编者按:

刚刚踏入 2018 年,信息技术产业领域就被“熔断”“幽灵”这两个几乎波及全行业的芯片漏洞所笼罩。孰料,该领域接下来上演的剧情——从美国断然发布对中兴通讯的出售禁令,到 Uber 无人驾驶汽车撞人致死导致业界对短期内实现无人驾驶的“梦断”;从谷歌幽魅般存在的超越最强经典计算机的 72 位量子计算机,到如幽灵般横空而出的“间谍芯片”……“熔断”和“幽灵”这两个关键词似乎主导着信息技术领域“断舍离”的戏码。

这一年,信息技术领域上演的“断舍离”

芯片漏洞 一石激起千层浪

1 月 3 日,谷歌零项目组(Project Zero)团队发表关于芯片漏洞的具体情况,熔断(Meltdown)和幽灵(Spectre)这两个波及全行业范围的芯片漏洞,给整个信息产业拉响警报。

随后,业内专家指出,由于两大漏洞“暴露的是最基本的问题”“是基于原理性的攻击”,熔断和幽灵对几乎所有计算设备和操作系统都有风险。

1 月 9 日,全球最大芯片厂商英特尔公司出面表示,测试结果表明,如果要给芯片安全漏洞打补丁,将会让使用其第八代“酷睿”处理器的电脑性能降低约 6%,但“这不会对一般用户产生太大影响”。不过,从各方反应来看,靠软件打补丁的办法只能“缓解”,并不能彻底解决问题。

“自主可控 CPU 的重要性”很快被摆在桌面上讨论,多年未起波澜的处理器微体系结构设计的命题再度引人关注,中国芯片厂商能否有机会挑战英特尔的霸主地位等话题也引人深思。

◎点评

上海高性能集成电路设计中心副主任田斌:

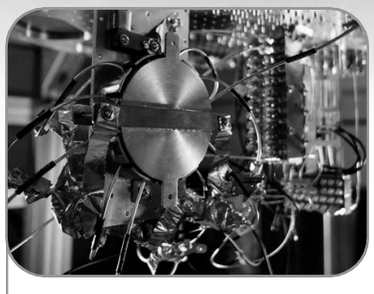
芯片巨头提供的 CPU 不在我们手里,研发团队也不在我们这边,建设防御漏洞的能力就是空谈。遇到类似 Spectre 的漏洞就只能等——什么时候更新补丁我们什么时候才能用,而且人家升级让你掏钱你也没办法。

天津飞腾信息技术有限公司战略规划部总经理张承义:

中国学术界和产业界都会对处理器微体系结构设计技术进行重新评估,加持了安全考量之后的新型微处理器设计技术研究或许会迎来一波研究热潮。

中国工程院院士、中科院计算所研究员倪光南:

中国要有自己的 CPU,应该放在网络信息安全体系框架下看待和发展。



谷歌发 72 比特量子计算机 BAT 纷纷布局

3 月 6 日,谷歌量子 AI 实验室研究科学家 Julian Kelly 在 Google Research 官博发文,介绍了其“经过同行评议”、最新 72 位量子比特通用计算机。消息一出,引发全球各大媒体转载。

随后,“谷歌实现‘量子霸权’”的话题甚嚣尘上。尽管一些媒体为其冠以“通用量子计算机”的称呼,但这并未得到量子计算领域专家的公允。并且,谷歌也未披露其“72 位量子比特通用计算机”的真身。

国内相关专家同时指出,现阶段我们应“清醒认识到国外的高速发展以及与其差距的扩大化”。

就在人们发问“谷歌研制了量子计算机,百度在干啥”之际,3 月 8 日,百度公司宣布成立量子计算研究所,并宣布由悉尼科技大学量子软件和信息中心创始主任段润尧出任所长,直接向百度总裁张亚勤汇报。

至此,BAT 三大互联网巨头全部在量子计算领域布局。然而,量子计算机的实现并非易事,在量子计算日益“热闹”的当下,专家们呼吁,量子计算现阶段应强调“合作”而非“竞争”。

◎点评

阿里巴巴阿里云首席量子技术科学家施尧耘:

