AI 与量子时代信息安全数学基础的教学探索

王兵
航天工程大学 基础部，北京 怀柔 101416
DOI: 10.61369/TACS.2025110052

摘　　要： 人工智能、量子计算与大数据分析的快速发展，正在深刻重塑了信息安全领域的格局，并对支撑密码协议、安全通信及数据保护的数学基础构成了前所未有的挑战。随着密码学向后量子密码学转型，数学工具的复杂度持续攀升，这对《信息安全数学基础》课程的教学提出了严峻挑战。本文聚焦当前教学的核心难题，并提出一项综合改革方案，旨在提升课程的前沿性与教学实效性，进而增强学生在新技术时代的核心素养与实践能力。

关 键 词： 信息安全；后量子密码学；人工智能；量子计算；课程设计；教学方法

Exploration of Teaching the Mathematical Foundations of Information Security in the AI and Quantum Era

Wang Bing
Department of Basic Sciences, Aerospace Engineering University, Huairou, Beijing 101416

Abstract: The rapid advancement of artificial intelligence, quantum computing, and big data analytics is profoundly reshaping the landscape of information security, while simultaneously imposing unprecedented challenges on the mathematical foundations supporting cryptographic protocols, secure communications, and data protection. As cryptography transitions toward a post-quantum paradigm, the escalating systemic and complexity demands of mathematical tools have rendered traditional pedagogical frameworks increasingly inadequate, thereby presenting severe challenges to both the content and objectives of the course "Mathematical Foundations of Information Security."

Keywords: information security; post-quantum cryptography; artificial intelligence; quantum computing; curriculum design; teaching methods

引言

近年来，人工智能的迅猛发展和量子技术的突破，在信息安全领域产生了深远而颠覆性的冲击与威胁，传统的信息安全数学基础的教学已经不能应对新时代的挑战。人工智能编程能力，特别是大型语言模型 和 AI 代码生成工具的兴起，正在深刻改变信息安全领域的编程实践。但它带来的不是简单的“取代”，而是一场深刻的“范式转移”[1]。因此，未来的安全专家，将不再仅仅是编程技巧娴熟的技术员，而是能利用 AI 时代新威胁复合型人才。伴随着量子技术的突破，特别是 Shor 算法对 RSA、ECC 等公钥密码体系的威胁，不仅仅是要求我们更换几个加密算法，而是从根本上动摇了传统信息安全的数学基石。传统信息安全数学基础主要围绕“计算复杂性”这一核心思想，即“某些数学问题在经典计算机上是难以计算的”。量子计算的发展对传统信息安全数学基础教学的影响是革命性的。教学内容必须从依赖“经典难解问题”转向“后量子难解问题”，并大幅加强量子算法原理和后量子密码数学基础的教学。教学的目标将从“培养能使用当前密码工具的学生”转变为“培养能理解、评估甚至创造未来密码系统的研究者与工程师”[2]。

信息安全的数学基础涉及代数、数论、概率论等多个领域。这些构成了确保数据安全传输和存储的算法基础。数论是核心，尤其是在公钥密码学中。欧拉定理和中国剩余定理等概念使得 RSA 成为可能，其安全性依赖于分解大整数的难度。代数支持对称加密和纠错码。概率论对于密钥生成中的随机性和分析攻击成功率至关重要。熵度量，如香农熵，量化了密码密钥中的不确定性。计算复杂性区分了可行与不可行的问题。P 与 NP 问题关系到单向函数是否存在，这对于像 SHA-256 这样的哈希函数至关重要[3]。传统的教学方法包括讲授这些主题，并辅以 Python 等语言的编程作业来实施算法。例如，中国科学院大学（UCAS）的课程涵盖了信息安全的概率、代数和复杂性。然而，这些基础正在演变。人工智能的兴起要求课程设置突破传统主题，教学内容必须包含人工智能在密码分析中的作用，比如利用神经网络测试高级加密标准（AES）或 RSA 等系统的加密漏洞。这可能要求教师掌握人工智能相关概念，包括机器学习算法，以便解释这些概念与数学安全原理之间的交叉点 [4]。另外，AI 也催生了复杂的攻击，如生成对抗网络（GANs）创建虚假数据以绕过身份验证。教学内容必须覆盖 AI 如何利用数学弱点，例如通过优化损失函数来发现加密缺陷。量子计算对经典密码学构成了生存威胁，

同时也提供了新的安全范式，改变了安全领域数学的教学方式。Shor 这样的量子算法通过量子傅里叶变换有效地进行因数分解，从而攻破 RSA。Grover 算法加速了暴力破解，影响了对称密钥。因此，教学内容必须包括量子基础知识：作为希尔伯特空间中的向量的量子比特，状态为，并通过幺正矩阵进行操作。后量子密码学应运而生，其中的格基方案如 Kyber 依赖于带误差的学习（LWE）问题。量子密钥分发（QKD）利用纠缠来实现无法破解的密钥，其安全性基于贝尔不等式和无克隆定理。像 MIT 的量子密码学课程这样，以最少的先决条件介绍这些内容。未来的课程应强调混合系统，教授适用于后量子混合系统的数学。总之，数学核心仍然至关重要，但教学必须纳入跨学科元素，以适应现代环境[5]。

