

# 信息安全专业硕博连续培养研究生培养方案

(专业代码: 070120)

## 一 培养目标

本专业培养的博士生应为面向世界、面向未来、服务于信息社会，德智体全面发展的，能从事计算机网络、网络安全、其它形式信息安全技术的教学、科研、关键技术开发的高层次创造性的信息安全专业人才。具体要求如下：

1、掌握马列主义、毛泽东思想和邓小平理论，坚持四项基本原则，具有良好的道德品质，遵纪守法，团结协作，学风严谨，有强烈的事业心和献身精神。

2、掌握本专业坚实广博的基础理论、独特的理论体系及系统深入的专业知识，能够独立地、创造性地从事科学研究、教学工作或担任信息安全技术工作，而且具有主持较大型科研、技术开发项目、或解决和探索我国经济、社会发展问题的能力，尤其是解决和探索与我国信息化社会密切相关的信息安全问题及相关技术。全面了解本学科领域的发展动向，并在科学或专业技术上做出创造性成果。

3、至少掌握一门外国语，并能运用该门外国语熟练地阅读本专业的英文资料，并具有一定的写作能力和国际学术交流能力。第二外国语为选修，要求有阅读本专业英文资料的初步能力，第一外国语非英语的硕博连续培养研究生，第二外国语必须选修，且语种必须为英语。

4、具有健康的体魄和良好的心理素质。

## 二 研究方向

- 1、对称密码的分析技术与设计技术
- 2、Hash 函数的分析与设计
- 3、群签名与电子钱币
- 4、密码协议的分析与设计
- 5、计算数论与密码学
- 6、计算机网络攻击与防御

## 三 学习年限

硕博连续培养研究生的学习年限一般为 5~7 年，基本学习年限掌握在 5 年。

## 四 应修总学分数

应修总学分：40 学分，其中必修 34 学分，选修 6 学分。

## 五 课程设置（具体见课程设置一览表）

### 1 必修课

马克思主义理论课 3 学分（硕士阶段）

马克思主义理论课 2 学分（博士阶段）

第一外国语 4 学分、专业外语 1 学分。

### 学位基础课、学位专业课

#### 硕士阶段:

- |            |      |          |
|------------|------|----------|
| 1. 学位基础课   | 2 门  | 7 学分     |
| 近世代数       | 3 学分 |          |
| 算法数论       | 4 学分 |          |
| 2. 学位专业课   | 2 门  | 10 学分    |
| 密码算法的分析与设计 | 4 学分 |          |
| 网络攻击与防御    | 3 学分 |          |
| 3、专业选修课    | 3 门  | 不少于 6 学分 |

#### 博士阶段:

- |          |       |          |
|----------|-------|----------|
| 1、学位专业课  | 1 门   | 3 学分     |
| 数论代数安全计算 | 3 学分  |          |
| 2、专业选修课  | 2 门   | 不少于 6 学分 |
| 前沿讲座     | 6 学分。 | （具体要求）   |

#### 3 补修课 数论与代数结构

（未学过该课程的跨学科或同等学历的硕博连读生硕士阶段的必修课）

具体的课程设置请参阅后附本专业教学计划表。

前沿讲座 6 学分

#### ①讲座的目的和内容

前沿讲座旨在使硕博连读研究生了解本学科和本研究方向的重要学术问题、前沿性问题及这些问题的最新研究方法、技术及进展状况，提高学生参与学术研究的兴趣和学术交流能力。前沿讲座的内容主要包括国内外研究动态、国内外一些重大文献讲座、本领域中的新方法与新思路介绍等。

#### ②前沿讲座的形式

一是硕博连读研究生本人做专题综述（讨论班），二是听取国内外本学科或相关学科做出杰出成绩的专家作系列报告等。可以有讲授、讨论和对话等多种形式。力求生动、活泼。

#### ③前沿讲座的次数

前沿讲座贯穿硕博连读研究生培养的全过程。

硕博连读研究生听取专家前沿系列报告不少于 60 学时。从二年级开始，硕博连读研究生每学期必须参加专业相关的学术讲座、学术报告和讨论班，提交书面专题综述报告

或在讨论班做的学术报告。参加讨论班本人主讲不少于6次，主讲者要写出讲稿，讲稿内容要充实，并有个人见解，能够反映所研究领域最新学术进展情况。

#### ④ 前沿讲座的考核要求和方式

个人主讲或书面前沿专题报告的考核由参加讲座的老师和指导教师共同进行，评定成绩，并写出评语，考核成绩按优、良、中、及格、不及格五级计分；听取学科或相关专业的的前沿报告的考核，要自存个人下载的前沿讲座听课记录表，每次听专家讲学或听学院组织的学术报告时，请专家或学院的组织者签字，以备毕业时存入个人学籍档案。硕博连读研究生满60学时的听专家讲座记录，个人主讲6次或书面报告6篇，考核成绩及格以上者记6学分。

