爱因斯坦的“幽灵”超距作用实现多方量子安全通信网*

项 玉　何琼毅†　龚旗煌

(北京大学物理学院 人工微结构和介观物理国家重点实验室　量子物质科学协同创新中心　北京　100871)

2015－04－14收到

† email：qiongyihe@pku.edu.cn

DOI：10.7693/wl20150505

量子力学理论可以完美地描述自然界中最小的物理体系，比如原子和光子。正如1935年爱因斯坦、波多尔斯基、罗森在他们著名的Einstein—Podolsky—Rosen(EPR)佯谬中提出的[1]，量子力学具有令人惊讶的特性：处于位置和动量理想关联量子态的一对粒子，一定时刻后在空间上完全分离，对其中一个粒子测量会瞬间影响相隔遥远的另一个粒子的性质，这被爱因斯坦称为“幽灵般”的超距作用。同年，薛定谔提出了量子纠缠的概念[2]，即处于量子纠缠的复合系统，其态矢量不能表示为各个粒子的态矢量的张量积形式(通常称为量子态不可分特性)。作为量子体系显著区别于经典体系的特征，量子纠缠不仅具有重要的理论意义，也是量子密码、量子计算、量子通信等量子信息处理的重要资源，对这方面的研究已经成为国际科技界激烈竞争的焦点。与一般的量子纠缠相比，EPR佯谬中描述的量子关联，除了具有不可分性，还具有非定域性，即：Alice对处于EPR态的A粒子某个观测量的测量，可以引导距离遥远且与之纠缠的B粒子量子态到她所选择的观测量的本征态，从而可以较为精确地预言Bob对B粒子的观测结果。这种关联现象最近被称为EPR量子引导纠缠(EPR steering entanglement)[3]。最新的研究表明，这种特殊的量子纠缠可以由三方或多方共享，用来作为安全通信加密所需的量子密钥，这意味着多方量子秘密通信成为可能[4]。

量子纠缠是量子信息处理中的重要资源，也是量子通信安全性和高效性的最主要原因之一。近年来，具有丰富纠缠结构和复杂性质的多体量子纠缠逐渐成为国内外研究的热点，它是人们了解量子退相干过程、量子与经典的过渡等诸多基础物理问题的关键。然而，多体量子纠缠具有多种不同的形式，随着每增加一个粒子，纠缠的复杂程度会迅速增加，目前人们对它的认识还很有限。因此，深入研究这些复杂的多体量子纠缠态，合理使用其特有的形式和性质，将为多粒子量子系统在未来技术中的各种新奇应用开辟道路。

包括我国科学家在内的多个实验组在多体量子纠缠领域做出了突破性贡献。T. Monz等人在离子体系中实现了14量子比特的GHZ纠缠态[5]；中国科学技术大学实现了8光子的GHZ纠缠态[6, 7]；山西大学成功制备出了8模连续光场的cluster纠缠态[8, 9]；澳大利亚国立大学也实现了连续变量光场的8模纠缠态[10]等；最近的研究还报道了更多时间[11]模式和频率[12]模式的纠缠态。随着多体量子关联研究的深入，人们自然而然会问这样一系列的问题：多体量子纠缠是否也像两体纠缠一样存在不可分性与非定域性的分类[13]？如何检测多体系统中有多少个体关联在一起[14]，是否是真正多体纠缠[4, 15]？如何判定它们之间的关联具有非定域性[16]？作为本领域理论和实验研究的

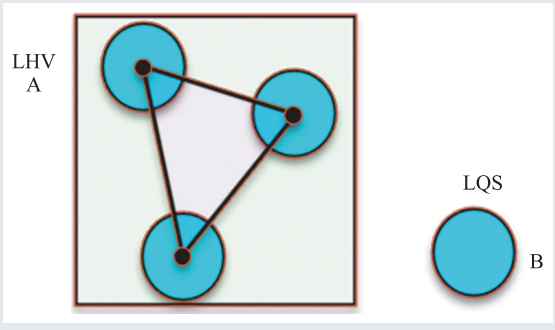

图1　多体系统局域隐态(LHS)模型[16]

