密码专业硕士学位研究生培养方案（2025年制订）

专业代码：1452

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、学习年限

基本学习年限为3年，最长学习年限可在基本学习年限基础上延长3年(含休学)。

三、培养方式

采用课程学习、专业实践和学位论文相结合的培养方式，在导师的指导下注重理论与实践并重，确保课程学习、专业实践和学位论文在培养中的同等重要性，共同支撑密码专业硕士学位研究生今后职业发展潜力的提升。

1. **课程学习**：课程设置注重基础理论、实际应用和前沿知识的结合，突出专业实践类课程和工程实践类课程。课程学习须按照培养计划严格执行，其中公共基础课程、专业基础课程、专业必修课程和选修课程主要在培养单位集中学习，校企联合课程、

案例课程以及职业素养课程可在培养单位或企业开展。

2. **专业实践**：专业实践是密码专业硕士学位研究生培养的重要环节。鼓励研究生到企业实习，通过集中与分段相结合的方式，完成密码技术方案设计、项目开发与管理等工作。积极开展校企联合培养，调动企业积极性，共建联合培养基地，推动产教融合、协同育人，提高校企联合培养质量。

3. **学位论文**：学位论文研究工作应紧密结合密码领域的工程实际或具有明确的工程应用背景，体现研究生综合运用所学知识解决实际问题的能力。学位论文研究工作一般应与专业实践相结合，时间不少于 1 年。

4. **导师指导**：建立以工程能力培养为导向的导师组指导制。导师组由培养单位具有较高学术水平和丰富指导经验的教师，以及企业具有丰富工程实践经验的专家组成。鼓励导师引进各种优质教育资源，支持与国内外一流科研院所、一流大学建立联合培养模式，开展协同育人，提升研究生的国际化视野和竞争力。

四、课程设置与学分要求

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，详细情况请参照附件 1 和附件 2。

五、实践教学的实施

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。

六、中期考核

1. **考核内容**：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。

（1）政治思想品德、学习态度评定：研究生要认真做思想小结，并认真填写中期考核表的自我总结。

（2）对课程成绩、完成学分情况进行审核。

（3）学位论文开题报告审核：中期考核前，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。

2. **中期考核时间**：一般安排在第四学期的5-6月份进行。

3. **考核程序**：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。

七、学位论文及学位授予

论文选题应直接来源于密码应用课题、密码技术实际问题或具有明确的密码技术背景，其研究成果应具有实际或潜在的应用价值。选题应紧密结合密码领域的技术需求，体现对实际问题的解决能力，同时具有一定的技术难度和工作量，能够体现综合运用密码学理论、方法和技术手段解决工程技术问题的能力。

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，语意通达，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》。

论文评审与答辩

1. 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。

2. 攻读密码专业学位硕士研究生完成培养方案中规定的所有环节，获得培养方案规定的学分，成绩合格，方可申请论文答辩。

3. 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。

学位授予

修满规定学分，并通过论文答辩者，经学校学位评定委员会审核，授予工程硕士专业学位，同时获得硕士研究生毕业证书。学位授予遵照《河南师范大学授予硕士学位工作细则》及学院的有关规定。

指导教师和学院学位评定分委员会要在答辩前对相关材料认真审核，主要材料包括：（1）成绩单；（2）开题审核表；（3）中期考核表；（4）参加学术讲座活动情况；（5）参加专业实践环节情况；（6）申请硕士学位的相关科研成果。其中，科研成果包括发表论文、科研项目参与证明、技术报告、软件著作权、专利、经评定的其他科研成果等，内容须符合研究生的专业方向，以河南师范大学数学与统计学院为第一署名单位，学位申请者为独著、第一作者或除导师以外第一作者。特殊情况下，经导师同意并经学院学位评定分委员会认定达到毕业水平者，可以不要求有相关科研成果。

