已经超过了或相当于星地链路大气湍流的影响,这为实现星地量子密钥分配技术提供了重要的实验依据,也使得星地量子密钥分配的实现成为了可能.

对于实际量子密钥分配系统而言,信道安全是非常重要的,需要考虑窃听问题^[20]. 一般来说,窃听者的窃听策略有两类: 主动窃听和被动窃听. 由于单光子源采用具有泊松分布的高度衰减激光脉冲,多光子脉冲的存在为信道安全带来了隐患. 窃听者可以采用光束分离器 (beam splitter, BS) 攻击量子信道,对多光子脉冲中的光子进行量子测量,而对量子密钥分配不产生影响. 因此,在实际量子密钥分配中,需要考虑光束分离器窃听问题,对窃听者能够获得的量子密钥信息量进行估价,从而为保密加强提供阈值,以保证量子密钥分配的绝对安全.

本文基于泊松分布单光子源,建立了光束分离

器窃听理论模型,给出了安全率和窃听率的表达式,分析了低轨卫星-地面站间量子密钥分配的光束分离器窃听问题.

1 理论模型

1.1 安全率

在实际量子密钥分配中,单光子源通常采用高度衰减激光脉冲即弱激光脉冲. 这样的光脉冲不是单光子数态而基本上是相干态,即光子不是一个个等间距地分布而是服从泊松分布,这样就可能出现一个脉冲含有一个以上光子的情况. 为了得到单光子数态,采用具有极低平均光子数 μ 的相干态来近似单光子数态. 在这样一个相干态中找到 n 个光子概率的泊松分布为

$$P(n, \mu) = \frac{\mu^n}{n!} \exp(-\mu) \quad (1)$$

根据式 (1), 单光子脉冲出现的概率为

$$P(1, \mu) = \mu \exp(-\mu) \quad (2)$$

多光子脉冲出现的概率即安全损耗为

$$P(n \geq 2, \mu) = 1 - P(0, \mu) - P(1, \mu) = 1 - (1 + \mu) \exp(-\mu) \quad (3)$$

安全率定义为: 单光子脉冲出现的概率与多光子脉冲出现的概率的比值, 记为 S , 其表达式为

$$S = \frac{P(1, \mu)}{P(n \geq 2, \mu)} = \frac{\mu \exp(-\mu)}{1 - (1 + \mu) \exp(-\mu)} \quad (4)$$

图 1、图 2 和图 3 分别给出了泊松分布安全损耗和安全率随每个脉冲平均光子数变化曲线, 可以看出, 当 $\mu = 1$ 时单光子脉冲出现的概率最大, 达到 37%, 多光子脉冲出现的概率为 26%, 这不满足单光子数态的要求. μ 值越小, 多光子脉冲出现的概率越小, 安全率越高. 因此, 为了达到单光子数态的要求, 必须使得 $\mu < 1$. 但当 $\mu \rightarrow 0$ 时, 空脉冲出现的概率趋近于 100%. 这就需要对 μ 值进行优化选择. 如果要求安全率大于 20, 那么就需要 $\mu < 0.1$. 如果光源为理想单光子源, 即每个脉冲有且只有一个光子, 那么安全率将无限高

1.2 窃听率

假设单光子沿光链路的传输或反射服从二项分布, 则接收机至少探测到一个光子的概率可以表示为

$$P_{n \geq 1} = \sum_{k=1}^n C_n^k (T_{\text{cha}} P_{\text{acq}} T_{\text{app}} \eta_{\text{det}} F_{\text{mea}})^k \cdot (1 - T_{\text{cha}} P_{\text{acq}} T_{\text{app}} \eta_{\text{det}} F_{\text{mea}})^{n-k} =$$

$$1 - (1 - T_{\text{cha}} P_{\text{acq}} T_{\text{app}} \eta_{\text{det}} F_{\text{mea}})^n \quad (5)$$

式中; T_{cha} 为量子信道传输率; P_{acq} 为单光子捕获概率; T_{app} 为系统装置传输率; η_{det} 为单光子探测器的量子效率; F_{mea} 为量子测量因子.

