一种基于诱骗态的广域量子安全直接通信网络方案*

权东晓，裴昌幸，刘丹，赵楠

（西安电子科技大学 综合业务网国家重点实验室，西安 710071）

摘　要：提出了一种基于诱骗态的广域量子安全直接通信网络方案. 在每一个局域网中设置一个服务器负责量子态的产生和测量，从而提高了通信距离；将诱骗态的思想引入量子安全直接通信，采用不同的强度发送光脉冲，能够克服光子数目分割攻击，从而提高通信的安全性；根据信道参量估计了不同通信距离的通过率，为信道编码提供了依据. 对所提方案进行了安全性分析，结果表明此方案能够实现远距离量子安全直接通信.

关键词：量子安全直接通信；广域网；诱骗态；通过率

中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1004-4213(2009)12-3283-5

0　引言

量子信息科学是量子力学与信息科学相结合的产物，是对未来人类社会产生重大影响的新兴前沿科学. 通过量子密钥分发（Quantum Key Distribution，QKD）[1-8]可以在发送端和接收端协商出绝对安全的量子密钥，从而利用此密钥对信息进行一次一密，就可以通过经典信道进行绝对安全的通信. 近年来量子通信又产生了一个新的分支，量子安全直接通信（Quantum Secure Quantum Communication，QSDC）. 2002 年，Bostrom 和 Felbinger 提出了“ping-pong”协议[9]，利用纠缠对作为信息载体，但是蔡庆雨证明这个协议是不安全的[10]. 2003 年，邓富国等利用块传输的思想，提出了两步的量子安全直接通信方案[11]. 满钟晓等提出了基于纠缠交换的 DSQC（Deterministic Secure Direct Communication）方案[12]. 2007 年，邓富国等又提出了利用单光子实现的经济的量子安全直接通信网络[13].

本文提出了基于诱骗态的广域量子安全直接通信网络，在每一个局域网中设置一个服务器负责量子态的产生和测量，当通信双方位于不同的局域网时，可以缩短光子的传输路径，从而提高通信距离. 由于目前量子通信中多采用弱相干光经过衰减近似代替单光子源，所以就可能存在光子数目分割（Photon Number Splitting，PNS）攻击，本文首次提出加入诱骗态的思想，采用两种不同强度的脉冲进行通信从而克服了 PNS 攻击. 本文还根据信道参量估计出不同通信距离的通过率，为信道编码提供依据. 此协议能够实现远距离的量子安全直接通信.

1　经济的量子安全直接通信网络方案

文献[13]提出的利用单光子实现的经济的量子安全直接通信网络方案如图 1. Alice 为服务器，Charlie 为接收方，Bob 为发送方，C_C 和 C_B 分别代表 Charlie 和 Bob 的编码操作，M_A，M_B，M_C 分别代表 Alice，Bob，Charlie 的测量操作，E_1，E_2，E_3 代表各种攻击. 在此方案中，采用同一个服务器来制备和测量量子态. 首先由服务器产生水平极化的单光子，并且把这些量子态发送给接收方 Charlie. 在此过程中可能存在扰乱攻击和木马攻击，Charlie 收到光子后选取部分光子进行测量，判断是否存在以上两种攻击. 然后 Charlie 通过 I 操作和 σ_Z（比特翻转）操作进行编码，并加入部分斜极化的诱骗光子，发送给 Bob. 在此过程中可能存在测量重发攻击和木马攻击，Bob 收到光子后首先检测是否存在以上两种攻击. 如果没有，则在要发送的信息中加入部分随机比特并通过 I 操作和 σ_Z 操作编码后发送给服务器，在此过程中可能存在扰乱攻击. 服务器对收到的光子进行测量，通过加入的随机比特判断是否存在攻击. 如果没有攻击，则服务器通过经典信道公布测量结

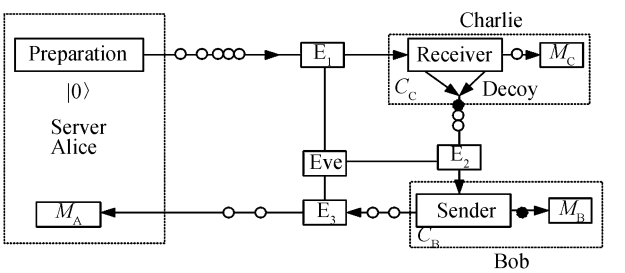

图 1　经济的量子安全直接通信网络模型

Fig. 1　Model of economical QSDC network

*国家自然科学基金（60572147、60672119）、高等学校学科创新引智计划（B08038）和国家重点实验室专项基金（ISN02080002）资助

Tel：029-88204434　　Email：dxquan@xidian.edu.cn

收稿日期：2008-10-28　　修回日期：2009-03-13

果，接收方 Charlie 可以根据此结果以及自己的编码计算出 Bob 要发送的信息.

