

划时代的量子通信——写给世界第一颗量子科学实验卫星“墨子号”

张文科

(中国科学技术大学上海研究院 201315, 中国科学院量子信息与量子科技前沿卓越创新中心 230026)

2016年8月16日凌晨1点40分,人类历史上第一颗用于量子通信研究的“墨子号”量子科学实验卫星在我国酒泉卫星发射中心发射升空(图1)。该卫星由中国科学技术大学和中国科学院上海技术物理研究所共同研制,经过前期准备,于2012年正式立项,并历时多年研制成功。该卫星将配合多个地面站实施星地量子密钥分发、星地量子纠缠分发和地星量子远程传态等量子通信领域的实验。



图1 长征二号丁运载火箭将世界首颗量子科学实验卫星发射升空
(新华社记者金立旺摄)

量子通信属于量子信息领域中最先实用化和产业化的方向,而量子信息是以量子物理学为基础的新一代信息科学技术。主要包含两个方面,一个是信息的传输,即量子通信。另一个是信息的处理,即量子计算。

自量子力学诞生以来,物理学家通过认识各种宏观物质背后的量子力学规律,产生了凝聚态物理学和量子光学等学科方向,并在此基础上发展出了各种高新技术来改变世界。例如通过量子力学研究中电子性

质而发现了半导体,通过量子力学研究电子能级受激辐射光子而发现了激光。在此基础上,20世纪50年代,物理学家们开始陆续研制出了半导体晶体管和激光器,从而催生了第一次信息革命,使得我们今天能便捷地使用各种计算机、智能手机和互联网。

但是第一次信息革命是属于“经典信息”的革命,虽然我们用量子力学才能理解半导体和激光的本质与工作原理,我们所处理的还是经典的二进制信息(即经典比特)。信息传输和计算都基于经典物理学规律。随着量子信息科学技术的诞生,这一条路逐渐发展到了一个全新的阶段,催生着第二次信息革命的出现,即完全属于“量子信息”的革命。信息传输和计算都将直接基于量子物理学,其中量子通信作为排头兵,走在这次信息革命的最前面,成为它的第一个突破点。

量子通信按照应用场景和所传输的比特类型可分为“量子密钥分发”和“量子态传输”两个方向,见表1。其中“量子密钥分发”使用量子态不可克隆的特性产生二进制密钥,为经典比特建立牢不可破的量子保密通信。目前量子保密通信已经步入产业化阶段,开始保护我们的信息安全;“量子态传输”是利用量子纠缠来直接传输量子比特,将应用于未来量子计算之间的直接通信。

表1 量子密钥分发和量子远程传态的区别

量子通信类型	量子密钥分发	量子远程传态
传输的比特类型	经典比特	量子比特
是否用到量子纠缠	否	是
通信的计算机类型	经典计算机	量子计算机
是否已经产业化	是	否

本文将通过“量子密钥分发”,“量子比特与量子不可克隆定理”,“量子纠缠”,“量子远程传态”,“卫星平台量子通信”五个部分,系统性地介绍量子

通信的原理和发展趋势。

1 量子密钥分发

目前实用化的量子密钥分发是由班尼特 (C. Bennett) 和布拉萨德 (G. Brassard) 在 1984 年提出的 BB84 协议。该协议利用光子的偏振态来传输信息。

因为光子的偏振有两个相互线性独立的自由度 (即偏振态相互垂直), 所以信息的发送者和接收者可以简单选取“横竖基”, 即“+”, 和“对角基”, 即“×”, 作为测量光子偏振的基矢。在横竖基中, 偏振方向“↑”代表 0, 偏振方向“→”代表 1; 在对角基中, 偏振方向“↗”代表 0, 偏振方向“↘”代表 1。这样选择测量基的好处是: “+”和“×”不是线性独立的, 相互不正交。于是若选择“+”来测量偏振态“↗”或“↘”时, 会得到 50% 的几率为“→”, 50% 的几率为“↑”。同理, 选择“×”来测量“→”或“↑”时, 会得到 50% 的几率为“↗”, 50% 的几率为“↘”。

