融合隐私计算研发能力培养的密码学基础实验教学改革探索*

宁建廷　吴黎兵　冯琦　何德彪**

武汉大学国家网络安全学院，武汉 430072

摘　要　随着信息技术的迅猛发展和网络攻防对抗的日益激烈，社会对高层次网络空间安全人才的需求愈发迫切。为弥补当前密码学基础实验教学在前沿视野与实践创新能力培养上的短板，本文提出融合隐私计算研发能力培养的教学改革新模式，从采用“价值导向式”的教学思政理念、发展“知识扩展式”的前沿教学方法、结合“学科交叉式”的实际教学场景案例和提供“师生讨论式”的线上线下灵活互动 4 个方面展开说明具体的改革措施。最后分析教学改革效果，实践结果表明该改革措施有效提升了教学质量与学生满意度，增强了学生的实践与创新能力，为其未来的职业发展和深造奠定了坚实基础。

关键字　隐私计算研发能力，密码学，实验教学，网络空间安全，课程思政

Refining Educational Approaches in Cryptography to Foster Skills in Privacy Computing Research and Development

Jianting Ning　Libing Wu　Qi Feng　Debiao He

School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China;

Abstract—With the rapid advancement of information technology and the escalating dynamics of cyber defense and offense, the need for advanced cybersecurity professionals is increasingly urgent. To bridge the current gaps in foundational cryptography education, particularly in cutting-edge perspectives and practical innovation skills, this paper introduces a novel teaching reform model that integrates the development of privacy computing R&D capabilities. This approach is detailed through four key facets: implementing a "value-oriented" educational philosophy, advancing "knowledge-expansion" teaching methods, integrating "interdisciplinary" practical scenarios, and facilitating flexible "teacher-student discussions" both online and offline. The analysis of these reforms demonstrates a significant enhancement in teaching quality and student satisfaction, bolstering students' practical and innovative skills and providing a robust foundation for their future careers and further academic pursuits.

Keywords—Privacy Computing Research and Development Skills, Cryptography, Laboratory Instruction, Cybersecurity, Value-Oriented Education

1　引　言

随着“网络强国”战略的深入实施以及《国家网络安全法》、《网络安全审查办法》等一系列法律法规的出台，构建坚不可摧的网络空间安全屏障，维护国家主权、安全和发展利益，已成为国家层面的战略抉择与行动指南[1-2]。在此背景下，网络空间安全专业应运而生并迅速发展成为高等教育中的热门学科，旨在培养一批既掌握深厚理论基础又具备实战能力的网络安全专业人才[3]。密码学作为网络空间安全专业的核心课程之一，其基础实验教学课程更是为学生熟练掌握网络通信安全、实现数据保密性和完整性提供实践路径。

隐私计算技术，作为数据安全与价值发挥的新范式，实现了“原始数据不出域，数据可用不可见”和“数据使用可控可计量”的安全目标。密码学是隐私计算技术的基石，隐私计算的发展依赖密码学的理论支撑。由于国内现有的密码学基础实验课程内容更新不及时，导致教学情况与行业发展之间存在差距。因此，迫切需要构建专业理论教学与实践操作有机结合的教学体系，以培养适应数字化时代新型需求的复合型人才[4-5]。

2　密码学基础实验教学中存在的痛点

2.1　国产密码算法及思政理念融合不足

密码学基础实验教学的课程内容目前主要聚焦于技术细节与算法实现层面，而对于国产密码算法在国

*基金资助：本文得到武汉大学国家网络安全学院的支持；蚂蚁密算科技-教育部产学合作协同育人项目《隐私计算开发与实践课程建设的支持。

**通讯作者：　何德彪　hedebiao@whu.edu.cn

家安全战略中所扮演的关键角色及其深远的社会价值，尚未得到充分展现与强调，这无疑限制了课程有效激发学生爱国情怀与社会责任感方面的潜力[6]。通过将思想政治教育理念与技术教学内容有机融合，能够更为全面地培养学生的综合素养，促进他们在技术能力与社会责任之间实现均衡且和谐的发展，进而激励学生为国家信息安全事业贡献更为强大的力量。

2.2 学生的隐私计算研发能力培养不足

在传统的密码学基础实验教学中，课程通常侧重于经典密码方案的实践操作。然而，这种教学模式往往忽视了对隐私计算研发实践能力的培养。对于网络空间安全专业的学生而言，隐私计算研发能力至关重要。隐私计算技术通过将数据隐私保护与数据利用效率有机结合，确保在不泄露数据的前提下实现有效地计算和分析。缺乏隐私计算实践的培养模式可能会限制学生的创新能力和技术适应性，使他们在快速变化的网络安全领域中难以保持竞争力。

