人工智能赋能网络空间安全方向研究生教学改革的初探*

殷红建 郝银凤** 马宇翔

河南大学计算机与信息工程学院，开封 475004

摘 要 针对网络空间安全方向研究生课程中隐私计算理论实践脱节、教学手段缺乏智能化等问题，提出一种人工智能（AI）赋能的教学改革方案，聚焦“安全多方计算”核心内容，探索大模型技术融入教学的有效路径。通过重新设计教学目标、优化教学内容模块、创新教学模式以及多元评价机制，将安全多方计算前沿知识与大模型相结合。教学中引入大语言模型辅助课堂讲解、实验实践和互动讨论，采用线上线下相融合的模式，强化案例研讨和项目驱动学习。所设计课程方案构建涵盖理论讲授、实践训练和 AI 辅助学习的教学流程，形成安全多方计算与大模型深度融合的教学模式。预期能够提升学生对隐私计算理论的掌握深度和实践能力，提高学习参与度和科研创新意识。多维度评价结果表明该模式有望改善传统教学中存在的效率和效果不足。AI 赋能的教学改革可有效弥补网络安全领域研究生培养中理论与实践脱节的短板，提升教学质量和人才培养效果，为新工科背景下网络安全人才培养提供有益借鉴。

关键字 AI 赋能，网络空间安全，隐私计算，大模型，教学改革

Preliminary Exploration of AI-Empowered Graduate Teaching Reform in Cyberspace Security

Yin Hongjian Hao Yinfeng Ma Yuxiang

School of Computer and Information Engineering of Henan University
Kaifeng 475004, China
haoyinfeng@henu.edu.cn

Abstract—To address the disconnect between privacy computing theory and practice and the lack of intelligent teaching methods in graduate courses on cyberspace security, this paper proposes an AI-empowered teaching reform focusing on secure multi-party computation as the core content, and explores effective ways to integrate large-model technologies into instruction. By redesigning teaching objectives, optimizing content modules, innovating teaching approaches, and employing multifaceted evaluation mechanisms, cutting-edge knowledge of secure multi-party computation is combined with large models. The teaching process incorporates large language models into classroom lectures, experimental practice, and interactive discussions, adopting a blended online-offline format that reinforces case analysis and project-based learning. The proposed course structure spans theoretical lectures, practical training, and AI-assisted learning, creating a deeply integrated teaching model of secure multi-party computation and large models. It is expected to enhance students' grasp of privacy computing theory and practical skills, as well as boost learning engagement and research innovation. Multi-dimensional evaluations suggest this approach can address inefficiencies in traditional instruction. AI-empowered teaching reform effectively bridges the gap between theory and practice in graduate cybersecurity education, improving teaching quality and talent development, and providing valuable insights for cultivating cybersecurity professionals under the new engineering paradigm.

Keywords—AI empowerment, cyberspace security, privacy computing, large models, teaching reform

1 引 言

当前，新一代人工智能技术蓬勃发展，对高等教育特别是研究生教育带来了深刻影响。研究表明，生成式人工智能可用于动态生成个性化的教学资料和学习环境，帮助教师更新课程内容、设计讨论问题和作业，并辅助评价反馈[1]。在研究生教育中有效利用人工智能手段，有望提供海量丰富的教学资源和精准个性化的学习路径，创造虚实结合的教学场景，从而极大推动教育教学的改革创新。与此同时，人工智能的应用也对研究生教学提出新挑战，例如人才培养目标需迭代更新、教学内容亟待重构创新、实践范式发生变革，以及教学质量评价方式也需随之改进。在网络空

*基金资助：本文得到河南大学校级教改项目-教师教学发展专项(HDXJJG2024-048，HDXJJG2024-028，HDXJJG2023-113)资助。

**通讯作者：郝银凤 haoyinfeng@henu.edu.cn。

间安全领域，数据安全与隐私保护已成为热点，国家政策层面强调推进安全多方计算、联邦学习、同态加密等隐私计算技术的部署应用[2]。安全多方计算（SMPC）是一种典型的隐私计算技术，允许多个参与方在不泄露各自私有数据的情况下共同计算函数结果。然而，由于 SMPC 理论复杂、实现门槛高，当前高校相关课程中存在理论讲授与实践应用脱节的问题[3]。同时，网络安全技术更新迅速、内容繁杂，研究生学习者背景多样，给传统教学模式带来挑战[4]。为此，有必要探索人工智能赋能的教学改革，创新教学模式，将“大模型”等先进 AI 技术融入网络空间安全研究生课程安全多方计算的教学中，以提升教学效果和培养学生的创新实践能力。本文面向上述需求，设计了一套融合 AI 大模型技术的网络空间安全研究生课程教学方案，重点围绕安全多方计算内容进行教学创新，以期为新工科背景下研究生教育教学改革提供参考。

