

后量子密码技术发展与高职院校开设密码学专业的可行性研究

摘要：随着量子计算机的不断发展，传统密码学技术面临着被破解的风险，后量子密码技术（以下简称PQC）的研究和应用变得越来越重要。本文旨在探究PQC的发展与实现,并基于PQC发展面临的潜在挑战对高职院校开设密码学专业的可行性进行讨论。此外，本文还使用liboqs库实现了密钥交换，并基于LRWE和NTT的后量子密码协议进行加解密，为了解PQC的应用与实现细节提供直接参考。

关键词：后量子密码技术（PQC）、LWE、RLWE、量子计算机、NTT

一、引言

量子计算机发展速度非常快，对现有密码系统的安全构成了威胁。后量子密码（PQC）旨在开发新的密码算法，抵抗量子计算机的攻击^[1]。

（1）量子计算机

量子计算机是一种利用量子力学原理进行复杂计算的计算机，其叠加性、量子位纠缠、量子加速等性质，使其能够进行并行计算。提供比经典计算机更快的解决复杂问题的潜力^[2]，随着量子位数量的增加，其计算能力也呈现指数增长^[3]。如用于大整数分解的Shor's算法和搜索未排序数据库的Grover's算法^[4]，就展示出比经典计算机更快解决特定问题的潜力，这是许多密码系统的基础。

（2）后量子密码

后量子密码，简称PQC，是指设计用于抵御量子计算机攻击的密码算法和协议。它是密码学的一个领域，专注于开发能够抵御大规模、强大量子计算机潜在威胁的加解密方案^[5]，这些密码方案基于经典和量子计算机都难以计算的数学问题设计。

（3）PQC研究现状

美国国家标准与技术研究院（NIST）于2016年启动后量子密码标准化项目，邀请研究人员和组织提出后量子密码算法。截至目前，该项目经历4轮，征集到了基于格、基于编码、基于多变量、基于哈希、基于同源等各类密码方法。NIST在2024年8月发布了首批3项后量子密码标准，详见表1，并计划在不久的将来推出第4项标准。这些标准包括多种技术和方法，以增强和维护数字基础设施的安全性和完整性。

我国也于2018年面向全国启动了密码算法设计竞赛活动，筛选出14个公钥密码方案。此外，国内相关企业和组织也在积极开展后量子密码应用标准的探索。

二、PQC的实现

（1）预备知识

带误差学习（LWE）问题^[6]代表了后量子密码中基于格的加密范式中的一个关键密码挑战。在LWE问题中，线性方程组包括一个误差项，该公式如(1)，给定一个矩阵A、密钥向量S和一个小的随机向量e，从观察向量b中恢复密钥向量S。这个问题的难度源于

噪声e，导致观察向量b与真实乘积A·S之间存在差异。

$$\begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{bmatrix} \cdot \begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix} + \begin{bmatrix} e_1 \\ \vdots \\ e_m \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} \pmod{q} \quad (1)$$

模多项式环^[7]是一种代数结构，由于其对多项式运算和系数算术的双重约束，在密码学中得到广泛应用。模多项式环的结构如(2)所示，主要由两个部分组成：(3)和(4)。Xⁿ+1的模的概念代表一种抽象的数学思想，定义为Xⁿ+1=0，因此，Xⁿ=-1。当处理一个多项式Z(X)，其中n≥m时，通过Xⁿ+1的模去除度数高于Xⁿ的项。

$$Z(x) \pmod{f(x)} \quad (2)$$

$$Z(x) = z_0 + z_1x + z_2x^2 + z_3x^3 + \dots z_mx^m \quad (3)$$

$$f(x) = x^m + 1 \quad (4)$$

RLWE（带误差的环学习）问题^[8]代表了LWE问题的一个变体。该方法不是使用通用矩阵A，而是使用更简单的循环矩阵。具体结构如下：

$$\begin{bmatrix} a_0 & -a_3 & -a_2 & -a_1 \\ a_1 & a_0 & -a_3 & -a_2 \\ a_2 & a_1 & a_0 & -a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix} + \begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ e_3 \end{bmatrix} = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} \pmod{q} \quad (5)$$

