

中国首个量子程序设计平台发布，期望

软件不再成量子计算“软肋”

■本报记者 胡珉琦

虽然量子计算机距离成熟和大规模应用还有很长的路要走，但国际IT巨头们早已开始在量子软件领域布局，以争夺未来真正控制量子计算机的先机。

2019年末，中国科学院软件研究所（以下简称软件所）发布消息，由其自主研发的国内第一个较为完整的量子程序设计平台isQ正式上线。平台包括了量子程序设计、模拟、分析与验证等一系列工具。

经典计算时代，国内工业软件自主研发至今步履蹒跚，而经典计算时代，软件不能再成为中国量子计算的“软肋”。

“软”“硬”并重

与经典计算机无异，量子计算的实现不仅需要硬件，还要有软件、算法、应用，而软件又被看作是计算机的“灵魂”。

不过，由于量子系统与经典世界相比有许多截然不同的特征，经典的软件理论、方法和技术在很大程度上不能直接适用于量子软件。因此，量子软件的开发复杂且困难。

早在十几年前，软件所研究员、学术副校长应明生就意识到，量子软件的理论和方法是一个极富挑战性的课题。他领导的团队在这十几年中已经研究了一整套量子程序设计、纠错、验证的相关理论。

只是，量子计算机尚未实现，研究量子软件是否为时尚早？就在大部分传统计算机科学家还在观望时，国外一些有远见的学术机构，以及微软、谷歌、IBM等IT巨头已经开始对量子操作系统和量子软件进行布局，甚至展开了在量子软件方向的人才竞争。

2011年左右，微软建立了从事量子算法、量子软件研究的QuArC团队。2017年年底，该团队发布了为驾驭规模化量子计算机而专门优化的新的编程语言“Q#”，协助开发者编写量子程序。同时发布的还有一款模拟器，供程序员在传统计算机上运行量子软件测试。

2019年5月，微软和谷歌还联合推出了一门在线互动课程《量子计算机编程》，初学者可以通过网页进行量子算法的模拟，并验证自己的模拟和编程是否正确。

这些IT巨头的长期目标，就是创造一整套软件来运行和控制量子计算机，并建立行业标准。

软件所量子软件团队副研究员应圣钢告诉《中国科学报》，“在经典计算时代，



“在量子程序设计方面，isQ平台包含的编译器能首先将高级语言编写的量子程序转化为指令集语言，从而对接不同的量子硬件，这一切工具的基础。”

我们不少工业软件开发的核心技术至今被人卡着“脖子”，到了量子计算时代，不该再重蹈覆辙。”

理论优势工程化

2018年12月4日，美国国家科学、工程与医学院发布的《量子计算：发展与前景研究报告》提到，量子软件的组成，包括能够让程序员描述量子计算算法的编程语言、分析它们并将其映射到量子硬件的编译器，以及可在特定量子硬件上实

现分析、优化、调试和测试程序的其他软件支持，例如，需要仿真和调试工具来调试软硬件、需要优化工具来帮助高效实现算法、需要验证工具来帮助确保软硬件的正确性。

此次，软件所团队与合作者在不使用任何国外量子程序设计开源软件的前提下，自主研发了集程序设计、测试、分析、验证于一体的工具平台。目前，已经上线

的功能主要包括编译器、模拟器、模型检测工具、定理证明器四部分。

应圣钢介绍说，isQ平台最大的特点

是把理论研究的优势工程化。团队在程

序设计与验证理论研究方面有长达十几年

的积累，提出了量子程序设计的新模型，

建立了量子程序设计逻辑基础，发现了量

子程序分析新算法等。“这是目前国际上

量子软件开发企业很少能做到的。”

在量子程序设计方面，isQ平台包含

的编译器首先能将高级语言编写的量子

程序转化为指令集语言，从而对接不同

的量子硬件，这一切工具的基础。

“其他编译器大多只能编译没有

while循环的顺序量子程序，我们的编译

器可以处理量子while循环、递归量子程

序，后续还将基于理论研究成果支持并行

量子程序，甚至还能验证编译器的正确性。”应圣钢说。

此外，量子程序和传统计算机程序相

比具有很大的不同，特别是由于量子叠加

和纠缠的存在，量子程序设计员可能更容易犯错，设计量子程序的调试和验证技术是推动量子计算发展的一项具有根本性挑战的基本要求。而量子程序验证研究的一个主要方向是发展适用于量子计算的程序逻辑。

应圣钢表示，团队设计的定理证明器基于量子Hoare逻辑，可以辅助量子程序设计、纠错，还可扩展用于量子密码协议验证。“这也让isQ成为了目前世界上首个能够对量子程序是否正确进行验证的平台，并且在经典计算机上克服了计算时间与存储空间的限制，为较大规模量子程序的设计提供帮助。”

接下来，软件所量子软件团队会进一步完善isQ平台的功能，包括定理证明器与编译器的对接等。团队也希望与国内量子硬件团队紧密合作，尽快将这一平台配置在国内自主研制的量子计算机上。

