

物联驱动 密码先行

专家表示,万物互联时代需要安全可信的密码技术保驾护航

■本报见习记者 韩扬眉

“我每次乘坐高铁时,都在想这里面有没有密码技术,如果没有的话,我担心如果有一天被黑客攻击怎么办?这是不得不防的一个问题,今天没有攻击不代表未来没有攻击。”密码学家、中国科学院院士王小云在近日举行的“2019 首届中国物联网安全高峰论坛”上以车联网为例强调,在万物互联的今天,密码技术是信息安全的重要保障。

近年来,网络攻击事件时有发生且规模趋大,人们在超市里、网站上留下大量购物记录,生物特征信息在人们不注意的时候被广泛采集……在专家们看来,大量的数据、隐私正以更隐蔽的方式被获取。

物联网对安全提出哪些新需求?密码技术如何融入物联网并发挥作用?密码技术未来发展的方向是什么?诸如此类的问题,是物联网安全保障最亟须解决的难题。

物联安全 以密码为基石

日前,有国际消费电子领域“风向标”之称的2019 美国拉斯维加斯消费电子展落下帷幕,本届展会上迈入商用时代的第五代移动通信(5G)技术是亮点之一。与4G相比,5G具有超高速、高可靠性、低时延性、可连接更大规模的终端设备等特点。

这将让所有行业以前所未有的方式传播分享数据,万物互联正在成为现实。

中国信息通信研究院日前发布的《2018

物联网白皮书》显示:全球物联网产业规模已由2008年的500亿美元增长至2018年的1510亿美元。截至2018年年中,我国物联网产业总体规模已达1.2万亿元。

从个人消费的智能家居、可穿戴设备,到容纳交通、安防、环保等各系统海量物联网感知终端的智慧城市,再到涉及金融、能源、工业控制系统的国家基础设施……世界正向更高效、智能、环保、便捷的方向发展。

然而,一切远没有看起来那么美好。2016年10月,世界上最发达的地区之一美国东海岸发生全球瘫痪面积最大(大半个美国)、时间最长(6个多小时)的分布式拒绝服务。这是一款名为“Mirai”的恶意软件发起的大规模物联网攻击,包括Twitter、亚马逊、华尔街日报等数百个重要网站无法访问,美国主要的公共服务、社交平台、民众网络服务瘫痪。

“物联网开放的网络环境,灵活多变的防护控制需求,使得许多情况下,终端控制、数据共享都超出了既有模式划定的网络边界。”国家密码管理局商用密码管理办公室副主任霍伟指出,密码将重构物联网边界。“密码是网络安全的核心系统和基础支撑,我们需要利用密码在身份鉴别、数据加密和信任传递等方面发挥重要作用,来维护物联网的安全秩序。”

密码为基因 实现“安全可信”

密码常被称作“卫士”“信使”,但中国工

程院院士沈昌祥认为,这些职能实现起来没那么简单,“没有控制权一切免谈,密码现在需要主动识别,主动防御”。

网络安全风险自然存在。由于设计IT系统时不能穷尽所有逻辑组合,必定存在逻辑不全的缺陷,“网络黑客们”正是利用缺陷挖掘漏洞进行攻击。

2016年出台的《网络安全法》和《国家网络空间安全战略》强调要推广应用“安全可信”的网络产品和服务。

“网络空间极其脆弱,原因在于过去计算机科学缺少防护理念,体系结构缺少防护部件,计算模式没有安全服务。”沈昌祥认为,要树立主动免疫的安全目标,确保用于完成计算任务的逻辑组合不被篡改和破坏,实现正确计算。

沈昌祥表示:“杀病毒、防火墙和入侵检测的传统‘老三样’封堵查杀已过时,难以应对人为攻击,且容易被攻击者利用,找漏洞、打补丁的传统思路不利于整体安全。”

他解释,要做主动免疫可信计算,也就是在计算的同时做到安全防护,以密码为基因实现身份识别、状态度量、保密存储等功能,及时识别自己和非己成分,从而破坏与排斥进入机体的有害物质,相当于为网络信息系统培育了免疫能力。

在提高密码能力方面,沈昌祥指出,要创新可信密码体系,包括采用对称与公钥密码相结合的体制,提升安全性和效率,全部采用

国有自主设计的算法和双证书结构,提升可用性和可控性。

“攻击者进不去,非授权者重要信息拿不到、窃取保密信息看不懂、系统和信息改不了、系统工作瘫不成、攻击行为赖不掉,这就是安全防护的效果。”沈昌祥说。

抓住需求 用好密码

物联网安全问题复杂多样,密码支撑网络安全,但有很多人却抱怨密码不好用、用不起来。那么,密码究竟应如何发挥作用,未来密码技术与产业发展将走向何方?