2 教学改革的背景与需求

2．1 行业发展与课程现状

网络空间安全已成为国家战略需求的重要领域，高校相继设立“网络空间安全”一流学科和学院，培养高层次网络安全人才。在大数据和物联网时代，海量敏感数据需要保护隐私安全，安全多方计算等隐私保护技术成为学术和产业关注焦点。近年研究显示，SMPC 虽然理论研究活跃，但在资源受限设备、大规模数据场景下的实用化仍面临挑战。这意味着研究生既需扎实掌握 SMPC 理论原理，又要了解最新应用进展和工具。然而传统课程往往偏重密码学理论推导，实践环节不足，导致学生对该技术“知其然不知其所以然”，难以将理论应用于实际场景。另一方面，人工智能技术的发展为课程改革提供了新机遇。生成式大模型（如 ChatGPT 等）具备强大的知识获取和内容生成能力，能够辅助教师快速更新教学案例和实验内容[4]。例如，教师可利用大模型生成贴近前沿的新问题作为课堂讨论材料，或让模型扮演虚拟助教解答学生疑问。这些 AI 赋能手段有望缓解网络安全课程内容更新速度慢、教学资源不足的问题。有研究针对网络安全教育进行了系统分析，发现约 19%的现有研究成果可以通过引入 AI 技术整合进安全课程，以丰富教学内容并提升教学效果。因此，本课程改革需要顺应隐私计算和人工智能的发展趋势，在教学中引入大模型技术，丰富课程内容和教学方法，以满足网络空间安全学科的人才培养新需求。

2．2 教学痛点与挑战

首先，安全多方计算理论复杂抽象，学生学习门槛高。现有教学中缺乏形象直观的案例和实践，学生难以理解多方协议的细节和作用。其次，网络空间安全技术更新快，课程内容需要不断更新，但传统教材和授课难以及时覆盖最新进展。再次，在“大模型”时代，研究生可能利用AI代写作业、代码，这对学术诚信和教学评估提出了新挑战[5]。教师需要投入精力引导学生正确使用AI工具，防止过度依赖造成独立思考能力下降。此外，传统教学方式以教师讲授为主，实践和讨论环节不足，难以培养学生解决复杂安全问题所需的创新能力和协作能力。最后，评价机制单一（如仅依据考试成绩）无法全面反映学生对前沿知识的掌握和实践应用能力，特别是在引入AI工具后的学习过程中，需要新的评估维度。综上所述，本课程改革亟需针对以上痛点进行改进：强化实践教学以降低SMPC学习难度，及时融入新兴技术内容，引导学生规范地使用AI大模型辅助学习，并建立多元评价体系确保培养质量。

3 教学设计方案

3．1 教学目标

本教学方案面向网络空间安全方向的研究生，围绕安全多方计算及相关隐私计算技术，设定以下四个方面的教学目标。

掌握核心理论原理：学生应系统掌握安全多方计算的基本原理、典型协议（如秘密共享、混淆电路等）及其在数据隐私保护中的作用，了解联邦学习、差分隐私等相关技术的概貌，为深入研究打下理论基础。

提高实践应用能力：学生能够基于现有开源框架或工具动手实现简单的多方安全计算任务，学会配置实验环境、设计多方协议流程，理解算法性能瓶颈，积累隐私计算实践经验。通过项目训练，培养将理论应用于解决实际网络安全问题的能力。

融合 AI 辅助创新：学生了解大型 AI 模型在网络安全和隐私计算领域的应用前景，掌握与 AI 大模型高效交互的技巧（如提示词工程方法）。能够借助大模型辅助文献调研、代码生成和结果分析，提高科研与学习效率[6]。在此过程中，培养学生的自主学习和创新思维，使其具备将 AI 技术与本专业前沿课题相结合的意识和能力。

发展软技能与学术素养：通过小组合作和课堂研讨，提高学生的团队协作能力和沟通表达技巧；强化对学术规范的理解，明确 AI 辅助下保持学术诚信的要求，树立正确的科研道德观。此目标确保学生在掌握新技术的同时，综合素质和职业素养也得到同步提升。

