doi:10.3788/gzxb20124103.0339

基于恶意攻击的多用户量子信令损伤模型及诱骗态修复策略

李超[1],聂敏[1],刘晓慧[1,2]

(1 西安邮电学院 通信与信息工程学院,西安 710061)

(2 西安电子科技大学 ISN 国家重点实验室,西安 710071)

摘 要:本文提出了一个多用户量子信令传输系统,并详细阐述了信令在信道中的传输过程.研究了传输过程中信令受到第三方恶意攻击的损伤模型,并将诱骗态的思想引入量子信令安全的直接通信中,分析了采用不同光强来发送光脉冲,以克服光子数分裂攻击的问题,从而提高了信令传输的安全性.仿真结果表明,本文所提出的对多用户信令攻击的修复策略可有效地检测到光子数分裂数攻击,并增加了安全传输距离,从而保证信令传输过程安全有效的进行.

关键词:多用户量子信令;信令传输;安全性;光子数分裂攻击;诱骗态

中图分类号:G301 **文献标识码**:A **文章编号**:1004-4213(2012)03-0339-4

0 引言

随着量子通信的发展,量子保密通信的研究不断发展和壮大,量子密钥分发协议[1-3]也越来越完善,但量子信令传输的安全性尚未有人研究,本文建立了一个多用户量子信令传输、交换模型,并利用量子态的不同偏振方向来承载大量不同的信令消息.并将诱骗态的思想引入量子信令安全的直接通信[4-5],采用不同的强度来发送光脉冲来克服光子数分裂攻击(Photon Number Splitting, PNS)[6],克服了信令在传输距离上的限制,从而提高有效通信安全.

1 多用户量子信令传输交换系统

本文提出了一个多用户量子信令模型,其信令传输交换过程如图 1 所示.

有 1 000 个西安的用户要将其信令消息传输到相应的上海的 1 000 个用户.这 1 000 个信令同时在同一信道上传输,经过西安和上海的两个量子信令交换机,使得最终信令从西安到达上海.如图所示 $n_1,n_2,\cdots n_{1000}$ 为西安的信令输入端,而 $n_1,n_2,\cdots n_{1000}$ 为上海的信令输出端.在量子交换机中,每个用户都有不同的身份编码(ID),主叫用户通过交换机识别被叫用户的编码,完成路由的建立和通信过程.在通常情况下,为了扩大系统的传输容量,采用量子波分系统,即不同用户根据不同的光子频率进行编码和接收信令.所以,接收端根据用户的 ID 号可正确区分用户身份的.

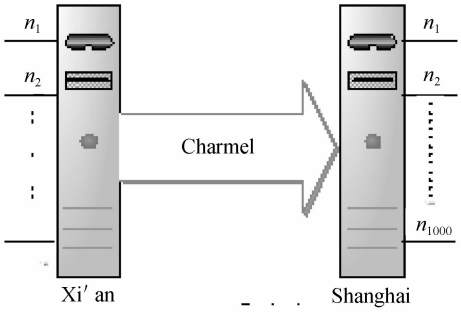

图 1 多用户量子信令传输交换过程

Fig. 1 Multi user quantum signaling transmission and switching process

从西安输入端发送的量子信令形为

$$|\varphi\rangle=a|H\rangle+b|V\rangle \tag{1}$$

式中 a 及 b 均为复数,满足 $|a|^2+|b|^2=1$. H 和 V 为单光子在水平和垂直方向的偏振,且单光子的偏振方向可取水平与垂直之间的任意角度.如图 2 所示,图中圆周的每一点都代表一个量子信令,在偏振方向 45°时其量子信令表示为

$$|\varphi\rangle=\frac{1}{\sqrt{2}}|H\rangle+\frac{1}{\sqrt{2}}|V\rangle \tag{2}$$

a 和 b 均取值 $1/\sqrt{2}$,满足 $|a|^2+|b|^2=1$.如果在垂

基金项目:国家自然科学基金(No. 61172071)、陕西省自然科学基础研究计划(No. 2010JM8021)、陕西省教育厅自然科学研究项目(No. 2010JK834)和西安邮电学院青年教师科研基金(No. ZL2010-05)资助