在传输一组二进制信息时, 发送者对每个比特随机选一个基矢, 即“+”或者“×”, 然后把每个比特 (在各自被选的基矢下) 对应的偏振光子发送给接收者。比如传输一个比特 0, 选择的基矢为+, 则对应的光子的偏振态为↑。光子可以通过不破坏偏振态的 (保偏) 光纤或者自由空间来传输, 称为“量子信道”。

接收者这边也对接收到的每个比特随机选择“+”或者“×”来测量。在测量出所有的 0 和 1 后, 接收者和发送者之间要通过经典信道 (如电话、短信、QQ 等) 建立联系, 互相分享各自用过的基矢, 然后保留相同的基矢, 舍弃不同的基矢。最终保留下来的基矢所对应的比特, 就是他们之间通过量子通讯传输的量子密钥 (表 2)。

表 2 BB84 通讯协议

发送的密钥比特	0	1	0	0	1	1	0	1
发送者选择的基矢	+	+	×	×	+	+	×	×
发送的光子偏振	↑	→	↗	↗	→	→	↘	↘
接收者选择的基矢	×	+	×	+	×	+	+	×
接收到的光子偏振	↗或↘	→	↗	↑或→	↗或↘	→	↑或→	↘
两者共有的量子密钥		1	0			1		1

通过表 2 可以看出, 只有当发送方和接收方所选择的基矢相同时, 传输比特才能被保留下来用作密钥。

如果存在信息截获者, 那么他也同样要随机选取“+”或者“×”来测量发送的比特。比如发送者选取基矢为“+”, 然后发送“→”来代表 1。如果截获者选取的基矢也为“+”, 他的截获就不会被察觉。但截获者是随机选取基矢, 那么他就有 50% 的概率选择“×”, 于是量子力学的测量特性使光子的偏振就变为 50% 的概率↗和 50% 的概率↘。

作为接收方如果选取了和发送方同样的基矢“+”, 则会把这个比特当做密钥。但是接收方测量的是经过截获的光子的偏振, 测量结果是 50% 的概率↑和 50% 的概率→。于是测量这个比特, 发送方和接收方结果不同的概率为 $50% \times 50% = 25%$ 。

因此想知道是否存在截获者, 发送方和接收方只需要拿出一小部分密钥来对照。如果发现互相有 25% 的不同, 那么就可以断定信息被截获了。同理, 如果信息未被截获, 那么二者密钥的相同率是 100%。于是 BB84 协议可以有效发现窃听, 从而切换通信信道, 重新分配密钥。换句话说, 只要能成功生成的量子密钥一定是没有被窃听过的无条件安全的密钥。

BB84 量子密钥分配协议使得通讯双方可以生成一串绝对保密的经典二进制密钥, 用该密钥给任何信息加密, 做最简单的加密 (表 3), 都会使该信息无法被解密, 从根本上保证了传输信息过程的安全性。

表 3 利用量子密钥给需要传输的原始信息做最简单的“异或”加密

原始信息	量子密钥	加密信息
0	0	0
0	1	1
1	0	1
1	1	0

在这个协议基础上, 世界各国都开展了量子保密通信网的建设。中国在这方面走在了世界最前面。中国科学技术大学潘建伟团队在合肥市实现了国际上首个全通型量子保密通信网络, 后又利用该成果为 60 周年国庆阅兵关键节点间构建了“量子通信热线”, 之后研发的新型量子通信装备在北京投入常态运行, 为“十八大”等国家重要政治活动提供信息安全保障。