人才培养是初衷

应明生曾说，中国正在大力提倡原始创新，而原始创新只有在新领域机会才更多。量子程序恰好是一个正在兴起的新领域，希望有更多的年轻人参与研究。

中国需要自己培养人才。而对于量子计算这种前瞻性的领域，需要长期的投入和布局。应圣钢认为，关键不是讨论现在的技术能在什么时候直接创造经济收入，而是要培养并储备一批能够开发量子程序的人才，为未来的机遇与挑战作准备。

这也是isQ平台建设的初衷。

应圣钢认为，目前，量子软件人才培养的困境，主要在于既懂数学又会大规模编程的学生十分稀缺。会编写大规模程序的，数学基础往往不够好；数学系毕业的，大多数不会大规模编程；而两者都具备的学生，又很少有意愿从事量子软件开发，以至于团队目前只能自己培养研究人员。

前些年，由于行业发展周期影响，团

队每一年甚至每两年才能招到一个博士生。这也让软件所团队下决心，要借助平

台建设跨学科学科人才的培养和储备。

尽管目前这个领域论文产出难，成长

周期长、回报慢，博士生甚至会为“能否按

时毕业”而发愁，但在应圣钢看来，“量子

软件，志在未来”。

学术经纬

目前，车联网已成为物联网在智能交通领域的重要支撑。作为车联网的主体，汽车内外部需要部署大量传感器等信息处理装置。随着各种部件/组件实现互联、设备种类和数量增多，内生安全问题也逐渐增多，车联网安全问题日益凸显。

除设计功能外，一个技术系统总存在隐藏功能或漏洞，例如设计脆弱性导致的漏洞、未向用户声明过的隐藏功能，我们将其称之为“未知安全威胁”。

如何应对或防御基于目标系统的未知安全威胁？这是网络安全空间安全的一大难题。车联网是网络空间的一部分，因此这也是车联网的难题。

新型安全挑战

车联网产业链较长，涵盖元器件供应商、设备生产商、软硬件技术提供商等，其网络安全问题涉及到体系架构的各个方面。

应用层是车联网数据汇聚与远程管控的核心，从安全防护角度看，应重点关注车联网云端系统的控制接口、Web访问接口、账户口令、数据保护等问题，现有的主要防护手段包括入侵检测、防火墙、数据隔离、数据加密、身份管理等。

网络层是车与服务平台之间的信息通信通道，从安全防护角度看，应重点关注车内网络、车际网络和车载移动互联网等安全，现有的主要防护手段包括身份认证、访问控制、流量检测、通信加密等。

感知层网络是实现车辆内部各设备交互的特殊无线传感器网络，从安全防护来看，应重点关注芯片安全、终端系统安全和车载应用软件安全等，现有的主要防护手段包括安全启动、硬件加密、应用加密、通信隔离等。

本质上，现有的防护手段是依托既有的防御技术减少黑客对车联网的安全威胁，但传统互联网附加式安全体制和技术方法本身就存在体制机制缺陷，无法保证防火墙、身份证件等附加型或外挂式软硬件防护设施的安全性，难以有效应对基于软硬件的未知安全威胁。

对于新型安全威胁，传统防御几乎没有任何可信可靠的应对措施。如果这些问题不解决，车联网没有未来。

安全问题如何解决

如果目标对象内部既存在某些传统类型的不确定扰动因素，也存在针对系统软硬件漏洞的未知攻击，我们将称之为广义不确定扰动。如果一种鲁棒控制构造既能在某些传统类型的不确定因素扰动下保持给定功能或性能在设计余度内，也能在基于系统内部漏洞后门等“暗功能”的不确定攻击作用下维持给定功能或性能，即可称之为内生安全功能，对应的体系构造可称之为广义鲁棒控制构造。

2009年，笔者提出拟态防御理论解决内生安全问题。在不依赖先验知识条件下，管控隐藏功

车联网内生安全问题

■ 郭江兴



郭江兴 中国自动化学会供图

能引发的内生安全问题。笔者发现相对正确公理能将未知问题转换为有感差模/共模问题。笔者借鉴可靠性理论与自动控制理论，发明了动态异构冗余构造（又称拟态构造），通过导入拟态的嵌入机制增强防御迷雾，形成“测不准效应”，从机理上使试错或盲攻失能，用时空一致性形成防御壁垒。由此，功能安全与信息安全问题可在同一架构下一并解决。

简而言之，基于拟态防御理论的内生安全功能能在不依赖攻击者先验知识和行为特征情况下，将网络空间不确定安全威胁问题统一划为可靠性与鲁棒控制理论和技术能够解决的问题。

拟态防御理论和技术实践表明，内生安全功能能有效抵御任何利用目标系统内部已知、未知软硬件漏洞后门实施的安全威胁，从而在技术架构层面保证了车联网设施提供的服务功能，具有“高可靠、高可信、高可用”三位一体属性。