3．2 教学内容与模块安排

按照教学目标，本课程内容涵盖理论讲授、案例研讨、实验实训等模块，结构如下。

隐私计算导论（理论基础）：介绍数据隐私保护的背景和意义，梳理隐私计算的发展脉络。重点讲解安全多方计算的基本概念、威胁模型和安全准则，比较SMPC与其他隐私保护技术（联邦学习、同态加密等）的异同，让学生建立全局认识。引用真实案例说明在金融、医疗等场景中隐私计算的必要性，激发学习兴趣。

安全多方计算协议原理：深入讲授SMPC经典协议和算法。包括：基于秘密共享的加法电路计算原理，Yao的混淆电路协议及其应用，两方/多方计算协议的安全性证明要点等。通过数学推导和示例演示，让学生理解协议的工作流程和安全保证。在课堂中穿插小型推演练习，例如两方安全求交集的步骤推演，加深对抽象原理的理解。

实践工具与实验模块：安排动手实验环节，指导学生使用开源的SMPC框架或平台（如PySyft、FATE等）完成简单任务。例如，将多方数据输入平台计算某统计量，验证各方仅获结果不泄露输入。实验内容循序渐进：先由教师演示一个完整示例，再由学生分组实践扩展。通过实验操作，学生体会算法实现细节和性能开销。引入AI助手支持：例如使用大模型生成部分代码模板或提供错误调试提示，降低实践门槛的同时强调对代码结果的验证。

大模型赋能专题：讲授人工智能大模型技术及其在网络安全中的应用概览。内容包括：大语言模型（如GPT）的基本原理、能力边界和局限；生成式AI在安全漏洞挖掘、威胁情报分析、隐私数据合成等方面的最新研究进展[4]。重点探讨大模型与隐私计算的交叉：例如介绍利用安全多方计算保护大模型训练数据隐私的案例，或利用大模型快速分析SMPC协议参数配置的可能性。安排讨论：让学生思考如何在保证隐私的前提下使用大模型，培养辩证思维。

综合案例与前沿研讨：在课程后期，引入综合性案例研讨和小型项目。案例例如“多方共享医疗数据的联合模型训练”或“联邦学习中的安全协议设计”，涵盖SMPC与AI的融合应用。学生分组分析案例中的问题和挑战，设计解决思路并讨论可行性。每组需查阅近期文献，利用所学提出改进方案。随后进行课堂报告分享，师生共同评议。在研讨基础上，邀请学生展望该领域未来发展，激发科研兴趣。

各模块按教学周序展开，理论授课与实践交替进行。课程开始侧重理论夯实，中期加强实验和案例，后期聚焦项目和研讨。通过上述模块化安排，实现知识传授与能力培养并重，为后续评价考核提供支撑依据。

3．3　融合 SMPC 与大模型的教学模式设计

本教学改革采用“课堂讲授 + 实践训练 + 探究任务”相结合的混合教学模式，旨在通过人工智能技术提升安全多方计算课程的教学效果，教学模式流程如图1所示。

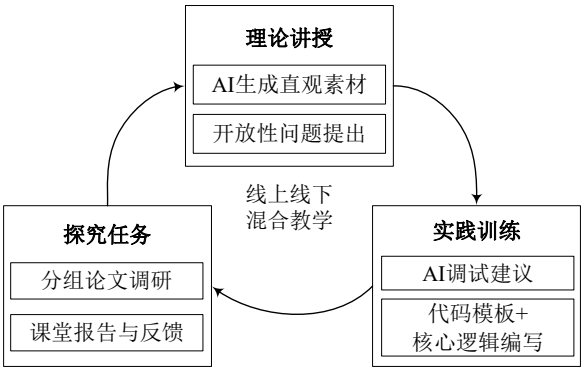

图 1　教学模式流程图

在课堂讲授中，教师利用大语言模型生成直观的教学素材。例如，在讲解Yao的混淆电路时，教师通过大模型生成一个简单的AND门电路混淆过程的步骤说明，包括混淆表格的构建和评估流程的演示。这些内容以图文结合的形式呈现，帮助学生理解抽象概念。课堂上，教师提出问题如“如何将混淆电路扩展到复杂函数？”，并利用大模型生成多种解答思路，引导学生展开讨论，教师再对模型输出进行点评，拓展课堂互动维度。

在实践环节，学生通过定制的AI聊天机器人获得实验支持。例如，在使用PySyft框架实现安全两方计算时，学生可能遇到代码错误，可向聊天机器人描述问题，如“为何我的协议未正确输出结果？”，机器人会提供调试建议或解释相关API用法。为避免过度依赖，系统要求学生验证AI建议的正确性，培养批判性思维。此外，教师提供部分由大模型生成的代码模板，学生需完成关键逻辑部分，确保理解算法核心。

