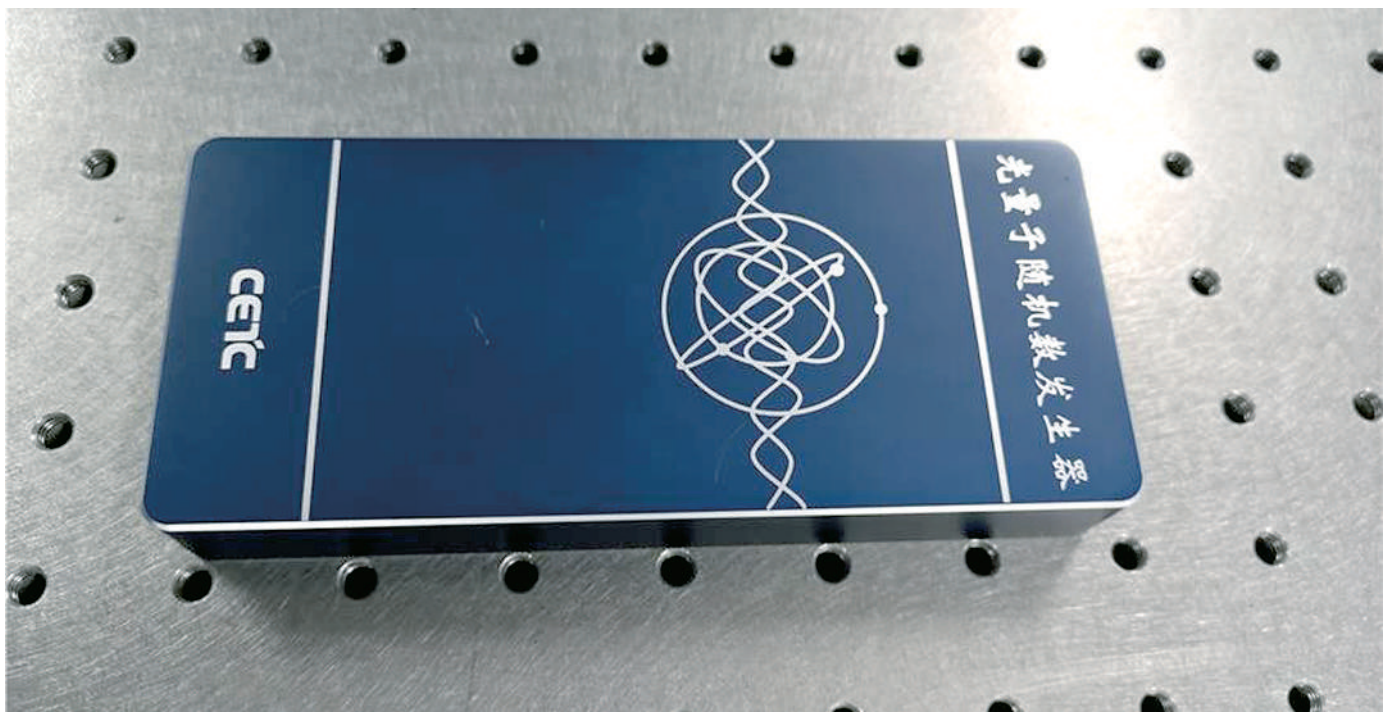
中国科学技术大学在国际上首次实现器件无关的量子随机数——

量子保密通信安全再升级

经济日报·中国经济网记者 沈 慧

热点追踪

我国量子保密通信安全研究迎来又一重大突破。前不久，中国科学技术大学教授潘建伟团队宣布，利用量子纠缠的内禀随机性，在国际上首次成功实现器件无关的量子随机数。这项突破性成果将在数值模拟、密码学等领域得到广泛应用，有望形成新的随机数国际标准



图为中国电子科技集团公司研发的随机数发生器。（资料图片）

无论经典密码学还是量子保密通信，都需要真正的随机数作为保障。在现有量子保密通信系统中，如果不小心采用了恶意第三方制造的量子随机数器件，就可能发生随机数泄露。根据中国电子科技集团公司首席专家、中国网络信息安全有限公司总工程师饶志宏的说法，“器件无关”是指，即使在随机数产生系统的部分乃至全部器件来自于不可信厂商的恶意器件情况下，也可以产生不会泄露的真随机数。也就是说，“系统的安全性与器件的具体情况无关”。