此方案仅适合于局域网通信，当通信双方距离较远时，因传输路径加长，丢失率提高，不能正常通信；并且由于目前还没有完美的单光子源，多采用弱相干光经过衰减近似代替单光子源，有的脉冲含有多个光子，可能存在 PNS 攻击.

2 基于诱骗态的广域量子安全直接通信网络方案

鉴于由单光子实现的经济的量子安全直接通信网络方案存在的上述问题，本文针对性地提出基于诱骗态的广域量子安全直接通信网络方案，网络拓扑如图 2. 其中量子交换机(Quantum Switch)由经典控制模块，交换网络和输入输出设备构成. 当客户端有信息需要传输时，通过控制模块进行路由查询，若信道空闲则控制交换网络建立物理连接. 该方案建议在每一个局域网设置一个负责量子态产生和测量的服务器，如果此局域网内的客户端需要进行通信，则都由此服务器来完成量子态的产生和测量. 现假设 Alice1 要和 Bob1 进行通信，则单次通信的示意图如图 3. 其通信过程为：首先 Server B 产生两种不同强度水平极化的光脉冲(图中用○和●表示)和空脉冲，传送给 Bob1，Bob1 检测之后进行随机编码，并加入部分斜极化的诱骗光子(图中用★表示)，然后传送给发送端 Alice1. Alice1 检测并编码之后发送给 Server A. Server A 测量之后公布测量结果，Bob1 可以根据自己的编码信息和测量结果计算出 Alice1 所传递的信息. 与文献[13]方案相比，本方案量子态经 Alice1 编码之后，只需要传递给自己局域网的服务器 A 就可以了，而不必传输给远方的服务器 B，从而缩短了传输路径，减小了丢失率，提高了通信距离. 而文献[13]中分析的方案相当于在局域网内部进行通信的情况.

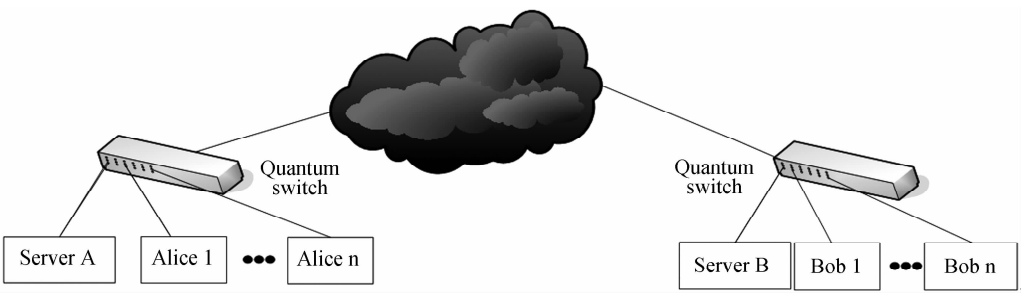

图 2 网络拓扑图

Fig. 2 Network topology

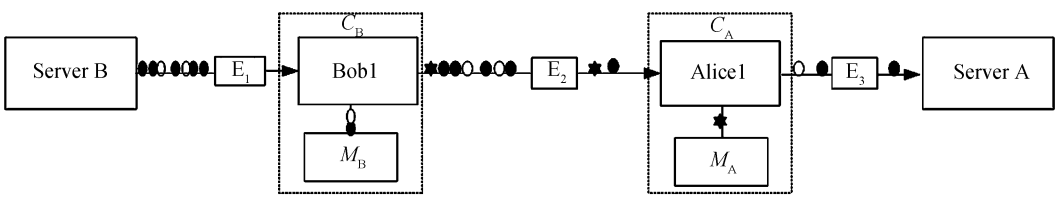

图 3 量子安全直接通信网络中单次通信过程

Fig. 3 Communication process from Alice1 to Bob1 of QSDC Network

具体的通信步骤可归纳为：

1)Alice1 向交换机发送通信请求，交换机为通信双方选择合适的路由，如果接收方空闲，则在收发之间建立起量子通路.