### 六 中期考核

硕博连续培养研究生在修满规定的学分后，于第三学期末由资格考试领导小组组织进行资格考试。

1、考试内容:包括政治思想、外国语和学科综合水平考试三个方面。

政治思想方面的考核主要包括对研究生平时的政治思想表现、道德品质、遵纪守法等方面作出实事求是的评价，并写出评语。

学科综合水平考试包括基础理论知识、分析问题和解决问题的能力、科研能力和创新能力等。

2、考试方式和成绩评定:考试方式可以是口试，也可以是口试、笔试兼用，具体采用那种形式，由资格考试小组提出意见，院、部资格考试领导小组同意后实施。

考试按百分制评定成绩并写出评语和转博意见。

3、通过资格考试者进入博士生学习阶段，从第五学期开始享受博士生待遇。进入博士生学习阶段后，应在半年内修完博士生期间应修学分(前沿讲座除外)。未参加资格考试或资格考试未通过者，仍按硕士生进行培养。

### 七 学位论文

博士生的学位论文应当是一篇完整的、系统的学术论文，应能表明作者具有独立从事科学研究工作的能力，并在科学或专门技术上做出创造性成果。博士生的学位论文应在导师的指导下，由博士生独立完成。

硕博连续培养研究生一般至少用3年的时间完成学位论文。

#### 1、开题报告

硕博连续培养的研究生应在导师的指导下，于进入博士阶段前完成学位论文的选题工作，研究课题应具备科学性、创新性和可行性，并强调与国家自然科学基金、博士点基金、省部级以上重点项目、重点学科科研项目等研究项目相结合。

硕博连续培养的研究生应于进入博士阶段的第一学期进行的中期考核时提交论文撰写计划，并向指导小组做开题报告，经过讨论认为选题合适，计划切实可行方能开展论文撰写工作。

## 2、论文中期进展报告

硕博连续博士生根据学位论文的实际情况确定论文的进度，以研讨班的形式向指导教师和指导小组成员系统报告论文进展情况，由指导教师和指导小组成员帮助博士生分析论文工作进展中的难点，及时给予指导，促进论文研究工作的顺利进展。

## 3、论文学术水平、创造性等要求

博士学位论文应该是具有一定创新性的研究成果。具体要求参考“博士学位论文创新成果要求”。

## 4、论文预答辩

硕博连续培养的研究生在申请学位论文答辩前 3-5 个月向本专业或相关专业有关教师、导师、论文指导小组成员全面报告学位论文进展情况及取得的成果，广泛征求意见，以便进一步修改和完善学位论文。指导教师和指导小组在考核博士学位论文满足“博士学位论文创新成果要求”的前提下，组织 3-5 位专业教师组织进行博士论文的预答辩。

## 5、严格执行各项规章制度，保证学位授予质量

博士学位论文完成后，导师、指导小组及院、部(所)学位评定分委员会主席和主管院长、主任，按照《山东大学授予博士、硕士学位工作细则》认真组织做好学位论文的审阅和答辩的各项工作，保证学位授予质量。

## 6、论文发表要求：

在学期间，本专业硕博连读研究生须有 SCI 收录刊物上公开发表（出版、出版清样或国外 SCI 刊物的录用通知）的学术论文，如果仅有一篇在 EI、CSSCI 或 ISTP 收录期刊上发表的文章，则需另有一篇核心期刊（不包括增刊）的文章。所取得的科研成果均要求研究生为第一作者（单位为山东大学数学与系统科学学院）。在学期间所有发表文章原则上以公开出版或出版清样为准。

