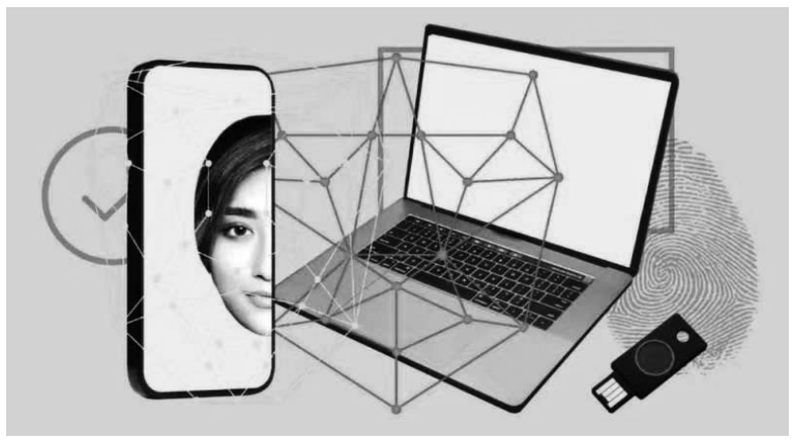
终结“口令”：信息安全的最终盾牌

——2022年度全球十大突破性技术解读（一）

编者按 自2001年起，美国《麻省理工科技评论》杂志每年评选出年度全球十大突破性技术，不少当年崭露头角的技术，如今已深刻改变我们的生活，推动了人类社会的进步。今年评选出的突破性技术包括终结“口令”、长时电网储能电池、AI 蛋白质折叠、除碳工厂。本报自今日陆续刊登2022年该杂志评选出的年度“突破性技术”和相关专家所作点评，以飨读者。



终结“口令”技术入选“全球十大突破性技术”（图片来自MIT Technology Review官网）

20世纪60年代，“口令”（Password，俗称“密码”）最早被图灵奖得主费尔南多·科尔巴托教授用于大型机的本地文件访问权限。20世纪90年代，互联网开始进入千家万户，“口令”也在互联网世界得到广泛应用。随着网络账号增多，用户为了方便记忆倾向使用流行“口令”、在“口令”中使用个人信息、在多个账号重用“口令”，导致严重的安全隐患。

自2000年以来，数以百计的新型身份认证方案陆续被提出。其中，无“口令”方案近年来受到企业的青睐，比如谷歌、苹果、微软等公司，都为用户提供了无需输入“口令”就能登录应用和服务的身份认证方案：在无“口令”身份认证方案中，要么用户拥有一部带摄像头或指纹识别器的移动设备，并安装相应的身份认证应用程序；要么用户拥有专门的硬件设备，以存储身份认证所需的密钥及算法参数。

当前无“口令”身份认证方案仍在初级阶段，面临可扩展性低、部署成本高、隐私泄漏等挑战。在可预见的未来，“口令”仍将是最主要的身份认证方法，无“口令”方案可能会使普通用户对“口令”的直接接触变少，但“口令”仍在幕后保护着我们的网络与信息安全。

点评专家

马建峰（西安电子科技大学网络与信息安全学院教授 ）

汪　定（南开大学网络空间安全学院教授、密码科学与技术系主任，天津市网络与数据安全技术重点实验室副主任）

陈晓峰（西安电子科技大学网络与信息安全学院教授）

身份认证是保障网络安全的第一道防线，“口令”是最常用的身份认证方法。近年来频频发生的大规模“口令”泄露事件，为黑客和不法分子破解用户账号“口令”提供了源源不断的信息，引起人们对“口令”安全性的担忧。在这一背景下，美国Okta、Duo等面向企业用户的公司，微软、谷歌等面向个人用户的公司，都为用户提供了无需输入“口令”就能登录应用和服务的身份认证方案，引起社会广泛关注。实际上，这是终结“口令”的第二次浪潮。

20世纪90年代以来，随着互联网服务，如电子邮件、电子商务、社交网络蓬勃发展，“口令”账号越来越多。为方便记忆，用户倾向使用流行“口令”，在“口令”中使用个人信息，如姓名、生日，在多个账号间直接重用或简单修改后重用“口令”，导致严重的安全隐患。在攻击者的计算能力不断增强这一背景下，自2000年开始数以百计的新型身份认证方案陆续被提出。

