当代世界科技

量子密钥：开启保密通信“安全锁”

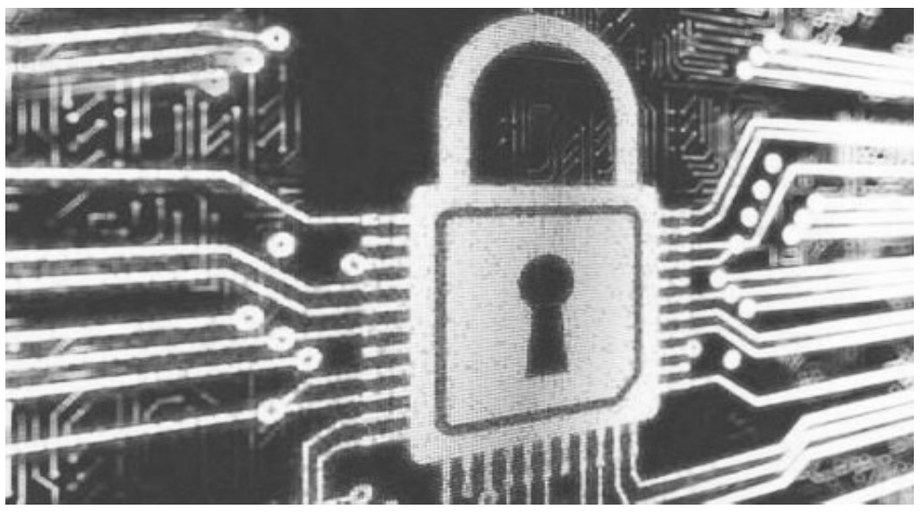
核心提示

近日，由我国自主研发的首颗量子科学实验卫星“墨子号”成功发射升空，该卫星主要用于开展高速量子密钥分发实验，并进行广域量子密钥网络实验，将在量子通信领域取得重要进展。

量子通信主要指将量子比特用作信息传输载体的新型通信技术。其中，以量子态作为符号描述密码的量子密钥技术，从理论上提供了一种不可截获和破译的绝对安全新型密码体制，将有望实现高安全等级的量子保密通信。未来，依托量子密钥技术将可组建高安全等级的保密通信网络，在信息化战场、国防建设和金融、大数据等民用领域得到广泛应用。

作为保密通信领域的“明日之星”，量子计算和量子密钥技术在最近几十年得到长足发展。利用诸如电子自旋状态和光子偏振状态的量子系统不确定性和概率性，量子密钥可以构建复杂的密码系统。由于对量子态进行测量将会改变最初的量子态，通过量子密钥建立的密码可第一时间发现密码被窃取，从而有效抵抗针对密码系统的截取重发攻击，具有高度的密码安全性。

此次发射的量子通信实验卫星，将作为跨区域量子通信地面基站的太空“二传手”，为远距离传输的光子提高信号中继，解决光子在自由空间大范围传递信号衰减问题，为构建区域量子保密通信网络构建空天“慧眼”。除进行量子密钥分发实验外，我国首颗“墨子”号实验卫星还将在空间尺度进行量子纠缠分发和量子隐形传态实验，以充分验证空间范围内量子通信系统的可行性。



□ 张乃千 唐 嘉

保密通信终圆梦

千百年来，进行安全信息传递一直是人类难以完成的梦想，不得不采取多种方法为信息传递保驾护航。《六韬》中就有利用不同长度阴符传递战场情报的记载，古罗马的凯撒密码盘和斯巴达人的“天书”密码等也提供了多种信息加密手段。第二次世界大战中，成功破译轴心国通信密码，对盟军最终取得战争胜利发挥了重要作用，至少使二战的时间缩短了8年。

事实上，无论多么高级别的密码系统，都不可避免地遭受着被破译的风险。尤其是在信息技术飞速发展的21世纪，人们对安全通信的需求越来越紧迫。为有效保护通信内容不被窃取，目前采取的主要方法就是加密通信。但现有的数据加密算法，并不能为保密通信提供绝对安全的“防火墙”。一方面，现有加密解密算法将随着数学理论的深入而遭到破解；另一方面，随着计算机技术的迅速发展，利用超级计算机针对经典加密算法进行破解已毫无技术障碍。传统加密算法已成为高悬在保密通信上方的“达摩克利斯之剑”，时刻威胁着国防、金融等领域保密通信系统的安全。

