

在当今数字化深度融入工作与生活的背景下，现代公钥密码构筑起守护日常沟通、金融交易及商业安全的坚固防线。然而，随着量子计算技术的迅猛发展，尤其是密码分析相关量子计算机的出现，互联网的信任锚和安全通信体系将面临崩溃风险，严重威胁着从个人数据安全到国家战略安全的各个领域。因此，如何在量子时代确保大型网络安全的持续发展，并在量子计算的冲击下稳固并重建安全体系，成为各国政府、企业及每位数字生活参与者亟须面对的重大挑战。

现代公钥密码学：大型网络的信任基石

20世纪70年代中叶，斯坦福大学的迪菲和赫尔曼通过提出Diffie-Hellman密钥交换协议，为公钥密码学的发展奠定了基础。公钥密码学的问世巧妙解决了大型网络中的信任难题与高效安全通信的挑战。它摒弃了传统对称密码学需双方共享唯一密钥的局限，而是采用公钥与私钥的配对机制：公钥公开用于验证，私钥则严格保密，专用于签名和解密。随后，美国麻省理工学院的里夫斯特、沙米尔和阿德曼提出了第一个比较完善和实用的公钥加密算法和签名方案——RSA算法，首次展示了依托复杂数学难题（如大整数分解）实现密码算法创新与突破的可能性。此机制下的签名系统，为动态网络环境构建了用户间的可靠信任机制，允许每个网络参与者生成独特的密钥对，通过私钥签名信息，并利用公钥进行验证。这种基于数学基础的强绑定签名，不仅能有效防止信息被篡改且能确保签名的不可抵赖性，为现代网络空间提供了证明自己唯一身份的电子签名，为互联网等网络空间构建了坚实的信任根、信任锚。

在实际应用中，公钥密码学极大地简化了密钥管理流程。传统对称密码学需预先在通信双方间交换密钥，

抗量子密码：为全球网络安全筑起新防线

□ 丁津泰 向 宏

导致频繁进行点对点密钥交换的繁琐与成本高昂，而公钥密码学允许用户通过公开的公钥加密通信密钥，接收方则用私钥解密，整个过程通过计算机网络安全协议自动化完成，无需人工干预，降低了成本并提升了效率。例如，微软通过私钥签名软件更新，全球用户利用公钥验证，确保了软件的真实性和安全性；中国电子证书体系也广泛采用公钥签名技术，增强了网络交易与信息传递的可信度。

因此，公钥密码学不仅是当今大型计算机网络通信的安全基石，也是全球网络空间不断演进的信任根。没有公钥密码学的支撑，就不可能有安全高效的大型计算机网络通信。

量子革命下的密码学：抗量子公钥密码的崛起

随着科学技术的发展，现代公钥密码技术正面临量子计算机的严重威胁。这一由美国加州理工学院著名的物理学家理查德·费曼于1981年提出的量子计算机概念，旨在利用量子物理原理与基本粒子等构件实现高效运算，模拟微观量子物理世界。然而，由于技术门槛极高，涉及全新体系架构、严苛的量子调控要求及巨额投资，加之早期对其潜在应用认知的局限，该技术初期并未获得广泛关注。

直到20世纪90年代中叶，量子计算领域取得重大突破，特别是麻省理工学院的彼得·舒尔在1994年发明的Shor算法，能高效分解大整数，直接

威胁到基于整数分解难度的现代公钥密码体系。这一发现预示着，一旦能够运行Shor算法的大型量子计算机被研发出来，现有的公钥密码算法将失去效用，互联网的信任与安全通信体系将面临瓦解，全球社会经济活动也将因此全面崩溃，后果不堪设想。

尽管全球科技强国在量子计算机研发上投入巨大，但真正对现代公钥密码产生巨大威胁的是一种与图灵当年研发的密码破译功能类似的新型量子计算机，美欧称其为密码分析相关量子计算机。一旦有国家成功研发密码分析相关量子计算机，它将在大型计算机通信网络中冒充各种身份进行窃密，对现代公钥密码体系构成巨大挑战。因此，各国政府对密码分析相关量子计算机的研发进展保持高度保密。