附件：

附件 1：密码专业硕士学位研究生培养方案课程设置表

附件 2：密码专业硕士学位研究生培养方案主要课程内容

附件 1

密码专业硕士学位研究生培养方案课程设置表

课程类别	课程编号	课程名称	总学时	学分	开课学期	考核方式	备注
公共必修课	09_002011	英语	72	4	第一学期	考试	11学分
	24_000002	新时代中国特色社会主义理论与实践(专硕)	36	2	第一学期	考试	
	21_000001	科研伦理与学术规范（线上课程）	32	1	第一学期	考试	
	21_000003	马克思主义经典著作研读（线上课程）	14	1	第一学期	考试	
	22_000004	研究生素养课——积极心理与情绪智慧	13	1	第一学期	考试	
	21_010001	科技论文写作与文献检索	36	2	第二学期	考试	
专业基础课	25_01145201	信息论	54	3	第一学期	考试	8学分
	25_01145202	密码中的代数学	54	3	第一学期	考试	
	25_01145203	概率统计与优化	36	2	第二学期	考试	
专业必修课	25_01145204	密码设计与分析	54	3	第一学期	考试	12学分
	25_01145205	密码协议与应用	54	3	第二学期	考试	
	25_01145206	C++高级程序设计	36	2	第二学期	考试	
	25_01145207	密码管理与测评	36	2	第三学期	考试	
	25_01145208	网络安全	36	2	第三学期	考试	
专业选修课	25_01145209	正交表	36	2	第三学期	考查	至少选修4学分
	25_01145210	代数编码	36	2	第三学期	考查	
	25_01145211	代数数论	36	2	第三学期	考查	
	25_01145212	密码前沿选讲	36	2	第三学期	考查	
	25_01145213	后量子密码学	36	2	第三学期	考查	
	25_01145214	区块链技术与应用	36	2	第三学期	考查	
	25_01145215	同态加密技术与应用	36	2	第三学期	考查	
	25_01145216	序列设计	36	2	第三学期	考查	
	25_01145217	人工智能安全	36	2	第三学期	考查	
	25_01145218	云计算及云安全	36	2	第三学期	考查	
	25_01145219	物联网安全	36	2	第三学期	考查	

	25_01145220	嵌入式系统与硬件安全	36	2	第三学期	考查	
公共选修课	22_000005	走近中华优秀传统文化	16	1	第二学期	考查	
专业实践环节		校外实践	108	6	第四学期	实践	6学分

附件 2　密码专业硕士学位研究生培养方案主要课程内容简介

课程编号：25_01145201　　**课程名称：**信息论

总 课 时：54　　**学　　分：**3

开课单位：数学与统计学院　　**开课学期：**第一学期

教学目的：信息论是密码学和通信领域的重要基础课程，通过本课程的学习，使研究生掌握信息论的基本理论与方法，包括信息熵、信道容量和数据压缩等核心概念，培养学生运用信息论分析密码系统安全性和随机性的能力，为后续专业课程奠定理论基础。

教学内容：信息熵与互信息，数据压缩与香农第一定理，信道模型与信道容量，香农第二定理，差错控制编码基础，信息论在密码学中的应用（如随机数生成与安全性证明）。

教材及主要参考书目：

[1] Thomas M. Cover, Joy A. Thomas, Elements of Information Theory (Second Edition), Wiley, 2006.

[2] David J.C. MacKay, Information Theory, Inference, and Learning Algorithms, Cambridge University Press, 2003.

课程编号：25_01145202　　**课程名称：**密码中的代数学

总 课 时：54　　**学　　分：**3

开课单位：数学与统计学院　　**开课学期：**第一学期

教学目的：代数学是密码学数学基础的核心课程。通过本课程的学习，使研究生掌握群、环、域等代数结构的基本理论及其在密码算法设计中的应用，培养抽象思维和数学建模能力，为密码学中的公钥加密和编码理论提供支持。

教学内容：群论基础（置换群、循环群），环与理想，有限域，线性代数的矩阵理论，多项式环与因子分解，代数学在 RSA 和椭圆曲线密码中的应用。

教材及主要参考书目：

[1] David S. Dummit, Richard M. Foote, Abstract Algebra (3rd Edition), Wiley, 2003.

[2] 林东岱, 代数学基础与有限域（第二版）, 北京: 高等教育出版社, 2022.

