双缝干涉实验恐怖吗？恐怖在哪？

> 这是有史以来第一次，人类在科学实验中正式遭遇「灵异事件」。

116 年前的 12 月 12 日，马可尼收到横跨大西洋、人类史上第一个无线电信号的那一天。

似乎什么都没有改变。

包括马可尼自己，当时没有人能够想象，在接下来的一百多年，通信会把世界变成什么样子。

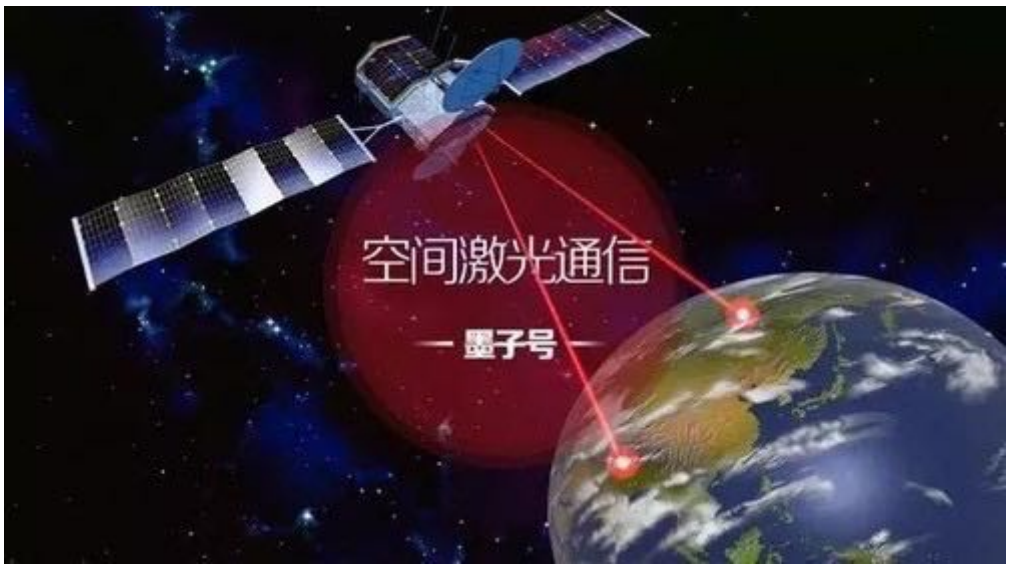
2016 年 8 月 16 日，世界第一颗量子通信卫星「墨子号」从酒泉发射的那一天。

就像当年的马可尼一样，我们也无从想象，未来的量子计算与量子通信，终将带来一个怎样的魔法时代。

绝对安全的信息传输?

智商秒杀全人类的人工智能?

瞬移、穿越不再是科幻?



潘建伟教授的量子通信卫星上天了。

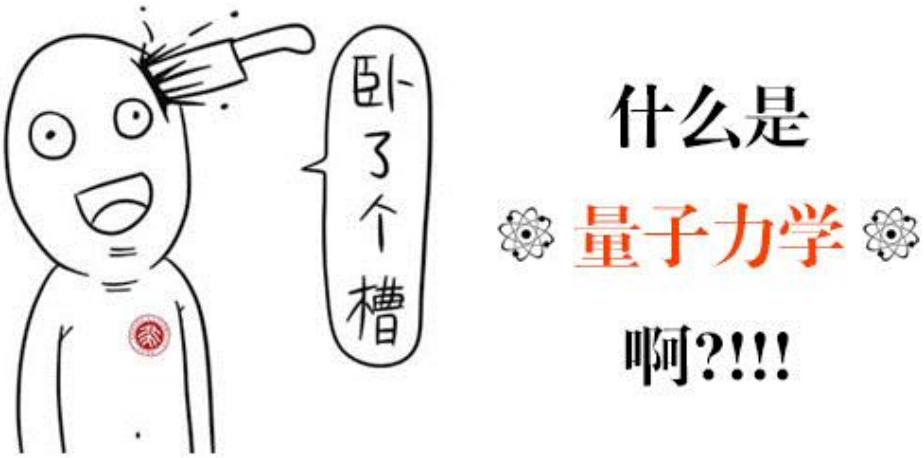
5 年后，人人都会用无法破解的加密网络刷信用卡。你还觉得量子理论是象牙塔里的黑科技，和你的生活毫无关系？

让我们先从神秘的量子理论开始，解密量子通信。

这注定是一场不可思议的旅程。

如果你完全不懂量子力学，请放心大胆地往下看，我保证不用任何公式就能让你秒懂，连 1+1=2 的幼儿园数学基础都不需要。

如果你自以为懂量子力学，请放心大胆地往下看，我保证你看完会仰天长叹：什么是量子力学啊？



正如量子力学大师费曼所说：没有人懂量子力学。如果你觉得懂了，那肯定不是真懂。

在烧脑、反直觉和毁人三观方面，没有任何学科能够和量子力学相比。如果把理工男最爱的大学比作霍格沃兹魔法学校，那么唯一和量子力学专业相提并论的，只能是黑魔法。

然而，量子理论之所以如此神秘，并不是因为物理学家的故弄玄虚。其实，在量子理论刚诞生的摇篮时期，它只是一门人畜无害的学科，专门研究电子、光子之类小玩意儿。

而 「量子」 这个现在看来很厉害的名字，本意不过是指微观世界中「一份一份」的 不连续能量 。

这一切，都源于一次物理学的灵异事件。

百年战争

20 世纪初，物理学家开始重点纠结一个纠结了上百年的问题：光，到底是波还是粒子?

- 粒派

所谓粒子，可以想象成一颗光滑的小球球。

每当你打开手电，无数光子就像出膛的炮弹一样，笔直地射向远方。

很多著名科学家（牛顿、爱因斯坦、普朗克）做了很多权威的实验，确凿无疑地证明了光是一种粒子。

- 波派

所谓波，就像往河里扔块石头，产生的水波纹一样。

如果把光看作是一种波，可以完美解释干涉、衍射、偏振等经典光学现象。

很多著名科学家（惠更斯、杨、麦克斯韦、赫兹）做了很多权威的实验，确凿无疑地证明了光是一种波，电磁波。

可问题是，波和粒子毕竟是两种截然不同的东西啊！

- 粒子可分成一个一个的最小单位，单个粒子不可再分；波是连续的能量分布，无所谓「一个波」或者「两个波」；
- 粒子是直线前进的，波却能同时向四面八方发射；
- 粒子可以静止在一个固定的位置上，波必须动态地在整个空间传播。

波与粒子之间，存在着不可调和的矛盾。

于是自古以来，塞伯坦星上的科学家就分成两派： 波派和粒派，两派之间势均力敌的百年撕逼战争从未分出胜负。

很多人问我：科学家为什么要为这种事情势不两立，大家搁置争议、共同研究不就得了。

为了一个字：

信仰!

千面之神

且问你：《权力的游戏》中，信奉七神的维斯特洛人民，为何要与信奉旧神的关外野人拼个你死我活?

自古以来，人们为了信仰争端大开杀戒，早已不足为奇。

唯一的和谐社会可能是古希腊：他们的神多达百八十号，有管天上、有管地下，各路神仙各司其职，倒也井水不犯河水。

人称：希腊众神。

要命的是，科学家们信仰的神只有一个，而且是放之宇宙而皆准的全能大神。这位神祇的名字，叫作 真理 。

大到宇宙的诞生，小到原子的运转，科学家们相信，这个世界的万事万物都是基于同一个规律，可以用同一个理论，甚至同一套方程解释一切。比如，让苹果掉下来把牛顿砸晕的是万有引力，让月亮悬在空中掉不下来的也是万有引力。用同一个方程，既能算出地球的质量，也能让马斯克的猎鹰九号火箭上天，这就是科学的威力。

想要一个宇宙、两种规律？

对不起兄弟，别在科学界混了，您可以去跳个槽，比如竞选总统。

当然，科学家们没有谁敢自称是真理的代言人，就连牛顿谦虚起来都是这样的：「我只是一个在海滩上捡贝壳的孩子，而真理的大海，我还没有发现啊！」

就算是捡贝壳，捡的多了，说不定拼到一起就能窥见真理之神的全貌呢！

整个科学史，就像一个集卡拼图的过程。做实验的科学家们每发现一个科学现象，搞理论的科学家们就绞尽脑汁推测它背后的运行规律。不同领域的大牛把各方面的知识、理论慢慢拼到一起，真理的图像就渐渐清晰。

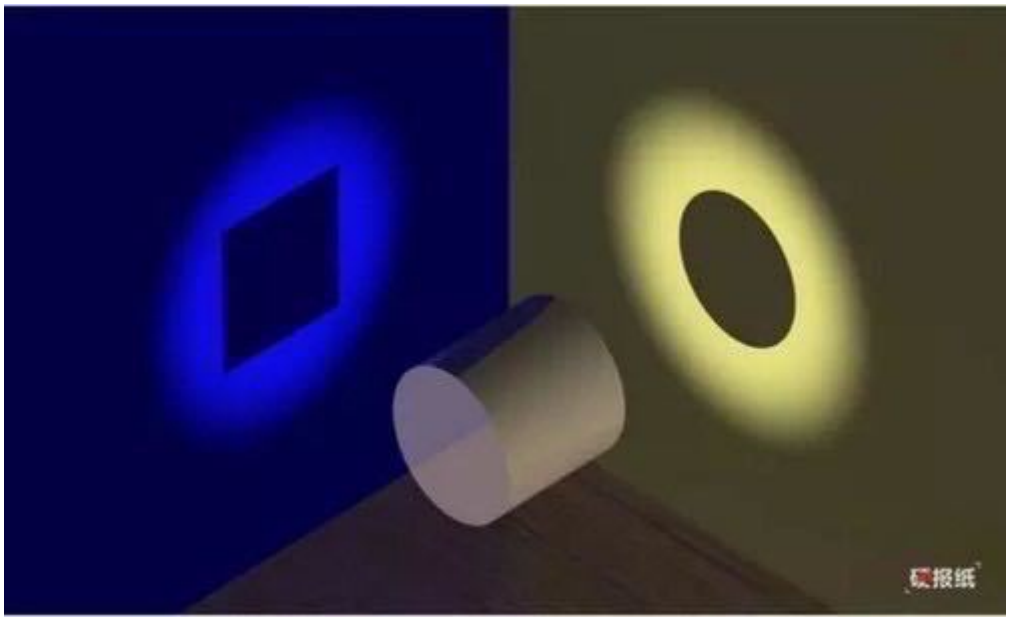
在 20 世纪初，光学的知识储备和数学理论越来越完善。大家逐渐觉得，这一块的真相总算有希望拼出来了——结果却发现，波派和粒派的理论早已背道而驰，还各自越走越远。这就好比你集了一辈子卡片，自以为拼得差不多了。这时突然发现，你拼出的图案居然和别人是不一样的，而且差的不是一点点！

是不是有种把对方连人带图都砸烂的冲动？

当时波派和粒派都坚信，自己手上的拼图，才是唯一正确的版本。

双方僵持不下直到 1924 年，终于有人大彻大悟： 波 **or** 粒，为什么光不能两者都是呢？

也许在某些时候，粒子看起来就像是波；在另一些时候，波看起来就像是粒子。波和粒如同阴阳一般相生相克，就像一枚硬币的正反两面（波粒二象性），只不过我们一直以来都在盲人摸象、各执一词。



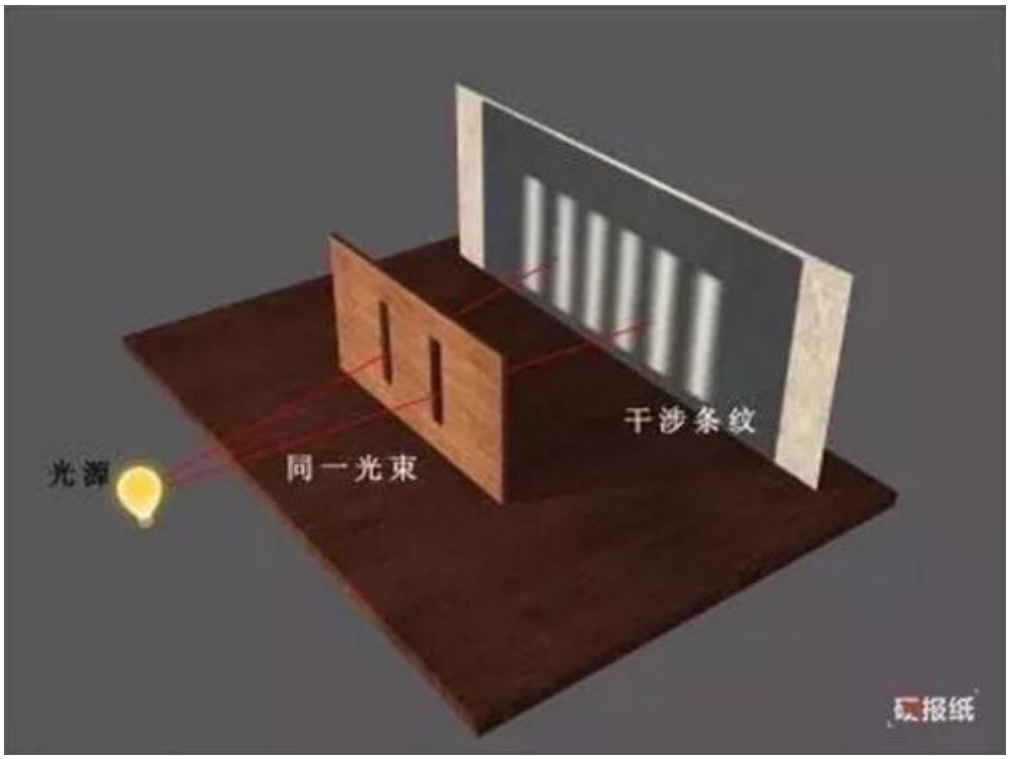
真理确实只有一个，但是真理的表现形式，会不会存在着多个版本？

难道真理就是那个千面之神，用千变万化的面目欺骗了我们如此之久？

灵异的实验

究竟是波，是粒，还是波粒二象，大家决定，用一个简单的实验来做个了断：

- 双缝干涉实验



双缝，顾名思义，就是在一块隔板上开两条缝。

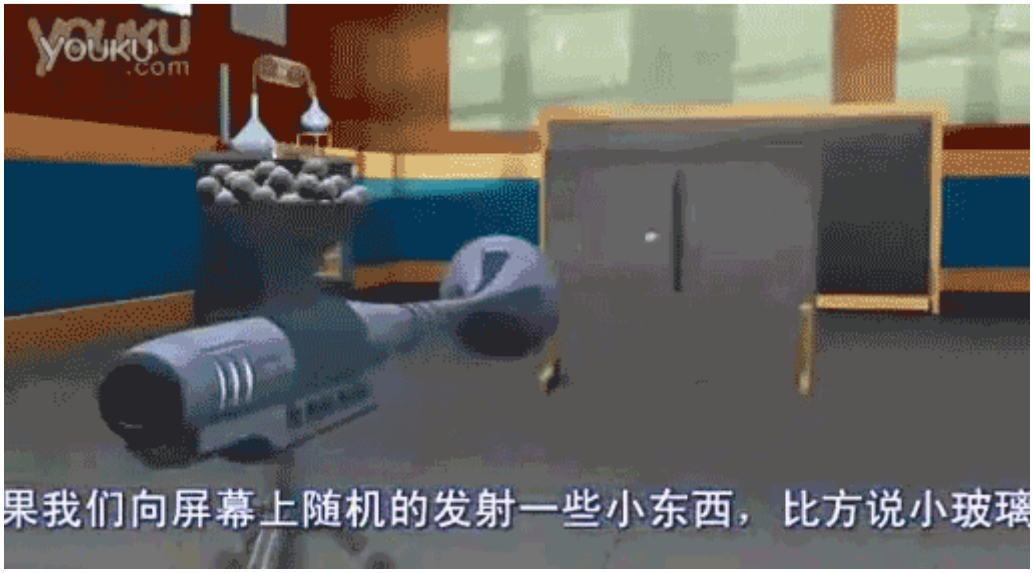
用一个发射光子的机枪对着双缝扫射，从缝中漏过去的光子，打在缝后面的屏上，就会留下一个光斑。（等效于 1961 年电子双缝干涉实验）

在实验之前，科学家的推测如下：

第一种可能

如果光子是纯粒子，那么屏幕留下两道杠。

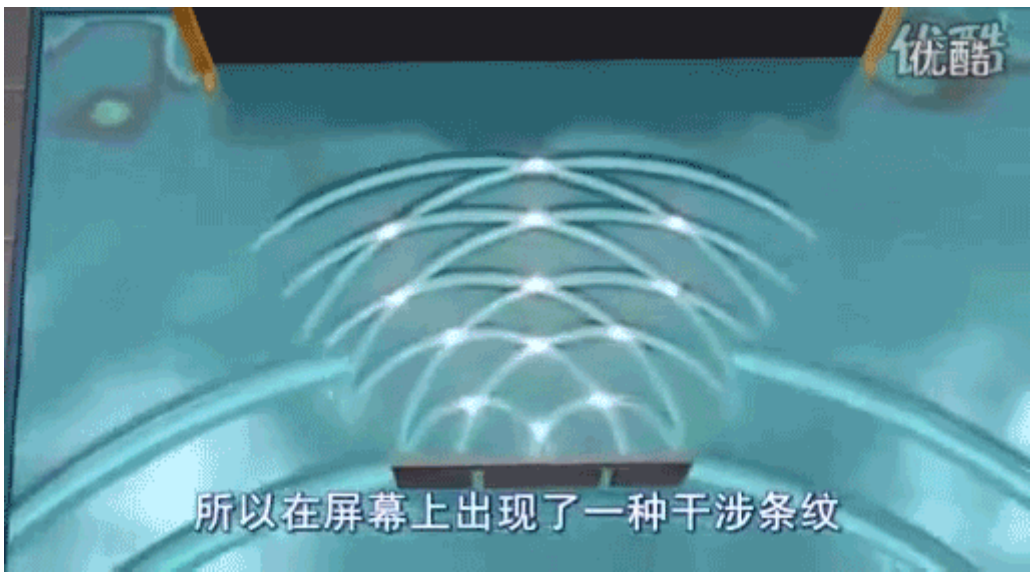
光子像机枪发射的子弹一样笔直地从缝中穿过，那么屏幕上留下的一定是 2 道杠，因为其他角度的光子都被板挡住了。



