“量子安全通话手机”要来了

手机使用会更安全吗

在竞争激烈的量子科技领域，我国科学家不断取得新的突破，量子计算原型机“九章”问世，树起了一座举世瞩目的里程碑，量子通信方面的研究更是走在了世界前列，天地一体化的广域量子通信网络正在向我们走来。

作为今年不断刷屏的热门话题，量子科技距离我们的生活还有多远呢？或许答案比想象的更近。在11月举办的2020天翼智能生态博览会上，中国电信宣布布局量子科技行业，构筑“量子+”产业生态。同时，中国电信展出了两台样机，分别根据华为和中兴现有手机改造而来，用户可在通话过程中选择两种通话模式——加密通话或普通通话，通话质量毫无差别。

毫无疑问，量子通信正从基础科学研究向应用推广阶段转化。那么，这种号称可以进行“量子安全通话”的手机究竟为何物？它的推出又意味着什么？

配备了量子密钥的保密手机

“可进行量子安全通话的手机在功能上与传统安全手机类似，其不同点在于前者配备了用量子信息技术制备的量子密钥。”中国电信安徽公司副总经理郑家升告诉记者，与其叫它“量子安全通话手机”，不如叫它“支持量子安全通话服务的手机”更为贴切。

据了解，量子安全通话服务可以理解为“安全通话+量子密钥”的服务，其中，安全通话与普通通话的区别在于——安全通话是对通话过程中的语音进行加密后再传送，可实现通话内容防泄漏的功能。

“量子密钥是指使用量子信息技术制备出的密钥。”郑家升说，目前，国内外可制备量子密钥的量子信息技术主要包括量子密钥分发（QKD）和量子随机数发生器（QRNG）两种技术，如上半年三星发布的“量子加密手机”就是手机内置了量子随机数芯片，据报道英国电信正计划使用QKD技术构建安全网络，将在5G基站与移动终端设备以及联网汽车之间建立“超安全链接”。

量子密钥的特点在于其随机性，密钥生成基于物理机制而非数学算法，其安全性是经过严格数学证明的。

量子密钥的特点在于它是编码在光子的量子态上，依据量子不可克隆定理，一个未知的量子态不能够被精确地复制，一旦被测量也会被破坏。因此这样的量子密钥的安全性也有量子力学的理论保证。

“在量子密钥传输过程中，试图窃听者不可能做到既偷听又不会被发现。”郑家升解释说，这种不依赖计算复杂性，而是基于量子力学基本原理的密码产生方式就是量子保密通信。

两种方式生成手机上的量子密钥

记者了解到，量子安全通话服务中使用的量子密钥从功能角度分为两种：一是用于认证的预充注在量子安全SIM卡上的量子密钥；二是用于语音加密的量子密钥，由量子密钥分发网络实时生成。

“使用量子安全通话服务时，用户拨号触发认证过程，使用预充注的量子密钥进行认证；同时从量子密钥分发网络实时获取量子密钥，对通话语音进行加密，每次通话均使用不同的量子密钥。”郑家升告诉记者。

这里所提到的安全SIM卡，结合了普通SIM卡和安全芯片的功能，在为手机提供安全保护的同时，又不会额外多占用手机卡槽。用户现有的手机通过安装安全SIM卡即可享受量子安全通话服务，也就是说，量子安全通话服务并不需要专用定制手机。但记者了解到，如果希望使用量子安全通话服务，则通话双方手机都需要支持这个功能。

据介绍，想要应用量子密钥的每个用户需要先到临近电信网点的服务站下载自己的专属密钥，这是用量子随机数发生器产生的真随机数（量子态的坍缩产生的随机数）。通话时，双方各自对应的服务站之间通过量子密钥分发共享应用密钥，再用两人各自的专属密钥将应用密钥加密后发给双方，然后双方就可以进行保密通话了。

“这样一来，通话信息具有高安全性，实现从主叫方手机到被叫方手机间的端到端的加密，网络上的语音信息即使被其他人获取也无法获得真实语音内容，做到了保持用户使用习惯基本不变，服务无感、高安全。”郑家升说。

那么，量子密钥足够多少人分配呢？这个问题完全不用担心，因为我国自主打造的量子保密通信京沪干线就是一个实时不断产生量子密钥的源头，能够满足安全通话等各应用场景的量子密钥需求。

“我们目前提供量子安全通话服务的量子安全SIM卡是基于国产密码芯片和国产密码算法的。量子安全SIM卡实现量子密钥的存储以及安全通话加解密服务，能够满足手机的量产需求。”郑家升表示。

对于部分网络媒体“在没有信号的情况下，量子安全手机可以工作并保证信息安全”的说法，郑家升表示，可进行量子安全通话的手机在基本功能上和普通手机一样，没有信号的情况下，无法正常通话。量子安全通话服务是将量子技术制备的密钥应用于安全通话，通话是需要网络的，没有信号无法进行通话。“目前在手机上主要提供量子安全通话服务，后期可能会根据市场需求逐步开发新的应用。”郑家升说。