2)Bob1 端局域网的服务器 B 产生空脉冲和另外两种不同强度的水平极化态的光脉冲(图中用○和●表示，量子态为$|0\rangle$)，并且把这些量子态随机的发送给 Bob1.

①在 Bob1 的前端接有滤波器(可以滤除不可见光子)，通过 Bob1 之后以一定的概率通过(50∶50)的 PNS(photon number splitter)，如果两个探测器都响应的概率比较大(存在木马攻击)，则终止通信；否则进行下一步.

②Bob1 随机的选取部分光子在 Z 基(垂直极化基)下进行测量，如果错误率大于门限值(存在扰乱攻击)，则终止通信；否则进行下一步.

3)Bob1 随机的选取部分量子态进行 45°的旋转，将他们的位置记为(B_1，B_2，B_3，B_4…)(图中用★表示)，其余部分以 1/2 的概率选择 I(0)操作或 σ_Z ①操作，然后将光子发送给发送方 Alice1.

①Alice1 收到光子之后，首先进行与 Bob1 一致的测量操作(步骤 2)中的①)，判断是否存在木马攻击，如果没有木马攻击，则进行下一步.

②Bob1 通过经典信道告诉 Alice1(B_1，B_2，B_3，B_4…)，Alice1 对这些位置的光子在 X 基(斜极化基)下进行测量，然后 Bob1 随机地选取部分其余位置的光子，Alice1 对这些位置的光子在 Z 基下进行测量. 如果其错误率高于门限值，则认为存在测量重

发攻击，终止通信. 否则进行下一步.

③Alice1 根据检测序列不同强度光脉冲的通过率判断是否存在光子数目分割攻击，如果没有，则进行下一步，否则终止通信.

4)Alice1 对自己要发送的信息进行信道编码，并在编码后的信息中加入部分随机比特组成新的信息串，标记随机比特的位置为(A_1，A_2，A_3，A_4…). 然后根据信息串对量子态进行 I(0)操作或 σ_Z(1)操作，并将光子发送给 Alice1 局域网的服务器 A 进行测量.

5)服务器 A 在垂直基下进行测量，记测量结果为 M. 并公布测量结果 M 给 Alice1 和 Bob1，Alice1 首先通过(A_1，A_2，A_3，A_4…)位置的测量结果判断在 Alice1 到服务器 A 之间是否存在扰乱攻击，如果信道是安全的，则 Bob1 可以根据下式从服务器 A 公布的结果计算出 Alice1 发送的信息.

$$M=C_B\oplus C_A\rightarrow C_A=C_B\oplus M \tag{1}$$

式中，C_A，C_B 分别为 Alice 和 Bob 的编码信息，编码规则为：0 不进行任何操作；1 进行 σ_Z 操作. M 为服务器的测量结果，如果得到水平极化态，则 $M=0$；如果得到垂直极化态，则 $M=1$.

6)Alice1 通过经典信道告诉 Bob1 信道编码的信息，Bob1 进行译码，得到 Alice1 传递的原始信息，并通知双方的交换机释放相应的资源.

在 Alice1 端由于无法检测每个脉冲中是否含有光子，而且量子信道的丢失率比较大，服务器的检测概率比较小，因此必须采用信道冗余编码. 忽略局域网内部传输的损耗，建议在通信之前，通过经典信道粗略估计通信双方的距离，然后据此计算出通过率，为信道冗余编码提供依据. 设信道的总的传输率为 η，它可以表示为 Bob1 到 Alice1 之间的传输率以及服务器的探测效率的乘积，即 $\eta=10^{-\alpha L/10}\cdot\eta_A$，其中，$\alpha$ 表示信道衰减，L 表示传输距离，η_A 表示服务器 A 的探测效率. 那么当 Bob1 发送 n 光子脉冲时，服务器 A 至少可收到一个光子的概率为：$\eta_n=1-(1-\eta)^n$. 设 Y_n 是 Bob1 发送 n 光子脉冲时 Alice1 端服务器 A 的探测概率，则

$$Y_n=\eta_n+Y_0-\eta_nY_0\approx\eta_n+Y_0 \tag{2}$$

Y_0 是探测器暗计数的概率. 强度为 u 的弱相干光的光子数目分布概率为

$$P_n=\frac{u^n}{n!}e^{-u} \tag{3}$$

整体通过率为

$$Q_u=\sum_{n=0}^{\infty}P_nY_n=\sum_{n=0}^{\infty}\frac{u^n}{n!}e^{-u}(1-(1-\eta)^n+Y_0)=Y_0+1-e^{-\eta u} \tag{4}$$

