“一体两翼、双向贯通”：AI 驱动的密码学课程体系构建与实践

宋秀丽**[1] 邓红耀[2] 先兴平[1] 吴涛[1]

1 重庆邮电大学网络空间安全与信息法学院 重庆 400065

2 长江师范学院大数据与智能工程学院 重庆 408100

摘 要 针对人工智能时代密码学教育存在的课程体系零散、理论与实践融合度低、AI 思维与密码内核的渗透不深等问题，本文在 AI 驱动下探讨“一体两翼、双向贯通”密码学课程体系，并基于此贯通本硕理论课程体系，打造“学-练-战”闭环的实践教学体系。深化跨学科融合与产教协同，构建以密码学基础为主体、AI 驱动的理论与实践并重、本硕贯通的学科交叉人才培养新模式。从课程模块、锚点项目、产业实践出发，对学生的综合基础能力、系统能力及创新素养进行全面考察与评价。试点班级学生在系统设计能力、工程实践能力、AI 模型创新能力等维度均有较大幅度的提高。对比 2023 年度，2024 年度的本科生/研究生的实践完成度分别增长了 2.73%/3.48%，教师的教学满意度分别提高了 2.25%/2.00%. 学生在国家级密码类竞赛和产业项目中也取得了较好的成果，为新时代密码学人才培养提供了可借鉴的改革范式。

关键字 AI 驱动，一体两翼，贯通本硕，密码学课程，实践创新

"One Body, Two Wings, Bidirectional Connectivity" : Construction and Practice of an AI-driven Cryptography Curriculum System

Xiuli Song **[1] Hongyao Deng[2] Xingping Xian[1] Tao Wu[1]

1 School of Cyber Security and Information Law
Chongqing University of Posts and Telecommunications
Chongqing 400065, China

2 College of Big Data and Intelligent Engineering Yangtze Normal University
Chongqing 408100, China

Abstract—In response to the problems faced by cryptography education in the era of artificial intelligence, such as a fragmented curriculum system, low integration of theory and practice, and insufficient penetration of AI thinking and the core of cryptography, this paper explores the construction and practice of a "one body, two wings, and two-way connection" cryptography curriculum system driven by AI. Based on this, a new model of talent cultivation will be established, which involves reconstructing and integrating the theoretical curriculum system of undergraduate and postgraduate studies, creating a closed-loop practical teaching system of "learning-practice-battle", deepening cross-disciplinary integration and industry-education collaboration, and building a new model of talent cultivation with cryptography knowledge as the main body, AI-driven theory and practice as the two wings, and the integration of undergraduate and postgraduate studies and interdisciplinary integration as the two directions. Through three levels: course modules, anchor projects, and industrial practices, a comprehensive evaluation of students' overall basic abilities, systematic capabilities, and innovative qualities is conducted. The students in the pilot class have made significant improvements in dimensions such as system design ability, engineering practice ability, and AI model innovation ability. When comparing the teaching effectiveness of 2024 with that of 2023, the practical completion rate of undergraduate and postgraduate students increased by 2.73%/3.48%, and the teaching satisfaction rate of teachers rose by 2.25%/2.00%. Students have achieved excellent results in national-level cryptography competitions and industrial projects, providing a reform model for the cultivation of cryptography talents in the new era that can be referred to.

Keywords—AI-driven, One body with two wings, Integrated undergraduate and postgraduate programs, Cryptography course, Practical innovation

1 引 言

随着人工智能技术的飞速发展和广泛应用，全球高等教育迎来新一波变革风潮和创新契机。在此浪潮之下，如何能够真正挖掘人工智能带来的全新经验与要素，更新网络空间安全学科课程内容、改革教学方法与手段以及思维方式，培养一批具备跨学科素养与创新实践能力的学生，对我国人工智能时代下密码人才培养来说至关重要。密码是网络空间安全的基石，

