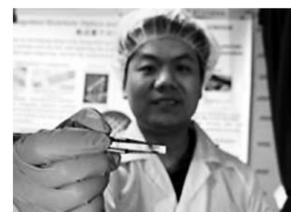


科技云

科技连着你我他

本期观察:张诗宏 李陈辉

集成光子芯片

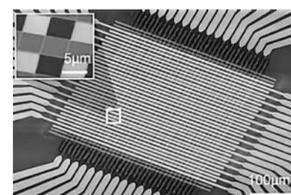


近期,山西大学联合北京大学研究团队,在集成光子芯片领域取得重要突破,成功实现全球首例基于集成光子芯片的“连续变量”量子纠缠态。相关研究成果已在《自然》期刊上发表。

据悉,传统离散变量光子芯片因量子纠缠成功率随比特数指数级下降,长期制约着大规模量子资源制备。研究团队创新采用连续变量技术路线,利用其确定性生产特性突破多比特纠缠操控瓶颈,为光子芯片的大规模扩展及其在量子计算、量子网络等领域的应用奠定了重要基础。

在技术实现方面,团队研发了超低损耗调控、多色相干泵浦等核心技术,通过双模光场压缩和非线性布拉格散射过程,成功制备出八频率模式纠缠态。为验证这一创新性能,研究团队专门构建协方差矩阵重构系统,实验数据表明,该芯片多模纠缠操控效率远超传统方案,展现出其在量子计算与通信领域的应用潜力。

神经形态半导体芯片

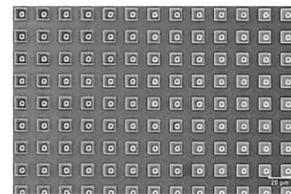


近期,韩国科学技术研究院团队开发了一款超小型计算芯片。该芯片能够实现自主学习和实时纠错功能,对人工智能硬件的小型化与高效化发展具有重要意义。这项突破性的研究成果已在《自然—电子学》杂志发表。

相较于传统数据处理,这款芯片基于忆阻器技术模拟人脑突触工作机制,首次实现数据存取与计算的同步处理。其并行运算特性使智能安防设备无需云端即可独立识别异常行为,处理速度较现有系统大大提升。

此外,该芯片创新地攻克了硬件误差动态修正难题。在实时图像处理测试中,系统可自主优化移动物体识别算法,其自适应学习准确率接近理想模型的98%。这标志着类脑计算系统正式迈入产业化应用阶段。

新型硅芯片



近期,哈佛大学科研团队在《自然—生物医学工程》杂志上发表了一项成果——某新型硅芯片。据悉,该芯片成功同步记录2000个大鼠神经元7万余个突触连接强度,首次实现神经网络功能图谱的大规模解析。

这项创新通过微孔阵列向细胞膜注入微电流,以90%耦合率完成3600个神经元并行记录。其水平微孔设计较传统纳米针电极制造效率提升5倍,同时保持膜片钳级的信号保真度,可精准捕捉突触信号的强度特征波形。

研究团队指出,该技术突破了脑科学领域长期存在的“规模—精度”矛盾。通过量化突触连接强度差异,科学家可构建兼具结构与功能属性的神经网络图谱,为解析记忆编码等高级脑机制提供关键突破口。

研究团队正在开发三维堆叠芯片系统,计划将记录规模扩展至百万级突触。这项技术或推动神经进行性疾病研究与高精度脑机接口的跨越式发展。

光速引擎照亮智能未来

光互连技术的成熟与普及,其意义远不止解决当下数据中心面临的能耗和带宽危机。它为未来科技引擎注入了光速燃料,赋能前沿科技领域,或将开启智能世界的新篇章。

未来的6G网络,追求极致的速度、极低的延迟和万物智联。这要求承载海量数据的通信神经网络,包括连接基站和核心网的前传/中传网络,以及核心网内部的高速数据交换中心,必须具备前所未有的吞吐能力和响应速度。光互连技术,特别是更高速、更集成、更低功耗的硅光和CPO解决方案,将是构建这张未来高速智能通信网络的核心基石,支撑全息通信、沉浸式XR、远程精准控制等革命性应用。

量子计算机已成为各国的研究热点。量子计算机的巨大潜力,在于其天然的并行性。但要想真正解决意义重大的复杂问题,可能需要构建由多个量子处理单元连接而成的大规模量子系统。连接这些对环境扰动极端敏感的量子比特,需要近乎无噪声、无干扰、高保真度的信息传输链路。而基于单光子或纠缠光子操控的量子光互连技术,因其天然的弱测量特性和抗干扰能力,成为构建未来量子互联网和分布式量子计算网络最具前景的沟通桥梁。