为培养学生主动学习能力，课程设计了探究式任务。例如，学生分组利用大模型调研安全多方计算在联邦学习中的最新应用，生成文献综述并进行课堂报告。此活动鼓励学生设计高效提示词，评估模型输出可靠性，并将AI辅助成果融入学术表达，培养自主学习和创新思维。整个教学过程坚持线上线下相结合，线下侧重讨论辩论和实操演练，线上拓展学习资源和智能辅导。教师发布扩展阅读和前沿论文，由大模型生成提要供学生参考，提高文献研读效率。同时，引入学习数据分析机制，利用AI分析学生在课堂测验、作业中的表现数据，及时发现共性问题反馈给教师，以便调整教学策略，实现因材施教。

在引入AI技术的同时，教师反复强调学术诚信与规范使用。课程开始即设置“AI工具使用守则”讨论

环节，明确哪些情景下可以使用大模型辅助、如何引用模型给出的材料等，防范不当使用造成抄袭或学术不端。

3．4 预期学期效果

表 1 教学改革前后学生表现对比

项目类别	改革前平均值	改革后平均值	提升幅度
安全多方计算实验完成率	62%	91%	+29%
期末理论测验平均成绩	73.1	86.2	+13.1
AI 工具使用熟练度（问卷得分）	3.2/5	4.5/5	+1.3
小组讨论参与积极度（教师评分）	中等偏低	高	显著提升

通过实施上述教学方案，预期将取得显著的教学成效。首先，在知识掌握方面，学生能够在较短时间内全面了解安全多方计算的核心概念和流程，对隐私计算相关技术形成系统认知。与传统教学相比，学生对抽象理论的理解更加深入，能够准确阐释关键协议的原理，并举例说明其应用场景。这体现在课程测验和提问回应中正确率和准确性的提高。

其次，在实践能力方面，学生经过多轮实验和项目训练，基本具备独立完成SMPC方案设计与实现的能力。例如，学生可以配置一个小规模的多方计算实验，正确执行并分析结果，对性能瓶颈有所体会。这种实践能力的提升为其后续科研奠定基础。

第三，在AI素养与应用能力方面，学生掌握了与大模型交互的有效方法，包括设计针对特定问题的提示词、评估大模型输出的可靠性等。他们可以熟练运用AI工具查找资料、辅助编程和分析数据，大幅提升了学习与研究效率。同时，学生对AI技术的局限也有清醒认识，知道如何避开“大模型”的潜在谬误，保证输出结果的准确性和可信度。

第四，在创新意识和综合能力方面，基于案例研讨和开放性项目训练，学生表现出更强的主动探索和创新思考能力。许多学生在课程末能够提出具有新意的想法，例如改进现有协议的思路或将SMPC应用于新场景的设想，展现出良好的科研潜质。此外，小组协作和课堂讨论的融入使学生的团队合作精神和沟通能力得到锻炼提升。

最后，在学术规范意识方面，通过对AI伦理和学术诚信的强调，学生更加自觉地规范使用AI工具，提交的作业报告中引用来源明确，杜绝了简单抄袭现象，学习风气更加严谨。综合来看，本教学改革方案有望培养出既精通网络空间安全专业知识，又熟练运用人工智能工具的复合型人才，满足新形势下行业对高层次网络安全人才的要求。表1展示了改革前后学生在实验完成率、理论成绩和AI应用熟练度等方面对比，结果显示学生在上述方面均有显著提升，体现出教学模式优化带来的积极影响。课程取得的实际效果也将通过科学的评估机制进行验证和反馈，以持续改进教学设计。

3．5 学习评价与考核机制

为了全面客观地评价学生的学习成效，本课程构建了多元化的评价考核机制。考核内容包括以下六个方面。

理论知识测验（20%）：通过期中、小测验等形式考察学生对安全多方计算理论基础的掌握情况，包括重要概念理解、协议原理推导等。此部分重点评估学生的知识理解深度。

实验与项目表现（25%）：根据学生在实验课和课程项目中的表现打分，考察其实践动手能力和问题解决能力。评分维度包含实验操作的熟练程度、项目方案的完整性与创新性、结果分析的准确性等。小组项目中还会根据个人贡献进行差异化评分。

