

融入思政的网络空间安全前沿技术教学探索

胡爱群, 李古月, 彭林宁, 李涛

(东南大学网络空间安全学院, 江苏 南京 210096)

摘要: 探讨在讲授网络空间安全新技术时融入思政元素的教学方法。以量子通信、公钥基础设施、物理层安全、区块链、可信计算、隐私保护6个方面技术为教学内容, 在讲授新技术的同时, 分析我国科技人员的奋斗历程、研究成果以及未来目标。组织学生分工协作, 交流学习体会, 探寻科研规律, 使学生不仅可以吸收最新技术知识, 还可以掌握攻克科学问题的方法及所需的科学政治素养。为研究生课程思政的教育教学方法可以提供有益参考。

关键词: 网络空间安全; 课程思政; 教育教学; 安全新进展

中图分类号: G642

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019026

Exploration of teaching method incorporating ideological elements for the cutting-edge technology of cyberspace security

HU Aiqun, LI Guyue, PENG Linning, LI Tao

School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China

Abstract: The teaching method was explored incorporating ideological elements for the advanced technology of cyberspace security. The teaching content of this course is constituted of six aspects, i.e., quantum communication, public key infrastructure, physical layer security, blockchain, trusted computing and privacy protection. Apart from teaching the related technologies, the remarkable achievements and efforts of Chinese scientists were shown and the future work was indicated. Students are grouped to do literature research, expand their knowledge, exchange the learning experience and explore the law of scientific research in these new aspects. Students can not only absorb the knowledge of cutting-edge technology, but also learn the method and spirit to address scientific problems. A useful reference for education and teaching method of course ideological for graduate students was provided.

Key words: cyberspace security, ideological elements, course teaching, advanced technology of security

收稿日期: 2019-03-09; 修回日期: 2019-04-26

通信作者: 胡爱群, aqhu@seu.edu.cn

基金项目: 东南大学研究生“课程思政”示范课程建设基金资助项目; 教育部科学事业费重大基金资助项目

Foundation Items: Constructing Model Teaching Course of Graduate Students “Courses for Ideological and Political Education” in Southeast University, Key Foundation of Scientific Operating of the Ministry Education

论文引用格式: 胡爱群, 李古月, 彭林宁, 等. 融入思政的网络空间安全前沿技术教学探索[J]. 网络与信息安全学报, 2019, 5(3): 54-66.

HU A Q, LI G Y, PENG L N, et al. Exploration of teaching method incorporating ideological elements for the cutting-edge technology of cyberspace security [J]. Chinese Journal of Network and Information Security, 2019, 5(3): 54-66.

1 引言

当今世界,网络信息技术日新月异,全面融入社会生产生活,深刻改变着全球经济格局、利益格局、安全格局。网络信息技术加快了社会发展步伐,同时也给各行各业带来越来越多新的安全问题。网络安全和信息化是相辅相成的。安全是发展的前提,发展是安全的保障,安全和发展需要同步推进。从世界范围看,网络安全威胁和风险日益突出,并日益向政治、经济、文化、社会、生态、国防等领域传导渗透。特别是国家关键信息基础设施面临较大风险隐患,网络安全防控能力薄弱,难以有效应对国家级、有组织的高强度网络攻击。网络安全成为全球技术创新的竞争高地与大国博弈的重要筹码。

1.1 网络空间安全与课程思政

网络空间的竞争归根结底是人才的竞争。习近平总书记多次强调网络安全人才的重要性,网络安全人才已成为国家竞争的核心所在。保卫网络空间国家主权已成为国家重要战略,打赢网络空间斗争的关键是人才,而教育在人才竞争中处于基础地位。习近平总书记要求“加强网络空间安全人才建设,打造素质过硬、战斗力强的人才队伍”。人才队伍的建设很大程度上依赖于我国高等学校的培养。高等教育的一个核心任务是培养德智体美全面发展的人才,根基在于立德树人。习近平总书记在全国高校思想政治工作会议上明确指出,要坚持把立德树人作为中心环节,把思想政治工作贯穿教育教学全过程,实现全程育人、全方位育人;中共中央、国务院《关于加强和改进新形势下高校思想政治工作的意见》指出,要将思想价值引领贯穿教育教学全过程和各环节,要加强对课堂教学和各类思想文化阵地的建设管理,充分挖掘和运用各学科蕴含的思想政治教学资源。“课程思政”理念正是对上述要求的积极回

应,也是当前形势下深化高校思想政治教育改革、全面提升教育实效所进行的有益尝试。高等教育以人才培养为核心,以立德树人为根本,其重心是实现学生德智体美全面发展。这一目标的实现有赖于高校所有学科与课程的共同作用,需要各类课程的协同合作,发挥思想政治教育作用。

近期,多位学者对思政课程和课程思政进行了探讨^[1-2],但是尚未涉及网络空间安全领域的课程改革研究。与传统领域不同,网络空间安全领域的人才需要有正确的价值观和职业操守;另外,该领域的人才不少是“怪才”“奇才”,他们往往不走一般套路,有很多奇思妙想。尽管这些人才在技术方面实力超群,但在思想政治方面往往并不成熟。此外,我国是科技人才资源最多的国家之一,同时也是人才流失比较严重的国家,其中不乏顶尖人才。因此,网络空间安全专业的课程不仅需要介绍突破网络发展的前沿技术和具有国际竞争力的关键核心技术,还应当做好学生思想引领和价值观的塑造工作。

1.2 《网络空间安全技术新进展》课程简介

《网络空间安全技术新进展》是东南大学网络空间安全学院的博士生专业学位课程及硕士生的选修课程,重点讲解和研讨网络空间安全的最新国际、国内技术进展,是一门与时俱进的课程。