2.3 实验教学案例资源缺乏

在网络安全领域快速发展的背景下，新型威胁和隐私保护技术层出不穷。然而，现有的密码学基础实验课程往往缺乏关于实际攻击场景的案例分析、最新隐私保护协议的应用实例，以及应对现代攻击手段的策略[7]。缺乏实践关联的教学案例使课程难以与企业的实际技术需求接轨，导致学生在将理论知识应用于真实情境时面临挑战。这种培养方式削弱了课程的实用价值，还可能使得教学内容显得枯燥乏味，难以激发学生的学习兴趣和主动性。

2.4 课堂答疑和反馈机制不完善

在密码学基础实验课程的教学实践中，学生因理解能力和兴趣爱好的差异，往往在遭遇具体问题时展现出显著的个性化需求，难以形成统一的解决路径。受限于答疑环节的紧凑时间安排，复杂而深入的问题往往难以在有限时间内得到详尽透彻的阐释，致使部分学生即便参与讨论，仍可能心存疑惑，未能完全解决困难。更为关键的是，实验结束后，学生通常缺乏系统而详尽的反馈机制以及针对性的改进建议，这使他们难以精准定位自身学习过程中的薄弱环节，进而制约了整体学习成效的提升与知识体系的牢固构建。

3 隐私计算研发能力的培养

3.1 采用“价值导向式”的教学思政理念

随着全球信息技术的迅猛发展，数据安全问题愈加突出。在国际关系日益复杂的背景下，国外对我国数据安全的威胁事件屡见不鲜。近期，我国的DeepSeek线上服务平台在人工智能领域取得了显著进展，其发布的R1模型在技术上实现了重大突破。然而，这一创新成果也引起了部分竞争对手和潜在威胁者的关注，平台持续遭受分布式拒绝服务攻击、反射放大攻击、应用层攻击和密码爆破攻击等多种形式的攻击。由此可见，数据安全的自主可控不仅关乎个人隐私的保护，更直接关联到国家安全和社会稳定。

为了有效应对数据安全的挑战，中国自主研发国产密码算法，如SM2、SM3、SM4等，这些算法已被纳入国际标准组织的相关标准中。这一里程碑式的进展不仅彰显了国产密码算法在国际舞台上的认可度和影响力显著提升，也为我国在国际信息安全领域争取到了更多的话语权和主动权，为国家信息安全构筑起一道坚实的防线。在此背景下，将国产密码算法融入密码学基础实验课程中显得尤为重要。在教学过程中，授课教师积极引导学生对国产密码算法产生兴趣并给予认可，通过详细介绍国产密码算法的实现细节和技术特点，激发学生的创新思维和探索精神，鼓励学生自主实现这些基本算法，并进一步思考在底层算法中增加丰富功能的可能性。

通过深入对比国产密码算法与经典密码算法的异同，授课教师将知识与技能转化为学生的内在德行和素养，培养其家国情怀和社会责任感。鼓励学生将个人成长与国家发展紧密结合，将个人奋斗融入到实现中华民族伟大复兴的中国梦中。始终坚守“立德树人”的根本任务，致力于培养既有专业技能又有高尚品德的复合型人才，为国家的繁荣富强和信息安全事业提供坚实的人才支撑。

3.2 发展“知识扩展式”的前沿教学方法

为提升和发展学生在隐私计算研发方面的能力，我们扩展设计了如表1所示的3个前沿实验课程活动，使学生通过课堂实验教学深入了解隐私计算的发展动态和研究热点，掌握最新的学科前沿动态，通过学科的协同推进，帮助学生构建多维知识结构体系。

隐私计算框架“隐语”的学习与应用。我们与蚂蚁智信（杭州）信息技术有限公司携手，共同培养具备密码学与隐私计算技术的复合型应用人才，通过教授隐私计算框架“隐语”的相关技术知识，学生能够快速通过官方文档和在线教程入门。在实验课程中，学生被分为小组，选择具体的应用场景，如医疗数据处理、金融数据分析或物联网数据聚合等，明确数据处理需求，并设计在加密数据上进行的计算任务。学生使用“隐语”框架实现其设计的应用，克服在保证数据隐私的同时实现高效计算的挑战。随后，授课教师指导学生对应用进行性能测试和隐私评估，深入分析同态加密对计算效率和数据安全性的影响。最后，各小组展示实验成果，分享开发过程中的挑战与解决方案，并通过讨论加深对同态加密潜在应用和局限性