**通讯作者：宋秀丽 songxl@cqupt.edu.cn

也是国家安全战略的重要组成部分，其人才培养质量决定着我国在网络空间的战略主动权。

近年来，人工智能和密码学交叉融合程度愈发加深，从“人工智能无感密码学”逐渐向“人工智能嵌入密码学”演进。这一技术融合趋势对密码学教育提出了全新要求：传统的密码学课程体系亟待重构，教学内容亟需更新，构建以AI赋能加密算法、智能密码分析及抗AI攻击密码等理论知识为主导的新时代密码学课程。同时，全球范围内对AI与网络空间安全融合型人才的需求激增，进一步凸显了密码学教育改革的紧迫性。2022年，我国教育部明确提出“一体、两翼、五重点”的职业教育改革思路，笔者认为其提出的“融合贯通、一体两翼、能力中心”等观点对于现阶段高等教育依然具有很强的借鉴意义，即要实现学科专业深度融合、整体联动；产教深度融合、交叉互动；信息技术集成应用，深度融合，促进教师实操能力和综合素养的全面提升。

在此背景下，构建以AI驱动为核心特征的密码学课程新体系，不仅是适应技术变革的被动应对，更是引领未来密码学发展的新举措，更是引导今后密码学方向的先决性布局。本文提出的"一体两翼、双向贯通"课程体系，在课程理论上注重系统重组和重新构建，在实践方面强调了教师和学生从各个维度去大胆创新，解决传统密码学教育中存在的课程体系零散、理论与实践融合度低、AI思维与密码内核的渗透不深等一系列突出问题，为目标达成培养出在AI领域掌握密码学知识的专业型人才提供全方案的整体育人对策。

2 国内外研究进展

由于密码学课程涉及的数学理论知识较晦涩难懂，一些学生在学习该课程时存在畏难情绪，因此为了提升教学效果和教学质量，一些研究者和高校教师从如何优化密码学课程的理论和实践教学内容和教学方法方面进行了探讨。

2.1 密码学教学研究现状

在国内，胡小明等学者[1]从理论与实践教学两个角度探讨了信息安全专业的密码学课程。提出了一种结合兴趣案例教学与讲座式教学的教学方法及相应的课堂评价标准。李艳俊等人[2]采用启发式教学法开展密码学实践教学，即教师根据具体的应用需求启发学生按实践步骤完成设计任务。吴旭光等人[3]提出了以培养学生密码实践技能、密码应用方案制定和密码问题解决能力为重点的任务部署、理论讲授、实践操作、小组讨论、报告撰写五个阶段的教学方法。杨建强等人[4]用 Plasptool 设计了包含所有密码学课程重要知识点的 7 个密码学类实验项目。葛爱军等人[5]将CTF 模式引入到密码学实践课程的教学中，采取了学生分组参赛和团队闯关得分的方式，从而提升了课程实践学习的趣味性与挑战性。董建阔等人[6]在新工科的背景下，提出了一种将 OBE 教育理念与 PBL 培养方式相结合的密码实践课程教学设计方案。

在国外，Uhsadel 等人[7]设计了一个以 RSA 加密为核心的结构化项目，引导学生探索不同的设计方案。受到 Feistel 基础研究的启发，Arboledas[8]开发出一款名为“Azrael”的对称字符级加密算法。这一算法由参与导师计划的学生通过三个实际完成的 Python 项目得以实现。González-Tablas 等人[9]则开发了一款实体卡牌游戏“Crypto Go”，借助游戏机制揭示密码学背后的数学原理及其在信息安全中的应用。Percival 等研究者[10]构建了一个名为“CryptoScratch”的框架，作为 Scratch 的扩展模块，通过可视化积木形式呈现密码算法。Abdelhamid 团队[11]开发了基于 Web 的密码学教育工具 vizLab，允许学生以图形化积木的方式直观搭建密码算法。此外，Rayavaram 等人[12]提出了一种结合体验式学习（EL）模型的密码学教学工具，其中融入了丰富的视觉元素以增强学习过程的吸引力。

2.2 AI 赋能密码学教学研究现状

为了适应人工智能时代的冲击，在 2025 年 16 届全国密码学与信息安全教学研讨会上，专门针对 AI 赋能设置课程改革议题，并聚集全国近 150 名专家和学者参加[13]。目前我国在高校开展 AI 与密码学教育已经有了一系列积极的探索。在课程建设方面，多所高校开设了融合性课程，如“AI 与网络安全”、“AI 驱动的网络工程实践”等[14]，并在其密码学课程中增加基于 AI 的加密算法相关的内容。这些课程不仅系统传授 AI 在密码学领域的核心技术，还通过理论与实践相结合的方式，培养学生的应用能力。