课程编号：25_01145203　　**课程名称：**概率统计与优化

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第二学期

教学目的：本课程旨在使研究生掌握概率统计与优化技术的基本原理，培养学生运用概率模型分析密码系统安全性和优化算法的能力，为密码协议设计和网络安全分析提供量化工具。

教学内容：随机变量与概率分布，期望与方差，大数定律与中心极限定理，假设检验与贝叶斯方法，线性规划与非线性优化，优化技术在密码学中的应用（如密钥生成优化）。

教材及主要参考书目：

[1] Morris H. DeGroot, Mark J. Schervish, Probability and Statistics (4th Edition), Pearson, 2011.

[2] 茆诗松, 王静龙, 濮晓龙, 高等数理统计（第三版）, 北京: 高等教育出版社, 2022.

课程编号：25_01145204　　**课程名称：**密码设计与分析

总 课 时：54　　**学　　分：**3

开课单位：数学与统计学院　　**开课学期：**第一学期

教学目的：本课程旨在使研究生掌握对称与非对称密码系统的设计原理与分析技术，培养学生设计安全算法和分析攻击方法的能力，为密码学核心技术的学习和研究奠定基础。

教学内容：分组密码与流密码设计，哈希函数构造，公钥密码原理，差分分析与线性分析，侧信道攻击与防御，密码算法安全性评估等。

教材及主要参考书目：

[1] Douglas R. Stinson, Cryptography: Theory and Practice (4th Edition), CRC Press, 2018.

[2] 吴文玲, 冯登国, 张文涛, 分组密码的设计与分析, 北京: 清华大学出版社, 2009.

课程编号：25_01145205　　**课程名称：**密码协议与应用

总 课 时：54　　**学　　分：**3

开课单位：数学与统计学院　　**开课学期：**第二学期

教学目的：本课程旨在使研究生理解密码协议的设计与实现原理，掌握协议安全性分析方法，培养将密码技术应用于实际系统的能力，为网络安全和数据保护提供实践基础。

教学内容：密钥交换协议，数字签名与认证协议，零知识证明，协议形式化分析，密码协议在 SSL/TLS 中的应用，案例分析与实现。

教材及主要参考书目：

[1] Oded Goldreich, Foundations of Cryptography: Volume 2, Basic Applications, Cambridge University Press, 2004.

[2] Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Wiley-India, 2007.

课程编号：25_01145206　　**课程名称：**C++高级程序设计

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第二学期

教学目的：本课程旨在使研究生掌握 C++高级编程技术，培养开发高效、安全的密码算法实现的能力，为密码学软件开发和系统设计提供技术支持。

教学内容：面向对象编程，模板与 STL，多线程编程，异常处理，C++在密码算法实现中的优化技术，项目实践（如 AES 实现）。

教材及主要参考书目：

[1] Stanley B. Lippman, Josée Lajoie, Barbara E. Moo, C++ Primer (5th Edition), Addison-Wesley, 2013.

[2] Bjarne Stroustrup, The C++ Programming Language (4th Edition), Addison-Wesley, 2013.

课程编号：25_01145207　　**课程名称：**密码管理与测评

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第三学期

教学目的：本课程旨在使研究生掌握密码系统的管理与测评技术，培养设计密钥管理方案和评估密码系统安全性的能力，为实际应用中的合规性与可靠性提供保障。

教学内容：密钥管理与分发，密码产品认证标准，安全性测评方法，漏洞分析与修复，密码管理案例分析，国家密码管理规范。

教材及主要参考书目：

[1] Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, Cryptography Engineering: Design Principles and Practical Applications, Wiley, 2010.

[2] 中国密码学会密评联委会, 商用密码应用安全性评估测评实施指引, 2024.

课程编号：25_01145208　　**课程名称：**网络安全

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第三学期

教学目的：本课程旨在使研究生理解网络安全的基本原理与技术，掌握结合密码技术保护网络系统的方法，培养分析和应对网络威胁的能力。

教学内容：网络安全威胁与防御，防火墙与入侵检测，VPN 与 IPSec，DDoS 攻击与防御，网络协议安全分析，密码技术在网络安全中的应用。

教材及主要参考书目：

[1] 刘建伟, 王育民, 网络安全—技术与实践（第三版）, 北京: 清华大学出版社, 2017.

[2] William Stallings, Network Security Essentials : Applications and Standards, (6th Edition), Pearson, 2016.

