

## 量子通信卫星很难懂？其实和异地恋像极了……

两千多年前，墨子在《经说下》中写下“光之人，煦若射。”这一句，并意识到“光沿直线传播”这一现象。

两千多年后，2016年8月16日，以“墨子”命名的量子科学实验卫星“墨子号”升空，将利用“光”继续书写人类信息传输的未来。

如今，设定使用寿命仅2年的“墨子号”，已经在轨道上运转6年时间，更是超额完成了不少拓展科研任务。

很多人可能看到“量子”两个字就满头疑惑，到底什么是量子？“墨子号”量子科学实验卫星进行了哪些工作？它又和“量子”有什么联系？别急，让我们一个一个了解它们的秘密。

## 重点一

什么是量子？

在生活里，我们可能经常会听到“遇事不决，量子力学”这句话，也经常会看到如“量子速读”这种打着“量子”旗号的伪科学，那么“量子”具体是什么？

这一问题其实不难理解。我们生活中的一切物体，都有构成其自身的最小单元，比如构成“水”的最基本单元是“水分子”。光也是如此，我们从一根激光笔中射出一束光线，将这束光线进行细分，分到的最基本单元就是“光子”。我们把构成物质世界的最基本单元，就叫做“量子”。“墨子号”在进行实验时使用的“量子”，就是“光子”，即“光子”。

## 重点二

“墨子号”都进行了哪些实验？

在回答这个问题前，我们先来聊聊大家比较热衷的“网购”这件事。

在手机还没有被开发出扫指纹、刷脸验证之前，我们网购下单时总需要在屏幕上输入支付密码，可能大部分人都考虑过一件事：万一我的密码被人截获了怎么办？确实，不仅是我们的支付密码，所有从A地到B地传送的通信信息，都有可能在中途被截获、破解，造成我们的信息泄露。

此刻可能有人就会想到，那么我们制作一个密码本，把我们发出的支付密码等信息先进行加密，然后在接收时候利用同一个密码本进行解密，这样不就可以完成信息加密了吗？道理是没错，但遗憾的是密码本可能会被破译甚至直接被窃取，这样一来加密也就没有任何作用了。

那难道就没有完全安全的加密方法了吗？别急，不要忘了我们今天的主角——“墨子号”。

“墨子号”的诞生，一个重要的使命就是为了保障通信安全。传统的密码本不够安全？没关系，我们用量子技术生成一个“密码本”，这个“密码本”足够随机，而且一旦被第三方截获就会被通信双方知晓。

作为量子科学实验卫星，“墨子号”有三个重要实验要完成：千公里级量子密钥(yuè)分发、千公里级星地双向量子纠缠分发，和千公里级星地量子隐形传态。在完成了这三大既定科学目标后，“墨子号”还开展了多项有重要意义的拓展实验，不断实现新的突破。

看到这些“量子”又要眼前一黑了？别紧张，它们其实并不难理解，让我通过墨子号的这三大既定科学实验来讲给你听。

## 重点三

量子密钥分发是在做什么？它有什么用？

刚才我们说到，为了保证真正的通信安全，需要用到量子技术来制作“密码本”。“墨子号”的量子密钥分发任务就是利用“墨子号”这颗卫星，通过从太空往地面发送一个个光子，来生成“密码本”。

那么这一个个光子，是如何形成“密码本”的呢？想了解这一问题，我们首先要学习一些关于光子的知识：

偏振：光子可以在某个方向上振动，叫做“偏振”，光子的偏振根据角度不同可以分为多种，但在这里我们只需要了解其中四种方向： $\uparrow$ 和 $\rightarrow$ （即偏振角度 $0^\circ$ 和 $90^\circ$ ）、 $\nearrow$ 和 $\searrow$ （即偏振角度 $45^\circ$ 和 $135^\circ$ ）；

光子偏振的几种形式，每个光子的偏振夹角为 $180^\circ$ ，所以漫画中 $135^\circ$ 光子偏振虽然为 $\searrow$ ，但其实和 $\nearrow$ 是等价的。图片来自墨子沙龙。

