跨越时空的骰子

量子通信/量子密码背后的原理

[瑞士] 尼古拉·吉桑 ◎ 著
周荣庭 ◎ 译

上海科学技术出版社

跨越时空的骰子

量子通信、量子密码背后的原理

[瑞士] 尼古拉·吉桑 著

周荣庭 译

上海科学技术出版社

图书在版编目(CIP)数据

跨越时空的骰子：量子通信、量子密码背后的原理 /（瑞士）吉桑（Nicolas Gisin）著；周荣庭译. —上海：上海科学技术出版社，2016.8

ISBN 978-7-5478-3134-2

Ⅰ.①跨… Ⅱ.①吉…②周… Ⅲ.①量子力学—研究 Ⅳ.①O413.1

中国版本图书馆 CIP 数据核字（2016）第 153949 号

跨越时空的骰子

量子通信、量子密码背后的原理

[瑞士] 尼古拉·吉桑 著

周荣庭 译

上海世纪出版股份有限公司
上海科学技术出版社 出版

（上海钦州南路 71 号 邮政编码 200235）

上海世纪出版股份有限公司发行中心发行

200001 上海福建中路 193 号 www.ewen.co

上海商务联西印刷有限公司印刷

开本 635×965 1/16 印张 11.25

字数 120 千字

2016 年 8 月第 1 版 2016 年 8 月第 1 次印刷

ISBN 978-7-5478-3134-2/N·114

定价：28.00 元

致　谢

感谢我的学生和合作者，和他们的交流对本书的完成有很大促进。我还要感谢阅读本书初始版本并提出意见的其他人，特别是法语版编辑维特科夫斯基（Nicolas Witkowski）。这本书得益于他们的耐心和能力。同样感谢瑞士国家科学基金会以及欧盟，它们对我的实验室提供了慷慨的资助；感谢日内瓦大学，在这里工作是如此诗意。最后，感谢上天给予我的幸运——允许我生活在如此一个对于物理学来说激动人心的时代，并允许我给予这个时代自己谦卑的贡献。

中文序

量子力学是当今物理学基石之一，也是近代自然科学技术和社会经济发展的支柱。1935 年，爱因斯坦等人针对量子力学的完备性提出著名的 EPR (Einstein-Podolsky-Rosen)佯谬：基于局域性和实在性这两个在经典物理学观念中非常合理的假设，利用所谓的“纠缠态”，可以同时精确测量微观粒子的位置和动量，而这与量子力学的“海森堡不确定性原理”不相容。据此，EPR 认为量子力学是不完备的，需要所谓“隐变量理论”，而当时以玻尔为代表的量子论捍卫者则坚持量子力学的完备性。该佯谬自提出之后，就处于哲学争辩的状态，但一直没有实验检验来最终判定。

直到 1964 年，约翰·贝尔(John Bell)提出了著名的贝尔不等式，成为验证上述问题孰是孰非最有力的判据，并使得 EPR 佯谬的实验检验成为可能。贝尔不等式的证明过程非常简洁，但在量子力学基础方面扮演着至关重要的角色，有人甚至认为“贝尔不等式是科学史上最深邃的发现之一”。20 世纪 80 年代初，法国物理学家阿兰·阿斯佩克特(Alain

Aspect)等人首次完成了贝尔不等式实验,人们终于可以用实验来检验 EPR 佯谬。至今为止,仍然有大量关于贝尔不等式各种版本的理论研究和实验检验结果发表。也正是对量子力学基础问题的持续、深入探索,才带来了如今量子信息与量子调控领域的蓬勃发展。

在本书中,著名量子物理学家、瑞士日内瓦大学尼古拉·吉桑(Nicolas Gisin)教授以诙谐的语言、深入浅出地解释了量子非定域性、量子纠缠、量子测不准原理、量子不可克隆定理等量子世界中特有的奇特现象;介绍了上述原理在量子通信领域中的应用,如量子隐形传态、量子密钥分发等;探讨了一些开放性问题,如无漏洞贝尔不等式的检验等。该书是量子信息领域很有价值的科普读物,原始版本为法语,已经先后被翻译成包括英语、德语在内的多种不同语言,适合于量子物理与量子信息领域的学生、青年学者以及其他对此领域感兴趣的读者。