第一作者(通讯作者):李超(1987—),女,硕士研究生,主要研究方向为量子通信、移动通信. Email: lc32514@163.com

导 师:聂敏(1964—),男,教授,主要研究方向为量子通信、移动通信、现代通信网理论和关键技术. Email: niemin@xupt.edu.cn

收稿日期:2011-11-22;**修回日期**:2012-01-05

直方向进行测量(让单光子通过垂直方向的偏振片)单光子通过的概率为$(1/\sqrt{2})^2=1/2$,通过垂直偏振片后单光子所处的状态就变成了$|V\rangle$不再是原来的45°偏振了,水平方向同样.由于圆周上有无数个点即a和b的取值有无穷多个,所以这1 000个信令以a和b的不同取值来进行区分,只要满足$|a|^2+|b|^2=1$即可.

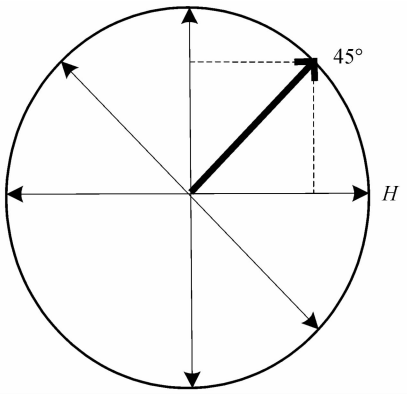

图2 单光子的偏振方向

Fig. 2 Single photon polarization

对于这1 000个信令消息,每一对确定的a和b代表相应的信令,a、b的取值不同对应不同的信令.对于上述多用户信令传输过程,取确定的1 000对a和b来进行信令的区分.为了确保信令的安全性,这1 000对a和b以每秒5000次的频率随机变换,其变换的范围不超出这1 000对取值.传输双方保持频率一致.

2 光子数分裂攻击

理想的单光子源在现实中是很难实现的,对应于一个实际光源往往制备不止一个光子,且这些光子携带相同的信令消息.对于弱激光脉冲光源,光子数分布服从泊松分布

$$P(n)=\mathrm{e}^{-\mu}\frac{\mu^n}{n!} \tag{3}$$

n为光脉冲中的光子数,μ为平均光子数,$P(n)$为n个光子数的光脉冲产生的概率,且$\sum_n P(n)=1$.光源将以$1-P(0)-P(1)$的概率产生多光子脉冲.

光子数分裂攻击(Photon Number Splitting, PNS)的主要思想如图3所示,攻击者Eve将Alice发给Bob的信令截取进行测量,如果光子数为1,则Eve丢弃这个信令消息;如果光子数大于1,则Eve从携带相同信令的多光子中分离出一个留给自己,另一个通过低损耗或无损耗信道发送给Bob,则Eve和Bob获得的信令是完全一致的,且Eve对量子信令的扰动可通过信道噪音或衰减等因素来弥补,使得Bob和Alice觉察不到攻击者Eve的存在.

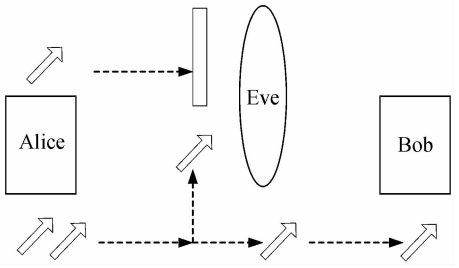

图3 PNS攻击原理图

Fig. 3 PNS attack principle diagram

对于本文提出的多用户量子信令传输交换过程中的攻击为有选择性的攻击,即在1 000个信令中隐藏了一个机密信令,即系数a和b确定的信令$|\bar{\varphi}\rangle=a_1|H\rangle+b_1|V\rangle$.攻击者Eve首先要在这1 000个信令中选取这个机密信令,通过偏振过滤器对其偏振角度即系数进行选定,然后再进行PNS攻击.

3 诱骗态及其修复策略

实验中为了得到近似的单光子源,通常是将相干光源进行衰减[7-8],光子数分布服从泊松分布式(3),光源有如下表达式

$$\rho=\sum_{n=0}^{\infty}p(n)|n\rangle\langle n| \tag{4}$$

$P(n)$为n个光子数的光脉冲产生的概率.

