量子密码:无条件安全的希望

密码的安全性有两种:
一种为计算安全性,原理上可破译,但须耗费大量的时间和资源;
第二种是无条件安全性,原理上不可破译,无论窃听者能力如何强大。

“现在很多东西都能克隆——甚至有人想克隆爱因斯坦——但量子态不能克隆,世界上没有一个‘量子机’能对任意一个未知的量子态进行完全相同的复制过程,这就是量子不可克隆定理。用量子态做密码的安全性就在于此。”日前,中科院院士、全国量子光学专业委员会主任郭光灿谈到量子技术的应用时说,“量子密码是量子学中第一个可用的技术。”

“未来的100年人类会进入量子调控新纪元，会有一批新的技术叫量子技术。影响最大的是量子计算机，大概还有10~20年以后才能实现；但是量子密码，现在已经到了实用阶段。”郭光灿说。

加密与破译如同盾和矛，它们之间的博弈永不停息

目前，人们已经可以使用专用芯片、并行计算等进行密码破译,而随着量子计算机的脚步越来越近,更是对现有密码体制提出了严峻挑战。郭光灿说:“量子计算机可以挑战现在所有保密方式，也就是说,挑战的是现代密码学。”

密码学研究信息从发端到收端的安全传输和安全存储,是研究“知己知彼”的一门科学。现有的密码体制各不相同,但它们都可以分为对称密钥(如DES密码)和非对称密钥(如RSA密码)。前者的加密过程和脱密过程相同,而且所用的密钥也相同;后者,每个用户都有各自的公开和私人密钥。

“对称密钥体制中加密和解密的密钥一样,因此密钥要保密,如果被第三者窃取,就失败了。”郭光灿介绍说,“现在证明(对称密钥)有一种保密方式绝对不可能被破译,即一次一密。密钥用一次就丢掉,这种密钥理论上不可破译。”

一次一密是在流密码中使用与消息长度等长的随机密钥,每个密钥使用一次后即销毁。由于使用与消息等长的随机密钥,产生与原文没有任何统计关系的随机输出,因此一次一密方案不可破解。

人类似乎找到了安全的通讯办法。然而,一次一密也有明显的缺陷

“一次一密的密钥就要大量的密钥,产生大量的随机数,密钥的更新是个大问题，比如密码本上的密钥用完了怎么办?被窃取就更麻烦。”郭光灿说,“尽管一次一密绝对安全,但密钥传输是漏洞。”

“有没有解决办法?有,就是非对称密钥,使用加密的密钥。”郭光灿说,由于公钥公开对外发布,想给私钥持有者发送信息的人都可以取得公钥，用公钥加密后,发送给私钥持有者，即使被拦截或窃取,没有私钥的攻击者也无法获得加密后的信息,可以保证信息的安全传输。

这样安不安全呢?人们能不能通过计算机破解加密信息呢?郭光灿介绍说,这又引申到一个数学问题,基于大数因子分解的难题,保证从公开密钥推导出私有密钥需耗费极为巨大的资源。

“比如将一个129位数分解成64位素数×65位素数,1977年的计算机水平要耗时400万年计算出来；到1994年,8个月就可以破解掉;而如果人们发明了量子计算机,2000个Qubit的量子计算机1秒就能破解。”

郭光灿说,这种密码方案也只是相对安全，即计算安全性——原理上可破译,但须耗费极大的时间和资源。而一旦量子计算机研制成功,现有的基于大数分解的RSA密钥将无密可保。

“在路上”的量子密码

“密码的安全性有两种：一种为计算安全性,原理上可破译,但须耗费大量的时间和资源；第二种是无条件安全性,原理上不可破译，无论窃听者能力如何强大。一次一密可以做到无条件安全,问题是如何分配密钥。”郭光灿指出,“现在我们可以靠量子密码来解决这个问题。”

量子密码是利用信息载体(例如光子等粒子)的量子特性,以量子态作为符号描述的密码。“利用量子的性质,量子的不确定性和概率性,可以规避经典密码中的短板。”郭光灿介绍说,经典比特只有0、1两种状态,例如对应着晶体管的电流导通和截止两种状态;由于态叠加原理,量子比特不仅可以处在0、1两种状态,还可以处在0、1的叠加态,例如对应着电子自旋状态、光子的偏振状态。

另外,量子密码的安全性由量子力学的物理原理保障。根据“测量塌缩理论”(对量子态进行测量将会改变最初的量子态),窃听者的存在会引入额外误码。“比如,无窃听者存在时,误码率为0;受截取重发攻击时,误码率为25%。当误码率超过了阈值，就表示信道中间存在窃听者。此时警报响起,停止密钥分发,已分发密钥丢弃不用。”郭光灿说。

“量子密钥建立密码的程序可以发现窃听,经典密码是做不到的,这是量子密码的安全性。”郭光灿告诉记者,理论上能够证明，量子密码不仅能抵抗经典的截取重发攻击,即使在量子攻击下也是安全的。