科大盾量子通信技术有限公司利用所转化的成果建成了覆盖合肥城区的世界上首个规模化量子保密通信网络，标志着大容量的城域量子通信网络技术开始成熟。

2013 年国家批准立项的光纤量子保密通信“京沪干线”由中国科学技术大学承建，于 2016 年年底前建成。该干线连接北京和上海，全长 2000 余公里，是世界首条量子保密通信主干网，将大幅提高我国军事、政务、银行和金融系统的安全性。

“墨子号”量子科学实验卫星也把千公里级的星地量子密钥分发作为三个主要目标之一。以卫星为发射端，地面站为接收端，通过激光的单光子传输实现星地间的量子密钥分发，从而实现星地间的量子保密通信，并为未来天地一体化的量子保密通信网络积累技术基础。

2 量子比特和量子不可克隆定理

传统的信息技术扎根于经典物理学，一个比特在特定时刻只有特定的状态，要么 0，要么 1，所有的计算都按照经典的物理学规律进行。量子信息扎根于量子物理学，一个量子比特 (qubit) 就是 0 和 1 的叠加态，可以写作

$$|\Phi\rangle = a|0\rangle + b|1\rangle.$$

这里用 Φ 代表 0 和 1 的叠加。 $|\rangle$ 为狄拉克符号，代表量子态。 a 和 b 是两个复数，满足关系 $|a|^2 + |b|^2 = 1$ 。于是一个量子比特可以用一个 Bloch 球来表示。相比于一个经典比特只有 0 和 1 两个值，一个量子比特的值有无限个，分布在整个 Bloch 球面上 (图 2)。

量子不可克隆定理可简要证明如下： $|A\rangle$ 态和 $|B\rangle$ 态是我们想要克隆的任意量子态， $|C\rangle$ 是我们用做克隆的基矢， U 是克隆算符。量子克隆过程就是 $U|A\rangle|C\rangle = |A\rangle|A\rangle$ 和 $U|B\rangle|C\rangle = |B\rangle|B\rangle$ 。于是我们能得到等式 $\langle B|A\rangle = \langle C| \langle B|U|A\rangle|C\rangle = \langle B| \langle B|A\rangle|A\rangle$ 。该等式要求 $|A\rangle = |B\rangle$ 或者 $\langle B|A\rangle = 0$ ，即要求 $|A\rangle$ 态和 $|B\rangle$ 态完全相同，或者正交。这和 $|A\rangle$ 和 $|B\rangle$ 都是任意态的假设矛盾，因此我们无法克隆任意量子态。

窃听者在窃听经典信息时，等于复制了这份经典

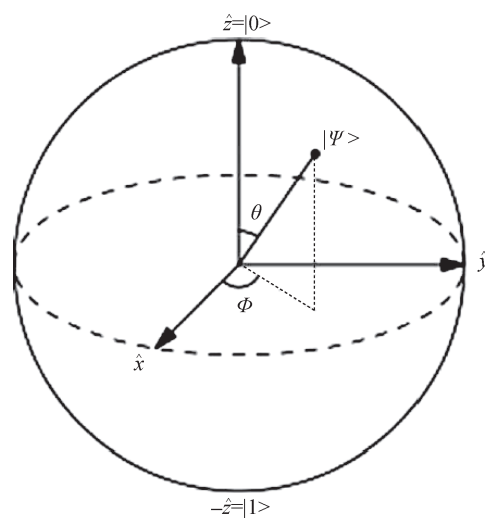


图 2 表示量子比特的 Bloch 球，球面代表了一个量子比特所有可能的取值

信息，使信息的原本接收者和窃听者各获得一份。但是在量子态传输时，因为无法克隆任意量子态，于是在窃听者窃听拦截量子通讯的时候，就会销毁他所截获到的这个量子态。

细心的读者可能会发现，如果想要克隆一个单独的量子态，或者几个相互正交的态，原理上还是可行的。但是这样的态无法提供足够的量子比特，因此不具有任何信息上的意义，也不会用到量子通信中。