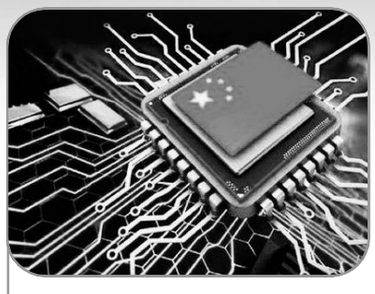
大规模的量子计算机还没有出现。但有意思的是,在它还没有出现的时候,影响就已经真实发生了。

腾讯量子实验室杰出科学家张胜誉:

量子霸权一词源于“quantum supremacy”,中文翻译“量子霸权”中的霸道意味有点误导,翻译成“量子优势”更确切一些。量子计算这个领域尚处于研发非常早期的阶段,应该多强调合作。

中科院量子信息重点实验室半导体量子芯片项目首席科学家郭国平:

量子计算机的研制、开发和应用是一个重大但同时又涉及多领域交叉的大事情,需要不同学科、不同产业方向间的融合与协作,合作互补非常关键。



中兴禁芯事件引行业大讨论 中兴之危 中国“芯”机?

4 月 16 日,美国商务部宣布将禁止美国企业向中兴通讯出售任何商品、技术和软件,且这一禁令长达 7 年,将这家来自中国的电信设备制造商置于万分凶险之地。

由于中国芯片高度依赖进口,尤其依赖美国,因此,美国此举虽然剑指中兴,其实是向整个中国集成电路产业“开刀”,以此牵制中国信息科技的发展。

中兴遭美全面禁售事件在计算机及集成电路行业内引发了尖锐的讨论。4 月 18 日晚,中国计算机学会青年计算机科技论坛(CCF YOCSEF)紧急召集特别论坛,主题就是“生存还是死亡,面对禁‘芯’,中国高技术产业怎么办?”

乐观者认为,这是中国集成电路产业痛定思痛、重整旗鼓再出发的契机;悲观者则看到中国集成电路产业底子薄、基础弱,面临严峻的人才短缺,并且各个因素之间形成的恶性循环短期难以改观。

历时近两个月,美国制裁中兴事件最终以“中兴认罚”14 亿美元、30 天内改组董事会和管理层及美方长达十年监管的惨重代价收场。

◎点评

中国工程院院士李国杰:

尽管目前国内已经可以生产一些芯片,包括以龙芯和海光为代表的通用 CPU,但国产芯片的制造水平与国外有两代以上差距,而且近几年差距并没有缩小。

北京交通大学计算机与信息技术学院副院长李浥东:

国内有多少高校在这个方向上有很强的人才培养课程体系和团队?有多少愿意做计算机体系结构的学生?没有学生愿意做这些事情,未来 10 年,我们的芯片靠谁开发?

浙江大学信息与电子工程学院教授储涛:

我们国家的科研经费虽然越来越多了,但是很少投到“应用基础研究”领域。中兴事件提醒我们,现在我们这块断裂了——起码是非常薄弱。

红芯浏览器“套壳” 真“可控”何必假“自主”

8 月 15 日,红芯时代公司宣布依靠“打破美国垄断,自主研发国产浏览器内核”的“红芯浏览器”完成 2.5 亿元的 C 轮融资。当晚,该公司被揭发其所谓的“自主研发”不过是对开源浏览器内核的包装和“套壳”而已。

8 月 16 日,红芯公司发布声明称,红芯浏览器内核是基于通用的浏览器内核架构,即 Chromium 开源项目,而非基于 Chrome 浏览器基础上进行技术创新。

这引发了超越计算机领域的又一轮关于“自主可控”的大讨论。迫于压力,8 月 17 日,红芯公司发表公开道歉并承认夸大宣传。红芯创始人兼 CEO 陈本峰在面对媒体时表示“我们在宣传上存在失误”,称之后会在措辞上进行改进。

业内专家随即指出,要判断一个网信产品或服务是否自主可控,往往涉及许多方面的问题,不是很容易做出结论。

正因如此,有关部门在推进国产自主可控替代中,正在实施“多维度测评”——除了实施常规的“质量测评”和“安全测评”外,还专门实施“自主可控测评”。

◎点评

中国工程院院士倪光南:

人们对“红芯”浏览器是否自主可控提出质疑,反映了大家对网络安全、对非传统安全有了更深的认识,这显然是一个进步,而并非孤立事件。在中国实现软件的自主可控,首先要建立一套评价软件自主可控与否的体系和制度。

中国科学院计算技术研究所研究员包云岗:

尽管中国软件行业的程序员和工程师数量堪称世界之最,却对世界开源社区的贡献寥寥。类似红芯强调的“站在巨人肩膀上创新”在我国的软件研发中很普遍,却最终难成巨人。

中国科学院计算技术研究所研究员张佩珩:

“自主”能够为实现“可控”打下良好基础,但“自主”并不是“可控”的充分必要条件。对于不同的行业和应用,“自主”与“可控”的权重并不相同。

彭博社 制造“间谍芯片”疑云

10 月 5 日起,一则“苹果、亚马逊被卷入,中国黑客利用微芯片入侵美国”的消息不胫而走,消息所波及的中美科技企业的股价应声下跌。而该消息的源头,来自于美国彭博新闻社一则题为“大黑客:中国如何用迷你芯片入侵美国公司”的封面新闻。

如果彭博新闻社的报道属实,这可能是有史以来公开报道的一个国家最大的硬件漏洞。

然而,作为这次所谓“间谍芯片”事件中首当其冲的公司,超微、苹果、亚马逊在该报道发出后迅速反应,发表清晰无误的声明否认有此事件,称彭博新闻社的报道是子虚乌有、无稽之谈。

10 月 6 日,美国国土安全部也发声声援上述企业,表示“没有理由怀疑苹果、亚马逊和超微否认此前彭博发布报道中的指控”。英国国家网络安全中心也“支持美国科技企业苹果和亚马逊对彭博新闻社报道的否认”。

10 月 9 日彭博社进一步指摘“黑客”在网卡接口处隐藏“间谍芯片”,但却没有拿出证据来证实这一点。

◎点评

天津飞腾信息技术有限公司某高级工程师:

感觉这是一个假新闻。如果这是真的,每年出口中国大量芯片的美国不是更有能力和条件来入侵中国 IT 设施吗?他们无非是想给本国禁售中国 IT 企业产品找点安全借口。

中国科学院计算技术研究所研究员韩银和:

“间谍芯片”事件提示我们,芯片安全不仅要重视“检”和“防”,更要重视“攻”,只有建立完整的“攻—检—防”技术体系,才能综合发挥作用。

360 集团技术总裁兼首席安全官谭晓生:

芯片的确是攻破安全屏障的一个进攻点,而且因为它在最底层,如果有预置后门或埋了木马,幕后操纵者可以“一层层地向上打”。网络安全领域有个理念是“零信任”,也就是追求全维度的分析检测,而这需要大量的存储、计算和分析,要舍得在安全上花钱。 **(本报记者赵广立整理)**

中国科学院数学与系统科学研究院 20 年:

“这里是数学的乐园”

■本报记者 沈春蕾 见习记者 韩扬眉

“从陈景润关于哥德巴赫猜想的工作到田野关于同余数与椭圆曲线 BSD 猜想的工作,这些成果都是处于国际的前沿。”中国科学院院士杨乐说。

“这里是数学的乐园,它有着辉煌的历史、骄人的地位,目前正处于蓬勃发展的时期。”中国科学院院士席南华说。

“数学与交叉科学研究意义深远、责任重大、使命光荣。促进数学与系统科学为国家服务,责任所在、力所能及。”中国科学院院士郭雷说。

“数学已成为我生命的一部分,作为科研人员,能找到自己热爱的职业、从事感兴趣的研究,是很幸福的一件事。”中国科学院院士袁亚湘说。

2018 年 12 月是中国科学院数学与系统科学研究院(以下简称数学院)成立 20 周年的日子。20 年前,为应对国际国内数学界面临的新形势,原中科院数学研究所、应用数学研究所、系统科学研究所、计算数学与科学工程计算研究所四所合并,成立数学院。

强强联合,实现了学科齐全、资源共享、人才聚集,科研实力有了跨越式的飞跃。从突破代数与数论、几何与拓扑等纯粹数学中的重大难题,到开创国内控制数学、计算数学与运筹学等新领域,再到解决金融和高科技中数学建模的关键问题……

在 2017 年接受国际评估时,由九位著名数学家(其中六位是欧美科学院院士)组成的专家组给出的评价是:“世界一流数学与数学科学中心之一”“在基础数学、应用数学与数学交叉方面都具有高水平的研究人员”“带动中国其他数学机构发展的火车头”。

“最高国际水准的纯数学”