无处不在的随机数

在众多领域，常常需要通过数值模拟进行计算，而数值模拟的关键就是要有大量随机数的输入

无论是在科学研究还是日常生活中，随机数都有着重要应用。

例如，天气预报、新药研制、材料设计、工业设计和核武器研制等领域，常常需要通过数值模拟进行计算，而数值模拟的关键就是要有大量随机数的输入。在游戏设计、人工智能等领域，需要使用随机数来控制系统的演化；在通信安全、现代密码学等领域，则需要第三方完全不知道的随机数作为安全性的基础。

随机数的获取通常有两种途径：基于软件算法实现或基于经典热噪声实现。软件算法实现的随机数是利用算法，根据输入的随机数种子给出均匀分布的输出。然而，对于确定的输入，固定的算法将给出确定的输出序列，从这个角度来说，这类随机数本质上仍是确定性的，并不真正随机。而基于经典热噪声的随机数芯片能读取当前物理环境中的噪声，并据此获得随机数，但这类装置最终获得的也只是某种更难预测的伪随机数。

量子力学的发现让故事有了新的转折——因为，其基本物理过程具有经典物理中所不具有的内禀随机性，从而可以制造出真正的随机数产生器。

所谓内禀随机性，饶志宏解释，任意量子态都具有内禀随机性，纠缠作为一种特殊的量子态，也不例外。在测量下，它会概率性输出其测量的本征值，这个测量结果具有理论上的不可预测性，即内禀随机性。而量子随机数发生器，是基于量子力学原理设计的一种新型随机数发生器，其工作原理是，通过观测量子随机噪声以产生不可预测的随机序列。

“随机数系统中的关键器件，比如光源、探测器等，可能来自于国外不可控厂商，因此存在安全隐患。”在饶志宏看来，基于量子纠缠内禀随机性的量子随机数产生机制是有科学意义的，此类方案可以排除由非可信器件所引入的安全漏洞，具有理论意义上最高等级的安全性，同时也是国际学术研究的热点。

量子力学内禀随机性

利用贝尔实验进行检验，能从根本上排除定域确定性理论，从而实现不依赖于器件的量子随机数，即器件无关量子随机数

关于量子力学的内禀随机性，科学界曾有过争议。爱因斯坦、薛定谔和温伯格等著名物理学家即是反对者。爱因斯坦坚信“上帝是不会掷骰子的”，他认为一定存在着一个更高的确定性理论，量子力学只是该理论的近似，而量子力学的内禀随机性则只是因为我们不了解这种理论而带来的误解。

围绕这一论断，支持者与反对派进行了长达30年的争论。但在当时，两种观念都没能给出在实验上可以加以严格区分的精确预言，所有争论都局限于哲学层面。直到1964年，美国物理学家贝尔发现，通过对量子纠缠进行关联测量，量子力学和定域确定性理论会对测量结果有着不同的预言。

在前人研究的基础上，长期从事量子力学基础检验的潘建伟团队，分别利用观察者自主选择和遥远星体发光产生的随机数，于今年分别实验实现了超高损耗下和大量观察者参与的贝尔实验检验，文章先后发表在学术期刊《物理评论快报》和《自然》上。

重要而有趣的是，贝尔实验的检验可以从根本上排除定域确定性理论，从而实现不依赖于器件的量子随机数，即器件无关量子随机数。这类随机数发生器被认为是安全性最高的随机数产生装置，即使采用恶意第三方制造的组件，或者窃听者拥有计算能力最强的量子计算机，也无法预测或获知它所产生的随机数。

“在现有的量子通信系统中，如果采用自己制备的或者可信制造商制备的量子随机数产生器，其安全性是可以得到保障的。但是，如果不小心采用了恶意第三方所制造的器件，就会发生随机数泄露。”潘建伟说，新的成果则确保即使在采用了不信任第三方器件的情况下，也可以产生真随机数，并且不会泄露，从而确保通信的安全。