吉桑教授是我的好朋友,自 20 世纪 90 年代初,他带领团队长期从事量子物理基础、量子通信理论与实验、实用化量子密码等方向的研究,是该领域具有重要影响力的科学家。由于在量子信息领域的杰出贡献,他先后于 2009 年、2014 年荣获约翰·贝尔奖(John Stewart Bell Prize)、量子信息领域最高奖——国际量子通信奖(International Quantum Communication Award)及瑞士国家最高奖——马塞尔·伯努瓦奖(Marcel Benoist Prize)。

在书中,吉桑教授介绍了他的团队在量子通信实验领域的一些进展。值得一提的是,我国在量子通信实验领域也取

得了系列具有国际重要影响力的成果。比如，2012 年，中国科学技术大学的团队在国际上率先实现八光子的量子纠缠，并在此基础上完成了百公里量级的自由空间量子隐形传态。2015 年，又首次实现多自由度量子隐形传态等。而在量子通信实用化应用方面，今年我国将建成连接北京、上海的光纤量子通信骨干网“京沪干线”，同时将在国际上率先发射“量子科学实验卫星”，实现高速的星地量子通信并连接地面的城域量子通信网络，初步构建我国的广域量子通信体系。

正如著名物理学家约翰·惠勒(John Wheeler)所言“过去一百年间量子力学给人类带来了如此之多的重要发现和应用，有理由相信在未来的一百年它还会给我们带来更多激动人心的惊喜”，我们相信，随着重大基础科学问题的解决和实验技术的迅猛发展，量子物理将会在诸如量子通信、量子计算与量子模拟、量子精密测量等领域不断地形成新的科学前沿，激发革命性的科技创新，产生重大的科学突破。

潘建伟

2016 年 7 月于合肥

序

“一见钟情!”这是吉桑(Nicolas Gisin)初次接触到贝尔(John Bell)的理论时所说的话。闻知其感受,我的脑海中也浮现出1974年秋日里自己沉迷于贝尔论文时的情形。尽管这篇论文在当时鲜为人知,我却完全明白,这将会是通过实验方式诠释量子力学,解决玻尔(Niels Bohr)和爱因斯坦(Albert Einstein)分歧的关键!

在当时,即便有些物理学家已经知道爱因斯坦、波多尔斯基(Boris Podolsky)和罗森(Nathan Rosen)提出的“EPR佯谬”,却很少有人听说过贝尔不等式,更别说去关注量子力学的基础概念了。1935年发表在《物理评论》(*Physical Review*)上的EPR佯谬论文,在一些大的图书馆里很容易查阅到。而贝尔的那篇论文就没有这份幸运了——它躺在一份不为人知的新期刊上,而那份期刊仅发行了四期便遭遇了停刊的噩运。在那个没有互联网的年代,那些没有发表在主流期刊上的论文只能借助复印机进行传播。在希莫尼(Abner Shimony)的一次来访中[受德帕尼亚(Bernard d'Espagnat)邀请访问奥尔

赛]，我得到了贝尔那篇文章的复印件——复印自光学研究所(Institut d'Optique)的年轻教授英伯特(Christian Imbert)所整理的文件。沉浸在贝尔带给我的震撼中，我决定将自己的博士学位论文聚焦于对贝尔不等式进行实验检验，而英伯特教授也欢迎我在他的麾下工作。