RLWE问题需将矩阵和向量映射到模多项式环中.这种映射选择适当的模多项式来约束最高幂级数，仅使用有限数量的元素，从而简化计算要求并提高效率。其表达式为：

$$A(x) \cdot S(x) + e(x) = b(x) \pmod{q \pmod{x^n + 1}} \quad (6)$$

（2）密钥交换协议

基于RLWE问题的密钥交换协议展开为三个不同阶段，详见图1。

假设Alice和Bob两个用户，旨在为后量子加密生成会话密钥。

①初始化阶段：Alice和Bob就公共矩阵A、素数模数q和误差e的分布达成一致；

②密钥生成阶段：Alice选择一个私向量S_A，并计算b_A=A·S_A+e_Amod q，其中e_A是从已知分布中随机选择的小误差向量，然后将b_A发送给Bob。类似地，Bob选择一个私向量S_B，并计算b_B=A·S_B+e_Bmod q，其中e_B也是来自相同分布的小误差向量，将b_B发送给Alice；

③共享密钥阶段：Alice利用Bob发送的b_B和自己的密钥S_A，计算U_A=S_A·b_Bmod q。Bob使用从Alice收到的b_A，计算U_B=S_B·b_Amod q。

（3）安全性

PQC密钥交换协议的安全性依赖于RLWE问题.重点对误差向量e的大小进行限制,如果误差向量过大,可能会导致秘密信息更容易被推测出来;而如果误差向量过小,则可能无法充分发挥其对秘密信息的保护作用.在合理范围内的e_A和e_B的可在不影响协议效率的前提下,防止第三方从传输的数据b_A和b_B中有效地恢复出密钥S_A和S_B,最大程度地确保协议的安全性。

（4）数论变换

PQC主要依赖于解决RLWE问题，而密钥生成计算量大，时间复杂度高。数论变换算法（NTT）能够降低计算复杂度，加快密钥生成速度，同时保持较高的安全性^[9]。NTT将多项式以系数表示转换为值表示，使乘法简化为特定点处的直接计算。详见图2，多项式A(x)和B(x)，计算其乘积C(x)，通过系数到值的转换、逐点乘法及逆变换回系数形式，并运用分治方法，将时间复杂度从O(n³)降低至O(nlogn)，实现了高效计算。

（5）代码实现

本文调用liboqs库中的Kyber算法

实现简单的加密和解密，并基于LRWE和NTT实现了加解密和密钥交换过程。代码详见“Post-quantum-cryptography-Demoipynb”（网址：https://github.com/IvyWang94/Post-quantum_cryptography_Demogit）。

三、PQC发展对高职院校专业设置的需求分析

（1）PQC发展面临的挑战

PQC的发展仍面临多重挑战,在理论安全方面,清华大学助理教授陈一磊提出针对解格问题及LWE问题的量子算法尝试^[10],虽因存在无法修复的bug而未成立,但若未来能找到LWE问题的解决方案,将对PQC构成根本威胁;在物理安全方面,PQC还面临侧信道攻击的挑战^[11],瑞典皇家理工学院研究团队已成功利用“递归学习”的技术开发了一种创新的侧信道攻击,成功破解了NIST标准化的后量子密码算法之一——Crystals-Kyber算法^[12],展示了加密实现中物理漏洞的潜在风险和影响.此外,考虑到密码系统过渡的历史经验,需要很长的一段时间^[13],如NIST发布的过渡到PQC标准的初始公开草案《Transition to Post-Quantum Cryptography Standards》，规划至2035年完成政府机构的加密系统转变.在我国,金融行业作为密码应用的重要领域,正着手前期研究以推动后量子密码迁移,预计从管理部门发布正式迁移通知到全行业采用将耗时3至5年。

（2）PQC技术推广与人才培养的紧迫性

随着技术的飞速发展,尤其是传统安全技术的发展赶不上量子计算机的发展速度,在推进PQC迁移过程中的人才缺口巨大,据估计我国对密码人才的需求人数约为30万人,未来5-10年将达到110万人左右^[14].在2023年,2024年的全国教育事业统计公报中公布的数据可知,高职院校毕业生数量超普通本科院校的毕业生数量,在大学生毕业生中占比约为53%至55.60%,且2024年招生人数约为55507万人（高职专科）和899万人（职业本科），高职院校的就业率普遍高于普通本科^[15]。因此,高职院校作为技术技能型人才培养的摇篮,开设密码学技术相关专业,对解决PQC面临的潜在挑战极为重要。

四、高职院校密码学专业建设的可行性

我国依托网络空间安全、计算机科学与技术等一级学科，在研究生、本科、职业教育阶段均设有密码学相关专业。根据2024年3月25日教育部发布的《关于公布2024年高等职业教育专科专业设置备案和审批结果的通知》（教职成函〔2024〕1号）文件，我国开设密码学技术应用专业的院校仅有14所，数量远不满足国家密码安全发展的需求。同时，根据《密码技术应用员国家职业技能标准》和《密码工程技术人员国家职业标准》，可为高职院校密码学专业开设提供直接指导，该专业建设体系可见图3。

