

基于教学实训靶场的“数据隐私保护”课程建设初探

孙哲, 宁洪, 殷丽华, 方滨兴

(广州大学网络空间安全学院, 广东 广州 541004)

摘要: 随着我国《数据安全法》和《个人信息保护法》等隐私保护相关法律法规的正式实施, 数据隐私保护技术人才需求急剧增长, 各高校网络空间安全专业逐步开设数据隐私保护课程。广州大学“方滨兴院士实验班”(简称“方班”)教学团队在长期的数据安全科研教学实践的基础上, 提出了基于教学实训靶场的“数据隐私保护”课程教学方法。针对选修“数据隐私保护”课程的学生进行了学情分析, 总结当前网络空间安全专业学生在理论学习、动手实践和创新运用上存在的问题, 并针对性地设计了课程的学习目标。在教学课程内容选取上, 教学团队遴选出匿名模型、差分隐私、可搜索加密、密文计算、对抗训练、多媒体隐私保护、隐私策略冲突消解、隐私侵犯行为溯源 8 个典型的隐私保护关键技术, 设计了相应的教学模块, 并部署在教学实训靶场中供学生学习训练。在教学方法设计中, 提出了理论与编程融合的知识应用导向教学方法、基于算法扩展改编的工程实践导向教学方法、面向实际应用场景的综合实践导向教学方法, 实现“学-做-用”的知识学习应用闭环。通过 3 年的隐私保护教学实践, “方班”在培养学生的知识应用能力、工程实践能力和综合创新能力等方面获得了显著的效果, 为“数据隐私保护”这门初建课程建设提供有益探讨。

关键词: 数据隐私保护; 实践创新能力; 教学靶场; 新课程建设

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023016

Preliminary study on the construction of a data privacy protection course based on a teaching-in-practice range

SUN Zhe, NING Hong, YIN Lihua, FANG Binxing

Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 541004, China

Abstract: Since China's Data Security Law, Personal Information Protection Law and related laws were formalized, demand for privacy protection technology talents has increased sharply, and data privacy protection courses have been gradually offered in the cyberspace security majors of various universities. Building on longstanding practices in data security research and teaching, the teaching team of "Academician Fang Binxing's Experimental Class"

收稿日期: 2022-06-21; 修回日期: 2022-11-02

通信作者: 殷丽华, yinlh@gzhu.edu.cn

基金项目: 广东省高等教育教学改革项目(20190485)

Foundation Item: Guangdong Higher Education Teaching Reform Project (20190485)

引用格式: 孙哲, 宁洪, 殷丽华, 等. 基于教学实训靶场的“数据隐私保护”课程建设初探[J]. 网络与信息安全学报, 2023, 9(1): 178-188.

Citation Format: SUN Z, NING H, YIN L H, et al. Preliminary study on the construction of a data privacy protection course based on a teaching-in-practice range[J]. Chinese Journal of Network and Information Security, 2023, 9(1): 178-188.

(referred to as “Fang Class”) at Guangzhou University has proposed a teaching method for data privacy protection based on a teaching-in-practice range. In the selection of teaching course content, the teaching team selected eight typical key privacy protection techniques including anonymity model, differential privacy, searchable encryption, ciphertext computation, adversarial training, multimedia privacy protection, privacy policy conflict resolution, and privacy violation traceability. Besides, the corresponding teaching modules were designed, which were deployed in the teaching practice range for students to learn and train. Three teaching methods were designed, including the knowledge and application oriented teaching method which integrates theory and programming, the engineering practice oriented teaching method based on algorithm extension and adaptation, and the comprehensive practice oriented teaching method for practical application scenarios. Then the closed loop of “learning-doing-using” knowledge learning and application was realized. Through three years of privacy protection teaching practice, the “Fang class” has achieved remarkable results in cultivating students’ knowledge application ability, engineering practice ability and comprehensive innovation ability, which provided useful discussion for the construction of the initial course of data privacy protection.

Keywords: data privacy protection, practice and innovation ability, teaching innovation, new course construction

0 引言

随着我国大数据战略的持续深入推进，以电子政务、医疗健康等行业为典型代表的大数据应用给经济社会发展、国家管理、社会治理、人民生活带来重大而深远的影响。2020年，我国数字经济核心产业增加值占国内生产总值（GDP）比重达到7.8%。据IDC《2021年V2全球大数据支出指南》预测，2025年中国大数据总体市场规模将超过250亿美元，数字经济为经济社会持续健康发展提供了强大动力^[1]。然而，由于数据本身具有极高的附带价值，且关系到用户的人身财产安全，如不落实数据隐私保护机制，一旦数据被泄露，将对社会民生，甚至公共、国家安全造成极大危害。

2022年1月，国务院印发的《“十四五”数字经济发展规划》对促进数字经济公平竞争、安全有序发展提出了极高的要求。2022年年底，《数字安全法》《个人信息保护法》等相关法律的正式实施，进一步展示了我国建立完善数字经济公平有序高质量发展的决心，也对当前数字经济市场在隐私保护合法合规方面提出了极高的要求。各行各业都在完善自身数据安全和隐私保护的技术标准，不少企业开始专门设立隐私保护专业技术人员的岗位，甚至模仿欧盟企业设置“首席隐私执行官”。由于数据隐私保护技术需要专业化的培训，目前隐私保护和数据合规人才出现了极大的缺口。

然而，数据隐私保护作为数据处理的一门伴生技术，其需要综合运用网络空间安全的各类理论知识和应用技术，解决实际数据应用场景中的隐私泄露问题，并满足用户个性化隐私需求和国家法律法规对数据服务的合规要求。隐私保护专业技术人员需根据不断变化的隐私需求和逐步完善的法律法规，以及具体应用场景问题完成隐私保护方案设计，并进行必要的理论和技术研究的创新。以上诸多隐私相关问题使得实际企业岗位对数据隐私保护从业人员的专业技术能力提出极高要求。

