网络空间安全

Cyberspace Security

（专业代码： 0839 ）

本培养方案依据《中国科学技术大学研究生培养方案总则（2019 版）》以及《中国科学技术大学研究生院关于开展科学学位研究生培养方案修订（制定）工作的通知》修订。

一、培养目标

本学科旨在培养德、智、体、美、劳全面发展，具有坚实系统的网络空间安全理论基础和专门知识、富有创新精神、能够适应我国经济、科技、教育发展需要的高水平人才。基本要求为：

（一）认真学习和掌握马克思列宁主义、毛泽东思想、邓小平理论、“三个代表”重要思想、科学发展观与习近平新时代中国特色社会主义思想的基本理论，具有坚定正确的政治方向；热爱祖国，遵纪守法，品行端正，学风严谨，身心健康；具有较强的事业心和奉献精神，积极为社会主义现代化建设服务；

（二）攻读硕士学位的研究生应掌握本学科坚实的基础理论和系统的专业知识，较为熟练地掌握一门外国语，具有从事科学研究工作或较强的实际工作能力；

（三）攻读博士学位的研究生应掌握本学科坚实宽广的基础理论和系统深入的专业知识，掌握科学研究的基本技能和方法，了解所从事研究方向的国内外发展动态，具有独立从事科学研究和独立担负专门技术工作的能力，在科学或专门技术上能做出创造性的成果。博士生应至少掌握一门外国语， 第一外语为其他语种者，必修英语。

二、主要研究方向

1. 密码学及应用：密码学、密码工程

2. 网络安全：区块链、网络安全协议、无线安全

3. 系统安全：软件安全、硬件安全

4. 数据安全：信息隐藏、多媒体安全、隐私计算

5. 应用安全：人工智能安全、社交网络内容安全、计算社会学、多模态感知安全

6. 量子信息安全

三、课程类型和学分要求

1. 硕士培养模式。通过硕士研究生招生统考或免试推荐等形式，取得我校硕士研究生资格者。研究生在申请硕士学位时，取得的总学分不低于 35 学分。其中公共必修课 7 学分，硕士学科基础课不少于 6 学分，硕士专业基础课不少于 6 学分，素质类课程不超过 3 学分，开题报告 2 学分。

2. 硕博一体化培养模式。本专业和相关专业在读硕士研究生完成硕士阶段基本学习任务，通过博士生资格考核，可以取得博士生资格。研究生在申请博士学位时，取得的总学分不低于 45 学分。其中公共必修课 11 学分，硕士学科基础课不少于 6 学分，硕士专业基础课不少于 6 学分，博士专业课不少于 4 学分，素质类课程不超过 3 学分，博士论文开题报告 2 学分。

3. 普通博士生培养模式。已取得硕士学位，通过我校博士生资格考核者。研究生在申请博士学位时，取得的总学分不低于 12 学分。其中公共必修课 4 学分，博士专业课不少于 4 学分，素质类课程不超过 3 学分，开题报告 2 学分。

四、研究生培养过程要求

1. 博士资格考试：研究生进入博士阶段之前须通过本学科统一组织的博士资格考试，时间安排在统考生的博士入学考试之后，与统考生复试合并进行。统考生未通过博士资格考试者视同复试未通过，不能录取；硕转博的研究生未通过博士资格考试者可以申请下一年度再次参加博士资格考试，再次不通过者，不能申请转为博士生。

2. 开题报告：

博士学位论文的开题报告及评审过程是博士研究生培养的必要环节。开题报告的时间由博士生导师根据博士生工作进度情况确定，一般应在博士培养阶段的第三或第四学期内完成（硕博连读研究生最早可在博士阶段第二学期内进行）；开题报告由博士生所在一级学科组织；博士学位论文开题报告评审小组由本学科及相关学科的专家组成，人数不少于 5 人（其中具有正高级职称的博士生导师不少于 3 人）；达到或超过三分之二的评审专家同意通过的方可通过；开题报告不通过的博士研究生可以申请在下一学期重新开题。