量子信道效率定义为: 发射机的弱激光脉冲中光子分布的泊松概率与接收机至少探测到一个光子概率的内积, 即

$$P_{\text{cha}} = \sum_{n=1}^{\infty} P(n, \mu) P_{n \geq 1} = \sum_{n=1}^{\infty} \frac{\mu^n}{n!} \exp(-\mu) [1 - (1 - T_{\text{cha}} P_{\text{acq}} T_{\text{app}} \eta_{\text{det}} F_{\text{mea}})^n] = 1 - \exp(-\mu T_{\text{cha}} P_{\text{acq}} T_{\text{app}} \eta_{\text{det}} F_{\text{mea}}) \quad (6)$$

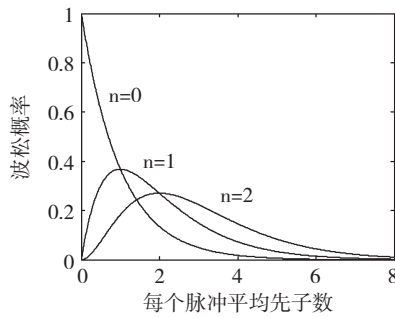


图1 泊松概率随平均光子数变化曲线

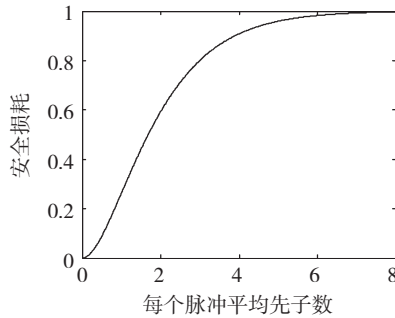


图2 安全损耗随平均光子数变化曲线

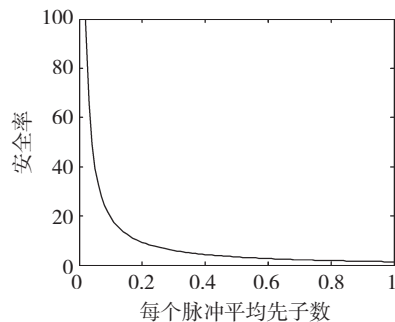


图3 安全率随平均光子数变化曲线

在量子密钥分配中, 单光子源采用具有泊松分布的高度衰减激光脉冲, 窃听者采用光束分离器攻

击量子信道. 在光束分离器攻击中, 窃听者接收二项反射概率, 接收机接收二项传输概率. 光束分离器窃听原理如图4所示.

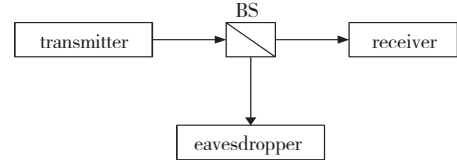


图4 光束分离器窃听原理

设光束分离器的传输率为 T_{BS} , 反射率为 R_{BS} , 且 $T_{\text{BS}} + R_{\text{BS}} = 1$. 由于窃听者和接收机的量子信道效率是相互独立的, 所以有

$$P_{\text{cha}}^{\text{B}} = 1 - \exp(-\mu T_{\text{cha}}^{\text{B}} P_{\text{acq}}^{\text{B}} T_{\text{app}}^{\text{B}} \eta_{\text{det}}^{\text{B}} F_{\text{mea}}^{\text{B}} T_{\text{BS}}) \quad (7)$$

$$P_{\text{cha}}^{\text{E}} = 1 - \exp(-\mu T_{\text{cha}}^{\text{E}} P_{\text{acq}}^{\text{E}} T_{\text{app}}^{\text{E}} \eta_{\text{det}}^{\text{E}} F_{\text{mea}}^{\text{E}} R_{\text{BS}}) \quad (8)$$