近年来，隐私保护技术在国内外研究机构 and 高校中受到了高度重视。研究者们针对各类隐私保护技术开展了大量的研究，如今隐私保护技术已成为一项门类体系较为齐全的研究领域。国内很多高校开始对隐私保护相关人才培养进行一些有益尝试，包括开展隐私保护技术讲座、开设隐私保护课程和出版相关教学图书。例如，复旦大学“隐私保护理论与实践”课程是国内早期也是影响较大的隐私保护课程之一，该课程主要关注差分隐私保护机制的介绍。《隐私保护数据发布：模型与方法》偏重隐私保护的数据发布机制，主要介绍了隐私保护机制中的匿名模型和差分隐私模型^[2]。当前的隐私保护人才培养还处在起步阶段，大多偏重某一方面的隐私保护理论概念和学术前沿，缺少系统深入的实践指导，尤其缺少隐私保护综合解决方案相关的实验和实践的指导。

在教学设计上,由于各高校隐私保护课程还处在初建阶段,相关教学文献和案例较少。本文调研了数据安全及密码学等相似课程的教学文献,现有的教学设计大致可分为案例教学模式^[3]、基于翻转课堂的教学模式^[4-5]和在线教学模式^[6-7]等方式。其中,张艳硕等^[3]面向零知识证明微课设计了一种分层次案例化教学设计,由于零知识证明课程的知识较为抽象,形象化的案例化教学方式可以帮助学生理解基本概念,增强学生的学习兴趣。但涉及核心密码学知识时,仍与传统教学方式较为相似,容易产生教学过程中学生的热情前后差距较大的问题。此外,张宁等^[6]将 SPOC 在线教育与翻转课堂相结合,并运用在密码学课程改革中,鼓励学生从被动学知识向主动讲知识转变,提升了学生的学习主动性。然而,以上方法更适合密码学这类以理论为主的课程教学,较难直接提升学生的动手实践能力和综合解决实际问题能力。数据隐私保护作为一种理论与运用并重的课程,亟须在动手实践教学方法上寻找新的突破口。

很多隐私攻击方法可能导致严重的安全事故,很多隐私保护技术实验并不能直接在真实生产场景中执行。为了解决数据隐私保护课程教学中理论教学与应用实践脱节的问题,广州大学网络空间先进技术研究院从 2019 年开始建设“数据隐私保护”课程,依托学院的人工智能和数据分析相关教学靶场,从数据集预处理、智能算法分析实现、业务场景应用和测试等环节为学生提供在线逼真的教学环境。通过指导学生在教学实训靶场进行实操和练习来掌握众多隐私保护算法和工具的应用方法,以迭代实验和反复拆解的方式分析理解内部机理、掌握评估重构方法,在业务场景牵引和数据靶标驱动下,锻炼培养学生的工程实践和技术创新能力。

综上,本文提出的基于教学实训靶场的数据隐私保护教学方法,其主要贡献在于:从传授知识向运用知识的方向改变;通过拆解经典算法培养学生的工程思维;利用教学实训靶场对业务场景进行仿真,培养学生解决实际问题的能力。

1 “数据隐私保护”教学目标

根据当前隐私保护专业技术人才的紧迫需

求,在开设“数据隐私保护”课程之前根据对授课对象的学情和目前存在的主要问题进行了分析,设置了以下教学目标,着重培养学生的3项能力。

1.1 培养知识运用能力

1) 学情分析:专业背景各异。报考网络空间安全(学硕)、网络与信息安全(专硕)专业硕士研究生(以下简称研究生)的本科专业种类多样,除了信息安全、计算机科学与技术、软件工程等专业外,还包括电子、通信、自动化、机械、地理信息系统等其他相关专业。因此,由于专业背景的不同,学生专业基础差距较大,对课程教学实施过程中的进度把握、学生个性化培养提出了较高要求。

2) 存在问题:知识体系不全。由于研究生的专业基础差距较大,“数据隐私保护”课程一般开设在研究生一年级下学期。非信息安全相关专业的学生缺少信息安全基础和数据分析相关基本课程的系统教学(前驱课程包括:数据库与大数据管理、人工智能与机器学习、密码技术及应用等),存在知识体系不全、掌握信息碎片化等问题^[8]。

3) 培养目标:知识运用能力。授课结束后,学生应具备熟练使用已有隐私保护相关理论、方法、工具来解决经典隐私泄露问题的能力;熟悉当前数据隐私泄露风险和主要的隐私增强技术,系统掌握信息论、信息内容安全、密码学、访问控制等信息安全相关课程的基础理论和应用方法。“数据隐私保护”课程注重培养学生跨学科关联知识和应用的思维,为灵活利用已学习的理论知识解决特定场景的问题奠定基础。

1.2 培养工程实践能力

1) 学情分析:认知转变特点。研究生一年级是学生从学习知识向科研实践转变的时期,在研究生身份认知上发生蜕变。在授课过程中,有依赖教师教授知识与独立思考解决问题等多种认知状态并存的情况。因此,教师需分辨学生认知状态,进行合理引导,帮助学生完成身份认知转变。

2) 存在问题:实践经验缺乏。一年级的研究生从本科学习以来,大多以理论教学为主,较少参与工程实践,存在动手能力较差、实践经验较

少的特点^[9]。因此，需要在教学过程中，给予学生充分的训练时间，提升实践开发能力。在课程设置过程中，需将实践考核的周期进行适当延长。

3) 培养目标：工程实践能力。授课结束后，学生应具备深刻理解和分析关键算法与工具的内部机理，依据实际情况对隐私保护算法进行评估重构的能力；根据应用场景利用现有工具分析隐私泄露风险点，能够利用已有的理论知识和工具设计隐私保护方案，解决指定目标的隐私泄露威胁，即具备根据暴露出的隐私泄露问题制定解决方案的能力。

