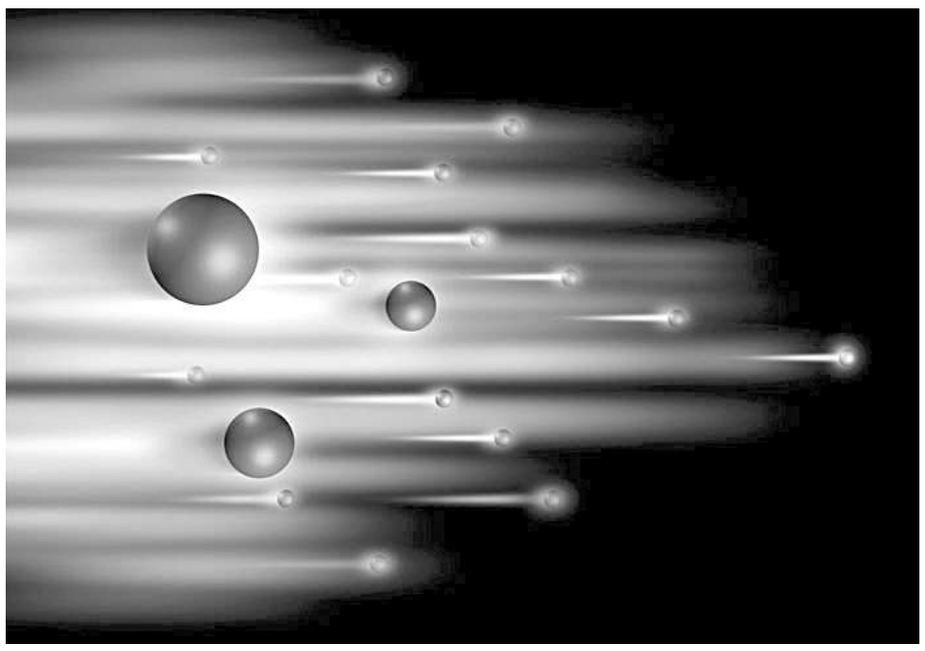
量子通信：绝密的未来通信

文·于笑潇

量子通信技术基于量子物理学的基本原理，克服了经典加密技术内在的安全隐患，是迄今为止唯一被严格证明是无条件安全的通信方式。为了拓展应用、与现有通信系统兼容以及大量减少成本，需对点对点的通信方式进行组网并充分利用经典通信设施。与此同时，量子克隆技术的出现也使得我们开始重新审视量子通信的安全性问题。量子通信是相对最安全的，但任何事情都不是绝对的，有矛就有盾。一方面有“量子非克隆原理”，另一方面有实现近似量子克隆的“量子克隆机”。怎样可靠地评估安全性？怎样进行攻击？是值得研讨的问题。在不久的将来，量子通信与经典通信的融合发展将会带来通信世界的新纪元。

近期，国内顶尖专家们来到西苑沙龙，就量子通信的现在与未来，展开了深刻的探讨。



什么是量子通信？

在量子的世界中，对于一个微观的粒子，测量过程本身将不可避免的给我们要测量的物体造成一个显著的扰动，而且即使在原则上，我们也完全没办法把这一扰动减小到零；另一方面，观测行为本身又会破坏粒子原来的状态，让你永远不可能知道粒子本来的状态是什么。这就是量子不可克隆原理：你不能够复制一个未知的量子态，而不改变量子态本身。量子不可克隆原理是量子加密的基础。如果我们把想要保密传输的信息，加载到一个个不可能被准确观测和复制的量子态上，而任何的窃听行为都会改变原本传输的数据。那么最后我们取一部分数据出来，检查原本传输的信息是否被破坏，就能够检测到窃听者是否存在。