竞相研发寻安全

世界上的所有物质都是由微小粒子组成的，也就是说它们是量子化的。量子是物理量的最小单元，组成世界的基本粒子如电子、光子、原子等都是量子的表现形态。由于量子的特殊性质，实际测量时可发现量子也有多个分身。量子保密通信就是利用量子叠加原理，将量子的多个分身作为安全通信的密钥，一旦该密钥被窃听或测量，量子的其他分身态会随机消失，窃听者的存在会引入额外误码，信息发送方和接收方都可以迅速测量到这一变化，从而中断该次密钥传输，重新设定量子密钥，直至量子密钥安全传输到信息接收方。

理论上，使用量子密钥加密的通信系统不可能出现盗听现象，“守口如瓶”的量子密钥系统因为各国竞相研发而变得“炙手可热”。20世纪70年代，英国和美国最早开展量子计算领域的研究工作。早在1993年，英国国防部就首次在光纤中实现基于BB84方案的相位编码量子密钥分发实验。1999年，世界上首个量子密钥分配的无条件安全性被成功证明。近年来，世界各主要大国都在开展量子通信技术的研究工作，量子计算的理论和实践都相继取得重大进展，产生了多种新的量子算法。丹麦科学家利用集成光学方法开展的量子密码芯片研究，目前已经取得初步成果。我国科学家早在2003年就开始构想量子科学实验卫星计划，目前已成功实现量子线路长度125公里的城际量子密钥通信实验，标志着量子密钥分配系统即将进入实用阶段。

在军事应用领域，各国军队围绕密码破译与反破译的斗争早已进入“白热化”阶段，量子密钥更成为引领未来军事革命的颠覆性、战略性技术。美国国防部高级研究计划局专门制定“量子信息科学和技术发展规划”、研发量子芯片的“微型曼哈顿”计划，加速推进量子信息技术的实际应用，目前白宫和五角大楼已安装量子通信系统并投入使用。日本研究人员用量子密钥技术实现87公里的信息安全传输，德国慕尼黑大学和英国军方研究机构成功在德国和奥地利边境的楚格峰和卡尔文德尔峰之间用激光传输量子密钥。此外，英、法、德、日、瑞典等国军方也相继制定并实施一系列发展量子信息技术的计划。

应用广泛领潮流

量子信息具有信息存储容量大等突出特点，同时使用量子密钥技术为通信提供独特安全保障，充分满足信息时代传递信息安全性、准确性、高效性、大容纳量等需求，将在安全密钥、数据加密、信息隐藏和身份认证等领域得到广泛应用，势必引领保密通信领域的时代潮流。

目前对于量子通信系统的构建设想主要包括：利用光纤实现城市内部以及城市与城域量子通信网络连通，利用量子中继技术实现邻近城市之间的连接，利用卫星平台和地面站之间的自由空间光子传输实现远距离区域之间连接。通过与地面的光纤量子通信网络协同工作，多颗组网量子通信卫星将构建空间广域量子保密通信网络。未来，量子通信技术将构建跨区域范围甚至是全球范围的量子通信网络系统，并具有极高的通信安全保障。

随着世界新军事革命的蓬勃发展，信息网络已经成为连接人与武器装备的技术纽带，军事物联网和各类信息终端将成为信息化军队作战和指挥神经中枢。同时，战场侦察、指挥协同、目标预警、装备操控和后勤保障都离不开网络系统的有效支持，安全可靠的战场网络是确保遂行作战任务的重要基石。依托量子密钥开展战场保密通信，将为战时信息传递提供安全屏障，可牢牢掌握战场保密通信的“技术差”。同时，利用量子计算技术可随时破译对方网络通信密码，占据战场绝对信息优势，甚至可以直接瘫痪和控制对方通信系统和作战指挥网络，达到出奇制胜的战略目的。