1.3 培养综合创新能力

1) 学情分析：目标导向强烈。学生在研究生阶段，已经对自己的职业规划具有较为清晰的认识。对毕业后去企业就业还是继续学术深造大多做出了决定，这就使得学生在研究生课程学习中具有较为明确的目标导向。因此教师在授课过程中，应为不同目标的学生提供合适的技能培训，实现课程授课目标的同时，满足学生的需求导向。

2) 存在问题：创新思维不足。研究生发现问题、设计新方案的能力较弱并非仅源于从事隐私保护专业理论学习和工程实践的时间较短，更多地源于思考问题不够深入，没有与其他从业人员进行充分讨论、激烈碰撞的机会。在思考问题过程中，经常出现“闭门造车”的情况。在课程设计中，需要增加“调研学习-发现问题-提出方案-接受质疑-完善方案”研讨创新环节。

3) 培养目标：综合创新能力。授课结束后，学生应熟悉学术前沿和技术发展动态，可以根据不断变化的隐私需求和逐步完善的法律法规，逐步完善已搭建的隐私保护系统；能够预先挖掘新的未知隐私泄露风险，并提前设计应对的隐私保护方案；具有一定的隐私保护理论研究和技術革新的能力。

2 “数据隐私保护”课程内容选取

“数据隐私保护”是一门综合运用信息安全技术解决实际应用场景中隐私问题的课程，它不仅拥有一些“数据隐私保护”课程专有的脱敏技术，如匿名技术、差分隐私等，还有利用密码学、访

问控制等其他信息安全知识实现的隐私信息防护技术，并最终需要将这些技术应用到位置服务、医疗辅助诊断、社会网络等具体应用场景中。

“数据隐私保护”课程在整个网络空间安全课程体系处于上游位置。网络空间安全课程体系从下向上可以粗略划分为物理安全、系统安全、网络安全、数据安全、内容安全5个层次。数据隐私保护横跨数据安全与内容安全两个层次，其安全目标是既要保证数据的机密性，也要防止发布后的信息内容被推断还原用户的隐私属性。

如何将复杂的隐私保护知识体系和交叉学科所涉及的理论知识融入实际应用场景，解决应用场景中的隐私保护问题，是“数据隐私保护”课程设计必须要考虑的问题。当前隐私保护课程和市面上的隐私保护专业书籍大多聚焦某个领域的学术前沿或某项技术的理论概念，缺少系统深入的实践指导，使得课程理论知识到解决实际问题中仍存在一个鸿沟。

为了帮助学生建立成体系的理论知识体系，教学组将现有隐私保护技术进行了梳理。具体在课程单元选取上，考虑到数据隐私保护涉及的技术种类多样，教学团队对各类技术进行了取舍。课程内容从基于信息损失机理的隐私脱敏技术、基于数据机密性保护机理的隐私防护技术、新技术衍生隐私问题及保护方法、隐私保护策略与隐私信息管理4个方面中选取了8个场景。并将每个场景和一个隐私保护关键技术相结合，形成一个课程单元，具体内容如表1所示。

1) 基于信息损失机理的隐私脱敏技术选取了匿名模型和差分隐私方法，这是隐私保护数据发布中的经典方法。学生可以在教学靶场中通过复现 k -anonymity 算法和拉普拉斯噪声生成机制，并将所编写的算法运用在位置隐私保护和医疗数据查询这两个传统隐私保护场景，从而指导学生理解隐私数据脱敏发布机理，培养学生运用理论知识解决经典隐私保护问题的能力。

2) 基于数据机密性保护机理的隐私防护技术采用了可搜索加密和密文计算。密码学是隐私保护方案中最常用的前驱基础知识，也是培养学生利用其他信息安全课程知识解决隐私保护问题

表1 “数据隐私”保护课程内容选取与设计
Table 1 Content selection and design of “data privacy protection” course

教学内容	理论基础与教学目标	核心算法复现与拆解	应用场景靶场训练
基于信息损失机理的隐私脱敏技术	匿名模型 ① 掌握匿名模型与用户标识符的概念 ② 了解传统匿名化方法与链接攻击 ③ 掌握 k-anonymity 模型及其变型	① k-anonymity 算法 ② l-diversity 算法 ③ t-closeness 算法	基于匿名模型的位置隐私保护场景
	差分隐私 ① 掌握相邻数据集、全局敏感度、局部敏感度、差分隐私 ϵ-DP、松弛差分隐私 (ϵ, δ)-DP、本地差分隐私的概念 ② 掌握拉普拉斯机制、高斯机制、指数机制、随机响应机制	① 基于拉普拉斯机制的差分隐私算法 ② 基于高斯机制的差分隐私算法 ③ 基于指数机制的差分隐私算法	基于差分隐私的医疗数据库隐私保护场景
基于数据机密性保护机理的隐私防护技术	可搜索加密 ① 掌握可搜索加密的基本原理 ② 掌握使用对称加密、公钥加密和布隆过滤器的方法	① 基于 SWP 算法的可搜索加密算法 ② 基于 Z-IDX 算法的可搜索加密算法	基于可搜索加密的电子病历密文搜索场景
	密文计算 ① 掌握椭圆曲线加密的半同态性质和算法原理 ② 掌握椭圆曲线数字签名算法原理 ③ 掌握 ECC 密码和 ECDSA 数字签名算法 ④ 掌握构建 MPC 协议	① 基于 ECC 密码算法的密文计算算法 ② 基于 ECDSA 数字签名算法的密文计算算法	基于密文计算的封闭式电子拍卖隐私保护场景
新技术衍生隐私问题及保护方法	对抗训练 ① 掌握 PyTorch 深度学习框架的使用，构造卷积神经网络 ② 掌握多任务学习算法的概念 ③ 掌握基于对抗训练的深度学习隐私保护方法	基于对抗训练的图像识别神经网络训练	基于对抗训练的人脸图像识别隐私保护场景
	多媒体隐私 ① 掌握多媒体文件中个人识别符的识别方法 ② 掌握图像处理、音频处理的基本原理和方法 ③ 掌握利用遮蔽、加噪等手段保护多媒体文件中的隐私信息	① 图片中人脸区域的识别与保护算法 ② 声纹隐私信息识别与保护算法	社交应用中的视频隐私保护场景
隐私保护策略与隐私信息管理	隐私策略冲突消解 ① 掌握访问控制及基于属性的访问控制的基本原理 ② 掌握基于属性的访问控制机制、隐私策略检测及冲突消解方法	① 面向社交网络的访问控制框架搭建过程 ② 社交网络隐私保护策略冲突及消解	面向社交网络的隐私策略冲突消解
	隐私侵犯行为溯源 掌握 LSB 数字水印算法和 DCT 数字水印算法的基本原理	① LSB 数字水印算法 ② DCT 数字水印算法	基于数字水印的图片转发溯源取证场景

