矩阵式结构化与乐高式模块化融合的教学改革

赵秀凤　高海英　宋巍涛

网络空间部队信息工程大学密码工程学院，郑州 450001

摘　要　针对密码协议分析与设计课程存在的知识碎片化、智能化支撑不足、国密融入不深等教学问题，本文提出矩阵式结构化与乐高式模块化深度融合的教学改革模式。以协议类型为横向、难度层次为纵向构建二维教学矩阵，将教学单元封装为可灵活组合的标准化知识组件，设计三类适配不同学情的实施路径；依托智能导学、知识图谱与路径定制实现教学数字化与个性化，建立“课前诊断—课中实训—课后评估”闭环教学体系，并深度融入国密标准与课程思政。教学实践表明，该模式有效提升学生系统化思维、实战攻防能力与创新意识，可为密码学与网络安全类课程改革提供可推广路径。

关键字　密码协议分析与设计，矩阵式结构化，乐高式模块化，国密算法，AI 融智

Matrix Structured and Lego Modular Integrated Teaching Reform

Zhao Xiufeng　Gao Haiying　Song Weitao

School of Cryptographic Engineering, Cyberspace Force Information Engineering University
ZhengZhou 450001, China
zhao_xiu_feng@163.com

Abstract—Aiming at the teaching problems existing in the course of Analysis and Design of Cryptographic Protocols, such as fragmented knowledge, insufficient intelligent support, and inadequate integration of national cryptographic standards, this paper proposes a teaching reform model that deeply integrates matrix-based structuring and LEGO-style modularization. A two-dimensional teaching matrix is constructed with protocol types as the horizontal axis and difficulty levels as the vertical axis, and teaching units are encapsulated into standardized knowledge modules that can be flexibly combined, with three types of implementation paths adapted to different learning situations designed. Relying on intelligent tutoring, knowledge graphs and path customization, the digitalization and personalization of teaching are realized, a closed-loop teaching system of "pre-class diagnosis — in-class training — after-class evaluation" is established, and national cryptographic standards and curriculum ideological and political education are deeply integrated. Teaching practice shows that this model effectively improves students' systematic thinking, practical attack and defense capabilities, and innovative awareness, and can provide a promotable path for the reform of cryptography and network security-related courses.

Keywords—Analysis and Design of Cryptographic Protocols，Matrix Structured，Lego Modular，national cryptographic algorithms，AI intelligence integration

1 引　言

网络空间已成为国家主权的重要新疆域，关键信息基础设施全面数字化，密码技术作为维护国家安全的战略基石，为数据安全、身份可信与业务可信提供核心支撑。密码协议是密码算法的工程化实现与标准化应用形态，是支撑身份认证、密钥协商、安全传输、数据可信等关键服务的重要载体，广泛部署于金融、政务、通信、能源及工业控制等关键信息基础设施领域。2019 年《中华人民共和国密码法》正式实施，明确要求加快密码人才培养，亟需培养兼具密码理论功底、工程实践能力、安全测评素养与法规标准意识的复合型密码人才[1]。2021 年教育部设立密码科学与技术本科专业，明确构建“密码理论—密码算法—密码协议—密码工程—安全测评”一体化人才培养体系。密码协议分析与设计作为衔接理论与工程实践的核心进阶课程，其内容体系、组织方式与实践环节直接决定密码专业人才培养质量。

国内学者对密码类课程的教学建设与思政教学模式进行了研究[2,3]。其中，矩阵式教学以其“双维度交叉、模块化组织、可裁剪迭代”的突出优势，在计算机类课程与密码学相关课程中得到广泛探索与实践。乔珂欣等将矩阵式教学成功应用于现代密码分析学课程，构建以算法对象为纵向、分析方法为横向的教学框架，有效解决知识点碎片化、内容庞杂无序、