第二种可能

如果光子是纯波，那么屏幕上会留下斑马线般的一道道条纹。

光子穿过缝时，会形成 2 个波源。两道波各自震荡交汇（干涉），波峰与波峰之间强度叠加，波峰与波谷之间正反抵消，最终屏幕上会出现一道道复杂唯美的斑马线（干涉条纹）。



第三种可能

如果光子是波粒二象，那么屏幕图案应该是以上两种图形的杂交混合体。

总之，

两道杠 = 粒派胜；

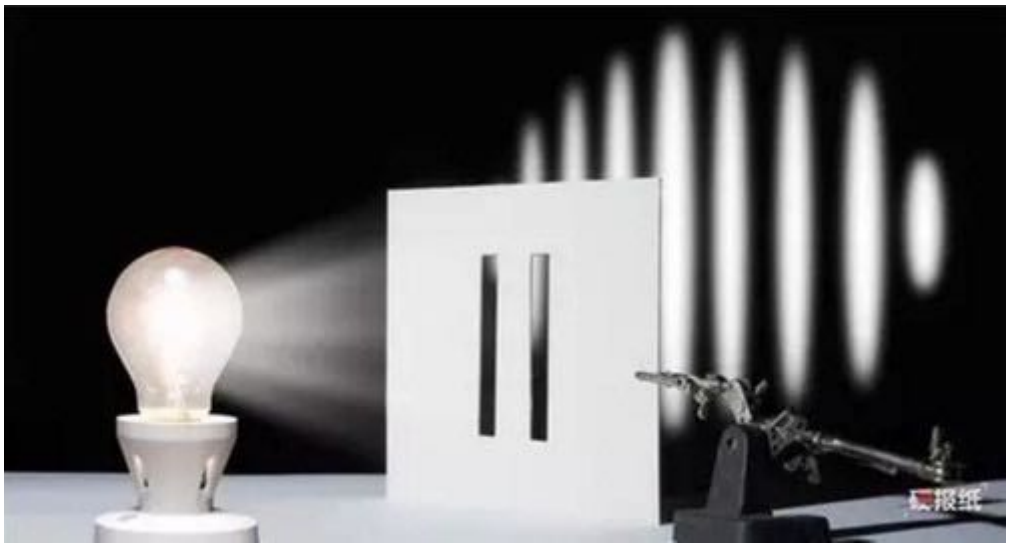
斑马线 = 波派胜；

四不像 = 平局。

是波是粒还是二合一，看屏幕结果一目了然，无论实验结果如何，都在我们的预料之中。

第一次实验：把光子发射机对准双缝发射。

结果：标准的斑马线。



根据之前的分析，这证明光子是纯波。OK，实验结束，大家回家洗洗睡吧。

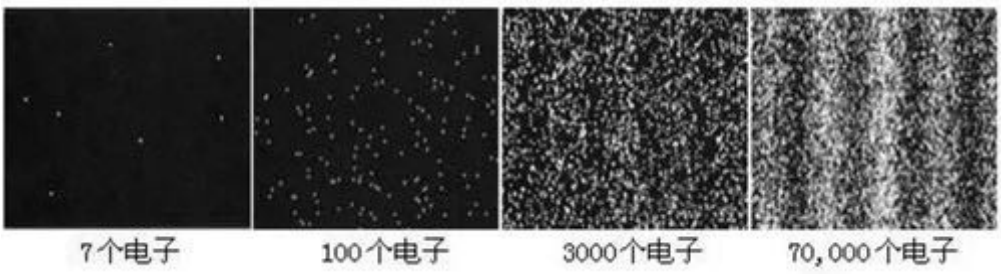
粒派不服：我明明知道光子是一个一个的粒子！

这样，我们再做一次实验，把光子一个一个地发射出去，看会怎么样，一定会变成两道杠的！

第二次实验：把光子机枪切换到点射模式，保证每次只发射一个光子。

结果：斑马线，竟然还是斑马线，怎么可能？我们明明是一、个、一、个把光子发射出去的啊！

最令人震惊的是，一开始光子数量较少时，屏幕上的光点看上去一片杂乱无章，随着积少成多，渐渐显出了斑马线条纹！



光子要真的是波，那粒派也不得不服。

问题是：根据波动理论，斑马线来源于双缝产生的两个波源之间的干涉叠加；而单个光子要么穿过左缝、要么穿过右缝，穿过一条缝的光子到底是在和谁发生干涉？

难道……光子在穿过双缝时分裂成了两个？一个光子分裂成左半光子和右半光子，自己的左手和右手发生了关系？事情好像越来越复杂了。干脆一不做二不休，我们倒要看看，光子究竟是怎样穿过缝的。

第三次实验：在屏幕前加装两个摄像头，一边一个左右排开。哪边的摄像头看到光子，就说明光子穿过了哪条缝。同样，还是点射模式发射光子。

结果：每次不是左边的摄像头看到一个光子，就是右边看到一个。一个就是一个，从来没有发现哪个光子分裂成半个的情况。

大家都松了一口气。 光子确实是一个个粒子，然而在穿过双缝时，不知怎么就会变形成两道波同时穿过，形成干涉条纹。

虽然诡异了些，不过据说这就是 波粒二象性 了，具体细节以后再研究吧，这个实验做得人都要精分了。

然而，就在这时，真正诡异的事情发生了……

人们这才发现，屏幕上的图案，不知什么时候，悄悄变成了两道杠！

没用摄像头看，结果总是斑马线，光子是波；

用摄像头看了，结果就成了两道杠，光子变成了粒子。

实验结果取决于看没看摄像头？

这不科学啊，做物理实验竟然见鬼了啊！

可以体会物理学家当时的心情吗？

一个貌似简单的小实验做到这份上，波和粒子什么的已经不重要了，重要的是现在全世界的科学家都懵逼了。

这是有史以来第一次，人类在科学实验中正式遭遇灵异事件。

观察者魔咒

你还没看出灵异在哪里？

好吧，请先看懂下面这个例子：

电视里正在直播足球比赛，一个球员起脚射门——

「咔」暂停，你预测一下这个球会不会进？

在球迷看来： 球进还是不进，和射手是不是 C 罗、梅西有关，和对方门将的状态有关，和裁判收没收钱说不定还有关。

在科学家看来： 有关的东西更多，比如球的受力、速度和方向，距离球门的距离，甚至草皮的摩擦力、球迷吼声的分贝数等等。

不过，只要把这些因素事无巨细地考虑到方程里计算，完全可以精确预测三秒后球的状态。但无论是谁，大家都公认的是，球进与不进，至少和一件事情是绝对无关的：

你家的电视。

无论你用什么品牌的电视，无论电视的屏幕大小、清晰度高低、质量好坏，无论你看球时是在喝啤酒还是啃炸鸡，当然更无论你看不看电视直播——该进的球还是会进，该不进就是不进，哪怕你气得把电视机砸了都没用。

你是不是觉得，上面说的全都是废话？那么，仔细听好：

双缝干涉的第三次实验证明了，在其他条件完全相同的情况下，球进还是不进，直接取决于在射门的一瞬间，你看还是不看电视！

看还是不看，这是一个问题！

光子从发射器射向双缝，就好比足球射向球门；用摄像头观测光子是否进缝、怎么个进法，就好比用电视机看进球。

第三次实验与第二次的唯一区别，就是实验 3 开了摄像头观察光子（看电视），实验 2 没放摄像头（不看电视）——两次实验的结局竟截然不同。

这，就是观察者的魔咒。

难道说，不看光子它就是波，看一眼，它就瞬间变成粒子？

难道说，「光子是什么」这一客观事实，是由我们的观察（放不放摄像头）决定的？

难道说，对事物的观察方式，能够改变事物本身？

三观崩塌

在所有人懵逼的时候，还是有极少数聪明人，勇敢地提出了新的理论： 光子，其实是一种智能极高的外星 AI 机器人。

之所以观察会导致实验结果不同，是因为光子在你做实验之前就悄悄侦查过了，如果发现有摄像头，它就变成粒子形态；如果发现是屏幕，就变成波的形态。

这个理论让我想起了传说中的：

难道机器人阿童木真的存在？（「阿童木」是日语「アトム」的发音直译，词语源自英语「Atom」，意即「原子」）

这种扯淡理论居然没被口水喷死，还要做实验去验证它，可见科学家们已经集体懵逼到了什么地步。

第四次实验：

事先，只有屏幕没有摄像头；

我们算好光子穿过缝的时机，等它穿过之后，再以迅雷不及掩耳之势加上摄像头。（等效于 1978 年惠勒延迟选择实验）

结果是啥?

无论加摄像头的速度有多快，只要最终加上了摄像头，屏幕上一定是两道杠；反过来，如果一开始有摄像头，哪怕在最后一刻秒秒钟撤掉，屏幕上一定是斑马线。

回到看球赛的那个例子，就好比：我先闭上眼睛不看电视，等球员完成射门、球飞出去 3 秒钟后，我突然睁开眼睛，球一定不进，百试百灵。

在你冲出门去买足彩之前，我先悄悄提醒你：这种魔咒般的黑科技，目前只能对微观世界的基本粒子起作用。要用意念控制足球这样的大家伙，量子还做不到啊！

请注意，加不加摄像头，是在光子已经穿过双缝之后再决定的。不管光子在穿缝的时候变成什么形态，过了缝应该就定型了。

既然光子的状态在加摄像头之前就定型了，为什么实验结果还是能在最后一刻发生变化？

难道说，在之后做出的人为选择（未来），能够改变之前已经发生的事实（历史）？

而且，加摄像头的速度，可以做到非常快（40 纳秒）。就算光子真的是个狡猾的微型变形金刚，当它变成波的形态穿过双缝，在最后一刻却发现面前是一个摄像头时，它也来不及再次变身了吧？

「主观决定客观」「未来改变历史」「外星人其实是无处不在的光子」……

好端端一个实验弄得谣言四起，物理学家们纷纷感到几百年来苦心经营的科学体系正在崩塌。

与之一起崩塌的，还有全人类的三观。

量子魔法时代的大幕，正在徐徐拉开。

为了一只猫的死活，100 年前的天才哲学家，学历最高的足球运动员，撩妹无数的量子力学教授……他们都在纠结个啥？

另一些人，却恰恰相反——他们做任何事，都是为了纠结，下面我要说的，就是另一些人的故事。

学历最高运动员

1908 年夏天。

丹麦，哥本哈根。

一名足球运动员正在思考自己的前程。

23 岁，是时候做个决定了。比自己小两岁的弟弟，已经成为国奥队的中场核心。在刚刚结束的伦敦奥运会上，哈那德·玻尔率丹麦队 17：1 血洗法国队，斩获银牌创造「丹麦童话」，一夜之间成为家喻户晓的球星。

而我，作为丹麦最强俱乐部——哥本哈根 AB 队的主力门将，居然从未入选国家队，这简直是一种耻辱。

国家队大名单里怎能没有我?

教练说我什么都好，唯一的弱点是喜欢思考人生。

上次和德国米特韦达队踢友谊赛，对手竟敢趁我在门框上写数学公式的时候，用一脚远射偷袭，打断我的思路！最后一刻不还是被我的闪电扑救解围，要是后卫早点上去堵枪眼，那场球踢完就可以交作业了。

是成为世界最伟大的门将，还是成为世界最伟大的物理学家，这是一个问题，我需要纠结一下。

第一章里我们讲到，100 多年前，为了搞清光子究竟是波还是粒子，科学家们被一个貌似简单的「双缝干涉」实验弄到集体「精分」。

这个实验明白无误地说明，光子既可以是波，也可以是粒子。

至于它到底是什么，取决于你的 观测姿势 。

装摄像头观测光子的位置，它就变成粒子；不装摄像头，它就是波！

我们曾经天真地以为，无论用什么样的姿势看电视直播，都不可能影响球赛结果，可是在微观世界中，这个天经地义的常识好像并不成立，这就是那么多高智商理工男懵逼的原因。

但是在玻尔看来，将宏观世界的经验常识套用到微观世界的科学研究上，纯属自寻烦恼。

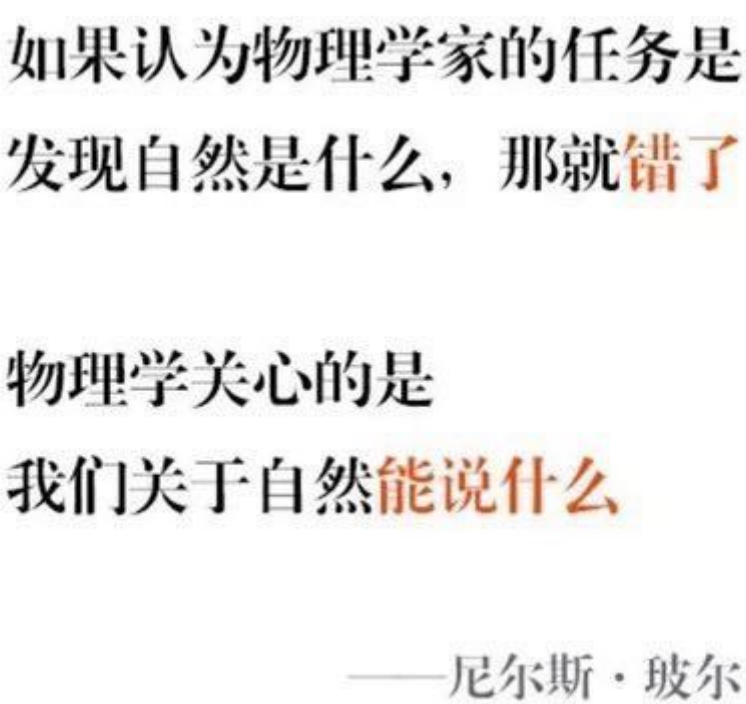
通过常识，我们可以理解一个光滑小球的物理属性；但是凭什么断定，组成这个小球的万亿亿亿个原子，也一定有着和小球完全相同的属性？

凭什么在微观世界中，原子、电子、光子，一定要遵循和宏观世界同样的物理法则？

一般人纠结的问题无非是：量子世界的物理法则为什么这么奇怪啊……

只有天才，能够直截了当问出关键问题：这些法则是什么？

严格来说，量子理论是一群人，而不是一个人创立的。但是如果一定要选出一个「量子力学代言人」的话，我觉得非玻尔莫属，因为当别人纠结的时候，他第一个想通了。



通过前面那些烧脑的实验，玻尔总结了量子世界的三大基本原则：

- 态叠加原理

在量子世界，一切事物可以同时处于不同的状态（叠加态），各种可能性并存。比如，在双缝干涉实验中，一个光子可以同时处在左缝和右缝。这种人类无法想象的叠加态，才是最普通不过的本质形态；而在我们看来「正常」的非黑即白，才是一种特例。

- 测不准原理

叠加态是不可能精确测量的。比如，精确测出了粒子的位置，但它的速度却永远测不准！这并不是因为仪器精度不够高，其实，仪器再好都没用。这个不可能是被宇宙规律所禁锢的「不可能」，而非「有可能但目前做不到」。

- 观察者原理

虽然一切事物都是多种可能性的叠加，但是，我们永远看不到一个既左且右、又黑又白的量子物体。只要进行观测，必然看到一个确定无疑的结果。至于到底看到哪个态则是随机的，其概率高低取决于叠加态中哪个态的成分居多。

这样一来，实验解释起来就轻松多了：

「双缝干涉」实验的官方解释：

没装摄像头：光子在未观测的情况下处于「多种可能性并存」的叠加态，以 50% 的概率同时通过了左缝和右缝，形成干涉条纹；

装上摄像头：光子被观测后只能处于一个态，不能神奇地同时穿双缝了，所以干涉条纹就消失了。

这就是目前量子力学教科书上的正统理论：哥本哈根解释。

终于，一切都有了答案。

有了答案吗?

因为完美解释了双缝干涉等灵异现象，玻尔一（四）夜（面）成（树）名（敌）。

但小伙伴们却纷纷表示：这个理论不仅反直觉反人类，而且 bug 点很多!

比如，没有观测时，光子是混沌中的叠加态；观测的一瞬间，光子就变成了单一的确定态，请问两种态是怎样无缝切换的?

按照玻尔的说法，观测的一瞬间，光子就随机蜕变成多种可能中的一种，还把这个过程取名叫 「塌缩」 。具体怎么个塌法，玻尔自己也说不清。

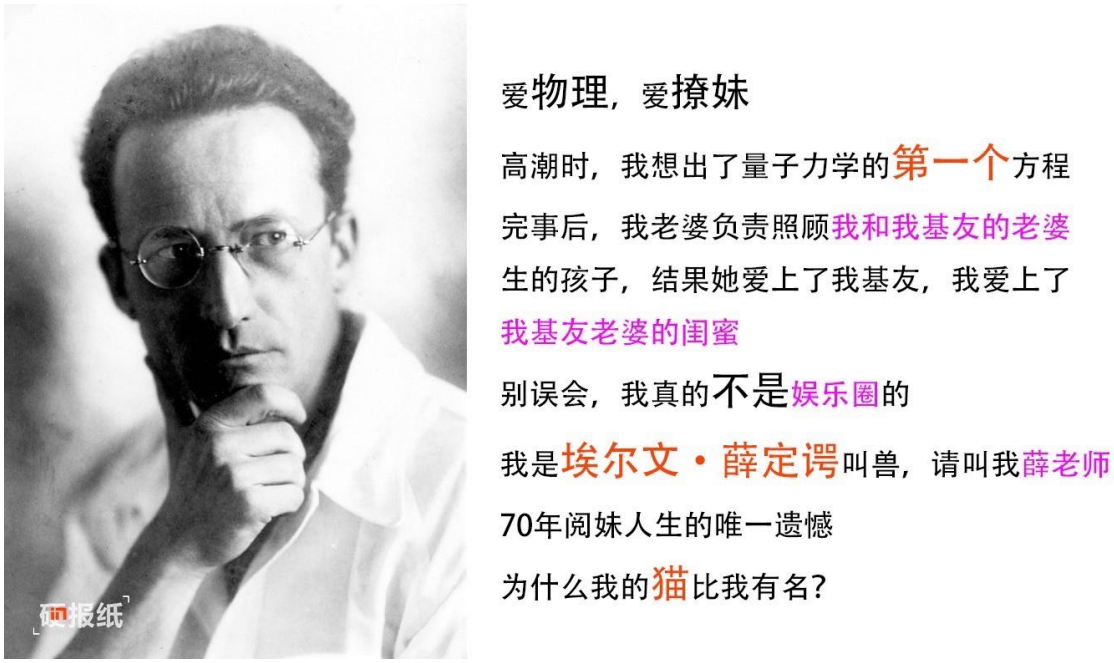
再比如，既然触发「塌缩」的前提是「观测」，那么谁能够成为合格的观察者呢?