关于国外 AI 赋能密码学前沿探索，在 SIGCSE 2025 会议上呈现出两个亮点：第一，注重实际问题反馈，并将算法的思想和过程融入实际问题中，让学生通过不断试错、不断纠正来达到问题的解决[15]；第二，注重学科交叉，相关领域的多所高校学者合作编写的《密码学与人工智能：从共同演进到量子革命》，用二维码的形式直观清晰地展示了密码学与人工智能同步发展，为跨学科课程设计提供了理论支撑[16]。

2.3 当前存在的问题与不足

通过梳理现有文献资料，以及自身教学实践反思，发现目前 AI 赋能的密码学教育具有如下突出的问题：

其一，密码课程体系缺乏系统设计，多呈现“孤岛式”分布。“应用密码学”、“密码技术应用实践”属于本科生的课程，“现代密码学”、“密码算法与协议分析”属于研究生的课程，它们在课程内容上缺

少有效的衔接，在课程目标上也并没有达到由浅入深、逐级进阶的效果，且学生难以构建完整的AI赋能密码学知识图谱。

其二，教学内容滞后于技术发展，教学内容和现实脱节。密码学技术正以前所未有的速度迭代更新，后量子密码、AI辅助密码分析等前沿领域进展迅速，而教学内容却更迭缓慢，所教授的知识，远远落后于行业发展，缺乏对AI环境下密码算法设计与分析的前沿内容，难以满足培养工程型人才的需求。

其三，实践环节薄弱，产教融合程度不足。密码学是一门实践性极强的学科，然而当前教学普遍存在“重理论、轻实践”的现象，且没有为 AI 赋能密码学相关的实践项目提供保障。现有实验项目多为验证性实验，缺乏探索性与创新性，产教融合停留在表面，企业真实需求未能很好地融入到教学过程中去，导致人才能力与产业需求有差距。

3 AI 驱动的密码学课程体系构建与实践

密码学是一门研究编制密码算法和破译密码算法的科学，涉及近世代数、数论、概率论等数学专业领域，在解决黑客攻击、病毒入侵、系统缺陷等诸多安全问题方面起着重要支撑作用。我校的密码学课程包括针对本科生开设的《应用密码学》、《密码技术应用实践》和《密码应用与破解实战》，针对研究生开设的《现代密码学》和《密码算法与协议分析》。其中，《现代密码学》中包含部分量子密码学内容。

为了弥补当前密码学教育中存在的不足，本文构建“一体两翼、双向贯通”的课程体系。其中，“一体”指以密码学核心知识体系为主体，“两翼”分别为 AI 驱动的理论课程体系与实践课程体系，“双向贯通”则强调本科与研究生课程的纵向衔接（纵向贯通）以及密码学与 AI、产业需求的横向融合（横向贯通）。以下从三个方面详细展开。

3.1 理论课程体系重构：分层赋能与动态演进

传统密码学理论课程存在内容滞后、与 AI 技术割裂等问题。本文以“分层赋能、动态演进”为原则，重构了本硕贯通的理论课程体系，如表 1 所示。

具体设计如下：

本科阶段：AI 作为辅助工具与增强视角。以《应用密码学》中古典密码、对称/非对称加密、哈希函数等内容为基础，增设 AI 增强视角。在“哈希函数”章节中添加 AI 增强模块，利用 GAN 生成模型模拟哈希碰撞攻击场景，辅助师生理解哈希的抗碰撞性；在《密码应用与破解实战》的“密码分析”章节，引入机器学习分类模型对密文进行算法识别。

表 1 理论课程体系中的 AI 驱动内容分层设计

课程层级	核心课程	AI驱动模块	能力培养目标
本科基础	应用密码学	机器学习密文分析、GAN哈希碰撞演示	AI工具使用能力
本科进阶	密码技术应用实践	智能密码配置器、AI辅助密码实现	AI工程应用能力
本科综合	密码应用与破解实战	LSTM异常流量检测、强化学习攻击路径优化	AI系统攻防能力
研究生基础	现代密码学	自编码器侧信道分析、可证明安全与AI	AI与密码理论交叉理解能力
研究生前沿	密码算法与协议分析	强化学习辅助形式化验证、GNN协议建模	AI驱动的研究创新能力
研究生跨界	量子密码学	后量子密码AI评估、量子机器学习	前沿领域探索能力