当前，量子密钥技术的应用化还面临一些障碍。实际器件与绝对理论的非理想性差距将可能导致量子通信系统存在安全漏洞，能否经受得住现有手段的攻击仍需实际应用检验。此外，如何有效提高量子密钥的传输速率和传输距离，加快研制实用型量子中继器等也是仍需深入研究的问题。面对以量子密钥为代表的量子信息技术带来的机遇与挑战，只有尽早规划、提前部署、主动作为，才能在技术竞争中占据先机和主动，为开启保密通信提供安全保障。

科技与社会

网信事业发展的四个关键

□ 程 玉

网信事业代表新的生产力，新的发展方向，在践行十八届五中全会提出的“创新、协调、绿色、开放、共享”的新发展理念时可先行一步。网络安全和信息化工作将成为“十三五”时期重头戏。发展网信事业要抓住以下四个关键问题。

建设良好的网络生态

网络生态关乎网络空间意识形态的安全，维护网上意识形态安全的工作要围绕着夯实我们党的执政基础，围绕坚持中国特色社会主义道路展开。一些敌对势力利用网络煽动宗教极端主义，宣扬民族分裂思想，教唆暴力恐怖活动，这些行为要坚决予以制止和打击。对于那些利用网络进行欺诈活动、散布色情材料、进行人身攻击、兜售非法物品的言行也要坚决管控。依法加强网络空间治理，加强网络内容建设，做强网上正面宣传，用社会主义核心价值观和人类优秀文明成果滋养人心、滋养社会，做到正能量充沛、主旋律高昂，为亿万网民特别是青少年创造一个风气清明、生态良好的网络空间，维护网络主权。

尽早突破核心技术

互联网核心技术受制于人是最大隐患。若要掌握我国互联网发展的主动权、保障网络安全、维护国家安全，就必须突破核心技术这个关键难题。笔者认为，核心技术尽早取得突破、进而实现关键技术自主可控有两个重要抓手：企业和人才。

企业直接面向市场，处在掌握群众需要第一线，市场感觉敏锐，为适应市场需求，必将主动创新。要鼓励和支持企业成为研发主体、创新主体、产业主体，鼓励和支持企业布局前沿技术，推动核心技术自主创新。要加大知识产权保护力度，为企业发展营造良好环境，积极拓展海外空间。

网络空间的竞争，归根到底是人才的竞争。我国要建设网络强国，发展网信事业，必须调动企业家、专家学者、科技人员的积极性、主动性、创造性，为他们创造宽松环境、提供广阔平台。要培养网信人才，建设一流的网络安全学院。对网信领域高端人才要有特殊政策，建立适合网信特点的人才评价机制、灵活的人才激励机制，打破人才流动的体制界限。

提升网络空间攻防能力

没有网络安全就没有国家安全。网络安全的本质在对抗，对抗的本质在攻防两端的能力较量。多年来，我国的网络信息系统重建设、轻防护，导致我国重要政府网站、关键信息基础设施、工控系统面临较大风险隐患，网络安全防护能力薄弱，难以应对国家级、有组织的高强度的网络攻击。我国正在从国家层面对关键信息基础设施和重点网站进行网络安全执法检查，目的就是要摸清家底、认清风险、找出漏洞、全面整改，提高网络安全的整体防护能力。同时要建立网络安全风险报告机制、情报共享机制、研判处置机制，把握网络安全风险发生的规律、动向和趋势。

积极开展我国网信领域基础技术、通用技术、非对称技术、前沿技术、颠覆性技术的部署攻关，研究的成果要形成市场产品、技术实力、产业实力，在应用中改进完善、提高质量，拥有自主可控可攻可守的网信技术。

