三个课题组关闭了验证贝尔理论实验中的漏洞

(清华大学 李 涛、龙桂鲁 编译自 Johanna Miller. *Physics Today*, 2016, (1): 14)

通常情况下，量子力学很难与经典世界的直觉相符。我们知道，经典粒子具有确定的位置和动量，而量子波函数仅能给出几率分布。除此之外，量子理论认为，无论两粒子相距多远，只要它们处于纠缠态，那么测量其中一个粒子，就可以瞬间改变另一个粒子的波函数。

在量子世界里，这些反直觉效应还有很多，那么它们是错觉吗？有科学家提出，或许利用系统隐变量可以补充量子理论，使其重新获得定域实在性。这样，每次测量的结果可仅依赖于过去光锥中已发生的事件。1964年，贝尔指出可通过测量相距很远的两个系统，观察它们之间的关联，以将量子理论和任何定域实在论区分开。已有的实验室中的贝尔验证实验已倾向于量子力学理论。但到目前为止，这些实验存在两类严重的漏洞，即定域性漏洞和探测漏洞，只有建立在部分假设基础之上才能证伪隐变量理论。

最近，三个课题组分别报道了关闭两类漏洞的贝尔验证实验，分别是代尔夫特理工大学的Hanson和Hensen课题组、美国国家标准与技术研究院(NIST)的Nam和Shalm课题组以及维也纳大学的Zeilinger和Giustina课题组。他们的结论不仅回应了对量子力学真实完备性的质疑，而且推动了量子信息和安全性的发展，如安全的量子秘钥分发和攻击免疫的精确随机数生成源等。

定域性和探测

在一个典型的贝尔验证实验中，Alice和Bob分别持有纠缠粒子对中的一个粒子，例如，极化纠缠光子或自旋纠缠电子。他们随机独立选取测量基矢，并进行相应测量。根据量子力学原理，尽管不能预知他们的每次测量结果，但在多次重复测量实验中，他们的测量结果存在很大的关联。而局域实在论认为只有局域变量，如粒子的状态等，可以影响测量结果。根据这一理论，Alice的测量结果和Bob的测量结果之间的关联度就会远低于量子理论的预期。

假若隐变量信号可以在Bob进行测量之前将Alice选取的测量基矢通知Bob，上述情形又会怎样呢？如果该假设成立，那么隐变量信号可以改变Bob所持有粒子的状态，在没有量子纠缠的系统中产生类似于量子关联的关联。这可能就是所谓的局域漏洞的核心问题。该漏洞可以通过图1所示的装置弥补，在该装置中，Bob在自己的测量完成之前没有机会获得Alice的基矢选择信息。

在实际的贝尔验证实验过程中，为了使得Alice和Bob获得充足的时间来选择基矢并完成测量，Alice和Bob至少需要相隔几十米。这一要求意味着用于贝尔验证实验的纠缠光子能够在该空间尺度上传输且量子态不能受到大的扰动。然而，效率有限的单光子操纵过程和单光子探测过程引入了另一个漏洞，即探测漏洞。具体说来，即使实验总体没有表现出量子关联，也

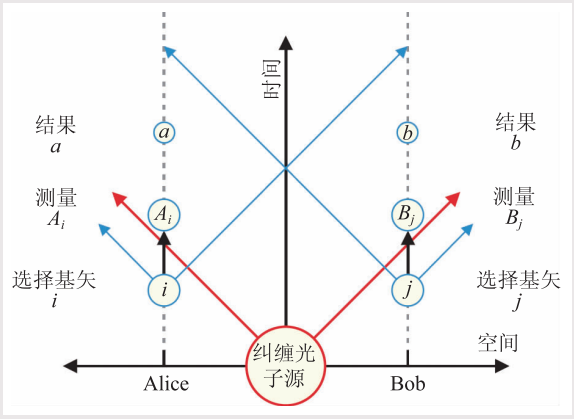

图1 基于纠缠光子源的无漏洞贝尔验证实验时空图

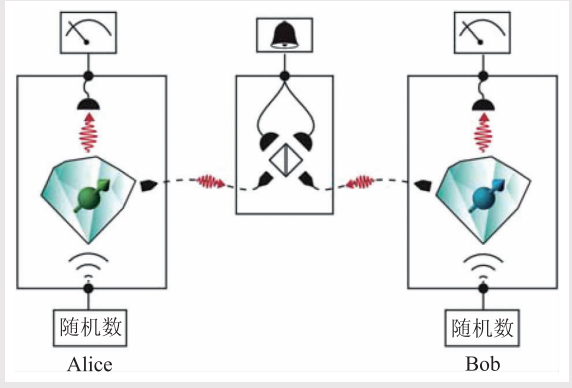

图2 基于固态自旋的无漏洞贝尔验证实验示意图

可能因为Alice端或Bob端的测量失败次数足够多，而导致测量成功的实验表现出量子关联。由于这种探测漏洞的存在，量子密钥系统可能会受到黑客的攻击，而消除该类攻击的唯一途径就是关闭漏洞。