硕士学位论文的开题报告及评审过程是硕士研究生培养的必要环节。开题报告的时间由硕士生导师根据硕士生工作进度情况确定，一般应在硕士培养阶段的第三或第四学期内完成；开题报告由硕士生所在一级学科组织；硕士学位论文开题报告评审小组由本学科及相关学科的专家组成，人数不少于 3 人（其中具有副高级以上职称的硕士生导师不少于 3 人）；达到或超过三分之二的评审专家同意通过的方可通过；开题报告不通过的硕士研究生可以申请在下一学期重新开题。

3. 中期检查：博士/硕士学位论文的中期检查报告及评审过程是博士/硕士研究生培养的必要环节。中期检查最早在研究生通过开题报告之后的下一学期内进行；中期检查报告及评审由研究生所在一级学科组织；中期检查报告评审小组的组成及通过办法同开题报告；中期检查不通过的研究生可以申请在下一学期再次进行

中期检查。

4. 毕业答辩：博士/硕士学位论文的毕业答辩应在研究生通过中期检查之后进行；具体要求参见研究生院的相关规定。

5. 国际学术交流：博士生在学期间须参加一次国际学术会议并交流学术论文，或短期出境访学一次。国际学术会议和短期出境访学后，博士生应及时向所在系教学办公室提交有关证明材料。

6. 学术报告：博士生/硕士生在学期间必须听取不少于 15 场次的学术报告会，并得到报告会组织单位的认定。博士生在读博阶段必须在学院组织的学术报告会中做一次公开学术报告。

7. 学术论文：研究生申请博士/硕士学位的成果要求参见《研究生手册》中关于信息与智能学部研究生学位申请要求。网络空间安全学院的学生发表学术论文，第一署名单位必须是我校网络空间安全学院，论文内容必须与学位论文研究内容相关。

五、选课要求和课程设置列表

1. 公共必修课和素质类课程列表由学校统一设置和要求。

2. 超出学分要求的基础课，学生可以申请调整为专业选修课。

3. 研究生中途由其他专业转入本专业的，应按照本专业课程要求补修课程，已修课程符合本专业要求的，经本专业相应课程任课老师认定，可以计入学位课程学分。

4. 研究生选修本专业培养方案以外的研究生课程，经导师签字同意，可以算作本专业的专业选修课（本专业的专业选修课至少选修 4 学分）。

5. 研究生补修本专业培养方案以外的本科生课程，所获学分不计入学位课程学分。

6. 经导师签字同意，研究生可以通过修读本培养方案之外的已被本学科点认定的研究生课程，来替代本培养方案中的相应课程。替代课程与被替代课程内容相似、学分不低于被替代课程。

7. 本专业课程设置列表如下：“▲”可作为博士专业课

硕士学科基础课：

CYSC6001P 代数数论与应用（4）　　CYSC6002P 随机过程与概率统计（4）

CYSC6003P 网络空间安全数学建模（3）　　CYSC6004P 高级信号处理（3）

INFO6101P 矩阵分析与应用（3）　　CONT6105P 最优化理论（3）

PHYS5253P 量子信息技术（3）

硕士专业基础课：

CYSC6201P 现代密码学(3)　　CYSC6203P 高级计算机网络与安全(3)

CYSC6202P 通信网络的安全理论与技术（3）CYSC6204P 机器学习与应用（3）

PHYS5251P 量子信息导论（3）

硕士专业选修课：

CYSC6401P 密码分析学（2）　　CYSC6406P 云计算与区块链（2.5）

CYSC6403P 先进无线感知与安全(2)▲　CYSC6404P 人工智能安全（2）▲

CYSC6405P 信息隐藏（2）▲　　CYSC6408P 计算机网络攻防（3）▲

CYSC6407P 数据安全与隐私保护（2）▲　CYSC6409P 硬件安全（2）▲

CYSC6410P 软件安全（2）▲　　CYSC6411P 多模态内容安全（3）▲

CYSC6412P 自然语言处理与应用（3）▲　CYSC6413P 机器博弈（3）▲

PHYS7652P 高等量子光学（4）▲

博士专业课：

CONT7101P 信息科学的数学理论（2）　　MSAE5003P 博弈论（3）

COMP7204P 机器学习与数据挖掘前沿（3）

CYSC7401P 网络空间安全专题（2）（必修）

注：本培养方案自 2023 年入学的研究生开始执行。