的理解，提升学生对隐私计算技术的掌握。

区块链与隐私交易的模拟。零知识证明作为一种关键的隐私计算技术，被应用于区块链的交易中以确保交易的隐私性。通过构建和模拟区块链交易平台，提升学生对隐私技术应用的理解。该实验活动使用 Solidity 语言撰写智能合约，以实现交易过程中的隐私保护和正确性验证。利用 Remix IDE 集成环境进行智能合约的开发和测试，通过 Truffle Suite 框架管理去中心化应用程序和合约部署，借助 Ganache 模拟个人以太坊区块链进行开发测试。为了将零知识证明集成到交易中，使用 ZoKrates 工具包。学生通过分享实验过程中的经验与挑战，深入了解零知识证明在金融、物联网等领域的应用潜力及其技术局限性。

表 1 扩展设计前沿实验课程活动

前沿实验课程活动名称	教学工具	课程活动目的
隐私计算框架“隐语”的学习与应用	蚂蚁智信（杭州）信息技术有限公司提供的“隐语”框架	加深学生对同态加密潜在应用和局限性的理解，提升学生对隐私计算技术的掌握
区块链与隐私交易的模拟	Remix IDE 集成环境、Truffle Suite 框架、ZoKrates 工具包	帮助学生深入了解零知识证明在金融、物联网等领域的应用潜力及其技术局限性
多方安全计算的实验	Fairplay 框架等	帮助学生了解多方安全计算领域最新研究进展和技术挑战，促进他们掌握多方安全计算的基础知识和应用技巧

多方安全计算的实验。多方安全计算允许多个参与方在各自维护数据隐私的情况下，协同完成复杂的计算任务。即使参与方之间缺乏信任，也能确保在不透露各自数据的前提下，共同得出准确无误的计算结果。该技术在保护数据隐私的同时，充分保障了计算的完整性和可靠性。实验采用 Fairplay 框架，设计协议以确保敏感数据在多方之间共享和传输时不会遭到泄露，同时高效地实现既定的计算目标。在实验过程中，帮助学生了解多方安全计算领域的最新研究进展和技术挑战，促进他们掌握多方安全计算的基础知识和应用技巧。通过多维度的知识整合，进一步提升学生在隐私计算领域的创新能力与实践技能。

3.3 结合“学科交叉式”的教学场景案例

将密码学基础实验课程教学内容与新工科建设紧密结合，聚焦人工智能、大数据、区块链等数字化领域的最新发展。同时，结合企业的实际应用需求与问题，打造如表 2 所示的面向企业需求的典型教学案例。通过将企业最新的技术资源或需求融入到典型的教学案例中，实现学生知识能力储备与企业需求的高效匹配，帮助学生在学习过程中解决实际问题，从而提升其在密码学领域的应用能力和创新能力。

表 2 设计面向企业需求的典型教学案例

设计的典型教学案例	案例教学目的
在数字签名教学课程中融入区块链场景	该案例通过将传统的数字签名技术与实际区块链场景相结合，帮助学生掌握基本密码技术并理解其商业价值
在密钥交换教学课程中融入物联网设备安全连接场景	该教学案例旨在帮助学生加深对密码技术理论的理解，并促进他们将所学应用于解决实际的物联网安全问题
在对称和非对称加密教学课程中融入人工智能模型保护场景	该案例帮助学生理解对称及非对称加密技术在人工智能模型保护中的关键作用，从而具备在实际应用中设计和实施安全方案的能力

（1） 在数字签名教学课程中融入区块链场景。区块链上的数字签名验证是确保区块链技术安全性和可靠性的重要组成部分。数字签名在区块链中用于验证交易发送者的身份，确保交易确实由持有相应私钥的实体发起。同时，数字签名确保交易数据在传输过程中未被篡改。只有合法拥有私钥的用户才能生成有效的签名，从而保障数据的完整性和真实性。使用数字签名后，交易发起者无法否认其已经发送过的交易，这种不可否认性在合约执行和法律合规中至关重要，尤其在金融和供应链等行业应用中显得尤为关键。通过将传统的数字签名技术与实际区块链场景相结合，帮助学生掌握基本密码技术并理解其商业价值。

