颠覆性技术快报

DISRUPTIVE TECHNOLOGY LETTERS

2017年 第 1 期（总第 1 期）

中国工程科技创新战略研究院　　2017年8月

本 期 要 目

观点荟萃

从 Bell 不等式看当前量子密码安全性水平

蔡庆宇[1]，孙昌璞[2]

（1. 中国科学院　武汉物理与数学研究所；　2. 中国工程物理研究院　研究生院）

量子力学尤其是哥本哈根学派对量子力学的解释由于和经典世界人们的日常经验或直觉相违背，而难以获得理解。许多在量子力学建立时居功至伟的科学家，如普朗克、薛定谔、德布罗意、爱因斯坦等，后来都不同程度地反对根本哈根学派的量子力学。其中最著名的，莫过于爱因斯坦对哥本哈根学派的质疑。1935 年，爱因斯坦联合普林斯顿高等研究院的另外两位科学家，波多斯基和罗森（简称 EPR），在《物理评论》上发表一篇论文，质疑量子力学的完备性。EPR 的观点是，一个完备的理论要满足两个条件，定域性和实在性，或合称为定域实在性。定域性是指任何物理信号的传递都不能超过光速；实在性是指对一个物理系统的任意一个物理量，总存在一个确定的值。由于哥本哈根学派的量子力学不满足定域实在性假设，因此被 EPR 三人认为是不完备的。

1964 年，数学家 J. S. Bell 提出了一个不等式，可以判断 EPR 定域实在性假设的正确性。若实验结果冲突该不等式，则说明 EPR 假设是错误的。Bell 的工作把 EPR 对量子力学的质疑从哲学范畴推进到实验层面，是一项伟大的创举。在 Bell 工作的启发下，1969 年，J. Clauser、M. Horne、A. Shimony 和 R. Holt 提出了一个不等式（简称

CHSH 不等式），定域实在性要求 CHSH 多项式的值不大于 2，而量子力学给出该多项式的值不大于 $2\sqrt{2}$。

1970 年代，科学家开始了实验研究 Bell 不等式的工作。其中影响较大的当属 1982 年法国学者 A. Aspect 小组的实验工作，给出了冲突 Bell 不等式的较强的实验证据。此后，越来越多的实验小组加入到实验研究 Bell 不等式的队伍中，包括 A. Zeilinger 小组使用多粒子纠缠态演示实验冲突 Bell 不等式的工作。这些研究工作虽然给出了 Bell 不等式可以被冲突的实验证据，但是并没有“彻底杀死”EPR 等人的定域实在性假设：这些 Bell 不等式实验演示工作，都存在这样或者那样的漏洞，从而无法给出令人信服的证据，彻底排除掉 EPR 等人对量子力学的质疑（这可能也是 Aspect 等人一直没有获得诺贝尔奖的主要原因）。Bell 等式实验工作的主要漏洞有两个：定域性漏洞；探测漏洞。Bell 不等式实验中需要对纠缠粒子对中的粒子分别测量，理论上要求两个测量装置在完成测量操作之前，不能有信号从一个装置传递到另一个装置。譬如，装置的测量响应时间为 t，如果两个装置的距离如果小于 tc（c 为光速），那么理论上一个装置的测量操作可以影响另外一个装置的测量结果（隐变量以小于或等于光速从一个测量装置传递到另外一个测量装置），使两个装置的测量结果建立起关联，冲突 Bell 不等式但又满足 EPR 定域实在性假设，这就是定域性漏洞。探测漏洞是指，在 Bell 不等式实验中，由于探测器效率过低，导致实验中许多粒子没有被探测到，如果只统计测量到的结果，Bell 不等式可以被冲突，一旦把没有探测到的粒子也计入在内，

则 Bell 不等式不会被冲突，这就是探测漏洞。一个严格冲突 Bell 不等式的实验，需要在实验中完全关闭所有的漏洞。理论上，如果使用纠缠光子对进行 Bell 不等式进行实验检验，需要单光子探测器探测效率在 83%以上，才可以关掉探测漏洞。

1991 年，A.Ekert 指出，Bell 不等式被冲突，可以用来保证量子密码（密钥）的安全性。以理推之，如果 Bell 不等式实验中存在漏洞，则无法保证量子密码的安全性。为确保最终密钥的安全性，需要进行无漏洞 Bell 不等式实验。然而，目前所有使用纠缠光子的量子密码实验，都无法满足无漏洞 Bell 不等式的要求，尤其是无法关闭探测漏洞。在实际密码实验中，光子损耗太高，而无漏洞 Bell 不等式要求光子损耗不能超过 17%。在光纤量子密码实验中，光子传输效率随距离指数衰减。使用商业光纤（0.2 dB 损耗），百公里量级量子密码实验光子探测效率小于 1%，低于无漏洞 Bell 不等式要求的 83%的探测效率。而在自由空间量子密码实验中，光子损失十分严重。譬如，最近的墨子号量子纠缠分发实验中，其文献报道损耗高达 60 dB 以上（最大高达 82 dB），距离无漏洞 Bell 不等式要求的 83%的探测效率相去甚远。如果在此基础上进行密钥分发，肯定无法实现量子密码“绝对安全”的要求。I.Gerhardt 等人实验显示，如果存在探测漏洞，窃听者可以完全控制 Bell 不等式实验的结果[1]。在此情况下，量子密码已经没有丝毫安全性可言了。

参考文献：
【1】 Gerhardt I，et al. Experimentally faking the violation of Bell's inequalities[J]. Phys Rev Lett,2011,107:170404.