

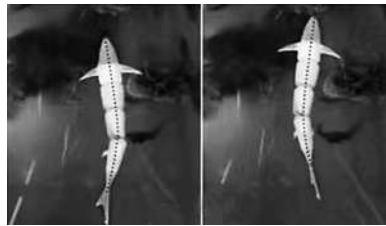


科技云

科技连着你我他

■本期观察:武郁琦 邱阳 毛英椿

软体机器鱼



中国科学院沈阳自动化研究所机器人研究室微纳米团队,近期研发出一款新型仿生软体机器鱼。该成果以鱼类生物学特征为设计基础,通过融合驱动感知一体化技术,实现了水下机器人的多模态运动控制。

自然界鱼类经过长期进化形成了独特的生物力学系统:其侧线器官具备环境感知功能,肌肉系统可实现精确动力输出。研究团队受此启发,开发了一种整合仿生人工肌肉驱动与感知功能的多模态软体机器鱼设计方案。该装置以鲦鱼为生物原型,采用三维打印工艺构建仿生脊柱结构,运用弹性压缩弹簧模拟椎体支撑,并通过层叠式柔性薄膜复现肌肉组织的动力传导特性。

相较于传统软体水下机器人,该成果在三个维度实现技术突破:首次完成驱动—感知—控制系统的功能集成;具备更丰富的运动模态数据库;拥有环境自适应决策能力。这些创新显著提升了水下仿生设备的运动效率与工况适应性。

微型医疗机器人

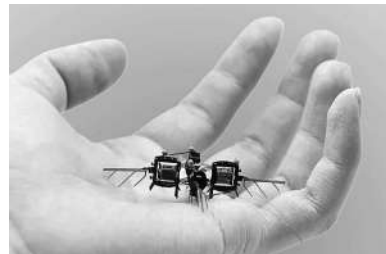


前不久,香港科技大学研究团队成功研制出一种用于介入诊断和治疗的微型医疗机器人。该机器人以0.95毫米的超微直径刷新世界纪录,较现有同类医疗机器人尺寸缩小近六成,攻克了精密器械领域长期存在的“功能集成、操作精度、微型化”三重矛盾难题。

这款医疗设备集高清成像、精准操控与微创介入3项核心功能于一体。其搭载的新型光学系统将障碍物探测距离扩展至9.4毫米,较传统理论极限提升10倍,成像覆盖范围更是突破传统影像受限约25倍。

该科研团队负责人表示,该机器人目前已在冠状动脉支架植入、消化道溃疡精准切除等手术场景完成技术验证,未来将重点拓展其在肿瘤早期诊断、神经介入治疗等领域的应用。

仿昆虫飞行机器人



最近,基于节肢动物生物力学原理,美国麻省理工学院一研究团队成功开发出一款仿昆虫飞行机器人。该仿生机器人系统采用与常规邮票贴片相仿的微型化体积设计,不仅实现了15分钟的持续滞空时长,更展现出优异的机动性能,可完成三维空间内的多轴旋转动作,相关研究成果已发表于《科学·机器人》学术期刊。

该研究团队指出,微型飞行装置需在低质量与高结构强度间取得平衡,常规设计中空气动力载荷常导致微机械结构在20秒内发生结构性失效,这使得科研人员难以获取足量实验数据优化飞行控制系统的参数。测试数据显示,新型仿生装置通过创新性的结构设计,将关节部位应力载荷降低至传统设计的1%。

研发人员称,该飞行器还采用模块化关节连接系统,实现结构性能突破。这种创新架构不仅使飞行器具备连续15分钟的稳定悬停能力,还赋予其完成前向/后向复合滚转动作的特技飞行功能。

从古今,秘密信息的守护与共享,始终受到人类重视。

商末周初,古人采用“阴书”传递军事领域的情报信息——他们将信息完整地刻画在竹简上,再将竹简拆分,随后委派多名信使分别传递竹简的不同部分,君主收到全部竹简后再将其拼合起来,即可得到完整的情报。这在一定程度上防止了情报信息被敌方军队窃取,是我国古代重要的保密手段。

当历史演进至20世纪末,一种更为安全的信息共享方式——安全多方计算,开始应运而生。

作为一种密码协议,安全多方计算可以在不泄露私有数据的情形下,实现多个

参与方共同完成某项计算任务,主要用于隐私保护场景下的协同数据分析、联合建模和敏感信息查询等方面。

据新华社报道,2025年1月1日起,我国《网络安全管理条例》正式施行,其中关于安全多方计算的规定,标志其在中国已成为保证数据安全流通的重要方式之一。

以数学命题破解安全难题,放眼世界,安全多方计算技术呈快速发展之势,正在建构起金融风控、医疗协作乃至军事联动的安全防护网,成为数据时代保证信息安全共享的“信任引擎”。