课程的主要教学目标如下。

- 1) 帮助学生了解网络空间安全技术的发展历史与沿革。
- 2) 培养学生的国际化视野,了解网络空间安全技术中“量子通信、公钥基础设施、物理层安全、区块链、可信计算、隐私保护”等新技术的主要内容和国内外研究动态。
- 3) 培养学生的创新能力、分析能力以及解决问题的思维能力。
- 4) 培养学生追求科学真理、热爱祖国、为保护网络空间安全努力奋斗的情怀。

在近几年的教学研究中,团队结合思政育人的目标,不断探索网络空间安全技术的前沿进展以及其中所体现的人文与科学思想。在授课过程中注重发挥深化和拓展作用,在知识传授中强调主流价值引领,挖掘课程中蕴含的“思政元素”。通过关键环节的案例设计和课程教学、研讨互动,帮助学生树立科学的发展观、提升社会责任感与家国情怀,进而增强学生投身创建世界一流的网络空间安全事业的荣誉感和使命感,具体包括以下内容。

1) 让学生了解我国在网络安全技术方面的需求、已取得的成果,以及与世界先进国家的差距,鼓励学生树立奋起直追的意识。

2) 增强学生在网络命运共同体、网络空间治理、网络强国等方面的责任和担当。

课程特别讲述我国在量子通信、公钥基础设施、可信计算等方面的最新技术成果与应用,打牢思政基础。此外,注重贯彻我国领导人关于网络安全的重要论述、指导思想以及法律法规,如网络安全法、空间治理强国的论述等。课程在教学方式上也由单纯的讲课方式改革为讲课与研讨相结合的方式,注重学生对课程的参与度,通过学生查找最新文献和技术成果,了解国家网络安全政策、精神,让学生组队研讨并登台讲解,深化对网络安全技术和政策的掌握,起到很好的学习效果,使学生将网络强国思想牢记于心。

本文具体探索网络空间安全技术前沿进展与思政教育的融合路径,把握科学方法,凝聚多元力量,为我国网络安全人才培养积聚力量。

本课程的教学手段主要包括3个方面。

1) 教师授课。讲授精心选择的网络空间安全若干新技术,兼顾前沿性、战略性和思政性。

2) 师生研讨。学生分组找素材、分工做PPT,教师和学生点评,拓展知识面,形成良性思政氛围。

3) 播放思政视频。播放国家战略相关的新闻报道和重大成果报道视频,增强思政权威性。教师进行进一步阐述。

下面具体阐述笔者所在高校在各个技术方向上将思政元素融入技术教学的做法。

2 量子通信技术思政教学

量子通信是量子力学和通信理论相结合产生的交叉学科,是基于量子的纠缠特性和量子态不可复制原理而设计的通信系统。

2.1 量子通信技术研究历程

1970年,美国科学家威斯纳最早想到将量子物理用于密码术。1982年,法国物理学家艾伦·阿斯派克特和他的小组成功地完成了一项实验,证实了微观粒子“量子纠缠”的现象确实存在。量子纠缠证实了任何两种物质之间,不管距离多远,都可能相互影响,不受四维时空的约束。

在此基础上,1993年,美国科学家Bennett提出了量子通信的概念。量子通信是由量子态携带信息的通信方式,它利用光子等基本粒子的量子纠缠原理实现保密通信过程。6位来自不同国家的科学家,基于量子纠缠理论,提出了利用经典的与量子相结合的方法实现量子隐形传送的方案。量子隐形传态不仅在物理学领域对人们认识与揭示自然界的神秘规律具有重要意义,而且可以用量子态作为信息载体,通过量子态的传送完成大容量信息的传输,实现原则上不可破译的量子保密通信。

在2008年8月14日出版的《自然》杂志上,瑞士的5位科学家公布了他们的最新研究成果:他们首次识别出从地球上空1500 km处的人造卫星上反弹回地球的单批光子,实现了太空绝密传输量子信息的重大突破。

我国中国科技大学的潘建伟院士和他的研究团队在2004年、2007年、2012年、2018年先后

实现了五光子纠缠态、六光子纠缠态、八光子纠缠态、十八光子纠缠态的制备与操纵,均居于世界第一位,连续刷新了世界纪录,在量子纠缠研究方面走在了世界的前列。同时,他们很好地完成了长程量子通信中紧迫急需的“量子中继器”的实验与制作,为实现广域量子通信网络乃至全球量子通信网络奠定了坚实的基础。另外,潘建伟院士团队还对远距离量子通信与空间尺度量子实验关键技术进行了验证,2005年在国际上首次实现距离大于垂直大气层等效厚度的自由空间双向纠缠分发,2010年在国际上首次实现16 km自由空间量子态隐形传输,2011年10月至2012年6月在国际上接连首次实现百公里量级的自由空间量子隐形传态和双向纠缠分发,为基于卫星的广域量子通信以及大尺度的量子计算、量子信息技术应用与实施打通了技术瓶颈。

我国在量子密钥分发技术领域处于国际前列。2009年量子密钥分发技术就已经在安徽芜湖电子政务系统中得到实际应用。之后,又在北京银行总部之间的通信系统中得到应用。2016年8月16日凌晨1时40分,我国科学家在酒泉卫星发射中心用长征二号丁运载火箭将世界首颗量子科学实验卫星“墨子号”发射升空,成功入轨运行。这使我国成为世界上首个实现太空和地面之间量子通信的国家,同时也建成了我国天地一体化的量子保密通信与科学实验体系^[3]。