走向应用尚需时日

要实现器件无关的量子随机数，需要满足极其苛刻的实验要求，实现技术难度高。因此，目前仅适合进行基础前沿研究

一切看上去是那么美，实现起来却困难重重。比如，整套随机数产生装置需要以极高效率进行纠缠光子的产生、传输、调制、探测；同时，不同组件间需要设置合适的空间距离以满足类空间隔要求，才能以最高的安全性保证任何窃听者不能通过内部通信来伪造贝尔不等式测试的结果。

“要实现器件无关的量子随机数，需要满足极其苛刻的实验要求，正因为实现技术难度高，一旦成功才更具有科学意义。”饶志宏称。

为抢占量子保密通信领域的制高点，目前，国际上纷纷开展了这种随机数产生器的研制工作。美国国家标准与技术研究院正计划利用器件无关的量子随机数产生器建立新一代随机数国际标准。最终，潘建伟等人经过3年多的努力，在世界上首次研发出器件无关的量子随机数产生器。

不过，安全性与实用性有时是个矛盾体。饶志宏说，由于此类方案实现技术难度高，对实现环境要求极高（例如，超导探测器需要极低的工作温度），且存在随机数产生速率低且成本高等不足，目前仅适合进行基础前沿研究，在现有技术条件下不适合作为实用性方案加以应用。

此外，器件无关并不是实用化随机数的必要条件。饶志宏认为，如果我们能保证所谓“器件相关”量子随机数产生方案是基于国产自主可信器件设计实现的，此类方案产生的随机数同样具有高安全性。

他介绍，去年中国电子科技集团公司发布的随机数发生器所采用的方案就是基于自主可信器件设计的“器件相关”的量子随机数产生方案，它的实现成本低且随机数产生速率极高（随机数产生速率达到5.4Gbps），目前处于国际领先水平，是实用化解决方案的一个良好选择。而潘建伟团队的“器件无关”方案科学意义较大，体现了我国在尖端实验技术上的进展。

潘建伟表示，该研究成果及后续研究工作将为密码学、数值模拟以及需要随机性输入的各个领域提供真正可靠的随机性来源；同时，由于可信任的随机数源是现实条件下量子通信安全性的关键环节，器件无关随机数的实验实现也进一步确保了现实条件下量子通信的安全性。

未来，中国科学技术大学团队将研发高速稳定的器件无关量子随机数产生装置，通过提供基于量子纠缠内禀随机性的、高安全性的随机数，争取形成新一代国际随机数标准。

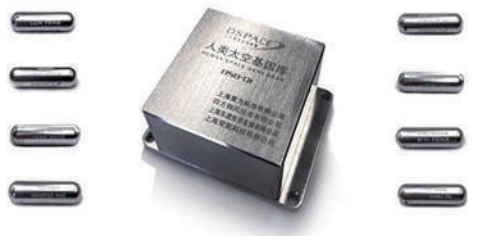
首个太空基因库成功发射

本报讯 记者沈则瑾报道：10月25日凌晨6时57分，世界首个太空基因库搭载长征四号系列火箭的太空试验平台，成功进入预定轨道运行。

此次活动由上海曼为科技有限公司（“曼为科技”）主导运作。2018年初，由御风集团董事长冯仑等人，以及国内外顶尖航天科学家和基因科学家共同发起组建了“曼为科技”。这是一家专注于生命科学研究和太空技术探索的公司，通过建立、长期管理和运营百万人级别的太空基因库，在未来条件成熟时，将运送基因至类地行星，通过基因技术创造出新的人类文明。

这一全球首个人类太空基因库项目，通过发射人类基因至太空，以及在地面模拟太空环境试验，获得太空环境对基因的真实影响数据；同时，还研制抵御宇宙辐照和高能离子的基因存储装置，在地球和太空中永久保存人类的种子——基因，为人类在未来的星际移民以及基因再生提供有力支撑。

据悉，从该项目8位参与者身上提取的基因将在太空中最长保存975年。同时，他们的基因也是人类首批进入太空存储的基因，在人类生命科学研究和太空探索历史上具有里程碑意义。



太空基因库存储单元和基因胶囊。（许跃飞供图）

河长制监督管理平台“显身手”——

“智慧治水”水常青

本报记者 崔国强

“过去发现河流污染，我们只能给镇里打电话，延误污染治理时间。现在小的污染问题可以就地解决，大问题半个小时就解决了。”在安徽黄山市黄山区耿城镇沟村村，村级河长王正齐说，工作比以前好开展了。