* 国家自然科学基金(批准号：11121091；11274025)资助项目

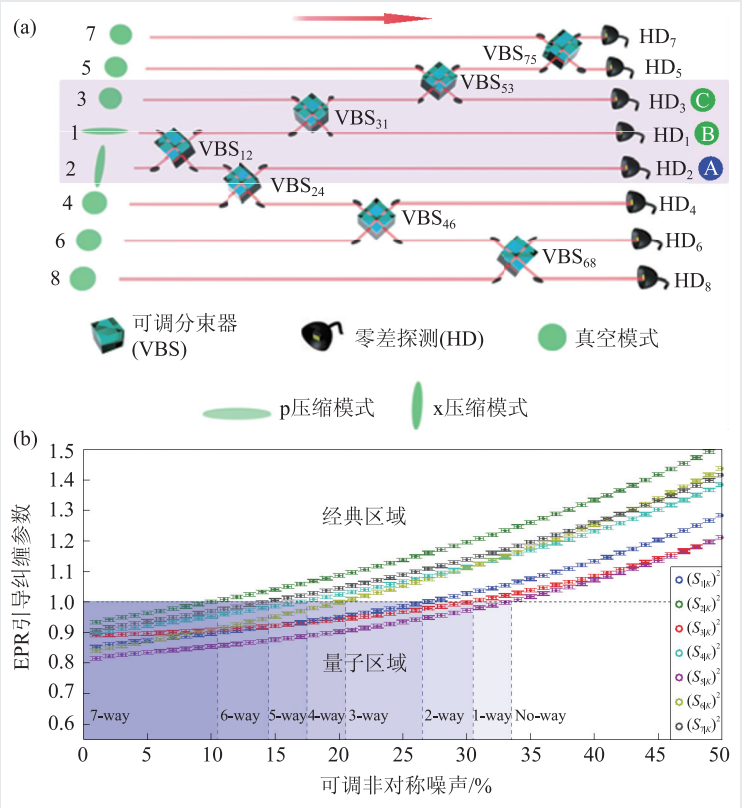

图2 (a)实验装置示意图。将光场压缩态1，2与真空态3—8经分束器VBS混合，调节系统参数至适当值后，能够实现多模光场的量子引导纠缠和真正三体量子纠缠；(b)7个连续变量光场模式的多体量子引导纠缠，即 $S_{i|K}<1$ [4]

基础性课题，这些问题的理解和澄清，将对量子力学基本原理、量子信息的物理实现以及超精密测量等方面产生重要影响。

2013年，何琼毅和M. D. Reid首先给出了多体量子系统中存在真正量子引导关联的判定依据[16]。如图1所示，系统中子体系B处于量子态(LQS：local quantum state)受到量子不确定性关系的约束，A中所有子体系的行为都遵循局域隐变量(LHV：local hidden variable)理论，分别对它们进行局域测量，再联合测量结果，如果可以推断出B的一对共轭物理量(如：光场的振幅和位相)的测量结果，且推断的不确定度能够违背海森伯不确定性关系，则证明系统中A与B之间存在多体量子引导纠缠，即A可以引导B到某一确定量子态。如果该行为针对处于混态系统中的任一子体系都成立，就说明该系统中存在真正多体量子引导关联。该理论一经提出就得到了国际理论与实验小组的热切关注。2015年，我们与澳大利亚国立大学P. K. Lam实验小组合作，成功实现了7模连续变量光学系统多体量子引导纠缠的实验验证[4]，实验装置示意图如图2(a)所示。研究结果表明，“量子引导纠缠”这种特殊的量子纠缠可以由三方或多方共享，如图2(b)所示。在N个输出模式中，不但可以实现任意一个模式i与其余N–1个模式的组合K之间的量子引导纠缠，即$S_{i|K}<1$，还可以通过调节某个输出光路上的损耗，逐渐使得一些组合失去对某个模式j的量子引导能力，即$S_{j|K}>1$。如果任意的N–1个模式与剩余的一个模式之间都不存在量子引导纠缠，称之为No-way steering，反之，称为N-way steering。这种从No-way到N-way具有一定指向性的多体量子引导纠缠，为未来构建不同任务需求的具有一定方向性的多方量子安全通信网络提供了可能。