事实上，不少国家正采用“先收集，再破译”策略，收集海量公钥加密数据包，以待未来用密码分析相关量子计算机破解这些数据。这一局势凸显了全球网络安全新挑战，强调了加强抗量子密码技术研发的重要性和紧迫性。2000年，美国IBM实验室的艾萨克·庄首次搭建了一台拥有7个物理量子比特的计算机运行Shor算法，成功将15分解为质数3和5，证明其不仅理论正确且实际可行，预示量子计算机威胁迫近。这一实验促使不少具有远见卓识的研究者开始涉足这一全新研究领域，探索新数学难题，构建能抵御未来量子攻击的新型公钥密码——抗量子密码（PQC），为全球网络安全筑起新防线。

抗量子密码迁移与标准化：保障未来互联网安全的新防线

彼得·舒尔和艾萨克·庄的开创性工作加速了量子计算机的发展，促使全球密码学、产业界及标准化机构提前布局应对策略。2006年，首次国际PQC会议在比利时召开，标志着抗量子计算的新一代公钥密码研发正式启动。2012年，美国国家标准与技术研究院启动PQC项目工作组。2015年，美国国家安全局公开宣布将更换现有公钥密码系统为抗量子版本。2016年，美国国家标准与技术研究院启动全球PQC算法征集，并于2022年7月公布了首批标准化算法名单。同时，美国白宫在2022年发布第10号国家安全备忘录《关于促进美国在量子计算领域的领导地位，同时降低易受攻击的密码系统风险的国家安全备忘录》，要求各类计算机网络采用抗量子密码保护；紧接着，美国国会也通过法案，要求全美计算机网络开始进行抗量子密码迁移工作，预计2035年达到抗量子计算威胁的安全状态。对于全球互联网，抗量子密码迁移能在不改变现有网络架构的基础上，以最小代价更新公钥密码系统，也能确保互联网能够继续拥有或重建抵御量子计算机攻击的信任机制及安全的通信体系。因此，抗量子密码迁移是确保当今互联网持续安全、可靠运行的关键所在。

需要强调的是，抗量子密码的安

全性基石牢固建立在全球密码学界和产业界广泛认可的公开数学难题之上。与各国在高度敏感信息系统中广泛应用的传统密码技术不同，抗量子密码作为商用密码，在保障数字经济安全方面扮演着十分重要的角色。尤为关键的是，抗量子密码为现有的大型计算机通信网络，涵盖金融、通信、能源、电力、交通等关键基础设施的计算机网络，以及未来蓬勃发展的物联网、车联网等，提供了独一无二且无可替代的身份认证机制，从而确立了其在全球数字经济时代作为信任根与信任锚的坚实基础。鉴于抗量子密码的商用性质，世界各国对其标准化进程及后续的产业化、市场化效应给予了高度重视。其中，美国国家标准与技术研究院今年8月正式公布了全球第一个抗量子密码标准，正深刻塑造着全球密码标准和产业布局的未来。值得注意的是，抗量子密码算法标准虽由美国国家标准与技术研究院选定，但其研发力量却遍布全球各国学界、工业界及国际标准化组织，共同推动抗量子密码技术的发展。

随着世界各国抗量子公钥密码标准化工作的开展，一个重要的工程领域展现在世人面前，即全球网络空间将面临安全信任根（即抗量子公钥密码）的替换，进而导致整个全球网络空间安全的大迁移。这种大迁移体现在以下几个方面。

首先，互联网及大型计算机通信网络的信任根替换，远非简单替换易受量子计算机攻击的公钥密码模块，而是一项紧迫且漫长、复杂的工程化

工作。自20世纪90年代互联网兴起以来，网络架构已高度集成，涵盖软硬件设备及通信协议。作为互联网的信任锚、信任根，现代公钥密码早已深深嵌入其中。加之全球IT产业历经沧桑，企业兴衰更替，为信任根的更换增添了额外难度。然而，抗量子密码迁移这个千载难逢的历史机遇，也预示着网络信息安全领域将迎来新的产业链、供应链和市场机遇。

其次，世界各国对重要信息系统基础设施信任根的更换策略各异，但均给予高度重视。美国、英国、加拿大等国倾向于迅速且全面地替换，以确保国家安全计算机网络免受量子计算机威胁。而欧盟则倾向于采用混合模式，即在保持现有公钥密码系统稳定运行的同时，引入抗量子密码系统，以平滑过渡到PQC时代。此举旨在在量子计算机真正威胁到现有系统之前，为大型计算机网络提供双重保障，并在必要时无缝切换至抗量子密码系统。