这源于安徽省大力推进的河湖长制监督管理平台相助。在前端，河长们可以打开“河长管理平台”APP迅速将污染情况拍照上传，通过这个“千里眼”，后端能迅速处理。当前，黄山区已有205名河长通过“河长管理平台”APP日常巡河，广大群众也可以通过扫描微信公众号“黄山区河湖长制”二维码参与河湖的治理工作，反映污染问题。

在“千里眼”的后端平台，是“智慧大脑”。在黄山区水利局办公室，工作人员黄磊打开系统，这里可以对全区的河流湖泊水质情况进行即时监控，动态掌握河长相关基础信息、问题处理等情况。当前，黄山区的区、镇、村三级河长使用该平台后可实现智能治水，自动生成巡河、巡湖记录。

“这个系统于今年5月25日上线，可以实现手机GPS定位，已实现巡河巡湖里程2万余公里，后续我们将进一步开发完善平台功能，实现河湖数据和视频信息共享。”黄山区河长办副主任孙敢告诉记者。

那么，“智慧治水”是怎样实现的？原来，“智慧大脑”这套系统借助的是统计分析模块，可以直观展现各级河长巡河巡湖的完成率、进度、问题处理情况。安徽移动黄山分公司总经理李坤滋介绍，统计分析模块就是将河湖长制相关数据进行大数据分析，并结合业务管理需求抽取统计，为河湖长实现科学治水提供有效手段。

现阶段，通过电脑端、手机APP、微信公众号，结合移动互联网技术将数据无缝衔接，黄山区的河流湖泊实现了一个数据中心统一管理、一个平台各级联动协同管理；结合微信公众号实现治水全民参与，全民治水监督；通过视频监控，做到河湖全天化管理监督。通过河长制平台的使用，不断完善实现河长治水无纸化、信息化，让数据充分“跑起来”。

“未来，我们将通过人工智能和大数据，对河流湖泊进行更加智能化的管理。”李坤滋说。

二手房交易有望实现可视化

本报记者 王轶辰

据北京东城区链家新奥洋房一店店长云强介绍，目前，他们已可以通过贝壳网实现VR看房，以及后续交易等整套可视化体系。图为云强在办理业务。马玲玲摄

“好不容易请了半天假，结果银行面签没搞定，为什么不给我选一个合适的银行？”“我是买卖连环单，时间必须卡得非常准，每天要多次询问经纪人进展情况，太麻烦！”……长期以来，二手房交易中存在交易流程繁琐、问题信息繁多且不透明、产权与资金的安全性存在风险、便捷性亟需提升等问题，难免会让消费者与经纪人、交易服务人员之间“吐槽”不断。

如今，二手房交易繁琐且不透明的弊端有望得到根除。在近日举行的媒体沟通会上，贝壳交易平台总经理伊凯透露，贝壳交易平台目前已覆盖从签约到过户、放款等所有环节的整套交易体系，保障消费者从签订经纪服务合同到房产过户完成的所有环节，进一步提升房产交易的安全便捷。

“房产交易环节直接关系到消费者的切实利益。外卖和快递都可以随时了解订单进展，在线互动交流，而买房这么大的事情，在周期很长的交易过程中，消费者却无法方便地了解进展、参与过程。”伊凯说，贝壳交易平台通过交易可视化，实现了多角色之间的扁平化沟通，用户可以通过手机随时了解房产交易进展，并与交易服务人员互动，大幅消除沟通障碍。

经济日报记者了解到，贝壳交易平台覆盖整个二手房交易流程，涉及从签约、贷款到房产过户、尾款放款的所有环节，包括签约前、签约中、签约后。具体而言，签约前，交易平台能够为经纪人提供消费者的购房资质、贷款情况、评估询值、税费计算等咨询服务；签约中，交易平台能助力交易服务人员现场陪签，有效识别并把控交易风险，设置资金框架，选择交易产品；签约后，交易平台将会助力交易服务人员专业、高效地完成评估、解抵押、贷款申请、缴税过户、资金存管等环节。

通过交易可视化，消费者、经纪人在签约甚至产生房产交易的意向时，就可以通过贝壳APP在线清晰准确地了解交易流程与办理进度。这其中，既包括整个房产交易的流程、节点，以及各个节点所需的备件资料、办理地点、所需时长、办理的具体时间点等，也包括交易中的整体资金架构以及资金流动情况，还可以让消费者、经纪人、交易服务人员等多个角色在线互动与交流。