的最佳教学案例。该模块从加密数据的检索和计算的角度，结合云外包和电子拍卖应用场景，让学生通过开发和迭代可搜索加密和密文计算算法，实现加密隐私数据的查询和匹配操作。

3) 新技术衍生隐私问题及保护方法围绕数据处理中常最用到的机器学习技术，设计了深度学习梯度保护和多媒体隐私保护两个教学模块。在深度学习梯度保护中使用对抗训练等新思路来解决随机梯度的隐私保护需求。在多媒体隐私保护中根据图像、视频属性挖掘特色属性（拍摄距离等）实现路人检测等隐私任务，培养学生熟悉

和利用新技术进行隐私保护问题的思维。

4) 隐私保护策略与隐私信息管理涵盖了隐私信息管理过程中的隐私策略冲突消解、隐私侵犯行为溯源等方面，以社交网络场景为实际教学靶场，分析社交网络中各主体的隐私策略，设定规则消除冲突，熟练掌握通过访问控制方法制定个性化的隐私保护方案。在文件多次转发场景中，利用数字水印技术记录用户对隐私信息操作行为，为溯源和取证提供支撑。

基于这种单元设置，学生可以较为容易地建立最初的隐私保护知识体系框架。当将来学习到

新的隐私保护技术,可以将其融入知识体系框架,并根据自身的理解不断完善和修正知识体系框架。以求在最短时间里,帮助学生解决专业背景各异、知识体系不全的问题,为提升学生知识运用能力打下基础。

在各个单元内部,教学组以单元的主导隐私保护关键技术为线索,贯穿整个单元理论教学、算法实现、实际应用的所有环节。学生在充分了解该技术所针对的隐私问题和演变历程的基础上,逐步明确理论知识机理和学习目标。与此同时,加入核心算法复现与拆解,通过不断动手演练,促进学生认知转变,解决学生实践经验缺乏的问题,提升学生的工程实践能力。

在此基础上,引入教学实训靶场、模拟真实隐私泄露场景。辅助学生将学习的知识机理和动手完成的算法原型在真实场景中运行,让学生充分认识到,学习的单一知识不进行灵活改动,并做出适应性调整无法解决实际中的隐私泄露问题。培养学生基于明确的目标导向,并通过创造性的思维,综合利用所学所做的知识工具解决实际隐私泄露问题。

为了实现以上目标,课题组在教学内容选取的基础上,进行了一些教学方法改进和实践。

3 教学方法设计与实践

针对学习“数据隐私保护”课程研究生的特点,本文依托教学实训靶场,面向培养学生创新实践能力的教学目标,提出了理论与编程融合的知识应用导向教学方法、基于算法扩展改编的工程实践导向教学方法、面向实际应用场景的综合实践导向教学方法,实现“学-做-用”的知识学习应用闭环。并通过与“方班研讨厅”思辨课堂的双课互动,提升学生的创新思维能力。在此基础上,辅之以隐私保护法律学习,从课程思政角度阐述隐私保护从业人员的职业公德,为国家、企业培养高素质的专业人才。

3.1 理论与编程融合的知识应用导向教学方法

隐私保护课程拥有一些自身课程的专有知识,如 k -anonymity 模型、差分隐私等。为了提升学生的知识应用能力,并做好与工程实践、综合创新能力的衔接,在教学实训靶场中设计了一些经典

算法复现的模块。在这些模块中,学生需要理解经典算法的运作原理,并完成指定任务的编程练习。在完成算法编写后,调用测试样例,并对编写的算法正确性与效果进行评估。通过这些经典算法的复现,帮助学生对所使用的理论知识和工具有了更清晰的认识,从而为灵活运用这些知识打下基础。

在教学过程中,不断积累学生在复现算法中易错和迷惑性较强的案例,并将其作为改错练习,在后续教学过程中,提升学生辨别错误的能力。

3.2 基于算法扩展改编的工程实践导向教学方法

隐私保护算法在技术演进过程中不断地更新,很多更加完善的算法是在经典算法的基础上发展出来。例如, l -diversity 和 t -closeness 都是在 k -anonymity 模型的基础上增加新的条件限制发展而来。为了提升学生的工程实践能力,在课程设计过程中,设计了基于经典算法的扩展训练,要求学生在已有算法的基础上增加新的功能,通过迭代实验和反复拆解算法,理解算法的内部机理,从而掌握评估算法的脆弱点和重构新的隐私保护方法的能力。