科学家、人类、一切生命体、还是包括人工智能在内的任何智慧形态?

众说纷纭之际，给玻尔带来致命一击的，是一只猫。

一只猫的拷问

10 年前，正是薛老师亲手写下了量子波动方程，与矩阵力学、路径积分一起，被后人并称为量子力学的三大基石。



10 年后的 1935 年，对「哥本哈根解释」的群起而攻之，薛老师打响了第一枪。

当时，几乎所有人觉得「叠加态」是个纯属幻想的玩意儿，却没人能真正驳倒玻尔和他的哥本哈根学派。

因为，「态叠加」「测不准」「观察者」无论这三大原理违和感多么强，都被玻尔视作量子世界不可挑战的公理。所谓公理，就像「两点之间有且只有一条直线」，或者牛顿力学三定律一样，是无法、也无须证明的宇宙基本大法。

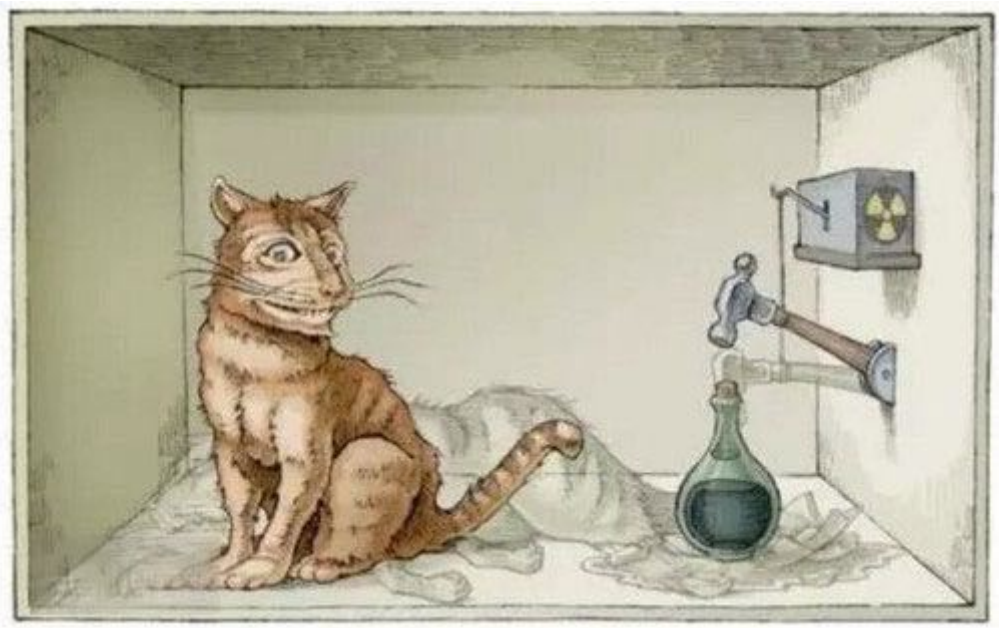
在玻尔看来，物理学家的任务是透过现象找规律，而不是去质问上帝：你为什么要把宇宙设计成这样子？

而且，凭什么微观世界的宇宙法则，一定要和宏观世界的生活经验相符呢?

无懈可击的玻尔之盾，也只有金枪不倒的薛定谔之矛能够与之一战。

「薛定谔的猫」 就是薛老师用来挑战玻尔的头脑实验（以下实验纯属想象、推理，没有任何无辜的猫因此而被害）。

把一只猫关在封闭的箱子里。



和猫同处一室的还有个自动化装置，内含一个放射性原子：如果原子核衰变，就会激发α射线->射线触发开关->开关启动锤子->锤子落下->打破毒药瓶，于是猫当场毙命。

在这个邪恶的连环机关中，猫的死活直接取决于原子是否衰变；然而，具体什么时候衰变是无法精确预测的随机事件。

只要不打开盒子看，我们就永远没法确定，猫此时此刻到底是死是活。

刑具准备完毕，现在，薛老师对玻尔的拷问开始：

1. 原子啊、衰变啊、射线啊，这些都属于你们整天研究的「微观世界」，自然得符合量子三大定律，没错吧？

2. 按照玻尔你自己的说法，在没打开盒子观测之前，这个原子处于「衰变」+「没衰变」的叠加态，没错吧？

3. 既然猫的死活取决于原子是否衰变，而原子又处于「衰/不衰」的叠加态，那是不是意味着，猫也处在「死/没死」的叠加态？

原子衰变 = 死猫；原子没衰变 = 活猫；叠加态原子 = 叠加态的猫。

所以，按照哥本哈根解释，箱中的猫是不死不活、又死又活的混沌之猫，直到开箱那一刻才瞬间「塌缩」成一只死猫或者活猫？

薛老师的逻辑，其实就是反证法：以子之矛，攻子之盾。先假装你是完全正确的，然后顺着你的说法推理啊，直到推出一个荒谬透顶的结论——那只能说明你从一开始就错了！

至于为什么要放进一只猫，这又是薛老师的高明之处。

以前大家研究原子、光子，总觉得那是与日常完全不同的另一个世界；无论量子多么诡异，我们总可以安慰自己说：微观世界的规律，不一定适用于宏观物体。

科学家们做完烧脑的实验，还能回归老婆孩子热炕头的正常生活。

现在，薛老师把微观的粒子和宏观的猫绑在一起，要么你承认叠加态什么的都是不切实际的胡思乱想，要么你承认猫是不死不活的叠加态——别纠结，二选一。

连三岁小孩都知道，如果打开箱子看到一只死猫，那说明猫早就死了，而不是开箱的瞬间才死的——只不过它被毒死的时候，你装作没听到惨叫声而已。

你的理论告诉我们，猫在被观测前是不死不活的；那么，如果把你关进一个密室，你不也变成不死不活了吗？或者，在密室中的你看来，全世界的人都是不死不活的僵尸态？还是说，地球和太阳是否存在，都变成不确定的了？

薛老师的猫，本意是想让玻尔下不了台，万万没想到，这只猫却引发了唯心、唯物主义的大辩论。

哲学家们突然发现，终于有机会以专家的身份，来对科学界说三道四了。

「我思故我在」的误会

400 年前，一个法国大叔的思考，奠定了唯心主义哲学的核心思想。

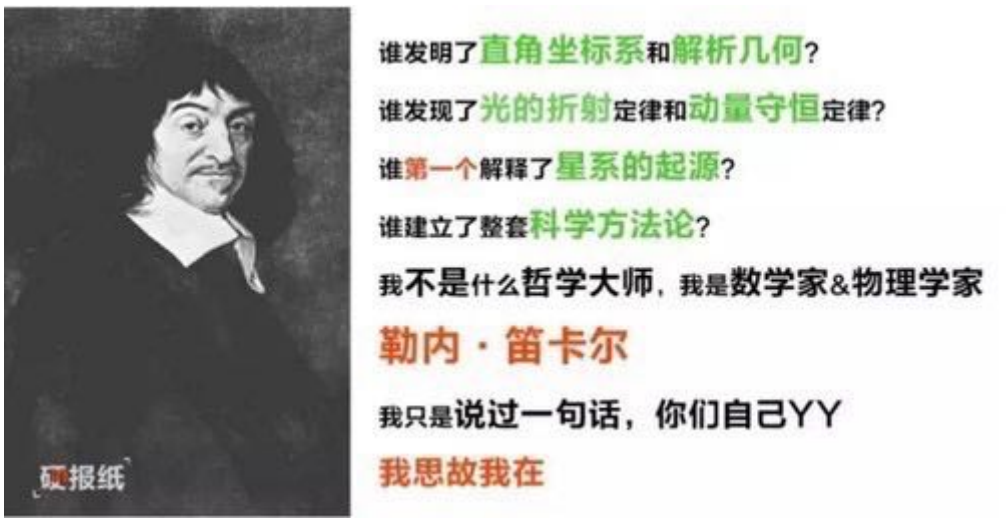
假设世间一切都是幻觉，所谓人生，也许只是我们的大脑在黑客帝国的 AI 里做的一个梦，说不定身体正插满管子泡在培养皿中。

那么问题来了：如果一切都可能是幻觉，那么，还有没有绝对不是幻觉的东西呢？

有。

唯一不可能是幻觉的，只有「我们正在思考世界是不是幻觉」这件事。

我在思考，至少说明我还是个东西。



其实，唯心主义并不是「我想要什么存在它就存在」，而是「只有我的意识（心）无可置疑，世界却可能是幻觉」。所

以，如果你认真看那些唯心主义哲学大师的著作，会发现他们的逻辑严密得令人发指。

而唯物主义者的观点则是「我在故我思」：世界肯定不是幻觉，不过每个人都把自己版本的幻觉当作客观世界的真相。但是，到底哪一个世界观才对呢？

由于唯物主义者无法证明这个世界一定不可能是黑客帝国，而唯心主义者也拿不出这个世界一定就是黑客帝国的确凿证据，所以谁也无法说服对方。

直到唯心主义者们听说了量子力学。

这么说来，主张「心外无物」的明代哲学家王阳明，早在 500 年前就发明了量子力学！

王阳明与友人同游南镇，友人问曰：

「天下无心外之物，如此花树，在深山中自开自落，于我心亦何相关？」

先生答曰：

「你未看此花时，此花与汝心同归于寂，你来看此花时，则此花颜色一时明白起来，便知此花不在你的心外。」

唯心所现，唯识所变。

未看此花时，花的存在是不确定的叠加态；起心动念的一刹，花才会从不确定态「塌缩」为确定态，你观察的世界因此呈现。

意识与物质互为因果，无法割裂。量子力学的「观测导致塌缩」就是唯心主义的铁证！

然而，很多人至今都不知道「意识决定观测结果」这个名声在外的量子黑科技，其实是道听途说导致的误会。

回到双缝干涉实验，如果科学家故意不观测实验结果，而是用机器自动记录；去掉人类的「意识」干扰，是不是量子态就不会塌缩了？

再比如，做实验时突然飞过一只苍蝇，在它的 N 只复眼注视下，光子的叠加态会因此而塌缩吗？（你以为苍蝇就没有意识吗？）

结果， 根本没有任何影响！

屏幕结果是代表波动的斑马线还是代表粒子的两道杠，只与实验设备的设置有关，和谁来观测、是否观测无关。

只要实验中双缝全开，哪怕有一亿双眼睛盯着，看见的仍然是未塌缩的叠加态光子产生的干涉条纹。

现在看来，比玻尔那句毁人不倦的「观察导致塌缩」更准确的表述是：

只要微观粒子处于「可能被精确测量」的环境下，它就会自动塌缩，并不需要等待「观察者」就位。

所以归根到底，量子实验仍然是不以主观意志为转移的。

眼见为实?

只不过，我们无法精确测量，只能用概率分布来计算这个客观世界，那么，薛定谔的猫真的存在吗?

一开始，包括薛老师和玻尔本人在内，没有人相信世界上真会有不死不活、既死又活的猫。

可是不久之后，科学家们惊恐地发现，这件看似显然的事，居然没法证伪（证明猫不是叠加态）。

按理说，猫到底是不是叠加态，做个实验不就明白了？

可惜，这个实验至今做不出来——毕竟，我们没法让猫产生干涉条纹啊！

证伪不行，证实的方法倒是有一个：把这只猫造出来。

令人细思恐极的是，我们已经做到了。

1996 年，美国人梦露（男）用单个铍离子制成「薛定谔猫态」并拍下了快照，发现铍离子在第一个位置处于自旋向上的状态，而同时又在第二个位置自旋向下，而这两个状态相距 80 纳米之遥！

这是人类有史以来第一次，亲眼「看」到活生生的量子叠加现象。

不过，这毕竟只是单个离子，和猫相比还差了十万八千里啊！

2004 年，潘建伟团队首次实现了多光子的薛定谔猫态。虽然这只猫的身材依旧苗条——浑身上下只有 5 个光子，但还是令玻尔的追随者信心大增。

这说明，从单个微观粒子到严格意义上的薛猫（宏观量子叠加态），也许只是量变而非质变，它被亲切地称为：薛定谔的小猫。

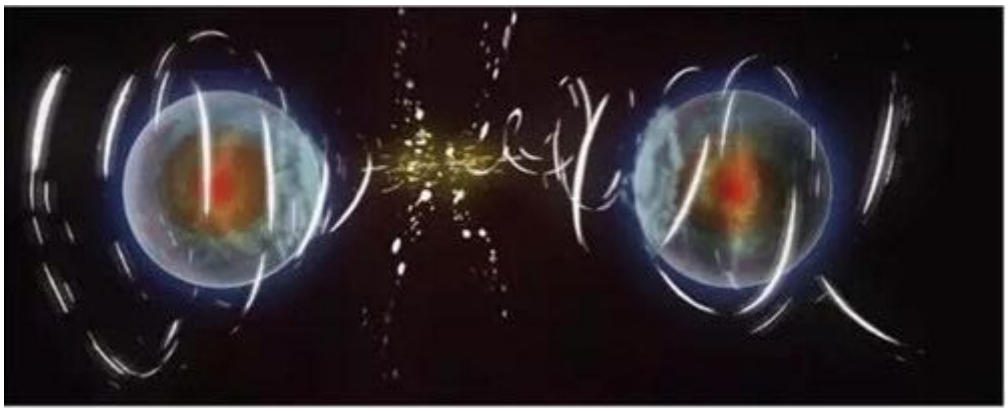
如果继续增加粒子数量，是不是能把小猫慢慢喂肥成大猫呢?

然而，现实很残酷：目前「薛猫」的最高纪录，仍然是潘建伟 2012 年实现的 8 光子叠加态。要知道，为了增加区区 3 个光子，实验用了整整 8 年时间。可想而知，要让猫身上亿个原子同时处于量子叠加态，绝非易事。

在乐观者看来，这不过是暂时的技术困难，假以时日迟早会攻克；但也有人认为，量子世界与宏观世界之间存在着一道天然的结界，像猫一样大的宏观叠加态，也许是这个宇宙明令禁止的。

有朝一日，能不能造出一只眼见为实的大薛猫，至少现在，我们还不知道。

但是我们已经知道：即使是小猫，也蕴含着无比惊人的能量。

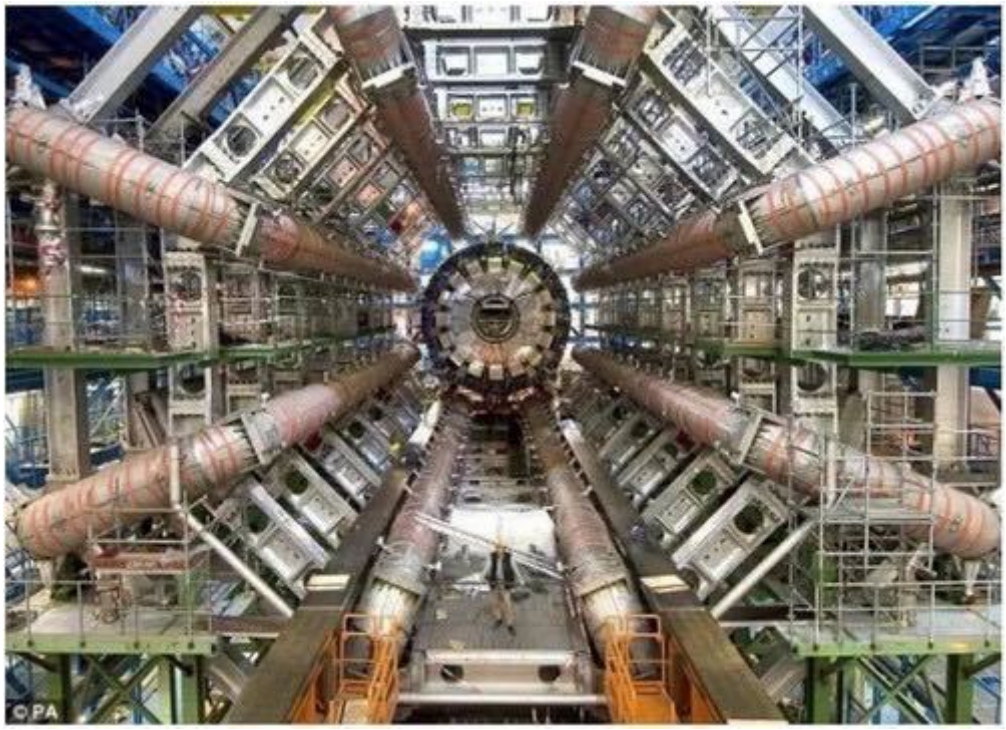


1935 年，薛老师很忙。

除了 N 多前女友和养猫以外，薛老师发现了量子的另一个诡异之处，而当时几乎没有人注意到这个问题。

为了研究微观世界，看看原子核这个大西瓜肚子里都有些什么籽儿，科学家祭出了最强大的武器：粒子对撞机。

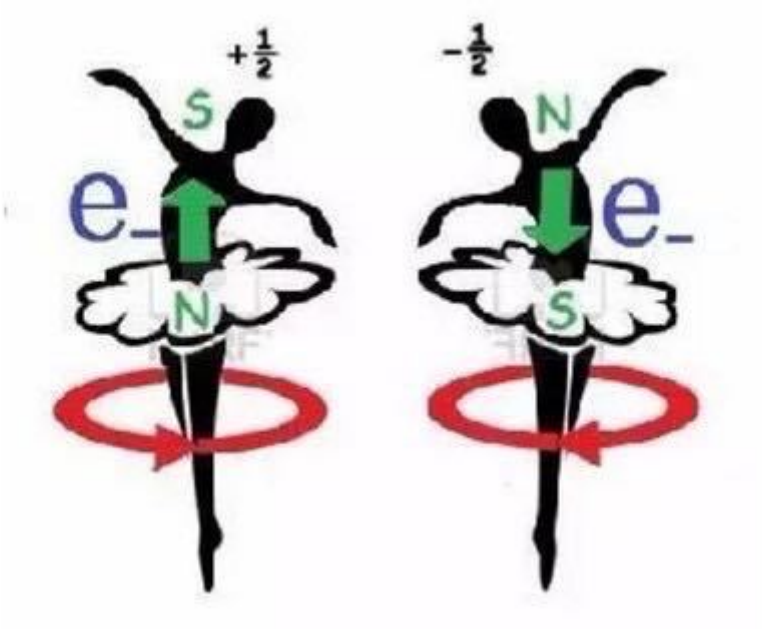
欧核中心（CERN）的加速器就是干这个的：



最常见的现象是：母粒子被撞击后，分裂成两个更小的粒子 A 和 B。

因为能量守恒原理，子粒子能量相同，方向相反。比如说，因为母粒子静止不动，所以分裂后的子粒子 A 向左边飞，B 一定往右边飞，这样才能左右抵消。同理，A
的自旋（角动量）向上，B 的自旋一定向下。

