无解的最强加密方法被证实存在

构建无法破解的密码,是众多密码学科学家的目标。一种被称为不可区分混淆(iO)的加密方式因为太过完美,多年来被认为无法实现。不过最近,3名研究者首次证明了不可区分混淆是可行的,这或许是通往完美密码的重要一步。

程序混淆保护代码

为保护代码,人们往往会在导出程序之前采取一些手段来混淆这些程序,现在一般有两种常用的程序混淆方法,即代码混淆和代码编译。代码混淆是在导出程序时,将所有标注性的符号摘除掉;代码编译则是输出编译后的代码,将人们可以看懂的源代码转换成只有电脑看得懂的机器码。程序混淆可以支持大量实际应用,但它包含未加密密码,因此易受攻击。

而虚拟黑盒(VBB)曾被誉为真正意义上的混淆,如果实现虚拟黑盒,用户可以使用程序却无法理解程序本身,那么就能让开发的程序永远不被破解,或是很简单地实现公钥加密。密码学中几乎所有比较高级的构造都可以非常简单地用虚拟黑盒实现。但虚拟黑盒的概念提出不久后,科学家们对这一概念做了系统性的研究,提出了一种特殊构造的程序,并证明其无法被虚拟黑盒混淆。

之后,科学家提出了不可区分混淆的概念,他能够隐藏数据集合和计算机程序的内部工作机制,从而构建一种可以实现几乎所有其他加密协议的加密算法,创造出强大的加密工具。有了强大的不可区分混淆,人们就能完美加密已有的程序,使其永远不会被破解。

探索2.5层多线性配对

对很多计算机科学家来说,强大到如此地步让不可区分混淆看起来难以实现。

2013年,密码学家阿米特·沙海和5位合著者提出了一个不可区分混淆协议,他们将程序拆成几部分,类似拼图,然后使用多线性配对来找出这些拼图。单个碎片看上去毫无意义,但如果将碎片正确地组合到一起,程序就能正常工作。但很快,其他研究者就发现了破解他安全性的方法。

由于多线性配对机制全都有安全性问题,华盛顿大学的林惠嘉开始探索通过约束多线性配对的层数来实现不可区分混淆,并在前几年想出了如何用30层多线性配对构建不可区分混淆。之后,林惠嘉、阿米特·沙海和其他研究者逐渐想出了只用3层多线性配对来实现不可区分混淆。表面上看,这是一个巨大的进步。但从安全的角度来看,3层多线性配对和其他任意层一样不稳固。

最终,他们与加州大学圣巴巴拉分校的普拉汉汉·安纳思、区块链项目Concordium的克里斯蒂安·马特一起,想出了一个折中方案:既然不可区分混淆需要3层,但从安全的角度出发需要2层,那么是否存在一个位于中间的2.5层?

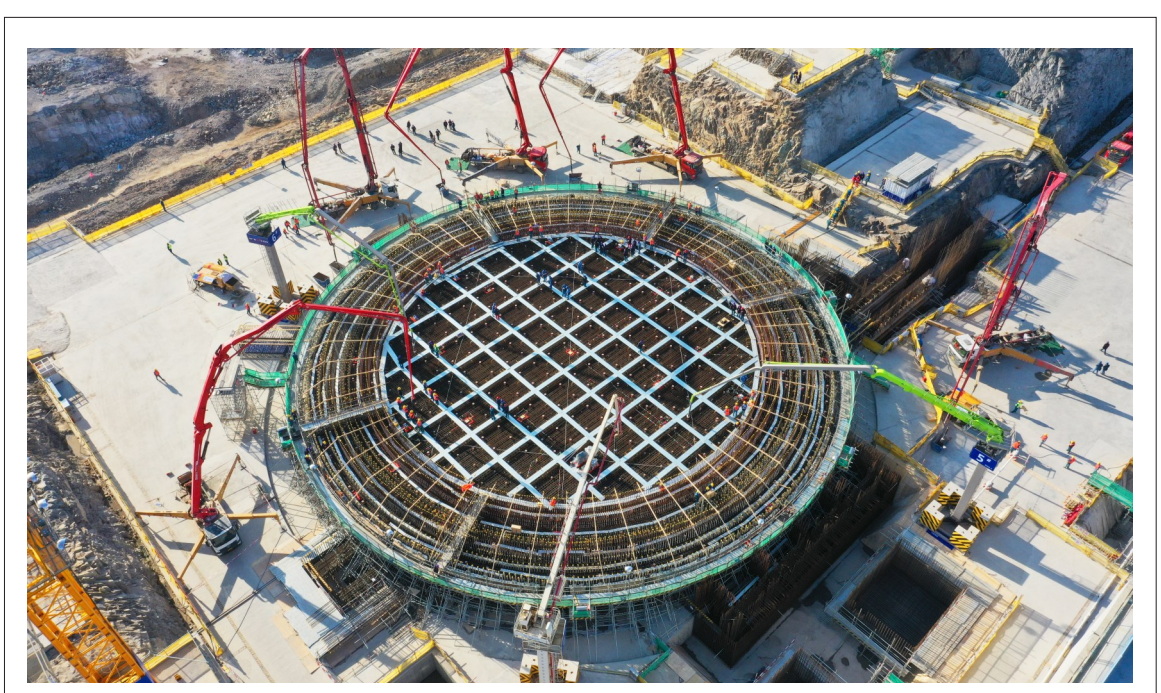
未来有望实际应用

前不久,加州大学洛杉矶分校的研究生杰恩与林惠嘉、阿米特·沙海一起证明了这种方法的可行性。他们在网上公开的论文里,首次展示了如何仅用"标准的"安全假设来构建不可区分混淆。"他们的结果看起来几乎是完美的。"康奈尔大学的拉斐尔·帕斯说。