在物理世界与数字世界深度融合的智能时代,每天有海量数据流淌在看不见的空间里。自动驾驶汽车上激光雷达每秒产生的数据、智慧城市中部署的无数环境监测传感器实时信息流、智能工厂里设备的毫秒级状态反馈、元宇宙中沉浸式体验所需的超高清流媒体和实时交互数据……这些海量、实时的感知信息,都需要在边缘侧和云端之间进行近乎瞬时的高速传输与处理。高速、可靠、低延迟的光互连网络,将成为支撑这些智能应用的感知神经和决策动脉。

光互连技术不仅是对物理极限的又一次革命性跨越,更是为即将到来的智能时代铺设了最关键的底层基础设施。从服务器机柜深处无声流淌的光信号,到未来连接量子比特的光子纽带,再到可能重塑计算架构的光电融合芯片,光互连技术正将我们引向一个算力无界、感知无限、万物智联的未来——在那里,信息的奔涌如同光本身一样,迅捷、高效、磅礴,并无限可能。

左上图:硅光引擎驱动下,光互连正在重塑数据中心。

资料图片

光互连:数据洪流的“光速运河”

王润鑫 本报特约记者 宋世杰



早在20世纪中后期,光纤通信在远距离通信领域的巨大成功,已经展现出光传输的巨大优势。相对于电传输,光传输具有超大带宽、超长距离、超强抗干扰能力等特点。

当时,想要把光引入更短距离,尤其是芯片和板卡级别的互连,却屡屡受挫。彼时的光器件体积庞大、制造成本高昂、功耗也不理想,与高度成熟、微型化、低成本的硅基集成电路工艺格格不入。在服务器和计算机内部使用光互连,被视为既不经济也不实用的选择。

真正的转折点出现在21世纪初。伴随着硅光子学技术的兴起与成熟,科学家和工程师们获得了一项革命性的认识:可以利用现有成熟的、用于制造电脑CPU和内存的半导体工艺,直接在硅晶圆上制造出纳米尺度的光波

导、调制器、探测器,甚至通过异质集成技术引入微型激光光源。硅光子技术的意义在于,它第一次将光器件的制造纳入了主流半导体制造的轨道,使得光器件的尺寸、功耗和成本大幅下降,从根本上解决了光器件与电子芯片在同一平台上集成的难题。

仅仅把光器件做小、做好、集成在芯片旁边还不够。为彻底解决芯片附近那段“堵车”最严重、能耗最高的电互连瓶颈,共封装光学(CPO)和近封装光学(NPO)闪亮登场。更深层次的集成革命正在爆发。

这两种技术的核心思想,是将处理光信号的硅光引擎与处理电信号的核心芯片如CPU、GPU、交换机芯片等,通过先进的2.5D/3D封装技术,紧密集成在同一个封装基板或载板上。这样,高速电信号只需在毫米级的超短距离内

传输,就立刻被硅光引擎转换成了光信号,送上高速低耗的光速通道。其中,CPO技术因其更紧密的集成度,在当前技术发展中尤为关键。这种技术最大程度规避了芯片出口处高频电信号传输的损耗、功耗和干扰问题,是释放光互连潜能的关键“钥匙”。

伴随着这些关键技术的突破与成熟,光互连正快速应用并席卷产业界。全球科技巨头纷纷重兵押注。在阿里云、谷歌、Meta、亚马逊AWS等企业的超大规模数据中心内部,基于硅光技术的400G、800G乃至1.6T光模块,正迅速取代传统铜缆和可插拔光模块,成为服务器间、机柜间高速互连的主流标准。

光互连,这个曾经的前沿概念,已毋庸置疑成为支撑当下全球算力增长的关键基础设施,引领涌起新的产业洪流。

高技术前沿

光子的奇妙之旅

光互连技术的核心思想极其精妙:摒弃拥堵发热的电子流,让信息搭乘近乎无损的光子在专属航道中飞驰。其工作流程宛如一场精密的接力。

整个过程始于光电转换。在数据的源头,电脉冲信号需要转换成光信号。这个关键的转换器件,通常是微型化的半导体激光器或硅基光调制器。它们被电信号精准驱动,通过改变光的强度或相位特性,将数字信息编码到光束之中。

承载着信息的光束,随即踏上光速通道。它们被注入比头发丝还细的透明光纤,或者在硅芯片上直接蚀刻出微型光波导。在这里,光子开始了近乎无阻的旅程。光子在玻璃或硅介质中传输,损耗极小,自身几乎不产生热量。更重要的是,光子对周围的电磁场不敏感,彻底免疫了电磁干扰的困扰。