2004年，时任微软董事长的比尔·盖茨，就对外宣称微软将不再使用“口令”，掀起了终结“口令”的第一次浪潮。微软与当时世界最大的安全公司RSA合作开发了一种名为SecurID的技术，这种技术本质上是一种“硬件设备+验证码”的双因子认证。与此同时，微软还开发了一种名为“tamper-resistant”的生物ID卡识别技术，本质是一种“生物特征+硬件设备”的双因素认证。随后，学术界陆续指出“安全的‘口令’记不住，能记住的‘口令’不安全”的问题，提出了数以百计的各类新型身份认证方法，如基于生物特征、行为特征的认证，基于图形“口令”的认证和单点登录等。

出乎意料的是，始于2004年的这波终结“口令”的浪潮，到2009年左右逐渐悄无声息了，“口令”的地位不仅没有被撼动，反而得到了更广泛的应用。

当前，无“口令”身份认证方案仍处于初级阶段，还存在明显的缺陷：一方面仅在大型公司的少数平台和设备上应用，未考虑旧版本的系统和不使用智能手机的人群；另一方面由于需要特定版本的系统或平台导致可扩展性低，涉及硬件导致部署成本高，生物特征的不可更改性导致存在隐私泄漏风险。此外，无“口令”认证方案降低了用户对身份的控制权，52%的被调研用户表示不接受把信任链条传递到手机等设备。截至2022年2月，78%的微软云服务企业用户仍将使用账号名和“口令”登录，只有22%的用户启用了基于“口令”的多因素认证或无“口令”方案。

在未来的日子里，“口令”仍将是最主要的身份认证方法之一，是一种应急认证手段。

（本文摘自国家自然科学基金委员会《中国科学基金》2022年第3期MIT Technology Review 2022年“全球十大突破性技术”解读，内容有删节）

科技已全面赋能竞技体育

□ 科普时报记者 项铮

现代竞技体育比赛不仅是各国运动员速度与力量的竞技场，同时也是世界各国展示形象、尖端科技与体育融合的大舞台。“优秀的运动员从选材到出成绩大概需要10年时间，要想成为奥运会级别的冠军，更需要科学性、系统性、个体化的训练。”国家体育总局科学研究所特聘专家、中国体育科学学会学术委员会副主任委员陈小平在近日由上海人工智能研究院主办的“AI+体育”专题研讨会上如是表示。

运动训练科学研究正在由比赛向训练转移

陈小平说，当前科技助力竞技体育主要表现在两个方面：运动关键环节的重大创新突破和运动训练科学化水平的整体提升。

什么是训练科学化？陈小平介绍说，训练科学化在于通过可智能穿戴、便携式等测试装备快速反馈影响运动表现的各项指标，通过数据计算搭建运动模型，最后应用于训练负荷过程中。

陈小平认为，运动训练科学化研究正在由比赛向训练转移，小数据向大数据发展。由于运动训练对科技安全、准确、稳定、便携以及实时反馈的要求非常高，导致很多科技水平很高的产品在辅助运动训练中的应用效果并不理想，这也是目前需要科技界、体育界共同思考的问题。

以数字化为基础的智能体育已成热点

上海交通大学体育系长聘助理教授柳文希表示，随着计算机技术的飞速发展，以数字化为基础、网络化为条件、智能化为核心的智能体育已成为热点。

“运动员素质检测就是基于人工智能技术。”柳文希说，运动员的身体素质检测系统可以在运动员选材、伤病分析、运动训练等方面，对生理和心理指标进行分析，通过测试确定运动员的身体素质和心理能力，为后续进行更好的个性化训练提供科学的依据。

在竞技体育的运动训练当中，同样要借助大量的人工智能相关的技术：借助360度全景视频或虚拟现实技术，构建出沉浸式、数字化的虚拟运动训练环境，有助于运动员模拟实际比赛条件进行练习，从而大大减少因练习而损伤身体的风险；也可通过计算机视觉技术引入智能运动系统，利用人工智能建模获取大量运动员信息和运动信息，根据运动员的特点制定比赛战术。