研究生阶段：AI 作为研究伙伴与创新引擎。在《现代密码学》课程中，增设 AI 及密码理论交叉专题“AI 与密码理论”，研究 AI 对密码安全模型带来的影响；在《密码算法与协议分析》课中加强形式化方法和 AI 融合的内容深度，讲授如何利用强化学习指导形式化验证工具在海量状态空间中高效发现算法漏洞；在《量子密码学》中增设“AI 驱动的后量子密码评估”模块，探讨将机器学习算法（支持向量机、聚类分析等）应用于格密码、多变量密码等后量子算法安全评估的问题。

3.2 实践课程体系设计：“学-练-战”闭环与虚实融合

针对实践环节薄弱、产教融合不足的问题，构建了以“学-练-战”为闭环的实践课程体系，并通过虚拟仿真平台开展实验，如表 2 所示。

表 2 实践课程体系的“学-练-战”闭环设计

阶段	核心活动	AI技术与工具	产出成果
学	虚拟仿真实验、AI评分引擎	PyTorch、OpenSSL、LSTM	实验报告、算法实现代码
练	锚点项目开发、跨课程协作	强化学习、联邦学习、同态加密	系统原型、安全评估报告
战	企业项目实战、国家级竞赛	AI攻防工具、可解释性AI	企业项目交付、竞赛奖项

具体设计如下：

（1）“学”阶段：AI 辅助的密码学基础实验

在虚拟仿真平台中集成 OpenSSL、Libsodium 等密码库与 PyTorch、TensorFlow 等 AI 框架，支持学生在线配置实验环境；内置 AI 评分引擎，对学生的实验报告提供迭代性、分步化反馈。设计 AI 增强实验项目，例如，在《密码技术应用实践》中，使用决策树模型推荐最佳密码算法与参数；在《密码应用与破解实战》中，通过 LSTM 网络分析网络流量，实时识别异常加密行为。

（2）“练”阶段：基于锚点项目的系统集成训练

以锚点项目为例，让学生在项目实践训练中提升创新能力。例如锚点项目选题为自适应智能加密网关，目标为实现动态调整加密策略的智能网关。将学生分成蓝方和红方两组，AI驱动点包括：蓝方使用LSTM/GRU模型检测加密网关中的攻击与恶意流量；红方利用深度学习技术探索最优攻击路径，生成对抗样本。并使用跨课程协作完成项目，例如《应用密码学》提供密码算法库，《密码攻防实践》负责算法的攻防实现，《现代密码学》验证协议的安全性。

（3）“战”阶段：参与真实企业项目或国家级竞赛

学生进入企业项目池，以企业提供的真实数据集（恶意流量日志、侧信道轨迹等）作为案例，供学生开展基于AI驱动的密码研究。邀请企业方专家作为产业导师加入指导学生的毕业设计之中，选题直接来源于产业需求，如“基于AI的区块链智能合约漏洞检测”。

组织学生参与国家级竞赛。将全国密码技术竞赛、CTF（Capture The Flag）赛题转化为密码课外实训项目；在竞赛中引入AI自动化攻防赛道，强调AI工具在漏洞挖掘与修复中的应用。