针对在PNS攻击中攻击者Eve对多光子脉冲截取其中一个光子从而得到与接收端相同的信息的做法,以及本文所考虑的多用户信令传输与交换系统.本文诱骗态的核心思想[9-13]为:在西安的发端将真实信令脉冲与诱骗态脉冲以相同的比例发送,诱骗态脉冲和真实信令脉冲的平均光子数不同(信令脉冲平均光子数小于诱骗脉冲,即$\mu_s<\mu_d$),这使得它们的单光子和多光子脉冲的比例相差很大.由于两种光脉冲模式完全一致,Eve无法区分截取到的光脉冲是属于真实信令态还是诱骗态.在量子信令传输之后,接收端通过比较两种脉冲的响应的通过率来检测是否被PNS攻击.如果被PNS攻击,就终止此次信令传输.

对于上述诱骗态方案:真实信令源主要发送单光子脉冲,用于传输信令消息;诱骗源主要发送多光子脉冲,用于探测PNS攻击.

当信令传输过程中没有受到PNS的攻击时,脉冲的通过率为

$$Q_\mu=\sum_n Y_n\rho=Y_0\mathrm{e}^{-\mu}+\sum_{n=1}^{\infty}Y_n\mathrm{e}^{-\mu}\frac{\mu^n}{n!} \tag{5}$$

Y_n是发端发送n光子脉冲时,收端有计数的概率.信道总得传输率为

$$\eta=10^{-\partial L/10}\eta_B \tag{6}$$

∂为信道衰减系数,L为信道的长度,η_B为收端探测

器的效率. 当发端发送 n 光子脉冲时，收端至少可以收到一个光子的概率为

$$t_n=1-(1-\eta)^n \tag{7}$$

所以，计数率可表示为

$$Y_n=t_n+Y_0-t_nY_0\approx t_n+Y_0 \tag{8}$$

所以通过率可化简为

$$Q_\mu=Y_0+1-\mathrm{e}^{-\eta\mu} \tag{9}$$

未受到 PNS 攻击时，信令脉冲的通过率随着通信距离的增加而快速衰减. 而 PNS 攻击的情况下，单光子被攻击者丢弃，而多光子可以到达接收端，且攻击者可通过低损耗信道来弥补通信距离对通过率造成的影响，所以其通过率可保持基本稳定. 当无攻击时通过率衰减到小于等于有攻击时的通过率时，则整个信令传输系统不安全. 这时考虑用主要为多光子脉冲的诱骗态来迷惑攻击者，可延长通信距离，且当诱骗态脉冲通过率远大于信令脉冲通过率时，可判断存在 PNS 攻击. 随着通信距离的增加，诱骗态的通过率越来越低可保证信令传输的安全性. 所以在这里攻击者进行光子数目检测：当多于一个光子时，以概率 P 从其中分离一个，将其余的光子送给收端，以概率 $1-P$ 来阻止多光子脉冲的通过.

对于上述诱骗态方案，发端发送 $n(n\geqslant 2)$ 光子脉冲时，收端有计数的概率为

$$Y_n=p((1-(1-\eta)^{n-1})+Y_0)+(1-P)Y_0=P(1-(1-\eta)^{n-1})+Y_0 \tag{10}$$

此时的通过率为

$$Q'_\mu=Y_0(1+\mu)\mathrm{e}^{-\mu}+\sum_{n=2}^{\infty}Y_n\rho=Y_0(1+\mu)\mathrm{e}^{-\mu}+\sum_{n=2}^{\infty}[P(1-(1-\eta)^{n-1})+Y_0]\mathrm{e}^{-\mu}\frac{\mu^n}{n!}=(Y_0+P-(1+\mu)P\mathrm{e}^{-\mu})-\frac{P\mathrm{e}^{-\mu}}{1-\eta}(\mathrm{e}^{\mu(1-\eta)}-1-\mu+\mu\eta) \tag{11}$$

4　多用户诱骗态协议分析

以上所进行的分析，是针对端到端的情况. 对于多用户诱骗态而言，Eve 对经过其范围内所有信令进行截取，根据不同频率选择 m 个用户进行攻击. 不同的 (a,b) 组合对应不同的频率 f（或波长 λ）如下

$$(a_1,b_1)\rightarrow\lambda_1$$
$$(a_2,b_2)\rightarrow\lambda_2$$
$$\vdots\qquad\vdots$$
$$(a_m,b_m)\rightarrow\lambda_m$$

对于多用户诱骗态协议，每个用户在发端同时发送一个信令态和诱骗态，即每个用户在其可能受到攻击时，使用其相应的诱骗态来检测是否受到 PNS 攻击.