在教学过程中,引导学生思考如何将算法分解成更细粒度的模块,通过更换相似功能的模块以适应不同的应用场景。例如,将差分隐私保护机制中的噪声生成机制从拉普拉斯噪声机制更改为高斯噪声机制,对输出的隐私保护效果有什么影响,且每种机制分别适用于什么样的场景。提升学生对所使用算法和工具的掌握能力。

3.3 面向实际应用场景的综合实践导向教学方法

隐私保护课程的最终目标是培养能解决实际隐私泄露问题的技术人才。为了提升学生综合解决隐私泄露风险的能力,课程设在教学实训靶场中构建了 8 个隐私保护具体业务场景靶场模块。通过虚拟环境与实际问题的结合,模拟仿真真实隐私保护业务的实验环境,从而达到在复杂应用场景下进行不同算法的应用实践效果。在业务场景牵引和数据靶标驱动下,通过算法设计与修改接口,鼓励和引导学生思考问题和提出不同解决方案,锻炼培养学生的综合解决问题和技术创新的能力。

如图 1 所示,学生在应用场景模块中,先发现位置查询服务中会泄露的隐私内容,通过实现

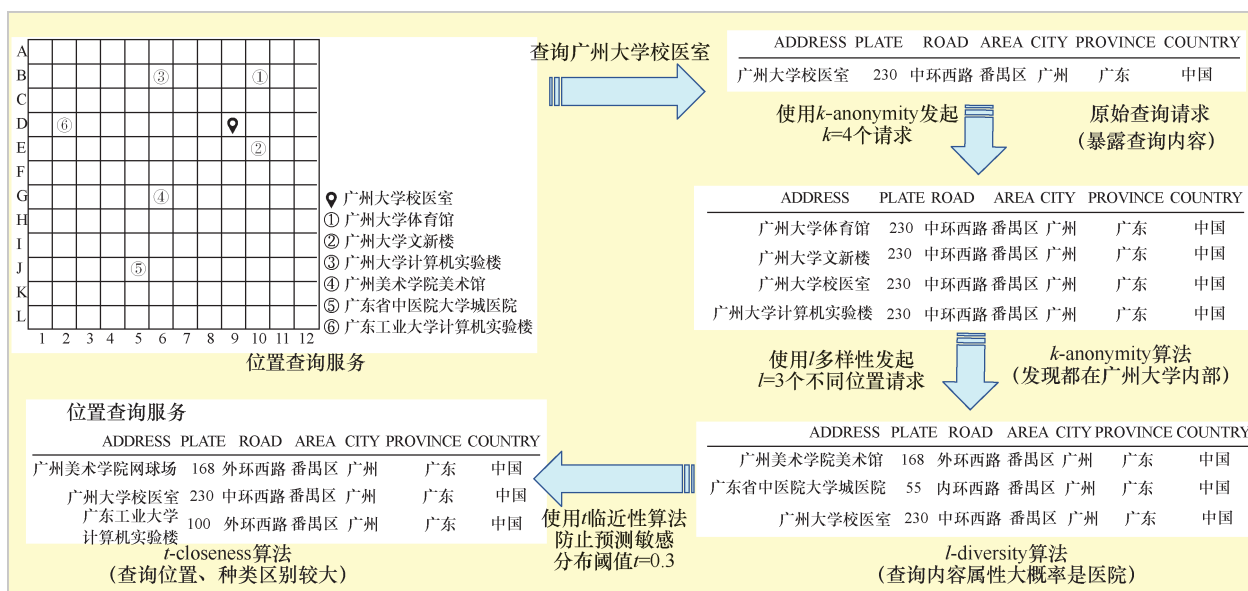


图1 基于位置服务场景靶场模块的综合实践导向教学方法

Figure 1 An integrated practice oriented teaching method based on location service scenario range module

经典算法,了解 k -anonymity 隐私保护的运行机理。然后通过不断增加的背景信息和攻击条件,在原有算法的基础上,扩展实现 l -diversity 和 t -closeness 算法。最终通过在教学实训靶场中反复拆解和扩展算法,提升学生解决实际问题的能力。

3.4 基于“‘方班’研讨厅”的创新思维训练

本课程在广州大学“方滨兴院士实验班”(简称“方班”)特色课程体系下,在授课过程中积极与其他相关课程联动,尤其与“‘方班’研讨厅”特色教学模式^[10-11]紧密结合。

“方班”特色课程体系是围绕实践创新能力培养而设计的立体式课程体系,构建了横向“知识线”、纵向“技能链”、立体“能力网”的“织网”式授课机制。“‘方班’研讨厅”课程按照研讨点评式教学模式建设,由方滨兴院士联合国际知名专家亲身授课,已完成 109 期的课堂教学活动,目前已推广到哈尔滨工业大学、电子科技大学、北京邮电大学、南京邮电大学等 16 所高校。该课程以“创新与思辨”为核心,主题由研究生和指导老师共同选定,从选题、演讲、提问、总结 4 个环节完成核心主题的汇报。在授课过程中,“‘方班’研讨厅”课程为学生创新思辨提供方法论,“数据隐私保护”课程为学生提供演练的内容素材。