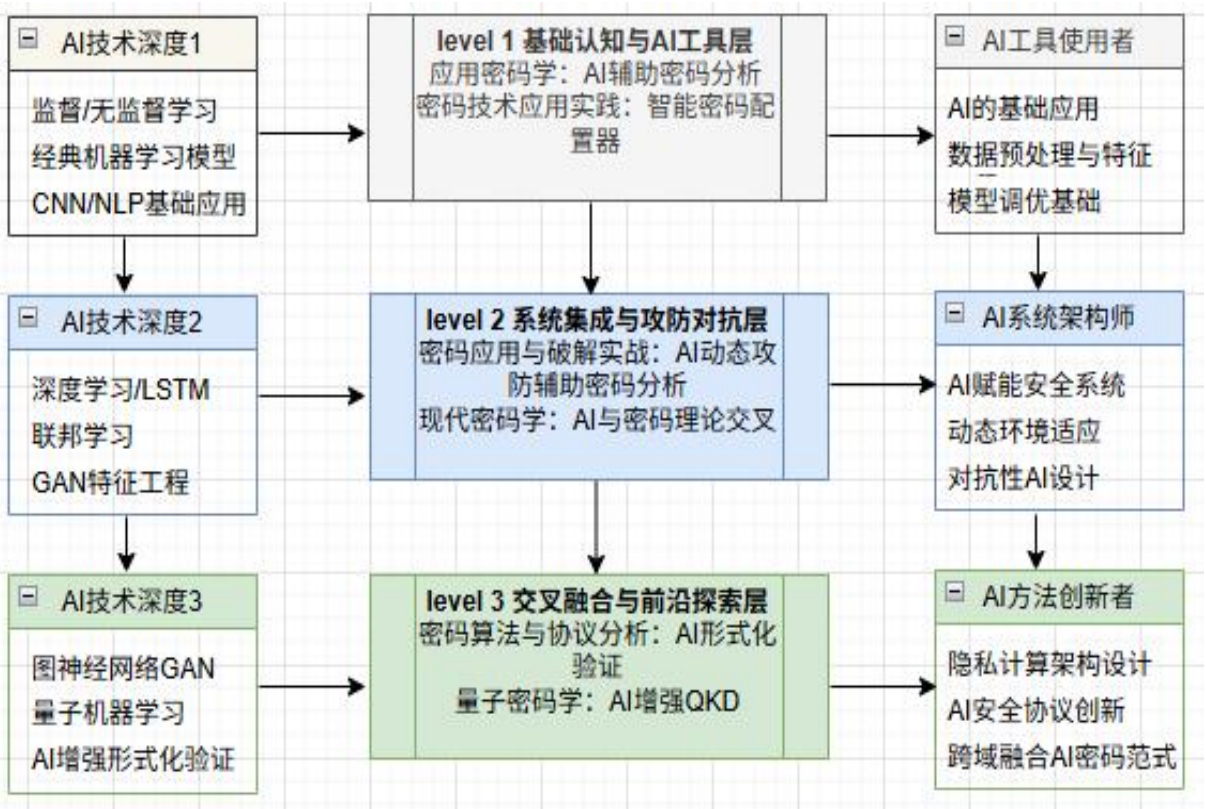

图 1 学生能力演进与技术深化框架图

4 学生能力演进与技术深化

执行上述 AI 驱动的密码学课程体系，将本硕两套课程融为一体，并按层次逐步把学生的认知和能力进行递进式提升，从学生的角度考虑即由一层到二层再到三层，从技术深度角度考虑，从认知和使用工具开始一步一步深入到交叉融合领域的最前沿。如图 1 所示，清晰地展示一位从学生到逐渐成长为具有创新能力的、在前沿交叉领域的资深专家的过程。

（1）Level 1：基础认知与工具应用层

目标能力：能够将 AI 作为增强型工具，解决特定、局部的密码学问题。技术深度：应用现成的 AI 模型和库，完成数据驱动的基础任务。

课程 1：应用密码学

AI 驱动实践载体：模块实验是有关 AI 辅助密码分析的内容，具体是使用 CNN 对密文进行算法识别分类，利用 NLP（如 Transformer）对古典密码进行自动破译。

技术深度体现：理解并应用有监督学习模型，同时掌握数据预处理、特征工程的相关知识，并且能将密码学的问题抽象为分类或者回归问题。

能力验证（产出）：完成实验报告，对比 AI 方法与传统密码分析方法的效率与效果。

课程 2：密码技术应用实践

AI 驱动实践载体：根据机器学习模型（如决策树）结合应用场景（IoT、Web）与安全需求来配置智能密码，具体是在上述智能密码配置器中选择适合的应用场景与安全需求来配置对应的密码算法以及参数等信息。

技术深度体现：理解并应用多目标决策模型，学习将领域知识（安全、性能）转化为模型特征。

能力验证（产出）：实现一个可交互的配置推荐系统。

（2）Level 2：系统集成与攻防对抗层

目标能力：能够将 AI 作为核心组件，设计与实现 AI 赋能的密码系统，并在动态对抗环境中应用。技术深度：集成并优化 AI 模型，处理时序、序列等动态数据，解决系统级安全问题。