构建高层次的竞技体育科技创新平台

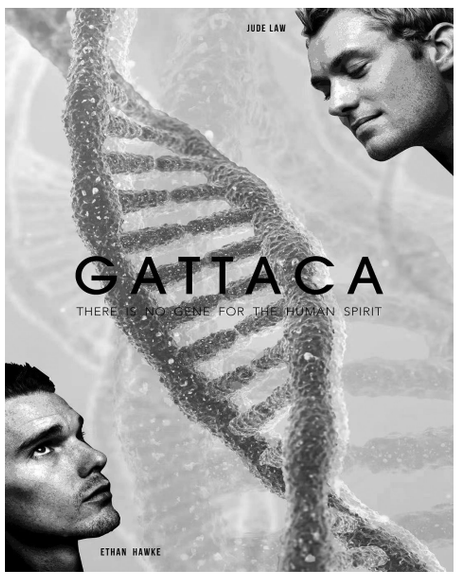
柳文希强调，要增强竞技体育训练的科技创新意识。他认为，竞技体育取得好成绩不仅仅是运动员个人能力的表现，也是国家、团队、集体力量的结晶。

柳文希认为，在我国多层次人才培养体系中，需要从上到下开展科技助力体育竞技。竞技体育应从思想上改变运动员的意识，使他们善于运用科学工具提升训练效果。

柳文希建议，要构建高层次的竞技体育科技创新平台，加强融合人工智能、物联网、大数据、云计算等多领域的体育科技协同创新平台建设，以竞技体育应用型研究为主攻方向，充分发挥科技创新中心优势，整合相关机构的技术与人才，以重大科研项目联合申报、重点研究领域优势力量交叉融合等多种形式开展有效合作，促进科研成果有效转化和利用，提升科技在竞技体育发展中的贡献率。

基因技术也不可超越伦理道德

□ 卢志浩



《千钧一发》电影海报 （图片由作者提供）

好的科幻电影历久弥新，不会过时。科技的发展不仅不会让一部经典的科幻电影失色，反而会让人们在新的科技背景下对影片内容产生更深入的思考、更现实的讨论。《千钧一发》就是这样一部常看常新的经典科幻电影。

《千钧一发》上映于1997年。在电影演绎的未来世界中，基因技术发达，经过基因筛查和编辑诞生的人英俊、健康、聪明，而自然受孕降生的人因具有各种基因缺陷，则有可能会增加患先天疾病或某种疾病的概率，还会使预期寿命缩短。在这个社会里，人们通过基因的优劣来判断一个人的优劣，基因优秀的人才有资格获得好工作，担任重要职位。

影片主角文森特是一位由父母自然孕育的人，由于基因缺陷而患有近视和心脏病，并被医生判定活不过30岁。他梦想进入招募航天员的戛塔卡公司，期望成为一名宇航员进入太空旅行，但戛塔卡公司只招收“基因精英”，于是他与基因完美却因事故致残的杰罗姆进行了一次交易，利用后者的血液和尿样等进入了戛塔卡公司。在付出了远超他人的艰苦努力后却遇到了预料之外的事——被卷入了一场发生在戛塔卡公司的命案。

从今天的视角来看，在某种程度上构建电影中描绘的未来世界所需的基因技术已经基本实现，比如我们已经在临床上应用的第三代试管婴儿技术。这种技术是在试管婴儿技术的基础上，利用基因技术对胚胎的遗传物质进行染色体或基因分析，选择染色体数目和结构正常、不具有遗传病基因的胚胎进行移植，帮助夫妻孕育健康的宝宝。目前，这类以规避遗传病、生育健康宝宝为目的的基因诊断，是社会认可与支持的。但未来社会如果超越了这个范畴，当基因技术向身体特征定制发展，开始致力于创造比一般婴儿更加健康、更加优秀的婴儿时，基因歧视就有可能成为现实，世界就有可能向着影片《千钧一发》所描绘的样子发展。

让我们换个角度来思考，拥有基因缺陷的婴儿就没有存在的意义吗？在工作和生活中，先天基因更重要，还是一个人的态度和努力更重要？拥有缺陷基因的人就不可能取得与拥有健康基因的人一样，甚至更高的成就吗？要知道，爱因斯坦患有阅读障碍，梵高患有精神疾病，周杰伦患有强直性脊柱炎……这些疾病都有遗传因素，如果他们在最初被父母抛弃，那么这个世界在少了病患的同时，也少了如此优秀的科学家、画家、音乐人……