固态自旋

金刚石NV色芯中与晶格缺陷相关的电子自旋的退相干时间较长。代尔夫特理工大学的课题组利用纠缠的金刚石NV色芯完成了无漏洞的贝尔验证实验。如图2所示，首先将每一个NV色芯与单光子纠缠，然后将单光子传输到中间位置并完成两光子符合测量(实际成功率10^{-8}量级)。当两光子符合测量成功时，这两个NV色芯便纠缠起来，Alice和Bob便可以开展贝尔验证实验。该方案的优点是，贝尔验证实验是在符合测量成功后进行的，即使考虑探测漏洞，测量失败的事件也可以被人为去除。

导致上述实验低概率的原因主要有两种：(1)初始时刻单个NV色芯与单个光子纠缠的成功概率仅有3%；(2)光子在光纤传输过程中的丢失。与NV色芯纠缠的单光子波长是637 nm，它远离光纤表现最佳的通信波段。相反，一旦建立NV色芯中电子自旋之间的纠缠，对电子自旋高效准确的测量便可以完成无测量漏洞的贝尔验证实验。2015年初夏时节，Hanson和同事在为期18天的220个小时内完成了245次贝尔验证实验。尽管他们的实验次数较少，但他们仍然观测到了明显的量子关联，因为非量子系统产生同等程度关联的概率仅为4%。

目前，代尔夫特理工大学的课题组正致力于通过光子频率转换提升他们的光子传输效率，进而提升贝尔验证实验的效率。Hanson预计他们可以将测量距离由1.3 km扩展到100 km。在100 km的空间尺度上，许多量子网络应用，如量子密钥分发等，就可以使用了。在量子密钥分发过程中，就像贝尔验证实验过程一样，Alice和Bob独立随机选取测量基矢，测量所持有的纠缠粒子对中的粒子状态。对于那些偶然选中相同测量基矢的实验，他们的测量结果相互关联。通过公开对比哪些实验中测量基矢相同，并根据他们各自的测量结果便可以获得一串安全的“1”和“0”密码。

高效探测器

NIST课题组和维也纳大学课题组的实验均是基于纠缠光子对，并利用了Nam和NIST研发的单光子探测器。其中，维也纳大学课题组使用的是探测效率高达98%的转变边缘传感器，NIST课题组使用的是具有高时间分辨率的超导纳米线单光子探测器(SNSPDs)。先前利用多晶超导材料的SNSPDs的探测效率是70%，而利用非晶体超导材料，SNSPDs的探测效率可以高达90%。

Shalm意识到新的SNSPDs性能已足够完成无漏洞的贝尔测量。他指出：目前已经具有工作在通信波段的探测器，接下来需要产生具有相同波长的纠缠光子对，这是一个很大的技术挑战。而另一个挑战是，提升纠缠光子由纠缠源传输到探测器的效率，因为通常情况下光子耦合进入和耦合输出光纤的效率仅有80%，而实验需要的效率为95%以上。

与代尔夫特理工大学课题组每小时一次的实验效率不同，NIST课题组和维也纳大学课题组每秒钟可以进行上万次实验。他们可以在一小时内收集到足够的数据来估计他们实验过程中的关联产生自随机事件的概率。

目前，很难将基于纠缠光子对的贝尔验证实验扩展到大尺度量子网络。因为即使是在通信波段，光子在光纤传输过程中的丢失概率也不容忽略，增长光纤的长度将进一步降低光子传输率而重新打开探测漏洞。NIST课题组正致力于利用他们的装置产生量子随机数。随机数被广泛使用于安全应用，例如，公钥密码学随机选取两个大的质数，并公布它们的乘积，任何知道乘积的人可以加密信息，但是只有知道上述两个大质数的人可以解密。

公钥密码学的安全基础就在于大数分解是一个非常难的计算问题。假若产生质数的过程可以被预测或重复，那么公钥密码就会失效。经典计算机只能运行确定的程序，由其产生的随机数是伪随机的，而量子态测量过程中产生的随机数确是真正的随机数并且不可预测。

NIST课题组计划将他们的随机数对外界公开，因此它不能用于加密密钥。但是一个公开的防撬破随机数源可以有其他应用，例如，选取不可预测的样本来实现民意调查、纳税人审计以及商品安全检测等。