通信加密需求有待市场考证

记者了解到，量子密钥分发网络的建设需要依托光纤网络。而中国电信作为全球最大的光纤宽带运营商，具备量子密钥分发网络所需的光纤资源。

今年11月，中国电信宣布正式启动“量子铸盾行动”并发布了量子城域网方案，布局量子安全产业，计划在未来5年，通过“量子铸盾行动”率先为10个城市的公共安全提供“量子安全云”，为100个城市提供量子安全组网方案，为1万个政企客户提供量子安全加密解决方案，为1000万移动终端用户提供量子安全通话服务。

量子城域网究竟是什么？中国电信相关人士表示，这是一种可建设覆盖整个城市的量子密钥分发网络，该网与传统通信网络相结合，能实现基于量子安全技术的高等级安全通信服务。上述量子城域网项目可以理解为量子技术和通信网络在实际商用中的结合。目前量子通信的相关试验网在安徽合肥已经建成，合肥量子通信广域网正在立项，根据中国电信的安排，预计在2020年底或2021年初，该项目将在部分区域小规模进行试用。

有关专家指出，量子保密通信技术仍属于新兴技术，不论是量子安全通话服务还是量子安全超级SIM卡，随机数还是QKD路线，都只是行业发展初级阶段进行的尝试探索，需要在实际应用过程中不断改善、加强。

业内专家表示，单纯从通话加密而言，这对手机并不是一个新兴功能，但加密方式有很多种，安全性也有差别，量子安全手机在加密的方式和安全性上有了新的突破。该类手机对于政企客户，会是一个非常值得关注的功能。但就普通消费者而言，对于加密通话功能的迫切性和必要性还有待观察，因通话加密目前并不是手机市场的主流需求，数据安全非常重要，却并不容易被消费者感知。但随着智能手机中存有越来越多的个人数据和金融信息，或许消费者对通信加密的需求会日益增长。

据新华网

我国新一代“人造太阳”放电了

12月4日14时02分，位于四川成都的中核集团核工业西南物理研究院内，我国新一代“人造太阳”装置——中国环流器二号M装置（HL-2M）正式建成并实现首次放电。这标志着我国自主掌握了大型先进托卡马克装置的设计、建造、运行技术，将为我国核聚变堆的自主设计与建造打下坚实基础。

放电温度 可达太阳芯部温度近10倍

核聚变并不神秘，只要将氢的同位素氘和氚的原子核无限接近，使其发生聚变反应，就能释放出巨大能量。其原理看似简单，但要让聚变反应持续可控，可以说难于上青天。

该项目负责人刘永说，要实现可控核聚变反应，必须满足三个苛刻条件：一是温度要足够高，使燃料变成超过1亿摄氏度的等离子体；二是密度要足够高，这样两原子核发生碰撞的概率就大；三是等离子体在有限的空间里被约束足够长时间。

而此次新建成的中国环流器二号M装置，于2009年由国家原子能机构批复立项，由中核集团核工业西南物理研究院自主设计建造，是我国目前规模最大、参数最高的先进托卡马克装置，是我国新一代先进磁约束核聚变实验研究装置。其等离子体体积达到国内现有装置2倍以上，等离子体电流能力提高到2.5兆安培以上，等离子体离子温度可达到1.5亿度，能实现高密度、高比压、高自举电流运行。

“放电是为了使HL-2M装置真空室内的气体变成等离子体态，我们科研人员将在这个装置上进行不同种类的放电，最终目标是让足够多的等离子体被加热到1亿摄氏度以上。我们太阳芯部温度是1500万到2000万摄氏度，这相当于太阳芯部温度的近10倍。等离子体只有被加热到了1亿摄氏度以上才可能实现可控核聚变。”相关研究人员表示。

实现多项突破 贡献“中国核聚变”智慧

在HL-2M装置建设过程中，核工业西南物理研究院联合国内多家研制单位，不断挺进科研“无人区”。在装置物理与结构设计、特殊材料研制、材料连接与关键部件研发、总装集成等方面取得了多项突破，实现了可拆卸线圈结构，增强了控制运行水平，提升了装置物理实验研究能力。

研发团队先后攻克了高镍合金双曲面薄壁件大型真空容器模压成型和焊接变形控制等关键技术；掌握了具有国际先进水平的异形铜合金厚板材制造成型工艺，实现了高强度膨胀螺栓组件的自主国产化；研制成功国际先进水平的国内首台大型立轴脉冲发电机组。

以该项目中研制成功的国内首台大型立轴脉冲发电机组为例，其研发团队首创了多项特有技术，攻克了六相大电流脉冲发电机、大惯量高速转子、宽频变化控保系统等技术难题，在研制过程中形成了一批拥有自主知识产权的创新成果。

在我国核能发展实施“热堆—快堆—聚变堆”三步走战略中，将聚变能作为解决能源问题的最终一步。开发核聚变能不仅是解决我国能源战略需求的途径，对我国未来能源与国民经济的可持续发展具有重大战略意义。

“瞄准本世纪中叶实现聚变能应用的目标，HL-2M装置是实现我国核聚变技术高质量发展的重要依托，将使我国堆芯级等离子体物理研究及相关关键技术达到国际先进水平，成为中国携手世界核聚变能开发的国际合作平台。”该项目相关负责人表示。

据新华网