光纤的衰减取 0.2 db/km，服务器探测效率 0.045，暗计数率为 1.7×10^{-6}[14]，当信源强度 u 分别为 0.1，0.3，0.5 时，可以得到传输率和传输距离的关系如图 4，可以根据不同传输距离的传输率为编码提供依据.

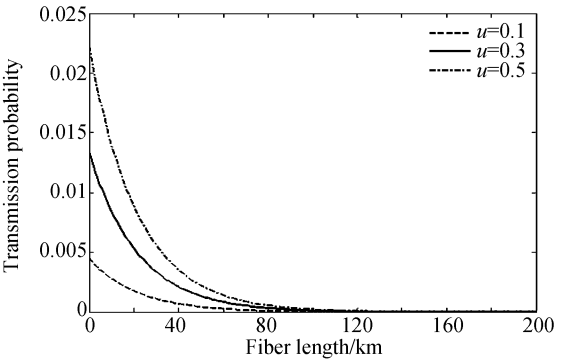

图 4　传输率与传输距离的关系

Fig. 4　Relationship of transmission probability and transmission distance

3　安全性分析

1)对于木马攻击

木马攻击主要包括不可见光子木马攻击和时间延迟木马攻击. 不可见光子木马攻击是指 Eve 在光子到达编码者之前插入与光子同步但波长不同的光子；时间延迟木马攻击是指 Eve 在光子到达编码者之前插入与光子时间稍微不同(仍然在操作门限时间以内)但波长近似的光子. 这样在编码的时候就会对木马光子进行相同的操作，Eve 在编码之后再分离出木马光子，通过对木马光子的测量就可以得知编码信息. 步骤 2)中的 ①和 3)中的 ①能够克服木马攻击.

2)对于扰乱攻击

在 Server B 到 Bob1 的传输过程中，虽然窃听者经测量得不到任何信息，但是他可以通过 σ_Z 操作来改变光子的初态，从而使得最终得到错误的信息. 步骤 2)中的②能够防止此类攻击.

同理，在 Alice1 到服务器 A 的传输过程中，窃听者 Eve 可以通过在 Z 基下测量得到最终结果 M，并不影响服务器 A 的测量结果. 但是由于它不知道 Bob1 的随机比特从而得不到 Alice1 的信息. 通过(A_1，A_2，A_3，A_4…)这些位置的随机比特能够判断这个过程是否存在扰乱攻击.

3)对于测量重发攻击

在 Bob1 到 Alice1 的传输过程中，插入的诱骗光子可以防止窃听者对量子态进行测量，读取 Bob1 所加载的信息. 如果有窃听者 Eve 存在，则在步骤 3)中的②窃听检测中就可以发现，这时 Eve 所得到的信息只是 Bob1 加载的部分随机比特，没有任何

意义.此过程的分析与 BB84 协议完全一致[1].

如果量子态先传递给 Alice1 进行编码,则在从 Alice1 到 Bob1 的传输过程中测量重发攻击能够得到部分信息.因此量子态必须先发送给 Bob1 进行随机编码,然后再发送给 Alice1 进行编码.

4)对于光子数目分割攻击

如果采用弱相干光经过衰减近似代替单光子源,有些脉冲仍然含有多个光子,当信道的传输率小于光源中的多光子概率时,就可能存在 PNS 攻击.

在 Bob1 到 Alice1 的传输过程中,Eve 首先对光子数目进行检测,如果含有单个光子则阻止;如果多于 1 个光子,则从其中分出一个光子保存,另外一个光子通过无损失的信道发送给 Alice1.在 Bob1 公布了诱骗光子的位置以后 Eve 就可以丢弃这些光子,对剩余的光子在 Z 基下测量就可以得到 Bob1 的随机比特,然后根据 Alice1 端服务器公布的结果就可以计算出 Alice1 发送的信息.