课程编号：25_01145209　　**课程名称：**正交表

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第三学期

教学目的：本课程旨在使研究生掌握正交表的数学理论及其在密码学中的应用，培养设计高效 S 盒和分析密码算法的能力，为密码设计提供数学工具。

教学内容：正交表的构造与性质，组合设计基础，正交表在实验设计中的应用，S 盒设计与差分分析，正交表在密码学中的案例分析。

教材及主要参考书目：

[1] A.S. Hedayat, N.J.A. Sloane, John Stufken, Orthogonal Arrays: Theory and Applications, Springer, 1999.

[2] 方开泰, 马长兴, 正交与均匀试验设计, 北京: 科学出版社, 2001.

课程编号：25_01145210　　**课程名称：**代数编码

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第三学期

教学目的：本课程旨在使研究生掌握代数编码的基本理论与方法，培养设计纠错码和分析编码安全性的能力，为数据传输和密码学应用提供支持。

教学内容：线性码与生成矩阵，循环码与BCH码，Reed-Solomon码，编码与解码算法，代数编码在密码学中的应用（如McEliece加密）。

教材及主要参考书目：

[1] Lekh R. Vermani, Elements of Algebraic Coding Theory, New York, Pearson, 1996.

[2] 万哲先, 代数和编码（第三版）, 北京: 高等教育出版社, 2007.

课程编号：25_01145211　　**课程名称：**代数数论

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第三学期

教学目的：本课程旨在使研究生掌握数论基本理论及其在密码学中的应用，培养分析和设计公钥加密算法的能力，为密码学研究提供数学基础。

教学内容：素数与同余，欧几里得算法，中国剩余定理，二次剩余，数论在RSA和椭圆曲线密码中的应用，初等数论案例分析。

教材及主要参考书目：

[1] 冯克勤,代数数论, 北京：科学出版社, 2000.

[2] 潘承洞, 潘承彪, 初等数论（第三版）, 北京: 北京大学出版社, 2013.

课程编号：25_01145212　　**课程名称：**密码前沿选讲

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第三学期

教学目的：本课程旨在使研究生了解密码学的前沿研究动态，培养跟踪学术进展和解决实际问题的能力，为深入研究和创新奠定基础。

教学内容：量子密码学，多方安全计算，零知识证明，密码学最新研究论文分析，前沿技术应用案例（如隐私计算）。

教材及主要参考书目：

[1] Crypto, Eurocrypt, Asiacrypt, SSENIX Security, S&P, CCS, NDSS 等相关论文集.

课程编号：25_01145213　　**课程名称：**后量子密码学

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第三学期

教学目的：本课程旨在使研究生掌握抗量子计算的密码技术，培养设计和分析后量子密码算法的能力，为未来密码学发展提供支持。

教学内容：量子计算威胁，格密码，基于编码的密码，签名方案，后量子密码标准化进展，算法实现与分析。

教材及主要参考书目：

[1] Daniel J. Bernstein，Johannes Buchmann，Erik Dahmen , Post-Quantum Cryptography, Heidelberg, Springer, 2009.

课程编号：25_01145214　　**课程名称：**区块链技术与应用

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第三学期

教学目的：本课程旨在使研究生掌握区块链技术的核心原理与应用，培养设计分布式系统和分析安全性的能力，为数字经济和安全领域提供技术支持。

教学内容：分布式账本技术，共识机制，智能合约，区块链安全与攻击分析，应用案例（如比特币、以太坊）。

教材及主要参考书目：

[1] 华为区块链技术开发团队, 区块链技术及应用（第二版）, 北京: 清华大学出版社, 2021.

[2] 王瑞锦, 区块链技术与应用, 北京: 中国工信出版集团, 人民邮电出版社, 2022.

课程编号：25_01145215　　**课程名称：**同态加密技术与应用

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第三学期

教学目的：本课程旨在使研究生掌握同态加密的理论与实现技术，培养设计隐私保护计算方案的能力，为云计算和数据安全提供创新工具。

教学内容：同态加密基础，部分同态与全同态加密，基于格的同态加密，应用场景（如隐私数据分析），性能优化与实现。

教材及主要参考书目：

[1] 陈智罡, 全同态加密—从理论到实践, 北京: 清华大学出版社, 2022.

