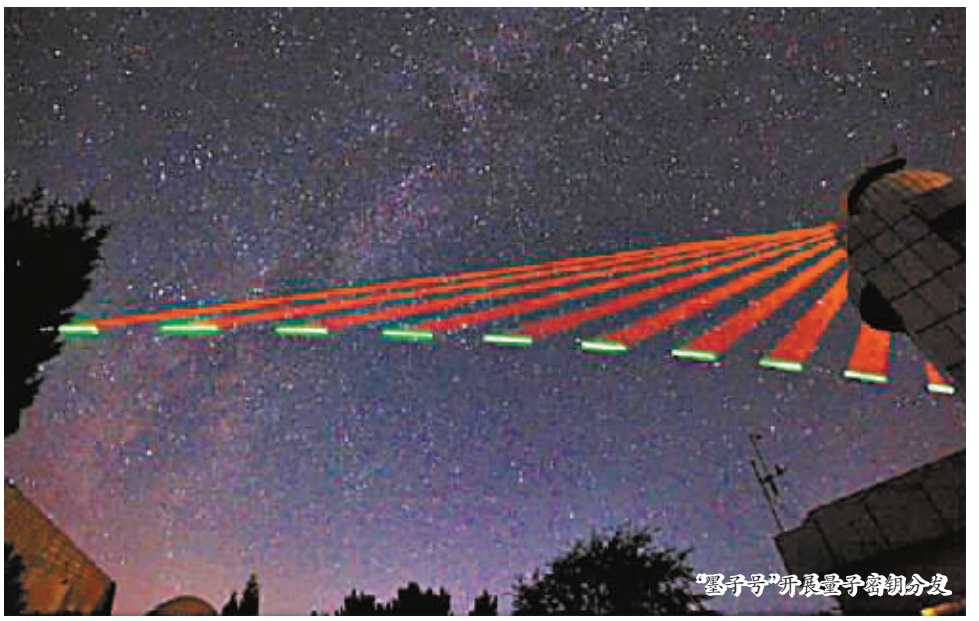
達州晚報
天下·连载
12
2017年8月11日
星期五

我国成功从太空发送不可破解密码

——“墨子号”通信卫星提前实现既定科学目标

中国“墨子号”量子科学实验卫星在国际上首次成功实现从卫星到地面的高速量子密钥分发，为建立最安全保密的全球量子通信网络奠定了可靠基础。



“墨子号”开展量子密钥分发

“墨子号”的这一成果发表在10日出版的国际权威学术刊物《自然》杂志上。《自然》杂志的审稿人称赞星地量子密钥分发成果是“令人钦佩的成就”和“本领域的一个里程碑”。

量子卫星首席科学家、中国科学院院士潘建伟说，“墨子号”量子密钥分发实验采用卫星发射量子信号，河北兴隆与新疆南山地面站分别接收的方式，在北京和乌鲁木齐之间建立了量子密钥。

据介绍，“墨子号”过境时与地面光学站建立光链路，通信距离从645公里到1200公里。在1200公里通信距离上，星地量子密钥的传输效率比同等距离地面光纤信道高20个数量级（万亿亿倍）。卫星上量子诱骗态光源平均每秒发送4000万个信号光子，一次过轨对接实验约10分钟可生成300kbit的安全密钥，平均成码率可达每秒1.1kbit。

“这样的密钥发送效率可以满足绝对安全的打电话或银行传输大量数据的需求。”潘建伟说。

他说，这一重要成果为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。以星地量子密钥分发为基础，将卫星作为可信中继，可以实现地球上任意两点的密钥共享，将量子密钥分发范围扩展到覆盖全球。此外，将量子通信地面站与城际光纤量子保密通信网（如合肥量子通信网、济南量子通信网、京沪干线）互联，可以构建覆盖全球的天地一体化保密通信网络。