在量子密钥分发里 (如 BB84 协议)，正是由于量子不可克隆定理，光子被截获时经过了测量，偏振状态就发生了改变。接收方就会察觉密码的错误，停止密码通信。这也就确保了通信时量子密码的安全性，也就保证了加密信息的安全性。

在传输量子比特时，由于量子不可克隆定理，销毁量子态就是销毁了它所携带的量子比特，于是无论是接收者还是窃听者都无法再获得这个信息。通讯双方会轻易察觉信息的丢失，因此量子比特本身具有绝对的保密性。量子不可克隆定理使得我们直接传输量子比特的时候可以不用再建立量子密码，而是直接依靠量子比特本身的安全性就可以做到信息不被窃取。

3 量子纠缠

量子力学中最神秘的就是量子叠加态，而“量子

纠缠”就是多粒子的一种量子叠加态。以双粒子为例，一个粒子 A 可以处于某个物理量的叠加态，可以用一个量子比特来表示，即 $\Phi_A = a|0\rangle_A + b|1\rangle_A$ ，其中 $| \rangle$ 为狄拉克符号，代表量子态。a 和 b 是任意两个复数，满足关系 $|a|^2 + |b|^2 = 1$ 。

同时另一个粒子 B 也可以处于叠加态，即 $\Phi_B = a|0\rangle_B + b|1\rangle_B$ 。当两个粒子发生纠缠，就会形成一个双粒子的叠加态，例如：

$$\Phi_{AB} = a|0\rangle_A |1\rangle_B + b|1\rangle_A |0\rangle_B$$

就是一个纠缠态：无论两个粒子相隔多远，只要没有外界干扰，当 A 粒子处于 0 态时，B 粒子一定处于 1 态；反之，当 A 粒子处于 1 态时，B 粒子一定处于 0 态。

用薛定谔的猫做比喻，就是 A 和 B 两只猫如果形成上面的纠缠态：

$$| \Psi \rangle = a | \text{死猫} \rangle + b | \text{活猫} \rangle$$

无论两只猫相距多远，即便在宇宙的两端，当 A 猫是“死”的时候，B 猫必然是“活”；当 A 猫是“活”的时候，B 猫一定是“死”（当然，真实的情况是，猫这种宏观物体不可能把量子纠缠维持这么长时间， 10^{-30} s 内就会解除纠缠。但是基本粒子是可以长时间保持纠缠，比如光子）。

量子纠缠态最早得到重视，正是始于爱因斯坦对量子力学的批评。量子力学在 20 世纪 20 年代诞生以后，爱因斯坦认为量子力学是不完备的，不符合自己根据相对论提出的“局域实在原理”（local realism）：(1) 物质实体独立于任何测量而存在；(2) 物质之间的任何影响都是时空局域的，即不能超过光速。

1935 年，爱因斯坦和波多尔斯基 (B. Podolsky)、罗森 (N. Rosen) 一同提出了著名的 EPR (即 Einstein—Podolsky—Rosen) 佯谬，用来论证量子力学的不完备性：根据海森堡的不确定关系，无法同时测量一个粒子的位置和动量的精确值。于是 EPR 佯谬设想两个相互作用的粒子 A 和 B，总动量确定（即一个 EPR 对）。当两个粒子分隔相距很远时，测量 A 的位置可得到精确值；同时测量 B 的动量也可得到精确值，从而计算出 A 的动量的精确值，这就同时精确测量了 A 的位置和动量，违反了不确定关系。这种跨越空间的瞬间影

响双方的量子纠缠曾经被爱因斯坦称为“鬼魅的超距作用”（spooky action at a distance）。

但现实世界不是这样。因为粒子 A 和 B 处于“纠缠态”，即共同组成一个纯的量子态，当你精确测量 A 的位置时，影响到了 B，使你无法精确测量 B 的动量，反之亦然。因为两个粒子已经相距很远并且无相互作用，于是 EPR 文章中认为量子纠缠暗示了：(1) 要么这两个粒子存在某种超过光速的非局域 (nonlocal) 相互作用而违背相对论。(2) 要么量子力学的描述是不完备的，存在未知的“隐变量”来抵消这种非局域相互作用，使 A 和 B 依然符合局域实在原理。EPR 的论文倾向于后者，随后经过美国物理学家波姆 (D. Bohm) 的发展而成为“局域隐变量理论”。