课程 3：密码应用与破解实战

AI 驱动实践载体：自适应智能加密网关。蓝方负责使用 LSTM/GRU 等时序模型检测实时网络攻击。红方负责使用强化学习探索最优攻击路径。

技术深度体现：掌握时序模型和异常检测技术，初探强化学习在安全场景的应用，理解 AI 在动态策略调整中的作用。

能力验证（产出）：完成系统原型与攻防报告，生成一个可演示的智能网关及详细的对抗分析报告。

课程 4：现代密码学

AI 驱动实践载体：当前的前沿研究是对AI与密码理论两个方向的融合，并提出了AI是如何将可证明安全形式化的，如何使用遗传算法自动生成S盒，并对其进行优化的，再探讨如何定义抵抗机器学习攻击的密码体制等问题的研究课题。

技术深度体现：从系统安全视角，批判性思考AI的能力与局限，探索生成式AI（遗传算法）在密码设计中的应用。尝试建立基于机器学习的安全模型。

能力验证（产出）：完成研讨报告，特定密码理论（如可证明安全）的潜在影响。产出开创性研究课题，为此方向奠定初步理论基础。

（3）Level 3：交叉融合与前沿探索层

目标能力：能够驾驭密码学与AI的深层融合，设计和验证保障AI自身安全（如隐私）的复杂系统。技术深度：运用高级密码学原语（同态加密、安全多方计算等）来建立AI系统的安全防护，并且用形式化的方法证明其安全性。

课程5：密码算法与协议分析

AI驱动实践载体：隐私保护的联合智能学习平台。内容包括设计并实现基于同态加密或安全多方计算的联合学习协议，使用形式化验证工具分析协议的安全性。

技术深度体现：深入理解隐私计算技术原理与实现，掌握形式化验证与AI增强的符号执行技术，确保协议安全，解决安全与性能的平衡难题。

能力验证（产出）：提出一种新的安全协议或优化方法，并完成安全性证明。

课程 6：量子密码学

AI驱动实践载体：后量子密码的AI辅助安全评估舱。使用深度学习从侧信道数据中挖掘PQC算法的实现漏洞，利用图神经网络分析PQC算法的数学结构弱点。

技术深度体现：将AI用于未知漏洞挖掘，超越传统分析范式。融合物理层攻击与数学层分析。在后量子时代建立新的安全评估方法论。

能力验证（产出）：发表关于PQC算法新型AI分析方法的创新性成果。

由图 1 可知，学生从使用 AI 工具、应用 AI 系统，直到提出新的 AI 问题，都是基于每个具体的内容来展开，是关于如何培养学生利用 AI 去做出难题的答案。图 1 中的框图是 AI 时代的密码学的人才成长线，在每个具体的场景中存在每一门课的位置与价值点，从而形成完整的链路过程，并能够满足从入门到精通全流程的教学培养需求。

5 课程评价与教学效果评估

5.1 评价体系与考核要求

构建全过程、多维度、可追溯的评价体系，注重考查学生知识掌握情况的同时，尤其强调考查学生的基本技能、系统能力和创新素养这 3 个方面的综合水平，具体考核体系如下：

课程模块（基础能力考核）：整学期都将在本课程中涉及并以此来考查学生对课程的基本理解和基本技能的把握。利用AI评分引擎评估效果占比为40%，考查其分析问题、解决问题的能力、以及实现效果和代码质量等；采用在线平台的交互数据作为学生主动学习态度、课程知识获取能力的考查依据，占比为30%；制定阶段性理论测试来考查学生对于AI密码学核心概念、原理的掌握情况，占比30%。

锚点项目（系统能力考核）：在学期中、学期末、举行阶段评审和期末答辩。用交叉评审（教师+企业导师）方式评审出每组同学综合评分及排名：采用5个维度分别打分方式，包括技术可行性（20%）、AI模型创新性（20%）、安全协议严谨性（20%）、系统设计与实现能力（20%）、团队协作与项目管理（20%）。设置“贡献度证明”，依据学生提供的代码提交文件、文档撰写情况及模型迭代过程的纪录来证明其是否为该项工作做出了相应的贡献，并以此来考察学生有没有较好的工程系统思维以及解决问题和沟通交流的能力。