影片最后发生在戛塔卡公司的命案真凶落网，文森特摆脱了杀人嫌疑，并且凭借自己的顽强、勇敢、真诚赢得了身边人的理解与支持，最终成功登上了前往泰坦星的宇宙飞船，挣脱了基因歧视的枷锁，实现了自己的太空梦想。

审视基因技术，影片中的一句台词道出真谛：“命运是没有基因的”。重视个人的品德、努力而非出身，尊重每个人的梦想并为所有人提供同等的机会，是这部影片留给我们的深刻启示。

（作者系中国科技馆展品技术部工程师）

媒眼看世界 栏目主持人：任贺春

未来，这些产业将颠覆我们的认知

（上接第1版）

“光辐降温技术可以在衣服纱线上添加对太阳光全波段反射的物质，直接反射紫外线和红外线。”姚蔚铭说，这种技术可让夏季的衣服穿起来不仅防晒还非常凉快。

到了冬天，人们对服装的要求无外乎是既轻薄又保暖，而这对传统服装材料而言就是个悖论，哪件羽绒服不是很轻很保暖但也很臃肿呢？

“改变，均源自科技创新。”姚蔚铭说，北京冬奥会上有的国家的队服就使用了一种特殊的面料，纱线会随着温度变化而自动收缩，从而控制羽绒服面料的蓬松度，这样衣服就能在室外有很好的保暖效果，在室内也不会觉得闷热。

智能终端更具“主观能动性”

AI技术发展已有几十年了，但智能终端设备的“主观能动性”提升并不是很快。

“5G时代的高可靠低延迟通信技术，基于分布式优化算法可以让终端智能设备自组网解决局部的人工智能问题。”牛津大学在读博士潘周聃接受记者线上采访时表示，多智能终端的协同问题，可以不用依赖通过把所有数据上传给中央服务器就能得到解决。

AI领域的解决方案多是需要一个极为高效的中央服务器，事无巨细地控制和安排着每一个智能终端。这种方式带来的问题，就非常考验中央服务器端高并发通信能力及其统筹全局的计算能力，而这两个能力挑战会随着机器人数量的增多而非线性地激增。

潘周聃说，分布式优化算法的核心架构是通过分布在智联体自身独立的“运算单元+彼此间通信”，迭代出一个解决局部问题方案。“与中心化服务器架构相比，这样的分布式算法并不需要把所有信息都分享出去，也不需要将信息时时刻刻传送给中央服务器，不给服务器算力添麻烦。”

当前，分布式优化算法面临的挑战首先是需要每台智能设备拥有足够智能，同时还需要一个延迟低的点对点通信，来加速沟通迭代的过程。前者随着最近10年移动互联网技术的发展，带来大量优秀的低功耗高性能智能终端设备处理芯片；后者在5G时代已经渐渐成为可能。

“随着芯片技术以及通信技术的进一步发展和迭代，AI未来必将给我们带来更多惊喜。”潘周聃展望道，未来的自动农业无人机可以结伴而行，自主组队规划路径完成农药喷洒任务；风电光电设备与当地的家庭、工厂组网，并一起完成发电、供电任务；高速公路上，无人驾驶汽车自主构建“车联网”有序地行驶……

面对婴儿人们会自然改变发声语调

（视觉中国供图）

科普时报讯（记者**吴桐**）施普林格·自然旗下专业学术期刊《自然·代谢》日前发表一项研究指出，在面对婴儿说话或唱歌时，不同文化背景的人们发出声音的方式是一致的。该研究结果表明，人们对婴儿说话或唱歌的方式可能具有一个共同的经过演化的功能。

婴儿指小于1周岁的儿童。婴儿在这个阶段生长发育特别迅速，是人一生中生长发育最旺盛的阶段，体重大约为9000—10000克。

来自对许多不同动物的研究结果表明，这些动物发声通常具有清晰的功能，比如能提醒同伴注意附近捕食者的报警声。之前对人类开展的一项研究表明，唱摇篮曲以及父母说话方式都对婴儿具有安抚作用，说明这种发声方式或许还有一个共同的功能，但对此跨文化背景的证据一直很有限。