1964 年爱尔兰物理学家贝尔推导出了一个不等式，可以用来判定量子力学和隐变量理论谁正确。如果实验结果符合贝尔不等式，则隐变量理论胜出。如果实验结果违反了贝尔不等式，则量子力学胜出。

贝尔不等式 (Bell's inequality) 的原始形式如下：

$$C_h(a, c) - C_h(b, a) - C_h(b, c) \leq 1.$$

令一个纠缠源连续不断地发出一对一对的纠缠粒子，用 a, b, c 代表测量两个纠缠粒子自旋（对光子来说是偏振）的三个任意测量方向，h 代表隐变量理论。于是 $C_h(a, b)$ 代表隐变量理论在对纠缠粒子对中一个粒子在 a 方向、另一个粒子在 b 方向上测量到的偏振结果的计数比：

$$C_h(a, b) = \frac{N_{++} + N_{--} - N_{+-} - N_{-+}}{N_{++} + N_{--} + N_{+-} + N_{-+}}$$

其中 N_{\pm} 就是纠缠粒子对中的一个在 a 方向透过，另一个在 b 方向没有透过。其他以此类推。

根据隐变量理论，在 a, b, c 三个方向的测量计数比要符合贝尔不等式。但是根据量子力学的计算结果，在这三个方向的测量计数比会违反贝尔不等式，也就是上面贝尔不等式的右边会出现大于 1 的结果。

80 年代，克劳泽 (J. Clauser)、弗里德曼 (S. Freedman) 和阿斯派克 (A. Aspect) 等人的一系列实验证实了量子纠缠的确违反贝尔不等式，从而否定了局域隐变量的存在。后续的一系列检验贝尔不等式的实验也都证实量子力学是对的，量子纠缠就是非定域的，

因此爱因斯坦的定域性原理必须舍弃。2015 年的无漏洞贝尔不等式测量实验，基本宣告了定域性原理的死刑^[1]。最新的一些理论研究提出，微观的量子纠缠和宏观的热力学第二定律，甚至是时间之箭的起源都有着密不可分的关系^[2]。

随着量子信息学的诞生，量子纠缠已经不仅仅是一个基础研究，它已经成为了量子信息科技的核心。例如，利用量子纠缠可以完成量子通信中的量子远程传态，可以完成一次性操作多个量子比特的量子计算。让更多的粒子纠缠起来是量子信息科技不断追寻的目标。

中国科学技术大学潘建伟团队从 2004 年开始，通过一个个在国际上原创的多光子干涉和测量技术，一直保持着纠缠光子数的世界纪录^[3]。2004 年在世界上第一个实现了 5 光子纠缠^[4]，2007 年在世界上第一个实现了 6 光子纠缠^[5]，2012 年在世界上第一个实现了 8 光子纠缠^[6]，并且保持该记录至今。2016 年 1 月潘建伟院士团队通过“多光子纠缠和干涉度量学”获得了 2015 年度国家自然科学一等奖。

“墨子号”量子科学实验卫星就把远距离量子纠缠分发来检验贝尔不等式作为三个主要目标之一。通过卫星对地面相隔千公里的两个站做量子纠缠分发，首次在千公里级的距离上检验贝尔不等式，验证量子力学的非定域性，比目前地面最远的实验(143 km)整整高了一个数量级。