完善信息化建设

没有信息化就没有现代化。网信事业要发展，必须贯彻以人民为中心的发展思想。要适应人民期待和需求，加快信息化服务普及，降低应用成本，为老百姓提供用得上、用得起、用得好的信息服务；加大农村互联网基础设施投入力度，加快农村互联网建设步伐，扩大光纤网、宽带网在农村的有效覆盖；做好信息化和工业化深度融合这篇大文章，发展智能制造，带动更多人创新创业；推进农业现代化，提高农业生产智能化、经营网络化水平，帮助广大农民增加收入；发挥互联网优势，实施“互联网+教育”“互联网+医疗”“互联网+文化”等，促进基本公共服务均等化；发挥互联网在助推脱贫攻坚中的作用，推进精准扶贫、精准脱贫，让更多困难群众用上互联网，让农产品通过互联网走出乡村，让山沟里的孩子也能接受优质教育；信息是国家治理的重要依据，发挥信息在推进国家治理体系和治理能力现代化进程中的重要作用。以信息化推进国家治理体系和治理能力现代化，鼓励各级政府部门打破信息壁垒，统筹发展电子政务，构建一体化在线服务平台，提升服务效率，分级分类推进新型智慧城市建设，构建全国信息资源共享体系，更好用信息化手段感知社会态势、畅通沟通渠道、辅助科学决策。

中国为什么必须有自己的大飞机

中国自主研制C919大型民用客机，引发强烈关注。在全球大飞机供应商和消费市场相对稳定的当下，中国为什么要下决心下大气力搞大飞机？大飞机对于中华民族的伟大复兴有着怎样的特殊意义？这是首先必须在思想上搞清楚的重大问题。

□ 黄庆桥

1 新中国航空事业的曲折发展

新中国成立之初，出于国防需要，制造飞机成为必需的战略选择。不过，那时领导人考虑的主要是制造战斗机以充实空军力量，民用飞机难以顾及。即便是制造战斗机，也主要是在苏联的帮助下进行的，后来比较有名的“歼击”系列和“歼教”系列，都有很深的苏制飞机烙印。主要依靠从苏联购买和引进相关机型，同时推进国产化。大规模研制飞机并没有成为新中国成立初期国防战略的重点，而原子弹、导弹才是重中之重。这主要是因为，仅凭新中国成立初期的经济实力、工业水平和制造能力，要想在短时间内大批量造出飞机并用于实战，的确很难做到。

中国的飞机事业，尤其是大飞机事业的转折，发生在1970年。那年夏天，毛泽东在上海视察，指示上海工业基础好，要造大飞机。这样，史上被称为“708”工程的大飞机专项研制任务很快上马。大型客机“运10”的研制任务在极其艰难的状况下，快马加鞭，竟真的造出来了。遗憾的是，囿于多种主客观原因，“运10”在1980年代之初黯然下马。

1980年代中期以来，中国与麦道、波音（1996年麦道被波音兼并）的合作一次次令人沮丧地失败，让人谈大飞机而色变，在此后20年的时间里，国家竟然没有发展大飞机的战略规划。而近30年却是世界航空业深刻变革的30年。且不说军事上的战略意义，单是庞大的世界民航市场的大飞机需求，几乎被美国的波音和欧洲的空客两家公司瓜分了，为此中国每年要支付巨额资金高价购买波音和空客的大飞机。而令人惊讶的是，空客的起步，仅仅比中国“运10”大飞机的起步早3年。

2 搞大飞机有巨大的潜在经济价值

21世纪之初，在酝酿大飞机工程的过程中，其实是有很大争议的。最终，下决心搞大飞机，原因既简单又复杂。简单来说，搞大飞机的原因，就两句话：一是有钱可赚，二是具有深远的战略意义。

首先我们来看，为什么搞大飞机具有巨大的经济价值。

2009年，波音和空客分别发表了关于未来20年的全球民航市场展望的报告。大体来说，他们的展望和预测是可信的。在干线客机方面，两家航空寡头对于2009—2028年全球民用干线飞机（100座级以上）的市场需求预测是一致的，更有意思的是，他们都认为中国经济的平稳较快增长将对市场需求产生重要的推动作用。据他们估算，中国未来20年将需要新增大飞机3689—3800架，直接经济价值达到4000亿美元左右。请注意，4000亿美元仅仅是中国市场，那么全世界呢？如果我们认同和平与发展是当今世界发展的主流这一判断，那么，可以推断，全球大飞机市场的经济价值将是一个天文数字。