此外，密码技术是一个实践性很强的领域，为此，高职院校在该专业建设过程中，需紧跟国家信息安全发展战略，通过与国家密码学会、密码企业的紧密合作，探索创新产教融合模式，建设先进的密码技术应用实训基地，增强学生职业技能和就业竞争力。

王燕懿

力,为企业提供定制化的人才培养服务,服务行业发展,实现双赢。

参考文献

- [1]Bernstein D J, Lange T. Post-quantum cryptography[J]. Nature, 2017, 549(7671): 188-194.
- [2]Ladd T D, Jelezko F, Laflamme R. Quantum computers[J]. Nature, 2010, 464(7285): 45-53.
- [3]Datta A, Flammia S T, Caves C M. Entanglement and the power of one qubit[J]. Physical Review A, 2005, 72(4): 042316.
- [4]Liu Y, Arunachalam S, Temme K. A rigorous and robust quantum speed-up in supervised machine learning[J]. Nature Physics, 2021, 17(9): 1013-1017.
- [5]Chen L, Jordan S. Report on post-quantum cryptography[R]. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology, 2016.
- [6]Bavdekar R, Chopde E J, Bhatia A, Tiwari K, Daniel S J. Post-quantum cryptography: Techniques, challenges, standardization, and directions for future research[Z]. Unpublished.
- [7]李梦甜. 基于环LWE的全态加密方案关键技术研究[D]. 战略支援部队信息工程大学, 2018.
- [8]高翔, 丁敬, 刘杰, 李琳. 基于RLWE问题的后量子安全远程口令协议[C]//信息安全与密码学: 第13届国际会议, Inscrypt 2017, 中国西安, 2017年11月3-5日, 修订精选论文. 卷13. 斯普林格国际出版, 2018: 99-116.
- [9]Bisheh- Niasar M, Azardera-khsh R, Mozaffari-Kermani M. High-speed NTT-based polynomial multiplication accelerator for post-quantum cryptography[C]//Proceedings of the 2021 IEEE 28th Symposium on Computer Arithmetic (ARITH). IEEE, 2021: 94-101.
- [10]Chen Y. Quantum algorithms for lattice problems[Z]. Unpublished, 2024.
- [11]吴伟波, 刘卓, 杨航, 张建平. 后量子密码学的侧信道攻击与对策综述[J]. 软件学报, 2021, 32(4): 1165-1185.
- [12]Dubrova E, Ngo K, Gärtner J. Breaking a fifth-order masked implementation of CRYSTALS-Kyber by copy-paste[Z]. Unpublished, 2022.
- [13]Barker W, Polk W, Souppaya M. Getting ready for post-quantum cryptography: Exploring challenges associated with adopting and using post-quantum cryptographic algorithms[R]. Dakota Consulting & NIST, 2021.
- [14]中国商用密码行业现状深度研究与发展前景分析报告（2023-2030年）[R]. 观研天下（北京）信息咨询有限公司, 2023.
- [15]高教发展资讯. 德州学院发展规划处[J]. 2024, 2(30): 6.

（作者单位：贵州水利水电职业技术学院）

规格编号	名称	技术基础	使用类型
FIPS 203, 模块化格基密钥封装机制标准 (Module-Lattice-Based Key-Encapsulation Mechanism Standard)	ML-KEM	Crystals-Kyber	密钥封装 (KeyEncapsulation)
FIPS 204, 模块化格基数字签名标准 (Module-Lattice-Based Digital Signature Standard)	ML-DSA	Crystals-Dilithium	数字签名 (Digital Signature)
FIPS205, 无状态哈希数字签名标准 (Stateless Hash-Based Digital Signature Standard)	SLH-DSA	SPHINCS+	数字签名 (Digital Signature)