整个量子通信中，具有短期内真实的应用潜能的就是量子保密通信，其中最有用的部分就是量子密钥分发。经典通信使用最广泛的公钥密码，是假定一些数学难题，最典型的是假定大型数据分解的数学难题。但是，随着计算能力的不断提高，特别是未来量子计算机如果实现的话，这种数学难题的复杂性就迎刃而解了，换句话说，经典保密通信基于的数学方法不能获得严格的数学证明。在这个背景下，量子保密通信最大的卖点就是它的安全性获得了严格的数学证明，这也可以从其基本的量子力学的基本原理来解释。

量子通信另一个核心内容是隐形传输，是利用了光子等基本粒子的量子纠缠原理来实现保密通信过程。纠缠是一种诡异的超距离相互关联的现象：两个纠缠在一起的粒子，即使被完全隔离，当观测一个粒子的状态时，另一个粒子的状态也会发生瞬时的改变。换言之，两个粒子的量子状态是完全关联的。量子物理让人最不可思议的地方在于，事物的状态并不是唯一确定的。对于宏观的硬币而言，只可能存在两种状态：正面朝上或是反面朝上。但对于一枚量子硬币，它可以既是正面朝上又是反面朝上。对于两枚纠缠在一起的量子硬币，如果发现其中一枚是正面朝上，另一枚也一定是正面朝上；当发现一枚是反面朝上，另一枚也一定是反面朝上；如果发现一枚既是正面朝上又是反面朝上，另外一枚也一定既是正面朝上又是反面朝上。因此，纠缠所包含的关联性，要比我们通常理解的宏观上的关联性强得多。

事实上，纠缠的两个粒子尽管可以在很远的距离上一个影响另一个，但它们无法传递任何信息。以密钥为例，当双方共享同一套密钥时，并没有发生信息的传递，直到加密的文本传来，密钥才有意义。量子通信和传统通信的唯一区别在于，量子通信采用了一种新的密钥生成方式，而且密钥不可能被第三方获取。

向全球的量子通信网迈进

发展量子通信技术的终极目标是构建广域乃至全球范围的绝对安全的量子通信网络体系。通过光纤实现城域量子通信网络连接一个中等城市内部的通信节点、通过量子中继实现邻近两个城市之间的连接、通过卫星与地面站之间的自由空间光子传输和卫星平台的中转实现遥远两个区域之间的连接，是实现全球广域量子通信最理想的路线图。

在这一路线图的指引下，欧洲、美国和中国等在过去几年中均进行了战略性部署，投入了大量的科研资源和开发力量，进行关键技术攻关和实用化、工程化探索，力争在激烈的国际竞争中占据先机。光纤量子密码技术目前正从点对点量子密钥分发的初级阶段向实现多节点网络内的量子安全性方向深入发展阶段，全球各地正在加紧进行量子通信系统的实用化和工程化建设。

由美国国防部高级研究署（DARPA）支持，BBN公司（具有很强的军方特色）技术部联合波斯顿大学与哈佛大学共同开展了量子保密通信与IP 互联网结合的五年试验计划。该计划主要内容是以BBN技术部、波斯顿大学和哈佛大学作为三个节点以构建融合现行光纤通信网、互联网和量子光通信的量子互联网，并在此基础上实现保密通信。

在欧盟发布的《量子信息处理和通信：欧洲研究现状、愿景与目标战略报告》中给出了欧洲未来五年和十年量子信息的发展目标，例如将重点发展量子中继和卫星量子通信，实现1000公里量级的量子密钥分配。欧洲空间局计划到2018年将国际空间站上的量子通信终端与一个或多个地面站之间建立自由空间量子通信链路，首次演示绝对安全的空间量子密钥全球分发的可行性。欧盟在2008年9月发布了关于量子密码的商业白皮书，启动量子通信技术标准化研究，并联合了来自12个欧盟国家的41个伙伴小组成立了SECOQC工程。

日本提出了量子信息技术长期研究战略，计划通过高强度的研发投入，在5至10年内建成全国性的高速量子通信网。日本邮政省将把量子信息确定为21世纪国家的战略项目，日本的NICT也启动了一个长期支持计划。日本国立信息通信研究院计划在2020年实现量子中继，到2040年建成极限容量、无条件安全的广域光纤与自由空间量子通信网络。