这项工作针对三模光场做了更为详细的实验研究和理论分析。首先，实现了连续变量光场的真正三体量子纠缠，如图3(a)所示。真正多体量子纠缠是一类特殊的多体量子纠缠形式，处于真正量子纠缠的多体系统，其量子态不能表示为任何单个粒子与其余粒子的态矢量的张量积的叠加形式。其次，实验验证了我们理论上提出的光场模式B和C对A的联合量子引导[16, 17]，如图3(b)中间的绿色暗影区域。该区域内光场模式B，C都不能单独对模式A实现量子引导。图中C→A，B→A的曲线都高于阈值($S_{A|B}>1$，$S_{A|C}>1$)，只有当B和C联合才能预言A的测量结果，并使图中BC→A线处于阈值以下($S_{A|BC}<1$)。该实验同时观测到了量子引导的单婚性[18]。即B，C不能同时与A之间实现量子引导纠缠。观察图3(b)的左

右白色区域可以发现，如果光场B可以引导A到某一特定量子态，即曲线B→A在阈值1以下($S_{A|B}<1$)，那么光场C就不可以，此时曲线C→A在阈值1以上($S_{A|C}>1$)。值得注意的是，此时A可以同时实现对B和C的量子引导，即图中A→B，A→C曲线都处于阈值以下($S_{B|A}<1$且$S_{C|A}<1$)，这也是对两体量子引导纠缠之间存在方向性的验证。

该研究结果提供了一种更安全的单方(接收方)设备不依赖的量子秘密共享方案[19, 20]。如图4所示，四方共享一个包含4个粒子的具有量子引导纠缠的量子态，发送方Alice把秘密信息加密在她拥有的粒子的振幅和位相上，其余三个接收方分别对自己的粒子进行测量，只有当所有的接收方相互协作、共享测量结果时，才能推断出Alice所拥有的粒子的测量结果，将加在上面的秘密信息解密出来。在通信过程中，只要发送方的测量是安全的，那么任何形式的黑客攻击，无论是对传输中的信息窃取还是对接收方测量装置的破坏，都会被探测出来。这种安全性是由多方之间共享的量子引导纠缠保证的，因此通信方式是绝对安全的。同时，由于发送方不需要信任接收方的测量，即使接收消息的装置已被篡改，量子传送的消息还将保持安全，从而可以实现对接收方设备不依赖的安全通信，这种对接收方设备的不依赖性是由爱因斯坦的“幽灵纠缠”的性质决定的。

这项研究成果最近在*Nature Physics*上发表[4]。我们的工作向实现单方设备不依赖的多方安全量子通信网络迈出了重要一步，原则上这种由多方共享的量子引导纠缠作为安全基础的保密通信，可以抵御信息传输过程中的任何黑客攻击，为未来构建多方量子通信网络提供前所未有的安全保证。