以色列理工学院的尤瓦尔·伊沙伊预测,他们的这项成果可能会吸引更多新的研究者进入该领域,并且在之后会为了使该方案更加实用而做出一些新的尝试。只不过在协议或是其变体可实际应用之前,计算机科学家还有许多的工作要做。但研究人员表示这都是在意料之中的。

哈佛大学的博阿兹·巴拉克也表示,该协议从理论突破到实际应用还有很长一条路要走,但可以想象,或许50年后的密码学教科书上会说:"这里有一个很简单的不可区分混淆构造,我们能从中得到所有其他加密协议的加密算法。"

(本报综合)



2020年12月31日,浙江三澳核电项目1号机组主体工程正式开工。

浙江三澳核电项目规划建设6台我国自主三代核电"华龙一号"机组,一次规划,分期实施。"华龙一号"是我国具有自主知识产权的三代核电技术,该技术充分利用了我国近30年来在核电站设计、建设、运营及研发等方面所积累的技术和人才优势,吸收了国内外压水堆核电站设计、建造、运行的成功经验,创新采用了能动与非能动相结合的安全设计理念。目前,中广核在建核电机组达7台,装机容量821万千瓦,在运核电机组24台,装机容量2714万千瓦。　新华社记者　王丰　摄

我国学者成功研制"按需式读取"的可集成固态量子存储器

新华社合肥电(记者　徐海涛)信息的存储与读出时间对构建量子网络非常重要。近期,中国科学技术大学郭光灿院士团队在该领域取得重要进展,团队中的李传锋、周宗权研究组首次研制出"按需式读取"的可集成固态量子存储器。

量子存储器是构建大尺度量子网络的核心器件。而按需式读取,是指光子写入存储器以后再根据需求决定读出的时间,这对实现量子网络中的同步操作等功能至关重要。但目前国际上已有的可集成固态量子存储器均基于简单的原子频率梳方案,读出时间在光子写入之前预先设定,无法按需读取。

李传锋、周宗权研究组长期致力于固态量子存储器研究,近年来发展了激光直写技术,在稀土掺杂晶体上制备可集成量子存储器。近期,为实现按需式读取,他们采用了一种改进的量子存储方案,即电场调制的原子频率梳方案,通过引入两个电脉冲可实时操控稀土离子的演化,从而控制存储器的读出时间。

使用飞秒激光等技术,研究组首次研制出按需式读取的可集成固态量子存储器,存储保真度达到99.3%±0.2%,表明其具有极高的可靠性。

该成果对实现大容量量子存储和构建量子网络都有重要意义。国际知名学术期刊《物理评论快报》日前发表了该成果。

研究人员开发出可用于制造锌空气电池的新化学成分

随着人们对绿色汽车和动力源需求的增加,全球研究人员正在努力发明新型电池,这些新型电池可以储存更多的能量,并允许车辆每次充电行驶更长时间。现在研究人员正在探索的新电池技术之一,就是锌空气电池(ZAB),不过,锌空气电池不够稳定的问题是他们面临的最大挑战。

由于锌空气电池的碱性电解质中会有寄生或副反应,如枝晶形成和空气电极失效,可能会导致电池失效。不过,研究人员现在已经解决了这一问题,他们开发了一种使用非碱性水电解质的新型电池化学成分,这种新的化学反应克服了寄生反应。

非碱性电解质采用了一种可逆的过氧化锌化学成分,与传统的强碱性电解质相比,新开发的非碱性电解质具有多种优势,优势包括锌阳极的使用效率更高、化学稳定性和电化学可逆性更强。目前的锌空气电池由于有水的参与,利用的是缓慢的四电子氧化还原反应。然而,利用锌盐与疏水性阴离子三氟甲磺酸能够去除空气阴极表面的水,使空气阴极在稀释的水电解质中发生高度可逆的2e ORR反应。

研究人员表示,由此产生的锌空气电池可以在常规空气环境中稳定运行320个循环和1600小时。研究人员明确表示,虽然锌空气电池是一种潜在的替代电池技术,与目前的锂离子电池相比具有优势,但该技术还需要更多的研究和优化。

(本报综合)

高精度3D打印仅需数秒

体积增材制造(VAM)技术可以直接通过光将液态前驱物直接固化,实现一次成型。科学家对这一方法进行了改进,改进后能以最高达每秒55立方毫米的凝固速度打印固体物质,且分辨率最高可达25微米。研究人员通过一种全新的Xolography技术,即两个不同波长的、交叉的X射线来加固物体。第一个光束是具有一定厚度的矩形光,能够穿过并激活溶解在树脂中的双色光引发剂分子(DCPI);第二个光束能将要打印的物体切片图像投影到光片的平面中,使得光引发剂分子能引发树脂的聚合反应,使其固化。相比于其他的3D打印方法,这种新方法不需支撑结构,打印材料的质量更高,且通过简化步骤提高了效率。　(本报综合)