至于具体是向上还是向下，这是个随机事件，必须观测后才能知道。



那么问题来了：根据量子理论，在不被观测的情况下，粒子处于多种可能性的叠加态。

举个例子。

就像箱子里那只不死不活的薛定谔的猫一样：A 和 B 这对龙凤胎粒子，自打出娘胎起，他们的性别就没确定，直到有人来看了一眼，这才瞬间分出男女！

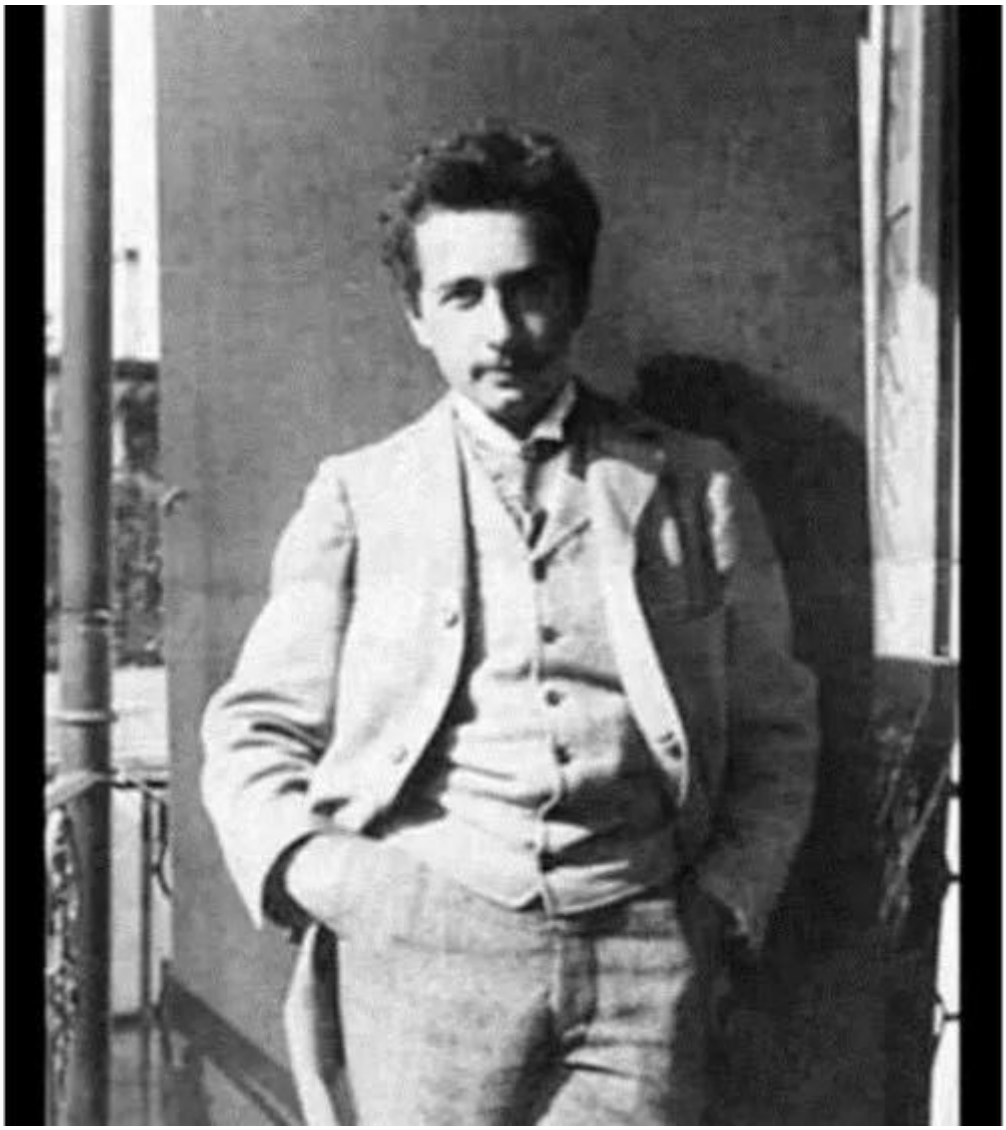
然而和薛猫不同的是，箱子里的猫只有一只，孪生粒子却有两个。而且，这两个粒子即使相隔很远很远，叠加态也能保持不变。如同在千里之外，瞬间产生联系……

是时候@爱因斯坦了。

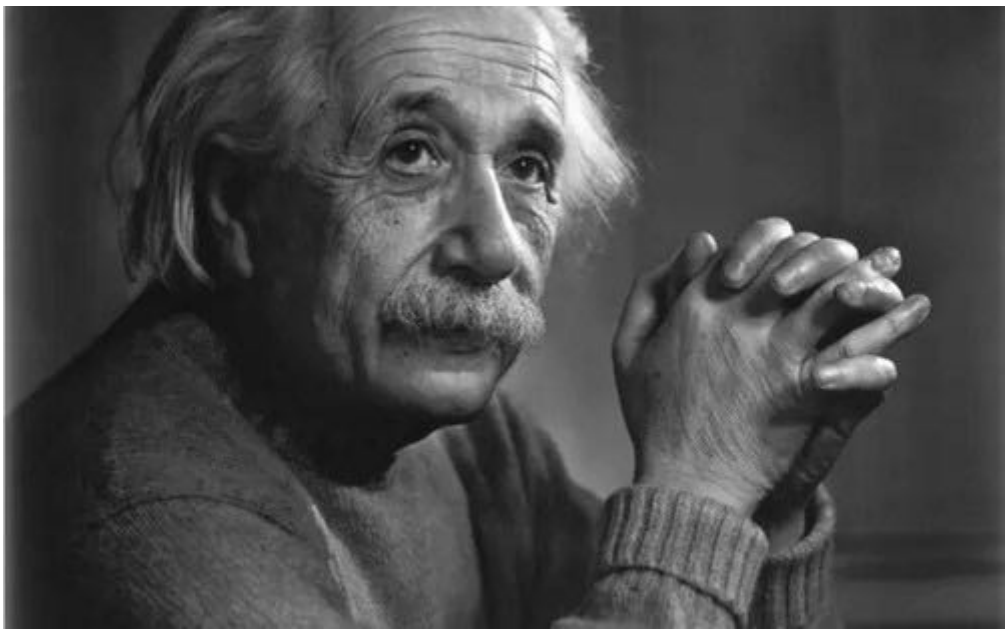
来自幽灵的威胁

大家都知道爱因斯坦创立了相对论。但很少有人知道，大神在 35 岁就已经功成名就（完成狭义+广义相对论），而在之后 40 年的悠长岁月里，他其实都在纠结一件事：量子力学。

曾经，他也是一个集美貌与才华于一身的男子：



研究量子力学 30 年之后：



能让爱因斯坦这种大神级人物「不明白」的，不是深奥的理论和复杂的公式，而是宇宙的意义。

爱因斯坦深信，宇宙在本质上是高度和谐的，这种和谐是可以通过数学之美体现出来的。

所以，一个理论如果不美，倒不是说一定是错的，但它肯定不够本质。

在更高的层面上，和谐，比对错更重要。而量子力学，在爱因斯坦看来，就是一种不和谐（不完备）的理论。

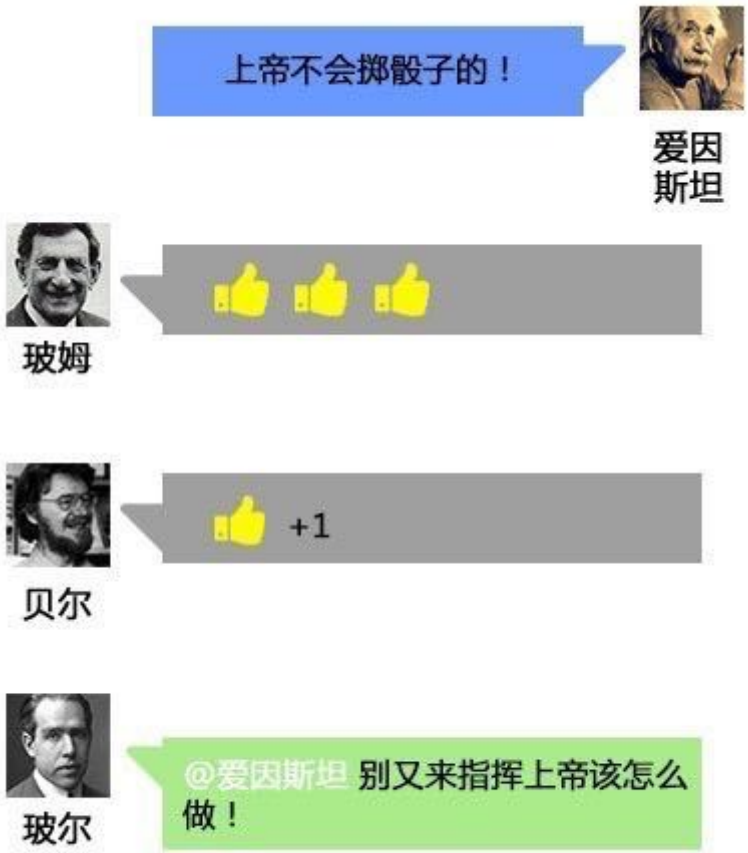
比如，量子力学的核心思想是：

微观世界的一切只能用概率统计来表达，而具体到单个的粒子，它的状态是不确定的叠加态。把这个粒子放大 N 亿倍，就成了薛定谔的猫。

这是第一个让爱因斯坦不爽的地方：量子力学否认了物质的实在性。

爱因斯坦认为，根本不存在薛定谔思想实验中那只不死不活的叠加态的猫。猫的死活在观测之前就是定数，只不过愚蠢的人类看不见箱子里发生的一切，只能推测出「50% 活 or 50% 死」的概率。

你是不是突然有一种，和爱因斯坦英雄所见略同的感觉？



打个不太恰当的比方（给量子打个恰当的比方真的好难！）：

比如，我在知乎的粉丝男女比例是 80:20。

我相信，每个关注我的知友，一定都对自己的性别深信不疑。

然而，那些发明量子力学的疯狂科学家们，他们竟然说：80:20 的比例，说明每位知友的性别是不确定的，见面时 80% 的可能性会变成男生，20% 的可能性变成女生！

因为只有这样我才能解释，为什么线下活动时见面的都是男生，而索要福利的都是女生。至于女生为什么没来，可能是出于一些很简单的原因，比如当天身体不舒服。

仅仅因为我们不知道背后的原因，就认为人的性别是可以按一定概率随机改变的，纯属不切实际的猜想。

这个「背后隐藏的原因」，学名叫作 「隐变量」 。

当时包括爱因斯坦在内的很多人都以为，一旦我们揪出了隐变量，量子力学那些混沌不清的阴暗角落，就会被照亮得一览无余。

一个不掷骰子的上帝，一个确定无疑的世界，一个可以被人类的直觉完全理解的宇宙——这就是爱因斯坦的终极梦想。到那时，「薛定谔的猫」之类的奇幻故事，只能给孙子当哈利波特讲了。

结果，猫的故事还没讲完，薛老师又想了一出「孪生粒子叠加态」，第二次触怒了爱因斯坦大神。

因为这一次，量子力学要挑战的是相对论。

研究微观小世界的量子力学，怎么会和研究宏观大宇宙的相对论结下梁子呢?

这又是薛老师「一不小心」捅下的篓子。

在薛定谔「孪生粒子」的思想实验中，两个相距万里的粒子，观测出 A 的状态，也就知道 B 的状态，因为 A 和 B 都是一个母粒子分裂而成的， **B** 的状态一定和 **A** 相反 。

因为 A、B 两个粒子的 命运紧密相连 ，牵一发而动全身，所以薛老师给起了个性感的名字： 量子纠缠 。

这就好比如：母亲把一双鞋分给兄弟俩，他们各带一只远走他乡。中国的哥哥打开盒子发现是左脚，就知道弟弟带到美国的另一只一定是右脚。

看上去，这并没有什么稀奇。

稀奇的是，根据量子力学的说法，弟弟那只鞋左还是右，不是他妈决定的，而是哥哥「打开盒子」的行为决定的。在哥哥看到左脚鞋的一瞬间，鞋里飞出一个神秘的信号，闪电般穿过千山万水，通知美国的另一只鞋变成右脚！

这个速度能有多快？

无限快。

但是，上帝允许无限快的瞬时传送吗？

在这个宇宙中，没有东西能超过真空光速。不要说超过光速，就是试图接近光速的行为，都会导致时空的畸变。

宇宙的尺度是以「亿光年」为单位计的，在恢宏的空间中，银河系一边发生的任何事情，不可能立即对彼岸的世界造成影响。

就算此时此刻太阳爆炸了，我们还能逍遥自在地活 8 分钟，因为 8 分钟后，光才来得及从太阳飞到地球。

通过对粒子 A 的观测，居然瞬间让远方的粒子 B 的量子叠加态塌缩了——这被爱因斯坦斥为「幽灵般的超距作用」。

在严谨的学术界，「幽灵」是一个让人联想起伪科学的词。不存在超光速，更不存在超距作用，因为这是相对论的大前提：局域性。如果量子纠缠允许超光速，那么，是量子力学错了，还是已经被无数次实验证实的相对论错了？

在爱因斯坦看来，这压根不是个问题。

一双鞋，俩兄弟当时分到的就是哥左弟右；两个粒子，在分裂的一瞬间 A、B 的状态就是确定的。尘埃落定之后，你爱怎么观察就怎么观察，为什么要信量子力学那一套「观察决定实验」的鬼话？

只可惜，在量子面前，人类的直觉和常识又一次大错特错。

终极黑客：约翰·贝尔

超距作用（量子）vs 局域性（爱因斯坦），人们曾经以为，这是个永远不会有答案的问题。

因为如果做实验验证，这两者根本没法区分啊！

比方说，先制备一对所谓的纠缠态粒子，然后一个运到北京，一个放在上海。我先测量到上海的 A 粒子自旋向上，然后打电话去问北京的同事：哥们，你那边测下 B
是什么态？

100% 是自旋向下！

爱因斯坦和量子理论都预言，B 的自旋一定和 A 相反。

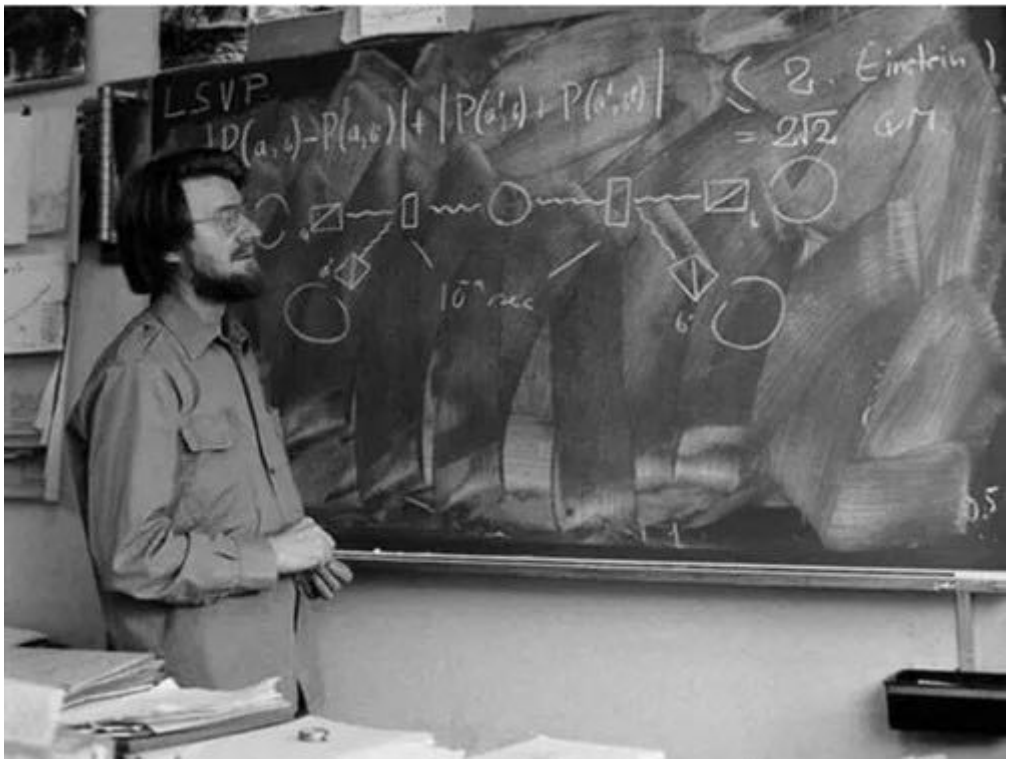
也就是说，仅凭测量是不可能区分两种说法谁对谁错的，这就好比两个人都赌同一个球队赢，如何分胜负呢？但是不测量，又怎么可能知道它在测量之前是什么？