令

$$\eta_{\text{B}} = T_{\text{cha}}^{\text{B}} P_{\text{acq}}^{\text{B}} T_{\text{app}}^{\text{B}} \eta_{\text{det}}^{\text{B}} F_{\text{mea}}^{\text{B}} \quad (9)$$

$$\eta_{\text{E}} = T_{\text{cha}}^{\text{E}} P_{\text{acq}}^{\text{E}} T_{\text{app}}^{\text{E}} \eta_{\text{det}}^{\text{E}} F_{\text{mea}}^{\text{E}} \quad (10)$$

则式(7)和式(8)变为

$$P_{\text{cha}}^{\text{B}} = 1 - \exp(-\mu \eta_{\text{B}} T_{\text{BS}}) \quad (11)$$

$$P_{\text{cha}}^{\text{E}} = 1 - \exp(-\mu \eta_{\text{E}} R_{\text{BS}}) \quad (12)$$

窃听率定义为: 窃听者所占有的发射机和接收机密钥信息的百分比, 即窃听者和接收机共享比特数与发射机和接收机共享比特数的比率. 如果在一个脉冲中只有一个光子, 那么这个光子或者被窃听者接收到, 或者被接收机接收到, 但不能被二者都接收到. 基于这个假设, 窃听者和接收机共享比特概率可表示为

$$P_{\text{B} \wedge \text{E}} = \sum_{n=2}^{\infty} \frac{\mu^n}{n!} \exp(-\mu) \sum_{k=1}^{n-1} C_n^k T_{\text{BS}}^k R_{\text{BS}}^{n-k} [(1 - \eta_{\text{B}})^k] [1 - (1 - \eta_{\text{E}})^{n-k}] \quad (13)$$

窃听率可表示为

$$E = \frac{\sum_{n=2}^{\infty} \frac{\mu^n}{n!} \exp(-\mu) \sum_{k=1}^{n-1} C_n^k T_{\text{BS}}^k R_{\text{BS}}^{n-k} [(1 - \eta_{\text{B}})^k] [1 - (1 - \eta_{\text{E}})^{n-k}]}{1 - \exp(-\mu \eta_{\text{B}} T_{\text{BS}})} \quad (14)$$

2 数值计算

下面考虑低轨卫星-地面站间量子密钥分配的光束分离器窃听问题. 这里, 假设窃听者和接收机具有相同的量子密钥分配系统. 系统参数分别为:

$$T_{\text{cha}}^{\text{B}} = T_{\text{cha}}^{\text{E}} = 80\%, P_{\text{acq}}^{\text{B}} = P_{\text{acq}}^{\text{E}} = 10^{-3}, T_{\text{app}}^{\text{B}} = T_{\text{app}}^{\text{E}} = 1, \eta_{\text{det}}^{\text{B}} = \eta_{\text{det}}^{\text{E}} = 65\%, F_{\text{mea}}^{\text{B}} = F_{\text{mea}}^{\text{E}} = 1.$$

图5为窃听者采用50/50 BS时窃听者和接收

机共享比特概率随平均光子数变化曲线. 可以看出, 当 $0 < \mu \leq 1$ 时, 共享比特概率在 10^{-8} 量级. 如果发射机脉冲重复率为 1 MHz, 那么窃听者和接收机共享比特率只有 10^{-2} Hz 的量级. 图 6 为窃听者采用 50/50BS 时窃听率随平均光子数变化曲线. 可以看出, 窃听率随着平均光子数的增加而增加. 当 $\mu = 1$ 时, 窃听率约为 2.6×10^{-4} , 这意味着在发射机和接收机所分享的 10 000 比特密钥中, 窃听者分享的密钥信息还不到 3 比特. 因此, 对于低轨卫星-地面站间量子密钥分配, 可以将平均光子数取为 1, 这时单光子脉冲出现的概率最大, 量子比特率最高. 虽然 $\mu = 1$ 时, 安全率降低为 1.4, 但窃听率更低, 只有 10^{-4} 量级. 通过数据纠错和保密加强, 可以使得窃听者所获得的密钥信息量降低到 1 比特以下.