一、信息安全数学基础教学的现状

人工智能（AI）和量子计算的快速发展正在重塑信息安全（infosec）领域，然而技术变革步伐的加快，使得理论教学与当代网络安全研究和实践所需技能之间的差距日益扩大，导致传统的数学课程常常无法满足新的密码框架、隐蔽攻击模型以及由人工智能和量子计算驱动的算法创新所带来的需求。这要求我们对信息安全的数学基础教育进行根本性的改革。传统上，信息安全教育侧重于经典数学，例如用于 RSA 加密的数论、用于风险评估的离散对数与概率论，以及用于网络安全的图论。然而，量子计算通过诸如 Shor 算法等手段威胁着许多经典密码学协议，该算法能以指数级速度更快地分解大数；与此同时，人工智能在威胁检测、异常分析和自动化攻击方面引入了新的范式。改革教学方法需要整合抗量子数学、AI 驱动的统计模型以及跨学科概念，以培养学生适应后量子时代和 AI 增强型世界的能力。此次改革强调模块化、可及性的课程设计，在现有 STEM 框架基础上构建，而非创建全新的项目[6]。

（一）当前课程内容面临的主要挑战

1. 量子技术对经典密码学的威胁：许多信息安全课程忽视了量子力学，导致学生对“Q 日”（即量子计算机攻破当前加密标准的时刻）毫无准备。随着量子算法（特别是 Shor 算法和 Grover 算法）的潜在威胁，传统的公钥密码学面临着结构性漏洞。然而，许多现有的教学大纲仅对量子计算原理进行了有限的讨论，几乎没有系统性地介绍后量子密码方案的数学基础。由于后量子密码学严重依赖于包括编码理论、格理论、基于同源的结构以及多元多项式系统在内的高级数学理论，未能纳入这些主题将使学生对未来的安全范式准备不足[7]。

2.AI 在安全领域的影响：人工智能（AI）的崛起正对信息安全的数学基础构成严峻挑战。首先，经典数论、代数与概率模型在应对 AI 驱动的新型攻击（如基于深度学习的密码分析、对抗样本生成）时显露出理论局限性，迫使教学需融入优化理论、张量代数等现代数学工具；齐次，传统以“正确性证明”为核心的静态知识体系，难以支撑对 AI 动态安全威胁（如模型窃取、数据投毒）的概率化防御策略设计，要求重构“攻防博弈”的动态教学范式；最后，单一数学抽象思维无法匹配智能时代的安全需求，亟需融合可解释性 AI、隐私计算等交叉领域的数学框架，培养学生运用微分几何、信息熵理论解决联邦学习安全或区块链共识机制等复杂场景的能力。这实质是一场从“密码学数学”向“智能安全数学”的认知革命[8]。

（二）当前教学面临的主要问题

1. 对计算思维和算法复杂度的重视不足：现代密码学本质上是计算性的，但许多数学课程过于强调理论证明，而未能将其与算法效率、复杂度分析或安全性规约等概念相结合。因此，学生难以培养出评估安全假设或理解对手模型所需的计算直觉。

2. 缺乏计算实验与工具支持的学习：数学基础课程的传统教学方式通常非常理论化，往往缺少能够增强概念理解的计算工具。学生们很少有机会使用 SageMath、Python（SymPy，NumPy）或 MATLAB 等平台来模拟密码构造、试验代数结构或通过计算验证其属性。这种计算实践的缺失削弱了学生内化数学原理并将其应用于现代密码系统的能力。

二、信息安全数学基础教学的改革与创新

1. 重构“问题导向”的内容体系，强化“数学－安全”关联：以安全需求驱动数学理论：将课程内容按“典型安全问题”重组。例如：模块1：“古典密码的数学破解”（凯撒密码→模运算；维吉尼亚密码→最大公约数）；模块2：“公钥密码的数学基础”（RSA →数论（欧拉函数、模逆元）；ElGamal →离散对数难题；ECC →椭圆曲线群）；模块3：“新型密码的数学支撑”（后量子密码→格理论；同态加密→环上容错学习问题）。每个模块明确“安全目标－数学工具－应用案例”的主线，避免“为数学而数学”。引入真实安全事件：结合历史案例（如“RSA-129破译”“心脏滴血漏洞”），讲解数学原理在实际攻击 / 防御中的作用，增强代入感[9]。

