新闻热线：010—58884063
E-mail:kbjdsm@126.com
■责编 段佳
科技日报 2018年2月1日 星期四

外有病毒“觊觎” 内有加密“隐忧”

隐藏复杂技术 让密码“轻松落地”

本报记者 **张佳星**

“全球约6300个平台提供勒索软件交易，2016—2017年期间勒索软件销售增长25倍。”《2017年度网络空间安全报告》日前发布，勒索病毒的出现和黑市传播，使得网络空间安全暴露出“危如累卵”的局面。

继2017年《网络安全法》实施以来，《中华人民共和国密码法（草案征求意见稿）》也开启立法程序，旨在通过制度建设应对外有病毒“觊觎”、内有加密“隐忧”的状况。“未来，关键信息基础设施应依规使用中国自己的密码算法，”北京炼石网络技术有限公司CEO白小勇说，以境外密码体系为基础的行业应用均需要升级。

面对法规的即将落地，有人在等“事到临头”，而有人却已先人一步。“做拉动者，而不是被推着走，”1月29日，炼石网络首席营销官岑义涛对科技日报记者说，创新者就是要顺势而为走在前面。

网路“裸奔”危险重重 加密研究必须领先

新华网此前报道，中国的银行业核心领域长期以来都是沿用SHA-1（美国国家安全局设计）、RSA（美国公司设计）等密码算法体系。尽管政府部门一直在积极推动试点示范，效果却并不明显，“长且阻”“难推进”的局面一直存在。

而早在《中华人民共和国密码法（草案征求意见稿）》出台的之前两年，炼石网络的密码团队就开始对我国的商用密码（SM）体系进行研究。既然要在中国做云计算安全的“守门员”，就要用中国自己的密码算法体系做加密，从2015年开始，团队除了研究应用很多的境外密码体系，也对国家密码管理局公布的SM2、SM3、SM4等一系列密码算法深度钻研、进行技术储备。

当时，中国大量的行业企业，包括金融、医疗、电力等，均使用境外密码技术，炼石网络的研发团队仍然坚定要做服务于中国密码算法产业化的技术储备。团队中有一位数学博士，他始终相信“在中国搞加密，不做SM是不行的”。这位博士正是主持设计了SM3的中国科学院院士王小云的学生。

“当时数据上‘云’很火，但是数据的拥有者并不放心直接放在云上，因为根本掌控不了云服务商会对这些数据做什么，”岑义涛回忆，“因此我们想让信息在传输到云的路上就被加密，用户自己拥有解密的钥匙，那就不怕泄密了。”

直到2017年4月，《密码法》（征求意见稿）发布，团队的选择遇上了政府制度的东风。“一旦法律通过，我国关键信息基础设施中的相关信息，在网路上不加密的‘裸奔’是不被允许的，也不应继续以境外密码体系为基础进行加密，”白小勇说，而应当依照法律、法规的规定和密码相关国家标准的强制性要求使用密码进行保护，同步规划、同步建设、同步运行密码保障系统。

填补产业链环节 衔接密码与应用的鸿沟

“没有强制力，主动性不强仅仅是一个方面，”岑义涛说，中国密码国产化“长且阻”的另一个原因还在于密码学相对艰深，中国开发的密码产品悬在半空，落地困难。

“我们发现国产的密码产品设计并不友好，提供的算法接口不够用、支持的开发语言也不够多，让应用开发者很为难。”白小勇感觉到，要衔接密码与应用之间的“鸿沟”，产业链条上可能需要补上一环。

“大量的已建应用系统很难通过改造来升级商用密码。”白小勇说，密码算法技术是信息世界的基础设施，底层架构的更迭门槛很高。“数学专业起码要是博士毕业，在这个基础上，还要精通各个场景，所以让所有行业都具备这样高水平的专业密码算法人才、推进有效更迭并不现实。”

炼石网络于是开始了“炼石补天”的征程，将艰深的密码算法通过“封装”的方式，隐藏底层，以帮助其融进不同的应用场景中。

如何让不懂密码技术的应用开发人员更方便、更安全地使用密码？

需要把很多密码的底层复杂技术“藏起来”，屏蔽底层实现，让开发者可以灵活选择底层硬件。炼石提出三层封装技术，即在传统的算法层和资源抽象层之上，进一步面向业务人员和业务场景进行“业务封装”，把不同的安全服务提供给应用开发人员直接调用。