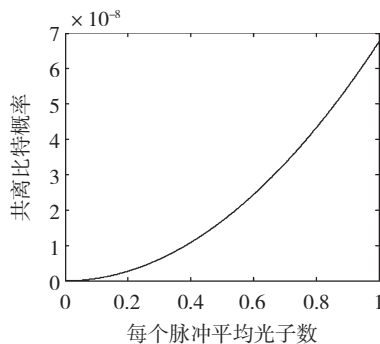


图 5 共享比特概率随平均光子数变化曲线

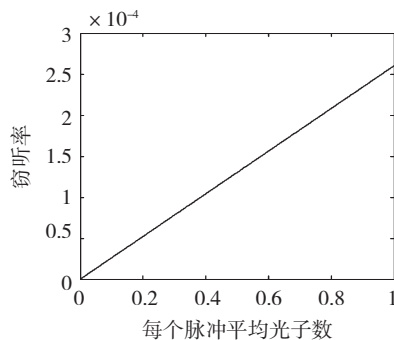


图 6 窃听率随平均光子数变化曲线

图 7 为 $\mu = 1$ 时窃听者和接收机共享比特概率随 BS 传输率变化曲线. 可以看出, 当 $T_{BS} = 0.5$ 时, 共享比特概率最大, 达到 6.8×10^{-8} . 图 8 为 $\mu = 1$ 时窃听率随 BS 传输率变化曲线. 可以看出, 窃听率随着 BS 传输率的增加而减小.

从上述分析可以看出, 当窃听者采用光束分离器对量子信道进行窃听时, 对于低轨卫星-地面站间量子密钥分配, 光源的每个脉冲平均光子数可以取最优值.

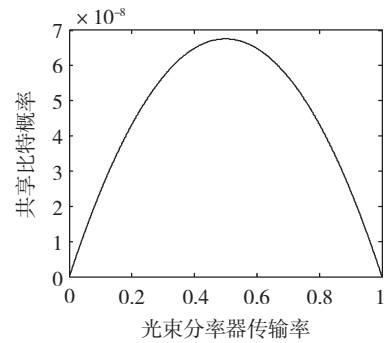


图 7 共享比特概率随 BS 传输率变化曲线

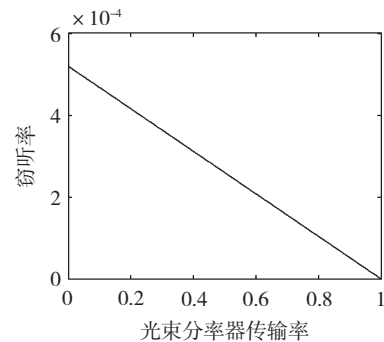


图 8 窃听率随光束分离器传输率变化曲线

3 结 语

本文建立了基于泊松分布单光子源的光束分离器窃听理论模型, 针对低轨卫星-地面站间量子密钥分配的光束分离器窃听进行了数值计算. 结果表明, 当发射机脉冲重复率为 1 MHz 时, 窃听者和接收机共享比特率量级为 10^{-2} Hz. 窃听率随着每个脉冲平均光子数的增加而增加, 随着 BS 传输率的增加而减小. 当 $\mu = 1$ 时窃听率量级为 10^{-4} , 当 $T_{BS} = 0.5$ 时窃听者和接收机共享比特概率量级为 10^{-8} . 理论分析和数值计算表明, 在低轨卫星-地面间能够进行安全的量子密钥分配.