另外，一些世界著名的公司也对量子信息技术投入了大量研发资本，介入了产业化开发，例如：美国电话电报公司（AT&T）、Bell实验室、IBM、Hewlett-Packard，荷兰Philips，日本Hitachi、NEC、NTT、Toshiba，英国电话电报公司，德国西门子公司等。2010年10月，日本在东京展示一个由NEC、Toshiba、三菱电子等公司支持建设的量子通信网络。由此可见，大型国际企业已经实际地介入了量子通信技术的研发和产业化。

而我国在这方面处于国际领先水平，已经实现了超过两百公里（世界纪录）的安全信息传输，实用化安全传输距离已达到几十公里，量子通信网络技术已发展成熟。

实用化进程：与经典通信的融合

从目前的实际应用来看，将量子通信网络与现有网络进行融合是最优的发展战略。互联网在设计时并没有深入地考虑安全性，这造成当今的网络安全问题十分突出。量子通信是人类能掌握的最保密的通信技术，量子通信和经典通信网络的融合研究对于提升未来网络的安全性具有重要的意义。

量子通信和经典网络的融合需要解决物理层和组网技术、中继技术和通信应用技术等几个方面的融合问题。对于未来网，应当从基础设施的建设和利用上就考虑和量子通信的融合。由于传统的光通信可能在很长一段时间内仍然是主要通信技术手段，在光通信网络上实现量子通信网络，将是融合的基础。

实际的量子通信中，量子通信与现有通信的融合是一个相互取长补短的过程，量子通信不会完全替代现有的通信技术，而是在现有的技术上在物理层、网络层、应用层将两者进行了融合。

从物理层来说，可以从光源、探测器和信道方面考虑。在光源方面，利用单光子源或者单离子源，或者将激光光源衰减到单光子量级应用到实际工程中；在探测方面，因为是单光子信号源，需要特测器有单光子量级特征，对量子密钥分发中的连续变量进行测量；在信道方面，对于不同的光源用不同波长的商用光纤即可满足条件。

从网络层来说，一方面我们可以采取独立的信道和统一的网络结构，也可以用一根光纤既传递量子信号又传递经典信号；除了光纤技术，还需要采取例如基于纠缠交换的量子中继技术来解决量子通信的远距离传输这一核心问题；此外，在组网的往来上，可以采取电路交换或者波长复用技术，并且增加量子路由器来进行控制。

从应用层来看，我们可以跟现有的互联网安全协议结合，用量子密码来替换现有协议中的初始密码，这样既可以得到更高的安全性也可以保持实际的通信速率。现在实际用到的量子保密分发的方法都是用诱骗态量子密钥分发的方法。而一旦用量子的方法产生密钥，则必须与后继的经典通信结合才能实际应用。比如，我们用量子密码生成种子密钥，然后用经典的方法进行扩张，这样既保证了种子密钥的安全，同时也有很高的通信效率。

西苑沙龙 West Garden Salon

“西苑沙龙”是科技部高技术研究发展中心为了推动国家科技计划相关领域发展战略研究，举办的以西苑饭店为场地的系列科技发展战略和学术研讨沙龙活动。沙龙重点围绕高技术、基础研究及其学科交叉领域的发展前沿与趋势、重大应用和产业发展需求方面的重大问题，探讨科技前沿、讨论最新突破性进展，展望未来发展趋势。沙龙鼓励与会者本着“客观、求实、融合、创新”的原则，以客观求实的态度，发表自己的学术观点；鼓励和引导多学科交叉融合，激励创新思想。

HTRDC

■专家视点

于渌 中国科学院物理研究所研究员，中国科学院院士

量子通信从原理走上小范围专用问题的实用化，是现在全世界都在努力的方向。中国的起步不错，也有很好的学术带头人，下一步的发展就是明确定位的问题。一方面是注意与现有通信的融合，要善于借鉴现有的通信技术；另一方面，安全性是量子通信在实际应用中的体现，应在未来制定量子通信安全性标准。

