量子计算虽然能指数级地加快大数分解等问题的求解速度，但是现在还没有证据表明量子计算能破解所有的数学困难问题。研究者们基于这些问题设计密码算法，并认为这些密码算法是具备抗量子攻击能力的，于是就形成了后量子密码。


视觉中国供图

未来量子计算或可快速破解现代公钥密码

后量子密码：能够抵御量子计算破译吗

◎本报记者 **吴长锋**

近日，在第三届雁栖湖国际后量子密码标准化与应用研讨会暨后量子技术成果发布会上，清华大学丘成桐数学中心、北京雁栖湖应用数学研究院教授丁津泰指出，随着量子计算的发展，作为当今网络形态安全信任根基的现代公钥密码学未来可能会被彻底颠覆。为此，与会专家呼吁，加强对能够抵御量子密码算法的“后量子密码”的研究部署，建立后量子密码标准，以保证未来网络空间安全。

量子计算的发展为什么可能会彻底颠覆现代公钥密码学？后量子密码与现代公钥密码有何不同？中国又为什么要建立自己的后量子密码标准？带着这些问题记者采访了相关专家。

量子计算超强算力威胁现代公钥密码安全

“现代公钥密码学的安全性取决于公钥算法所依赖的数学困难问题的计算复杂性。”科大国盾量子技术股份有限公司（以下简称国盾量子）产品研发中心资深技术专家赵于康博士告诉科技日报记者，现代公钥密码学诞生于20世纪70年代，其基本思想是：基于数学上难解的计算问题生成一对密钥，一个为加密密钥，一个为解密密钥。由于在有限计算资源和计算时间内，由加密密钥推算出解密密钥的计算量很大，在实践上十分困难，因此保证了密码的安全性。

赵于康表示，通常来说，最具代表性的应用于公钥密码设计的数学困难问题，包括质因数分解、离散对数、椭圆曲线等。最具代表性的公钥密码包括RSA、ElGamal、ECC等。

公钥密码主要用于加解密、密钥分发、数字签名和认证等，它们对于保障数字安全十分重要。“例如数字签名和认证可为办公终端、物联网终端等建立身份、行为的信任保证；加解密可为数据传输提供有限的加密或对称密钥分发保障。”赵于康说。

量子计算机的快速发展有可能对现代公钥密码学形成挑战。“由于量子计算机能指数或多项式量级地加快某些复杂计算问题的求解速度，因此现代公钥密码学很有可能被量子计算技术彻底颠覆。”赵于康告诉记者，以Shor量子算法为例，其可以在多项式时间内解决大整数分解和离散对数求解等复杂数学问题，因此可以快速破解广泛使用的RSA、ECC、ElGamal等公钥密码。

“例如，分解一个400位的大整数，经典计算机需要约5×10^{22}次操作，而量子计算机仅需要约6×10^{7}次操作，后者所需操作数仅为前者的八十万亿分之一。”赵于康说。

赵于康表示，近年来量子计算机硬件快速发展，各式量子计算机相继实现了“量子计算优越性”。若再结合特定的量子算法，它们就可能对现代公钥密码构成更直接、更紧迫的威胁。

基于新的复杂问题构建量子计算机无法破解的密码

“量子计算虽然能指数级地加快大数分解等问题的求解速度，但是现在还没有证据表明量子计算能破解所有的问题，比如格问题、非线性方程组求解问题、纠错码的一般译码问题等。”赵于康说，研究者们基于这些困难问题设计密码算法，并认为这些密码算法是具备抗量子攻击能力的，于是就形成了后量子密码（PQC）。

“后量子密码指的是可以抵御已知量子计算攻击的现代公钥密码，这类密码算法的安全性同样依赖于计算复杂度，不同的是它基于的是新的复杂问题。”赵于康表示，这些问题的破解目前对于量子计算来说比较困难，且科学家们认为在很长一段时间内量子计算破解这些问题都会比较困难。中国科学院量子信息重点实验室郭国平教授则认为，虽然现在量子计算破解一些后量子密码比较困难，但随着量子计算机的快速发展，两者之间将会形成“道高一尺魔高一丈”的局面。