如图 2 所示,研究生在正式汇报之前的 2~3 周与指导老师沟通,选择合适的隐私保护主题,内

容可以是阅读的学术前沿论文、发现的科研问题以及自己提出的解决方案。在两周的查询资料、阅读文献之后,了解当前隐私保护学术前沿中的方法,对其进行文献分析,挖掘现有方案的隐私风险和不足,设计有针对性的改进方案,并在条件允许情况下进行一定的实验评估,验证自身的想法。在离正式汇报前一周的时候,研究生将自己调研、分析、设计的内容制作成汇报 PPT,并进行演练。在正式汇报时,研究生要进行 20~30 min 的汇报,并接受同学和老师的提问。在提问中维护自己的立场,并吸收别人问题中有用的部分,进行思辨。最后经过方滨兴院士等专家的点评,对汇报中的优缺点进行分析,挖掘内部的机理。在汇报结束后一周内,对所汇报的过程进行反思和总结,并在修改后向指导老师和同方向同学进行二次汇报,用以评估反思和改正的效果。

在双课程联动过程中,学生在数据隐私保护领域发现问题、分析问题和解决问题的能力得到了深度锻炼。在训练过程中掌握创新思维的方法,并以实际问题进行实践。部分学生在训练过程中,确定了自己学位论文的研究方向和突破点,其中不少学生以此为出发点申请或发表了具备一定创新性的国家发明专利和学术论文。

3.5 以职业道德为基础的课程思政教育

“数据隐私保护”课程培养专业技术人员的出

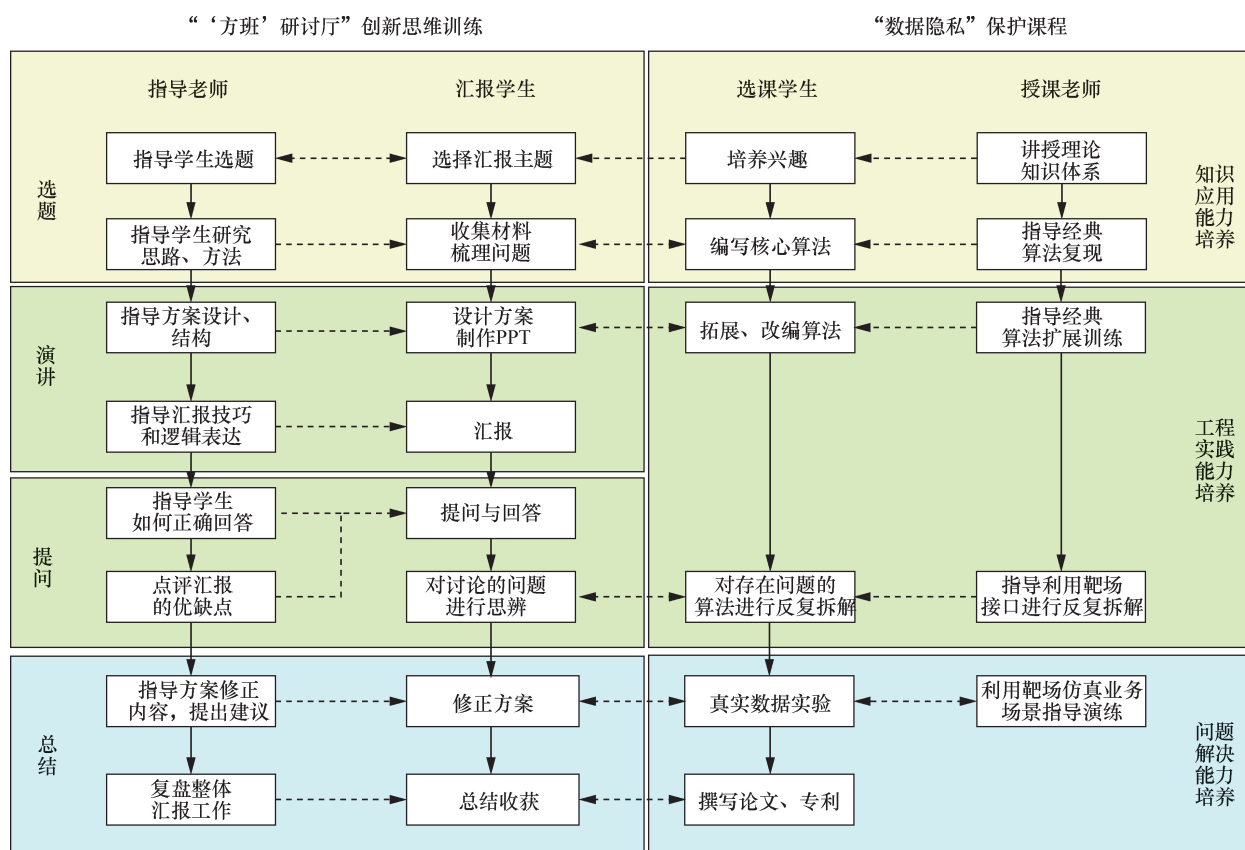


图2 基于“方班研讨厅”的隐私保护创新思维培养

Figure 2 Innovative thinking cultivation of privacy protection based on "Fangban seminar room"

发点是维护国家和公民的基本隐私权利, 隐私保护方向教师应进一步促进“课程思政”与“思政课程”两者的有机融合, 更好地服务学生思想教育。数据已成为国家基础性战略资源, 其在为社会创造价值的同时, 遭到非法收集、泄露和滥用, 严重威胁了公民的隐私权益和国家的安全稳定。因此, 隐私保护从业人员就是保护国家数据战略资源的一道重要防线。

在课程讲授过程中, 通过法律法规、行业动向、技术标准、国际形势等方面的学习, 提升学生思想认识、文化素养、道德品质、政治觉悟, 引导学生“肩负历史使命, 坚定前进信心, 立大志、明大德、成大才、担大任”。

(1) 法律法规学习

近年来, 以欧盟《通用数据保护条例》为标志, 各国针对数据安全和隐私保护颁布了符合本国情况的法律法规, 加强了对数据和个人信息的保护。数据跨境流动政策变动已经导致世界贸