**基金资助：信息工程大学教学研究课题（No. JXYJ2025C050）

实践脱节等问题[4]；郭世仁等提出教学矩阵驱动的课程思政模式，实现专业知识点与思政元素的深度融合[5]；崔青构建三维矩阵体系，推动课程思政、教学内容与教学方法一体化设计[6]；曹雪丹等将矩阵式教学应用于临床实践教学，验证其在多维度能力培养上的显著效果[7]；邢长友等将矩阵模式引入网络安全协议课程，提升了内容组织与实践教学的规范性[8]。总体来看，现有矩阵式教学成果多以密码算法分析或单一思政融合为侧重点，面向密码协议全生命周期、覆盖设计—分析—攻防—验证—国密适配一体化的矩阵式教学体系仍较为缺乏，难以满足新时代密码领域高层次人才培养需求。

全国人大代表、上海交通大学校长、中科院院士丁奎岭强调，应通过课程微课化、模块化，支持学生依据自身创新发展需求动态化制定个性化学习路径，倡导人才培养多一些“乐高式”自主构建、少一些“流水线”式知识填鸭[9]。李晖教授提出构建模块化、可组合、适配多类型人才需求的网络安全课程体系，建立分层渐进式实践能力培养路径[10]。上述理念为破解传统教学模式僵化、个性化不足、实践与创新素养薄弱等问题提供重要指引。

为此，本文针对密码协议分析与设计课程存在的知识碎片化、智能化支撑不足、国密融入不深、个性化教学缺失等痛点，将乐高式模块化自主构建理念与矩阵式结构化教学架构深度融合，构建覆盖协议全生命周期的矩阵式结构化教学内容体系与可灵活适配的乐高式模块化实施路径，以期为密码类专业课程改革与高质量人才培养提供理论参考与实践借鉴。

2 教学问题与改革思路

2．1 教学问题

密码协议分析与设计课程具有理论抽象、协议类型多、攻防逻辑强等特点，传统教学模式存在以下教学痛点：

（1）知识碎片化，体系构建不足：密码协议设计与分析方法线性讲授，学生难以建立“密码协议—设计原理—攻击方法—安全增强”的整体关联，容易陷入“记流程、背漏洞”的浅层学习。

（2）智能支撑缺失，个性化教学不足：教学以课堂讲授为主，缺少AI助教、知识图谱、智能推送、实时诊断等数字化手段，难以实现分层教学与精准辅导。

（3）协议应用融入不深，国密标准覆盖不足：内容偏重基础密码协议，对Kerberos协议、TLS协议应用协议，以及实体认证、密钥交换等国密标准协议覆盖不足，价值引领与典型行业场景（如军事、金融、政务、能源）的应用结合不够紧密，影响学生工程视野与岗位适应能力。

2．2 改革理念与思路

为解决上述教学问题，本课程以“矩阵构框架、乐高组模块、AI强支撑、思政铸底色、评价促达成”为整体改革思路，如图1所示：以矩阵式结构化方法搭建系统化知识与能力双维度结构；以乐高式模块化封装实现教学单元可独立、可组合、可扩展，支撑学生自主构建个性化知识体系；以AI融智课堂提升教学效率、个性化适配与过程可视化水平；以全生命周期闭环实训强化协议设计、安全分析、攻防对抗与工程实践能力；以国密协议为主线深化课程思政与自主可控教育；以矩阵式全程评价实现可量化、可追踪、可视化的目标达成监测。

图1 教学改革与设计思路

3 矩阵式教学内容体系设计

矩阵式结构化教学以横向研究对象、纵向能力层次为双轴架构，通过知识点与能力点的交叉耦合形成结构化教学体系，具备层次清晰、单元独立、裁剪灵活、迭代便捷等显著优势，能够有效破解密码协议分析与设计课程知识点分散、逻辑关联性弱等共性难题，实现知识体系化、能力实战化、教学个性化、育人价值化的统一。将矩阵式教学模式引入密码协议分析与设计课程，可从教学内容组织、实施路径规划、学习效果评价、学习动机激发等维度系统性提升教学质量，推动课程教学模式创新。