（作者系中国工程院院士，本报记者韩天琪采访整理）

速递

数字信息企业扎堆入驻张家湾设计小镇

本报讯

日前，由中关村管委会和北京通州区区政府联合打造的张家湾设计小镇正式开始运营，吸引了苍穹数码、华胜信息、终极科技等多家数字信息企业扎堆入驻。

企业扎堆入驻，有助于产业融合发展。“这么多优势企业在一起，也给了我们一个学习借鉴的机会。在今后的城市设计中，我们将借力这些企业的技术，推动城市设计的自动化、信息化、智能化。”

（郑金武）



会议现场

示，2020年~2025年期间，我国5G商用将直接带动经济总产出10.6万亿元，直接创造经济增加值3.3万亿元，间接带动经济总产出约24.8万亿元，创造直接就业岗位310万个。

“全球人口几乎都生活在移动通信世界中，移动经济支撑着数字经济的发展。”中国工程院院士邬贺铨估计，随着5G逐渐普及，预计到2025年中国将拥有4.3亿个5G连接，5G用户将达到我国移动用户数量的28%，占全球总量的1/3，成为全球最大的5G市场。

“5G的发展，将与数字经济形成价值环的关系。”北京大学光华管理学院教授武常岐认为，数字经济结合了供给侧调整和需求侧变化，目的是解决国防、农业、工业、金融等领域社会问题，进一步推动网络安全和政府治理；同时，5G通信技术和集成电路相关技术，也支撑了物联网、大数据、人工智能等技术。“5G与数字经济互为促进。”

“数据是新时代的‘石油’，是现在数字经济发展的内驱动力。没有数据，许多商业模式也就失去了存在价值。”北京互联网金融协会研究院院长易欢欢表示，5G的开放创新，带动效应十分明显。

根据中国信息通信研究院的测算显示

大类高品质工业品资源，入驻供应商190余家，上架商品1.7万种。该平台对工业品进行统一采购、交易、物流配送及售后服务，实现商品垂直化供应。

网络货运平台专注“互联网+物流”数字经济新模式，利用无车承运人、无船承运人资质，打造运输资源线上交流、交易平台。目前，已汇聚34

河钢上线铁铁工业品超市和网络货运平台

本报讯 近日，河钢钢铁工业品超市、网络货运平台在河北正式上线。两大平台的上线是河钢集团推动传统业务的产融结合与商业模式创新，以数字化技术驱动钢铁行业加快新旧动能转换的重要举措。

铁工业品超市将着力打造“门类齐全、性价优良”专业化工业品电商平台。目前，已汇聚34

构建5G生态尚需融合创新

当前，世界各国正在积极部署5G商用，加快推进全球5G产业化。

来自中国通信标准化协会的数据显示，截至2019年10月，全球109个国家的328家运营商宣布投资5G，69家运营商宣布已部署3GPP标准5G网络。随着2019年6月中国正式启动5G商用，全球目前已50家运营商正式提出5G应用和服务。

“5G加速与新兴技术融合创新，将构建全球新的生态。”中国通信标准化协会理事长奚国华指出，5G具备超高带宽、超低时延、超大连接移动接入能力，正与工业互联网、人工智能、大数据、云技术等新兴技术融合创新。

“随着工业互联网等新兴基础设施建设不断增强与完善，新技术、新业态、新模式、新生态等还将不断演进和升级。”奚国华说。

“从5G、6G再往后，还会有一些新的应用提出来，形成陆海空天的一体化通信，同时又会出现一批空间通信设备。”中国工程院院士余少华指出，未来5G、6G网络的应用场景将更加丰富，“5G可能会

AI融合应用要直面伦理挑战

我国人工智能技术在应用方面已在世界前列。

“要及时把握人工智能技术跃迁的机

会窗口，针对我国原创理论基础薄弱、重

大系统和平台缺失等突出问题，面向中长

期持续加强研发攻关。”中国工程院院士

高文说，应密切结合当前人工智能应

用的显著特征，依托我国在大数据、应

用场景、政策环境等方面的巨大优势，大

规模推动人工智能深度应用。

高文强调，应进一步健全人工智能国

家研发体系，全面提升人工智能持续创

新能力；大力培养聚集高端人才，形成人

工智能人才高地；加强人工智能法律理

论研究，引导人工智能安全可控发展。

人工智能伦理与规范是未来智能社

会的发展基石，已经引起了各国政府和

学术界、企业界等的广泛关注。欧盟、英

国、日本等国际组织和国家，均发布了人

工智能的伦理准则。

2019年5月，《人工智能北京共识》（以下简称《共识》）发布，针对人工智能的研发、使用、治理，提出了各参与方应该遵循的有

开放创新助推数字经济

“数据是新时代的‘石油’，是现在数

字经济发展的内驱动力。没有数据，许

多商业模式也就失去了存在价值。”北京

<p