后量子密码的应用范围与现代公钥密码类似，可用于政务、金融、通信、数据、能源等领域。“但需要注意的是，后量子密码的安全性分析仍然是个复杂问题。”赵于康解释说，一方面，后量子密码算法设计往往需要对它依据的原始计算困难问题进行改动。而这种改动，可能会使得算法的安全性并不等价于数学上的困难问题，其安全性分析也会随之变得更加复杂。另一方面，现有的后量子密码是针对已知的一部分类型的量子攻击而设计的，对于新的量子攻击，或者经典攻击可能并不免疫。例如，2022年7月，美国国家标准和技术研究所（NIST）宣布了首批四种后量子加密算法，包括CRYSTALS-Kyber、CRYSTALS-Dilithium、FALCON和SPHINCS+。同年12月，瑞典皇家理工学院研究人员发文称，在CRYSTALS-Kyber特定实现中发现一个安全漏洞，攻击者利用该漏洞可以发起侧信道攻击。

“其实，中国在另一实现‘量子安全’的重要技术路径——量子密码方面更具优势。在最有可能实现量子密码实用化的量子密钥分发（QKD）领域，我国不论是技术还是应用都在领跑，并取得了一系列世界瞩目的成果。”赵于康表示。

建立标准是后量子密码落地应用的前提

赵于康认为，任何一个密码算法的设计都是为了最终落地应用，而标准是一项技术走向产业化、规模化，并实现商业落地的重要前提。

在赵于康看来，目前美国、日本、韩国、欧洲等国家和地区均在进行后量子密码的标准化工作，中国在这方面则起步较晚。标准的形成本身也是一种技术创新的过程，完善的标准可以加快科技创新成果产业化推广应用，加速科技成果向现实生产力的转化。

赵于康告诉记者，由于后量子密码在密钥长度、算法构造等方面与现有密码存在的差异较多，与应用系统的接口相较于量子密钥分发也更多，因此从现有公钥密码算法迁移到后量子密码算法的过程是一项巨大的工作。“据专家估计，这个迁移过程大概需要10—15年。只有后量子密码算法早日实现标准化，才能为尽早落地应用、对抗量子计算攻击做好准备。”赵于康说。

我国在以量子密钥分发为代表的量子密码领域已实现“换道超车”，而后量子密码与量子密钥分发的融合应用方案也是国际研究的方向之一。“例如，后量子密码可用于初始身份认证，这种认证只需要很短的时间，一旦完成，后续生成的量子密钥就是长期安全的。”赵于康补充道，此前，中国科学技术大学、云南大学、上海交通大学与国盾量子等单位联合，在国际上率先探索了在量子密钥分发网络中使用后量子密码进行认证的方案，该方案提供了一种高效解决预置密钥关键问题的有效途径。

“我国的后量子密码标准化推进工作虽起步较晚，但可以参考欧美等国已有的成熟经验。与此同时，应该加强产学研用协同，在相关部门牵头和指导下，融合学术界、产业界等多方力量，尽早布局中国自己的后量子密码标准。”赵于康表示。

推进央国企上云用云进程

◎本报记者 **刘 艳**

由中国信息通信研究院（以下简称中国信通院）和中国通信标准化协会主办的2023年可信云大会日前在京落幕，《云计算白皮书（2023年）》发布，可信云最新评估结果出炉，央国企高质量用云创新赋能计划、一云多芯应用创新生态社区等同期启动。

正如中国电子学会理事长张峰所言：“在国家政策支持和推动下，我国云计算产业市场规模、行业应用、产业生态等均呈现良好态势。”以云计算为代表的新一代信息技术快速发展，在催生新兴产业的同时不断激发传统产业的发展活力。

中国互联网协会常务副秘书长陈家春强调，云计算在数字经济和数字技术高速发展的环境下仍将处于黄金发展期，机遇与挑战并存。它已从一种IT资源的服务形式演变为企业数字化转型的重要底座，推动着企业管理和生产经营模式创新，是新一代软件架构范式，更是未来数字经济发展的关键着力点。