在贝尔清晰无误、让人印象深刻的论文中，我找到了实验者将面临的严峻挑战：当**纠缠的粒子**(entangled particle)从放射源发射到测量区域时，如何改变偏振检测仪的方向？解决这一技术难题的关键是：借助相对论基本原则，即物理效应不能以超光速传播，我们可以避免改变偏振检测仪方向对粒子放射机制或测量方法所造成的影响。通过这样的实验，我们可以精确地检验两种互相冲突的理论到底哪一个是正确的：是玻尔的量子力学还是爱因斯坦所坚守的**局域实在论**(local realism)？局域实在论包含两个基本原则。首先，系统存在**物理实在**(physical reality)；其次，**局域性假设**(locality assumption)成立，即由于相对论基本原则，一个系统不会被遥远空间外的另一个封闭系统内所发生的任何事情立即影响。最终，实验证明量子力学是正确的，并迫使大多数物理学家放弃了爱因斯坦所竭力维护的局域实在论。但是，我们是否就要因此抛弃**实在论**(realism)或者**局域论**(locality)呢？

放弃物理实在的论点无法把我说服，因为我觉得物理学家的使命在于精确地描述这个世界的实在，而不仅仅是预测测量仪器上所呈现的结果。不过，倘若量子力学在这方面被证实了(时至今日，这看似已经确凿无疑)，我们是否该认定，这个明显与爱因斯坦相对论准则相违背的**非局域相互作用**

(nonlocal interaction)是存在的呢？我们能否利用这种**量子非局域性**(quantum nonlocality)来传输有用的信号，比如，以超越光速的速度来点亮一盏灯，或者在证券交易所下个订单？但是，我们还不得不受量子力学另一特性的制约，即**基本量子非决定论**(fundamental quantum indeterminism)。这个理论认为，在任何具体实验中，我们都不可能左右实验的实际结果，尽管通过量子力学我们可以预见到可能出现的各个结果。可以确定的是，量子力学虽然可以对实验中各种可能结果的概率进行极其精确的计算，但是这些概率仅在相同实验多次重复时才有统计学上的意义。正是这种**基本量子随机性**(fundamental quantum randomness)禁止了信息的超光速传播。

在许多介绍量子物理最新进展的科普读物中，吉桑的这本书清晰地强调了基本量子随机性的关键地位。比如，如果没有基本量子随机性，有朝一日我们可望设计出超光速电报系统！假使我们能发明出这种只有科幻小说里才有的神秘装置，就不得不对以前所有的物理理论进行一次彻底的修正。我不认为有什么不可触碰、无法更改的物理理论。恰恰相反，我本人一直坚信，任何物理理论都有可能被适应领域更广阔的理论所取代。然而，如果要修改一些基石理论，就会引发一场真正意义上影响深远的物理观念变革。虽然人类历史中出现过几次非同凡响的观念变革，但这些根本上的观念变革是极其罕见和震撼的，人们不能轻易希冀这样的奇迹时刻会再次发生。尽管非局域性量子物理充满了奇特之处，吉桑也未曾推翻爱因斯坦相对论中禁止超光速传播的基本法则。我觉

得这是本书很值得注意的一个重要特征。

在上述问题上，本书坚持如此独特的立场而不是跟着其他科普图书人云亦云，这一点也不让人惊讶。原因是，吉桑在20世纪最后25年那场量子理论革命中是一位关键人物。

第一次量子革命于20世纪初开始，标志是波粒二象性的发现。我们因此能极其精确地描述构成物质的原子，形成金属、半导体内电流的电子云以及构成光束的数以亿计的光子的统计特征。我们也终于能理解固态物质的力学属性，例如由相互吸引的正负电荷组成的物质为何不会自我塌缩，这一点经典物理完全无法解释。量子力学使人们可以对物质的光学性质、电学性质进行精确的定量描述。同时，量子力学也为描述神奇的超导现象和某些基本粒子的独特属性提供了必要的概念框架。在首次量子革命的照耀下，物理学家们发明了晶体管、激光发射器、集成电路等新装置，正是这些发明引领我们步入了现今的信息时代。

到了20世纪60年代，物理学家们开始追问在第一次量子物理革命中被搁置的两个问题：

第一个问题：我们如何把可以做出精确统计预言的量子物理运用到单个微观粒子？

第二个问题：量子物体的**纠缠对**(entangled pair)的惊人特性是否真的与自然规律相一致？它在1935年的EPR论文上被描述过，却从未被观测到。我们在这个问题的探索上是不是触及到了量子力学的边界？