“这几年,很多物联网的应用对密码需求很迫切,但实际上的应用基本没有,问题和难点在于物联网和密码的融合,尤其是在‘物’端,即密码如何融入各种设备和终端。”国家商用密码应用技术体系研究总体工作组组长刘平表示,要理清思路,对密码从业者和供给方来说,建立适合于物联网环境的轻量级算法体系、基于物联网的如何使用密码的技术体系、针对物联网的密码应用标准体系等。

霍伟表示,密码发展的未来,要突出应用融合,在物联网产业发展、产品研发的时候,把密码设计进去,提供基于密码的支撑能力和定制规则。

“抓好需求,就一定能用好密码。”北京商用密码行业协会会长詹榜华说。

专家呼吁重视钱学森第六次产业革命理论

本报讯(记者王卉)提起两院院士钱学森,很少有人将他与农业、草产业、沙产业联系起来,了解他关于第六次产业革命理论的人更少。日前,在北京召开的钱学森科学思想论坛上,专家认为,钱学森第六次产业革命理论的意义和作用还未得到足够的认识和重视。

论坛由中国系统工程学会草业系统工程专业委员会、中国国土经济学会沙产业专业委员会、上海交通大学钱学森图书馆、中国管理科学院农业经济技术研究所共同发起和主办。

早在上世纪八十年代,钱学森就提出要开展第六次产业革命。他认为,第六次产业革命是由现代生物技术推动的大农业产业革命,它将提高农业生产率,达到资源集约、物质循环、科学管理、生态良好、产品优质、效益提高的新形态。

由于化石能源面临枯竭的危机,钱学森认为,一旦人类实现了知识密集的农产业、林产业、草产业、海产业和沙产业,建立通过生物充分利用太阳光能生产的事业,整个经济结构就能改观。“这才是新的产业革命”,而这场产业革命“是从小弟弟沙产业做起”。

中国国土经济学会沙产业专业委员会研究员田裕钊认为,钱学森的沙产业理论可概括为“变不毛之地为沃土,在荒漠戈壁建立新绿洲”。

如今在青海、甘肃、内蒙古等地出现了一些草产业、沙产业的典型,“这些典型能够发展成为一二三产业联动,提高农民收入水平的典型。”原农业部政策体制改革司司长郭书田说。

让中国农业大学教授胡跃高焦急的是,第六次产业革命迄今仍较多地停留在理论层面上,多数人甚至从未耳闻。

中国系统工程学会草业系统工程专业委员会名誉主任李毓堂认为,不能盲目借鉴西方的农业治理举措来解决中国的“三农”问题,应该参考钱学森第六次产业革命理论,以新型经济机制体制确保生物、信息等新技术的转化和普及,确保农业迅速摆脱化学危害,加快向绿色生态转型升级。

专家建议,应研究制定2020—2050年第六次产业革命发展规划,每年召开相关理论与实践研讨会、培训班,建立省域试验示范区,动员多方面力量参与。

首届“青少年科学小会”在深举行

推出科学看点榜单和“科学年历”小程序

本报讯(记者赵广立)1月20日,由中国科学技术协会(以下简称中国科协)指导、腾讯公司主办的首届“青少年科学小会”在深圳举行。会上,腾讯联合国际权威学术杂志《科学》发布了全球首个青少年科学看点榜单,中国科协与腾讯公司携手开发的“中国青少年科学年历”(以下简称“科学年历”)小程序也在会上推出。

《中国科学报》了解到,入围《青少年科学看点榜单》的候选主题,均由《科学》的新闻团队以及《科学》/美国科学促进会(AAAS)定制出版办公室的科学编辑与全球科学家,从过往近十年数十个年度科学突破中精心挑选出来;

