河南師範大學

专业学位授权点建设年度报告

（2025 年）

授权学科 （学院公章）	名称：密码
	代码：1452

授权级别

□博士

☑硕士

2026 年 1 月 6 日

河南师范大学 数学与统计学院 4107002323084

一、目标与标准

(一) 培养目标

密码专业硕士学位培养目标是面向国家战略需求、经济社会发展和行业产业创新发展需求，培养思想政治素养高、德智体美劳全面发展的应用型、复合型高层次工程技术和工程管理人才。具体要求为：

1. 拥护中国共产党的领导，热爱祖国，遵纪守法，具有服务国家和人民的高度社会责任感、良好的职业道德和创新创业精神，以及科学严谨和求真务实的学习态度和工作作风。

2. 掌握密码专业领域坚实的基础理论和宽广的专业知识，熟悉密码行业领域的相关法律、标准和规范，理解各类密码算法的应用场景和相关安全需求，了解密码技术的发展现状和动态。

3. 具备较强的创新意识和实践能力，能够运用新技术与新理论解决密码领域的技术难题和工程问题，具有独立从事密码理论研究、密码设计与研发、密码管理与测评等某一方向工作的能力。

4. 掌握一门外语，具备良好的外语阅读、理解和撰写能力，能够开展国际化学术交流与合作，具有国际视野和跨文化沟通的能力。

5. 具有良好的团队合作精神、自主学习能力和抗压能力，能够适应密码行业快速发展的需求，胜任政府部门、科研院所、大型企业、互联网企业等单位的密码管理、研发、运维等岗位。

(二) 学位标准

本学位点授予工学硕士学位，按照学校及学院的相关规定，申请学位的研究生需达到课程学分、实践教学、学位论文等基本要求，方可授予学位。

1. 课程学分

课程分为公共必修课、专业基础课、专业必修课、公共选修课、专业选修课和专业实践环节，总学分不少于 41 学分。

2. 实践教学

密码专业硕士学位研究生在校期间，必须参加不少于半年的实践环节教学，可以采用集中实践和分段实践相结合的方式。依托校外实践基地完成，在校内外导师联合指导下，结合工程实践岗位，主要进行专业综合实践和应用能力训练。校外专业实践合格者记 6 学分。

3. 学位论文

研究生的学位论文必须开题，并由指导小组统一组织学生做开题报告，一般安排在第三学期，须认真填写《研究生开题报告审核表》。开题报告应包括密码相关的研究背景和拟开展的研究工作两方面内容，并进行详细答辩。开题报告主要考察学生对研究背景知识和密码相关研究领域的最新研究动态的了解，同时考察学生的文献综述能力，采用口头报告（10-15 分钟）和书面报告结合形式。开题第一次未通过，允许 1-2 月内再进行一次，仍未通过者，按学籍管理规定处理。

研究生中期考核要认真填写《研究生中期考核登记表》，学院对研究生的政治思想、课程学习、科研和实践能力等各个培养环节进行全面、综合测评。中期考核一般安排在第四学期的 5-6 月份进行，以专业为单位组成考核小组，考核小组由研究生导师和任课教师组成，对研究生的政治思想品德和学习态度、课程成绩及所修学分情况、论文进展情况、科研和实践能力、学术道德等方面进行审核和评定。学习成绩优良，达到考核内容要求的，进入硕士论文写作阶段；学习成绩较差，未达到考核内容要求的，不得申请硕士学位。

学位论文形式可以多样化，包括但不限于：应用研究类论文（应该注重从实际问题中提取关键问题和技术进行研究，提出创新性解决方案，并对其有效性和实用性进行验证）、设计类论文（如密码系统设计、密码协议设计等，应注重设计的完整性、可行性和实际部署效能）、产品开发类论文（如

密码算法实现、密码工具开发、密码应用系统研发等，应注重产品的完成度、技术先进性和实际应用效果）等。论文应具备一定的技术要求和工作量，体现在密码领域的综合能力，包括理论分析、技术实现和实际应用等方面。论文应具有一定的理论基础，同时注重先进性和实用性，能够为密码领域的技术发展或实际应用提供一定的参考价值。论文工作须在导师指导下独立完成，确保内容的原创性和学术规范性。