显然，这个问题无解。

30 年过去，爱因斯坦、玻尔、薛定谔等一代宗师已经成为逝去的传奇，然而还是没有人认真思考过这个问题。

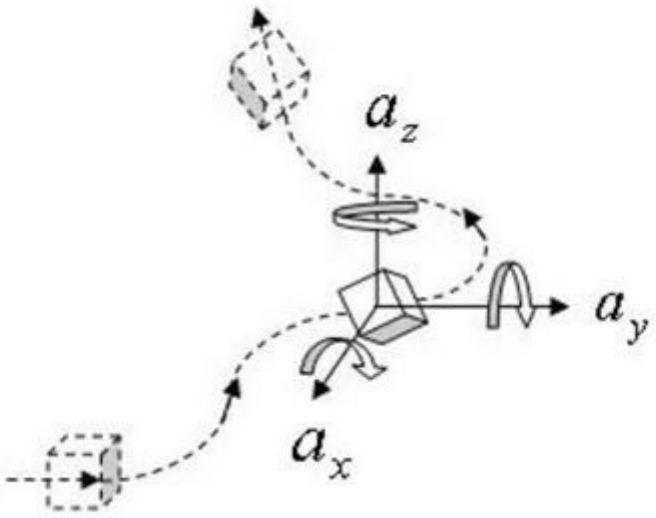
也许这就是为什么，做出这个近代物理学最重要的大发现的人，不是某位著名的教授，而是一位当时还默默无闻的工程师，也难怪当他投稿之后，文章居然被杂志编辑「不小心」弄丢了，拖了一两年才发表。

约翰·贝尔，36 岁提出「贝尔不等式」，欧核中心（CERN）加速器设计工程师，爱因斯坦的脑残粉，业余爱好是研究量子力学的基础理论。



我一直觉得，贝尔不像个正统科学家，更像个「物理学黑客」。虽然和计算机黑客相比，他破解的是原子而非比特；但是，论及思维之独特、技巧之高超、发现漏洞之敏锐，则是有过之而无不及。

众所周知，粒子 A 的自旋一定和 B 相反；但贝尔发现，所有人都忽略了一件事：自旋在三维空间是有 3 个分量的。



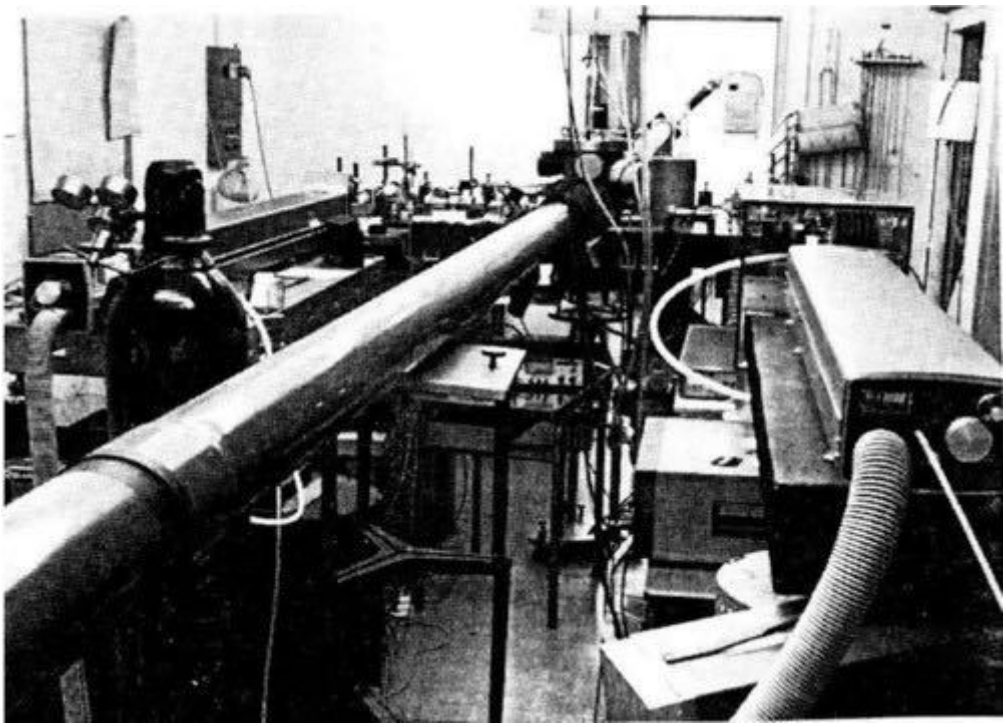
A 在 X 轴的自旋分量（Ax）如果向上，B 在 X 轴的自旋（Bx）一定向下，但是 B 在 Y 轴和 Z 轴上的自旋（By、Bz）呢?

如果爱因斯坦的局域性理论是对的，By、Bz 应该和 Ax 一毛钱关系没有，但是用量子力学算出来的结果，却有着微妙的区别：在某些情况下，By、Bz 和 Ax 之间竟存在着微弱的关联!

其他科学家们看到「贝尔不等式」先是嗤之以鼻，接着目瞪口呆，最后是深深的悔恨。这个深藏 30 年的宇宙级 bug，就这样被贝尔这位工程师挖了出来。

贝尔不等式的诞生，宣告了量子局域性之争，从哲学思辨变为实验可证伪的科学理论。

20 年后（1982），法国人阿兹派克特（Aspect）第一个成功验证了贝尔不等式，结论： 量子力学获胜，幽灵般的超距作用，是真的!



万万没想到，实验结果揭晓之后，最高兴不起来的居然是贝尔本人。原来贝尔是爱因斯坦的忠实信徒，人家下班不约会而去搞不等式的目的，就是为了证明量子力学错了！

之后，贝尔花了大半辈子的时间，试图找出实验的漏洞，直到去世之前还在思考如何修正局域性理论。

当然，这一切并没有什么用。

从阿兹派克特实验至今 30 多年，人们在光子、原子、离子、超导比特、固态量子比特等许多系统中都验证了贝尔不等式，所有的实验无一例外，全部支持量子理论。

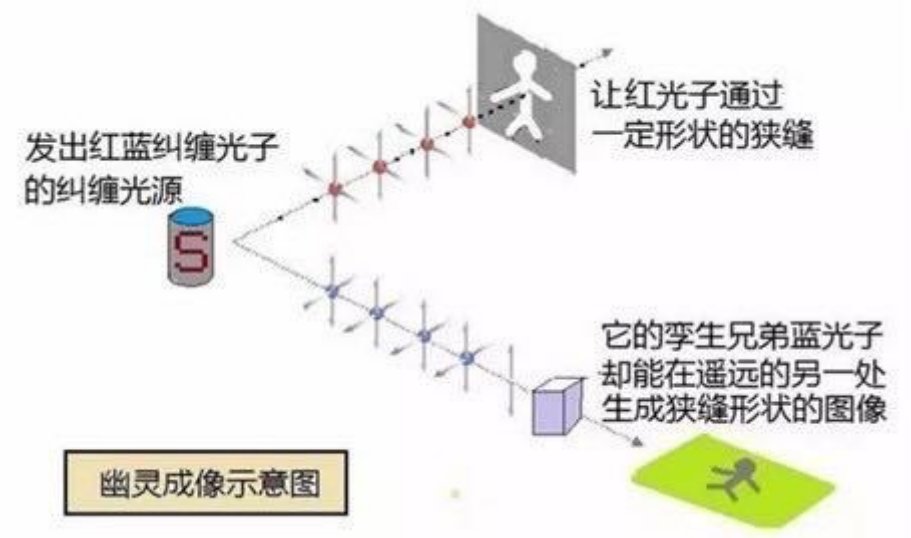
如今，除了层出不穷的民科，已经没有人怀疑量子世界的奇异和真实。但很多人还是忍不住会想，贝尔不等式什么的还是太抽象了，能不能亲眼见证量子纠缠的魔力呢?

幽灵成像实验

比起喜欢用数学公式讲道理的贝尔，搞量子光学的史砚华可就实在多了。

我觉得，史教授 2008 年发明的「幽灵成像」，应该是证明量子纠缠绝非幻想的最直观的实验。

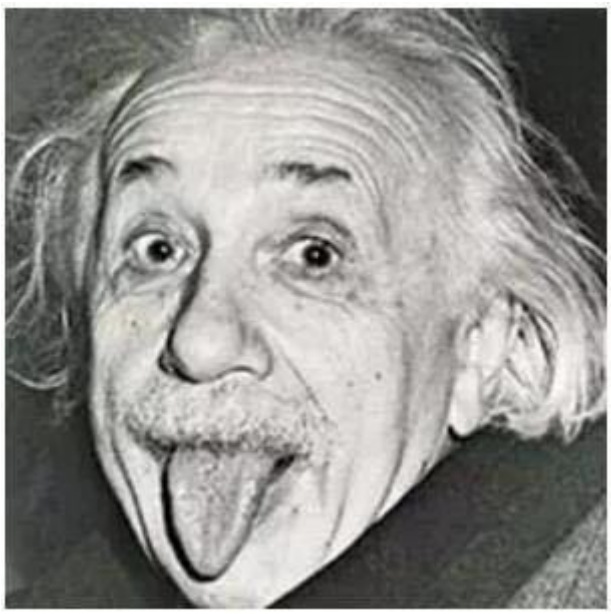
请认真看下图：



幽灵成像的原理通俗易懂：先把红光子和蓝光子「纠缠」到一起，然后两者分开各走各路。红光穿过狭缝打出一定形状的图案，蓝光不穿缝正常走。

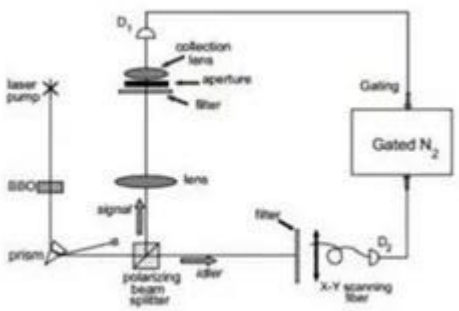
实验结果绝对震撼：明明没有穿过狭缝的蓝光，竟然也投射出了与红光相同形状的图像！

如果这个实验能够早 70 年做出来，我真想看看爱因斯坦的表情。

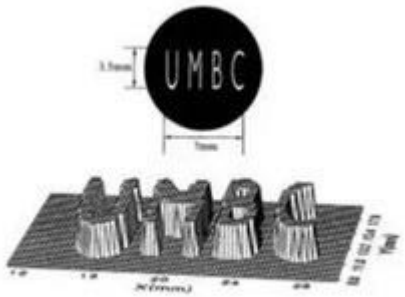


这次，你总不能说：光子在纠缠之前就已经是那个形状了吧！

穿缝还是不穿缝，显然是在光子出发后才决定的。发生在红光子身上的所有事，蓝光子也会分毫不差地经历一遍。这样看来，仅仅把量子纠缠比作龙凤胎还远远不够，他们出生时珠联璧合，长大成人之后仍然是生死与共！而且，通过改变红光那边狭缝的形状，想让蓝光打出什么样的图案都可以。



Schematic set-up of the first "ghost" image experiment.



experiment results

这就意味着，我们可以远程发送图像甚至视频，而无论距离多远、哪怕从宇宙的另一端传过来都是瞬时传输的，延迟时间永远为 0。

然而，这岂不是违反相对论（任何信息和物质不能超过光速）的公理了吗？

并没有！

虽然信息是瞬时传送过来了，但要把其中的乱码剔除，提取出真正的内容，还是必须把图像用不超光速的传统方式再发一遍。让爱因斯坦操碎了心的「超光速」问题，原来只是杞人忧天！

大自然就是如此微妙。

宇宙的规则也许看似奇怪，内在却有着惊人的自洽性。

我们只能说相对论和量子力学之间存在着理论上的矛盾，但从来没发现物理规律本身有自相矛盾的地方。

如果把宇宙看作一个产品，最令人细思恐极的是：无论狡猾的人类捣鼓出多么刁钻古怪的实验，这个同时在线用户数高达 10^80（1 后面跟 80 个 0）的产品却从来不会被搞出 bug。

如果宇宙真有一个产品经理的话，请收下我卑微的膝盖，顺便想问一个问题是：为什么您的宇宙中会有量子纠缠呢？

量子纠缠背后的秘密

100 年前，量子力学的祖师爷玻尔说： 如果谁没有被量子力学惊到，那他肯定不懂量子力学。

爱因斯坦： 我思考量子力学的时间百倍于广义相对论，但依然不明白。

造出第一颗原子弹的费曼更直接： 没有人懂量子力学！

学了 100 多年的量子力学，今天，我们懂了吗？

墨子号首席科学家、中国量子通信第一人潘建伟说：「如果能搞清楚为什么有量子纠缠，我可以现在去死」，接着潘老师又说：「但是现在还没搞清楚，所以我想活得长一点……」

考虑到潘院士今年才 46 岁，这句话似乎暗示着，我们在 50 年后都不一定能搞懂量子了。

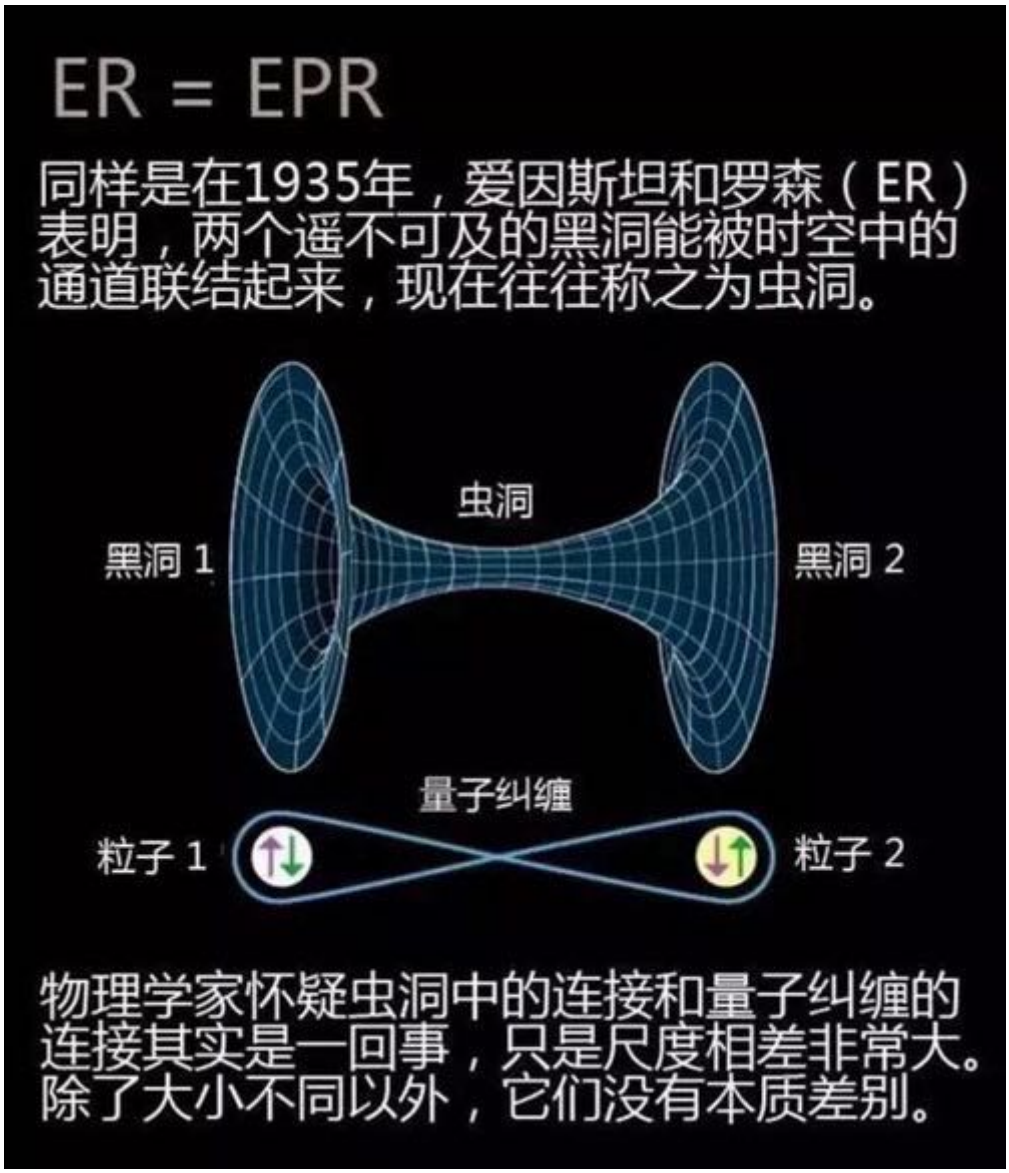
这些牛人说的「不懂」，可不是小学生学不会四则运算的那种「不懂」。我们已经搞清了微观世界的所有基本规则，建立了强大的数学模型，算出来的理论预测和实验结果分毫不差，但我们还只是一个拿到使用说明书的孩子，对于其意义和目的一无所知，莫名地好委屈。

然而现在，越来越多的线索显示，量子纠缠的背后，可能隐藏着一个巨大的秘密。

2013 年，Maldancena 和 Susskind 发现，量子纠缠和虫洞（虫洞即爱因斯坦·罗森桥）在数学模型上非常相似。他们猜想，量子纠缠也许就是一个微型虫洞。