实际上,量子密钥分配的理论安全性已得到了严格的数学证明。1999年,首个量子密钥分配的无条件安全性证明被提出;2001年，理想的BB84协议被证明无条件安全。

“现在已经快到实用阶段了。”郭光灿介绍说,2004年，其课题组在国际上首次成功分析实际光纤量子密码系统不稳定的原因,并使用法拉第反射镜的迈克尔逊干涉方案实现了国际上第一个城际量子密码实验,量子线路长度125公里,创下了当时的世界纪录。

当前，量子密码技术的应用化还面临若干障碍，主要的有量子密码系统的实际安全性问题，即由于器件等的非理想性导致安全性漏洞。量子密码系统必须能经受得住现有所有可能手段的攻击才可以实际应用。另外，提高密码比特率、研制实用量子中继器等也是重要的问题。

最近，丹麦Aarhus大学教授Martin Kristensen着手研究使用集成光学的方法制造量子密码芯片，已取得了初步成果。“预计在5到10年内，就会有能够投入市场的量子密码芯片成品。”郭光灿说。

《中国科学报》 2014.3.28 文/赵广立

大数据与国家治理

大数据具有海量、多源、复杂的信息属性和高端、前沿的技术特征,是继云计算、物联网之后又一次颠覆性的技术革命。大数据使人的思维方式、行为模式、管理理念发生全方位变革，在公共管理领域蕴含巨大的应用潜力和创新空间。

大数据在国家治理中的重要价值

提升科学决策水平。大数据,作为一种新兴数据处理技术，能够更为有效地集成国家政治、经济、文化、社会、生态等各领域方方面面的信息资源，为国家治理提供重要数据基础和决策支撑。如医疗、“三公”经费、保障性住房、食品药品安全等改革焦点问题，都可借助大数据来辅助决策。通过对政府海量数据的交换、整合和分析,还可以挖掘新知识,带来新发现,创造新价值,增强国家战略制定的前瞻性和先导性。更为重要的是,大数据的广泛应用,利于形成用数据分析、用数据决策、用数据创新的治理思维和文化,对于实现“数据治国”具有深远的影响和价值。

增强国家治理能力。大数据与公共危机管理的有效对接，能够强有力地推动公共安全信息网络完善,促进跨部门、跨区域管理信息协同共享，提升公共危机事件的源头治理、动态监控、应急处置和事前预警能力；大数据与互联网、微信、微博等新媒体的深度融合,可以突破时间和空间的限制,从更深层次、更广领域促进政府与民众之间的互动;同时,大数据是维护国家数据主权、增强信息和网络安全的新引擎。

提高政府服务效能。大数据与物联网、云计算等技术的联姻,能够加快智慧城市的建设步伐,推进智能交通、智能物流、智能社区、智能医疗、智能教育的快速发展;我国的工业化、城镇化、信息化、生态化建设也将因大数据的革命而加速转型升级。大数据所集成的数据挖掘、遗传算法、机器学习等前沿技术,具有智能判断分析、智能纠错优势,应用于财政、金融、税收、政府转移支付等领域重大项目的跟踪审计，可实现对项目实施过程的实时动态监控与预警，减少差错和舞弊行为,对建设阳光、高效、服务型政府具有积极意义。

建设大数据强国的战略路径

我国是数据大国,随着国家金关、金税、金盾、金审等一大批电子政务“金字工程”的深入实施,积累了海量的数据资源，构成了新时期国家治理领域改革和创新潜在的巨大“数据红利”。但我国还不是数据强国，数据资源共享协同程度低、技术支撑体系不完善、立法滞后等问题突出，当务之急还需做好以下方面工作:

将大数据上升为国家战略。2012年3月,奥巴马政府投资2亿美元,推出了“大数据研究与发展先导计划”，开创了各国政府竞相发展大数据的先河。同年9月，日本总务省发布的2013年行动计划，将大数据作为新ICT（信息通讯技术)战略的重点。2013年2月,法国发布的政府《数字化路线图》,将大数据列为国家创新战略重点实施领域之一。

建立健全大数据公共服务体系。大数据是完善国家治理的金矿，其价值的充分挖掘与创造离不开完善的公共服务体系。要紧密围绕数据治国的战略所需,加强大数据标准体系建设，建立面向不同类型、涵盖各个领域、不断动态更新的大数据建设标准，为实现各级各类信息系统的网络互连、信息互通、资源共享奠定数据基础；积极开展国家大数据技术创新战略联盟、产学研协同创新平台建设,重点攻关一批大数据关键技术,形成集海量数据的搜集、存储、管理、分析、挖掘和运用于一体，具有自主知识产权的技术支撑体系;着力开展典型应用示范,选取医疗卫生、食品安全、终身教育、智慧交通、公共安全、科技服务等惠及民生的关键领域,率先开展大数据服务。