产业实践与竞赛（创新素养考核）：学期末或活动后，评判创新素养，主要考察学生的创新实践和产业应用能力。评分内容包括企业项目的交付成果、参加各类竞赛获得奖项、申请专利等各类创新实践活动，按照创新实践分级认定标准赋分：产业项目实践（占比 40%），高水平竞赛成果（占比 30%），学术创新产出（占比 30%）。主要考察学生技术、产业、学术等方面的创新能力、产业观察能力及潜力，分数达到要求即可抵扣一定的成绩。

本评价体系采用从知识层、技能层和综合应用层三个层次逐层深入的方式来进行考核评价，将知识掌握和能力培养融合在一起、个人发展与团队合作兼备、学术需求与产业需求兼顾、保障了 AI 驱动密码学人才培养的质量效果。

5.2 教学效果评估

为了准确测评“一体两翼、双向贯通”课程体系的实践成效，选取了定量与定性相结合的方式展开测评工作，从学生活力、课程满意度、社会认可度三个方面分别对学生开展评价，并对其所属班级学生：2023年春学期29名本科学生、2024年春学期35名本科学生、2023年秋学期47名研究生、2024年秋学期79名研究生，共两届190名开展为期两个学期的跟踪评估。

（1）学生从知识接受者转变为问题解决者

定量数据：在锚点项目评估中，学生系统设计与实现能力的优秀率从改革前的28% 提升至65%。尤为突出的是，学生在“AI模型创新性”与“安全协议严谨性”两个维度的平均得分提升了42%，证明其AI与密码学交叉创新能力得到实质性锻炼。

定性反馈：多于 85％被访学生认为“锚点项目”将以往所学的知识点串联起来形成解决问题的方案，“以 AI 驱动为纲”使自己的批判性思维、拆解复杂问题的能力以及团队协作能力得到极大考验和锻炼。一名学生在实验体会中写道：“印象最深刻的还是从只会调用密码库到现在知道如何设计出一套联邦学习的安全聚合协议的过程”。

（2）课程满意度与学习动力创历史新高

课程满意度调查显示，学生对改革后课程的总体满意度达到 95%，远高于传统模式的 88%。其中，“教学内容前沿性”与“实践项目挑战性”两项指标获得最高分。

（3）竞赛获奖与产教融合成果丰硕

竞赛成绩突破：试点学生团队在 2024 年全国密码技术竞赛中，获得了“基于 AI 与量子搜索的 ECC 密钥恢复软件”等 6 项国家奖项，在 2025 年全国密码技术竞赛中，也获得了“深度学习和量子枚举的 LWE 密钥恢复软件”等 6 项国家奖项。整体来看，试点学生团队的实践创新能力得到了较大的提高。

高质量学术与就业产出：基于课程项目，学生共登记软件著作 4 篇，申请专利 10 多项。毕业生在就业市场中展现出强大竞争力，首批试点学生中，80% 以上进入大型科技企业从事 AI 安全相关岗位。

6 特色与创新

本论文的特色与创新主要体现在以下三个方面：

（1）体系化构建的创新：提出并实践了“一体两翼、双向贯通”的课程新范式。

特色：突破了传统课程“孤岛式”分布的局限，进行了系统性的顶层设计。

创新点：将密码学核心知识体系（一体）、AI 驱动的理论与实践的深度融合（两翼）、本硕纵向衔接与跨学科横向交叉（双向贯通）有机整合为一个整体模型，实现了从“知识灌输”到“能力建构”的范式转移。

（2）深度融合的创新：实现了 AI 与密码学从“工具应用”到“范式驱动”的跨越。

特色：AI 不是外在的“点缀”，而是内生于课程机理的“引擎”。

创新点：构建了从本科（AI 作为工具）到研究生（AI 作为研究伙伴）的递进式能力培养路径，并将机器学习、深度学习、强化学习等 AI 前沿方法系统性嵌入密码分析、协议验证、后量子密码评估等核心教学环节，重塑了密码学课程的内容生态。

（3）实践模式的创新：设计了“锚点项目”驱动的“学-练-战”闭环实践体系。

特色：以复杂的真实问题（例如：自适应智能加密网关）为导向，打破各门课程之间的壁垒。

创新点：采取跨课程、跨年级的“锚点项目”，用虚仿平台和企业的真实环境把相关联的理论知识点通过解决具体问题串起来，形成一条有内在联系的解决实际问题的价值链，从基础实验、系统集成到产业实战按难易程度层层递进的实践路径，使理论教学和实践教学有机结合起来。