量子纠缠中最神秘的现象「超距作用」其实并没有超越光速，而是像虫洞那样穿越了时空。这就是为什么，孪生粒子能够异地千里，同呼吸、共命运的真正原因。

请认真看下图：

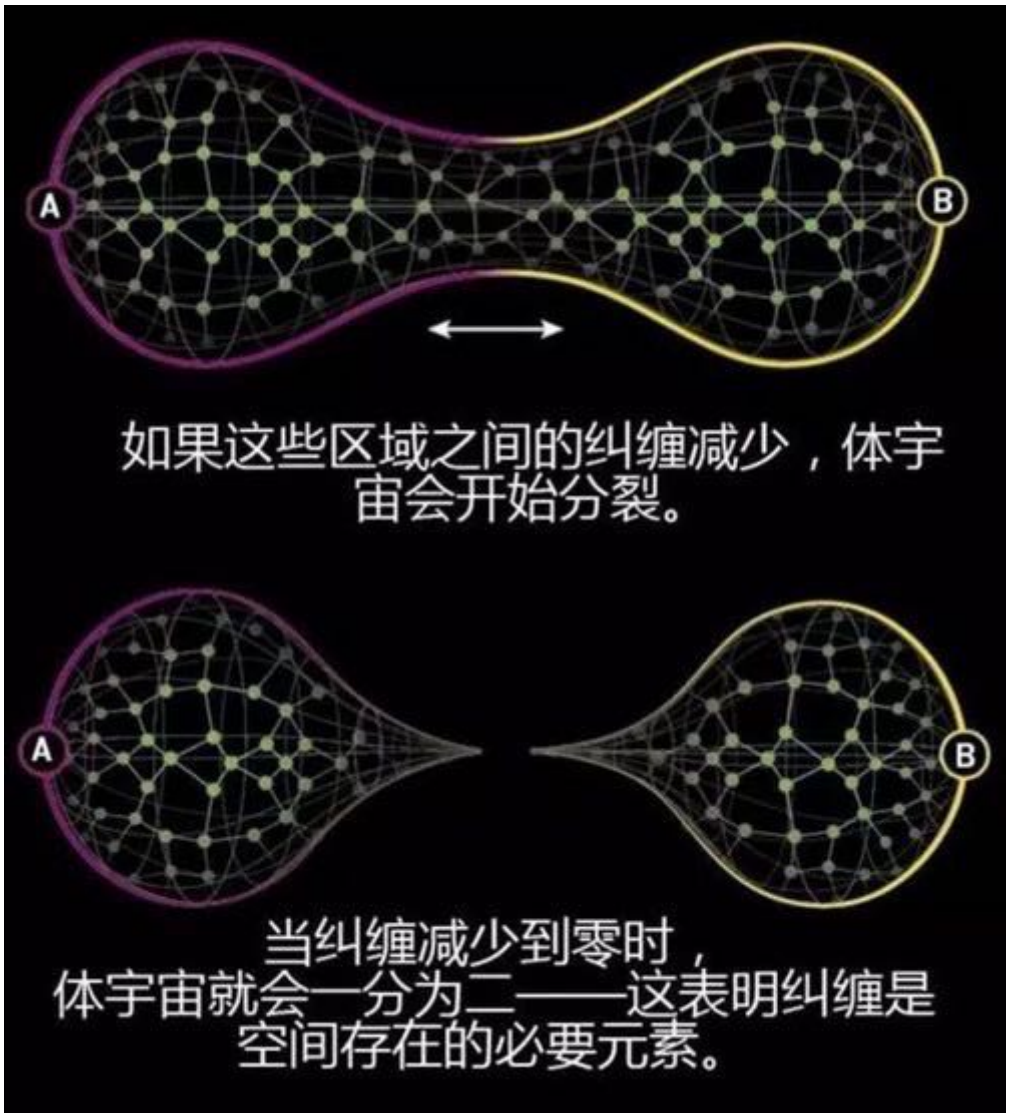


而在 2010 年 Van Raamsdonk 的独立研究中，发现了更为惊人的线索。

他建立了一个类似真实宇宙的三维宇宙模型，一旦在模型中去掉量子纠缠，时间和空间就会被打乱成碎片。

正是无处不在的量子纠缠，像建筑物的钢筋结构件一样，把本应支离破碎的时空编织成了一个整体。

请认真看下图：



在有进一步的实验证据之前，我们无法评价这些猜想有多靠谱。但是令理论物理学家们心跳加速的是，各条独立的线索似乎指向着同一个宝藏。找到它，发现量子纠缠真正的秘密，就有可能理解在开天辟地、宇宙洪荒的大爆炸时刻，宇宙是怎样被建造出来的。

为了传说中的 One Piece，越来越多身怀绝技的人踏上了量子时代的大航海之路。

有人说：哲学家们总是用各种方式解释世界，但问题在于改变世界。其实，科学和文明的高度，取决于我们对于世界理解的深度。

通过认识和理解世界，猿人把手中的石块换成了自然规律，拥有了改天换日的力量。当一群不食人间烟火的理工男在实验室热烈地争论原子模型时，谁能想到，30 年后广岛在火海中的哭喊？

自从 1900 年普朗克发明「Quantum」这个单词至今，量子终于从哲学辩论会的题材，变成了魔法般的黑科技。

基于量子纠缠，可以造出比现在快 1 亿倍的量子计算机，而超距作用和贝尔不等式，则把量子纠缠变成了加密通信领域的终极武器。

改变世界的时刻真的到了！

公元前 54 年，深冬。

高卢，毕布拉克德。

罗马共和国高卢行省长——尤里乌斯·恺撒，借着帐篷里的烛火，正在一张羊皮上写着什么。

战况紧急！ 恺撒的爱将西塞罗，突然遭到维尔纳人的围攻。

现在，必须立刻派一名骑兵送信给西塞罗，命令他重整旗鼓，两军合力突围。

可是，万一这封信被敌人截获怎么办？

想到这里，他不由自主地停下了笔，棱角分明的脸上，分明掠过一丝狡猾的微笑……

恺撒大帝、福尔摩斯与密码学

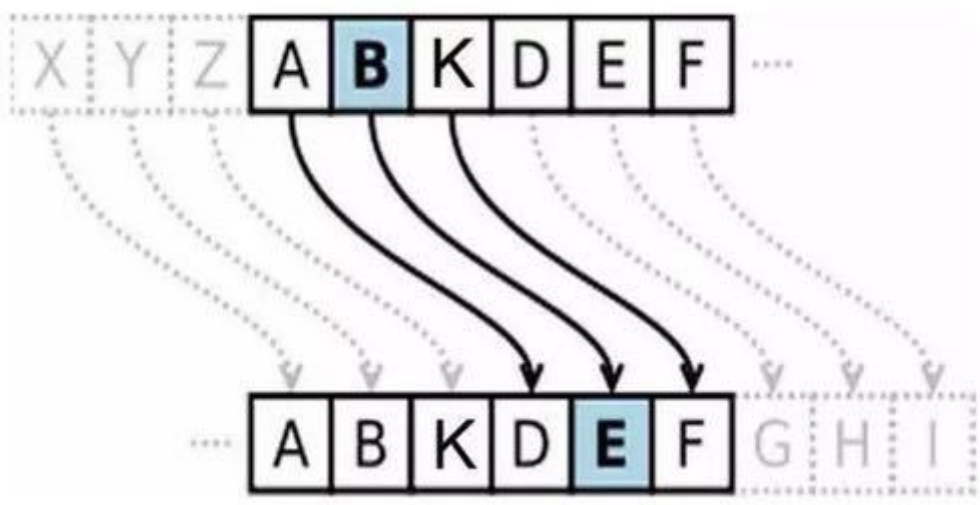
作为罗马的第一位独裁者，恺撒大帝还有一个鲜为人知的技能点：

其实，大帝不是历史上第一个想出加密算法的人。据说，我朝的姜子牙在 3000 年前，就发明了古装版密码本「阴书」。

但恺撒密码，却很有可能是首个广泛运用到军事通信领域的加密技术。

恺撒密码的原理，说白了就是一个字： 替换！

如果心里想的是字母 A，纸上就写 B；要写 B，就用 C 代替。当然，我也可以用 D 替换 A，用 E 替换 B，以此类推（偏移 3 个字母）。



只要收发双方都知道偏移量是几，就能轻松加密和解密；而外人看到的无非是一堆乱码。

这就让上课传小纸条，有了新招数！心里想（明文）：I love U，老师看到（密文）：L oryh X。

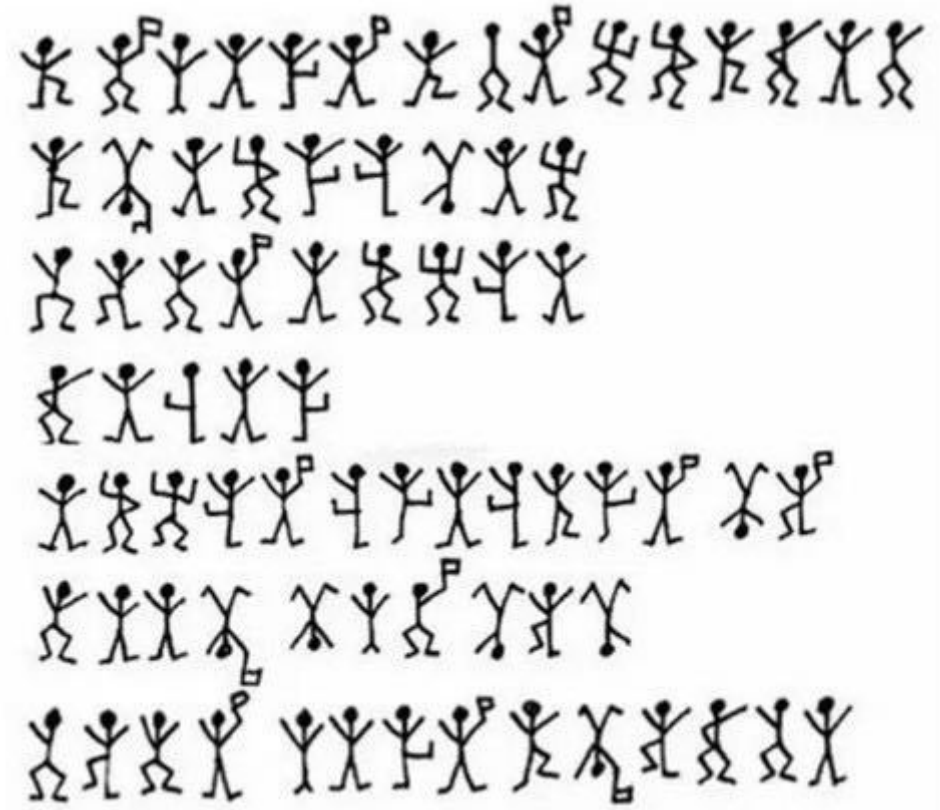
在今天看来，这种算法极易破解，毫无技术含量可言。但在当年的罗马战场，这就是令吃瓜群众望而生畏的黑科技！

在恺撒制霸罗马的全盛时期，就连教主耶稣都不得不服： 上帝的归上帝，恺撒的归恺撒。

然而讽刺的是，这样一位狂拽酷炫屌炸天、还精通密码谍战的军事天才，却死于一场密谋政变，生生被戳了 23 刀。为了纪念大帝，人们把恺撒制成了扑克牌上的标本：方块 K。

又过了一千多年，恺撒大帝和他的罗马帝国早已灰飞烟灭，恺撒密码和扑克却被后人发扬光大。

原版的恺撒密码，是用字母替换字母，而且所有字母还是按照偏移量顺序替换的，极大地降低了破解难度。到了维多利亚时代，这两个弱点终于被改进。于是，连福尔摩斯逮到的一个普通黑帮小弟，都学会原创这样的密码了：



我们来看，传说中的卷福，是怎样破解这种图形密码的。

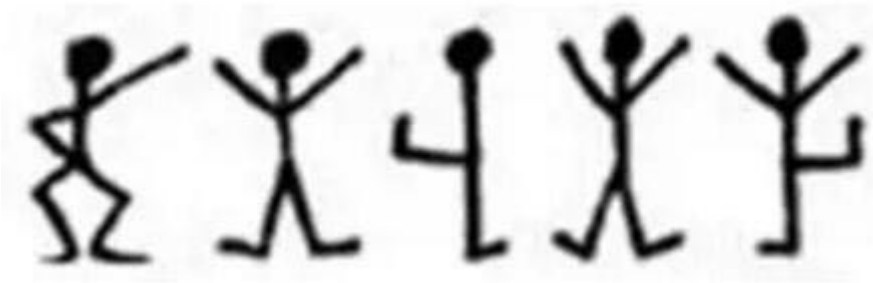
在英文字母中 E 最常见。第一张纸条上的 15 个小人，其中有 4 个完全一样，因此猜它是 E。

这些图形中，有的带小旗，有的没有小旗。从小旗的分布来看，带旗的图形可能是用来把这个句子分成一个个单词。

现在最难的问题来了。

因为，除了 E 以外，英文字母出现次数的顺序并不很清楚，要是把每一种组合都试一遍，那会是一项繁琐且无止境的工作。

根据似乎只有一个单词的一句话，我找出了第 2 个和第 4 个都是 E。



这个单词可能是 sever（切断），也可能是 lever（杠杆），或者 never（决不）。

毫无疑问，使用 never 这个词来回答一项请求的可能性极大，所以其他三个小人分别代表 N、V 和 R。

如此这般以此类推，福尔摩斯利用上（主）下（角）文（光）逐（环）个（的）击（加）破（持），分分钟破译了全部 52 个密文：

不过，所有基于替换法的加密算法，都有一个致命的弱点：因为凡是用字母构成的文字，其字母分布都要符合语言规律，比如英文单词中 E 最常见，Z 和 X 最罕见，无论把字母替换成多么奇葩的东西，符号的分布规律永远不会变，用概率统计+穷举法+玩填字游戏的基本技巧，任何密文的破解只是时间问题。

就当小伙伴们都以为恺撒密码的发展已经走到头的时候，德国人谢尔比乌斯却给替换式密码来了一次大升级，造就了有史以来最可靠的加密系统，一度令盟军绝望的噩梦，让希特勒成也萧何败也萧何的二战谍报神器——英格玛密码机，又叫恩尼格玛密码机（ENIGMA）。

二战谍报神器跌落神坛

英格玛（**Enigma**）密码机牛在哪里？

1．机器加密

这是世界首台全自动的加密机器，而此前编码、译码一直靠人力。

我国由于国情原因，直到 20 世纪 80 年代还在用铅笔+纸的人肉编码方法。

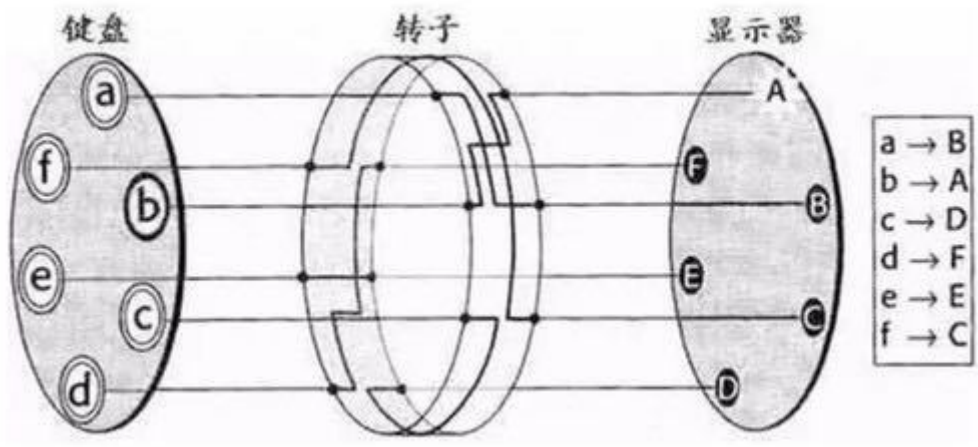
用机器的好处不仅是省力，而且，可以轻松搞定人力难以企及的复杂算法。

2．复式替换

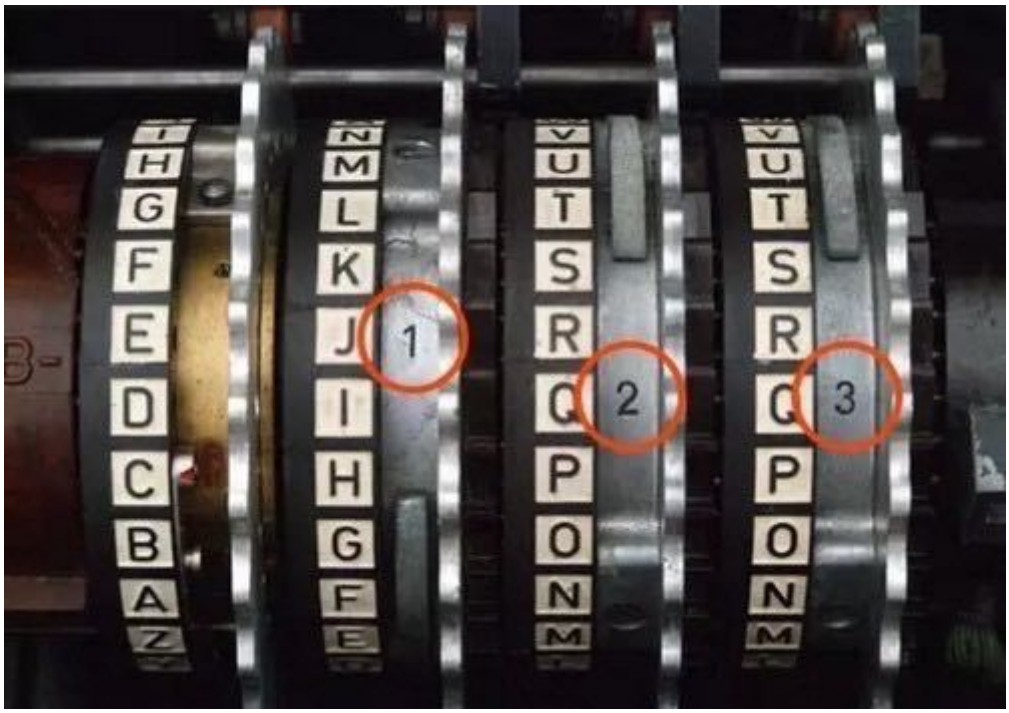
虽然基础原理和恺撒密码相同，但英格玛的字符替换方式却高级了不止一个档次：复式替换。

也就是说，如果你连打 3 个 A，恺撒密码的密文可能是 DDD，但英格玛的密文却可能是 BDA。

英格玛的神奇之处在于「转子」，它通过转动的方式实时改变替换方式，每敲一个字所用的替换方式都不同，这让依赖频率分析、概率统计的破解方法从此无的放矢。



原版的英格玛密码机只有一个转子，二战时期德军为了万无一失，把转子加到了 3 个。



每个转子都有独立的设置，3 个转子所有可能的设置，高达 105654 种组合！这样一来，连穷举法暴力破解的一线希望都断了念想。

正因为英格玛在当时太过逆天，以至于德军从此高枕无忧，以为盟军这辈子也别想破解了。

他们说得没错。单凭人力，是不可能干过英格玛密码机的。能够破解这台机器的，只能是另一台机器，一台算力更强大的机器。

马拉松运动员同志阿兰·图灵 1941 年发明的机器解码，用传统的频率分析+机器暴力穷举干掉了英格玛，从此军情六处把德军的情报兜了个底朝天。直到盟军诺曼底登陆，德国人还没有反应过来，他们正是被自己的传家宝坑死的。

而图灵的这台机器，就是世界上第一台计算机。

在计算机时代，复式替换加密从此跌落神坛、万劫不复。

而且实战中还发现，有时最容易攻破的反而不是算法，而是人。

只要搞定那个掌握密码本的人，一切密钥都不攻自破。

全民加密：**RSA** 技术

显然，拥有密码本的人越少越好。

但问题是 How?