参 考 文 献:

- [1] HUGHES R J, NORDHOLT J E, DERKACS D, et al. Practical Free-space Quantum Key Distribution over 10 km in Daylight and at Night [J]. New Journal of Physics, 2002, 4: 43.
- [2] KURTSIEFER C, ZARDA P, HALDER M, et al. A Step Towards Global Key Distribution [J]. Nature, 2002: 419-450.
- [3] FURST M, WEIER H, SCHMITT-MANDERBACH T, et al. Free-space Quantum Key Distribution over 144 km [J]. Proceedings of SPIE, 2006, 6399: 63990G-1-7.
- [4] SCHMITT-MANDERBACH T, WEIER H, FURST M, et al. Experimental Demonstration of Free-space Decoy-state Quantum Key Distribution over 144 km [J]. Physical Review Letters, 2007, 98,

- 010504 – 1 – 4.
- [5] ASPELMEYER M, BOHM H R, GYATSO T, et al. Long-distance Free-space Distribution of Quantum Entanglement [J]. Science, 2003, 301: 621 – 623.
- [6] PENG C Z, YANG T, BAO X H, et al. Experimental Free-space Distribution of Entangled Photon Pairs over 13 km Towards Satellite-based Global Quantum Communication [J]. Physical Review Letters, 2005, 94(15): 150501 – 1 – 4.
- [7] RESCH K J, LINDENTHAL M, BLAUENSTEINER B, et al. Distributing Entanglement and Single Photons through an Intra-city, Free-space Quantum Channel [J]. Optics Express, 2005, 13(1): 202 – 209.
- [8] MARCIKIC I, LAMAS-LINARES A, KURTSIEFER C. Free-space Quantum Key Distribution with Entangled Photons [J]. Applied Physics Letters, 2006, 89(10): 101122 – 1 – 3.
- [9] WEIHS G, ERVEN C. Entangled Free-space Quantum Key Distribution [J]. Proceedings of SPIE, 2007, 6780: 678013 – 1 – 9.
- [10] URSIN R, TIEFENBACHER F T, SCHMITT-MANDERBACH T, et al. Entanglement-based Quantum Communication over 144 km [J]. Nature Physics, 2007, 3: 481 – 486.
- [11] ZHANG G Y, SONG S Y, LI J L, et al. Free-space Quantum Key Distribution with Polarization Compensation [J]. Journal of Russian Laser Research, 2011, 32(6): 579 – 583.
- [12] NORDHOLT J E, HUGHES R J, MORGAN G L, et al. Present and Future Free-space Quantum Key Distribution [J]. Proceedings of SPIE, 2002, 4635: 116 – 126.
- [13] RARITY J G, TAPSTER P R, GORMAN P M, et al. Ground to Satellite Secure Key Exchange Using Quantum Cryptography [J]. New Journal of Physics, 2002, 82(4): 1 – 82. 21.
- [14] MIAO E L, HAN Z F, GONG S S, et al. Background Noise of Satellite-to-ground Quantum Key Distribution [J]. New Journal of Physics, 2005, 7: 215 – 223.
- [15] VILLORESI P, JENNEWEIN T, TAMBURINI F, et al. Experimental Verification of the Feasibility of a Quantum Channel between Space and Earth [J]. New Journal of Physics, 2008, 10: 033038 – 1 – 12.
- [16] ZHANG G Y, YANG Z, ZHANG C L, et al. Dynamic Polarization-basis Compensation for Free-space Quantum Communications [J]. China Communications, 2013, 10(2): 27 – 32.
- [17] TOYOSHIMA M, TAKENAKA H, SHOJI Y, et al. Polarization-basis Tracking Scheme in Satellite Quantum Key Distribution [J]. International Journal of Optics, 2011, 10: 254154 – 1 – 8.
- [18] BONATO C, ASPELMEYER M, JENNEWEIN T, et al. Influence of Satellite Motion on Polarization Qubits in a Space-Earth Quantum Communication Link [J]. Optics Express, 2006, 14(21): 10050 – 10059.
- [19] BENNETT C H, BRASSARD G. Quantum Cryptography: Public Key Distribution and Coin Tossing [C] // Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India: IEEE, New York, 1984: 175 – 179.
- [20] BUTTLER W T, HUGHES R J, KWIAT P G, et al. Free-space Quantum Key Distribution at Night [J]. Proceedings of SPIE, 1998, 3385: 14 – 22.

(编辑: 温泽宇)