同时，在交易过程中的各个环节，消费者与经纪人还可以对交易服务人员做出满意度评价，并对交易单的整体服务过程进行满意度评价。而这些评价结果，将直接影响到交易服务人员的收入、职级评定等，从而反向促进交易服务人员、交易服务机构不断提高服务质量。

值得注意的是，贝壳交易平台通过和银行的系统直联，实现了贷款办理信息的线上传递与交互，打破了两个行业的信息孤岛状态。目前，贝壳已与工商银行、中国银行、光大银行等8家银行总行，建设银行和农业银行等银行的多家分行达成直连合作意向。以与工商银行的直连为例，他们目前已经覆盖超过20个城市的分行，实现了贷款进度线上可视，大大提升了用户体验。

“无论处在消费的哪一端，大家都有服务升级的需求。”伊凯表示，贝壳交易平台希望通过互联网思维、产品、技术手段，真正有效地赋能交易服务人员、经纪人，并通过生态共治，让房产交易服务更专业、更透明、更便捷，用平台的力量推动行业整体进步。

此外，贝壳交易平台通过大数据与智能服务，减少了经纪人90%以上的沟通与咨询工作量。一方面，经纪人可以通过交易助手等产品及时准确地了解、掌握最新购房政策和银行贷款信息；另一方面，经纪人和交易服务人员在办理业务的过程中，可以随时随地互动、交换信息，携手保证交易服务的品质。而店东、交易服务机构负责人等管理者，也可以通过业务数据看板、红绿灯、额度预警等大数据工具，实现精细化管理和智能协作，提升作业效率，有效防控风险。

目前，贝壳交易平台已面向全国50个城市开放，计划年内服务近百座城市。未来，交易平台将向全行业全面赋能——即便不是已入驻贝壳找房的经纪品牌，只要有需求，也可以享受平台上的各类交易赋能服务。

《自然—通讯》发表研究发现——

减肥或有新路径

本报讯 记者佘惠敏报道：减肥靠啥？管住嘴，迈开腿。吸烟可降低食欲，相当于管住嘴；挨冻能增加能量消耗，相当于迈开腿。德国科学家最新研究表明，不必冒着肺癌风险吸烟，也不必顶着感冒风险挨冻，只要针对身体中的尼古丁（烟碱）受体和冷暴露受体给药，就能取得减肥效果。

这是日前《自然—通讯》发表的一项研究，研究者使用药物同时针对小鼠的尼古丁（又名烟碱）和冷暴露信号传导通路，发现可以降低小鼠体重并改善小鼠的代谢健康。化合物冰素（icilin）和二甲基苯基哌嗪，会刺激食欲抑制通路和产热促进通路，从而调节全身能量平衡以促进肥胖小鼠减重。

肥胖是代谢疾病（例如糖尿病）的风险因素，对健康构成重大威胁。吸烟和冷暴露是人体能量代谢的环境调节因子，分别抑制食欲，增加能量消耗。目前，人们正在寻求通过药物方式增加产热，希望可以借此模拟冷暴露，从而促进减重。然而，同时带来的食物摄入的增加往往会抵消这些影响。

德国环境健康研究中心研究人员采用一种联合疗法，即同时使用烟碱型乙酰胆碱受体，以及瞬态电压感受器阳离子通道后发现，这种疗法降低了肥胖小鼠的体重，并纠正了葡萄糖耐受不良。

这项医学研究表明：针对尼古丁和温度受体的药物疗法可以缓解小鼠肥胖。研究者指出，以上研究结果为治疗肥胖开辟了一条潜在新途径，不过还需要进一步研究，以确定这些发现是否可以转化至人类身上。

本版编辑 郎 冰

联系邮箱 jjrbxzh@163.com

社址：北京市西城区白纸坊东街2号 读者服务：13911270606（同微信号） 查号台：58392088 邮编：100054 传真：58392840 零售每份：1.00元 广告许可证：京西工商广登字20170090号 广告热线：58392178 发行热线：58392172 昨日（北京）开印时间：3:25 印完时间：4:45 本报印刷厂印刷