曾经，这是个无解的难题。

道理很简单：密码本必须人手一本，否则卧底同志们还拿什么来加密通信呢?

历史告诉我们，当所有人都认为无解的时候，换个思路，往往就是柳暗花明、醍醐灌顶的时刻。

传统的密码学中，无论采用何种加密算法，都默默地遵循着一个思维定式：加密和解密是互逆的，也就是说，只要知道如何加密，就一定知道如何解密，反之亦然。

这被称为「对称加密」。

而世间还有一种「非对称加密」（RSA）：我可以把加密方法公开给全世界（公钥），但解密算法（私钥）只有我一个人知道，就算你知道如何加密，也不可能据此推出如何解密。

RSA 为什么能做到「知道加密算法也推不出解密算法」？

这基于一个数学事实：将两个大素数相乘十分容易，但对乘积因式分解、还原成两个素数却极其困难，而且数字越大，困难级别指数上升。

解密靠的是私钥，而破解私钥的唯一方法是猜出公钥是哪两个数字的乘积，因此，把大数乘积作为公钥公开是非常安全的。

举个例子：

37×97=3589 小学生都会手算，但是，问 3589 是哪两个数的乘积？你回答得出来吗？

如果觉得靠运气能凑出答案，你可以挑战一下这个：

```
123018668453011775513049495838496272077285356959533479219732245215172640050
726365751874520219978646938995647494277406384592519255732630345373154826850
791702612214291346167042921431160222124047927473779408066535141959745985690
2143413
```

你能看出它其实不过是

```
334780716989568987860441698482126908177047949837137685689124313889828837938
780022876147116525317430877378144679994 89
```

和

```
367460436667995904282446337996279526322791581643430876426760322838157396665
112792333734171433968102700927987363089 17
```

在对称加密时代，密码本只能人手一本；有了 RSA，真正的密码本（私钥）只要总部的领导一个人知道就行，在各地卧底的

特工们靠公钥就能加密发密文。

这就是为什么 RSA 能在短短 40 年内取代流传两千多年的恺撒，成为当今世界全民加密的事实标准：方便。

生活中，当你网购时，浏览器用公开下载的公钥把你的付款信息加密发送给服务器，服务器用没人知道的私钥解密信息，这一切是在你没有丝毫察觉的情况下悄然完成的。更给力的是，RSA 还是一个相当坚固的加密算法。

比如，上面那个用来吓人的数字，有 232 位（768 比特），这已经是当今地球上计算机能分解的最大整数了。

而你在网上随便申请一个免费的 https 加密证书，长度都有 2048 比特！

在回顾了人类几千年来的密码学成果之后，请你，把它们统统忘掉。

因为现在，无敌的量子通信来了。

它靠的可不是什么逆天的算法，而仅仅是两枚神奇的硬币。

当所有的密码都可以秒破，只有量子通信可以做到无条件安全。

未来，已来。

由一枚硬币开启的超距传输

喂，年轻人！我看你骨骼精奇，是万中无一的创业奇才。

我这里有一对魔法硬币，与你有缘，就十块钱卖给你吧！

别看它长得和普通的一元硬币差不多，这种硬币有一项：

神奇的技能点

就算相隔千山万水，

只要一枚硬币翻到**正面**朝上，

成对的另一枚硬币，

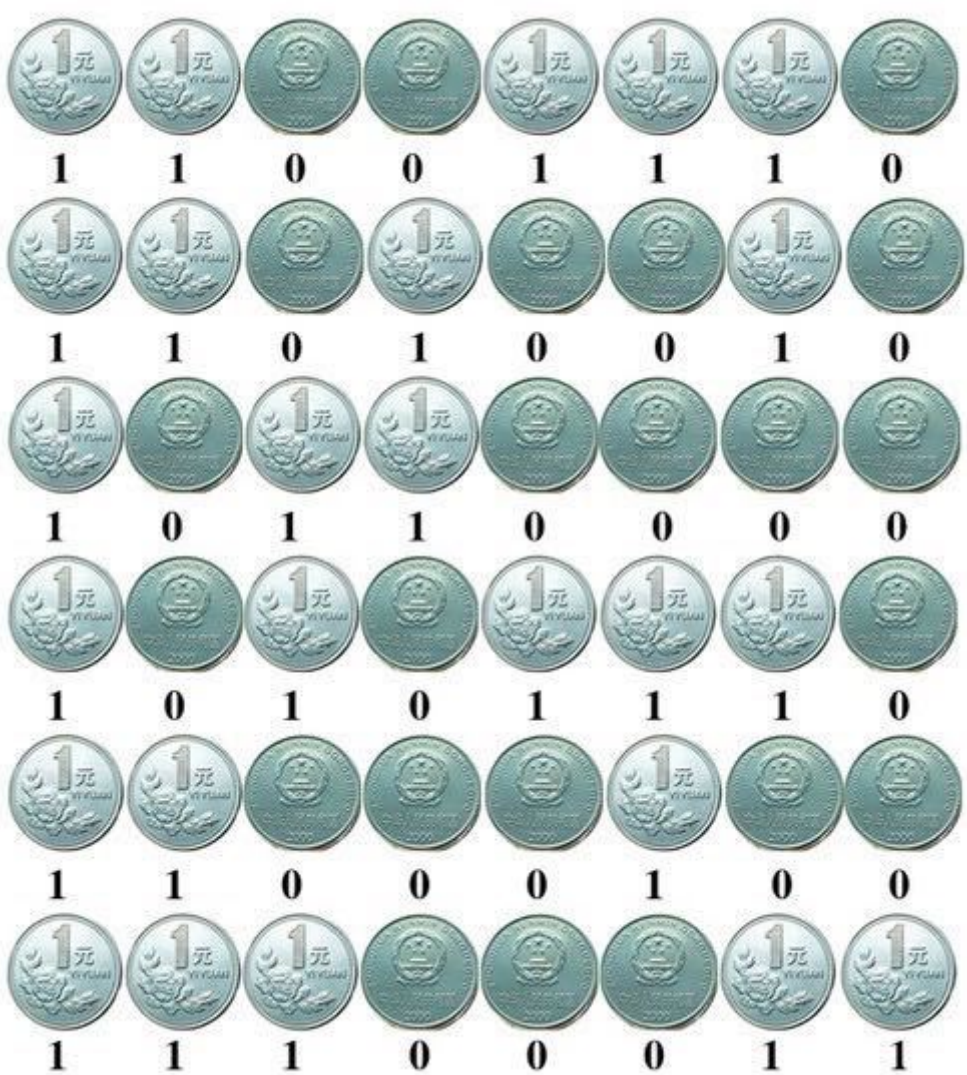
一定会**瞬间**自动翻到**反面**朝上。

你想啊，这种硬币如果做成情侣版，肯定大卖！尤其是异地恋：

你和你伴侣人手一枚，你在北京不断抛硬币 A，发出「正正反反」之类的信号，她在西雅图的硬币 B 就会自动变成「反反正正」，编码成「0011……」，再转成
ASCII 码就是：

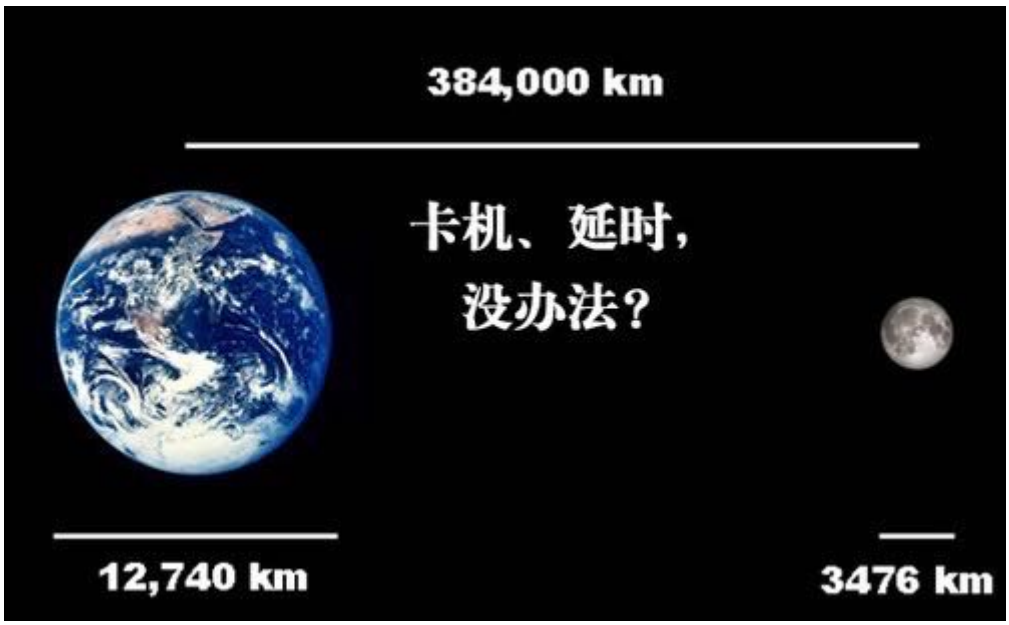
I LOVE U

理工男的浪漫，你懂不懂！



再想想，如果能好好包装一把，还能卖给国家航天局、NASA 之类的土豪机构！

从月球到地球 38 万公里，电磁波信号需要走 2 秒多。月球的宇航员别说游戏玩不了，打个电话都卡死机。火星就更远啦，1 亿公里，得延迟 5 分钟！



但是用无延迟的魔法硬币做星际通信，网游不卡了，电话不等了，干啥都流畅！

要问魔法硬币有没有缺点？

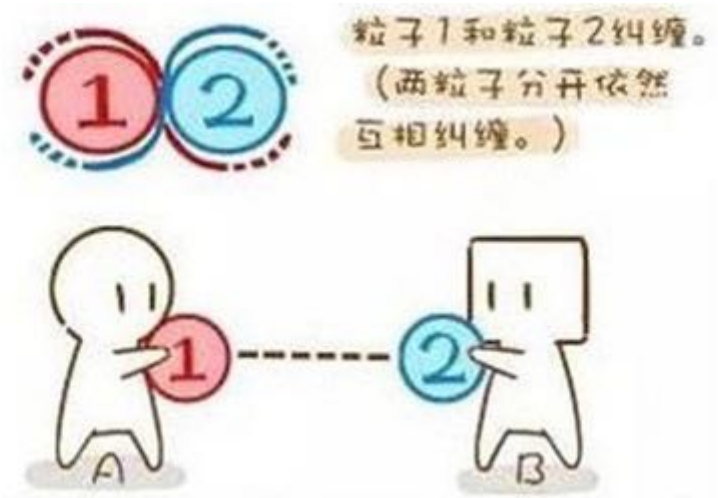
你还别说，是有个小问题，不过不影响使用啦——就是每次抛硬币时，翻到正面还是反面，要看人品（喂，喂！年轻人，别走啊……）

好啦！以上故事是玩笑，但魔法硬币可不是玩笑。

用量子纠缠态的一对孪生粒子，自旋向上=硬币正面，自旋向下=硬币反面，就能做出如假包换的「魔法硬币」。

无论相隔多远的距离，处于「纠缠态」两个孪生粒子就像有心灵感应般，零延迟、发生同步反应。如果把孪生粒子放在两

地，在地球观测粒子 A 发现自旋向上，火星上的粒子 B 会因此而瞬间变成自旋向下，仿佛两个粒子之间始终有一道穿越时空的纽带——这就是传说中的「超距作用」。



因为 A 的粒子自旋态始终和 B 的相反，所以地球人只需观测一下粒子 A，就能实时改变粒子 B 被火星人观测到的自旋态。当火星人读取出 B 的自旋态时，相当于接收到了地球发来的一个比特。

如果把孪生粒子比作一对魔法硬币，通信双方重复以上步骤、通过「抛量子硬币」传送信号的方式，就叫作量子通信。

问题在于，就算拥有把爱因斯坦吓傻的超能力「超距作用」，量子通信却没法用来瞬时传数据！

因为，每次硬币（自旋）是正是反，是个完全随机事件，不要说控制，连影响都做不到。你想发「正正反反」，它给你来个「反正反正」——试想如果不能畅所欲言，对方接收到的都是乱码，还谈何通信呢？

既然发的是一团乱码，那么就算能够穿越宇宙瞬时传送，也称不上是真正的通信。

爱因斯坦当年杞人忧天的「超光速通信」问题，就这样被「随机性乱码」天衣无缝地解决了。

要想用量子传点有意义的东西，解决的办法只有一个：

用量子通信发完「反正反正」之后，赶紧再用微信给对方补个留言「错对对错」，告诉他哪些信号是发错的，让他自己纠正。

也就是说，对方收到量子信息虽然是瞬时的，但要从一团乱码中找出真正的意义，还得靠传统通信方式，微信、电话延迟多久，量子通信就延迟多久。你是不是在想：既然如此，不如我直接发个微信得了，还要用量子通信干吗？

所以，只有聪明人才能看出，量子通信真正的威力。

无条件安全，可能吗？

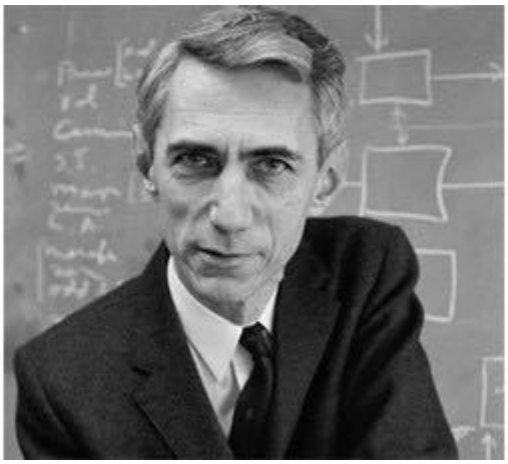
每次我和朋友聊起「无条件安全」的量子通信，几乎所有人都认为我在吹牛。

大多数人直觉上认为，凡事无绝对。

你说破解难度很高，OK；说 99.99% 安全，或许吧；但打死我也不信，世界上存在无懈可击的东西。

但是他们忘了，绝对安全的加密通信，其实早在 75 年前就被发现了。

1941 年，信息论的祖师爷香农，在数学上严格证明了：不知道密码就绝对无法破解的安全系统，是存在的。



而且，更令人惊讶的是，这种绝对安全的密码出人意料的简单——只需符合以下 3 个条件：

- 一次一密：每传一条信息都用不同的密钥加密，断了敌人截获一本密码本后，一劳永逸的妄想；
- 随机密钥：生成的密钥是完全随机的，不可预测，不可重现，破解者更不可能猜出规律，自己生成所有密钥；
- 明密等长：密钥长度至少要和明文（传输的内容）一样长，破解者穷举所有密钥，相当于穷举所有可能的明文。

谁要是有本事通过穷举猜出明文，还来劳什子破解密钥干吗？

奇怪的是，香农发明「无条件安全」的 75 年后，我们居然还没能用上这个黑科技。因为在当时的技术条件下，要同时符合这 3 个要求根本不可能！

先说「随机密钥」：请计算机程序 rand() 生成的随机数其实 并不是真正的随机，理论上，如果知道已经产生的随机数，就有可能获得接下来的随机数序列（可预测）。

再看「明密等长」：如果我能轻松吧这么长的密钥安全地发送给对方，为什么不干脆发送明文呢？这样岂不是多此一举？

最后「一次一密」：每发一次信息就要更新密钥，但通信双方又不能天天见面接头，否则还要加密通信干什么？

然而，在不计成本的最高级别通信场合下，「一次一密」还真的用上了。

比如先编写一部超级长的密码本，派特工直接交到对方手里，然后双方就可以暂时安全通信了。

仅仅是暂时。

密码本用完之后，特工又得出动再送一本新的……（007：你以为我是快递小哥吗？）

就这样，我们研究了 75 年的密码学，什么对称加密、非对称加密（RSA）和黑客们展开了无数次「道高一尺魔高一丈」的攻防大战……

直到我们遇见了香农 75 年前预言的密码学终极形态：无条件安全的量子通信。75 年前没有人能想到，那些「看上去几乎不可能实现」的三大要求，简直就是为量子通信量身定做的。

就拿最简单的量子通信协议——孪生粒子的量子纠缠来举个例子：

1. 随机密钥：服务器生成一对孪生粒子 A 和 B，分别发送给通信双方。注意，A、B 被观测后的自旋状态是完全随机的，不要说敌人，就连自己人都看不出规律来！。

2.明密等长：要发送的「正正反反」是明文编码，量子通信随机产生的「反正反正」相当于密钥，微信发送的纠错码「错对对错」是加密后的传送内容。此时，正文、密钥、纠错码，三者的长度完全相同。

3. 一次一密：为了发送 4 个比特的明文编码「正正反反」，服务器总共生成了 4 次随机密钥，每次传输 1 比特明文，都有 1 比特密钥保驾护航。

此时，破解的可能性，不是万分之一，也不是亿万分之一，就是 0。而且，最令人不可思议的是，量子通信不仅无法破解，还自带反窃听属性。就算敌人截获了每一次密钥，同时拿到了「正正反反」「反正反正」「错对对错」三条信息，量子通信仍然是安全的！