比英特尔快近30% 不让“大佬”用专利“卡脖子”

“他们是第一个在中国研发出这样的技术，并且得到了快速的转化。”360企业安全集团总裁吴云坤评价，之所以能够落地，炼石网络除了解决“易用”的问题之外，还让商用密码变得更高效。

事实上，由于我国商用密码在安全性上的要求，计算更复杂，使得在性能方面，用户如果用原来境外密码算法加解密数据时处理每个字节需要2个CPU时钟周期，而我国的商用密码产品目前普遍在10几个CPU时钟周期。

“提速加解密”，这是产品能够获得市场的关键、也是技术能够转化应用的关键。“例如文档加密后会更安全，但是如果你要看个加密文档，解密会拖延1分钟，就有可能让你因为这1分钟而弃用它，”岑义涛说，安全性的增强不能以降低应用的效率为代价。

为此，2016年下半年，团队开始着手研究基于中国商用密码的算法提速。“我们先了解了一下有没有人做过，却发现跨国公司英特尔也很早就意识到了这一点，并在中国布局了专利。”岑义涛回忆，听到这个消息时，是崩溃的。如果真被跨国大佬“卡住脖子”，中国密码国产化将需要巨额的专利使用费。

“但仔细研究后，我们发现英特尔的算法加速实现模式和我们的实现模式是有细微差异的。这样的差异，有可能会帮我们绕过英特尔的专利。”岑义涛说，随着技术实现代码化，并进行多次测试，炼石团队发现，他们不仅绕过了英特尔布局的专利，还在算法执行效率上高出近30%。这意味着，英特尔布局的专利无效了。

马不停蹄地，炼石网络申请了PCT（专利合作协定）专利，布局在美国、日本、中国等国家。

“我们正在和金融设备制造商合作，将国密SM又快又好地用于金融业。”岑义涛说。

随着“区块链”技术的名噪一时，密码技术越来越被人们熟知。除了帮助关键信息基础设施依规升级外，炼石网络还将中国商用密码融入到新领域的底层架构中。白小勇介绍，“我们跟合作伙伴众享比特一起把商用密码升级替换到区块链技术里，让新事物在进入我国的初期就能够做好信息安全工作，而不是先发展再弥补短板。”

相关链接

我国商用密码行业仍投入不够

1999年10月7日，国务院273号令发布施行《商用密码管理条例》，我国密码的应用从此开始走向社会，并孕育出商用密码产业。截至目前，国家商用密码管理办公室制定了一系列密码标准，包括SM1（SCB2）、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法（ZUC）等，整个行业有1900多款商用密码通用产品，900多家从业单位。

商用密码技术已广泛应用于电子政务、电子商务等领域。例如，第二代居民身份证使用了商用密码技术，有效地增强了防伪造、防变造的能力，假身份证不再有生存的空间；商用密码在支付密码器系统中的应用防止了金融票据的伪造、假冒和涂改，保证了来往资金的安全。

我国自主知识产权的密码算法由于技术上的先进性，也逐渐走向国际，成为国际标准。祖冲之算法是中国第一个成为国际密码标准的密码算法，于2011年9月正式被3GPPSA全会通过成为3GPPLTE第三套加密标准核心算法。2017年11月3日，通过SM2、SM9数字签名标准正式成为国际标准，这也是我国商用密码标准首次进入ISO。

但我国网络安全投入还很不够，仅占整个IT产业比重的1%至2%，低于世界5%至10%的平均水平，更低于欧美国家8%至12%的水平。按照国家有关部署，金融和重要领域正在强化密码应用，大量网络和信息系统涉及密码保障系统的新建或改造，市场空间很大。密码应用将会带动更多安全投入，拓展更大安全市场空间。