3．1 横向维度：协议类型模块化

横向维度按照密码协议类型进行模块化设计，覆盖密码协议的主要类型：

第一类实体认证协议：包括基于对称密码算法的实体认证协议、基于数字签名算法的实体认证协议、基于零知识思想的实体认证协议、口令认证协议等。

第二类密钥交换协议：包括DH密钥交换协议、STS协议、SIGMA协议、KEA协议、SM2密钥交换协议、抗量子密钥交换协议等。

第三类高级数字签名协议：包含盲签名、群签名、环签名以及抗量子数字签名等。

第四类安全多方计算协议：包括不经意传输协议、比特承诺与零知识证明协议、数值大小比较协议等。

3．2 纵向维度：协议难度分层递进

按基础-核心--应用-前沿及标准划分协议层次，降低门槛、突出重点、兼顾拓展。

基础层：针对某类密码协议，体现密码协议设计思想并实现基础功能的密码协议，如DH密钥交换协议、基于对称密码算法的实体认证协议；用于快速理解协议流程、体验攻击方法、获得正向学习体验。

核心层：针对某个类型的密码协议，既能实现功能性需求又具备抗典型密码协议攻击的协议实例，如基于零知识的实体认证协议、SIGMA协议等；用于协议安全性增强、对接协议具体应用需求作为课程主要内容，强化面向具体应用场景的安全问题解决方案设计与分析。

应用层：针对某个类型的密码协议，对标国密协议标准落地，作为课程重点内容，强化自主可控与工程应用。

前沿层：包括抗量子密钥交换协议、混合TLS协议、以及基于全同态密码的隐私计算协议等，旨在拔高学生科研视野、竞赛能力与创新思维，衔接毕业设计、学科竞赛、科研入门培养。

3.3 双维交叉：教学内容矩阵构建

在教学内容设计方面，主要坚持四个原则，分别是：（1）坚持全覆盖，即每类协议、每层协议至少包含1个教学单元，保证知识点可落地、可评估；（2）典型性，即主要选取设计方法优、具有工程价值的案例；（3）按需选取：标注必学/选学单元，适配课时与学情，避免冗余。（4）闭环培养：每个单元遵循需求分析→设计思想→安全分析→安全增强→实践应用流程，形成能力闭环。以密码协议分析与设计课程为例，构建了矩阵式结构化教学内容体系，如图2所示。