安全多方计算——

以数学命题破解安全难题

■杨伊叶清 张佳豪



图为去中心化网络中,多个发光节点通过加密链路直接交互,协同处理数据,无需依赖第三方信任机构。

作者供图



高技术前沿

借助多种密码学组件实现信息安全共享

安全多方计算技术的核心优势,在于该技术能有效实现“数据可用而不可见”。

以在医疗行业中的应用为例。安全多方计算技术能够在不暴露患者敏感信息的前提下,实现联合分析多机构间的匿名化数据,帮助医务工作者推进医学研究和临床试验,进而为患者提供个性化医疗和健康管理方案。

换句话说,安全多方计算技术的核心是设计一种特殊的加密算法和协议,从而实现利用加密数据直接进行计算,获得计算结果,同时用户不知道数据明文内容。

支持安全多方计算技术实现信息安全共享的核心运转齿轮,是秘密共享、不经意传输、同态加密等密码学组件。这些组件好似用数学打造的安全防线,各自发挥着特有功效,为数据共享构建起坚实的信任支柱,让“数据可用而不可见”从理想变为现实。

——秘密共享。

秘密共享密码学组件的核心特性,是把原始秘密拆成若干个片段(份额),而这些片段在单独留存时没有意义。

该密码学组件能构造出一个特殊多项式,原始秘密就隐匿在这个多项式的某一特定位置。每个片段对应这个多项式在不同位置的数值,只有集齐规定数量的片段,用户才能借助计算还原出完整的多项式,最终得到原始信息;若片段数量未达标,使用者就无法将原始信息拼凑出来。可以看出,通过分散存储的方式,秘密共享密码学组件降低了秘密泄露的风险。

——不经意传输。

不经意传输密码学组件,就像一种隐私性极强的“通信方式”。当发送方向外传递出若干条信息,接收方只能从中选一条获取接收。在传递信息过程

中,发送方无法知道接收方选了哪一条信息,同时,接收方也不能获知发送方拥有的其他信息,只能解密自己选中的那条信息,最终获取的完整信息需要依靠特定协议实现。

——同态加密。

这种密码学组件的关键作用,是保证解密后的计算结果与直接对原始信息进行计算的结果相同,实现了数据处理阶段的隐私保护。该组件通过设计特殊的加密方式,使密文内容也能进行数学运算。这些数学运算包括多种类型,如仅支持加法、仅支持乘法、同时支持多种运算等。

借助多种密码学组件,安全多方计算技术能使参与方之间实现数据协同计算,同时满足挖掘数据价值与保护数

据隐私两种刚性需求。

从“百万富翁问题”到安全多方计算技术

关于安全多方计算技术研究的开端,最早可以追溯到1982年。

当时,我国姚期智院士提出了“百万富翁问题”,即两个富翁想要比较谁更加富有,但都不愿将具体的财产数额透露给彼此。最终,他们通过构造特殊的联合建模效率较低,在一定程度上限制了该技术大范围应用;另一方面,安全多方计算技术的处理对象往往是敏感的数据资产,试错成本较高,增加了用户的接受成本。

也正是从这时开始,隐私计算的帷幕正式拉开。

1987年,米卡利、戈德雷奇和威格德森3位密码学家提出了GMW协议,该协议首次提高了安全多方计算的通用性能。本质上,该协议是将计算任务转化为一种加密逻辑电路,参与者只能凭借持有的密钥片段进行本地运算。这如同多人共同看管一个带有多个密码的密码箱,每人持有一个密码钥匙,只有集齐所有人的钥匙才能开启密码箱。

此后数十年间,安全多方计算技术发展迅速:2018年,Dover微系统公司发布了CoreGuard芯片,该芯片能每秒进行百万次隐私计算;2022年,我国一家企业推出了一款隐私计算平台,该平台能把亿级金融数据的处理时延控制在

