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

热点透视 rediantoushi

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。

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。

视觉中国供图

“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。

吴长锋

“数实融合”增强工业经济发展新动能

科学观察 kexueguancha

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。

张辛欣

（上接A1版）他希望借本次论坛举办契机交流发展经验，凝聚各方智慧，深入探索健康中国战略实现新路径，共同探求康养产业合作发展新机遇，推动中国康养产业发展再上新台阶。

王黎表示，近年来，山西省民政厅坚持强化顶层设计、标准示范引领、融合创新发展、突出比较优势，积极打造了全链条、全周期、全要素的康养服务供给体系，推动形成养老事业和产业协同发展的工作格局，不断提升老年人的获得感、幸福感、安全感。省民政厅也将借此契机，围绕健康与养老主题与各位专家学者共同探讨健康养老发展先进理念，共同推进健康与养老事业的发展，为广大民众的健康福祉作出应有贡献。

随后，丁纪岗、吴华芳共同为山西合聚碧绿园服务有限公司“晋城市科普教育基地”揭牌；王黎和晋城市民政局党组书记、局长王涛为“山西合聚养老产业发展有限公司”揭牌。合聚集团党总支书记、董事长杨肖峰与中国老龄产业协会医健委秘书长牟丽娜签订战略合作协议。

开幕式结束后，举行了院士报告会。报告会由晋城市科协党组书记、主席吴华芳主持。

报告会上，从斌院士以《全方位维护人类健康和生存安全》为题作主旨报告。他从健康系统工程、法律制度以及科学技术等角度阐述了全方位、全周期维护人类健康的重要性，并从不同层次、不同视角多样化展示了研究领域的学术宽度和深度。他讲到，健康是身体、心理和社会幸福的完好状态，不仅是没有疾病和虚弱。健康的内涵是要合理的膳食、适量的运动、心理平衡并且戒除不良生活习惯。健康需要靠自己维护，也需要靠他人支持，更需要依赖与生态环境和社会环境的互作。他建议大家要善待自己、善待他人、善待环境，真正实现天人合一，天人相应。

赵继宗院士在题为《脑心同治》的报告中从心脑血管病的现状、临床诊治遇到的挑战入手，阐述了创建脑心同治学科的必要性。他表示，脑心同治代表了临床医学一个潜在的创新领域，脑心同治即五同“同防、同研、同治、同康和中西医同用”，更需要多学科联合，早期诊断，精准治疗，从心脑血管病发病机制入手，才能为脑心血管病的防治开创新局面。

本次论坛由山西省科学技术协会、山西省民政厅、民革山西省委会、中共晋城市委、晋城市人民政府主办，晋城市科协、晋城市民政局、民革晋城市委会、中共泽州县委、泽州县人民政府、合聚集团、山西科技新闻出版传媒集团承办，中国老龄产业协会医养结合与健康管理委员会、《社区天地》杂志、山西省院士专家服务中心、山西省养老事业发展联合会、山西省医学会、山西省专家学者协会、晋城市卫生健康委员会、晋城市医学会、晋城市工商业联合会、泽州县科协协办。来自晋城市政府部门相关负责人、全省医学机构代表、全国健康领域企业负责人以及新闻媒体等170余人参加论坛。

创新杂谈 chuangxinzatan

技能成才 技能报国

陆建华

党的二十大报告提出：“加快建设国家战略人才力量，努力培养造就更多大师、战略科学家、一流科技领军人才和创新团队、青年科技人才、卓越工程师、大国工匠、高技能人才。”

当前，我国正处于从“中国制造”向“中国智造”、从“中国速度”向“中国质量”、从“中国产品”向“中国品牌”转变的关键时期，呼唤着更多执着专注、精益求精、一丝不苟、追求卓越，能够“吃透”技术的大国工匠，一起推动高质量发展，共同谱写中国式现代化新篇章。

匠心筑梦，技能报国，于平凡中彰显不凡。作为我国广大一线技术工人的杰出代表，大国工匠们在新时代的伟大实践中，勤学苦练、深入钻研，勇于创新、敢为人先，同科学家和工程师相互配合、协同攻关，用智慧和汗水创造了一个个举世瞩目的科技和工程奇迹，在强国建设中发挥出主力军和先锋队的作用。他们中，有扎根电能表计量检定一线近40年的黄金娟，也有为“探索一号”科考船加工零部件“零差错”的周皓，有把双手作秤捞出温润宣纸的周东红，还有矢志创新获得8项国家发明专利的谭文波……把想法变成方法，把规划图化为施工图，大国工匠们勤勤恳恳、脚踏实地，数十年如一日深耕本职，用实际行动践行着技能成才、技能报国的理念。