诱骗态的思想是信号源发送两种不同强度的光脉冲,如果存在 PNS 攻击,则强度小的脉冲受阻止的概率就大,因此通过率减小的比较多,而强度大的脉冲含有的多光子的概率较大,因此通过率减小的较少,通过比较他们的通过率就可以判断是否存在 PNS 攻击.

本文所提方案将诱骗态的思想引入到量子安全直接通信中,信号源随机的发送空脉冲和另两种不同强度的光脉冲,通过空脉冲的通过率可以估计出探测器暗计数的概率,通过另两种不同强度脉冲的通过率可以判断出是否存在 PNS 攻击.

4 结论

本文提出了一种基于诱骗态的广域量子安全直接通信网络方案,在每一个局域网内设置一个服务器负责量子态的产生和测量,这样当通信双方处于不同的局域网时可以缩短光子传输路径,提高通信距离,从而可构建量子安全直接通信广域网.其次,将诱骗态的思想与量子安全直接通信相结合,采用不同的强度发送光脉冲可以克服 PNS 攻击,有效的提高了协议的安全性.最后,还计算出了不同传输距离的通过率,从而为编码提供了依据.

参考文献

[1] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and cointossing[C]. *IEEE*, 1984: 175-179.

[2] MAYERS D. Unconditional security in quantum cryptography [J]. *J Assoc: Comput Math*, 2001, **48**(1): 351-406.

[3] SHOR P W, PRESKILL J. Simple proof of security of the BB84 quantum key distribution protocol[J]. *Phys Rev Lett*, 2000, **85**(2): 441-444.

[4] 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.

[5] CHEN Xia, WANG Fa-qiang, LU Yi-qun, *et al*. A differential phase shift key distribution QKD system combing with efficient 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.

[6] PENG Cheng-zhi, ZHANG Jun, YANG Dong, *et al*. Experimental long distance decoy-state quantum key distribution based on polarization encoding [J]. *Phys Rev Lett*, 2007, **98**(1): 010505.

[7] CHEN Zhi-xin, TANG Zhi-lie, LIAO Chang-jun, *et al*. Practical security problem of six states QKD protocol[J]. *Acta Photonica Sinca*, 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.

[8] SCHMITT-MANDERBACH T, WEIER H, FURST M, *et al*. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km[J]. *Phys Rev Lett*, 2007, **98**(1): 010504.

[9] BOSTROEM K, FELBINGER T. Deterministic secure direct communication using entanglement[J]. *Phys Rev Lett*, 2002, **89**(18): 187902.

[10] CAI Qing-yu. The "Ping-Pong" protocol can be attacked without eavesdropping [J]. *Phys Rev Lett*, 2003, **91**(10): 109801.

[11] DENG Fu-guo, LONG Gui-lu, LIU Xiao-shu. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block[J]. *Phys Rev A*, 2003, **68**(4): 042317.

[12] MAN Zhong-xiao, ZHANG Zhan-jun, LI Yong. Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations [J]. *Chinese Physics Letters*, 2005, **22**(1): 18.

[13] DENG Fu-guo, LI Xi-han, LI Chun-yan, *et al*. Economical quantum secure direct communication network with single photons[J]. *Chinese Physics*, 2007, **16**(12): 3553-3559.

[14] GOBBY C, YUAN Z L, SHIELDS A J. Quantum key distribution over 122 km of standard telecom fiber [J]. *Applied Physics Letters*, 2004, **84**(19): 3762-3764.

Scheme for Wide-area Quantum Secure Direct Communication Network Based on Decoy States

QUAN Dong-xiao，PEI Chang-xing，LIU Dan，ZHAO Nan

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

Abstract：A scheme for wide-area Quantum Secure Direct Communication (QSDC) Network based on decoy states is proposed. A server which is used to prepare and measure photons，is set in each local area network，so the communication distance increases. In addition，the idea of decoy states，which is to send photon pulses of different intensities to detect Photon Number Splitting (PNS) attack，is introduced to QSDC to improve the security of the communication. And，the transmission probability is estimated based on the channel parameter，which can be used as a reference for channel coding. Security analysis result shows that this protocol can be used to realize long distance QSDC.

Key words：Quantum secure direct communication；Wide-area network；Decoy state；Transmission probability

QUAN Dong-xiao　was born in 1980. She received her M. S. degree from Xidian University in 2003. At present，she is pursuing her Ph. D. degree and works as a lecturer at Xidian University. Her research interests focus on quantum communication.