下面，就是见证奇迹的时刻。

反窃听，掌握主动权

量子通信为啥能反窃听？

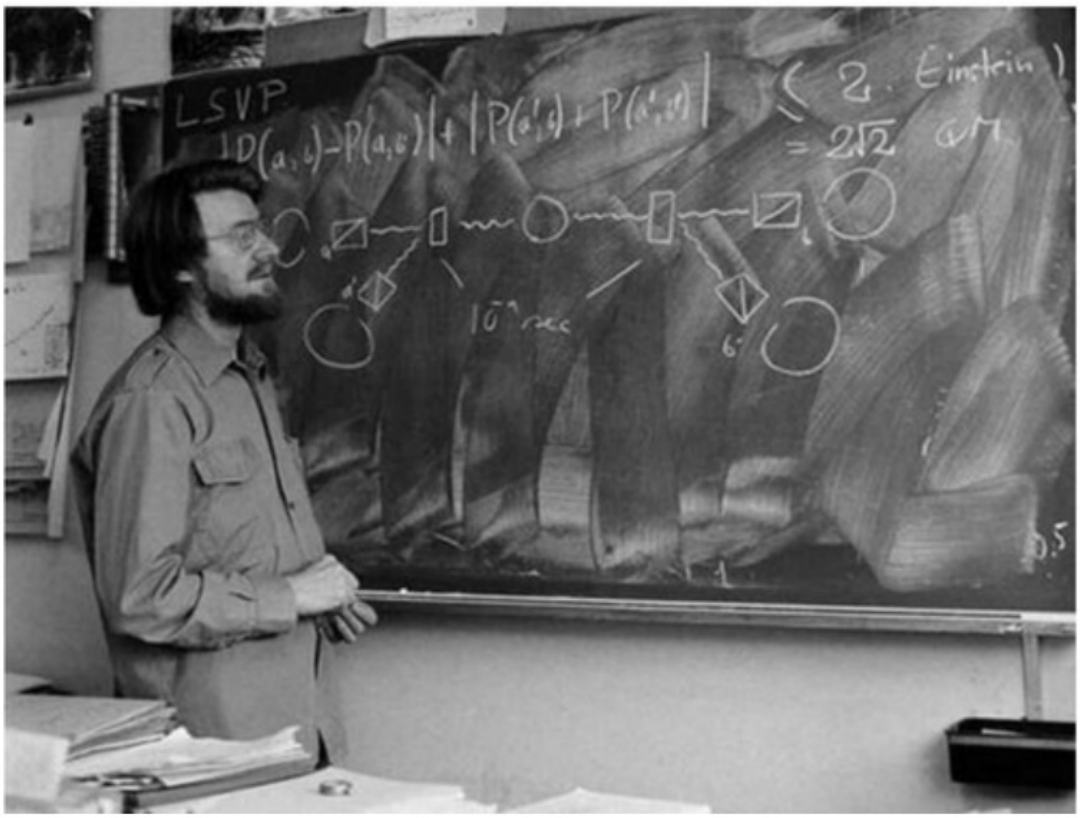
因为量子世界三大定律之一：测不准原理。

如果敌人想要截获量子密钥，必须先截获 A、B 两个纠缠态粒子，然后测一下自旋态。

问题就出在这里。

量子态不是先天决定的，而是被你的测量决定的：你测了，它就从魔法般的量子纠缠态，变成平淡无奇的确定态了。

还记得前面提到的工程师贝尔吗？



约翰·贝尔

他发明的「贝尔不等式」原理，就是用来检测纠缠态粒子之间是否存在「超距作用」。

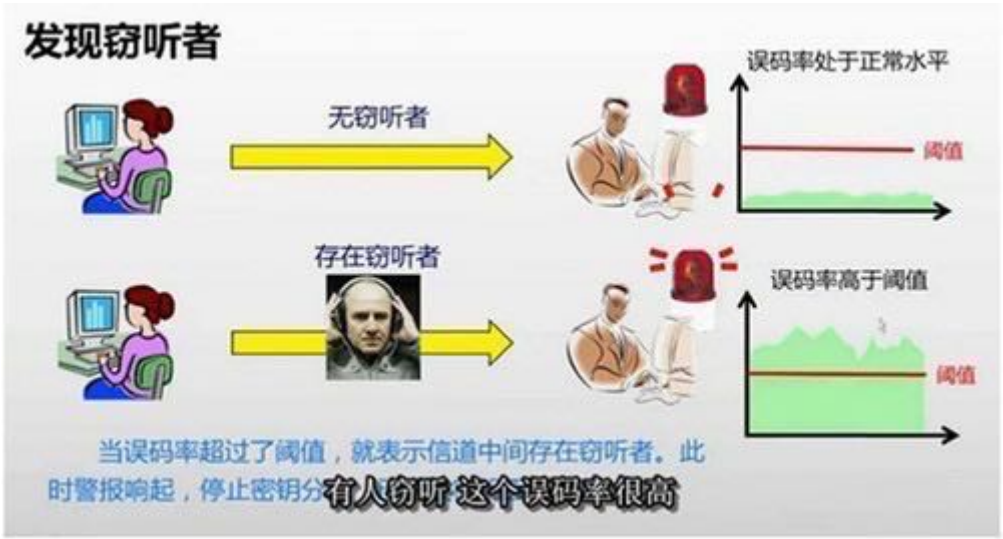
当被敌人测过的 A、B 粒子到达我们的同志手中，他们只要做一件事，就能看出量子密钥是否被动过手脚：用阿斯派克特实验

验证贝尔不等式——如果发现 A、B 之间的超距作用已然消失，只能说明一件事：在我方测量之前，已经有人测过了。

虽然在原理上，通过验证贝尔不等式已经足以确保信道的安全，然而在实际应用中，做阿斯派克特实验实在太麻烦了。

所以量子通信卫星「墨子号」用的是更先进的量子密钥分配协议——BB84 协议。和原版量子纠缠通信的不同之处在于，它利用光子的偏振方向（而非自旋态）产生随机化的 0 和 1（量子比特）。

当然，BB84 的安全性同样依靠量子「测不准原理」：窃听者对量子信号的测量会改变信号本身，导致接收方收到的信号中乱码大增，从而暴露了自身的存在。



从军事的角度来说，比无法破解的通信更安全的，是无法窃听的通信；比无法窃听的通信更安全的，是能发现窃听者的通信；比能发现窃听者的通信更安全的，是我能发现有人窃听，但窃听者却不知道被我发现了的通信。

「不被窃听」很重要，「发现窃听者」很重要，这些都容易理解，但为什么「窃听者不知道被我发现」更重要呢？

因为，如果窃听者不知道他已经暴露了，我军可以将计就计，故意发一些假消息引君入瓮！把谍战的主动权抓到自己手中，在军事上，比被动地单纯反窃听更管用。

就拿二战的逆转战役「诺曼底登陆」来说，其实希特勒早就料到盟军会把赌注押在诺曼底，但盟军情报部门用了一年的时间给德军传送假情报，发出几千封加密电报供德军破译，硬是忽悠得元首大人连自己都不相信了。

量子通信就属于第三种：「我方可以轻松发现窃听，而窃听者却不知道被我发现」的加密通信，而且是当今所有已知加密手段中，唯一能做到第三层次的技术。

当然，窃听者也知道量子通信的厉害。正因为如此，没有哪个间谍敢随便窃听量子通信的信息，就算窃听到了也没人信：我怎么确定这次窃听到的情报不会把元首坑死？

而攻击量子通信的唯一方法，不是窃听、破解，只能是干扰：例如用强激光照射接收器将其「致盲」，量子信道被干扰成乱码，把敌我双方拉回到同一起跑线。

毕竟，量子通信的特长是反窃听，而不是抗干扰。

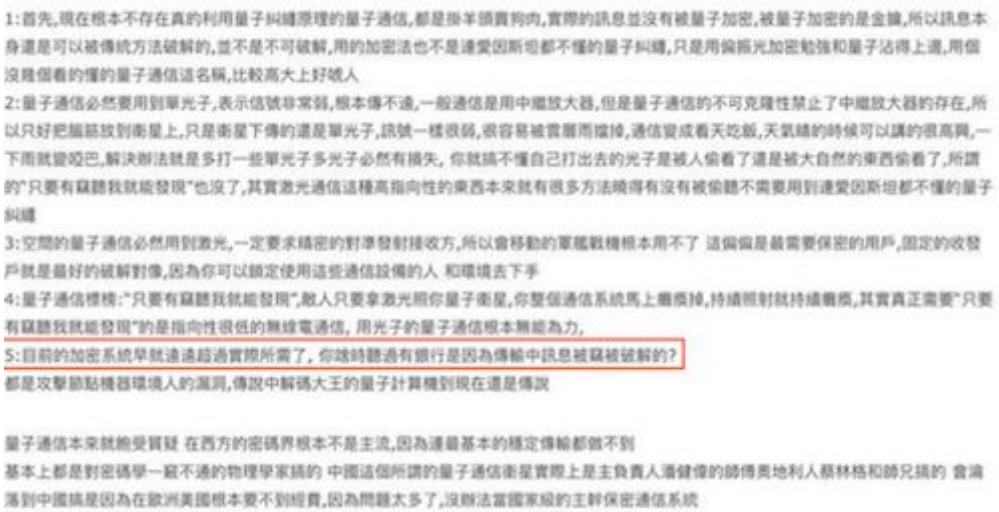
但这称不上是量子通信的弱点。其他所有传统通信方式，在干扰下都会难以为继，「无条件不受干扰」的通信，目前还没发明出来呢。

最强之矛与最强之盾

量子通信卫星「墨子号」上天之后，立刻遭到了某些民科的抵制。

有说阴谋论的，有说浪费纳税人钱的，就是没有一个能说清量子通信究竟是怎么回事。

不过，在这群流言之中，让我印象最深的，是一个网友的发帖。


1:首先,現在根本不存在真的利用量子糾纏原理的量子通信,都是掛羊頭賣狗肉,實際的訊息並沒有被量子加密,被量子加密的是金鑰,所以訊息本身還是可以被傳統方法破解的,並不是不可破解,用的加密法也不是連愛因斯坦都不懂的量子糾纏,只是用偏振光加密勉強和量子沾得上邊,用個沒幾個看的懂的量子通信這名稱,比較高大上好唬人
2:量子通信必然要用到單光子,表示信號非常弱,根本傳不遠,一般通信是用中繼放大器,但是量子通信的不可克隆性禁止了中繼放大器的存在,所以只好把腦筋放到衛星上,只是衛星下傳的還是單光子,訊號一樣很弱,很容易被雲層雨擋掉,通信變成看天吃飯,天氣晴的時候可以講的很高興,一下雨就變啞巴,解決辦法就是多打一些單光子多光子必然有損失,你就搞不懂自己打出去的光子是被人偷看了還是被大自然的東西偷看了,所謂的"只要有竊聽我就能發現"也沒了,其實激光通信這種高指向性的東西本來就有很多方法曉得有沒有被偷聽不需要用到連愛因斯坦都不懂的量子糾纏
3:空間的量子通信必然用到激光,一定要求精密的對準發射接收方,所以會移動的軍艦戰機根本用不了 這個個是最需要保密的用戶,固定的收發戶就是最好的破解對像,因為你可以鎖定使用這些通信設備的人 和環境去下手
4:量子通信標榜:"只要有竊聽我就能發現",敵人只要拿激光照你量子衛星,你整個通信系統馬上癱瘓掉,持續照射就持續癱瘓,其實真正需要"只要有竊聽我就能發現"的是指向性很低的無線電通信, 用光子的量子通信根本無能為力,
5:目前的加密系統早就過過超過實際所需了, 你啥時聽過有銀行是因為傳輸中訊息被竊被破解的?
都是攻擊節點機器環境人的漏洞,傳說中解碼大王的量子計算機到現在還是傳說

量子通信本來就飽受質疑 在西方的密碼界根本不是主流,因為連最基本的穩定傳輸都做不到
基本上都是對密碼學一竅不通的物理學家搞的 中國這個所謂的量子通信衛星實際上是主負責人潘健偉的師傅奧地利人蔡林格和師兄搞的 會淪落到中國搞是因為在歐洲美國根本要不到經費,因為問題太多了,沒辦法當國家級的主幹保密通信系統

前 4 个问题，看完前面的内容，读者应该都可以自己回答了。不过，起码人家还说对了一点：「目前的加密系统早就超过实际所需了，你啥时听过有银行是因为信息窃听被破解的？」

讲真，目前的加密系统并不是没法破解，而是破解成本太高。就拿银行最常用的非对称加密算法 RSA 来说，2009 年，为了攻破一枚 768 比特的 RSA 密钥，一台超级计算机足足算了几个月，这几乎是当今计算机性能的极限！

虽然理论上，RSA-768 已不再安全，但由于 RSA 算法的破解难度随着密钥长度指数级上升，所以让 RSA 再次固若金汤非常简

单：把密钥位数加长到 1024 比特，就会让破解时间增加 1000 多倍。

其实，现在网上交易最普遍的 RSA 密钥，至少是 2048 比特。然而，在互联网时代大获成功的 RSA 加密，真的能让我们高枕无忧地用上 500 年吗?

未必!

RSA 加密的前提是「加密容易解密难」。在 RSA 的核心算法中，用到了大数因式分解：把两个素数相乘(A*B=C)，比把这个乘积 C 做因式分解还原出 A 和 B 容易得多，数字 C 的位数越多，因式分解的时间就越长。

你可以挑战一下：

1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413

你能看出它其实不过是

3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308773781446799489

和

3674604366679959042824463379962795263227915816434308764267602283815739666511279233373417143396810270092798736308917

的乘积吗？

但是，有没有这样一种可能：随着算力越来越强，解密的时间越来越短，会不会有朝一日再长的密码都可以秒破呢？甚至，有没有可能出现，解密的速度比加密还快的尴尬局面？

这就是困扰计算机系的同学们 50 年的经典问题：P 是否等于 NP？

P 就是能在多项式时间内解决的问题，NP 就是能在多项式时间验证答案正确与否的问题。抛开复杂的定义不谈，P=NP 实际上问的是：如果答案的对错可以很快验证，它是否也可以很快计算？

一开始人们觉得，P 显然不等于 NP。

比如，「找出大数 53308290611 是哪两个数的乘积？」很难，但要问「224737 是否可以整除 53308290611？」这小学生都会算。

在密码学领域，这正好是我们想要的结果：加密（相乘）容易解密（因式分解）难。

如果 P=NP，就势必存在一种算法，使得对 53308290611 做因式分解和验证 224737 是否是因子一样快（加密和解密同样容易）。

如果 P 真的等于 NP，为什么这么多年，都没人想出这种逆天的算法呢？

然而，令人细思恐极的是，我们至今还没法严格证明 P 不等于 NP，反而有人发现，在某种特定的计算模型下： **P=NP** 竟然是成立的！

这种 「特定的计算模型」 叫作 量子计算机 。和非 0 即 1 的传统计算机不同，量子计算机的「量子比特」可以处于「既是 0 又是 1」的量子态。

在量子世界，这种不可思议的「既死又活」，反而是最平常的现象：量子叠加态。还记得薛老师那只不死不活、又死又活的混沌猫吗？

量子叠加，使得量子计算机具有传统计算机做梦都想不到的超能力：

在一次运算中，同时对 2^N 个输入数进行计算。

举例说：

如果变量 X=0，

运行 A 逻辑；

如果变量 X=1，

则运行 B 逻辑。

这种最普通不过的条件判断程序，在传统计算机内部，永远只会执行 A 或 B 的一种逻辑分支，除非把 X=0 和 X=1 的两种情况各运行 1 次（共运行 2
次）。

但对于量子计算机，A 和 B 在一次计算中就同时执行了，因为变量 X 是量子叠加态，既等于 0，又等于 1，这就意味着，普通计算机要算 2
次的程序，量子计算机只需算 1 次。

如果把量子比特的数量增加到 2 个：

如果变量 X=00，运行 A；

如果变量 X=01，运行 B；

如果变量 X=10，运行 C；

如果变量 X=11，运行 D。

有了 2 个量子比特，普通计算机要算 4 次的程序，量子计算机也只要算 1 次。

如果把量子比特加到 10 个，那么普通计算机要算 2^10=1024 次，或用 1024 个 CPU 同时算的程序，量子计算机只需要用 1 个 CPU 算
1 次。

看出问题的严重性了吗?

把量子比特加到 100 个以上，那么，当今地球上 所有计算机同时运行 **100** 万年的工作量，量子计算机干完只要几分钟!

对于曾经需要消耗巨大算力才能破解的 RSA 加密，这是一个灾难性的未来。

1994 年，全球 1600 个工作站同时运算了 8 个月，才破解了 129 位的 RSA 密钥。若用同样的算力，破解 250 位 RSA 要用 80 万年，1000 位则要 10^25 年——而对于量子计算机，1000 位数的因式分解连 1 秒钟都不到。

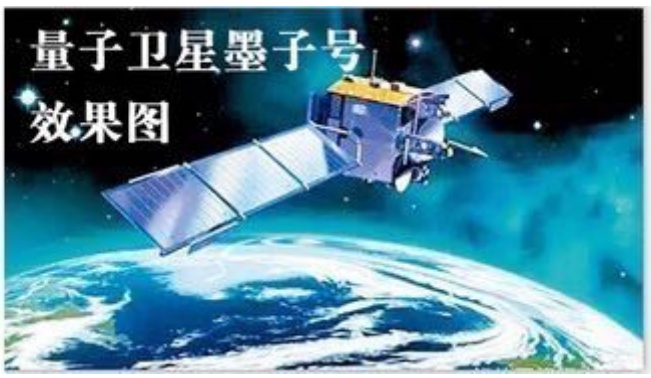
在量子计算机的最强之矛面前，现在最流行的 RSA 加密将无密可保，所有基于 RSA 的金融系统将瞬间变成透明人。

唯一能防住量子计算机的，只有最强之盾：量子加密通信。

和 RSA 等依赖计算复杂度增加破解成本的加密方式不同， 量子加密通信是「无条件安全」的，对量子计算机的恐怖计算能力先天免疫。

虽然量子比特的制备极为困难，目前最高纪录只有可怜的 5 个量子比特，但谁也不知道，量子计算机的爆发——或者说传统加密的末日，将会在何时到来。

这就是为什么，在广大人民群众一片「看不懂」的声音中：量子通信卫星「墨子号」上天了；京沪量子通信干线快建成了；工商银行在北京用上了量子通信做同城加密传输；阿里云的数据中心已经在用量子通信组网。



暂时落后的欧盟，也信誓旦旦，要在 2018 年投入 10 亿欧元做量子通信。

就连扎克伯格未满月的女儿，都让他爹读《宝宝的量子物理学》。

你还觉得这种高深的学问，懂不懂也没什么关系，反正全世界也没几个人能懂?

未来，已来。