这些问题的答案，先由实验物理学家给出，随后理论物理学家对其加以完善。这一系列工作引发了第二次量子革命，

并持续至今！

单个量子的行为是目前物理学家们热烈讨论的焦点议题。在过去相当长一段时间里，大部分物理学家都认为这个问题没有什么意义，也不重要，因为尝试观测单个量子已是不可思议的事了，更别提去控制它，操纵它了。引用薛定谔(Erwin Schrödinger)的话：

> "……完全可以说，就像我们不能在动物园里养鱼龙[①]一样，我们难以对单个微观粒子开展实验研究。"

20世纪70年代是转折点，实验物理学家设计出了观测和操控像电子、原子、离子这样的单个微观粒子的实验方案。我一直对1980年于波士顿举行的原子物理国际大会上人们所表现出的热情记忆犹新。当时托谢克(Peter Toschek)展示了第一张单个囚禁离子的成像图片——该种离子在激光照射下会发射荧光光子，实验中便是据此成像的。从那时起，实验上的不断进展使得观测者能直接观测到量子的跃迁，这让数十年的论战画上了句号。这个故事表明，只要能正确解释计算上的概率结果，量子理论可以完美地描述单个量子的特征。

第二个问题和量子纠缠这一特性有关。关于这个特性的量子理论预测首先通过基于**光子对**(pair of photons)的实验获得了检验；随后一系列努力把实验场景逐步推进到了贝尔等理论物理学家所追求的理想状态。无论这些实验看起来多么不可思议，它们却非常一致地验证了量子理论的有效性。

---

① 鱼龙，大型海栖爬行动物，最早出现于2.5亿年前，于9 000万年前灭绝。——译者注

在20世纪80年代，吉桑不仅组建了一个研究光纤的应用物理团队，而且一直保持着对量子力学基础问题的强烈个人兴趣和理论上的执着追求。因为当时对这类问题开展研究尚未被视为有价值的工作，他还要对项目负责人保密，至少是保持低调。所以，他成为首批对光纤中光子对的纠缠现象进行检验的实验物理学家之一是再正常不过的事了。凭借博学的光纤技术知识，吉桑可以很好地使用日内瓦周边的商业电信光纤网络来展示相距几十公里依然存在的量子纠缠性，这让参加实验的人员也颇感意外。通过一些基于基础概念的简单实验，他证实了遥远物体间能发生纠缠，并让**量子隐形传态协议**(quantum teleportation' protocol)投入应用。他既是量子基础方面的优秀理论家，也是光纤应用方面的专家，因此，他成为首批将量子纠缠性应用于**量子密码**(quantum cryptography)和**真随机数**(truly random number)生成的科学家之一。

我们能在这本充满奇幻的书中发现吉桑的智慧所在。他用对大众来说浅显易懂的语言来描述量子物理中最特殊、最难以琢磨的问题(这一点是冒险的，而他成功了)，并且避免使用数学公式。他解释了什么是量子纠缠、量子非局域性以及**量子随机性**(quantum randomness)，同时还为我们展示了与这些理论相关的应用。但是，这本书又不仅仅是一本科普书，专业量子物理学者也可以就其中一些现象进行深层次的讨论，正如吉桑所强调的：我们还远没有搞清万物运行的机制以及运行结果。那么，即使局域实在已被实验否定，我们是否就要抛弃物理实在或者局域性呢？对于这个问题，我跟吉桑

处于同一个战壕：局域论和实在论曾经密不可分，并且作为同一个理论在逻辑上是自洽的，那么将它一分为二并坚持其中之一也就是不可取的。如果某个局域的系统会立即受到空间上相互隔离的另一系统的影响，我们该如何定义这个局域系统中物理实在的独立性？这本书为我们提供了较为温和的解决方法。如果基础量子随机性存在，那么非局域性物理实在就能和爱因斯坦的相对论共存了。