2.2 量子通信技术思政分析

量子通信是我国的战略性信息产业,我国在量子通信领域的产业化进程远超过欧美国家,已处于产业化发展前期。

由国家发展和改革委员会批复的“京沪干线”量子通信项目于2013年7月立项,经过42个月的艰苦努力,突破了高速量子密钥分发、高速高效率单光子探测、可信中继传输和大规模量子网络管控等关键技术,于2016年年底完成全线贯通,连接

了北京、济南、合肥、上海,全长2 000余千米。京沪干线北京接入点将与“墨子号”量子科学实验卫星兴隆地面站连接,全线密钥率大于5 kbit/s,已形成星地一体的广域量子通信网络雏形^[4]。

由以上分析可以看出,量子通信技术的发展经历了以下阶段。

- 1) 自由探索阶段。科学家根据自己的强烈兴趣,探索量子纠缠现象和量子隐形传态机理。
- 2) 群体攻关阶段。多个国家的科研团队,进行联合实验,探索在自由空间量子传输的可能性。
- 3) 国家立项阶段。国家根据战略预判,将量子通信作为发展战略,以国家重大项目的方式组队攻克系统性和应用性难题,以期推进信息产业跨越式发展。
- 4) 产业化阶段。研制、测试和批量生产量子通信系统中的各个模块,并针对具体应用环境,构建应用系统。

量子通信是一个典型的通过原创技术引领产业发展的案例。崇尚科学的精神、持之以恒的追求、不畏艰难的素质以及团结协作的精神,是取得成功的关键。我国量子通信技术的进步,不仅表现在技术上取得重大进展,更表现在国际舞台上获得尊重和话语权。

2.3 量子通信教学互动环节

在量子通信的教学中,要求学生研讨的内容如下。

- 1) 国际团队的量子通信研究进展。
- 2) “墨子号”卫星量子通信原理和工程实施情况。
- 3) “京沪干线”量子通信原理和工程实施情况。
- 4) 我国和国际主流媒体对量子通信进展的报道。
- 5) 量子通信的应用及未来发展分析。

学生的PPT报告拓展了量子通信全球研究动

态和未来技术走向；播放的主流媒体报道视频传播了我国政府关于量子通信和信息产业跨越式发展的正面宣传。

本节的教学增强了学生的民族自豪感，激发了学生勇于创新、不畏艰辛的潜能。

3 公钥基础设施技术思政教学

3.1 公钥基础设施技术发展历程

在绝大多数信息系统中，为了保障信息安全，需要对用户和实体进行身份认证、保护信息传输的机密性和完整性、对用户的操作进行非否认鉴别等。这些共性的安全机制和措施，一般可以基于或借助公钥密码技术达到，由此形成了公钥基础设施（PKI，public key infrastructure）。

公钥密码技术为在大规模群体间实现密钥分发管理、安全通信和非否认服务等提供了可能。公钥基础设施技术基于公钥密码技术发展而来，它以数字证书方式为用户提供身份证明和授权服务，以及一系列延展服务（如时间戳等）。服务机构称之为 CA（证书认证机构），已广泛应用于电子政务和电子商务中。

PKI 的核心技术是：为用户签发数字证书；通过验证数字证书的签名，证明证书的真实性，并进一步证明证书上的公钥属于谁；在多个 PKI 域之间互联时，通过根 CA、桥 CA 或交叉签名等，实现信任扩展。

在 PKI 中涉及多个密码算法标准、接口规范和管理标准，我国已相继颁布了公钥密码算法、对称密码算法、摘要算法、签名算法、随机数算法等系列密码算法，以及与 PKI 管理与接口相关的系列规范、标准等，如在线证书状态协议、证书管理协议、组件最小互操作规范、数字证书格式、时间戳规范、CA 认证机构建设和运营管理规范、安全支撑平台技术框架、电子签名卡应用接口基本要求、XML 数字签名语法与处理规范、

《PKI 系统安全等级保护评估准则》等，为推动 PKI 的应用奠定了坚实的基础。

我国对 PKI 的研究始于 21 世纪初，到目前为止，已形成全套算法和标准体系。在金融、政务、商务等领域，已经建立设施齐全、服务周到、接口便捷、应用丰富的 CA 系统，支撑着我国重要信息系统的安全。

随着 Internet 的普及，人们通过因特网进行商务活动越来越多。电子商务为我国企业开拓国际国内市场、充分利用国内外各种资源提供了良机，真正体现了平等竞争、高效率、低成本、高质量的优势，能让企业在激烈的市场竞争中及时把握商机。发达国家已经把电子商务作为 21 世纪国家经济的增长重点，我国有关部门也正在大力推进企业发展电子商务。但如何保障电子交易的安全尤为重要，如如何保证电子商务敏感信息在公开网络的传输过程中不被窃取、如何保证电子商务中交易信息不被中途篡改、如何保证交易双方身份的正确性、如何保证交易的任何一方无法否认已发生的交易等。PKI 技术为上述问题提供了很好的解决方案。

3.2 公钥基础设施技术思政分析

PKI 技术是电子政务的核心支撑技术。电子政务是指国家机关在政务活动中，全面应用现代信息技术、网络技术以及办公自动化技术等进行办公、管理和为社会提供公共服务的一种全新的管理模式。电子政务是我国信息化深入发展的产物，也是阳光政务的迫切需求。电子政务将岗位职能、办事流程、管理权限等全面优化，并使各项业务进程处于监管状态，大大提高了办事效率，深受百姓和官员的欢迎。同时，电子政务可以促进电子商务与国家税收、金融、进出口等体系的良好对接，加快经济发展，既是信息时代进一步发展的切实需要，也是国家提高竞争力的必由之路。