中科院举锤：千件专利将首次拍卖

第二看台

本报记者 **李大庆**

今年3月，中科院将推出建院以来的一个属于“第一次”的活动：向社会拍卖中科院的专利。

1月24日，中科院2018年工作会议在北京举行。会议期间，中科院科技促进发展局局长严庆透露，中科院知识产权运营管理中心启动了“中科院专利拍卖”活动。中科院将有57家院属机构参与，面向全社会发布了1006件拟拍卖专利。中科院拟采取线上和线下相结合，网上竞价和拍卖举牌联动，全方位多渠道予以推进知识产权的运营。

作为科技国家队的中科院，虽然每年都产出大量的专利，但集中拍卖专利还是首次。中科院知识产权运营管理中心为此还推出了“中科院专利估值模型”，从专利的先进性、技术支撑度、市场关联度三个维度进行评价，生成拟拍卖专利的预估值。严庆认为，中科院的这次拍卖活动将是我国专利公开拍卖有史以来数量最大、质量最高的一次，拍卖标的覆盖了电子信息、生物医药、新材料、节能环保等多个国家重点支持的战略性新兴产业。

去年，中科院知识产权运营管理中心还面向中小企业推出了“普惠计划”，以共享中科院专利为抓手，企业签订协议成为专利池的共享人，按照入池协议的约定可以在两年期限内免费自行实施使用专利。“普惠计划”城市路演活动已经在上海、深圳等11个城市举办了15场活动。首批入池的专利有774件，入池和意向入池的企业有200多家，已转让了专利25件，授权共享专利230件。

在推进科技成果转化方面，中科院狠抓重大科技成果的转化工作，示范应用亮点纷呈。

2017年，拥有自主知识产权的全球首套煤基乙醇完成工业示范，实现产业化，标志着我国已率先具备设计和建设百万吨级大型煤基乙醇工厂的能力，对于缓解我国石油供应不足和实现煤炭清洁利用具有战略意义。低阶煤专项已落实20个工业示范项目，预期带动社会投资400亿元，建成后可实现年产值234亿元，年利税45亿元。大气灰霾监测关键设备在“一带一路”峰会期间，为保障空气质量提供了重要的大气立体观测数据，是北京市环保局大气环境会商的重要依据。改性粘土治理赤潮技术实现商品化与市场化，成功应用于厦门金砖峰会期间的赤潮应急处置，保障了近海环境安全。禽流感亚单位二价疫苗和寨卡灭活疫苗实现技术转移，抗阿尔茨海默症、超长效抗糖尿病、抗肿瘤创新药物等多种新药的临床工作取得进展。

去年9月4日，中科院上海有机化学所与信达生物制药（苏州）有限公司就肿瘤免疫靶向小分子药物的授权开发达成了合作协议。信达生物以首付款、研发里程碑和销售里程碑付款共计的合作方式，以4.57亿美元获得IDO小分子抑制剂的全球独家开发许可权。这是目前国内科研院所与本土生物制药企业达成的合作金额最高的项目，成为中国科研院所与企业创新药合作的重大里程碑事件。

2017年，中科院还部署了10项科技成果转移转化重点专项（弘光专项），部分项目已取得可喜进展。“机场安检智能识别系统”已示范应用于国内61个机场的旅客安检，在全国旅客吞吐量超过3000万人次以上机场的示范覆盖率达到80%，覆盖了超过540条安检通道，其中29条为要客安检通道。根据相关机场试用情况的反馈，在使用机场安检智能识别系统后，机场安检通行效率和准确率得到明显改善，抓获冒用他人身份证乘机的人数较之前显著增加。其中，厦门高崎机场启用民航安检人脸识别辅助验证系统6天内查获9宗企图持用他人证件乘机事件。“卫星移动通信终端基带芯片”（简称“晶芯”）实现量产并成功应用，解决了制约我国空天地一体化通信产业发展的高端核心器件供给瓶颈难题，成功占据“卫星+”产业战略制高点，中科晶上公司成为国内首屈一指的卫星移动通信全系统解决方案提供方。中科院将与南京市政府共建国家卫星移动通信与计算创新与产业化基地，共同打造全球领先的空天地一体化网络技术创新中心和产业引领中心。