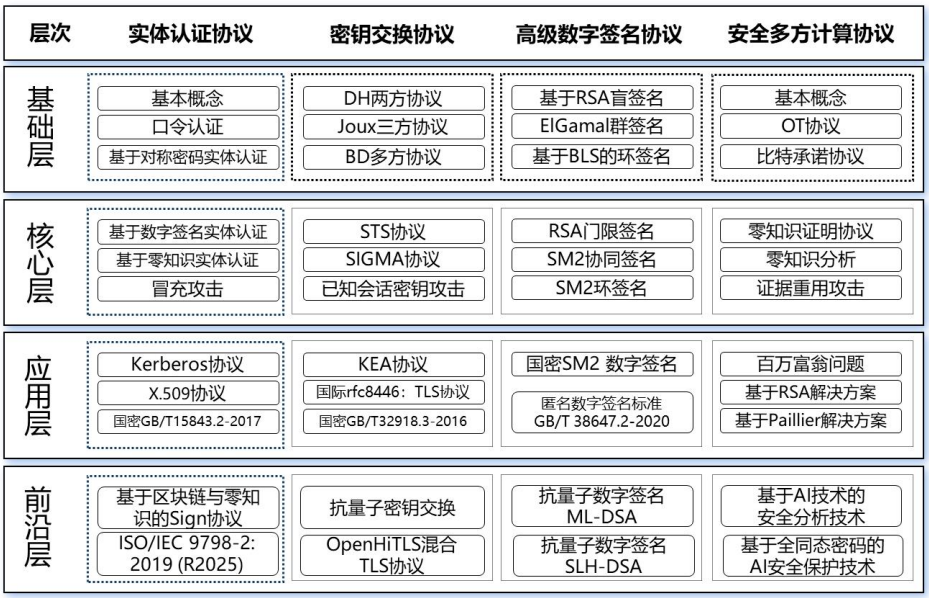

图 2 矩阵式结构化教学内容体系

3.4 AI 融智支撑体系设计

为支撑矩阵式教学组织与乐高式模块化拼接的灵活实施，依托长江雨课堂一体化教学平台构建AI融智支撑体系。基于矩阵式教学内容结构，在知识图谱建设过程中对所有知识点进行横向协议类型、纵向能力层次双维度标准标注，实现每个教学单元与矩阵单元格的精准映射。在此基础上，对电子教材、课件、微课视频、拓展资料等数字化资源进行标准化封装与结构化关联，提取协议类型、安全属性、分析方法、攻防场景等知识实体与关联关系，形成统一规范的知识表示，将零散的密码协议专业知识组织为结构化、可定位、可拼接的乐高式知识组件，构建乐高式知识组件库。

依托智能平台搭建AI助教、智能诊断与个性化推送三位一体支撑机制，通过智能批改、实时答疑、学习行为分析精准定位学生知识薄弱模块，动态匹配对应矩阵单元与乐高式学习组件，实现学习资源按需推送、学习路径智能规划与学习过程全程可视，为模块化自主构建、分层递进训练与个性化能力达成提供智能化保障，显著提升矩阵式教学的实施效率与精准度。

4 乐高式模块化教学实施路径

依托横向协议类型、纵向协议层次的二维教学矩阵，本文引入乐高式模块化拼接教学范式，将矩阵内各教学单元抽象为可独立封装、标准接口、按需组合、动态扩展的标准化知识组件，以组件化、可重构、分层嵌套思想重构实施逻辑，结合课程教学规律、学时约束与认知递进规律，设计三类适配性实施路径。三条路径均遵循“先基础组件后综合组件、先单点拼装后体系构建、先理论建模后工程实践”原则，教师可依据培养目标、授课对象与课时灵活选配，实现教学组织的精准化、个性化与体系化。

4.1 横向驱动路径：协议类型递进式

该路径遵循同主题组件串行拼接逻辑，以横向协议类型为主题组件包，依次完成实体认证、密钥交换、高级数字签名、安全多方计算四大模块的系统化拼装。沿纵向将基础、重点、应用、前沿协议封装为递进式组件，由低阶到高阶逐块拼接。该路径以同主题组件有序拼接形成稳定能力结构，契合建构主义学习理念，助力学生建立分类清晰、逻辑连贯的协议认知体系，形成可迁移的分析与设计方法论。

4.2 纵向驱动路径：协议层次嵌套式

该路径采用跨主题分层嵌套拼装模式，以纵向协议层次为架构层级，逐层融合横向四类协议组件，构建覆盖全生命周期的能力模型。基础层以简易协议为底层基座组件，快速完成知识框架拼装；重点层以零知识认证协议、SIGMA、SM2协同签名、零知识证明等核心功能组件为支撑，强化协议安全分析与安全增强能力；应用层以国密标准、TLS、百万富翁问题等工程化组件为主体，实现攻防验证、漏洞加固与国密落地一体化集成；前沿层引入抗量子签名、混合密码、全同态计算等高阶扩展组件，实现创新拓展。该路径以多层级嵌套拼装实现多类型组件深度耦合，贴近实战攻防与工程开发场景，显著提升学生综合应用与对抗能力，适配学科竞赛、问题解决能力导向的培养。

4.3 曲线精简路径：核心组件拼装式

该路径遵循核心组件精简拼装机制，沿矩阵对角线选取代表性交叉单元作为关键支撑组件，以最小组件集完成核心能力体系快速构建。以基础协议组件搭建认知底座，以重点协议组件强化核心能力，以国密与应用协议组件完成工程化落地，以前沿协议与综合实训组件实现能力闭环。路径不追求全组件覆盖，通过核心组件高效拼装快速形成可用能力结构，具备轻量化、高适配、强通用性特征，满足短学时与通识课程教学需求。