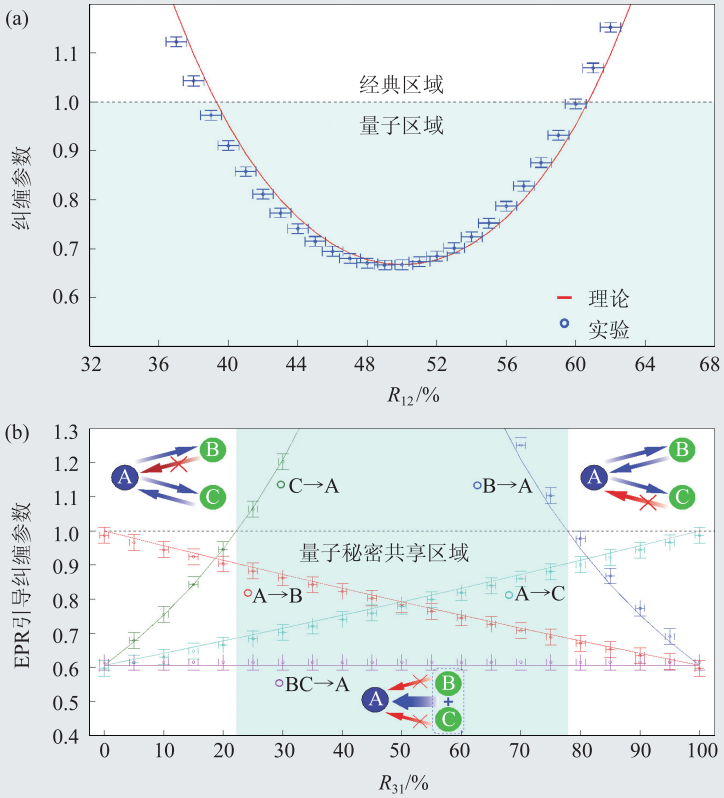

图3 (a)连续变量光场A，B，C之间实现真正三体量子纠缠(阈值1以下区域)，此时系统的态矢量不能表示成任何光场模式与其余两个光场模式的态矢量的张量积的叠加形式，即$\rho\neq P_1\rho_{A|BC}+P_2\rho_{B|AC}+P_3\rho_{C|AB}$；(b)三模光场量子引导关联的联合性(绿色阴影中)、单婚性(左右两侧白色区域)以及方向性[4](图中横坐标R_{12}和R_{31}分别对应图2(a)中VBS_{12}(混合光路1和2的可调分束器)和VBS_{31}(混合光路1和3的可调分束器)的反射率)

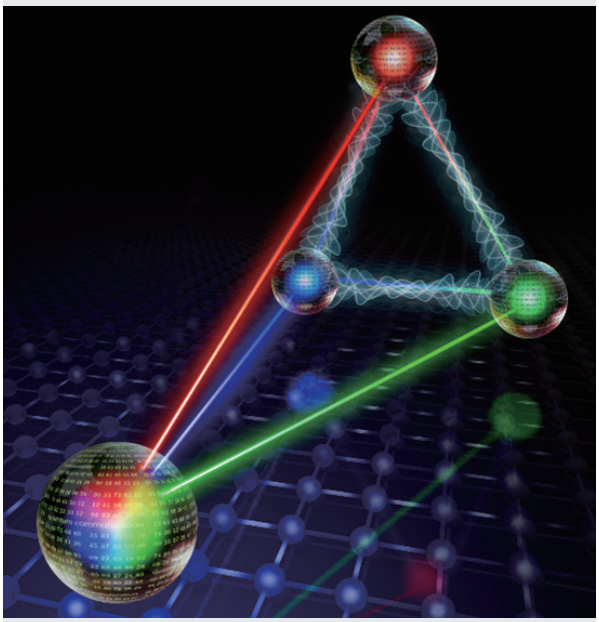

图4 单方(接收方)设备不依赖的量子秘密共享方案

参考文献

[1] Einstein A, Podolsky B, Rosen N. Phys. Rev., 1935, 47: 777

[2] Schrödinger E. Proc. Cambridge Philos. Soc., 1935, 31: 555

[3] Wiseman H M, Jones S J, Doherty A C. Phys. Rev. Lett., 2007, 98: 140402

[4] Armstrong S, Wang M, He Q Y *et al*. Nat. Phys., 2015, 11: 167

[5] Monz T, Schindler P, Barreiro J T *et al*. Phys. Rev. Lett., 2011, 106: 130506

[6] Huang Y F, Liu B H, Peng L *et al*. Nat. Commun., 2011, 2: 546

[7] Yao X C, Wang T X, Xu P *et al*. Nat. Photonics, 2012, 6: 225

[8] Su X L, Hao S H, Zhao Y P *et al*. Frontiers of Physics, 2013, 8: 20

[9] Su X L, Zhao Y P, Hao S H *et al*. Opt. Lett., 2012, 37: 5178

[10] Armstrong S, Morizur J F, Janousek J *et al*. Nat. Commun., 2012, 3: 1026

[11] Yokoyama S, Ukai R, Armstrong S *et al*. Nat. Photonics, 2013, 7(12): 982

[12] Roslund J, De Araujo R M, Jiang S *et al*. Nat. Photonics, 2014, 8(2): 109

[13] He Q Y, Gong Q, Reid M D. Phys. Rev. Lett., 2015, 114: 060402

[14] Reid M D, He Q Y, Drummond P D. Frontiers of Physics, 2012, 7: 72

[15] Shalm L K, Hamel D R, Yan Z *et al*. Nat. Phys., 2013, 9: 19

[16] He Q Y, Reid M D. Phys. Rev. Lett., 2013, 111: 250403

[17] Wang M, Gong Q, He Q Y. Opt. Lett., 2014, 39: 6703

[18] Reid M D. Phys. Rev. A, 2013, 88: 062108

[19] Hillery M, Bužek V, Berthiaume A. Phys. Rev. A, 1999, 59: 1829

[20] Branciard C, Cavalcanti E G, Walborn S P. Phys. Rev. A, 2012, 85: 010301(R)