表1 NIST发布的首批3项后量子密码标准

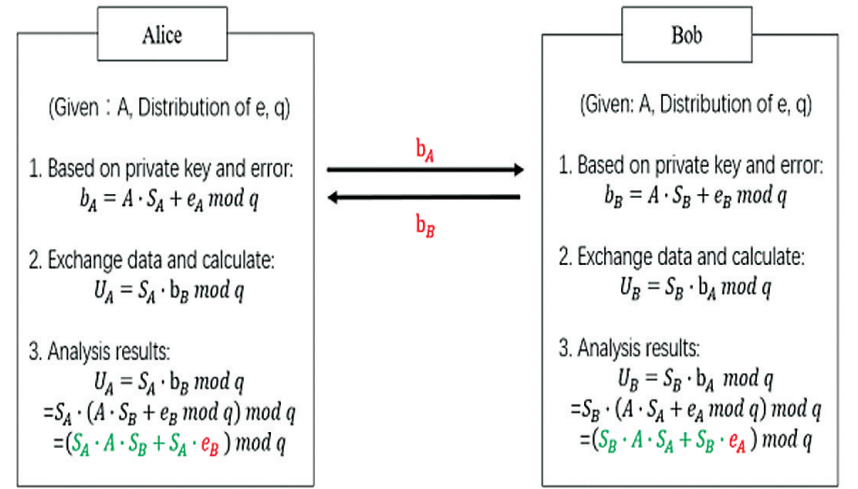


图1 密钥交换协议流程

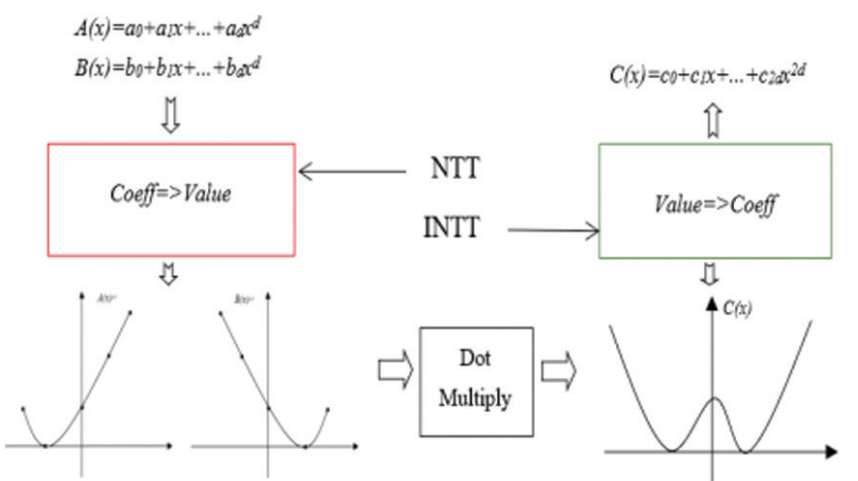


图2 数论变换

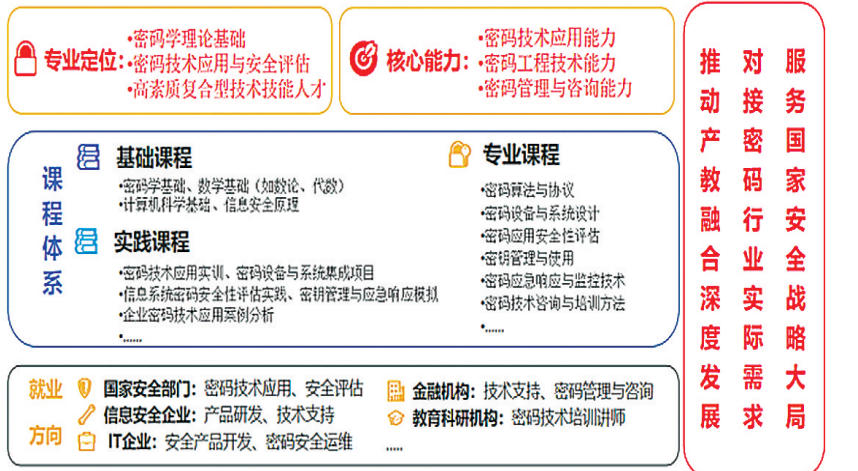


图3 密码技术应用专业

教学实践

在“双减”政策的大背景下，如何在保证教育质量的同时减轻学生的课业负担，成为了当前教育领域亟待解决的重要课题。课后作业作为教学过程中的重要环节，其设计不仅关系到学生对知识的巩固与应用，更直接影响到学生的学业负担与学习兴趣。沿河四中课题组在近两年的探索实践中，对初中数学课后作业的设计进行了深入思考与实践尝试，揭示了这一看似简单实则复杂的议题。

一、问题分析

（一）课后作业设计的挑战与困境

在落实“双减”政策的过程中，课后作业被视为提高教育质量与控制学生作业量的重要出路。然而，这一看似简单的策略在实施过程中却面临

诸多挑战。首先，学生的个体差异是课后作业设计的一大难题。不同学生的学习能力、兴趣与需求各不相同，设计难度适中的作业往往难以兼顾所有学生。若作业难度过高，部分学生可能无法完成，导致挫败感；若作业过于简单，则无法满足优秀学生的学习需求，缺乏挑战性。