绝对安全的保密通信

通信安全是国家信息安全和人类经济社会生活的基本需求，也是当代世界的难题。窃听、反窃听；加密、解密……这些密码学中的矛与盾处于恒久的博弈之中。

保密通信的原理在于，唯有掌握密钥，才能轻易重现传递的信息。信息的安全性主要依赖于密钥的秘密性。然而，传统加密技术在原理上存在着被破译的可能性。随着数学和计算能力的不断提升，经典密码被破译的可能性与日俱增。20世纪90年代，美国数学家肖尔证明量子计算可以攻破目前广泛使用的公钥体系。2015年11月，美国科技公司谷歌推出的D-Wave量子计算机，宣称其在解决问题时能够比其他任何计算机都快一亿倍，并能破解任何现有密钥体系。

有没有绝对安全的保密通信，让窃听、破译者无计可施？所幸的是，量子物理提供了解决这一问题的办法。如果量子计算机是针对传统密码的“利剑长矛”，那么量子密码技术就是抵御它的“坚固盾牌”。量子密码提供了一种不可窃听、不可破译的新一代密码技术。

专家介绍，与经典通信不同，量子密钥分发通过量子态的传输，在遥远两地的用户共享无条件安全的密钥，利用该密钥对信息进行一次一密的严格加密，这是目前人类唯一已知的不可窃听、不可破译的无条件安全的通信方式。

潘建伟说，量子密钥就是在A和B之间共同生成一串只有他们两边知道的随机数，然后用这个随机数来加密。量子密钥一旦被截获或者被测量，其自身状态就会立刻发生改变。截获量子密钥的人只能得到无效信息，而信息的合法接收者则可以从量子态的改变中得知量子密钥曾被截取过。将量子密钥应用于量子通信中，就是量子保密通信。与传统通话方式相比，量子保密通信采用的是“一次一密”的工作机制，通话期间，密码机每分每秒都在产生密码，一旦通话结束，这串密码就会立即失效，且下次通话不会重复使用。

潘建伟打了个比方，古人在信封上用火漆封口，一旦信件被中途拆开，就会留下泄密的痕迹。量子密钥在量子通信中的作用比火漆更彻底，因为一旦有人试图打开“信件”，量子密钥会让“信件”自毁，并让使用者知晓。

从太空突破极限

他说，量子通信通常采用单光子作为物理载体，最为直接的方式是通过光纤或者近地面自由空间信道传输。但是，这两种信道的损耗都随着距离的增加而指数增加。由于量子不可克隆原理，单光子量子信息不能像经典通信那样被放大，这使得之前的量子通信的局限在百公里量级。

“根据数据测算，通过1200公里的光纤，即使有每秒百亿发射率的单光子源和完美的探测器，也需要数百万年才能建立一个比特的密钥。因此，如何实现安全、长距离、可实用化的量子通信是该领域的最大挑战和国际学术界几十年来奋斗的共同目标。”潘建伟说。

他说，利用外太空几乎真空因而光信号损耗非常小的特点，通过卫星的辅助可以大大扩展量子通信距离。同时，由于卫星具有方便覆盖整个地球的独特优势，是在全球尺度上实现超远距离实用化量子密码和量子隐形传态最有希望的途径。从本世纪初以来，该方向已成为了国际学术界激烈角逐的焦点。

潘建伟团队为实现星地量子通信开展了一系列先驱性的实验研究。2003年，潘建伟团队提出了利用卫星实现星地间量子通信、构建覆盖全球量子保密通信网的方案，随后于2004年在国际上首次实现了水平距离13公里（大于大气层垂直厚度）的自由空间双向量子纠缠分发，验证了穿过大气层进行量子通信的可行性。2011年底，中科院战略性先导科技专项“量子科学实验卫星”正式立项。2012年，潘建伟领衔的中科院联合研究团队在青海湖实现了首个百公里的双向量子纠缠分发和量子隐形传态，充分验证了利用卫星实现量子通信的可行性。2013年，中科院联合研究团队在青海湖实现了模拟星地相对运动和星地链路大损耗的量子密钥分发实验，全方位验证了卫星到地面的量子密钥分发的可行性。随后，该团队经过艰苦攻关，克服种种困难，最终成功研制了“墨子号”量子科学实验卫星。“墨子号”于2016年8月16日在酒泉卫星发射中心发射升空，经过四个月的在轨测试，2017年1月18日正式交付开展科学实验。