4 量子远程传态

量子纠缠是非局域的，即两个纠缠的粒子无论相距多远，测量其中一个的状态必然能同时获得另一个粒子的状态，这个状态的获取是不受光速限制的。于是物理学家自然想到了是否能把这种跨越空间的纠缠态用来进行信息传输？于是基于量子纠缠态的量子通信便应运而生，这种利用量子纠缠态来传输量子比特的通信就是“量子远程传态”(quantum teleportation)。

量子远程传态虽然借用了科幻小说中隐形传态(teleportation)这个词，但实际上和科幻中的隐形传态关系并不大。它是通过跨越空间的量子纠缠来实现对量子比特的传输。量子远程传态的过程(即传输

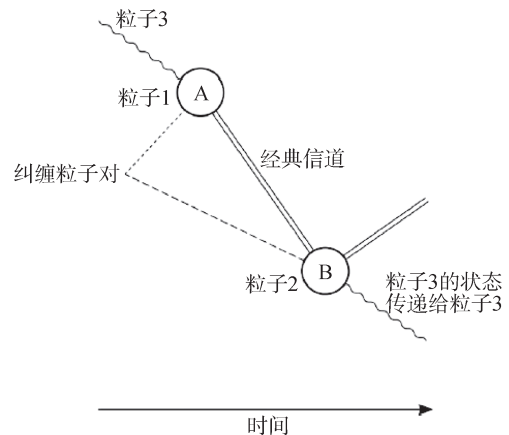


图3 量子远程传态示意图

协议)一般分如下几步(图3):

(1) 制备一个 EPR 对。将其中一个粒子发射到 A 点，另一个发送至 B 点。两个粒子之间的纠缠态为如下四个“贝尔基”(Bell states)之一:

$$|\phi_+\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle),$$

$$|\phi_-\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle - |1_A 1_B\rangle),$$

$$|\varphi_+\rangle = \frac{1}{\sqrt{2}}(|0_A 1_B\rangle + |1_A 0_B\rangle),$$

$$|\varphi_-\rangle = \frac{1}{\sqrt{2}}(|0_A 1_B\rangle - |1_A 0_B\rangle).$$

(2) 在 A 点另一个粒子 C 携带想要传输的量子比特 $|\psi\rangle = a|0_C\rangle + b|1_C\rangle$ 。假设 A 点和 B 点的 EPR 对处于的纠缠态为 $|\phi_+\rangle$ ，则 EPR 对和粒子 C 形成的总的态，由如下 4 个态等概率叠加而成:

$$\frac{1}{\sqrt{2}}(|0_A 0_C\rangle + |1_A 1_C\rangle)(a|0_B\rangle + b|1_B\rangle),$$

$$\frac{1}{\sqrt{2}}(|0_A 0_C\rangle - |1_A 1_C\rangle)(a|0_B\rangle - b|1_B\rangle),$$

$$\frac{1}{\sqrt{2}}(|0_A 1_C\rangle + |1_A 0_C\rangle)(a|0_B\rangle + b|1_B\rangle),$$

$$\frac{1}{\sqrt{2}}(|0_A 1_C\rangle - |1_A 0_C\rangle)(a|0_B\rangle - b|1_B\rangle).$$

在 A 点的一方用某个贝尔基同时测量 EPR 粒子和粒子 C，得到测量结果为以上 4 个态之一。这个测量使得 EPR 对的纠缠解除，而 A 点的 EPR 粒子和粒子 C 则纠缠到了一起。

(3) A 点的一方利用经典信道(就是经典通讯方式，

如电话或短信等)把自己的测量结果告诉 B 点一方。

(4)B 点的一方收到 A 点的测量结果后,就知道 B 点剩下的 EPR 粒子处于哪个态。如果 A 点一方的测量结果是 4 个态里的 1 或 3,则 B 点的一方不需要任何操作,A 点到 B 点的隐形传态实现。如果测量结果是 2 或 4,则 B 点的一方需要对 B 点的 EPR 粒子做一个幺正变换,将其变为 $a|0_B\rangle + b|1_B\rangle$,于是隐形传态实现。