看到这里，可能有人要质疑了：即便你造成了大飞机，国际市场不一定买，因此，也就是咱们的国内市场，可是上面的论述却没有计算搞出大飞机要花多少钱。保守估计，大飞机项目的前期直接投资超过2000亿人民币，要真正搞成，还不知道要砸进去多少钱。因此，即便搞成了，也不一定赚钱，说不定还赔钱呢。有这样的疑问的人可能还不少，我们不妨来分析一下。

确实，如果只把未来某一段时间我们造出的大飞机的售价总和与投资总额进行比对，可能会得出不合算的结果。但是，这种做法有个极大的漏洞，就是没有考虑到大飞机产业的经济溢出效应。航空工业是知识密集、技术密集、资本密集产业，产业链很长，其发展不仅能够促进本国科技进步，而且能够带动大批相关产业的持续发展，其智力、技术和经济的溢出效应是难以估量的。仅以航空发动机的研制为例，据日本业界的一项研究，在单位重量创造的价值比这一数值上，船舶为1，轿车为9，计算机为300，支线飞机是800，而航空发动机高达1400，被称为世界工业产品“王冠上的明珠”。因此，搞大飞机赚不赚钱、合不合算，根本就不是一个问题。

3 搞大飞机有深远战略意义

其实，搞大飞机有着更为深远的战略意义，非经济价值所能衡量。

先看两个小例子。2008年汶川特大地震，中国人民难以忘却。地震发生的最初几天，震区交通中断，地面人员难以接近受灾最严重的核心区。此时，最好的救灾方式就是空投救灾人员和物资，并通过空中力量运出受灾人员。必须肯定，人民子弟兵尽了最大的努力，媒体上已有充分的报道。可是，由于汶川特殊的地形条件，能够承担救援任务的只有少量进口大型直升机。另一个例子，是关于我们的南海的。我们要更好地保护祖国南海的广袤海疆，不仅海军力量要强，空中力量也要强。相当长一段时间我们在南海处于被动的局面，与我们的海空力量薄弱有很大关系，中国远程投送能力不足，这是人所尽知的。

上面这两个例子与大飞机有什么关系呢？

现代航空业从其诞生开始，就带有明显的国防工业色彩，早期的飞机就最先用于军事用途上。因此，现代航空工业被认为是典型的“军民结合”产业，世界上所有的航空工业企业（尤其是波音和空客两大寡头）都是同时生产军用飞机和民用飞机，美国军方就一直是波音公司的最大客户。道理很简单，主要原因在于减低成本、增加利润，根本在于技术的通用性。对于一个国家而言，民机的水平上不去，军机的水平不会好到哪里去。这一点特别适合解释中国的状况。因此，中国通过搞大飞机工程，提高飞机研制的水平和能力，不仅具有潜在的经济价值，其战略意义更是不能用经济价值来衡量的。也就是说，即使搞大飞机不赚钱，我们也必须搞。我们搞大飞机，主要并不是算经济账。自2007年中国正式立项大飞机工程以来，已经不知道多少次在被西方媒体做文章了。

飞机在现代社会的特殊功能与价值日益凸显。如果说核武器是战略威慑力量，那么飞机就是战略任务的执行力量。核武器是不能轻易用的，核战争的门槛是极高的，大量的常规战略任务是要靠战略轰炸机去执行完成的。未来，重型运输机将在国家的重大紧急状态中发挥无可替代的重大作用，比如抢险救灾、大规模人员与物资的紧急调动等。并且，一旦国家进入紧急状态，95%的民用飞机都可以转为军事运输或是其他特殊用途。类似这种情况的电影镜头在美国大片中已是司空见惯的了。因此，对中国而言，不是要不要搞大飞机的问题，而是怎么样又好又快搞成的问题。

上世纪50年代，毛泽东就曾说过：“我国是一个大国，世界上有的东西，我们不能样样都有，但是重要的东西，如飞机和汽车，我们就一定要有。”或许，国产C919大飞机就是对这句话的最好回应。

科技战略