最后，尽管量子计算机尚未公开破解现有公钥密码，但全球IT强国已前瞻性地布局后量子安全时代。这将导致未来全球网络空间安全迎来巨变，不仅涉及抗量子密码技术本身，还将逐步波及到网络软硬件设备、安全技术研发、国际标准竞争及网络安全市场的未来格局。

总之，抗量子密码技术的革新与产业供应链的发展，正推动全球网络空间迈向新的安全纪元。这场大迁移大变局的复杂性和挑战远超“千年虫”问题。面对量子安全挑战，任何国家都无法独善其身，需携手合作，共同构建网络空间的安全防线。

（作者分别系清华大学丘成桐数学科学中心教授，重庆大学大数据与软件学院教授）



为什么要加装抗量子攻击护盾？

□ 窦猛汉



随着量子计算的快速发展，传统加密技术面临“Q-day”的挑战，即量子计算机可能破解现有加密体系，威胁经济稳定、国家安全和个人隐私。为此，抗量子密码（PQC）作为创新技术应运而生，被认为是能够有效抵御量子计算机攻击的方法，让我们在享受数字便利的同时，能更加安全地迎接量子计算的未来。全球尤其是欧美国家正积极部署PQC迁移战略，构建抵御量子计算机攻击的安全体系，确保量子时代下数字资产、通信安全和社会运行的安全与稳定。

“本源悟空”装备抗量子攻击护盾，行业先行推进抗量子密码应用

尽管“Q-day”尚未来临，但不少企业已经开始逐步推进抗量子密码算法应用开发，并在实践中验证抗量子密码的有效性。

本源量子在今年4月采用PQC混合加密方法为中国最新的第三代自主超导量子计算机“本源悟空”成功装备国内首个“抗量子攻击护盾”。该团队开发的端到端的PQC混合加密方法将传统加密算法、国密系列算法和抗量子密码、格基密码算法相结合，为量子云服务的用户端和服务端之间的信息传输提供多重安全保护。后续，本源量子还将进一步引入抗量子密码和国密签名算法的混合方案，实现抗量子密码认证，不断完善系统安全性，这一实践为中国探索了有效抵御量子计算机攻击的可行性方案。

2023年2月，法国泰雷兹集团在其旗舰移动安全应用Cryptosmart中创建抗量子密码的首个真实世界应用，利用5G SIM卡实现抗量子密码。同年8月，美国谷歌浏览器在其最新版本中部署了混合后量子密码协议，旨在建立安全的TLS协议网络连接期间保护对称加密数据的共享。美国苹果公司于今年2月宣布利用抗量子密码技术对其iMessage通讯平台进行升级，以抵御未来将会出现的来自量子计算

机的攻击，这也是迄今为止最大规模的抗量子密码应用案例之一。

现阶段，抗量子密码算法仍然相对较新，只经过了较少的“战斗测试”，还需要鼓励行业开展抗量子密码算法应用技术，以经典+PQC混合方案或纯PQC迁移方案设计，搭建多种抗量子密码迁移模型，探究其基础设施适配度与性能和稳定性。在我国抗量子密码算法标准及迁移方案未选定和实施之前，倡导企业通过“百家争鸣，争奇斗艳”，预先清除后续迁移过程中的层层障碍，提前开展网络安全基础设施建设，选择行业内认可的抗量子密码迁移方案，稳扎稳打地为后续的抗量子密码整体迁移服务。

同时，建议行业开展量子计算与抗量子密码算法结合分析，提前加强量子计算机应用生态建设，探索“量子计算+PQC算法”创新应用模式。鉴于在美国国家标准与技术研究院征集PQC算法过程中，部分先前提备受看好的算法遭遇了挫折，信息安全从业者应高度关注抗量子密码算法的安全性评估，以及哪些算法能够经受住时间的考验。特别是在量子计算或量超融合计算模型下，抗量子密码算法的安全性究竟如何，以及它们受量子计算威胁的程度有多深，已成为行业科研与技术人员亟须共同探究的前沿课题，以推动抗量子密码算法的安全性检验，及时查缺补漏，全面打造我国抗量子密码算法和应用落地的安全防护盾牌。