据初步统计，2017年，中科院通过科技成果转移转化使社会企业新增销售收入4080亿元，新增利税503亿元；中科院下属院所投资企业实现营业收入4007亿元，净利润107亿元，创造就业岗位16万个。

展示台

河南：开建我国首个杂交小麦产业化基地

我国首个杂交小麦项目产业化基地在河南省邓州市正式开工建设。

该项目以我国首创的二系杂交小麦技术为依托，主要开展杂交小麦育繁推一体化经营，打造国家级高标准种子生产基地和国际领先的杂交小麦商业化育种平台。开工建设的一期工程包括60亩的科研中心和种子检测加工中心，370亩的基因资源圃和育种站，1万亩的杂交小麦种子生产示范区。该项目预计到2018年12月可全部建成，并在3年内形成年产优质杂交小麦种子250万公斤的能力。

国家杂交小麦项目（邓州）产业化基地是北京与邓州市对口协作项目之一，是双方签署的《农业科技合作框架协议》中的一项重要内容，获得了南水北调对口协作项目和国家重点研发计划项目等的资金支持。（记者**乔地** 通讯员**王中献**）

贵州：农业技术交易增长近8倍

1月25日，贵州省科技厅在贵州省技术市场工作会上公布数据：去年，贵州省技术合同成交5847项，成交金额196.56亿元，同比增长分别为99.4%和15.9%。

近年来，贵州省创新科技工作体制机制，着力解决技术到经济最后一公里难题，大力推进技术市场工作，采取了包括在全国省级科技部门率先推出科技创新券政策、出台技术市场培育发展资金后补助办法等举措，有力地促进科技成果转移转化，使得全省的技术交易规模和质量显著提升。去年，贵州省技术合同成交5847项，成交金额196.56亿元，同比增长分别为99.4%和15.9%。数据显示，贵州省成为全国引进技术成果转化运用增长最快的地区之一，其中，以技术开发和技术服务类合同为主，重大技术交易合同为全省技术交易“主力军”，在企业继续保持技术交易主题地位的同时，农业领域交易额快速增长，同比增长799.37%。

下一步，贵州省将把技术转移体系作为推进科技成果转化的重要抓手和平台，补齐技术转移短板，打通技术转移链条，建立完善符合我省科技创新、技术转移和产业发展规律的技术转移体系。

（记者**何星辉** 实习生**洪永**）

谈经论道

健全科技成果转化责任制

新的科技成果的产生并不等于新产业的形成，要使科技成果转化成现实的生产力，尤其要形成规模效益，还需要相关部门制定具体的落地措施以及大力度的财政支持，为科技成果转化创造更加有利的环境条件。依法建立健全转化科技成果责任制，加快科技成果转化已成为关键问题。如此，才能为科技企业提供科技成果转化的责任制路径，政府相关部门才能为创新、创业主体营造出引导、协调、监督、服务等全方位的社会环境。

——1月30日，山西省政协委员、山西全安新技术开发有限公司董事长郭春平在山西省的两会上建议。

在科技成果转化中引入民营科技中介

应制定政策，明确民营科技中介的地位和作用；完善在川科研院所科技人员创业与服务企业的政策措施，明确民营科技中介在四川省科技成果转化中的作用和地位，形成多部门、多行业和多领域统筹规划、协调推进的工作格局。

——1月29日，四川省政协委员、民盟成都市委常委、电子科大资源与环境学院院长胡光岷在四川省的两会上表示。

建设科技成果转移转化承载区

济南今年已经给各区县下达了科技招商和科技成果转化的任务目标，各区县今年都将建设科技成果转移转化承载区。要给科学家提供拎包入住的服务，所有转化的项目都要进园区，不能放任不管，服务更专业化。

——1月28日，山东省政协委员、济南市科技局局长吕建涛在省政协十二届一次会议举行的专题记者会上说。

推动更多科研成果的产业化

中关村的企业家要更多的与中科院这样的科研机构展开合作，推动更多科研成果的产业化，为我国经济发展贡献更大的力量。

——1月29日，联想控股董事长柳传志在参观完中国科学院创新成果展之后说。

（本版图片来源于网络）