观测：在接收光子时，会利用一副“特制墨镜”对这些光子进行观测。这副墨镜正着摆放的时候，形态像“+”一样，可以允许 $\uparrow$ 和 $\rightarrow$ 偏振的光子通过；倾斜摆放的时候，形态就像“x”，可以允许 $\nearrow$ 和 $\searrow$ 偏振的光子通过；

比特：科学家规定，用“+”观测后，获得 $\uparrow$ 偏振的光子则代表比特“0”，获得 $\rightarrow$ 偏振的光子则代表比特“1”；同样，用“x”观测后，获得 $\nearrow$ 偏振的光子则代表比特“0”，获得 $\searrow$ 偏振的光子则代表比特“1”；

不确定性：但是，光子比较特殊。即便是 $\uparrow$ 和 $\rightarrow$ 偏振的光子，也可以通过倾斜摆放的“x”墨镜（ $\nearrow$ 和 $\searrow$ 也同样可以通过“+”）。比如，硬挤进“x”的 $\uparrow$ 偏振的光子，出来后就会变成 $\nearrow$ 或 $\searrow$ ，但具体是哪个？别问，概率都是50%，具体不清楚。

如果你还是晕晕的，那下面这个表格会让你更清晰一些：

了解了这些规则后，我们就可以开始着手发送光子、进而制作“密码本”这件事了，步骤如下：

首先，发送者会随机生成一串比特密码，比如是：01001011；

随机选择一种观测形式（“+”或“x”）；

根据随机产生的比特以及观测形式，来制备一个偏振光子，例如：当随机产生的比特是0，观测方式是“+”时，就制备出 $\uparrow$ 偏振的光子；当随机产生的比特是1，观测方式是“x”时，就制备出 $\searrow$ 偏振的光子；

然后将光子发送给接收者；

接收者接收到这些光子后，再随机选择一个观测形式“+”或“x”对接收到的光子进行观测，获得观测结果。

最后，发送者和接收者再打个电话沟通一下他们各自的观测方式，将相同观测方式时的结果保留下来，其他的舍弃，就可以获得一个完全随机产生的、安全的初始“密码本”了。

这是一项充满了“随机”的工作。

我们也看到了，接收者如果使用了“+”对 $\nearrow$ 进行观测，便会获得两种结果，即：对光子进行观测后，会使光子的偏振发生改变。这样，中途如果有第三者对光子进行截获，那么一旦使用了“错误”的观测方式，就会让光子的偏振产生改变。从而接收者和

观察者通过“对答案”（这次是交流部分初始“密码本”）就能发现问题，舍弃这次生成的“密码本”。

如此一来，获得的“0100”这串密码，就是双方生成的一次性量子“密码本”。

以上，便是“墨子号”所进行的量子密钥分发这项实验所使用的方法之一。这种方法名为BB84协议，是1984年，查理斯·本内特(Charles Bennett)和吉勒·布拉萨(Gilles Brassard)所提出的一种方法。这种方法可以有效发现通信中出现的窃听情况，从而立刻关闭通信，并重新进行新的量子密钥分发。

2017年8月，升空一年后的“墨子号”在国际上首次成功实现千公里级星地量子密钥分发实验。后来，“墨子号”还基于另一种量子密钥分发协议E91实现了无中继千公里级的量子保密通信。这为后续构建覆盖全球的量子保密通信网络奠定了可靠的技术基础。

## 重点四

量子到底在“纠缠”什么？

量子纠缠分发又是在做什么？

提到“纠缠”你会想到什么？两个人之间的心心相印？情侣之间的心有灵犀？没错，在两个量子之间也存在“心有灵犀”，科学家把量子之间的这种“心有灵犀”式的联系，称为“量子纠缠”。

在量子力学中有这样一个神秘的名词：叠加态，即对于一个量子，在没有观测它的时候，它可能是两种状态的叠加；而一旦对叠加态的量子进行观测，量子叠加态就会坍缩成其中一个状态。引用一个经典例子就是薛定谔那只既“死”又“活”的猫，被关在密闭容器里的猫身上叠加着“死”和“活”两种状态，这便是猫的“叠加态”；而我们一旦打开盒子，猫的叠加态就会坍缩，我们就可以知道猫到底是“死”是“活”。