统筹布局抗量子密码迁移，应对量子计算威胁

在看到量子计算飞速发展的同时，我们应注意其作为前沿技术的双刃剑特性，尤其是潜在的被恶意使用的风险。一些国家正在采取“现在存储，稍后解密”策略，现阶段拦截并存储加密数据，等到量子计算机足够强大时破解这些数据。因此，向量子密码的过渡是技术演进的必然趋势，更是维护加密体系安全、防止未来数据泄露的关键步骤。

从历史上看，部署现行的公钥密码体系花费了将近20年的时间。而将现行公钥密码体系向抗量子密码迁移则大概需要10到15年，这是一项长期

且花费巨大的工程。

美国政府自2022年起已经开始统筹布局抗量子密码迁移计划：2022年5月，白宫发布《关于促进美国在量子计算领域的领导地位，同时降低易受攻击的密码系统风险的国家安全备忘录》，建议采用政府一体化的模式来促进和激励向抗量子密码迁移，评估和盘点易受攻击的密码风险，并强调迁移中应关注提升密码敏捷性。次年3月，美国发布《2023年国家网络安全战略》，提出政府应增加对抗量子密码迁移的有关投资，广泛更换容易被量子计算破坏的硬件、软件和服务。5个月，美国网络安全与基础设施安全局、国家安全局和国家标准与技术研究院联合发布《量子准备：向后量子密码迁移》指南。通过若干文件指引，美国目前已经启动联邦政府在抗量子密码实用化方面的具体行动计划、建立起量子准备路线图、梳理并形成易受量子攻击的系统和资产清单。

国内在抗量子密码迁移方面，尚且缺乏指引，无论是政策层面还是企业层面，都应对抗量子密码及其迁移保持高度关注，强化布局谋划。结合我国量子信息技术发展基础，尽快在国家层面统筹开展为期10—15年的抗量子密码研发和迁移计划，研判向抗量子密码迁移的安全性风险以及对我国相关制度的影响等，尽早规划和总体布局，并与密码学研究人员、行业和标准化组织密切合作，采取多管齐下、协调一致的措施确保安全性和平稳过渡。

加速抗量子密码算法标准制定，构筑后量子计算安全基石

如何在全球量子计算竞赛中抢占先机，率先为国家安全打造“抗量子攻击护盾”？只有抗量子密码算法早日实现标准化和落地，才能为向抗量子密码的过渡做好准备。

当前，全球世界范围内已经有多个国家开展了抗量子密码标准化的研究。2015年，美国国家安全局宣布该国将由现行的公钥算法过渡到抗量子密码算法系统。2016年4月，美国国家标准与技术研究院正式启动PQC项

目，面向全球范围征集PQC标准算法和协议。今年7月，韩国移动运营商LG Uplus宣布与韩国国家情报院共同提出的光传输网络中的抗量子密码应用规范已被韩国电信技术协会采纳为该国首个相关标准，韩国国家情报院计划将该标准应用于今年建成的开放量子测试平台。目前，以美国国家标准与技术研究院为主导的抗量子密码标准化工作在全球范围内位于领跑地位，并于今年8月已完成抗量子密码算法的标准化。

中国抗量子密码标准化工作起步较晚，但自2019年起，中国密码学会已先后举办三届后量子密码算法竞赛征集活动。2023年12月，中国抗量子密码战略与政策法律工作组正式成立。该工作组旨在深入研究抗量子密码技术、产业及业务现状，同时对比分析国内外相关政策与法律法规，通过多渠道发布蓝皮书、专题研究报告等成果，以加速形成中国抗量子密码的共识与行动方案。

在推进抗量子密码标准化的过程中，我国可借鉴欧美等国的成熟经验，瞄准国际水平，依托国家密码主管部门的统筹规划，加速标准化进程，组织制定抗量子密码算法标准，为量子计算企业及行业提供政策法规与标准化指引。同时，要全面考量其安全性，这涉及多个层面。在算法设计上，结合量子计算技术全面评估抗量子密码算法的安全；在算法软件开发上，全面评估抗量子密码算法在软件层面的安全性；在算法硬件开发上，做好抗量子密码算法的硬件安全防护。此外，抗量子密码算法的标准落地还必须考虑其在软硬件层面实现上的性能与稳定性，以及是否适配当前的基础设施。以上是抗量子密码算法标准化落地的关键技术指标，需要各行各业积极参与和推进、协同合作，共同推动我国抗量子密码算法的标准化实施。