综上所述，本论文的特色在于其系统性、深度融合性、实践性，为解决新时代密码学人才培养的痛点提供了一个具有前瞻性和可操作性的完整方案。

7 结论与展望

本文构建“一体两翼、双向贯通”的 AI 驱动密码学课程体系，是新时代智力时代背景下对密码人才培养提出的新要求，解决了传统课程体系零散、理论与实践融合度不高、AI 思维渗入密码内核不够等问题。采用“两翼齐飞”的方式既讲授知识又教会学生面对新技术变化的本领，采用“双向贯通”的方式打破本硕之间以及校企之间的壁垒，培养的人才是完整且连续的。实践证明“锚点项目”将学生由经验提供者变为了问题解决者，实现其对真实任务的整体把握与全面应对。通过教学评价可以看到学生的学习热情得到了极大程度的激发，创新意识得到了充分调动。未来，笔者将继续建立更具弹性的课程内容更新机制，与 AI 技术发展同步，拓展跨学科融合的深度和广度。

参 考 文 献

[1] 胡小明, 杨寅春, 吴秀梅，等.信息安全专业密码学课程教学改革[J]. 计算机教育，2014(1): 49-52.

[2] 李艳俊,刘冰,郑秀林.密码学课程体系建设探讨[J].北京电子科技学院学报,2016,24(3):68-74.

[3] 吴旭光, 韩益亮, 朱率率, 等. 密码应用与实践课程建设探讨[J]. 计算机教育, 2020(3): 8-11.

[4] 杨建强, 吴中博, 李学锋, 郑 毅.“信息安全基础”课程密码学类实验设计[J]. 计算机时代，2021(9): 88-94.

[5] 葛爱军, 曾光, 王永娟. CTF 模式在密码分析实践教学的探索与实践[J]. 计算机教育, 2022(3): 68-72.

[6] 董建阔, 肖甫, 沙乐天. 新工科背景下融合 OBE 与 PBL 的密码实践课程教学设计[J]. 计算机教育, 2023(1): 136-140.

[7] Uhsadel L, Ullrich M, Das A, et al. Teaching HW/SW co-design with a public key cryptography application[J]. IEEE Transactions on education, 2013, 56(4): 478-483.

[8] Arboledas Brihuega D. A new character-level encryption algorithm: How to implement cryptography in an ICT classroom[J]. JOTSE: Journal of Technology and Science Education, 2019, 9(3): 257-268.

[9] González-Tablas A I, Gonzalez Vasco M I, Cascos I, et al. Shuffle, cut, and learn: Crypto go, a card game for teaching cryptography[J]. Mathematics, 2020, 8(11): 1993.

[10] Percival N, Rayavaram P, Narain S, et al. CryptoScratch: Developing and evaluating a block-based programming tool for teaching K-12 cryptography education using Scratch[C]// 2022 IEEE Global Engineering Education Conference (EDUCON). IEEE, 2022: 1004-1013.

[11] Abdelhamid S, Patterson S, Patterson B. Enhancing cryptography education using collaborative visual programming[C]//Conference Proceedings. The Future of Education 2022. 2022.

[12] Rayavaram P, Ukaegbu O, Abbasalizadeh M, et al. CryptoEL: A Novel Experiential Learning Tool for Enhancing K-12 Cryptography Education[C]//Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1. 2025: 980-986.

[13] 中国密码学会教育与科普工作委员会.第十六届全国密码学与信息安全教学研讨会会议纪要[C].河南师范大学大学，2025.8. https://www.htu.edu.cn/2025/0819/c21138a353401/page.htm

[14] SKF:“智能+”时代的网络安全虚拟教研室重构模式——联邦学习与知识图谱的课程群协同建设实践[J].高等工程教育研究,2026,(01):47-52.

[15] Nelson C,Adam D, Shoshitaishvili Y. SENSAI: Large Language Models as Applied Cybersecurity Tutors[C]//Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1. 2025:833-839.

[16] Behrouz Z,Hamid N,Naoto Y,Khodakhast B.Crypto and AI: From Coevolution to Quantum Revolution[M]. Springer,2023.