电子政务经常涉及大量的机密数据，对信息

的有效性、机密性、完整性和修改的不可抵赖性等安全性要求非常严格。但由于网络的开放性和复杂性,各种各样的网络犯罪、网络欺诈和攻击入侵对电子政务的安全性构成了严重威胁。因此,如何构建具有高可信度的电子政务系统是目前政府部门和软件行业急需解决的重要问题。

目前,新型电子政务系统^[5]的安全涉及:应用环境安全;应用区域边界安全;网络和通信传输安全;安全管理中心;密码管理中心。支撑上述各个方面安全的核心是公钥基础设施技术。利用 PKI 技术,可为电子政务的用户进行身份认证,为用户进行授权管理,支撑用户间保密通信所需的密钥分发管理,为用户的操作提供非否认服务等。

PKI 技术在电子政务中的应用,充分保障了电子政务活动的安全性。电子政务改善了传统政务部门林立、条块分割、等级森严、行政信息流通渠道不畅、信息处理手段落后、行政效率低的问题,有效降低了公共成本,有力促进了政府职能转变。

3.3 公钥基础设施技术教学互动环节

在本节的互动环节,希望达到以下目标:开拓学生的国际化视野;掌握公钥基础设施的关键技术;了解公钥基础设施技术在电子政务和电子商务中的信息安全解决方案。

要求学生准备的 PPT 包括以下内容。

- 1) CA 系统介绍。
- 2) 电子政务中的 PKI 应用案例。
- 3) 电子商务中的 PKI 应用案例。
- 4) 我国电子政务建设及成效分析。

在研讨中,播放我国关于电子政务的视频及 CA 系统建设的成功案例,让学生了解 PKI 技术对电子政务的重要性,以及电子政务工程的实施对提升我国政务办事效率和改善民生的效果。

通过本节的教学,学生可了解到我国 PKI 技

术的长足进展和为电子政务、电子商务等实际应用发挥的支撑作用,鼓励学生积极创新,将网络空间安全技术服务于国民经济主战场。

4 物理层安全技术思政教学

4.1 物理层安全技术发展历程

物理层安全技术是一种重要的信息安全技术,它希望利用网络物理层的自然特性(也是独一无二的特性)构建安全体系,保护接入安全和传输数据的安全。物理层安全技术从另一个角度寻找信息安全的解决方案,力图在保障安全性的前提下,使安全管理更简单。

物理层安全技术^[6]自 2009 年左右受到国际上的关注,主要集中在两个方面:从通信设备发射的信号中提取设备指纹信息,用于对设备进行身份认证;从通信线路或无线信道中提取信道特征,并将其转换为对称密钥,用来加密上层传输的数据。经过近 10 年的研究,目前物理层安全技术已较为成熟,有些已经开始应用,主要的研究集中在无线网络方面,如 ZigBee、Wi-Fi、TD-LTE、LoRa 等。

无线通信设备指纹(即射频指纹 RFF)是通信设备的内在物理特征,具有唯一性和难以复制特性,可以作为通信设备的身份特征。由于接收信号中混杂有 RFF 和 CSI,需重点解决 RFF 与 CSI 的分离问题,才能对发射机进行身份识别。目前,已经能够解决在多天线接收条件下,采用 ESPRIT 算法有效分离 RFF 与 CSI 信号^[7]的问题,以及在低信噪比条件下的 RFF 提取问题^[8]。

在信道特征提取方面,重点是提取通信双方上行和下行具有良好互易性的信道特征,对它们进行量化、信息调和以及隐私放大,最后生成双方一致的密钥。由于无线信道的动态性、上下行通信时间的偏差以及信道噪声等因素,要获得良好的信道互易性并非易事。目前,已经提出了主

成分分析法 (PCA) 及酉变换的方法^[9], 有效改善了信道互易性, 并产生出高一致性密钥。目前, 在移动通信情况下, 可产生随时间变化的对称密钥, 每帧密钥量可达到 256 bit, 用于 SM4 等对称密码算法的密钥输入。

无线物理层安全技术可解决无线通信设备的身份认证和无线信道的加密问题, 无须密钥的分发和管理, 特别适合用于自组网、车联网、物联网等密钥分发和密钥更新困难的场合, 用以构建物理安全的无线网络。

尽管目前在无线物理层安全方面已经取得不错的进展, 但仍然有许多问题需要进一步研究, 如: FDD 双工场景下的信道互易性研究及利用问题; 固定通信场景下密钥量不足问题; 面向现代通信巨量天线数的射频指纹提取及信道互易性问题等。

综上所述, 虽然无线物理层安全技术尚不完美, 但其改变了人们对传统安全方式的认知, 并在未来应用中展示出巨大的潜力。

4.2 物理层安全技术思政分析

无线物理层安全技术中的射频指纹识别技术可用来进行无线目标识别。以前, 进行无线目标识别, 一般是以无线目标的 ID 或 MAC 地址为依据, 而这些参数很容易遭到假冒。在开放的无线环境中, 攻击者很容易窃听到合法目标的 ID 或 MAC 地址, 并把自己的地址改为合法地址, 进而伪装成合法目标。黑飞无人机就可能这样做。

在无线目标的敌我识别应用中, 也常常存在这样的需求。为了扰乱和欺骗我方判断, 敌方的目标 (如战机) 可能在通信信号中不断改变身份信息, 以显示有大量战机的存在。传统的方法依靠解调敌方信号中的识别码, 判定敌方的身份, 难以发现这种欺骗伎俩。而射频指纹识别技术是直接识别发射机的物理特征的, 编码可以改变而射频指纹难以改变, 因此可以准确判别敌方是否