而量子纠缠，是两个量子的组合的某种奇特的叠加态，它们之间“冥冥中自有定数”——一旦其中一个量子被观测，另一个量子的状态也会立刻被知晓。再次用猫咪举例便是：我有两只被关在密闭盒子中的猫，它们都处在“生”或“死”的叠加态，而且它们是“纠缠”在一起的，即如果我打开一个盒子，看到了一只叠加态坍缩为“死”的猫，那么另外一个盒子里的猫的叠加态也会坍缩，而且一定坍缩为“生”。

这种量子纠缠是不受距离限制的，是“非定域性”的。即便是一只猫在地球上，另一只猫在宇宙的另一角，这种奇特的联系仍然会瞬时发生。爱因斯坦将这种跨越空间的量子纠缠现象称为“鬼魅的超距作用”，他对此感到忧心忡忡，转而提出“定域隐变量理论”来解释这种神奇的联系。

为了验证孰对孰错，物理学家贝尔提出了一个不等式和一个实验方法，如果实验结果符合不等式，那么就支持爱因斯坦的“定域性”理论；如果实验结果违背了不等式，则驳斥了爱因斯坦的“定域性”理论。

可惜，实验结果并没有站在爱因斯坦这边，量子力学中的这种“鬼魅的超距作用”是真实存在的，量子纠缠确实是“非定域性”的。实验是检验真理的唯一标准，真理来自于严密的实验结果，即便提出反对的是爱因

斯坦。

直至今日，许多科学家仍然在进行着贝尔提出的这个量子纠缠实验：将两个纠缠态量子放在足够远的距离，随后进行观测，看得出的观测结果是否符合贝尔不等式。同样，我国也在云南丽江和青海德令哈两个地面站之间进行了量子纠缠实验，并且是全世界最远——相距1200千米的量子纠缠实验。

“墨子号”的作用，就是在太空中向这两个地面站发射一对纠缠的量子。这个实验的成功，为将来我国基于量子纠缠的量子保密通信打下了基础。2020年，墨子号实现了基于纠缠的千公里级量子保密通信。

通过“墨子号”卫星进行量子纠缠分发，来验证贝尔不等式。图片来自墨子沙龙。

## 重点五

量子隐形传态是什么？

可以实现远程物质传输吗？

在回答这个问题前，我们先来看一个异地恋小故事：

有一对情侣A和B，其中B比较恶毒，但双方依然进行着异地恋，相互“纠缠”。同时，他们有两个共同的朋友C和D，分别在两地观察着A和B。

有一天，A遇到了X，X不像B那么恶毒，很友善，于是A和B断绝“纠缠”，和X在一起，开始一种新的“纠缠”。

此时朋友C观察到这一事件，拍了照片告诉了朋友D，D看了照片之后，对B进行了一些友谊上的教育，B被教育后幡然醒悟，弃恶从善，从此也变成像X一样变成了一个善良的人。

在这个例子里，我们可以将A和B作为两个纠缠的量子，C和D分别为A和B所在位置的科学家，而X则是未知量子态，科学家希望通过“量子隐形传态”的方式将这一未知量子态传送到B上。

整个传输过程中，量子X本身并没有被传送，而是X的状态被传送到B上——正如异地恋例子里X善良的状态传给了B，从而让B的状态也从“恶毒”变成了“友善”。这便是“量子隐形传态”。不过要注意的是，在“量子隐形传态”时，A和B的纠缠消失，和A和X产生新的纠缠，几乎是同时发生的。

你会发现，在“量子隐形传态”中，只是把量子X的状态进行了传输，而量子本身并没有被传送。这和科幻作品中的物质远程传送有很大区别，想将物体通过量子技术从A地传送到B地，目前来看还不现实。

## 重点六

“墨子号”到底能为我们做什么？

如果你看到这里，那么恭喜你，你已经基本了解了“墨子号”量子科学实验卫星所承载的三项主要科学实验是什么了。不过这时你可能会问：这三个实验，对我又会有什么影响呢？

每一个新理论的发现和新技术的实现，从根本上都代表着人类对未知世界迈出新的一步。“墨子号”是我国最先进的量子通信技术结晶，在国际上也是领先水平。量子通信技术已经开始出现在民用和商用领域，在未来，更加成熟的量子通信技术将会更广泛地应用在通信、金融、国防等诸多方面。