AI 工具应用（15%）：评价学生在课程中使用大模型等 AI 工具的情况。例如，学生需提交一次“AI 助理实验报告”，记录其为解决某问题与大模型交互的过程、提示词设计及获得的收获。评分关注其提示设计是否有效、对 AI 输出结果的判断是否准确合理。该项考核鼓励学生善用 AI 又不盲从 AI。

课堂参与与讨论（15%）：根据学生平时回答问题、参与讨论和案例研讨的积极性给予评分。重点考察其表达沟通能力、逻辑思辨能力以及将理论应用于分析实际问题的能力。鼓励发表有见地的见解和建设性意见。

综合报告与反思（15%）：在课程末要求每位学生提交一份学习报告或心得反思，总结自己在安全多方计算与 AI 赋能学习中的收获、存在不足及改进计划。评分依据报告内容的深度、对课程知识的融会贯通程度、以及自我认识的客观性和独到见解。此环节促使学生对自身学习进行沉淀思考。

团队协作（10%）：对于分组完成的任务，由组内互评和教师评价结合，考察学生合作态度、任务分工执行情况以及团队成果。这一指标激励学生在协作中学习，在互助中进步。

上述各项考核指标按设定权重计入总评成绩，使最终成绩能够综合反映学生在知识、能力、素质等方面的学习成果。权重设置上相对均衡（各项权重范围10%~25%），避免单一考试定成绩的局限，更加全面、公平地评价每位学生。此外，评价过程中注重定性与

定量相结合：既有客观题得分等量化数据，也有教师对项目报告的质性反馈，力求对学生表现的评价科学有效。通过多维度考核与反馈，不仅可以衡量教学目标的达成度，也为后续教学改进提供了依据，形成教学评估—反馈—优化的闭环，持续提升教学质量。

4 结束语

面向“人工智能+隐私计算”背景下研究生教育教学的新要求，本文探索了人工智能赋能的网络空间安全研究生课程教学改革方案，以安全多方计算课程为载体，将大模型技术融合进教学全过程。通过明确教学目标、丰富课程内容模块、创新教学模式以及重构评价机制，本方案构建了理论与实践并重、人机协同的教学新模式。预期实施效果表明，该模式能够显著提升学生对复杂安全技术的学习效率和理解深度，培养其运用 AI 工具解决实际安全问题的能力，促进创新思维和科研素养的养成。特别是在安全多方计算这一隐私计算前沿领域，AI 赋能的教学手段有效弥合了学术理论与工程实践之间的鸿沟，使学生在掌握先进理论的同时，具备将其应用于数据安全实际场景的能力。这对于加快培养既精通网络安全专业知识又熟练掌握人工智能技能的复合型人才具有重要意义。

教学改革的推进过程中也认识到 AI 在教育领域应用的双刃剑效应，既要善用其便捷强大的功能，又需防范其带来的学术规范挑战。因此，在后续实践中将持续关注 AI 在教学中的作用效果，严格守护教学诚信与质量。

总之，本研究所提出的教学改革思路与实践，对推动研究生教育与前沿科技的深度融合具有积极示范意义，可为相关课程的教学改革提供借鉴参考。未来可进一步通过教学实践数据验证和完善该方案，不断迭代优化，促进研究生教育教学的高质量发展。

参 考 文 献

[1] 余超, 冯旸赫, 张俊格. “人工智能”课程教学模式改革及创新实践[J]. 计算机技术与教育学报, 2022, 10(4): 42-45.

[2] 霍炜, 郁昱, 杨糠, 郑中翔, 李祥学, 姚立, 谢杰. 隐私保护计算密码技术研究进展与应用[J]. 中国科学: 信息科学, 2023, 53(9): 1688-1733.

[3] Idoia Gamiz, Cristina Regueiro, et al. Challenges and future research directions in secure multi-party computation for resource-constrained devices and large-scale computations[J]. International Journal of Information Security, 2024, 24:27.

[4] Ryan T. Simmons, Joon S. Park. Innovating cybersecurity education through AI-augmented teaching[C]// Proceedings of the 23rd European Conference on Cyber Warfare and Security (ECCWS), 2024: 476-482.

[5] 赵兴娟, 王靖淞, 时术华, 李鲁艳, 马衍东, 贾曰辰. 人工智能时代新工科背景下“科技写作”研究生课程教学改革的探索[J]. 教育进展, 2025, 15(2): 625-632.

[6] 罗洪盛, 刘毅恒, 何军. AI 大模型虚拟实验辅助学术科研的教学改革探索[J]. 创新教育研究, 2025, 13(1): 424-429.