## 八 实践环节

硕士研究生期间，学院将提供教学实践、科研实践和社会实践的岗位供研究生选

择和锻炼，参加实践的学时不能少于 32 个。各岗位负责人要对实践者写出考核评语，合格者记入研究生学籍档案。

1 教学实践 与山东大学数学与系统科学学院信息安全专业的课程、习题、试验课程的安排，适当安排研究生的教学实践。

2 根据研究生所作研究论文的研究方向，一般围绕信息安全专业所承担的国家自然科学基金等重要研究项目，鼓励自己选择研究课题的原则。相关的科研实践在山东大学信息安全专业实验室或者在省科学院的山东省计算机网络实验室完成。

3 社会实践的实验主要围绕 IT 业公司的信息安全技术与产品开发工作。

#### 附：需阅读的主要经典著作和专业学术期刊目录

##### （一）专业学术期刊

中国科学	科学通报
计算机学报	软件学报
通信学报	通信技术
密码学进展-CHINACRTPT	电子学报

Journal of Cryptology

Advances in Cryptology\_EUROCRYPT

Advances in Cryptology\_CRYPT0

Advances in Cryptology\_AUSCRYPT

Advances in Cryptologu-ASIACRYPT

Public Key Cryptography (PKC)

Workshop on Selected Area in Cryptgraphy(SAC)

IEEE Transactions on Information Theory

IEEE Symposium on Foundations of Computer Science

ACM Conference on Computer and Communications Security

ACM Symposium on Theory of Computing

Communications of ACM

SIAM Journal on Computing

另外全国性学术会刊、教育部直属院校学报及其它相关学科的一级学术刊物，皆在此范围内。

(二) 主要经典著作

1 B. Schneier, Applied Cryptography.

2 A. J.Menezes, Handbook of Applied Cryptography.

3 PKI: A Wiley Tech Brief, John Wiley&Sons, 2000。

附 信息安全专业硕博连读培养研究生教学计划表

类别	序号	课程编号	课程名称	开课学期	总学时数	学分	授课教师	考核方式	
必修课	学位公共科	1	MP09001	科学社会主义的理论与实践	1	30	1	马列教学部	考试
		2	DP09001	现代科学技术革命与马克思主义	5	54	2	马列教学部	考试
		3	MP91001	第一外国语	1-2	216	4	外国语学院	考试
		4	C019002	专业外语			1	信息安全所	考试
	学位基础课	5	M019003	近世代数	1or2	48	3	数学与系统科学学院	考试
		6	C019107	算法数论	1or2	64	4	展涛、王明强	考试
	学位专业课	7	C019103	密码算法的分析与设计	1	64	4	王小云	考试
		8	C019112	网络攻击与防御	2	64	4	王美琴	考试
		9	D019051	数论代数安全计算	5	48	3	展涛 王明强	考试
		10	C019001	前沿讲座	2-10		6		考查
选修课	1	C019097	分组密码分析与设计	4	48	3	王小云	考试	
	2	C019113	公钥密码学	3	48	3	秦静	考试	
	3	C019100	椭圆曲线与密码学	5	48	3	刘建亚, 王小云	考试	
	4	C019105	PKI 公钥理论与关键技术	3	32	2	王明强	考试	
	5	C019106	密码实现技术	3	32	2	孙秋梅	考试	
	6	C019115	防火墙原理与配置	3	32	2	王美琴	考查	
	7	C019116	电子商务	4	48	3	秦静	考查	
	8	Mp91022	第二外国语	3	72	2	外语学院	考试	
	9	C019108	布尔函数与流密码	4	48	3	王小云	考试	
	10	C019101	Hash 函数的分析与设计	4	32	2	王小云	考试	
	11	C019098	群签名与电子钱币	5	48	3	王小云	考试	
	12	D019027	漏洞扫描技术与入侵检测技术	5	48	3	王美琴	考试	
	13	M019035	椭圆曲线基础	2	48	3	王明强	考试	
	14	C019104	密码协议	2	48	3	王明强	考试	

	15	M019108	新一代网络安全计算	3	32	2	王美琴	考试
	16	D019052	计算机网络安全	4	48	3	王美琴	考试
	17	D019054	密码系统的安全证明模式	4	48	3	王明强	考试
	18	D019053	信息安全产品开发技术	5	32	2	王美琴	考试
补修课	1	C019109	数论与代数结构	1	64		王明强	考试