5　仿真分析

信令传输系统受到 PNS 攻击时，在一定的距离范围内（已证实为 33.5 km）是可以根据信令脉冲的通过率来检测是否存在攻击的. 由于信道衰减等因素，信令的通过率随着通信距离的增加而衰减，当其小于等于 PNS 攻击下的通过率时，则通信双方无法检测到 PNS 攻击的存在性，使得信令传输极不安全，在下列仿真中 $\partial=0.2$，$Y_0=10^{-5}$，$\eta_B=0.002$.

图 4 为在本文诱骗态方案下，信令脉冲通过率在无攻击和 PNS 攻击下的对比图. 从图中可看到在 PNS 攻击下，信令脉冲主要为单光子，到达收端的为少数多光子脉冲，所以对通过率影响不大；而未受 PNS 攻击时，随着信道衰减等因素影响，通过率大幅衰减. 由图中可知在 100 km 处两种情况下的通过率相等，即安全通信距离为 100 km，与不使用诱骗态时有大幅提高.

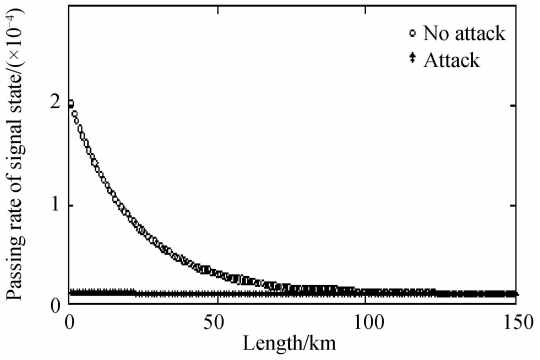

图 4　信令态在无攻击和攻击下的通过率

Fig. 4　Signaling state in the absence of attacks and attacks of pass rates

在 PNS 攻击下信令态中主要为单光子，其在传输过程中被攻击者丢弃，只有少量多光子脉冲可到达收端；而对于主要为多光子脉冲的诱骗态来说，其通过率相对大很多. 所以比较 PNS 攻击下两者的通过率，当诱骗态通过率远远大于信令态时可认为系统不安全. 如图 5 所示，诱骗态通过率要远大于信令态，说明存在 PNS 攻击.

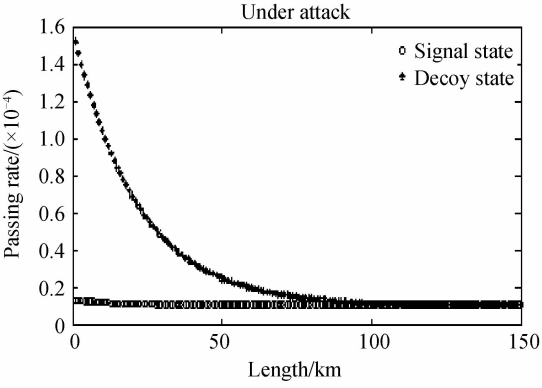

图 5　PNS 攻击下诱骗态与信令态通过率

Fig. 5　The pass rate of decoy state and signal state under PNS attack

6 结论

本文构建了一个多用户量子信令传输、交换系统，并对其安全性进行了分析. 选用不同的偏振角度来标记不同的信令，使得同时可进行多用户的传输. 在传输过程中为了确保其安全性，使得偏振角度以每秒 5000 次的频率进行有规律的变更，降低了被攻击的可能性. 具体对某一用户的信令安全方面，仿真分析及结果表明使用诱骗态方案能有效地检测到光子数分裂攻击的存在，并增加了通信距离，确保信令传输安全有效的进行. 本文的研究为今后量子信令传输安全性的发展可提供必要的技术支持.