作为数字世界的操作系统，云计算的价值正全面展现，它向下重新定义着算力资源使用方式，向上定义着数字应用新界面。中国信通院云计算与大数据研究所云计算部主任马飞认为，央国企应合理选择上云路径，并从云化改造、云上全链路安全保障、云上生态建设及数据互联互通等多方面发力，推进上云用云进程。

大会期间，天翼云携手中国信通院及央国企产业生态合作伙伴共同启动央国企高质量用云创新赋能计划，天翼云与中国信通院开启《央国企用云白皮书》研究，将聚焦央国企用云发展现状，探究央国企深度用云技术路径。

可信数网框架及系列成果发布

科技日报讯（记者**刘艳**）记者8月4日从中国信息通信研究院（以下简称中国信通院）获悉，由中国信通院等单位共同提出的可信数网（TDN）框架及系列成果于近日发布。

中国信通院云计算与大数据研究所副所长魏凯介绍，为解决数据供给不充足、机构相互不信任、安全流通无范式、数据使用不可控等问题，中国信通院、隐私计算联盟联合行业多家企业共同提出了可信数网。它是数据流通各个参与方在互认、互信、互联的机制下，形成的跨区域、跨行业、跨主体的数据流通基础设施，对实现公关数据、企业数据和个人数据的可信流通具有重要意义。

据了解，中国信通院联合蚂蚁集团、洞见科技、海光、Intel、冲量在线和龙蜥社区等单位在大会共同发布的“可信数网（TDN）测试床”，目前已完成部分关键能力的建设。

魏凯介绍，该测试床一方面将服务于可信数网建设与运行过程中的准入、审查与监控，另一方面能够为行业内更多技术提供方、应用需求方提供一系列定制化测试服务。

为夯实可信数网的技术互联基础，解决不同企业间数据流通技术互操作性不足、架构不统一等问题，中国信通院联合产业各方发布了“可信数网（TDN）隐私计算互联互通第二批试点项目”，该项目包括3个算法（ECDH-PSI、SS-LR、PHE-FLR）的开放协议及实践和3个管理调度层的互联实践。

中国信通院相关负责人表示，将继续联合行业生态伙伴采取循序渐进的步骤建设可信数网，丰富可信数网测试床检测能力、搭建可信数网实验网，逐步将实验网的各项能力拓展落地到真实业务场景，全方位构建可信数网生产网，从而高质量支撑数据要素市场建设。

“数实融合”增强工业经济发展新动能

◎新华社记者 **张辛欣**

拓展5G应用规模，今年推动不少于3000家企业建设5G工厂，加快算力资源统筹和互联互通……近日，工业和信息化部推出一系列举措，加快数字技术与实体经济融合。

工业和信息化部总工程师赵志国表示，将以智能制造为主攻方向，全面推动制造业数字化普及，系统推进智能化升级，通过数字技术的“赋能”不断增强工业经济发展的新动能。

在鲁南中联水泥有限公司，3条新型干法水泥生产线正有条不紊生产。通过云洲扁鹊生产智能化服务系统，技术人员可以远程查看并实时控制水泥生产。“这套系统在关键设备及关键工艺上部署600余个传感器，采集生产过程中的数据，配合数字孪生仿真系统，可实现全流程精准控制。”鲁南中联水泥有限公司有关负责人介绍，通过智能化改造，水泥生产质量进一步提高，实现了节能减排。

近年来，我国加快工业互联网规模发展，推动数字技术在实体经济领域的融合应用。今年以来，面对需求收缩等多重压力，大量制造业企业通过数字化应用降本增效、积极应对。

当前，智能、绿色生产的实践正在各地展开。工业和信息化部数据显示，智能工厂建设规模不断扩大。截至目前，各地建设数字化车间和智能工厂近8000个，其中，2500余个达到了智能制造能力成熟度2级以上水平，数字化转型基本完成。这些示范工厂，产品研发周期平均缩短20.7%，生产效率平均提升34.8%，产品不良品率平均下降27.4%。

在汽车、工程机械等装备制造业，协同设计、远程运维等模式加快推进；在家电、服装等消费品行业，通过大规模定制、用户直连制造、共享制造等，不断挖掘体验价值；石化、冶金、建材等原材料行业，跨工序质量管控等模式促进产业提质增效和节能降耗……工业和信息化部运行监测协调局局长陶青说，数字技术加速向工业生产制造各环节各领域推广，智能制造新场景、新方案、新模式不断涌现。