（2） 在密钥交换教学课程中融入物联网设备安全连接场景。课程帮助学生理解密钥交换技术的基本原理和核心算法，特别是诸如 Diffie-Hellman 协议等经典方案。通过实例演示，在复杂的物联网环境中，成千上万的设备如何高效且安全地实现密钥交换。密钥交换技术的核心在于使设备能够在无预先共享密钥的情况下，安全地协商并建立一个共同的密钥。这些生成的密钥随后被用于后续的加密通信中，从而有效防止数据的窃听和篡改风险。该教学案例旨在帮助学生加深对密码技术理论的理解，并促进他们将所学应用于解决实际的物联网安全问题。

（3） 在对称和非对称加密教学课程中融入人工智能模型保护场景。该教学案例旨在让学生掌握对称和非对称加密的基本概念、核心算法及其广泛应用的能力。通过将经典加密算法与新兴应用背景结合，引

导学生理解如何巧妙地将这些加密技术应用于人工智能模型的保护之中，确保模型的敏感数据和算法逻辑得到强有力的安全保障。该案例提升学生在现实场景中使用密码学技术的能力，帮助学生获得理论与实践相结合的学习体验，理解对称及非对称加密技术在人工智能模型保护中的关键作用，从而具备在实际应用中设计和实施安全方案的能力。

3.4 提供“师生讨论式”的灵活互动

在课堂上，通过如图 1 所示的“提问-思考-评价-反馈”流程进行结构化讨论，与学生进行深度的教学互动与思维碰撞，鼓励学生从被动接受转为主动探索，通过提出问题激发学生的好奇心与求知欲，鼓励学生自由表达观点、分享见解，促进知识内化，培养批判性思维和创新能力。授课教师根据学生的作答结果，及时调整和再说明课程的重难点，从而灵活调整教学策略，确保每位学生都能扎实掌握核心概念与技术。

在课后，充分利用丰富的线上平台资源，为学生提供便捷的答疑渠道，确保他们在遇到困惑时能够及时获得解答，从而有效巩固课堂所学。同时，授课教师会定期在平台上发布补充材料，这些材料可能是对课程内容的深入拓展，或是前沿研究的简介，旨在拓宽学生的知识视野，激发他们的探索兴趣。此外，线上平台还为学生们提供交流渠道，便于分享学习心得，形成持续的学习社群。为支持学生的自主学习，授课教师精心挑选一系列自学资源，包括视频教程、在线课程、专业文章等，这些资源不仅覆盖了密码学的基础理论，还涉及其在实际应用中的前沿探索，帮助学生在课外时间也能保持学习的连贯性和深度。