学位论文的基本要求遵照《河南师范大学授予硕士学位工作细则》的有关规定。学位论文应包括：摘要（中、外文）、目录、引言、正文、参考文献、致谢、必要的附录和在校期间科研成果情况。学位论文应做到具有创新性，达到硕士学位论文要求，概念准确，推理严密，语义通达，数据可靠，结构完整。论文按规定统一格式排版，具体见《河南师范大学研究生学位论文及其摘要编写格式的要求》。

论文评审应审核：作者综合运用科学理论、方法和技术手段解决密码技术问题的能力；论文工作的技术难度和工作量；解决密码技术问题的新思想、新方法和新进展；新工艺、新技术和新设计的先进性和实用性；创造的经济效益和社会效益等方面。论文除经导师写出详细的评阅意见外，还应有 2 位密码领域或相近领域的专家评阅。答辩委员会应由 5-7 位与密码领域相关的专家组成，成员一般应具有副教授及以上相当专业技术职务。

二、基本条件

(一) 培养特色

本学位点依据河南省社会经济发展的需求，优化师资队伍结构，注重人才培养与质量保证体系建设，形成了密码理论、密码工程与技术、密码应用等三个特色培养方向。具体如下：

密码理论主要研究基于编码的密码体制设计与安全性分析、编码与密码的代数理论等。其特色优势为：正交表作为组合数学的核心工具，其“平

衡性、对称性、抗干扰性”与密码学中“安全性、高效性、容错性”需求高度契合，形成密码理论的特色研究方向；聚焦非对称嵌套正交表的界限分析、不饱和正交表的汉明距离研究，将其转化为密码编码的“安全边界”与“容错阈值”；基于非对称可分解正交表的结构特性，设计分布式密钥管理机制。通过正交表的“可分解”属性实现密钥的分片存储与动态重构，结合 2 水平最优正交表的高效性，降低密钥分发与更新的计算开销，适用于区块链、无线传感器网络等多节点场景。近五年，在 Annals of Statistics, Information Science, Designs,Codes and Cryptography 等权威期刊上发表论文 53 篇，主持国家自然科学基金等项目 7 项。

密码工程与技术主要研究大数据安全与人工智能、区块链、密码协议的设计、安全多方计算、对称密码的安全性分析等。其特色优势为：元素中心化子相关的群论研究，为密码协议的“抗攻击能力、密钥生成效率”提供核心理论支撑。利用“每个元素中心化子为 TI-子群”的群结构特性，设计安全的密钥交换协议。TI-子群的“平凡交”性质可避免密钥被恶意截取后通过子群交集推导，结合群的代数运算复杂度（如离散对数难题），提升协议抗量子攻击、中间人攻击的能力，适用于涉密通信、金融交易等高危场景。基于“非中心元素中心化子为次极大”的有限群结构，构造高效数字签名方案。次极大中心化子的层级特性可简化签名生成与验证的计算流程，同时利用有限群的离散数学难题保证签名安全性，解决传统签名方案中“计算复杂度高、签名长度长”的问题，适用于移动终端、物联网等资源受限设备。近五年，在 Theoretical Computer Science, Information Science, Designs,Codes and Cryptography 等权威期刊上发表论文 45 篇，主持国家自然科学基金项目 7 项。

密码应用主要研究信息隐藏、版权保护、密码应用与安全性评估、密码算法的概率描述与统计分析等。其特色优势为：彩虹连接相关的图论研究，

为密码隐私保护的“数据匿名性、传输安全性”提供创新思路。利用大团数图的正常（强）彩虹连接、正常（强）彩虹顶点连接特性，设计匿名通信协议。通过对图中边/顶点的“彩虹着色”实现通信路径的隐藏，避免攻击者通过路径追踪获取通信双方身份，结合大团数图的高密度连接特性提升通信效率，适用于暗网通信、隐私社交网络等场景。基于(1,2)-彩虹连接数的研究成果，设计数据加密传输方案。(1,2)-彩虹连接的颜色使用规则可转化为数据加密的“分组密钥”，通过控制连接数的大小调节加密强度，实现“按需加密”（如低敏感数据用低强度加密提升效率，高敏感数据用高强度加密保障安全），适用于云存储、大数据传输等多场景数据保护。近五年，在信息隐藏、对称密码算法的概率统计分析技术等领域的权威期刊上发表论文32 篇，主持国家自然科学基金项目 3 项。