沿河四中课题组在初期尝试采用例题变式的方法，以期在保持作业难度的同时增加题目的多样性与灵活性。然而，这一方法并未达到预期效果，大多数学生认为作业过于简单，缺乏挑战性，无法满足他们的学习需求。

（二）分层作业设计的探索与实践

鉴于例题变式方法的局限性，课题组进一步展开了分层作业设计的探索。分层作业设计旨在根据不同学生的学习能力与需求，为同一班级的学生设计三类不同难度的作业。这一方法在一定程度上解决了作业难度与学生个体差异之间的矛盾，使得每个学生都能在适合自己的作业中获得成长。

然而，分层作业设计也面临着诸多困难与挑战。首先，设计三类

作业需要投入大量的时间与精力，增加了教师的工作负担。其次，分层作业可能引发学生的歧视感与不公平感，认为自己被区别对待。因此，在实施分层作业设计时，教师需要谨慎考虑，确保作业的分层标准合理、公正，同时加强与学生的沟通与引导，消除学生的疑虑与不安。

（三）课后作业设计的长期性与复杂性

沿河四中课题组的探索实践表明，课后作业设计并非一蹴而就的简单任务，而是一个长期研究与实践的过程。在设计课后作业时，教师需要综合考虑学生的学习需求、个体差异、学科特点以及教育政策等多方面因素，确保作业既具有挑战性又符合学生的实际情况。

此外，课后作业设计还需要关注作业的反馈与评价机制。通过有效的反馈与评价，教师可以及时了解学生的学习情况与作业完成情况，为后续的教学提供有针对性的指导与调整。同时，学生也可以通过反馈与评价了解自己的学习情况，明确自己的优点

与不足，为后续的学习提供方向与动力。

二、解决办法

（一）分层课后作业设计。学校实施分层作业制度。老师们根据学生的学习水平和兴趣爱好，将作业分为基础巩固、综合应用和思维拓展三个层次。基础作业旨在巩固课堂知识，综合作业则是对知识的深化和应用，而思维拓展作业则鼓励学生进行跨学科的思考与实践。这样的设计，既满足了不同层次学生的需求，又激发了他们的学习兴趣。

（二）项目式课后作业设计。学校推行了项目式作业。老师们结合课程内容，设计了一系列具有实际意义的项目，让学生在完成作业的过程中，能够综合运用所学知识，解决实际问题。这样的作业形式，不仅锻炼了学生的实践能力，还培养了他们的团队合作精神 and 创新能力。

（三）生活化课后作业设计。学校鼓励老师们创新作业形式，将书本作业向生活化作业融合。首先，生活化作业能增强学生的实践能力

和动手能力，让他们将所学知识应用到实际生活中，提高学习的兴趣和积极性。

（四）“传帮带”模式完成课后作业。要求优秀學生根据自己的能力和时间，选择一带一或一带多的方式，对其他学生进行辅导。课后作业完成实现了日日清、周周清的目标。学生们对自己的学习进度有了清晰的认识，知道自己在什么时间需要完成什么任务。这有助于他们更好地规划自己的学习时间，提高学习效率。

（五）教师参与研究课后作业设计。数学组以学生实际需求为导向，充分考虑学生的学习特点和负担，开展了10余次课后作业设计专题研讨。在研讨过程中，教师们积极分享经验，深入探讨，不断优化作业设计，最终设计出1000余个课后作业案例。这些案例既注重知识的巩固，又注重能力的培养，更注重兴趣的激发，切实减轻了学生的负担。

（六）在校交流中探讨课后作业设计。学校与铜仁学院附中、铜仁十中、松桃四中、沿河教育教研中心等建立了良好的合作关系，通过共

享资源、交流经验、共同研讨等方式，不断提升自身的教育教学水平和研究能力。

（七）送教下乡送课后作业设计。少数民族地区城乡教育差距较大。为了缩小这一差距，沿河四中积极开展“送教下乡”活动，将优质的教育资源带到乡镇，组织学校优秀教师团队深入乡镇学校，开展教育教研活动，分享教育经验、送去课后作业设计理念，让农村教师了解到当前教育发展的最新动态，提高乡村教师的教育教学水平。

初中数学课后作业设计是一个复杂而长期的研究课题。在落实“双减”政策的过程中，教师需要不断探索与实践，寻找适合学生的作业设计策略与方法。通过关注学生的学习需求与个体差异、加强作业的分层设计与反馈评价机制建设等方面的努力，我们可以为学生提供更加优质、高效的课后作业体验，促进他们的健康成长与全面发展。

（作者单位：沿河土家族自治县第四中学）