王向斌 清华大学教授

量子密钥分发的实际产业化应用应该着眼于未来并注重定位，重点发展局域性的重点需求网络，而不是强调现有网络一样的广泛性和高功能效率。另外，任何实际的系统都不是绝对安全的，量子通信目前重点先要解决的安全问题应放在光源、信道和检测方面。最终目标是促进量子保密通信产业化。

余少华 武汉邮电科学研究院总工程师、光纤通信技术和网络国家重点实验室主任

量子通信不会完全替代现有的通信技术，实际的量子通信中，量子通信与现有通信的融合是一个相互取长补短的过程。密钥分发与传统密码要区分开来，要突出有优势的“一次一密”角度。另外，量子通信还要解决速度的问题，努力实现大规模广覆盖。

范桁 中科院物理研究所研究员

量子通信从量子力学的原理上来说是绝对安全的，但是实际上量子态可以被近似的克隆。比如在信道中将部分量子态截获下来，这就是量子克隆机对量子密钥分发的攻击。目前，我们可以用一种特殊的相位量子克隆来对量子态进行一定的攻击。未来我们希望有更接近实际的安全性证明。

赵勇 中国科学技术大学高级工程师，中科院量子技术与应用研究中心副主任

对于量子密钥的推广，我们不能摸着石头过河，而是要重点关注现在需要解决的问题。怎么利用现有和未来发展的互联网技术或者下一代网络优势，提出更满足未来需要的网络，是一个取长补短，互相融合、互相学习的过程，也是将来的工作方向。

纪越峰 北京邮电大学教授

量子通信下一步发展重点是量子密钥分发中的量子通信联网应用，其中可信传输与光子交换技术是重中之重。量子通信面临四项难点：可扩展、强抗毁、广覆盖、立体化，另外光网络上的基本特征怎么融合量子通信也是要考虑的问题。总之，量子密钥分发在未来推广应用方面面临两大挑战：融合性和安全性。

银振强 中国科学技术大学副教授

任何实际系统总是存在安全性问题，量子密码的时代也必然存在密码安全性的问题。深入研究量子密码分配系统各种器件的物理性质才有可能解决安全性的问题，研究更安全的实际系统的设计与架构，探索新的量子密钥的协议。

李凤华 中科院信息工程研究所研究员

量子通信首先应该在互联网时代找准自己的定位，另外量子通信目前应该重点关注量子密钥分发。相对于传统的通信来说，量子密钥分发在速度方面的“一次一密”的角度上还是有优势的，目前应该应用的重点在高端、重要的通信当中，特别是在干线网络上。

龙桂鲁 清华大学教授

量子通信从原理上可以保证安全，但实际上由于器件、单光子发射、探测等方面的缺陷，出现了种种攻击。改善器件有一个过程，每一个阶段有一定的发展水平，对于重要的实际应用方面的安全问题，可以在现有的水平上把量子通信与现有通信结合起来，来加大信息的安全。

（本栏目稿件素材由西苑沙龙提供）

作物的节水专家和私人医生

——记国家863计划之农业生物环境控制与生物修复

文·本报记者 马爱平

筛选出9个作物节水品种，构建了作物节水型种植制度决策技术与平台，研发了50个抗旱节水材料、制剂等农业高效用水产品和设备，制定了8项作物高效用水与精量灌溉技术标准与规程，取得了66项国家发明专利，获25项实用新型专利……

两年多来，国家863计划现代农业技术领域之“农业生物环境控制与生物修复”主题，从农业高效用水精量控制技术与产品、农业生境检测监测与修复技术研究、重要农林有害生物高通量分子检测技术，组织了57个国内相关领域优势单位开展研究。

调控和灌溉技术显身手

中国工程院院士康绍忠介绍，该主题通过“作物生命需水过程调控技术”的研究，建立了长期定位观测试验站与分层分布式作物生命需水信息试验监测系统等，开发了3种适合大田作物的额非充分小定额施灌控制技术与配套产品，开发了2种新型抑蒸降耗产品……