量子通信在国防、军事、金融等领域应用前景广阔。有专家预测，量子通信技术可能在20至30年后对人类社会发展产生难以估量的影响。量子通信因其传输高效和绝对安全等特点，被认为是下一代通信和计算机技术的支撑性研究，也已成为全球物理学研究的前沿与焦点领域。 （据新华社）

连载

闪耀的星群

·市老促会·

4月中旬，张开基奉命率独立第二旅参加洛川战役，攻打洛川外围和洛（川）白（水）公路，与敌人反复冲杀。他指挥部队运用炸药包炸坦克的方法，最后迫使敌人后退，将其打败，并沿洛白公路追击从延安南逃之敌。连续两天两夜急行军，独立第二旅俘敌1900余人，缴获山炮、汽车、坦克等大量重武器和辎重无数。

11月，胡宗南部四个兵团集中在以大荔为中心的关中各县，对抗人民解放军。在大荔以北的永丰战役中，张开基率独立第二旅经过李家村后与敌李日基军展开了永丰镇（澄城县）大战，于11月28日仅用六个小时就全歼李军，活捉军长李日基。

1949年2月，独立第二旅整编为中国人民解放军第一野战军第三军第七师，张开基任师长。21日，张开基率第七师与第九师一起，共歼敌陕西保安第四旅旅长赵国珍以下1000余人，解放了蒲城。

7月，张开基率第七师参加关中地区最后大会战的扶眉战役。第七师作为第三军的前卫部队，直攻法门寺，力夺丁家据点，迅速渡过渭河，攻打马家庄、高王寺之敌，俘敌2900余人，缴获各种火炮40门，为西北野战军歼灭胡宗南、王治歧集团四个军倾注全力。张开基作为师长，虽曾九次负伤，但仍坚持同战士一样行军，冒着烈日，徒步行军115里，在21小时内连续作战五次，先后攻占扶风法门寺、清化镇、莫庄、洛村等许多重要集镇。

在陇东追击“二马”（马步芳、马鸿逵）的战斗中，张开基率第七师不顾疲劳，克服重重困难，连续两天急行军，于7月下旬至8月上旬，连克陇县、通渭、庄浪等要地，随即沿天宝公路挥师甘肃至省会兰州城外。

8月23日，作为担任主攻兰州的第七师师长张开基，装扮成“甘肃老乡”，带着几个年轻人，在风雨和夜幕的掩护下，机警地越过敌人一道道封锁线，沿着黄河边的一条小路，神不知鬼不觉地闯进兰州市区。在摸清了国民党驻军的布防情况和大街小道的路线之后，像以往那样，凭借亲手掌握的第一手资料，制定了周密的作战计划。尔后，他指挥所属的第十九、二十、二十一团，首先占领黄河铁桥、西门、东门、南门和飞机场，接着和兄弟部队一起，与敌人展开激烈巷战，肃清市内残敌，共俘敌7000余人，仅用十多个小时，就解放了西北重镇——兰州市，实现了8月26日中午请西北野战军司令员彭德怀进城的誓言。

兰州解放后，张开基又率第七师乘胜前进，与兄弟部队一起挺进河西走廊，占领古浪、山丹，行军17天，前进700余公里，于9月底到达张掖地区，接受了敌第八补给区、第九十一军、第一〇二军在酒泉的起义。至此，“青马”、“宁马”覆灭。张开基兼任张掖军分区司令员。

在解放战争时期，张开基指挥部队作战上百次，功勋卓著，为解放大西北做出了重要贡献。

1950年6月，张开基到南京军事学院高级班学习。毕业后，于1952年8月被任命为西北军区炮兵副司令员兼军械部部长、西北炮校校长，为西北军区炮兵部队正规化、现代化建设辛勤工作，其经验得到中央军委的肯定并转发推广。

1956年1月，张开基任陕西省军区副司令员。1966年离职休养。1985年5月享受副兵团级待遇。1986年5月回到家乡，看望父老乡亲，参加了万源保卫战战史陈列馆揭馆庆典。

1955年，张开基被授予少将军衔，荣获三级八一勋章，二级独立自由勋章，一级解放勋章。1988年7月30日荣获一级红星功勋荣誉章。

（六十三）

主编 王爱民
编辑 林 海

官方微信 dzwbwx
官方微博 dazhouxinwen

报料热线：2382258