50毫秒以内。

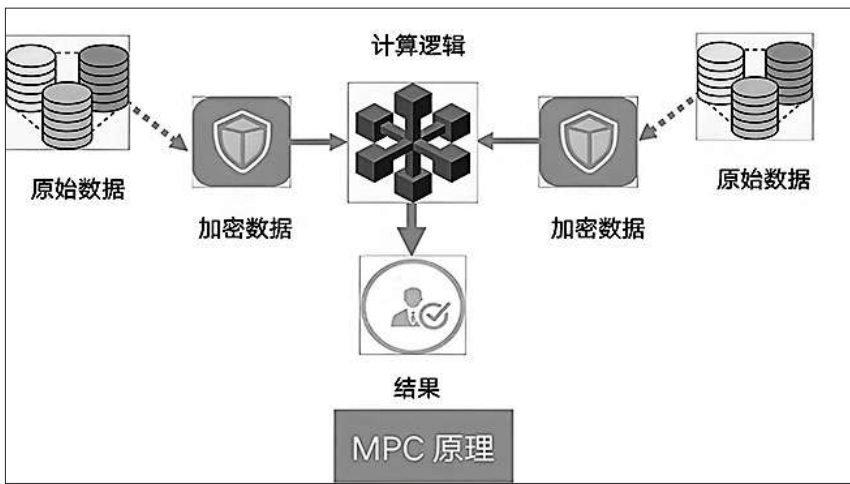
此外,中国人民银行、中国信通院、中国电子标准研究院等机构分别开展了安全多方计算相关标准的研究与探索,发布了《多方安全计算金融应用技术规范》《基于多方安全计算的数据流通产品技术要求和测试方法》《区块链隐私计算服务指南》等一系列标准与规范,大大降低了数据泄露风险。

不过,目前安全多方计算技术的发展也面临一定挑战。一方面,由于安全多方计算技术的加密机理复杂,在大规模数据和复杂计算场景下,当流通的数据量较大或结构较为复杂时,复杂算法的联合建模效率较低,在一定程度上限制了该技术大范围应用;另一方面,安全多方计算技术的处理对象往往是敏感的数据资产,试错成本较高,增加了用户的接受成本。

43年前,当姚期智院士提出“百万富翁问题”,进而点燃安全多方计算的星火时,也许没料到如今会发展为保证数据安全共享的重要技术,帮助人们在大数据的洪流中构建起安全信任的屏障。

构建未来战场上的“数据同盟”

情报安全,对军事行动的重要性不言而喻。目前,世界上已有多个国家将安全多方计算技术应用于跨军种通信



安全多方计算数据流转过程。

作者供图

轻量化材料的前世今生

■于童 陈尚庚

在今年7月召开的亚洲汽车轻量化展览会上,厚度仅0.8毫米的碳纤维构件与可再生复合材料等轻量化材料的亮相,引起了人们的关注。

从最初为了满足航空航天领域减轻飞行器重量的迫切需求,到在汽车、建筑、电子等众多行业的普及,轻量化材料正广泛影响着人们的生活。

轻量化的理念早已有之。几千年前,古埃及人建造金字塔时,将石灰、火山灰等作为黏合剂与砂石混合,形成了原始的颗粒增强复合材料;在西安半坡遗址中,工作人员发现了草拌

泥墙壁砖坯,这是古人利用植物纤维增强泥土强度的早期实践……这些质朴的尝试,被视为轻量化材料的雏形和前身。

最早的轻量化金属材料可以追溯到1906年。当时,冶金工程师阿尔弗雷德·维尔姆在研究铝—铜—镁—锰合金时,意外发现了淬火后的合金硬度随时间增加而增大的“时效强化”现象。

基于此,他在1909年成功研制出首种可热处理强化的铝合金“杜拉铝”,即硬铝。该材料的强度远超纯铝,后来成为最早应用于航空领域的

轻量化金属材料。

在此后很长一段时间内,铝合金成为航空、军工领域的关键材料。凭借质量轻、强度高、耐腐蚀等特点,该材料被广泛应用于大型客机的机翼、机身等关键部位。

人类对轻量化材料性能的持续探索,也催生出了新型轻量化组合物材料。

1942年,玻璃纤维增强聚酯树脂复合材料问世,即人们俗称的玻璃钢。玻璃钢密度低于金属,且具有绝缘、耐腐蚀等特性,研发初期主要应用于雷达罩和船体制造等。

1963年,世界上不少国家实现了碳纤维的工业化生产。碳纤维性能优越,强度是钢的5倍,密度仅为钢的1/4,早期因成本高昂,主要应用于航天等尖端领域。

20世纪70至90年代,芳纶纤维(凯夫拉)和碳化硅纤维等新型纤维材料问世,进一步丰富了复合材料的种类。芳纶纤维凭借出色的抗冲击性,被广泛应用于制作防弹衣和轮胎等产品。

随着技术不断进步,进入21世纪后,轻量化材料在各个领域受到越来越多的重视:在航空领域,飞机机身、



科学的历程