以上就是通过量子纠缠实现量子远程传态的方法,即通过量子纠缠把一个量子比特无损地从一个地点传到另一个地点。这也是量子比特无损传输目前最主要的研究方向。

需要注意的是,由于步骤 3 是经典信息传输而且不可忽略,因此它限制了整个量子远程传态的速度,使得量子远程传态的信息传输速度无法超过光速。

因为量子计算需要直接处理量子比特,于是“量子远程传态”这种直接传的量子比特传输将成为未来量子计算之间的量子通信方式。未来量子远程传态和量子计算机终端可以构成纯粹的量子信息传输和处理系统,即量子互联网。这也将是未来量子信息时代最显著的标志。

“墨子号”量子科学实验卫星就把远距离量子远程传态作为三个主要目标之一。通过地面站到卫星的纠缠光子发射,共享纠缠光子对。在地面站制备需要传输的量子比特,通过隐形传态将该量子比特发到卫星上。这将是人类第一次在空间尺度上实现量子比特传输。

5 基于卫星的量子通信

2016 年 8 月 16 日,中国成功发射了世界第一颗量子科学实验卫星“墨子号”,用于探索卫星平台量子通信的可行性。

基于卫星等航天器的空间量子通信有着地面光纤量子通信网络无法比拟的优势。第一个原因是,在同样距离下,光子在光纤中的损耗远高于自由空间的损耗。因为光子在自由空间的损耗主要来自光斑的发散,大气对光子的吸收和散射远小于光纤。第二个原因是,受到地面条件的限制,很多地方无法铺设量子通信的

专用光纤。因此想建设覆盖全球的量子通信网络,必需依赖多颗量子通信卫星。

该卫星由中国科学技术大学和中国科学院上海技术物理研究所共同研制,卫星上装备了量子密钥通信机、量子纠缠发射机、量子纠缠源等载荷设备,是世界上第一个太空中的量子通信终端。与此同时,地面配备了北京兴隆、云南丽江、乌鲁木齐南山、青海德令哈四个地面站用于星地量子密钥分发和星地量子纠缠分发实验,并配备了西藏阿里地面站用于地星量子远程传态实验。

“墨子号”的成功研制并发射,使得中国进一步扩大了在量子通信领域世界领先的优势。欧洲和美国也感受到了危机,并提出了一系列追赶计划。欧盟在 2016 年 3 月提出的十亿欧元量子技术项目《量子宣言》(quantum manifesto)中,将地面和卫星之间的量子保密通信作为一个主要目标。美国国家科学基金(NSF)也启动了 1200 万美元的量子保密通信项目。因此“墨子号”和后续多颗量子通信卫星计划会进一步引发量子通信的国际竞争,加速全球量子保密通信网络的实现。

以中华文明的物理学创始人墨翟(墨子)命名,“墨子号”量子科学实验卫星将开创人类量子通信卫星的先河,在实现一系列量子通信科学实验目标的同时,尝试通过地面站与地面光纤量子通信网络链接,为未来覆盖全球的天地一体化量子通信网络建立技术基础。

参考文献

- [1] Hensen B *et al.* Nature, 2015, 526: 682
- [2] Short A J, Farrelly T C. New Journal of Physics, 2012, 14: 013063; Malabarba A S L *et al.* Phys. Rev. E, 2014, 90: 012121
- [3] Pan J W, Chen Z B, Lu C Y *et al.*, Reviews of Modern Physics, 2012, 84: 777
- [4] Zhao Z, Chen Y A, Zhang A N *et al.* Nature, 2004, 430: 54
- [5] Lu C Y, Zhou X Q, Gühne O *et al.* Nature Physics, 2007, 3: 91
- [6] Yao X C, Wang T X, Xu P *et al.* Nature Photonics, 2012, 6: 225

本文选自《物理》2016 年第 9 期