参考文献

[1] ZHAO Yi, QI Bing, MA Xiong-feng, *et al*. Experimental quantum key distribution with decoy states[J]. *Physical Review Letters*, 2006, **96**(7): 070502-1-070502-4.

[2] QUAN Dong-xiao, PEI Chang-xing, ZHU Chang-hua, *et al*. New method of decoy state quantum key distribution with a heralded single-photon source[J]. *Acta Physica Sinica*, 2008, **57**(9): 5600-5604.
权东晓，裴昌幸，朱畅华，等. 一种新的预报单光子源诱骗态量子密钥分发方案[J]. 物理学报，2008, **57**(9): 5600-5604.

[3] CHEN Xia, WANG Fa-qiang, LU Yi-qun, *et al*. A differentialphase shift key distribution QKD system combing wit hefficient BB84 scheme[J]. *Acta Photonica Sinca*, 2008, **37**(5): 1052-1056.
陈霞，王发强，路轶群，等. 结合高效 BB84 协议的差分密钥分发系统[J]. 光子学报，2008, **37**(5): 1052-1056.

[4] LIUD, PEI C X, QUAN D X, *et al*. A new quantum secure direct communication scheme with authentication[J]. *Chinese Physics Letters*, 2010, **27**(5): 306

[5] CHEN Zhi-xin, TANG Zhi-lie, LIAO Chang-jun, *et al*. Practical security problem of six states Q KD protocol[J]. *Acta Physica Sinica*, 2006, **35**(1): 126-129.
陈志新，唐志列，廖常俊，等. 实际量子密钥分配扩展 BB84 协议窃听下的安全性分析[J]. 光子学报，2006, **35**(1): 126-129.

[6] BRASSARD G, LÜTKENHAUS N, MOR T, *et al*. Limitations on pratical quantum cryptography[J]. *Physical Review Letters*, 2000, **85**(6): 1330-1333.

[7] MO X F, ZHU B, HAN Z F, *et al*. Faraday-Michelson system for quantum cryptography[J]. *Optics Letters*, 2005, **30**(19): 2632-2634.

[8] YUAN Z L, SHIELDS A J. Continuous operation of a one-way quantum key distribution system over installed telecom fibre[J]. *Optics Express*, 2005, **13**(2): 660-665.

[9] HU J Z, WANG X B. Reexamination of the decoy-state quantum key distribution with an unstable source[J]. *Physical Review A*, 2010, **82**(1): 012331.

[10] WANG X B, PENG C Z, ZHANG J, *et al*. General theory of decoy-state quantum cryp tography with source errors[J]. *Physical Review A*, 2008, **77**(4): 42311.

[11] PENG C Z, ZHANG J, YANG D. Experimental long-distance decoy-state quantum key distribution based on polarization encoding[J]. *Physical Review Letters*, 2007, **98**(1): 10505.

[12] SCHM ITT-MANDERBACH T. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km [J]. *Physical Review Letters*, 2007, **98**(1): 10504.

[13] WANG X B, PENG C Z, PAN J W. Simple protocol for secure decoy-state quantum key distribution with a loosely controlled source[J]. *Applied Physics Letters*, 2007, **90**(3): 031110.

The Damage Model of Quantun Signaling of Multi-user Based on Malicious Attack and Repair Strategy

LI Chao[1], NIE Min[1], LIU Xiao-hui[1,2]

(1 *School of Communication and Information Engineering, Xi'an University of Post and Telecommunication, Xi'an* 710061, *China*)

(2 *State Key Laboratory of ISN, Xidian University, Xi'an* 710071, *China*)

Abstract: A quantum signaling transmission system of multi-user is presented, and the transmission process signaling channel is introduced. The damage model maliciously attacked by the third party is analyzed in the transmission process, and the idea of decoy state is introduced to the safety of quantum signaling in direct communication. To overcome photon number splitting(PNS) attack, light pulses are sent using different light intensities, which also improve the safety of the signal transmission. The simulation result shows that repair strategy of multi-user quantum signaling transmission system being attacked can effective detect the PNS attack, and increase distance of security transmission, to ensure the signaling transmission process safely and effectively.

Key words: Multi-user quantum signaling; Signaling transfer; Security; Photon number splitting attack; Decoy state