工匠精神，薪火相传，于坚守中引领创新。从奉献焊工岗位50多年的艾爱国到捧起“阿尔伯特大奖”的青年匠人宋彪，我们看到植根于中华优秀传统文化之中的工匠精神不只有“但手熟尔”，还有创新不止。在新征程上，我们不仅要培养出更多具备复合知识结构和创新意识的高技能人才，更要以工匠精神去教育激励年轻人坚定走技能成才、技能报国之路。面对严峻复杂的国际形势和担当中华民族伟大复兴的历史使命，广大科学家、工程师和工匠群体，将秉持心有大我、至诚报国的理念，将个人理想与国家命运紧紧联系在一起，紧盯关键“卡脖子”领域，以科学严谨的态度，以破釜沉舟的决心，以敢为天下先的勇气，以创新驱动发展占据技术制高点，不断提升我国发展的独立性、自主性、安全性，努力为实现高水平科技自立自强，推动构建新发展格局、实现高质量发展和高水平安全作出应有贡献。

铁电材料首次制成『橡皮筋』

拉伸两倍仍保持特性，有望让传感器造型多变

常见于存储器、压电元件等领域的铁电材料，如果获得橡皮筋一样的弹性，有望让传感器造型多变、手机更易弯曲折叠。

8月4日，国际学术期刊《科学》刊登了中国科学院宁波材料技术与工程研究所柔性磁电功能材料与器件团队的科研成果——在全球率先研发出兼具弹性回复与铁电性的新型高分子铁电材料，有效解决传统铁电材料难以在大形变下保持稳定性能的难题，填补弹性铁电材料领域的空白。

铁电材料受到拉伸容易失灵

“铁电材料是一种神奇的绝缘性功能材料，表面自带电荷，没有外加电场时，这些电荷处于无序状态。”该论文通讯作者、中国科学院宁波材料所胡本林研究员介绍，一旦有电场作用在铁电材料上，这些电荷就会重新排列，而且排列的方式会随着电场的变化而变化。

此外，铁电材料还有记忆能力，即便电场不再作用，排列后的电荷也会保持原来的状态而不发生改变。这就使得铁电材料具备高介电常数、压电性、热电性、电制冷性等特性，可以用在计算机存储器、高精度电机、超敏感传感器和声呐设备等电子产品中，也是手机、平板电脑等电子设备中必不可少的材料之一。

近年来，有关柔性可穿戴器件的研究热度不减，这类器件被认为在便携式移动电子设备和人体运动检测等领域有广阔的应用前景。作为制造柔性可穿戴器件的重要材料之一，铁电材料若能实现弹性化，对这一产业发展可起到推波助澜的作用。

“但是研究制备弹性化铁电材料却举步维艰。”胡本林解释说，传统的铁电材料主要为线性结构，排列规整的部分形成结晶区提供铁电性，而剩余的分子链相互缠绕在一起。由于线性的分子链间没有共价连接，一旦施加外力，这种相互缠绕就会解开，进而导致结晶区被破坏，影响其铁电性。

该论文第一作者、中国科学技术大学纳米学院和中国科学院宁波材料所的联合培养硕士生高亮补充道，晶体本身几乎不具备弹性，拉伸率一般低于5%且没有回弹能力，因此铁电材料很难兼顾铁电性和弹性。

“微交联法”编织“渔网”获得弹性

甘蔗就不能两头甜？这项研究中，科研人员通过对材料结构的精准设计和控制，制备出了在高频率大形变下仍然具有良好铁电响应的弹性材料，把它拉伸到原来长度的两倍后，不但能保持原有的铁电性，而且还能在外力撤除后迅速恢复原状，实现了铁电材料铁电性与弹性的平衡。

制备弹性铁电材料的方法被团队称之为“微交联法”——用微量的柔软链状聚合物，让铁电晶体周边非晶的缠绕部分交联起来，相互交织形成具有弹性的渔网状结构。类似于通过化学交联将晶体和缠绕部分置于“渔网”中，制成具有良好的弹性回复能力的铁电“橡皮筋”。

胡本林介绍，团队尝试了几十种材料才找到合适的链状聚合物。这种渔网状结构松散地将铁电晶体连接在一起，在外力作用时，可以产生可逆的形变来吸收外力，避免外力对结晶部分的破坏，进而使材料在一定拉伸范围内依旧能够保持稳定的铁电性；在外力撤销时，这种弹性的渔网状结构能够回复至初始状态。

“此外，精确控制链状聚合物的用量，可以确保铁电晶体能够均匀地分布在交联网络中，使材料在交联后也能保持较好的铁电响应。”胡本林说，这种弹性铁电材料可以承受数千次的反复拉伸而铁电性依然保持稳定。它在受力后能够恢复原状，避免永久变形，大大提高了可靠性和使用寿命，拓展了使用范围。

《科学》期刊审稿人评价道，在铁电材料被发现后的百年历史中，和铁电陶瓷的不超过0.2%的拉伸应变到聚合物铁电材料小于2%的弹性回复相比，这是一个突破性工作，开辟了全新的“弹性铁电”学科方向。

江耘