九层之台,起于垒土。

作为数学科学研究的“国家队”,数学院既在中国数学科学崛起中发挥着不可替代的奠基性和引领作用,也是国际上一个重要的数学科学研究中心。

时光追溯到 66 年前,由华罗庚担任首任所长的中科院数学所成立,确立了纯粹数学与应用数学协同发展的方针,开启了国内数学科学研究的新时代。

数十年来,数学院在数学重大基础前沿问题的研究中,形成了优良的传统与坚实的研究基础。华罗庚的“典型域上的多元复变数函数论”开辟了一个重要研究领域;吴文俊的“吴示性类”和“吴示嵌类”成为拓扑学领域影响深远的经典成果;陈景润和王元的“哥德巴赫猜想研究”至今仍保持国际领先水平……

沿着前辈的足迹,数学院一大批杰出的中青年数学家继续攀登着数学高峰。席南华对仿射 A 型 Weyl 群证明了 Lusztig 关于基环的猜想,成为国际上很多后续工作的基础之一;周向宇带领研究生解决了多复变中的“经典问题”最优 L2 延拓问题、证明了 Demailly 强开性猜想,在美国《数学评论》上被评论为“近年来多复变与代数几何领域最伟大的成就之一”;“新生代”数学家田野首次给出 7 个千禧数学问题之一“椭圆曲线 BSD 猜想”的重要线索;人称“论证骑士”的孙斌勇与李文威对朗兰兹纲领一系列重要问题的探索,以及青年学者黄飞敏在玻尔兹曼方程的流体力学方面,都取得了重要的突破。

数学院在多领域形成的“最强研究群体”在国际数学界有着重要影响力,他们长期关注着朗兰兹纲领、BSD 猜想、黎曼猜想、素数分布、纳维—斯托克斯方程、希尔伯特第 6 问题、希尔伯特第 15 问题、双曲猜想等基础数学中的“未解之谜”。

数学院在基础数学研究中取得的成果,被国际同行所公认。最让人惊喜的是,数学院这种重大的研究成果还在以更强劲的势头涌现。

“应用数学界的‘中国学派’”

“数学院在纯数学和应用数学领域都做出了大量具有最高国际水准的研究工作。”

“数学院几乎是国际上唯一一个在纯数学和应用数学如此众多的方向上开展研究,且做出高质量工作的研究机构。”

这是在 2012 年中科院组织的国际评估中,多位国际著名数学家组成的评估组对数学院的评价。

理论“顶天”、应用“立地”。除了解决古老的数学难题,数学院在探索数学如何更好地服务社会发展、人民生活的过程中,不断开拓新的研究方向和领域。

控制科学研究诞生于此。上世纪 60 年代,航空航天事业的发展催生了现代控制理论的研究热潮,钱学森先生倡议在数学院组建了中国第一个专门从事现代控制理论研究的机构——控制理论研究室,中国现代控制理论开拓者和奠基人关肇直担任首任室主任。获得 1985 年国家科技进步特等奖的“尖兵一号返回型卫星和东方红一号”项目中,关肇直负责该项目的轨道设计和轨道测定两个子项目。

郭雷首次提出定量研究反馈机制最大能力的理论框架,发现并证明了反馈机制最大能力的“临界值”和“不可能性定理”等一系列基本结果,被认为他是“一项具有深远意义的根本性研究”。2014 年在三年一度的国际自动控制联合会(IFAC)世界大会上作大会报告(Plenary Lecture),是 IFAC 半个多世纪历史上,应邀作大会报告的唯一大陆学者。

该系统控制团队近年来提出非线性不确定系统的控制新方法,突破了复杂环境下飞行器控制的关键科学问题;完善布尔网络控制理论,助力揭开疾病病理等生命奥秘……数学院在复杂系统与控制科学的关键问题上捷报频传,年富力强的学者在国际舞台上脱颖而出,形成“中国学派”,在国际学术界具有重要学术地位。

数学院也是我国计算数学与运筹学的发源地,建有我国数学领域唯一一个国家重点实验室“科学与工程计算国家重点实验室”。在这里,冯康等老一辈数学家开创了我国的计算数学研究。冯康独立于西方创始了有限元方法,在国际上首次提出基于辛几何原理计算哈密尔顿体系的新方法,后被广泛应用到物理等科学领域,获得 1997 年国家自然科学奖一等奖。