(二) 师资队伍

本学位点现有教学科研人员 24 人，其中教授 6 人、博士 24 人、具有国外留学访问经历者 8 人、教育部新世纪优秀人才、河南省科技创新杰出青年、河南省优秀青年科技专家 1 人、博士研究生导师 3 人。学科带头人苗雨、庞善起等教授均在各自的学术领域取得了突出的研究成果，并在国家及省级学会担任重要职务。

（三）科学研究

2025 年本学位点教师获批国家自然科学基金青年项目 1 项(睢君朕)，国家资助博士后研究人员计划 1 人（张慧），河南省自然科学基金面上项目 4 项（马迎宾、李海锋、李恒哲、杨玉星），河南省自然科学基金青年项目 2 项（杨启玉、毛永霞）。2025 年共发表 47 篇学术论文，其中 SCI 期刊 46 篇。

2025 年，举办河南师范大学密码专业硕士学位点建设论证会，其中中国科学院数学与系统科学研究院田野院士，国家教学名师、合肥工业大学朱

士信教授，国防科技大学理学院院长屈龙江教授等国内编码密码领域专家参与论证。3 月，举办“2025 年数论及其应用学术研讨会”。4 月，举办“2025 组合设计及其应用研讨会”和“魅丽数学系列会议-图的极值相关问题研讨会”。11 月，举办“2025 年新乡图论与组合数学研讨会”。

学院继续加大学术交流支持力度，鼓励老师开展积极有效的学术交流工作。2025 年学位点教师作大会报告 5 人次，分组报告 10 人次，邀请中国科学院院士田野研究员，国家教学名师、合肥工业大学朱士信教授，IEEE 信息理论法国分会主席、法国巴黎第八大学 Sihem Mesnager 教授等专家讲学 30 人次，学术交流层次逐年增高。

（四）教学科研支撑

河南师范大学数学与信息科学学院现是国家天元数学中部中心共建单位，拥有国家大学生创新性试验计划项目研究基地、河南省应用数学中心、大数据统计分析与优化控制河南省工程实验室、数学与科学计算河南省重点学科开放实验室、河南省高等学校学科创新引智基地、河南省首批中小学学科教育教学研究基地等。学院拥有数学与应用数学（国家级首批一流本科建设专业、国家级特色专业）、信息与计算科学（河南省首批一流本科建设专业、河南省特色专业）、信息管理与信息系统三个本科专业。学院拥有河南省高校目前占地面积最大、藏书最早的数学图书资料阅览室，馆藏图书 11 万余册，中外文期刊杂志 850 多种。

（五）奖助体系

按照《河南师范大学研究生奖助体系实施方案（试行）》、《河南师范大学研究生奖励管理办法（修订）》等规章制度，设立了国家奖学金、学业奖学金、国家助学金、“三助”（助管、助研、助教）岗位津贴和研究生科研项目资助、学术交流资助、研究生科研成果奖励、优秀学位论文奖励和特殊困难补助、国家助学贷款等多渠道、多途径、全覆盖的奖助体系。

表 1：奖助体系

名称	覆盖比例	奖助水平（元）
学业奖学金	设立一、二、三等奖学金 100%（40% /30% /30%）	10000/7000/5000
国家奖学金	5%	20000
国家助学金	100%	6000
“三助”岗位津贴	10%	4000
其他奖助项目	科研创新项目 10% 科研成果奖励 优秀学位论文奖励（校级 14%，省级 5%）	1000-10000 200-1000 500/1000

三、人才培养

（一）招生选拔

持续贯彻教育部有关研究生招生制度改革文件精神，落实学校有关学位与研究生教育工作精神，加大研究生教育结构调整优化力度，结合我院实际，优化 2025 年招生简章，合理设置相关专业考试科目和招生条件，进一步确保招生规模，提高生源质量。积极抓好“校内-校外”两个阵地，构建“学校-学院-学科-导师”四级招生宣传工作体系，通过学术交流充分发挥导师的学术影响力进一步吸引优质生源。学院通过中国教育在线-掌上考研宣讲平台举办线上研究生招生宣讲会，4000 余名考生参加线上宣讲会活动；学院组建了一支由学院领导，学院骨干教师和专业负责人协同参与的高水平招生宣讲团，宣讲团先后赴洛阳师范学院、安阳师范学院、河南科技学院、周口师范学院、新乡学院等多所省内院校开展一系列内容丰富的招生宣讲活动。2025 年招收博士研究生 10 人、密码专业硕士 15 人。