三条路径均以乐高式模块化拼接为理论内核，实现教学单元独立可封装、组合可重构、迭代可扩展，统一遵循“需求分析—设计思想—安全分析—安全增强—实践应用”能力闭环，深度融入国密标准与课程思政，讲解我国密码技术自主创新成果，强化总体国家安全观、网络强国意识、自主可控理念、职业伦理与责任担当，实现知识传授与价值引领统一。矩阵式教学实施路径在提升教学灵活性与个性化水平的同时，为密码协议类课程提供具有理论创新性与实践推广价值的新型教学范式。

5 全程评价体系

建立过程评价（25%）+实验实训评价（25%）+结果评价（50%）体系，总分为 100。通过课堂表现、实验实训、期末考核、攻防竞赛等多维量化，实现学习全周期、能力全维度的量化监测与闭环改进。

过程性评价依托 AI 融智平台采集课前预习、课堂互动、模块进度等学习行为数据，结合课堂表现、作业任务完成质量综合评分，实时追踪学习投入与知识掌握情况。实验实训评价聚焦能力达成，以协议设计、攻防复现、国密协议部署、面向具体场景的协议设计与实现等实践任务为核心，评价编程能力、问题解决能力与工程规范意识以及创新素养，突出模块化实践结果。终结性评价采用综合性考核方式，全面检验学生对密码协议体系、安全分析方法、国密标准的整体掌握程度与综合应用能力。

评价体系可以实现模块化、动态化、可视化、即时化，与教学模式高度协同，形成“教学—学习—评价—改进”闭环，有效保障人才培养质量。

6 教学改革成效分析

经过连续两个学期的教学实践，矩阵式结构化与乐高式模块化深度融合教学模式在密码协议分析与设计课程中取得显著成效。本次各项调研、数据统计均以 2024 与 2025 两届密码学专业共 76 名选课学生为样本开展。

知识体系系统化，课程脉络清晰可感知。教学实践反馈表明，矩阵式知识框架重构了课程整体脉络，特别是知识图谱加持，实现专业知识体系系统化建构。面向 2025 届 48 名学生开展课程满意度调研由课程满意度调研数据（图 3）可知，92%的学生对改革后课程教学效果持肯定态度，其中 46%的学生认为课程逻辑层级清晰、知识体系完整，28%的学生表示课程学习难度合理下降，18%的学生反馈结构化学习模式有效减少知识遗忘问题。仅 8%学生认为教学效果无明显变化，充分印证矩阵框架在整合零散知识点、构建结构化密码协议认知体系中的实践价值。

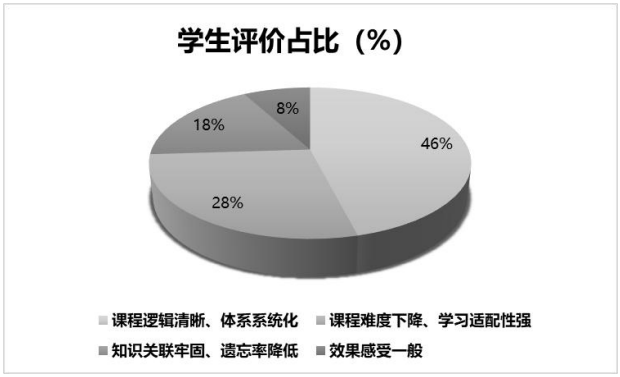

图 3 学生对教学改革效果的评价占比

核心能力闭环形成，工程实战能力显著提升。学生可独立完成：密码协议常见漏洞攻击复现、国密协议接口开发与部署测试、以及面向应用场景的密码协议综合设计与实现。实验完成率从传统教学的65%（2024秋季）提升至94%（2025秋季），代码实现质量、AI工具使用熟练度明显提高。

学习兴趣与主动性大幅提高。教改实施过程中，通过矩阵闯关、快速攻防、小组对抗等多元化课堂机制，打破传统“被动听课”的教学模式，引导学生主动参与探究式学习，同时结合国密主题任务，强化学生专业价值认同与归属感，有效提升学生学习兴趣与主动性。结合课堂考勤、平台行为数据及问卷统计（样本76人）由图4可知，教改后学生课堂参与度从62%提升至88%，课后主动学习比例从45%提升至79%，自主拓展学习比例从38%提升至71%，学生满意度从83%提升至96%，稳定在95%以上。