“研究还系统提出了节水调质高效灌溉理论与优化决策方法，建立了膜下滴灌棉花、酿酒葡萄、温室蔬菜的节水调质高效灌溉综合技术体系，形成了5套主要作物节水调质高效生产技术标准。其中，膜下滴灌棉花节水霜前花产量比例提高10.6%，酿酒葡萄节水单宁提高15.0%。”中国农业大学教授杜太生说。

西北农林科技大学研究员牛文全介绍，其科研团队研制了微润灌水关键技术与产品，将平均粒径为2.6微米易萃取化学填充剂均匀混合到高分子材料中，形成均匀而微小的孔隙，最小的土壤颗粒都无法进入孔隙内发生堵塞，适合干旱、小水源灌溉，该技术为续灌，使根区土壤保持一定的湿度范围内，田间灌溉水利用系数可达95%以上。

该主题还提出了新一代微润带生产技术与产品，将惰性填料由单一无机填充剂调整为无机有机共混型填充剂。攻克了壁厚增加对于流量的影响，使微润带适合机械铺设和抗损能力。目前已制成了厚度达990um的世界上最厚的高分子半透膜，使产品的形态由微润带转变成微润管。该生产工艺已经形成全自动化生产线1条等，微润灌技术产品成为比滴灌更节水高效，在我国形成微润灌技术研发与生产基地，单条生产线的年生产能力达到500万米。

科研人员还通过“水稻滴灌技术”初步建立了水稻品种滴灌适应性的评价体系，研发播种滴灌水稻高密度精量播种机3种，筛选安全高效水稻土壤除草剂2种等。2012年9月对20亩膜下滴灌水稻高产高效栽培技术集成示范基地进行产量测定，实测亩产达836.9公斤。目前，该技术已推广到新疆、江苏、宁夏、黑龙江等地，试验示范面积达5030亩。

检测与修复技术更快更科学

面对常规有毒有害重金属，西北农林科技大学教授韦革宏介绍，研究人员建立了土壤重金属及抗生素分子探针快速检测技术，可将国际检测最低标准量再降低2—15倍。同时，开发出单通道、多通道快速检测免疫金标试纸条，可同时或单独对四种农药进行快速准确的检测，检测时间为5—7分钟，这显著提高了我国农药快速检测的能力。

针对不同污染物类型，上海交通大学教授周培说，研究人员研发出Cd、Zn、Pb物化稳定技术与产品，建立物化稳定—低积累作物水稻的联合阻控技术等修复技术。同时，以农田有机复合污染为靶标，获得了30多个优良降解菌及菌系、正在形成6个复合农药和多环芳烃污染的土壤修复菌剂及酶制剂产品。

在“重要农林有害生物高通量分子检测技术”研究中，科研人员分析大豆、瓜类等作物或林木为所传代的危险性病原生物的种类，对每一种选定的植物病原生物的基因组进行分析，对每种病原生物选定的分子检测靶标，建立高通量、高精准度和超快速的病原检测技术体系。目前，对不同的检测靶标生物建立了6种检测技术，并对所选的病原生物，筛选了核心基因，设计了高可信度的引物或探针；建立的检测技术体系可同时检测样品中传带的10种以上病原生物，具备高精准度、高灵敏度和超快速，使我国的有害生物检测技术处于世界领先水平。

在“农业有害生物分子免疫调控技术研究”中，科研人员已鉴定和分离了8个细菌和真菌源蛋白类和1种真菌多糖类免疫物，获得了1株防效好、定殖久、性状稳定的无致病力青枯雷尔氏菌突变株，获得最优化的免疫诱导活性多肽，解析了2个真菌源蛋白的晶体结构，获得了1个茄科作物青枯病免疫接种剂“鄂鲁冷特”初产品，防效达75%，建立了3000亩的生产示范基地，转让了1项发明专利等。

（国家863计划现代农业技术领域办提供素材）

■ 数 字

8347家

环保部数据显示，今年以来，全国空气质量最差的10个城市中，河北每月都占5至7个。为防治大气污染，这个省目前已完成脱硫、脱硝、除尘等减排工程426个，关停取缔重污染小企业8347家，拆除分散燃煤锅炉1225台，建设煤质快速检测站20个。