转瞬之间,旅程已达终点——光电转换。在数据的接收端,高速光电探测器扮演着“解码员”的角色。它能够迅速捕捉到抵达的光信号,将其精准地转换回芯片能够理解的“0”和“1”电信号,完成信息的最终传递。

光互连带来的革命性优势,正是对铜互连痛点的精准弥补:光传输自身能耗极低,尤其在长距离传输时优势巨大。整体系统能耗比铜互连显著降低,散热压力骤降。同时,利用波分复用技术,如同让不同波长的光在同一根光纤中并行不停地流淌,一根光纤就能轻松承载几十倍、上百倍于铜线的数据量,带宽轻松突破Tb/s量级。光信号在光纤中衰减非常缓慢,可以轻松跨越从芯片内部几厘米到数据中心几公里甚至更远的距离,信号质量保持清晰稳定。电磁干扰也对光子束手无策。

光互连,如同为信息时代的数据洪流,开凿了一条高速、低耗、畅通无阻的“光子运河”,彻底重构了数据流动的底层逻辑。

从微光初现到产业洪流

光互连的概念并非一蹴而就,它的发展历程见证着人类不断追求更高信息传输效率的历史,伴随着材料科学、器件物理和集成工艺的一次次突破。

滑动验证码:用“不完美”筑防线

李建松



注册账号时的身份核验、找回密码时的安全校验、敏感操作前的信息确认……在互联网世界游走,验证码早已成为一道人们习以为常的关卡。

滑动图块验证码是最常见的验证码形式之一,主要目的是为了防止机器人或自动化程序对网站进行恶意攻击、滥用和非法访问。它通常在用户

登录、注册、评论、支付等操作过程中使用。那么,如此简单的滑动验证码,是怎么区分人类和机器人呢?

2023年,加州大学欧文分校的一项研究显示,在破解各种类型验证码的时间和准确度上,机器人的表现几乎都优于人类。最简单的点击识别,人类最快需要3.1秒,准确率最高为85%,而机器人只需1.4秒就能通过,且准确率高达100%;扭曲文本的识别,人类最快需要9秒,准确率最高不过84%,而机器人在不到1秒的时间内就能完成识别操作,准确率高达99.8%;难度较大的图片验证,机器人的速度虽然稍有下降,需要17.5秒,但人类也没快多少,大约需要15秒到26秒,准确度上,机器人与人类相当,均在80%以上。

从这些数据来看,在与机器人的“智力比拼”中,人类似乎毫无胜算。既然如此,滑动验证码为何还能成为互联网安全的一道重要防线?答案很简单,科学家们换了个思路——既然拼

“聪明”拼不过,那就在“不够聪明”上做文章。

以滑动验证码为例,它由背景图片和滑块图片组成。在验证过程中,用户按住滑块沿着轨道将其滑动到背景图片的指定位置。这一轨道通常是有一定长度的直线。从表面上看,滑动验证码的验证方式是“滑块是否被正确拖放到缺口处”,实际上其校验的信息却是“拖放轨迹是否符合真实用户的行为特征”。因此,有时滑块和缺口即使没有对齐,也能验证成功。

对机器人而言,模拟直线运动易如反掌,但复刻人类的自然轨迹却十分困难。人类的生理特性决定了操作的“不完美”:拖动滑块时,手部难以避免地轻微颤抖会让轨迹产生无规律波动;接近目标时,人类下意识放慢速度的微调,也会让运动曲线呈现独特的节奏变化。反观机器人,其程序设定的运动往往匀速且平滑,这种“完美”恰恰暴露了其非人的身份——一旦系统检测到过

快且均匀的滑动轨迹,就可能判定为机器操作。

人类的局限性,反而成了通过验证的隐形密码。注意力分散时,面对复杂背景图既要定位缺口又要控制滑块,手眼脑的协调偏差会让轨迹更显扭曲。神经传导的天然延迟,则让修正动作滞后于视觉判断,进一步放大了操作的不规律性。这些在机器人看来是缺陷的特征,恰恰成了人类的专属“身份标识”。

如今,这类利用人类行为特征的验证方式已延伸出更多形态:旋转图片拼图、绘制指定手势轨迹等,本质上都与滑动验证一脉相承——不依赖复杂的认知考验,而是通过捕捉机器难以模仿的人类行为细节,在安全防护与用户体验间找到平衡。

下次滑动验证后,若看到“打败99%的人”的提示,或许不必欣喜。这背后,是人类用自身的“不完美”筑起的防线,也是在与机器人的博弈中,属于人类的独特优势在默默守护着数字世界的秩序。

左图:滑动验证码图片。

资料图片

趣闻·新知