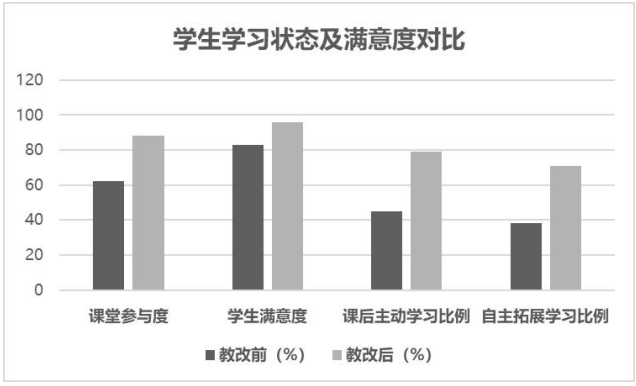

图 4 学生学习状态及满意度对比

竞赛与实践成果突出。实施矩阵式教学后，学生在全国高校密码数学挑战赛、全国密码技术竞赛中获奖数量增加50%，作品聚焦基于国密算法的密码协议设计、基于全同态密码的隐私安全密码协议设计、抗量子密码协议组件优化、密码协议的自动化分析等方向，与课程内容高度契合。

矩阵式教学内容框架标准化、模块化、可扩展，可灵活新增前沿协议、攻击方法与工具链；三种实施路径适配不同学时与专业方向；评估体系与兴趣机制可直接迁移至密码学、网络安全、信息安全等同类课程，已形成可复制、可推广的课程改革范式。

7 结束语

本文将矩阵式结构化教学架构与乐高式模块化拼接理念深度融合，构建“横向协议类型、纵向难度层次”二维教学矩阵，封装标准化教学组件并设计三类适配性实施路径，结合 AI 融智支撑、国密标准与课程思政，形成闭环教学体系。教学实践表明，该模式有效破解传统教学痛点，显著提升学生核心素养与学习成效。

该模式具备标准化、可重构、可迁移特性，可推广至密码学、网络安全、信息安全等同类课程。未来将持续优化教学矩阵，融入前沿内容，完善实践支撑与评价体系，深化 AI 与模块化教学融合，为培养高素质密码与网络安全人才、服务国家网络空间安全战略提供有力支撑。

参 考 文 献

[1] 全国人民代表大会常务委员会. 中华人民共和国密码法(2019-10-26)[EB/OL].(2019-10-26)[2026-06-21].http://www.npc.gov.cn/npc/c2/c30834/201910/t20191026_301700.html 中国人大网.

[2] 郑世慧, 肖达, 毕经国等.《密码应用与安全》课程面临挑战与建设思路. 计算机技术与教育学报, 2024(10): 45-50.

[3] 张际焱, 邵昕童, 沈盼等. 密码学课程思政教育探索研究. 计算机技术与教育学报, 2025(3): 69-73.

[4] 乔珂欣，孙思维，王安，祝烈煌. 现代密码分析学课程的 “矩阵式” 教学方法探索 [J]. 计算机教育，2025 (09):84-89.

[5] 郭世仁，王俊红，连剑波，黄灏然. 教学矩阵驱动的面向对象程序设计课程思政 [J]. 计算机教育，2020 (9): 64-67.

[6] 崔青. 数据结构与算法课程思政三维结构内容体系构建 [J]. 计算机教育，2023 (6): 12-16.

[7] 曹雪丹，梁群，张淼等. 矩阵式教学体系在重症医学临床教学中的应用与思考 [J]. 中国中医急症，2023 (7): 1281-1283, 1289.

[8] 邢长友，刘晓明，胡晓惠. 网络安全协议课程矩阵式教学模式研究 [J]. 计算机教育，2022 (7): 112-115.

[9] 沈湫莎. 乐高式创业拼出 AI 时代“独角兽”[N]. 文汇报, 2026-04-2(001). DOI: 10.28814/n.cnki.nwehu.2026.001288.

[10] 李晖,刘樵. 提高网络安全人才自主培养质量[J]. 中国网信, 2022(12):50-51.