而后由腾讯公司运用社交平台、大数据和综合调研分析,结合超过10万名年轻用户的兴趣,从入围主题清单中最终遴选。

按照年轻用户对这些主题的排列次序,这十大科学看点依次是:火星上发现液态水、发现操纵记忆的原理、揭示睡眠可能有清洁神经连接的作用、“芯片上的大脑”(神经拟态芯片)、摩洛哥智人化石改写人类起源、“基因剪刀”CRISPR的发明、270万年前“冰芯气泡”揭示的气候变化、通过合成生物学升级细菌(生命的2.0版本)、协作式机器人“Cobots”崛起、微生物揭示的健康状况。

在首届青少年科学小会现场,腾讯还邀

请一代物理学大师斯蒂芬·霍金的女儿、儿童科普作家露西·霍金,哈佛大学医学院睡眠医学部主任、NASA国家空间生物医学研究所首席研究员查尔斯·采斯勒,斯坦福大学神经科学家、《西部世界》科学顾问大卫·依格曼等科学家、科普学者与百位“问号少年”面对面交流,解读榜单中前沿科学领域的奥秘。

中国科协与腾讯公司携手开发的“科学年历”汇集了2019年科学事件、科普活动和科技竞赛,将通过提供活动资讯获取、科普内容分享、科学活动参与三大功能,为12~18岁的国内中小學生及其学校及家长群体提供服

务,帮助热爱科学及科普活动的青少年及时获得更好、更全的科普活动资讯。记者使用该小程序,可以便捷地找到诸如“倒计时101天:2019年中国科学院公众科学日”之类的一年里重要的科普活动,并可查看参与方式和报名渠道。

针对为青少年打造的科普盛会取名“科学小会”,腾讯集团副总裁程武解释,“小”指代“面向小观众、聚焦小目标、关注小问题”,寓意“播撒科学种子”。他还宣布,腾讯将推出“青少年科普创作计划”,鼓励具备专业知识青少年在腾讯内容平台上创作科普内容,让科学知识持续惠及更多人。



1月20日,昆仑站天文区一角,正前方为8米高铁塔上的视宁度测量望远镜,左后方为南极巡天望远镜AST3-2。

连日来,中国第35次南极科考队昆仑队队员在昆仑站天文区安装、调试和维护天文台址监测设备和天文观测设备,调查南极冰盖之巔冰穹A地区天文观测条件并开展天文观测。

新华社记者刘诗平摄

内蒙古库伦旗优秀师生走进中科院

本报讯(记者闫洁)1月17日,内蒙古库伦旗优秀师生“走进中科院、走近科学家”助学助教项目在京正式启动。

启动仪式上,中科院行政管理局(以下简称行管局)党委书记肖建春宣读了中科院院长白春礼写给库伦旗师生的一封信。信中白春礼希望师生们通过参观丰硕科技成果,

不断提升科学素养,为进一步增进民族团结,实现伟大“中国梦”作出积极贡献。

中科院行管局局长顾全介绍说,“走进中科院、走近科学家”项目由北京中科科教发展基金会捐助,计划3年内资助百名库伦旗优秀师生走进中科院,感受科技魅力,拓展科学视野;走近科学家,学习科学精神,励

志科学事业。

据了解,在中科院精准扶贫工作指导意见的统领下,2018年5月,行管局与库伦旗政府开展系列帮扶协作工作。此次助学助教项目将进一步围绕“构建一个纽带、建设两个基地、打造三个平台”,助力库伦旗精准扶贫、科技扶贫工作按期高质量完成。

发现·进展

中国科大

开发出医学电阻抗成像新方法

本报讯(记者杨保国)近日,中国科学技术大学杜江峰院士领导的中科院微观磁共振重点实验室在医学电阻抗成像领域取得新突破,开发出一种精准、高效且稳定的动态医学电阻抗图像重构方法,成功获得动物血胸、气胸状态下高分辨电阻抗图像。相关研究成果近日发表于《IEEE医学影像学》。

电阻抗成像技术是利用生物组织与器官的电特性及其变化规律提取与人体生理、病理状态相关的生物医学信息的成像技术。该技术的基本测量方式是通过体表电极阵列向检测对象施加安全的电激励(电流或电压),在体表测量响应电学信号,由所测信号重构出人体内部结构与功能电特性图像。由于人体不同组织和器官的电特性不同,这种电特性图像不仅包含了丰富的解剖学信息,而且能够反映出组织和器官电特性相应的生理、病理状态和功能信息,在研究人体组织与器官功能变化和疾病诊断方面有重要的临床价值。