面对量子计算带来的数据安全威胁，随着技术的不断进步和完善，抗量子密码将为更多关键领域的数据安全提供保障，为量子计算时代安全格局构建“防护墙”。

（作者系中国第三代自主超导量子计算机“本源悟空”软件研制团队负责人、安徽省量子计算工程研究中心副主任）

健全新型举国体制

□ 田德录



科研机构、高水平研究型大学和科技领军企业功能定位，分类部署实施重大任务，对目标明确的重大战略产品研发或重大科技攻关任务，采用总承单位负责制，发挥国家实验室、国家科研机构等作用；对行业特色突出且任务边界清晰、主要目标为具体交付物或重大装备的任务采用业主负责制，由科技领军企业牵头组织实施。

第三，加强科技创新资源统筹配置。面向国家重大需求，通过政府和市场协同发力，更大范围、更深层次统筹科技创新资源。建立适应新型举国体制下重大任务实施需要的创新资源组织调配机制，破除跨部门、跨军民、跨央地的资源整合障碍。引导社会资本投入科技创新，加强对国家重大科技任务、新领域新赛道的金融支持。

第四，强化攻关成果转化应用。国家重大科技任务部署在考虑技术链的同时，要统筹考虑产业链与价值链。要健全应用场景驱动的技术攻关体系，统筹部署重大科技攻关与成果转化，加速培育科技攻关成果应用市场，布局建设一批概念验证、中试验证平台，促进应用牵引、研用一体、迭代升级的良性循环。

党的二十届三中全会通过的《中共中央关于进一步全面深化改革、推进中国式现代化的决定》明确提出健全新型举国体制，这是党中央立足新一轮科技革命和产业变革发展态势，以及当下激烈的国际科技竞争形势作出的重大制度安排，不仅是新时代加快实现高水平科技自立自强的必然要求，也为新形势下健全新型举国体制指明了方向。

面对新形势新要求，我国新型举国体制的实施机制尚不健全，难以满足当前科技竞争和未来发展战略的制高点需求。一是国家重大战略需求凝练不够精准，过多依赖高校和科研院所专家，企业作用发挥不足，导致与产业实际需求脱节。同时，重大任务的全链条部署机制不健全，创新链、产业链、人才链、资金链之间的衔接不够紧密。二是我国科技创新的组织化和协同化程度不高，现行科技项目多以竞争性课题方式运作，导致科研组织小而散，任务由团队自行申报管理，且科研单位对项目监督手段有限。同时，这也使得国家战略科技力量的科研组织趋同化，难以在不同需求场景中发挥各自特色和优势进行协同攻关。三是科技资源分配分散、低效问题依然显著，全社会创新资源的统筹调配制度尚不健全，导致部分重大任务难以高效汇聚所需的人才、资金、平台等要素。央地间、军地间的体制分割问题较为突出，力量和资源的整合配置缺乏灵活性。政府引导、多元投入的大资源配置格局尚未形成，且引导社会投入服务国家战略目标的手段有限。四是技术攻关和成果应用缺乏统筹部署，常常在技术突破后才推动成果转化，导致攻关技术成果难以快速与市场对接。创新技术成果缺乏示范应用场景，熟化和迭代升级效率较低。

针对上述问题，要坚持“四个着力点”，以解决国家战略急需为目标，更加科学凝练提出重大任务需求，不断加强创新资源统筹和力量组织，构建高效协同的组织运行体系。第一，完善国家重大任务决策部署。优化重大科技任务需求凝练机制，由部门、地方、学术专家和产业界多方参与，站在国家角度切实找准需求与任务。建立重点领域科技创新全链条部署机制，一体统筹基础研究、技术创新、成果转化与产业化，一体配置资金投入、力量组织、政策配套、金融支持和市场应用资源。

第二，改革重大任务组织实施模式。构建场景驱动下的“大兵团”协同攻关机制，立足国家实验室、国家