模仿量子纠缠的“伪造态”

Bell 不等式是对一个系统的量子本质的最根本的检验.但实验表明,这个检验可以被欺骗.

在 1935 年,爱因斯坦、波多尔斯基(Podolsky)和罗森(Rosen)共同辩说量子力学并非完备,因为对某个系统进行测量会立即影响另一个系统的波函数,这与信息传输的光速极限相矛盾[1].若想避免此“鬼魅般的超距作用”,各系统实际蕴含的内容必须比波函数所描述的要多.量子力学也许需要增补,例如通过引入隐变量理论,使得每一次测量仅依赖定域的自由度.

近 30 年后,J. Bell 指出这不仅仅是个哲学问题,并设想一个可鉴别量子力学与隐变量理论的实验:在相隔很远的两个测量中,其关联测试结果如果违背了 Bell 不等式,则只能用量子力学来解释[2].然而,这种检测受限于若干条件,即存在漏洞.例如,要消除定域性漏洞就必须建立光速通信不影响实验结果的实验条件.而且要消除测量漏洞,测量效率必须足以排除观测单次事件违背而总的系综不违背 Bell 不等式.实验中,Bell 检测给出的结果与量子力学保持一致[3],但至今还没有任何实验可以同时排除所有漏洞.目前,这些检测实验的主要实际运用并不是为了消除对量子力学正确性的疑虑,而是作为“纠缠证据”去证明某光源的量子本性.

现在,挪威科技大学的 V. Makarov、新加坡国立大学的 C. Kurtsiefer 及其同事已经证明:若忽略漏洞中的任一个,一个明显没有纠缠的系统也能违背 Bell 不等式[4].他们利用所谓的伪造态,用经典的光脉冲去欺骗探测器,让探测器误认为探测到单光子.在实验系统中,偏振纠缠光子对中的两光子由光纤发送到接收者 Alice 和 Bob,两人各自利用两个偏振基中的任一个进行偏振检测:Alice 随机选取 0°基 A 或 45°基 A′;Bob 选取 22.5°基 B 或 −22.5°基 B′.如果是理想的纠缠光子对,Alice 和 Bob 具有相同测量结果的概率是 $\cos^2(22.5°)$,即 85.3%,除非 Alice 选取 A′基且 Bob 选取 B′基,这种情况下测量结果不同的概率是 85.3%.随后计算量 $S=E_{AB}+E_{A'B}+E_{AB'}-E_{A'B'}$,其中前 3 个 E 是测量结果一致的几率,最后一项 E(对应 A′B′基)是结果不同的几率.对于任何经典系统,$|S|\leq 2$,此即 Bell 不等式.但对于理想纠缠态,$S=2.83$,违背不等式.

每个接收器由一个偏振分束器(PBS)和两个雪崩光二极管(APD)单光子探测器组成.在 PBS 前放置半波片,通过旋转半波片来改变测量基.一个入射光子将触发电子雪崩放大,APD 输出一个脉冲,表明探测到一个光子,随即复原等待下一个光子.当足够强的光子流入射到探测器时(100μW 更低亦可),APD 来不及复原,被致盲了,看不到单光子.此时,一个更亮的光脉冲(5mW 量级)与之前的入射光叠加入射,不需要雪崩效应就能产生足够大的光电流使探测器产生一个脉冲输出.

研究小组将一束连续圆偏振光和一束亮的线偏振光脉冲叠加合成伪造态.圆偏光被均等分束到两个 APD 上,无论半波片位置如何放置,两探测器均被致盲.叠加在其上的亮脉冲的偏振方向设置成研究者想让接收者探测到的方向.

假定伪造态要在 Bob 选择 B 测量基时产生一个“0”.如图 1(a)所示,如果 Bob 恰好选取 B 基,亮脉冲将全部入射到输出为“0”的 APD 上,引起一个响应.但是若 Bob 选取 B′基,亮脉冲将在两探测器间分配,光强度均不够产生响应(见图 1(b)).