改变身份。

另外, 无线物理层安全中提取的信道信息是与通信设备的位置相关的。利用这个信息可以辅助判定敌方的位置是否发生变化。

由上可知, 无线物理层安全技术不仅在车联网等新型网络中具有普适性, 还将在军事应用上发挥重要作用, 不仅可以装备军事通信网络, 还可以应用于敌我识别和电子对抗, 有力提升我国的网络安全防御能力和电子对抗水平。

4.3 物理层安全教学互动环节

本节的互动环节要求学生以创新的思维, 挖掘物理层安全技术新的应用, 特别是军事应用, 查阅的文献内容如下。

- 1) 物理层安全技术国内外研究进展。
- 2) 军事通信对物理层安全技术的需求。
- 3) 射频指纹技术在敌我识别中的应用。
- 4) PUF 技术与射频指纹技术的比较。
- 5) 无线密钥的安全性分析。

选择视频播放内容侧重在军事无线自组网对物理层安全技术的需求、电子对抗系统、雷达目标识别系统等的介绍, 进一步拓展学生对无线物理层技术的应用思考, 特别是运用射频指纹技术做目标识别、运用无线密钥构建安全通信链等。

通过本节的学习, 学生可初步掌握无线物理层安全技术这一崭新的技术及其应用场景, 启发他们对安全解决方案有新的认识和思考。

5 区块链技术思政教学

5.1 区块链技术研究进展

区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构, 并以密码学方式保证不可篡改和不可伪造的分布式账本。它是利用块链式数据结构验证与存储数据、利用分布式节点共识算法生成和更新数据、利用

密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算方式。

区块链针对交易的信任和安全问题,提出了4项技术创新^[10]。

1) 分布式账本。交易记账由分布在不同地方的多个节点共同完成,每一个节点记录的都是完整的账目,都可以参与监督交易合法性。

每一个节点的交易信息经过隐私保护处理后在网上发布,记录在区块链中。所有参与节点都记录这一交易信息,确保交易信息的可查询、可证明,省去了中心化的管理。

2) 非对称加密和授权技术。存储在区块链上的交易信息是公开的,但账户身份信息是加密的,只有在数据拥有者授权的情况下才能访问到。

除了交易事件本身的信息外,交易者身份信息及交易内容均可以被加密后挂载在区块链中。任一节点被授权后,均可查阅这些秘密信息。由于每个节点都存储有所有交易信息,因此,查阅迅速,不易受网络状况影响。

3) 共识机制。所有记账节点之间如何达成共识,确认一个记录的有效性。

区块链中的所有节点都遵守统一记账规则,少量不守规则的节点最终不会被记录进区块链。目前的共识机制是通过“挖矿”机制达成的,算力强大者获得记账权的概率大,有利于形成唯一的区块链,但存在巨量无效消耗的问题。

4) 智能合约。基于这些可信的不可篡改的数据,可以自动化地执行一些预先定义好的规则和条款。

在区块链结构和共识机制基础上,可以设计很多应用。例如,各大银行间可以通过区块链进行跨行支付;企业联盟可以借助区块链从事企业间的商务活动;各高校之间可以利用区块链设计跨校选课系统等。

5.2 区块链技术思政分析

区块链是一种技术上较为成熟、应用上正在不断拓展的技术。它可以以链式方式记录信息,具有时序性,可以带来公平、透明、扁平化的管理,它以绝大多数节点的信息为依据,不易被篡改。区块链技术在金融、供应链管理、粮食分配、医疗管理、网络空间治理等方面具有很大的应用潜力。

区块链技术被正当使用,确实可以为企业、联盟等带来管理上的便捷。但这种便捷同样可能被不法分子滥用,在全球范围内广为传播违法和有害信息。

我国国家互联网信息办公室2019年1月10日发布《区块链信息服务管理规定》^[11]:区块链信息服务提供者应当落实信息内容安全管理责任,建立健全用户注册、信息审核、应急处置、安全防护等管理制度;区块链信息服务提供者开发上线新产品、新应用、新功能,应当按照有关规定报国家和省、自治区、直辖市互联网信息办公室进行安全评估;区块链信息服务提供者和使用者的不得利用区块链信息服务从事危害国家安全、扰乱社会秩序、侵犯他人合法权益等法律和行政法规禁止的活动,不得利用区块链信息服务制作、复制、发布、传播法律和行政法规禁止的信息内容等。

因此,应在国家法律许可的框架下,正确使用区块链技术,让其服务于国民经济主战场;同时,应积极创新区块链技术,突破其中的瓶颈或不合理问题,如算力无谓消耗问题,设计更为合理、低能耗的共识机制;面向各行各业,开发更多的区块链应用,不断降低社会运行成本。

5.3 区块链技术教学互动环节

在区块链技术的教学过程中,要求学生查阅以下方面的文献。

- 1) 区块链中的共识机制。
- 2) 区块链的防篡改原理。
- 3) 区块链的安全性分析。
- 4) 区块链的典型应用案例分析。
- 5) 国内外对区块链应用的管理。

研讨时播放的视频选择了央视关于区块链的专家对话、以太坊创始人关于数字货币的观点、巴菲特对比特币的看法等,让大家全面了解业界关于区块链的各个方面。

通过本节的教学,学生可掌握区块链技术的基本原理及其在多个行业应用的可能性,认识到正确使用区块链技术服务国民经济的重要性,以及必须对区块链技术的应用实施的监管。

6 可信计算技术思政教学

6.1 可信计算技术发展历程

可信计算是面向一个计算系统的概念,是指一个计算系统所计算出来的结果是可信的。可信计算组织(TCG)用实体行为的预期性来定义可信:如果它的行为总是以预期的方式朝着预期的目标进行,则一个实体是可信的。ISO/IEC 15408 标准则定义可信为:参与计算的组件、操作或过程在任意的条件下是可预测的,并能够抵御病毒和物理干扰^[12]。