之后石钟慈、林群、崔俊芝、袁亚湘、陈志明等在有限元边界元的新型算法、非线性优化、复杂系统的电磁问题计算、材料物性的多物理多尺度计算等方面取得突破性进展,解决了一批航天航空、核能工程、石油勘探、水利建筑交通运输等领域的重大计算难题。这一团队已经成为我国计算数学实至名归的国家队。

其中,袁亚湘等最早使用子空间技术分析计算方法,相继提出了子空间共轭梯度法、非线性优化子空间法与子空间拟牛顿法等方法。该方法被称为 Dai-Yuan 方法,并且与 FR 方法、HS 方法、PRP 方法并列,被认为是“四个主要方法”。该成果 2014 年获得“发展中国家科学院数学奖”。

陈志明提出了自适应有限元方法收敛性分析的全误差估计技巧,已成为自适应有限元方法收敛性分析的常用方法;提出了自适应 PML 方法,解决了 PML 方法在实际应用中的参数选取问题与指数收敛性,得到层状介质无界区域计算的第一个严格理论结果,获国家自然科学奖二等奖。

三维不可压缩 Navier-Stokes 方程整体光滑解是 7 大千禧年问题之一。Boltzmann 方程的流体力学极限是 Hilbert 第六问题的重要内容之一。张平和黄飞敏团队证明了各向异性不可压缩 Navier-Stokes 方程整体适定性;证明了在黎曼解这一重要情形下 Boltzmann 方程的极限是可压缩 Euler 方程。此成果获 2011 年、2013 年国家自然科学二等奖。

华罗庚曾不止一次提出,中国数学未来的发展应包括纯粹数学、应用数学和计算技术三部分。20 年来,数学院始终面向国家需求,瞄准科学与工程发展的重大应用难题,站在数学学科发展的“潮头”,乘风破浪辟新路。

“交叉融合‘最强战队’”

数学的触角几乎伸向一切领域。当前数学学科的发展趋势不仅需要数学各分支的融汇,更需要与其它科学进行深度融合。

数学院是国内乃至世界上数学分支最齐全的研究机构,涵盖了几乎所有数学学科,在基础数学与应用数学的大部分重要分支都有很强的队伍,具有从事交叉融合、协同创新的坚实基础。2010 年,国家数学与交叉科学中心正式成立,这是中科院实施“创新 2020”启动的第一个科学中心。

基于在众多学科上具有高水平团队和研究平台,数学院不同学科交叉融合形成“最强战队”,共同研究跨学科的重大难题,并由此培育了系统科学、数据科学、金融数学、系统生物学、计算材料学、复杂网络、密码学、知识科学、管理科学、质量科学、量子信息等数学前沿交叉学科。

随着计算机科学的发展,数学院在计算机数学这一新兴交叉领域的成果全球瞩目。吴文俊在数学机械化方面的开创性成果,获得“自动推理国际最高奖”“首届国家最高科学技术奖”和“邵逸夫数学奖”。近年来,一批中青年骨干在机器证明、密码方面取得重要成果,获得了“国家自然科学奖二等奖”与“国家发明二等奖”,被称作符号与代数计算方面“国际上最强的研究群体之一”。

稀疏结式是代数几何基本概念与计算理论强大工具。高小山团队建立了微分 Chow 形式理论与微分稀疏结式的理论,给出了高效算法。此成果获国际计算机学会 2011 年唯一“ISSAC 最佳论文奖”。

陈锡康与杨翠红团队首次提出用国内增加值测量两国贸易新思想,成为国际贸易失衡的一个新测算标准方法,2011 年 WTO 在全球范围内力推以增加值为基础的贸易测算;2014 年 APEC 批准了《全球价值链中的 APEC 贸易增加值核算战略框架》。

另外,汪寿阳团队在区间计量经济模型建立了一个新的方向——区间数据建模理论与分析方法,开发了“国际收支风险监测预警和决策支持系统”,自 2016 年投入运行,有力支撑了国家外汇管理局的科学决策。

数学院通过各个学科的交叉融合,形成了综合实力强、在国内领先、在国际上有重要影响的若干研究团队,现已承担了 8 个基金委创新群体项目。

“无论是现在,还是将来,数学院这个研究机构的地位决定了我们只关心最核心的问题、最主流的方向。”数学院负责人告诉《中国科学报》。

20 岁的“桃李年华”,数学院正怀揣着新的目标与希望走向活力无限的未来。