[2] 钟焰涛, 蒋琳, 方俊彬, 彭泉, 同态密码学原理及算法, 北京: 机械工业出版社, 2022.

课程编号：25_01145216　　**课程名称：**序列设计

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第三学期

教学目的：本课程旨在使研究生掌握序列设计的前沿理论、多元方法及专业工具，培养研究生分析洞察、创新构思和解决实际问题的能力，为后续深入研究和创新实践奠定理论基础。

教学内容：序列的相关概念，经典序列理论界，最优序列设计，序列在工程中的应用（如无线通信系统）。

教材及主要参考书目：

[1] Pingzhi Fan, Michael Darnell, Sequence Design for Communications Applications, Research Studies Press, 1996.

[2] Solomon W. Golomb, Guang Gong, Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar, Cambridge University Press, 2005.

课程编号：25_01145217　　**课程名称：**人工智能与安全

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第三学期

教学目的：本课程旨在使研究生理解人工智能在安全领域的应用与挑战，培养利用 AI 技术解决安全问题和保护 AI 系统的能力。

教学内容：AI 在威胁检测中的应用，恶意代码分析，AI 系统的对抗性攻击与防御，隐私保护机器学习，案例分析与实践。

教材及主要参考书目：

[1] 曾剑平,人工智能安全, 北京: 清华大学出版社, 2022.

[2] 李剑, 人工智能安全: 原理与实践, 北京: 机械工业出版社, 2025.

课程编号：25_01145218　　**课程名称：**云计算及云安全

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第三学期

教学目的：本课程旨在使研究生系统掌握云计算及其安全领域的核心理论与技术，培养学生分析和解决云安全实际问题的能力，提升其在密码技术与云计算安全交叉领域的创新实践能力，以适应行业发展需求。

教学内容：云计算安全基础与威胁分析、密码学驱动的云安全技术、云安全攻防实践与合规性，前沿技术与行业案例。

教材及主要参考书目：

[1] Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy, O'Reilly, 2009.

[2] 杨东晓, 张锋, 陈世优, 云计算及云安全，北京: 清华大学出版社, 2020.

[3] 陈驰, 于晶, 马红霞, 云计算安全, 北京: 电子工业出版社, 2020.

课程编号：25_01145219　　**课程名称：**物联网安全

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第三学期

教学目的：本课程旨在使研究生深入掌握物联网系统的安全技术，培养设计轻量级安全方案和应对分布式威胁的能力，为智能设备及物联网生态的安全运行提供理论与实践支持。

教学内容：物联网架构与安全需求，设备认证与加密，轻量级密码算法，边缘计算安全，分布式攻击防御，案例分析（如智能家居安全）。

教材及主要参考书目：

[1] Madhusanka Liyanage, An Braeken, Pardeep Kumar, Mika Ylianttila, IoT Security: Advances in Authentication, Wiley, 2020.

[2] 翁健, 物联网安全: 原理与技术, 北京: 清华大学出版社, 2020.

课程编号：25_011452120　　**课程名称：**嵌入式系统与硬件安全

总 课 时：36　　**学　　分：**2

开课单位：数学与统计学院　　**开课学期：**第三学期

教学目的：本课程旨在培养研究生在嵌入式系统与硬件安全领域的核心能力，使学生系统掌握硬件安全设计与防护的基本原理和技术方法，以及具备分析硬件攻击手段、设计安全防护模块以及优化嵌入式系统安全性的能力，为保障嵌入式设备在实际应用中的安全性提供理论与实践支持。

教学内容：硬件安全基础，侧信道攻击与防御，硬件加密模块设计，嵌入式系统安全架构，物理不可克隆函数（PUF），案例分析（如智能卡安全）。

教材及主要参考书目：

[1] Kleidermacher David,Kleidermacher Mike, 嵌入式系统安全: 安全与可信软件开发实战方法, 北京: 机械工业出版社, 2015.

[2] Bernard Candaele, Dimitrios Soudris, Iraklis Anagnostopoulos, Trusted Computing for Embedded Systems, Springer, 2015.

[3] Catherine H. Gebotys, Security in Embedded Devices, New York, Springer, 2010.