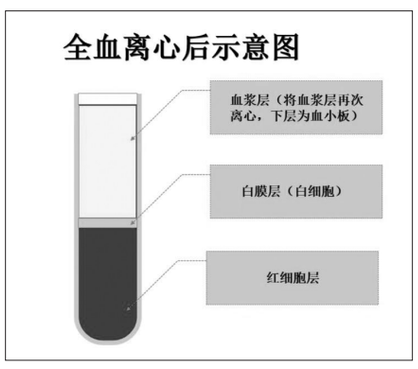
论文作者和同事收集了六大洲1615份人们说话和唱歌的录音，并利用计算机分析研究了面对成人和面对婴儿发声的声学特征差异后发现，面对婴儿和面对成人的录音之间，始终具有不同的声学特征，比如面对婴儿时说话音色更纯净，歌声更柔和，说话的音调也更高。在对187个国家51065名讲英语的人播放了这些录音后，发现听者能猜出哪些发声是对婴儿的，准确率超过了偶然概率。

这项研究结果增进了我们对人类语言和唱歌的理解，提示了人类在不同文化背景下，面对婴儿说话或唱歌时改变发声方式具有高度一致性，能被普遍识别，而且这种发声方式可能具有相同的功能。

国际前沿

血液为什么不能一次大量采集按需使用

□ 文/图 聂东航



食品都有保质期，血液是否也有保质期？能否像粮食一样保存起来，在几年内按需使用？答案是否定的。这是因为血液是包含血细胞和血浆的混合物，每种血液成分的保存期各不相同。除了血浆外，红细胞血液成分、冷沉淀、血小板制剂、冰冻红细胞等其他细胞成分保质期都在5—35天以内。

分离全血后，加入一定量有营养血细胞功能的添加剂就可得到浓缩的红细胞，目前国内普遍采用全密闭多联袋采血袋制备，在4±2℃条件下储存，红细胞保存期为35天。

血浆根据分离时间、储存方法的不同，分为新鲜液体血浆、新鲜冰冻血浆、普通冰冻血浆。新鲜液体血浆是将全血在采集后6小时内分离得到的只含血浆成分的血液制剂，保存期不超过24小时。新鲜冰冻血浆是将全血在采集后6小时内分离，并在−20℃下冻结的血浆制剂，在−20℃条件下保存期为1年。普通冰冻血浆含有稳定的凝血因子和血浆蛋白等成分，和新鲜冰冻血浆的区别是缺乏不稳定的凝血因子Ⅷ和Ⅴ，在−20℃下保存期为4年。

冷沉淀是从新鲜冰冻血浆中分离出来的富含第八凝血因子的血液制剂，在−20℃以下保存期为1年。

机采浓缩血小板，在22±2℃并摇荡的条件下可保存5天，在低温或超低温条件储存的冷冻血小板保存有效期较长，实际中未普遍采用。

实验证明，在−150℃以下，生物细胞几乎所有的生物学行为或者物理化学变化都将不再进行，因此人们将红细胞保存在−80℃条件下冰冻起来，其保存期可延长至10年。不过，冰冻过程必须添加甘油作为冰冻保护剂，而添加甘油和清除甘油的过程会造成红细胞损失，使用前因为需要解冻也影响了输血及时性。因此除稀有血型红细胞外，常规血型红细胞不采用这一方式保存。

临床上用于急救的红细胞类血液制剂，现阶段无法实现长期保存。血液的保存时间限制了血库的最大库容量。以武汉为例，按照可供20天用血的需求测算，红细胞类血液制剂最高库存为两万单位（400万毫升）；按3.5天用血量测算，血小板制剂的最高库存为650个治疗量。

在气候适宜的春秋季节，献血人数增加，血液库存会逐步达到最高值，这时则需要请爱心献血者延期献血，而在冬夏季血液库存也会降到低点。了解到这一规律后，很多团体单位和固定献血者已将无偿献血时间定在每年的一二月份和七八月份，这种做法有利于保持献血量和用血量的平衡，让每份献血都转化为拯救生命的能量。

（作者系武汉血液中心副主任医师）

十万个为什么 foooodwhys 新“十万个为什么”