电阻抗成像技术具有无损、无创、无辐射、低成本、操作简单、功能信息丰富等优点,但电阻抗图像重构本身是一个严重病态的非线性逆问题,传统方法重构出来的图像空间分辨率和对比度较差。在硬件采集系统满足一定测量精度的前提下,引入有效的图像重构算法对于高精度、高分辨率的电阻抗成像研究至关重要。因此,如何提高重构图像的分辨率,改进重构算法的稳定性,以及加快重构速度实现实时成像成为当前电阻抗技术研究极具挑战性的问题。

杜江峰团队基于形状先验信开发出一种高分辨、高对比度的动态电阻抗图像重建算法,成功实现了精准、高效且稳定的动物血胸、气胸状态下电阻抗图像重建。该算法具有失真小、速度快、对比度高、鲁棒性强、稳定性好的特点。据介绍,该成果为开展临床医学精准、高效且稳定的动态电阻抗成像奠定了坚实的基础,有望加速推进电阻抗成像技术的临床应用发展。

相关论文信息:

<https://ieeexplore.ieee.org/document/8416750>

上海交大医学院等

揭示早期营养不良如何增加哮喘风险

本报讯(记者黄辛)上海交通大学医学院附属国际和平妇幼保健院、上海市胚胎源性疾病重点实验室黄荷凤院士带领团队,利用生命早期营养不良小鼠模型,通过对小鼠免疫细胞的代谢水平以及表观遗传学的调控来影响其功能,最终影响了小鼠子代哮喘的发病。相关成果近日在线发表于《变态反应与临床免疫学》杂志。

最新的流行病学调查发现,胎儿宫内生长受限可影响子代呼吸系统的发育和功能,并显著增加从儿童到成人哮喘发生风险,但其发生机制尚不清楚。研究人员通过蛋白质组学限制来模拟营养不良的状态,构建了生命早期营养不良的小鼠模型,发现生命早期营养不良的小鼠较生命早期营养正常的小鼠实验性哮喘易感。而这哮喘易感性表现出一定的性别差异,在雌性子代中没有发现哮喘加重的迹象,这可能与发育源性疾病存在性别偏好有关。

值得关注的是,研究人员发现母体妊娠期即子宫内的营养状况相较于哺乳期的营养状况对子代实验性哮喘易感性影响更大。这也提示准妈妈们更要注重妊娠期的营养水平和营养均衡。

同时,CD4⁺T淋巴细胞在过敏性哮喘发病中发挥了关键作用。研究人员利用 Seahorse 能量测定仪的代谢分析等技术,发现生命早期营养不良的小鼠 CD4⁺T 淋巴细胞活化后表现出更强的糖酵解速率,而氧化磷酸化速率没有发生显著改变。重要的是,当阻断糖酵解途径之后,生命早期营养不良小鼠的 CD4⁺T 淋巴细胞的功能和分化水平被显著抑制,实验性哮喘症状也得到明显缓解。

研究人员表示,这为胚胎源性疾病机制的探索提供了新的思路和视角,为生命早期营养不良所致的哮喘易感性提供了潜在的干预策略。

相关论文信息:

DOI: <https://doi.org/10.1016/j.jaci.2018.12.999>

简讯

秦巴吕梁山主要经济作物提质增效项目启动

本报讯1月17日,国家重点研发计划“秦巴山、吕梁山主要经济作物提质增效技术集成研究与示范”启动会在西安举行。

科技部中国农村技术开发中心副主任聂善明指出,该项目是为精准扶贫、乡村振兴提供科技支撑的项目,重在体现“三个度”:精准扶贫的参与度、解决关键问题的创新度、与产业的关联度。

项目首席科学家、陕西省微生物研究所研究员万一表示,项目旨在解决秦巴山区食用菌和吕梁山旱作农业提质增效关键问题,在秦巴山区建立主栽品种和高附加值品种有机结合的食用菌产业发展模式,在吕梁山建立全生物降解渗水地膜机械化旱作高产技术模式,在生态资源可持续利用的前提下,提质增效、精准扶贫。(张行勇)

一种海人树种子萌发及育苗方法获发明专利

本报讯中科院华南植物园涂铁要等科研人员完成的“一种海人树种子萌发及育苗的方法”近日获国家发明专利授权。据悉,该发明提高了海人树种子出苗率,解决了中国南海海洋岛屿生态重建过程中海人树种子育苗问题,使其能够通过播种繁殖开展育苗栽培,达到规模化育苗的目的。(朱汉斌 周飞)