2. 动态更新教学内容，对接前沿需求：增加“格理论”（用于抗量子密码）、“编码理论”（用于纠错码与密码）、“概率图模型”（用于侧信道分析）等内容，简要介绍其在 NIST 后量子密码标准中的应用。融合交叉学科知识：与“密码学”“网络安全”课程联动，例如在讲解“双线性配对”时，同步介绍其在“短签名”“基于属性的加密”中的具体实现，避免知识割裂。引入开源工具与数据集：利用 SageMath、OpenSSL 等工具，设计“从数学公式到代码实现”的实验（如生成椭圆曲线参数、模拟离散对数攻击），让学生直观感受“数学→算法→代码”的转化过程。

3. 实施“分层分类”教学，满足差异化需求：针对数学基础薄弱的学生，开设“预备模块”（如初等数论、线性代数速成），通过在线微课（MOOC）+ 翻转课堂形式，确保学生具备必要的

前置知识。拓展提高通道：为基础扎实的学生提供“进阶内容”（如代数数论、椭圆曲线密码的高效实现），通过“导师制”引导参与科研（如优化 SM2 算法的标量乘法），或结合竞赛（如全国密码技术竞赛）设计课题。个性化学习路径：利用智慧教学平台（如雨课堂、学习通）跟踪学生学习数据，动态推荐资源（如基础薄弱学生推送“模运算”动画讲解，学有余力学生推送“格基约减算法”论文）。

4. 构建“理论 - 实践 - 创新”一体化的实践体系：三级实验设计：基础层：验证性实验（如用 Python 实现 Miller-Rabin 素性测试）；综合层：设计性实验（如基于椭圆曲线设计一个简单的密钥交换协议，并分析其安全性）；创新层：研究性实验（如对比不同格密码方案的效率，提出优化建议）。虚实结合的平台建设：开发虚拟仿真实验平台（如“量子攻击下的 RSA 破解模拟”），降低复杂数学实验的成本；同时开放实验室，支持学生自主设计实验（如侧信道攻击的能量轨迹分析）。

5. 创新教学方法，激发主动学习动力：翻转课堂 + 混合式教学：将基础理论（如“群的定义”）制作成微视频供学生课前自学，课堂时间聚焦“疑难解答”和“案例讨论”（如“为什么是循环群？”）。项目式学习（PBL）：以“设计一个安全的即时通讯协议”为总任务，引导学生拆解问题（如密钥协商需 Diffie-Hellman，身份认证需数字签名），通过小组协作完成数学推导与代码实现。设计“数学闯关”小程序（如“破解 RSA-100”挑战赛），通过积分、排名机制激发竞争意识；优秀作品可推荐至学术会议或竞赛。

6. 完善多元化考核，聚焦能力评价：过程性评价：提高平时成绩占比（如 40%），包含“实验报告”“小组讨论贡献度”“阶段性测验”等，重点考察“数学工具的应用能力”（如“能否用中国剩余定理优化 RSA 解密”）。创新性加分：对参与科研项目、发表论文、竞赛获奖的学生给予额外加分，鼓励探索前沿问题。反思性总结：要求学生撰写“课程学习档案”，记录“最困惑的数学问题”“最意外的应用关联”，促进元认知能力发展。

三、总结

《信息安全数学基础》的改革需以“服务安全需求”为核心，打破“纯数学”的教学惯性，通过内容重构、方法创新、实践强化，将课程从“数学理论课”转型为“安全能力奠基课”。最终目标是培养学生“用数学思维解决安全问题”的核心能力，为其在密码学、网络空间安全等领域的深入研究与职业发展奠定坚实基础。

参考文献

[1] 张兴兰 . 信息安全专业数学课程的教学研究 [J]. 计算机教育 ,2011(13):45-46.

[2] 朱士信 . 量子常循环码的构造研究 [J]. 四川师范大学学报 (自然科学版),2023,46(5):569-580.

[3] 聂旭云 , 陈大江 , 熊虎 . 以算法为核心的信息安全数学基础教学体系探索与实践 [J]. 大学数学 ,2021,37(3):59-65.

[4] 李功丽 , 彭晚红 , 张聪品 , 等 . 高效的信息安全教学模式探索 : 与德国高校教学交流后的总结与反思 [J]. 计算机教育 ,2020(3):30-34.

[5]Xu,F.;Ma,X.;Zhang,Q.;Lo,H.K.;Pan,J.W.Secure quantum key distribution with realistic devices.Rev.Mod.Phys.2020,92,025002.

[6]D.J.Bernstein,J.Buchmann and E.Dahman(eds),Post-Quantum Cryptography,Springer-Verlag,Berlin,2009.

[7]G.L.Butler,Simultaneous packing and covering in Euclidean space,Proc.London Math.Soc.25(1972),721-735.

[8]Hellman,M.New directions in cryptography.IEEE Trans.Inf.Theory1976,22,644 - 654.

[9]V.S.Miller,Use of elliptic curves in cryptography,Advances in Cryptology,CRYPTO'85,Santa Barbara,1985.LNCS,218(1986),417-426.