可信计算通过对计算过程的可管可测和计算程序的合法性检验,为通用计算平台提供对部分恶意代码或非法操作的主动免疫能力。我国的可信计算是以国产密码算法为可信基础,将可信密码模块(TCM)作为信任根,并将可信主板作为可信计算平台,将可信网络作为可信过程交互的纽带,对上层业务应用进行透明支撑,保障应用执行环境和网络环境安全^[13]。2013年,我国发布了3个可信计算技术标准:《可信平台主板功能接口(GB/T 29827-2013)》《可信连接架构(GB/T 29828-2013)》《可信计算密码支撑平台功能与接

口规范(GB/T 29829-2013)》。目前,我国可信计算已经发展到3.0阶段,以可信免疫为目标,着重解决好用、易用的问题。

在资源受限的移动和嵌入式环境中,如ARM TrustZone、智能卡等,也可以通过软件方式实现可信计算环境。另外,物理不可复制函数PUF可以为可信计算提供物理安全特征,实现密钥安全存储、认证、信任根等功能,可应用到物联网、可穿戴设备、BYOD等场景中。Global Platform 开放式联盟定义了关于卡、设备、系统等各个方面的规范,其中包含与可信计算联系比较紧密的GP-TEE规范。

随着量子计算机的出现,可信计算机制及其中的密码算法面临量子计算分析的风险。目前国内外纷纷加大了对抗量子计算密码算法及抗量子计算TCM的研究。出于紧迫性,国际上从2006年开始举办“抗量子计算密码学术会议”,每两年举行一次,已经产生了一批重要的研究成果,包括基于Hash函数的数字签名方案、基于纠错码的密码、基于格的密码以及多变量公钥密码学等,让人们看到了抗量子计算密码的新曙光^[14]。

构建可信计算环境除了要有可信密码模块以外,还需要CPU和操作系统的支持。以边缘计算为例,边缘接入设备负责汇集末端设备的信息,进行整理加工,通过网络报送给远程服务器。它一般部署在远端,常年无人值守,很容易遭受病毒攻击。对其应用可信计算技术以对抗各种网络攻击,是个不错的选择。但如果所使用的操作系统存在漏洞,可信校验机制就可能被绕过。如果大量的边缘接入设备被网络劫持,不仅会造成信息泄露、假冒,更可能造成全网的瘫痪。

6.2 可信计算技术思政分析

从上面的分析可以看出,可信计算技术是网络安全的基石。在2017年6月我国施行的《网络安全法》中,明确规定要推广安全可信的网络产

品和服务。安全可信，即信息系统中的软硬件，包括 CPU 主板、操作系统和应用程序，被权威机构检测后得出的结论是安全的，没有可以被利用的漏洞；这些在信息系统中运行的软件来源合法、未授权不能修改；信息系统中运用了可信计算技术，能够形成信任链，发现和控制不安全的软件被安装、运行和升级。

网络安全是国家安全的重要基础，也是经济安全、社会安全、民生安全的重要保障。国家互联网信息办公室公布的《网络产品和服务安全审查办法（试行）》把网络安全审查分成“安全性”审查和“可控性”审查^[8]。当前，我国网信领域要求采用自主可控技术、产品、服务、系统的呼声越来越高，这里的“自主可控”强调的就是可控性^[15]。自主可控是实现网络安全的前提，是一个必要条件，但并不是充分条件。因此，为了实现网络安全，首先要实现自主可控，再结合其他各种安全措施，达到保障网络安全的目标。

信息系统安全的核心是操作系统的安全。由于操作系统代码量巨大，要想发现其中的全部安全漏洞非常困难。因此，一方面要不断研发检测类技术和系统，形成强大的安全检测能力；另一方面应从源头控制，自主研发安全相关的核心产品，减少未知环节。不难看出，自主可控是实现安全可信的前提。

在我国工业物联网建设中，应大力提倡应用国产化设备、国产化操作系统和国产化可信计算技术，在利用工业物联网将大量数据汇聚产生增量价值的同时，保护好工业网络和工业设备免受外来侵犯。

6.3 可信计算技术教学互动环节

在可信计算技术教学互动环节，要求学生查找以下方面的文献，并进行研讨。

- 1) 国内外可信计算技术发展现状。
- 2) 我国《网络安全法》和相关政府部门对可

信计算的要求、措施。

- 3) 我国的可信计算相关标准解读和分析。

- 4) 可信计算芯片及应用案例分析。

- 5) 当今可信计算应用的瓶颈和最适合应用的领域。

选择主流媒体对可信计算技术应用成果的报道、可信计算技术在对抗病毒攻击等方面的成功案例等，进行宣传 and 讲解。

通过本节的学习，学生可认识到可信计算技术对我国网络安全的重要性。把国产密码算法应用于可信计算芯片，并面向行业应用设计端、管、云可信安全体系，是解决当前我国网络安全问题的重要途径。

7 隐私保护技术思政教学

7.1 隐私保护技术进展历程

随着互联网技术的发展和信息技术的深度应用，人类社会越来越依赖信息终端和信息网络。随之而来的隐私信息泄露问题逐渐显露出来。许多浏览器、终端应用软件、云端应用软件等肆无忌惮地获取用户隐私信息，包括身份信息、位置信息、购物信息、浏览信息等。隐私信息的泄露对绝大多数人造成了困扰，危及个人经济安全，甚至危及人身安全。目前，最大的隐私泄露途径主要是云端数据共享引起的批量信息泄露，以及巨量的手机端 App 肆意收集用户信息造成的隐私泄露。