（二）思政教育

本学位点高度重视学生思想政治教育工作，深入贯彻党的教育方针，全面落实“立德树人”根本任务，坚持价值塑造、能力培养与知识传授有机融合，努力推动“思政课程”和“课程思政”同向同行、同频共振，切实形成

协同育人效应。确保思想政治工作贯穿于教育教学的全过程，逐步构建起具有学科特色的全员全过程全方位一体化育人新格局。

（三）课程教学

2025 年本学位点开设的核心课程及主讲教师如下：

表 2：核心课程及主讲教师

核心课程名称	主讲教师			学时	开设对象（博士、硕士）
	姓　名	专业技术职　务	所在单位		
密码中的代数学	赵先鹤	正高级	数学与统计学院（密码学院）	27	硕士
密码中的代数学	睢君朕	讲　师	数学与统计学院（密码学院）	27	硕士
实验设计	庞善起	正高级	数学与统计学院（密码学院）	72	硕士
数据科学与实践	李钧涛	正高级	数学与统计学院（密码学院）	54	硕士
密码协议与应用	董　乐	副高级	数学与统计学院（密码学院）	54	硕士
密码设计与分析	杜　蛟	副高级	数学与统计学院（密码学院）	54	硕士
群与设计	陈光周	副高级	数学与统计学院（密码学院）	72	硕士
有限域	张　涛	副高级	数学与统计学院（密码学院）	72	硕士
信息论	高　强	讲　师	数学与统计学院（密码学院）	54	硕士
密码学与置换群	张　慧	讲　师	数学与统计学院（密码学院）	72	硕士

依据本学位点培养研究生的目标定位以及授予学位的基本标准，本学位点对课程设置、教学内容、教学方法和课程评价进行了一系列改革，学生对教学的满意度得到了提高，效果十分显著。

（四）导师指导

学院要求导师要切实履行立德树人职责，积极投身教书育人，教育引导研究生坚定理想信念，要求导师严格遵守《新时代高校教师职业行为十项准

则》、研究生导师指导行为准则，不安排研究生从事与学业、科研、社会服务无关的事务。要求导师关注研究生个体成长和思想状况，与研究生思政工作和管理人员密切协作，共同促进研究生身心健康。学院每年依托新生入学教育、师生见面会、研究生学术活动月等活动，通过专家报告、经验分享、学习研讨等多种形式，构建新聘导师岗前培训、在岗导师定期培训、日常学习交流相结合的培训制度，帮助新晋导师深入理解导师的岗位职责和要求，掌握教书育人的传统和方法，了解研究生教育发展的新情况和新要求。2025年，本学位点2位教师参加河南师范大学新晋研究生导师2025年专题培训，采取线下集中培训和网络课程自学两个阶段进行；50 人次参加国内外学术会议。

（五）实践教学

本教学周期内，密码专硕实践教学紧扣行业发展趋势与企业实际需求，构建了“课程实践+集中实训+企业实习+毕业设计（论文）”四位一体的实践教学体系，覆盖密码算法实现、密码协议应用、信息安全防护、密码产品研发等核心领域，累计完成1门课程实践，实践教学总学时达36学时，学生实践参与率100%。

（六）学术交流

2025 年，本学位点研究生积极参与国内外学术交流活动，主要如下：赵于欣同学参加2025年第十八界中国密码学会年会；张涵姣等2位同学参加第九届编码密码组合研讨会；赵于欣同学参加2025年纠错码与后量子公钥密码研讨会；赵于欣同学参加布尔代数及其应用研讨会；柴清杰等 3 位同学参加第七届河南省图论组合学术研讨会；王心茹同学参加“数启天元，智算无界”2025国产科学计算软件大会暨北太天元产品发布会；刘婷等10位同学参加2025年新乡图论与组合数学研讨会；贾满等4名同学参加第十三届海峡两岸图论与组合数学会议。