完善大数据立法。大数据的应用涉及公民个人隐私、政府信息公开及国家网络安全等重要领域,离不开完善的法律保障。当前要进一步加强大数据立法,妥善处理相关法律法规制定、修改、废止之间的关系;强化电子政务、信息安全、政府信息公开、个人信息保护等方面的法律法规体系建设;加强大数据法制建设中的国际交流与合作,积极参与相关国际规则的研究和制定,以此营造大数据发展的良好法制环境,促进大数据与国家治理对接的法制化、规范化发展。

《光明日报》 2014.3.27 文/贺宝成

垃圾焚烧也能变成大好事

日本实现无害化处理

记者最近在日本参观了大阪市环境局下属的大正垃圾处理厂。这里不仅通过焚烧可燃物大大减少垃圾数量，同时还高效利用废热发电、提供热能,可谓一举多得。

记者在大正垃圾处理厂厂区看到,巨大的垃圾竖井深达40米,容量8000立方米,可以装入约2400吨垃圾。工作人员在顶端的玻璃幕墙后遥控吊车，一次就能抓起3吨重的垃圾送入焚烧炉。

虽然垃圾如此之多,但厂区内并没有令人作呕的异味。这是由于垃圾产生的异味被抽风机抽取，利用空气预热器加热到150至200摄氏度，再送入焚烧炉,由于炉内的高温,异味物质都被分解了。

为了避免焚烧时产生致癌物二噁英,焚烧炉利用850至950摄氏度的高温使垃圾实现完全燃烧。工作人员通过监控屏幕,可以实时观看焚烧炉内的情形。

垃圾焚烧过程中产生的粉尘使用电气集尘器吸附,废气还要经过洗涤装置、过滤式集尘装置等处理程序，符合安全标准后才从烟囱排放。

可燃垃圾焚烧后最终形成的灰烬只有原来体积的二十分之一左右，对其中不能完全避免的一些有害物质则使用药物进行无害化处理。灰烬最后被运到大阪湾填埋。

当然，以焚烧为主的垃圾处理厂,还有一项增值业务,就是对于铁柜、床垫、自行车等大件不可燃垃圾，提炼有用资源。工厂内也有各种大型粉碎设备,在将上述类别物质细细粉碎后，用磁选机选择出金属部分作为资源出售；而金属上附着的纸、碎布条等，则用风力筛选去除,与其他可燃部分一起送入焚烧炉。

垃圾焚烧产生的热被用于制造蒸汽,再由管道输送给蒸汽涡轮机进行发电,这些热量还能同时给工厂提供热水和暖气等。2011年,这里焚烧了约13.34万吨垃圾，发电量达到1910万千瓦时，卖电286万千瓦时,收入达到2340万日元。

据介绍,仅在大阪,像大正这样的垃圾处理厂还有7家。在全日本,众多城市垃圾焚烧处理厂的良好运营,对避免“垃圾围城”“垃圾填埋场污染水源”等问题有重要意义。

德国垃圾“零填埋”

德国环境部发言人沙夫施韦特日前在接受新华社记者采访时说,实际上,德国已实现社区里的垃圾“零填埋”。对于实在无法回收的垃圾，焚烧起到了十分重要的作用,用沙夫施韦特的话说,焚烧成为德国垃圾处理的“支柱”。

欧盟统计局数字显示,2011年德国所有社区垃圾中,45%回收利用,37%焚烧,余下的基本上转化为堆肥。

既然严重依赖垃圾焚烧,却几乎没有垃圾填埋，德国是如何把全国巨量垃圾进行回收和分拣的呢?

沙夫施韦特说,首先,德国有着严格的垃圾分类标准,有机垃圾、纸张、包装、残余废物等都有自己的专属垃圾箱,民众对垃圾分类是垃圾分拣的第一道程序。也正因分类清晰,不可回收的残余废物很快被直接拉走,它们通常相对干燥,热值较高,方便采取焚烧方式处理。

针对垃圾焚烧设施可能排出的废气废水,德国依靠《排放保护条例》《水法》等法律法规设定排放标准。例如，德国《排放保护条例》第17条就废气中二噁英、呋喃和汞等成分作出严格限定。

沙夫施韦特说,实际操作中,焚烧设施的排放往往比上限值低出不少。废气排放由焚烧设施运营商在网上向有关负责部门汇报。另外，焚烧设施运营商还要将废气测量数据等结果公布在每年的环境报告中,数据得到政府专门机构的监测。

沙夫施韦特说，垃圾焚烧可用于产电、产热、产蒸汽。焚烧后的灰渣部分可被加工成修路材料等。因此,只要做到安全可靠,垃圾焚烧是一举多得的大好事。

《科技日报》2014.2.28 文/蓝建中 郭洋