从古至今,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《网络数据安全管理条例》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



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

原始数据

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

加密数据

安全多方计算数据流转过程。



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

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。

计算逻辑

结果

MPC 原理

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

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

加密数据

原始数据

作者供图

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 的交互协议,解决了这一问题,使双方 能够在不泄露任何资产信息的情况下, 比较出谁更加富有。

也正是从这时开始,隐私计算的帷

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 自密码箱。

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 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

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 身份认证等作战环节,以避免传统密钥 共享时的安全风险。具体来看,安全多 方计算技术在军事领域至少具有如下 应用前景。

一安全传输情报。

试想这样一个画面,某指挥中心警 报骤响,某海域突现不明舰队,一场无 声的博弈在指挥员面前展开。想要精 准研判对方的威胁等级,必须尽快整合 陆、海、空各方电子干扰频率等关键情 报数据。借助安全多方计算,关键情报 数据可实现安全共享传递: 先将核心数 据拆成"碎片",随后将这些"碎片"打乱 并分发,形成"你持几片、我握几个"的 混合状态,最后依托协同计算机制,将 手中碎片完成联合运算,就能在绝对安 全的情况下,精准算出指挥员需要的情 报数据。整个过程如同将数据锁进"数 学黑箱",实现信息安全共享。

——核查可疑坐标。

假设在未来战场上遇到这样一种 情况,一艘舰艇的声呐突响报警:水下 300米发现可疑目标。是敌方潜艇? 还是海洋生物?此时,指挥员可借助 安全多方计算技术,将反潜数据封装 成100个"加密漂流瓶",每个瓶子对应 不同海域的防御信息,瓶身被"锁死", 连封装方自己也无法拆解。随后将可 疑坐标加密成"磁性鱼钩",悄然投入 "漂流瓶"群中——这把"鱼钩"带有特 殊"磁力",仅能吸起与目标坐标匹配 的那个瓶子。最后,被吸中的瓶子自 动解密,但仅反馈一个关键信息:"该 坐标是否存在威胁?"整个过程如同深 海中的"魔术戏法"——封装方看不见 哪只瓶子被打开,数据在"无形之手" 中安全流转。

——火力协同优化。

假设在某联合行动中,各参与方共 同执行对某目标的拦截任务。如何能 在完成任务的基础上,保证各方火力覆 盖、目标探测等核心能力不被泄露?借 助安全多方计算技术就可以实现:首 先,参与方将自己的弹药储备量数据等 加密为密文;随后,系统基于拦截算法, 对加密后的弹药数据进行协同运算(如 关联分析、阈值判断等), 在数据完全隐 身的状态下推导演绎,生成代表最优拦 截方案的新密文。整个过程如同各方 在"数据隐舱"中协作——原始数据始 终隐匿,仅通过加密后的"影子"完成推 演,最终仅输出关键结论。

通过安全多方计算技术,未来战 场上的精准作战决策与严格保密要求 便不再是对立选项,而是共同构建起 更具韧性的联合作战体系——既避免 了关键信息的暴露风险,又确保了协 同效率的最大化,为复杂战场环境下 的信息传输、火力调配等提供更灵活 的安全解法。

我们看到,当数据逐渐成为21世 纪的重要战略资源,一场信任革命正 在算法深处涌动。安全多方计算技 术把人类协作时遇到的安全难题转 化为可验证的数学命题,正在重构组 织间的可信协同、个体间的隐私边 界,也在为人类数字文明的进步打造 "信任引擎"。

机翼等部位使用碳纤维等轻量化复合 材料,相比其他金属材料大大减轻了 重量,帮助飞机提高燃油效率;在汽车 领域,聚碳酸酯等轻量化材料因成本 低、重量轻、可塑性强,常用于车灯外 壳和仪表板等部位,广受欢迎;在建筑 领域,铝型材和钛合金构件正逐渐替 代部分钢材,在实现轻量化的同时保 证了相同的材料性能;在电子设备领 域,镁合金和铝合金轻量化外壳的广

实现轻薄化…… 可以这样说,轻量化材料的发展 史,也是人类不断追求材料性能进步的 历程。未来随着纳米技术、3D打印技 术等与轻量化材料技术不断融合,轻量 化材料或将在新能源、智能制造、生物 医疗等更多领域创造新的价值。

泛应用,助力笔记本电脑、手机等产品

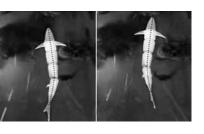




科 技 云 科技连着你我他

■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 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。该装置以鲭鱼为生物原型,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

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 破传统传像束限约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

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资贴片 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

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·维尔姆在研究铝一铜一镁一锰合金 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

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

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、