易规则的重构, 对企业和个人服务提供者产生了重大影响。

在我国, 随着《网络安全法》《数据安全法》《个人信息保护法》以及《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》等法律法规的正式实施, 对数据安全, 特别是个人信息保护的合规性提出较高的要求。通过学习这些法律法规, 加强隐私保护专业学生的专业素养, 铭记国家法律红线。

(2) 职业道德培养

2019年9月, 习近平总书记对国家网络安全宣传周作出重要指示, 国家网络安全工作要坚持网络安全为人民、网络安全靠人民, 保障个人信息安全, 维护公民在网络空间的合法权益, 网络安全的发展要走好以人民为中心的网络群众路线, 更需要每一个从业者和公民的不断支持与参与。

数据隐私保护技术岗位作为新兴职业, 无论

其工作范畴还是职业道德都在缓慢形成中。但无论其发展走向如何,隐私保护岗位而立身根本在于保护公民隐私,作为一门保护公民合理利益的岗位,其职业道德的要求则高于其他相关行业。因此在教学过程中,始终穿插职业道德培养是重要且不可或缺的。

隐私保护从业人员,并不仅是帮助企业生产过程中的合规人员。在工作过程中,不能为了利益对隐私保护效果进行夸大,或者对隐私泄露事件进行隐瞒。一旦隐私保护防线变成了可有可无的装饰,势必会导致该岗位的消失。因此,坚守职业道德,既是坚持立业初心,也是隐私保护从业人员的自身需求的延续。

4 教学效果

本课程的教学内容与教学方法在2019—2021级“方班”研究生培养过程中进行教学实践。在理论知识构建、工程能力训练和创新思维培养等方面成效显著,积累了一系列教学案例和教学成果,为后期提升与改进奠定了基础。

(1) 理论知识构建

教学团队为选课的研究生设计了一条快速构建知识体系的学习路径。由于选课学生存在本科专业多样的问题,且各自掌握的专业背景知识程度不同,因此将前驱课程背景知识按照模块化进行细粒度分解。学生可以根据自身背景情况,选择合适的起点开始学习。此外,为了在最短时间里,让跨专业学生跟上课程进度,前驱课程背景知识中只包含必要知识点,剩下相关知识作为条目供学生扩展学习。学生可以再根据自己的学习能力,进行灵活调控而不至于跟不上知识结构。

为了实现课程设计中的理论知识运用能力,教学团队依托广州大学研究生院,设立了广州大学研究生“网络空间安全之隐私保护创新实践”项目。共有7名研究生入选,专业分别为信息安全、软件工程、信息工程、网络工程、信息与计算科学、数学与应用数学、高分子材料与工程,涵盖了不同程度的专业背景知识。针对特定应用场景的隐私保护问题,指导研究生分析隐私保护需求,梳理隐私保护技术及其前驱知识,运用课

本所学的理论知识,解决实际场景中特定的隐私泄露问题。在此基础上,教学团队积累实际教学经验,了解了不同专业背景的学生在运用隐私保护理论知识解决实际问题中的痛点和难点,不断完善教案和实验指导书。

(2) 工程能力训练

工程能力需要反复练习和实践才能逐渐掌握。广州大学“方班”教学团队从2019年开始建设人工智能和数据分析相关教学靶场,从数据集预处理、智能算法分析实现、业务场景应用和测试等环节为学生提供在线仿真的教学环境。

课程的理论知识构建让学生学习了隐私保护及其前驱课程的经典算法,为后续工程实践、科研创新提供了算法基础。教学实训靶场为复现隐私保护领域经典算法的问题分析、算法设计和效果评估提供了实训平台,并为隐私保护算法的高级应用和创新性改造提供实战演练环境。算法拆解与编排课程,为学生提供数据库、地理位置、图像数据集、社交网络数据集等的经典数据集和效果评估接口,学生通过反复拆解、重构,学习经典算法的内在机理。应用场景模块拓展了隐私保护算法,将算法与业务紧密结合,提供某个隐私保护算法在具体领域的应用和安全探索。教学团队通过一系列课程创新,从算法、数据集、扩展、应用等层面拆解隐私保护学习的阶段,为学生提供更加深入、体系、可实训的教学环境。

(3) 创新思维培养

教学团队与京兰大数据、奇虎360、奇安信、海康威视等企业建立了医疗大数据应用及安全、物联网智能应用及安全、云安全、移动终端安全等10余家校企联合实验室,为教学提供了实际的业务逻辑和应用场景。在此基础上,教学团队将工业界的实际隐私保护问题和教学相结合,将实际项目中的算法模块融合教学环境,在教学实训靶场上提供仿真数据集、示例算法等让学生实践,并启发学生设计新算法,解决实际项目中的难题。

通过实际问题和教学指导的深度融合,学生可以将业务需求或科研难题作为课程作业解决,也可将课程上学到的算法应用于实际工业界的业

务场景,有助于学生提前接触工业界的业务场景和学术界的科研课题,培养创新思维。在此基础上,通过充分准备和设计的解决方案,在“方班研讨厅”上进行思维碰撞和反复迭代,培养解决真实场景问题的能力。

(4) 课程教学成果

在教材编写方面,针对当前市面上数据隐私保护教材“重理论、清实践”的问题,广州大学“方班”教学团队整理数据隐私保护课程的教学过程中的教学经验,整理编著了一套实践导向的教材《隐私保护技术实验教程》^[12]。

在学术成果方面,选课学生在隐私数据安全聚合、隐私脱敏、隐私保护与可用性优化、隐私数据审计等方面设计了多个新颖的隐私保护方案,并在 TNSE、DCN、Computer Communications、WCMC 等国际会议和学术期刊上发表论文 10 余篇,申请国家发明专利 20 余项。