（七）论文质量

本学位点高度重视学位论文的质量提高，要求学生严格按照《河南师范大学研究生学位论文格式要求》撰写学位论文。全日制研究生申请学位需要全部参加双盲评审，双盲评阅的学位论文上应去掉论文作者及导师的姓名信息，由研究生学院统一组织，博士论文聘请 5 位同行教授级专家进行“双盲”评阅，硕士论文邀请 2 位校外专家进行“双盲”评阅。申请优秀博士学位论文需公开发表一定数量的与学位论文密切相关的高水平科研成果（学位论文中的研究成果已在本学科 SCI 一区期刊上发表，学位论文中的研究成果获得授权发明专利且获得应用成果转化，学位论文中的研究成果获得国家级（限前 5 名）或省部级科技成果二等奖及以上（限前 2 名））；申请优秀硕士学位论文需参加双盲评审两份，并且需要公开发表有与学位论文相关的高水平科研成果（若科研成果为学术论文，须在中文核心期刊及以上刊物公开发表）。在河南省学位委员会学位办公室组织的硕士学位论文抽检活动中，本学位点被抽中的学位论文均获得通过。

（八）质量保证

本学位点遵循学科发展和人才培养规律，根据《一级学科博士硕士学位基本要求》，按照密码专业与本单位办学定位及特色相一致的学位授予质量标准，并制定了对应的《密码专业硕士学位研究生培养方案（2025 年制订）》，做到培养环节设计合理，学制、学分和学术要求切实可行，关键环节考核标准和分流退出措施明确。实行研究生培养全过程评价制度，关键节点突出学术规范和学术道德要求。学位论文答辩前，严格审核研究生培养各环节是否达到规定要求。

在学位评定分委员会指导下，成立学院研究生教学督导委员会，负责落实研究生培养方案、监督培养计划执行、指导课程教学、评价教学质量等工作。加快建立以教师自评为主、教学督导和研究生评教为辅的研究生教学评

价机制，对研究生教学全过程和教学效果进行监督和评价。进一步加强和严格课程考试，切实发挥资格考试、学位论文开题和中期考核等关键节点的考核筛查作用，完善考核组织流程，丰富考核方式，落实监督责任，提高考核的科学性和有效性。

（九）学风建设

学院持续加强科学道德和学风建设，健全学术不端行为预防和处置机制，加大对学术不端行为的查处力度。定期组织学生认真学习《高等学校预防与处理学术不端行为办法》、《河南师范大学研究生纪律处分管理办法（试行）》、《河南师范大学学术道德与行为规范（修订）》和《河南师范大学研究生学位论文作假行为处理实施细则》等规章制度，并按照文件要求严格执行。将科学精神、学术诚信、学术（职业）规范和伦理道德作为导师培训和研究生培养的重要内容，把论文写作指导课程作为必修课。结合学校最新博士学位授予细则和数学学科专业特点等实际情况，出台了《数学学科博士研究生学位申请科研补充条件》、《数学与信息科学学院校外兼职学术型研究生导师管理办法》等文件，为了破除科技评价中“唯论文”不良导向，回归论文“初心”，文件对预警期刊提出严格要求。2025 年本学位点未发现学术不端行为。

（十）管理服务

学院坚持实行“立德树人，以人为本”的育人方针，保障实现全方位育人，将研究生权益贯穿研究生科研、生活全过程。学院设立由研究生工作主管副院长，学生工作副书记，研究生工作秘书，学位点建设工作办公室主任为骨干，全体导师参与的研究生管理服务机构。学院成立研究生会，研究生助管团队，研究生权益管理团队。上述团队由学院党委领导，研究生权益管理团队具体负责。研究生管理团队宗旨是全心全意为研究生服务，及时反映研究生生活、学习、科研等各方面权益诉求，充分发挥好学校与广大研究生之间的桥梁纽带作用，合理有序地表达和维护研究生正当权益，助推研究生成长

成才。2025 年，学院通过问卷和座谈会等形式对本学位点研究生进行满意度调查，调查内容包括：导师、课程教学、学术研究、管理服务以及发展前景等方面，调查结果显示绝大多数研究生的评价为满意或非常满意。