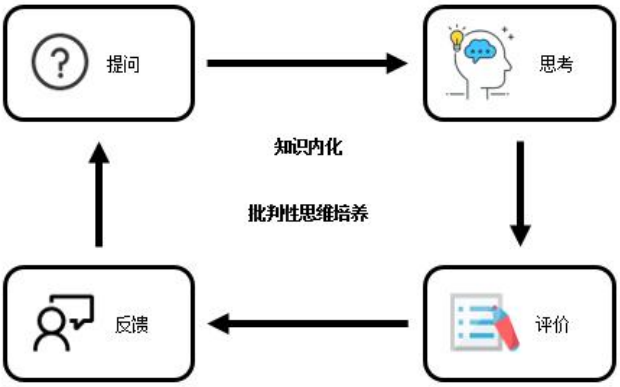

图 1 结构化师生讨论方式

4 教学改革效果分析

武汉大学国家网络安全学院密码学教学团队借助蚂蚁智信（杭州）信息技术有限公司的支持，自推行密码学基础实验课程改革以来，取得了显著成效。

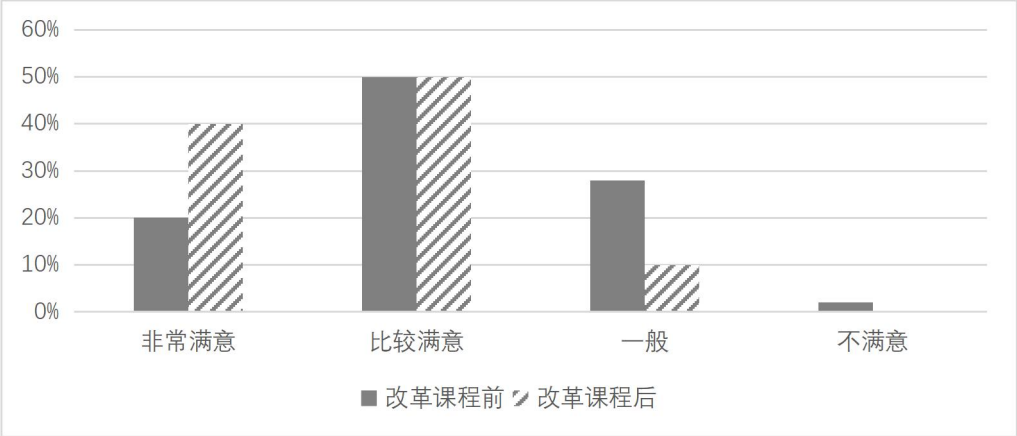

图 2 教学改革前后学生满意度对比

（1）学生体验与反馈良好。团队通过引入匿名问卷及多维度教学评价机制，全面收集并分析了学生对于改革课程的反馈意见。结果如图 2 所示，学生们对改革后的密码学基础实验课程给予了高度评价。改革后的课程成功引起了学生对密码学的浓厚兴趣，他们不仅开始关注国产密码技术的最新发展动态，还积极思考讨论国家数据安全事件。

许多学生表示，这样的课程内容让他们感受到了密码学与实际生活的紧密联系，从而自发地加入到相关的科研项目之中，积极探索未知领域，为国家的网络安全事业贡献自己的力量。

（2）学生实践与创新能力提升。通过一系列精心设计的实验活动，学生们的动手能力得到了全面锻炼。这不仅帮助他们熟练掌握各种密码学工具和技术，还培养他们将所学知识灵活应用于解决实际问题的能力。改革后的课程同样重视创新意识和批判性思维的培养，鼓励学生勇于挑战传统观念，提出独特见解。在这种创新和探索精神的引导下，学生们积极参与各类网络安全竞赛，并屡获佳绩，如在全国密码技术竞赛中荣获特等奖和一等奖、在 CCF 第三届大学生区块

链技术与创新应用竞赛中荣获二等奖等，这些奖项充分展现了理论知识与实践操作深度融合的卓越成果。

（3）学生职业发展和就业思维拓宽。团队紧密追踪行业发展趋势，灵活调整课程内容，确保传授的知识与技能始终紧贴市场需求脉搏。通过与蚂蚁智信（杭州）信息技术有限公司等业界领先企业的深度合作，为学生提供丰富实习和实训机会，创造参与真实企业项目的宝贵机会，使学生在实践中深化对密码学理论的理解，并显著提升解决实际问题的能力。改革课程紧密对接社会需求，帮助学生扩宽就业思维，为其职业发展奠定坚实基础。

5 结束语

针对密码学基础实验教学课程中存在的问题，采用“价值导向式”的教学思政理念，发展“知识扩展式”的前沿教学方法，同时结合“学科交叉式”的实实际教学场景案例，并提供“师生讨论式”的线上线下灵活互动 4 项教学改革措施。通过结合隐私计算研发能力的培养，密码学基础实验教学的改革已初见成效，未来将进一步深化教学改革，持续创新教学方法，为国家培养更多具备扎实密码学基础与隐私计算能力的优秀网络安全人才。

参 考 文 献

[1] 国务院办公厅.习近平：高举中国特色社会主义伟大旗帜为全面建设社会主义现代化国家而团结奋斗：在中国共产党第二十次全国代表大会上的报告[EB/OL].[2022-10-25]. http://www.gov.cn/xinwen/content_5721685.htm.

[2] 宋晓锋,倪林,韩鹍等. CTF 竞赛融入网络安全人才培养过程的探索与实践[J].计算机教育,2021(11):1-5.

[3] 本报评论员.坚持把立德树人作为中心环节[N]. 光明日报,2016-12-09(001)

[4] 邓芳,叶文,卢向群,梁美玉.《数据库系统原理》实验环节课程思政研究与实践[J].计算机技术与教育学报,2022,10(03):43-46.

[5] 王彤，陈锦柱等. 面向新工科的计算机类专业软硬件协同创新实践教学模式探索[J].计算机技术与教育学报,2022(11):1-8.

[6] 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,2017,38(1):43-46.

[7] 李德顺,姚姜源,羊秋玲等.本科院校密码学课程体系建设研究与实践[J].高教学刊,2021(36):93-96.