重庆推出制造业数字化转型行动计划，明确到2027年重庆规模以上制造业企业基本进入数字化普及阶段；《上海市推动制造业高质量发展三年行动计划（2023-2025年）》提出，到2025年实现40万家中小企业上云上平台……各地围绕拓宽数字化应用推出一系列举措。

当前，“数实融合”正迎来更多“政策包”。

在数字基础设施建设上，工业和信息化部明确，将坚持适度超前原则，积极推进5G网络建设，持续拓展5G网络覆盖广度深度，并将出台指导算力基础设施高质量发展的政策文件，加快构建云边端协同、算存运融合的一体化、多层次的算力基础设施体系。

在丰富行业应用方面，培育一批高水平的5G全连接工厂标杆，加速5G由生产外围向核心控制环节延伸，拓展5G在工业、矿业、电力、港口等领域的应用规模，打造“5G+工业互联网”发展升级版，不断壮大融合产业生态。

在推动企业上云方面，将进一步降低数字化门槛，深入实施数字化赋能、科技成果赋智、质量标准品牌赋值中小企业“三赋”专项行动，支持企业加快数字化转型，在制造业强链补链中发挥更大作用。

“下一步，将继续加大政策供给，坚持分业施策，激发数字技术应用赋能价值。”赵志国说，工业和信息化部将持续深入推进场景模式推广、解决方案攻关、标准体系建设，推动各方加强低成本、轻量化的5G工业级产品研发和产业化，着力提升制造业高端化、智能化、绿色化水平。


图为在一实现5G专网应用智能化生产的工厂内，自动化机械手臂正转动工作。
新华社发（胡肖飞摄）

数字交互引擎：走出游戏，服务各行各业

◎本报记者 **张佳星**

7月28日，2023中国国际数码互动娱乐展览会召开。在同期论坛中，中国音像与数字出版协会（以下简称中国音数协）常务副理事长敖然发布了《数字交互引擎的应用与价值研究报告》（以下简称报告）。

据介绍，报告由中国音数协游戏工委和中国游戏产业研究院联合完成，面向国内多家游戏企业开展了广泛调研，获得了游戏企业与多领域专家对于数字交互引擎的专业意见。报告指出，业内普遍认同数字交互引擎代表着游戏产业原生的科技力量。

敖然介绍，以数字交互引擎为代表的游戏科技正越来越广泛地进入游戏之外的领域。随着人们对虚拟世界的探索从视听层面走向更深层次的感知、交互层面，数字交互引擎正持续推进技术能力迭代、打磨跨平台通用能力，并有望在游戏特有组件的基础上，形成面向行业的“通用引擎”。例如，基于图形建模、实时渲染、物理仿真、音效制作、动画制作等核心功能模块的数字交互引擎已能够实现虚拟重现、虚实融合、虚拟仿真和虚实互动等功能，成为构建实时虚拟世界、实现虚实交互的关键工具集。

据介绍，带有游戏“基因”的数字交互引擎已经在文化领域、实体产业等方面有了很多创新实践。作为数字内容创作与交互的重要工具，数字交互引擎正高效助力影视、演艺、文保、会展、旅游等文化领域的内容生产。数字交互引擎也可以和传统工业软件结合，增强传统工业软件在3D显示、实时交互等方面的能力。

未来，数字交互引擎在工业、商业、教育等领域均具有广阔的应用场景。敖然表示，在行业应用方面，数字交互引擎有望成为面向垂直行业的“标准化引擎”；在大众应用方面，数字交互引擎有望提供助推媒介升级的便捷工具。此外，作为底层工具的数字交互引擎也正在与生成式人工智能互相融合。

“数字交互引擎已经成为我国文化科技领域的基础性核心技术，‘数字交互引擎是重要科技力量’这一观点已成业内共识。”敖然表示，应加强对于数字交互引擎技术的研究与应用，强化游戏企业与高校的产学研合作及人才培养力度。