在竞赛成果方面,选课学生组队参加了中国人工智能学会主办的第六届全国青年人工智能创新创业大会,其设计的多方数据共享隐私保障系统获创新组一等奖。所开发的基于区块链的隐私数据安全分享系统、基于联邦学习的多方数据隐私保护系统通过了 CMA 第三方测评,并在国家电网、中国电科等单位进行项目交付。

在持续改进方面,在经过 3 年的课程教授和学生反馈过程后,教学团队不断充实优秀教案,并可根据技术发展增加新的课程内容单元,如联邦学习、区块链等。在授课过程在不断优化授课单元内部的环节,对授课进度进行调整。在此基础上,学院逐步扩大数据隐私保护课程的授课归并,并扩展到本科生的选修课中进行试点。

5 结束语

广州大学“方班”教学团队面向当前我国隐私保护技术人才培养需求,针对当前研究生存在的知识体系不全、实践经验缺乏、创新思维不足等问题,提出了基于教学实训靶场的数据隐私保护教学方法,并结合“‘方班’研讨厅”的创新思维训练模式,通过教学团队近 3 年的教学实践,所培养的研究生在知识应用能力、工程实践能力、

综合创新能力等方面得到了较大的提升,为“数据隐私保护”课程提供了初步的建设思路和有益的探讨。

参考文献:

- [1] IDC 中国. 2021 年 V2 全球大数据支出指南[R]. 2021.
IDC China. V2 Global big data spending guide 2021[R]. 2021.
- [2] 吴英杰. 隐私保护数据发布: 模型与方法[M]. 北京:清华大学出版社, 2015.
WU Y J. Privacy-preserving data publication: models and methods [M]. Beijing: Tsinghua University Press, 2015
- [3] 张艳硕, 李泽昊. 零知识证明的分层次案例化教学设计[J]. 北京电子科技学院学报, 2020, 28(4): 92-101.
ZHANG Y S, LI Z H. A hierarchical case-based instructional design for zero-knowledge proofs[J]. Journal of Beijing Electronic Science and Technology Institute, 2020, 28(4): 92-101.
- [4] 黄靖. 基于翻转课堂的医学伦理学教学设计——以“隐私保护权”为例[J]. 成都中医药大学学报(教育科学版), 2017, 19(3): 59-60, 95.
HUANG J. The teaching design of medical ethics based on flipped classroom——taken privacy protection as an example[J]. Journal of Chengdu University of TCM (Education Science Edition), 2017, 19(3): 59-60, 95.
- [5] 范新民. 基于移动学习和翻转课堂深度融合的网络信息安全课程教学创新实践与探索[J]. 网络与信息安全学报, 2017, 3(9): 61-66.
FAN X M. Practice and exploration of network information security course teaching innovation based on mobile learning and inverted classroom depth integration[J]. Chinese Journal of Network and Information Security, 2017, 3(9): 61-66.
- [6] 张宁, 谭示崇, 傅晓彤, 等. 基于 SPOC 和翻转课堂的现代密码学课程改革总结与分析[J]. 网络与信息安全学报, 2019, 5(3): 89-95.
ZHANG N, TAN X C, FU S T, et al. Summary and study on the curriculum reform of modern cryptography based on SPOC and flip classroom[J]. Chinese Journal of Network and Information Security, 2019, 5(3): 89-95.
- [7] 魏悦川, 韩益亮. 计算机密码学课程的混合式、参与式教学研究与实践[J]. 计算机教育, 2019, 291(3): 27-29.
WEI Y C, HAN Y L. Research and practice of blended and participatory teaching in computer cryptography courses[J]. Computer Education, 2019, 291(3): 27-29.
- [8] 姜顺荣. 面向网络空间安全的计算机网络教学改革研究[J]. 科学大众(科学教育), 2017 (11): 147.
JIANG S R. Research on the reform of computer network teaching for cyberspace security[J]. Science Public (Science Education), 2017(11): 147.
- [9] 陈雪飞. 应试教育背景下大学生学习心理分析[J]. 校园心理, 2019, 17(3): 210-212.
CHEN X F. Psychological analysis of college students' learning in the context of test-based education[J]. Journal of Campus Life &

Mental Health, 2019, 17(3): 210-212.

- [10] 鲁辉, 王乐, 田志宏. 网络空间安全人才培养新模式探索[J]. 保密科学技术, 2018, 10: 54-57.

LU H, WANG L, TIAN Z H. Exploring the new model of cyber-space security talent development[J]. Secrecy Science and Technology, 2018, 10: 54-57.

- [11] 王乐, 田志宏, 鲁辉. 聚焦人才安全的网络安全研究生品格教育探索[J]. 杭州电子科技大学学报(社会科学版), 2020, 16(4): 64-67, 72.

WANG L, TIAN Z H, LU H. Exploration of character education in cyber security graduates based on talent security[J]. Journal of Hangzhou Dianzi University (Social Sciences), 2020, 16(4): 64-67, 72.

- [12] 殷丽华, 孙哲, 何媛媛, 等. 隐私保护技术实验教程[M]. 北京: 科学出版社, 2022.

YIN L H, SUN Z, HE Y Y, et al. Experimental tutorial on privacy protection technology [M]. Beijing: Science Press, 2022.

[作者简介]



孙哲 (1987-), 男, 安徽安庆人, 博士, 广州大学副教授, 主要研究方向为隐私保护、数据安全。



宁洪 (1961-), 女, 河北丰润人, 广州大学教授, 主要研究方向为软件工程。



殷丽华 (1973-), 女, 辽宁朝阳人, 博士, 广州大学教授、博士生导师, 主要研究方向为网络空间安全、隐私保护。



方滨兴 (1960-), 男, 江西万年人, 博士, 中国工程院院士, 广州大学教授、博士生导师, 主要研究方向为计算机体系结构、计算机网络与信息安全。