“我们要兑现3年有所好转、5年明显改善的承诺，完成好向中央立下的军令状，必须在今年工作的基础上，像拧螺丝一样越拧越紧。”河北省委书记周本顺在18日召开的省委八届六次全体（扩大）会议上谈及大气污染防治时说。

135亿立方米

江西罕见冬季暴雨于18日上午结束。这轮降雨过程雨量折合成水量约为135亿立方米，极大缓解了江西境内江河湖库的低枯水位状况。

江西省防汛抗旱总指挥部介绍，这次降雨从14日0时开始至18日8时，全省平均降雨量81毫米，为有记录以来12月份单场降雨量第三位；降雨极大地缓解了江西境内江河湖库的低枯水位状况，为今冬明春生产生活用水储备了水源。

■ 资 讯

环保中间件方案改善人居环境

科技日报讯（滕继濮）“环境保护需要将水利、农业、园林绿化等其他部门纳入工作范围，形成‘大环保’综合防治体系。”北京东方通科技股份有限公司（以下简称“东方通”）咨询顾问12月16日向记者表示，智能环保建设首先需要解决多个部门之间的信息融合难题，将环保涉及的所有组织机构（包括政府部门、企业）、应用系统、传感设备等集中到统一的平台上，在此前提下，根据业务需求采集传感网上的各类环保数据，并与人口、法人、地理空间等基础信息资源进行融合，从而为领导决策、相关部门业务协同、公众服务提供所需信息，充分挖掘水质监测数值、空气污染指数等各类环保数据的现实意义。

为此，东方通创造性地推出环保业务应用支撑平台解决方案，以应用集成中间件TongIntegrator、消息中间件TongLINK/Q等产品为核心构建数据集成平台，并与操作系统、数据库管理系统、J2EE应用服务器等应用支撑软件组合应用，既能支撑各类环保业务系统运行，又能实现跨区域、跨部门、跨系统信息资源共享交换，破解了智能环保信息融合难题。目前，东方通已成功参与实施中国环境监测总站环境监测数据平台、国家环境信息与统计分析能力建设、四川省环保应急平台等环保信息化项目，其中国家环境信息与统计分析能力建设项目投资达到5.8亿，建成了四级三层网络，覆盖全国环保系统，并通过500多套东方通中间件产品的部署应用，在多个部门之间实现信息资源共享交换，有效提升生态环境综合治理水平。

多种科技手段助推管理提升见成效

科技日报讯（张召 滕继濮）12月16日，记者从中铁四局五公司获悉，该公司把“苦练内功，降本增效”作为管理提升的重要内容，使管理向标准化精细化发展。

该公司借助“中国中铁对外支付管理系统”信息平台，加强公司成本部、物机部、财务部之间的信息联通，把劳务、物资和租费结算审批程序与公司资金支付程序对接，进一步完善出台了劳务结算数量、物资消耗数量、劳务结算单价等数量核算体系，实现了合同报审制度、结算审批制度、资金支付制度的有机统一。

同时，下发了《五公司专业片区项目施工管控管理办法》，成立了专业片区管控小组，并利用司务交班会和季度生产形势分析会等平台，对局项目管控检查存在问题的项目通过即时通平台进行督办通报。通过创建片区管控情况移动飞信群，加强了公司领导、总部各部门负责人、各项目部经理、书记、总工和安全总监的联系，促进公司各单位相互对照查找问题，避免共性问题在其它项目重复出现，初步形成了项目管控与局管控组之间“全程跟踪问题、督促整改落实、反馈整改结果”的“无缝对接”机制。

在规范外协队伍管理上，公司下发了《外部劳务企业员工工资管理暂行办法》，并在公司50余个项目使用人脸视觉识别系统对农民工进行考勤管理，录入农民工信息7819人，外协队伍百余家，建立农民工和外协队伍信息库，实现民办管理信息化。