数据共享是信息化时代的大势所趋，而隐私保护与数据共享天生是一对矛盾。差分隐私保护技术通过把数据加扰以后进行共享，保护了原始数据中的隐私信息，并使从共享数据或多个数据库中通过关联分析等手段反推出用户的隐私成为不可能^[16]。最近几年，出现了不少关于隐私保护的成果。文献[17]提出了满足本地差分隐私的位置数据采集方案，文献[18]提出了无线传感器网

络隐私保护数据聚集技术,文献[19]提出了基于属性加密的用户隐私保护云存储方案等。除此以外,通过数据替换、数据加密、数据随机化、字符串屏蔽等手段也可以实现隐私保护,具体使用哪一种技术,取决于应用场景和隐私保护的程度。

解决隐私泄露问题需要从技术和管理两个层面进行,缺一不可。从技术上看,一方面,要解决隐私信息的授权获取问题,即只有在授权情况下,才可以获取隐私信息;另一方面,要解决获取隐私信息后的使用追溯问题,即能够追溯到是谁泄露了隐私信息。目前,学术界对数据跟踪、溯源的研究相对较少,已应用于产品中的技术更少,使隐私泄露执法检查缺乏抓手,这也是隐私泄露现象屡禁不止的原因之一。数据水印技术常用来进行数据跟踪,但如何对批量数据添加顽健水印以及对经过很多次转发的数据在每个环节添加顽健水印,仍需要进一步研究。

从管理上看,一方面需要界定数据管理者的法律责任,我国《网络安全法》规定:网络运营者应当对其收集的用户信息严格保密,并建立、健全用户信息保护制度;另一方面,要规范数据采集者的责任,对有害 App 的生产者追究经济责任和法律责任。国家互联网信息办公室、工业和信息化部及各地政府都加大了对有害 App 的审查力度,工业和信息化部泰尔实验室发布 App 安全审核平台,有力净化了 App 市场,维护了用户权益。我国应加大对隐私保护的体系性建设,加强对检测、检查工具的开发和应用。

7.2 隐私保护思政分析

保护隐私信息、净化网络空间是人类共同的责任。欧盟议会于 2016 年 4 月 14 日通过的《通用数据保护条例》(GDPR, General Data Protection Regulations)于 2018 年 5 月 25 日在欧盟成员国内正式生效实施。该条例的适用范围极为广泛,

任何收集、传输、保留或处理涉及欧盟所有成员国内的个人信息机构组织均受该条例的约束^[20],被媒体称为“欧盟最严数据保护条例”。欧盟数据监管机构表示,Facebook、推特、微软、苹果都或多或少地违反了 GDPR,罚单正在路上。2019 年 1 月 21 日,法国数据保护监管机构 CNIL 根据《通用数据保护条例》对 Google 处以 5 000 万欧元(约 4 亿人民币)的罚款,理由是 Google 在处理个人用户数据时存在缺乏透明度、用户获知信息不充分以及缺乏对个性化广告的有效同意等问题。

2018 年 5 月 1 日,我国颁布在保护个人信息方面的推荐性国家标准——《信息安全技术 个人信息安全规范》^[21],使我国在隐私保护方面走在了亚洲的前列。本标准针对个人信息面临的安全问题,规范个人信息控制者在收集、保存、使用、共享、转让、公开披露等信息处理环节中的相关行为,旨在遏制个人信息非法收集、滥用、泄露等乱象,最大限度地保障个人的合法权益和社会公共利益。另外,我国在《宪法》《网络安全法》《侵权责任法》《民法通则》等多部法律文件中就个人隐私的保护进行了规定。

在 2015 年 12 月 16 日召开的第二届世界互联网大会上,习近平总书记指出,互联网虽然是无形的,但运用互联网的人们都是有形的,互联网是人类的共同家园。让这个家园更美丽、更干净、更安全,是国际社会的共同责任。我国作为国际上负责任的大国,在网络空间治理、隐私保护方面理应走在国际前列,应平衡好数据利用与隐私保护的关系,发展好隐私保护技术,研制适用的隐私保护设施,保护好网络空间安全。

7.3 隐私保护教学互动

在本节的教学互动环节,要求学生查阅的文献和研讨的内容如下。

- 1) 国内外隐私保护法律法规。
- 2) 隐私保护技术进展。

- 3) 隐私泄露原因分析。
- 4) 隐私保护体系建议。
- 5) 数据利用与隐私保护的关系分析。

选择的视频播放内容包括:国内外主流媒体关于隐私泄露重大事故的报道和评价;我国政府关于隐私保护法律法规的立法与宣传;有关专家对隐私保护的建议等。

通过本节的学习,学生可认识到隐私泄露的危害性,对如何保护终端隐私以及云上数据隐私给予很大的重视,激发学生研究隐私保护技术的兴趣和努力为国家治理网络空间的积极性。

8 结束语

本文在介绍网络空间安全若干技术进展历程的同时,充分分析了各项前沿技术原理、技术突破过程以及可能的应用。进一步进行思政分析,挖掘这些技术对政治、经济、管理、法规的影响与支撑作用。通过技术引导、思政分析以及互动教学,有效激发学生的正能量。本文方法是对思政课程教学方式的有益探讨。

参考文献:

- [1] 高德毅,宗爱东.从思政课程到课程思政:从战略高度构建高校思想政治教育课程体系[J].中国高等教育,2017(1):43-46.
GAO D Y, ZONG A D. From ideological and political course to course ideological and political course: constructing the course system of ideological and political education in colleges and universities from a strategic perspective[J]. Higher Education in China, 2017 (1): 43-46.
- [2] 高燕.课程思政建设的关键问题与解决路径[J].中国高等教育,2017(23):13-16.
GAO Y. Key issues and solutions of course ideological and political construction [J]. Higher Education in China, 2017 (23): 13-16.
- [3] 吴华,王向斌,潘建伟.量子通信现状与展望[J].中国科学:信息科学,2014,44(3):296-311.
WU H, WANG X B, PAN J W. Status and prospect of quantum communication [J]. Chinese Science: Information Science, 2014, 44 (3): 296-311.
- [4] 王晋岚.世界首条量子保密通信干线开通[J].科学源流,2017(6):52-52.
WANG J L. Successful opening of the world's first quantum secure communication trunk [J]. Origin & Development, 2017(6):52-52.
- [5] 李建华.新型电子政务及其安全保障技术[J].上海交通大学学报,2018,52(1):1370-1381.
LI J H. New e-government and its security technology[J]. Journal of Shanghai Jiaotong University, 2018, 52(1): 1370-1381.
- [6] 李古月,胡爱群,石乐.无线信道的密钥生成方法[J].密码学报,2014,1(3):211-224.
LI G Y, HU A Q, SHI L. Key generation method for wireless channel [J]. Journal of Cryptography, 2014, 1(3): 211-224.
- [7] WANG D, HU A Q, CHEN Y, et al. An ESPRIT-based approach for rf fingerprint estimation in multi-antenna OFDM systems[J]. IEEE Wireless Communications Letters, 2017, 6(6): 702-705.
- [8] XING Y X, HU A Q, ZHANG J Q, et al. On radio frequency fingerprint identification for DSSS systems in low SNR scenarios [J]. IEEE Communications Letters, 2018, 22(11): 2326-2329.
- [9] LI G Y, HU A Q, ZHANG J Q, et al. High-agreement uncorrelated secret key generation based on principal component analysis pre-processing[J]. IEEE Transactions on Communications, 2018, 66(7): 3022-3034.
- [10] KHAN M A, SALAH K. IoT security: review, blockchain solutions, and open challenges[J]. Future Generation Computer Systems, 2017.
- [11] 钱卫宁,邵奇峰,朱燕超,等.区块链与可信数据管理:问题与方法[J].软件学报,2018,29(1):150-159.
QIAN W N, SHAO Q F, ZHU Y C, et al. Research problems and methods in blockchain and trusted data management [J]. Journal of Software, 2018,29(1):150-159.
- [12] 任春卉,王志皓,赵保.《可信计算体系结构》标准产业化应用,信息安全与通信保密,2019(1):43-49.
REN C H, WANG Z H, ZHAO B. Standard industrialization application of trusted computing architecture[J]. Information Security and Communication Secrecy, 2019(1): 43-49.
- [13] 张焕国,罗捷,金刚,等.可信计算研究进展,武汉大学学报(理学版),2006(52):513-518.
ZHANG H G, LUO J, JIN G, et al. Research progress in trusted computing[J]. Journal of Wuhan University (Science Edition), 2006(52): 513-518.
- [14] 徐震.我国可信计算现状与发展思考[J].中国信息安全,2010(9):69-70.
XU Z. Thinking about status and development of trust computing in China [J]. China Information security, 2010(9):69-70.
- [15] 王甬平.建立自主可控、安全可信的国家网络安全体系:访信息系统工程专家、中国工程院院士沈昌祥[J].宁波通讯,2015(1):68-69.

WANG Y P. Establishing autonomous and controllable, secure trusted national network security system: visiting information systems security engineering professional, chinese academy of engineering, Sheng changxiang [J]. Ningbo Newsreport, 2015(1):68-69.

- [16] Differential privacy[EB/OL]. <https://baike.baidu.com/item/Differential Privacy/22415732?fr=aladdin>.

- [17] 高志强. 满足本地差分隐私的位置数据采集方案[J]. 清华大学学报(自然科学版), 2019, 59(1): 23-27.

GAO Z Q. Location data acquisition scheme for local differential privacy[J]. Journal of Tsinghua University (Natural Science Edition), 2019, 59(1): 23-27.

- [18] 张晓莹, 彭辉, 陈红. 无线传感器网络隐私保护数据聚集技术[J]. 通信学报, 2018, 39(10): 130-142.

ZHANG X Y, PENG H, CHEN H. Data aggregation technology for privacy protection in wireless sensor networks[J]. Journal of Communications, 2018, 39(10): 130-142.

- [19] 曹来成. 基于属性加密的用户隐私保护云存储方案[J]. 清华大学学报(自然科学版), 2018, 58(2): 150-156.

CAO L C. Cloud storage scheme for user privacy protection based on attribute encryption[J]. Journal of Tsinghua University (Natural Science Edition), 2018, 58(2): 150-156.

- [20] TIKKINEN-PIRI C, ROHUNEN A, MARKKULA J. EU general data protection regulation: changes and implications for personal data collecting companies [J]. Computer Law & Security Review, 2017:S0267364917301966.

- [21] 董贞良. GB/T 35273—2017《信息安全技术, 个人信息安全规范》解读[J]. 中国质量与标准导报, 2018, 248 (6):25-27.

DONG Z L. GB/T 35273—2017《understanding of personal information security specification for information security technology》[J]. China Quality and Standards Review, 2018, 248(6):25-27.

[作者简介]



胡爱群(1964—), 男, 江苏南通人, 东南大学教授、博士生导师, 主要研究方向为无线网络安全、无线通信安全。



李古月(1989—), 女, 东南大学讲师, 主要研究方向为物理层安全、无线通信安全。



彭林宁(1984—), 男, 博士, 东南大学副研究员, 主要研究方向为物理层安全。



李涛(1984—), 男, 博士, 东南大学副教授, 主要研究方向为网络空间安全。