即使了解这些问题的物理学家们也将在吉桑的书中找到让他们思考更上一层楼的资料；而一般读者在世界上最优秀的前沿专家的精心指引下，将直入问题的精妙之处，欣赏到量子纠缠和量子非局域性的神奇特性。

阿兰·阿斯佩克特（Alain Aspect）[①]

2012年5月于帕莱索

① 法国物理学家，完成了贝尔不等式的第一个实验检测。曾获得沃尔夫物理学奖、爱因斯坦奖章等。——译者注

前 言

如果你生活在牛顿学说盛行的年代，你会想了解当时发生的一切么？

而当今的量子物理给世界带来的震撼与那时经典力学所引起的震撼是差不多的。现在，我们有机会去体验这种震撼。

这本书能帮助你了解现今发生的一切；书中没有繁琐的数学公式，却并未试图去规避量子物理概念的难以理解之处。探索物理学理论所能预言的结论或者精确地去进行理论预言，物理学家需要借助于数学；然而数学不足以呈现出物理那无尽的内涵。因为物理最吸引人的一点不是数学，而是它的概念。在物理中关键不是公式计算，而是理解。

这本书中的某些章节需要读者们认真开动脑筋，努力去理解。每个人都会有所理解，没有人会全部理解！在这个领域中，理解基础概念会很艰难。不过，我打赌你们所有人都能理解这场我们正在进行的概念革命的部分内容，并且会因理解而身心愉悦。为此，需要有以下心理准备：并不是所有的内容都是简单明了的；不要时常给自己“我根本搞不明白物

理!”的暗示。

如果某个章节对你来说太难了,请继续阅读下去,后面的内容可能会点醒你。这样或许你会理解,我那些追寻灵感的物理学同事们为何能从这本书中得到那么多的乐趣。如果必要的话,翻回前面,重新阅读那些曾让你困惑的章节。告诉自己:重要的不是读懂一切,而是要有全局的视野。这样到最后,你能发现你不借助数学知识,就已然对量子物理有了很大程度的理解。

对量子物理的讲述总是充满了长篇累牍的说教和含糊其辞的哲学评论。为了避免这种误区,除了“基本事实”以外我们什么都不借助。当物理学家做实验时,他们是在对永恒的实在进行探寻。物理学家会决定提出什么问题,以及什么时候提出。比如研究一个发着红光的灯泡时,物理学家不会纠结于灯光到底是不是真是红色的,或者这来源于一种错觉。他们会认为:灯泡是红的,仅此而已。

在阅读中,你会在不同章节中读到一些轶事。同时,我的教学经历告诉我,应当在不同的情境或章节中重复一些要点。最后,我在这本书中评判前人的历史或成就并不是出于自负。我对那些大名鼎鼎的前辈们的评论只是我个人的看法,这些看法是建立在我人生中三十多年的专业物理生涯之上作出的判断。

导 读

从小开始，我们就知道该如何接触一个我们够不到的物体：要么我们向它挪动，比如像婴儿那样爬过去；要么我们得用一个物件，比如说一根木棒，作为我们延长的手臂触碰它。后来，我们了解到，更复杂的机制也是同一原理。比如：把一封信放进信箱，信会先由邮递员集中起来，手工分类或者用机器分类，接着装上大货车、火车或者飞机，然后运往目的地。网络、电视以及其他数不胜数的日常案例告诉我们：任何两个相隔的物体之间的相互作用总是从一点到另一点连续发生的——这些传播方式依据的也许是某些复杂的机理，但是这些传播都是连续的，我们能在空间和时间中定位其轨道，至少原理上是可以的。

然而，量子物理，这种研究我们日常感知世界之外的学科，断言相互之间距离很遥远的物体有时能构成一个整体。这样，尽管两个物体被遥远的空间所分割，如果我们触碰两个物体中的一个，这两个物体都会振动！如何才能相信这种事情？能对这样一个观点进行实验验证么？我们需要搞清其原