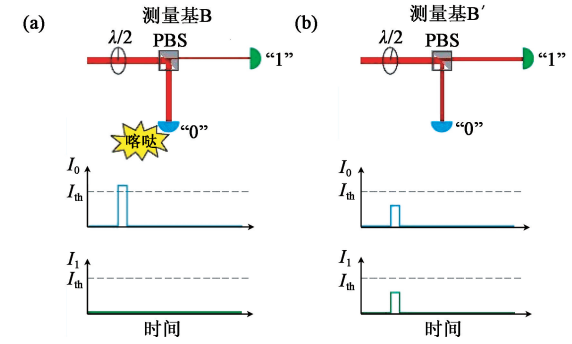

图 1　伪造态的 Bell 检测实验

通过分别发送给 Alice 和 Bob 一连串的伪造态,可以产生任何想要的关联花样,可以模仿纠缠光子对的关联,甚至可以创造任何经典或量子系统看来不可能的关联.但是,Alice 和 Bob 每次探测到的只是他们所接收伪造态的一半,因此探测漏洞没有被消除.对于使用真实光子的 Bell 检测实验,探测效率往往远小于 50%.这些实验要依赖于探测的所有事件发生概率都相同的假设.这种假设虽然合理,但在伪造态的实验中,当选取错误基导致探测不到信号时,证明这一假设不成立.

如果接受方使用被动选基方案,在普通分束器之后再用 2 个 PBS 选择测量基(见图 2),便可消除探测的漏洞,但是定域漏洞没有被消除.当入射光是一个真正的单光子时,分束器的作用恰好如同旋转半波片的作用,确保了基的随机选择.但是攻击方使用伪造态时,可以强制接收器在任何一个他们希望的基响应.一束圆偏振光被均匀地分成 4 路入射到 4 个 APD 上,将它们全部致盲.然后,线偏光只在目标基中产生一个响应脉冲.

这个分束器装置没能消除定域性漏洞,因为存在一些随光子一起传播的经典参数支配着所选探测基的可能性.在真单光子的系统中这种可能性看似难以置信,但这就是伪造态所能做到的.

基于纠缠态的量子密钥分发在很多方面与 Bell 实验相似:偏振纠缠光子对被发送给 Alice 和 Bob,两人随机地选取测量基,不同的是,他们只从两个基选取.然后两人对照所用的基,丢弃所有用不同基的测量结果(以及没能探测到光子

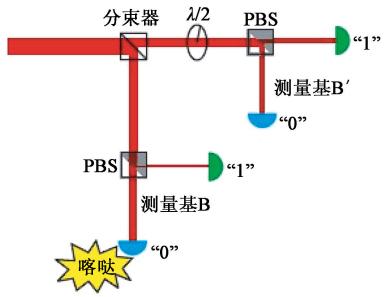

图 2　以普通分束器选择测量基

的情况),最后保留只有他们两人知道的同样的 0、1 序列.

原则上,上述过程无法破解,因为物理上不可能测量一个未知量子态并且准确地复制一个相同态(即量子态不可克隆),且任何在光子传播过程中的窃听都应能立即被发现(参见 *Physics Today* 2009 年第 2 期第 76 页). 但是,如果窃听者 Eve 拦截了光子并且取而代之发送相应的伪造态,Alice 和 Bob 并不会怀疑发生了任何差错. 基于这种方法,Makarov, Kurtsiefer 和他们的同事们证明了他们可以窃听量子密码系统,包括商用系统[5]. 他们的做法也并非无懈可击,因为窃密流程利用的是设备的漏洞而不是量子密码学本身的漏洞. 正如一个无漏洞的 Bell 不等式检测实验一样,一个完全安全的量子密码系统仍是一个卓越的目标.

参考文献

[1] Einstein A, Podolsky B, Rosen N. Phys. Rev., 1935, 47: 777
[2] Bell J S. Physics, 1964, 1: 195
[3] Aspect A. Nature, 1999, 398: 189
[4] Gerhardt I *et al*. Phys. Rev. Lett., 2011, 107: 170404
[5] Gerhardt I *et al*. Nat. Commun., 2011, 2: 349; Lydersen L *et al*. Nat. Photonics, 2010, 4: 686

(中国科学院物理研究所 李明飞、李申、吴令安 编译自 Johanna Miller. *Physics Today*, 2011, (12): 20, 原文详见 http://ptonline.aip.org)