（十一）就业发展

学校及学位点始终把研究生的就业工作摆在突出重要位置，不断加大工作力度，创新工作方式。通过建立用人单位信息库、开展就业市场调查、用人单位回访、毕业生跟踪调查、举办各种类型的校园专场招聘活动等，积极开拓研究生的就业渠道。此外，结合学位点的优势和特点，针对有意向深造的研究生，学位点构建了全方位的支持体系。依托硕士生导师资源，为毕业生提供博士报考方向选择、科研项目实践指导等精准帮扶；组织优秀博士生校友开展经验分享会，传递备考技巧与科研规划经验；邀请中科大、华东师大等高校的博士生导师来校讲学，解读学术前沿动态，为研究生与名校科研团队搭建沟通桥梁，提升深造竞争力。

四、服务贡献

（一）科技进步

本学位点庞善起教授团队在嵌套正交表、特别是混合嵌套正交表的构造方面取得重要突破。相关成果以 Construction of Asymmetric Nested Orthogonal Array 为题在国际旗舰期刊 Journal of the American Statistical Association（JASA）上发表。庞善起教授为第一作者，合作者为学校数学与统计学院 2021 级博士研究生林霄、北京大学艾明要教授（通讯作者）和美国 University of Wisconsin-Madison, Peter Chien 教授。河南师范大学为第一署名单位。

嵌套正交表，作为一种特殊类型的正交表，在计算机试验和统计学中有着广泛的应用。它由一对正交表组成，其中一个小的正交表嵌套在另一个大的正交表中。论文中提出了一系列通用的构造方法，成功构造出试验次数、

水平数和强度灵活的非对称嵌套正交表，使得大表和小表都能在尽可能少的试验次数下达到最大的因子数。此外，论文还引入了“完美性”这一新概念，根据嵌套正交表的大小和饱和性，将其划分为九种类型，并成功构造出其中七类新型的嵌套正交表。

该研究不仅详细列出了新生成的小规模和适中嵌套正交表，还包括优化的嵌套正交表，同时给出了相应的矩阵形式。这些成果为理论研究者和实际使用者提供了强有力的工具，不仅为其他特殊正交表的构造提供了宝贵的经验，也为正交表在统计学、密码学、编码和量子信息等领域的应用带来了更广阔的前景。

（二）经济发展

本学位点依托李钧涛老师两个横向项目，深化产学研融合，以技术创新赋能经济发展，成效显著。在数字经济领域，家居在线销售分布式爬虫技术研发项目落地实施，构建高可用分布式架构，攻克动态页面爬取与反爬难题，数据抓取效率提升，综合成本降低显著，为合作企业精准挖掘市场需求，助力家居电商数字化转型，带动相关业务营收增长。在低空经济赛道，无人机编队分布式隐私保护协作学习算法项目，融合联邦学习与密码技术，实现数据本地训练与参数加密共享，规避隐私泄露风险。成果支撑无人机在农业监测、应急响应等场景协同作业，推动低空经济安全合规发展，拓展产业应用边界。项目实践中，专硕研究生深度参与技术研发与成果转化，强化应用能力培养。两大项目累计带动合作企业经济效益提升，为学位点构建“技术研发-成果转化-人才培养”良性生态，彰显密码技术服务实体经济的核心价值。

（三）文化建设

本位点紧扣“筑牢密码信仰、培育专业素养”核心，以精神引领、实践赋能、氛围营造为抓手，构建兼具专业性与育人温度的文化体系，助力人才全面发展。深化思想引领，厚植密码情怀。通过开展“行业专家思政讲堂”

等活动，邀请领域专家解读密码技术在国家信息安全中的战略意义，覆盖师生 30 余人次，引导学生树立“密码为民、护网有责”的使命担当。丰富文化载体，锤炼专业本领。参加密码算法竞赛等专业活动，搭建“以赛促学、以练促能”平台，激发学生创新活力；组织密码文化研习活动，开展经典文献共读、技术案例研讨，形成浓厚学术氛围。强化师风学风，凝聚育人合力。推行“导师领航+朋辈互助”机制，导师全程参与学生成长指导，培育严谨务实的科研作风；开展学风建设月活动，通过优秀学子分享会、学术诚信宣讲，筑牢学术道德底线。本年度，学位点文化建设成效显著，学生专业认同感与团队协作能力显著提升，为培养德才兼备的密码领域应用型人才筑牢文化根基。