Research on Teaching Reform of Combining Cryptographic Theory with Its Engineering Applicaton

ZHANG Luguo[1], LI Zheng[2]

Zhengzhou Information Engineering University, Zhengzhou 450004*, China*

1. *hbtmzlg@126.com.*, 2. *Lizheng_zz@163.com*

Abstract: The general situation of teaching reform, which combines cryptographic theory with its engineering application in the major of information research and security, is introduced. It gives the curriculum system frame of cryptographic theory and cryptographic engineering, and explains how to join and inherit the knowledge architecture in the curriculum system frame. Moreover, it provides many teaching reform thoughts as to teaching method research, experiment teaching, grade evaluation and so on.

Keywords: teaching reform, curriculum system frame, cryptographic engineering application, teaching method research

密码理论与工程应用相结合的教学改革研究

张鲁国[1]，李　峥[2]

*郑州信息工程大学，郑州，中国，*450004

1. *hbtmzlg@126.com,* 2. *Lizheng_zz@163.com*

【摘要】本文介绍了信息研究与安全专业密码理论与工程应用相接合教学改革的概况，给出了密码理论与密码工程课程体系框架，简要说明了课程体系框架中知识结构的衔接与继承问题，以及教学方法研究、实验教学与成绩考评等相关教学改革思路。

【关键词】教学改革，课程体系框架，密码工程应用，教学方法研究

1 引言

为适应信息研究与安全专业学生对以应用为核心的密码工知识结构的需要，2009 年在教研室主持并完成了本科信息安全与研究专业密码工程应用方面的课程标准制定，课程体系建设、相关教材的编写和部分实验课程的开设，并组织实施教学的基础上，启动了大学立项的“密码理论与工程应用相结合的教学改革研究”项目，旨在进一步理顺和完善信息研究与安全专业的专业基础课和专业课的衔接与继承问题，规范相关教学实践，引导教学改革向深层次方面推进。下面将该项目研究情况介绍如下。

2 该教改项目立项背景

密码工程应用课程体系建设规划了以专业课《密码工程基础》及其课程设计为主干，以《密码算法 IP 核设计》、《嵌入式安全操作系统》、《微型密码系统设计》等选修课为支撑的密码工程应用培训方案。构成了以密码算法模块设计为基础，高效密码服务为目标，工程实际应用为牵引的密码工程应用与密码理论相结合的课程体系结构。制定了《密码工程基础》、《密码算法 IP 核设计》等 11 门课程的课程标准，为提高授课质量、相关教材的编写和实施教学奠定了坚实的基础。

为适应教学的实际需要，在上级部门的支持和我们的努力下，建成了供教员和研究生使用的基础科研环境，初步拥有了密码嵌入式芯片及系统的教学和科研平台。形成了密码芯片系统集成、密码嵌入式系统设计和密码服务接口设计三个特色研究方向。在密码安全体系结构、公钥密码加速器和密钥产生算法设计、ECC 加速器、真随机数发生器设计、嵌入式操作系统设计及体系结构研究与实现和密码服务中间件研制上处于国内先进水平，研究成果在相关信息安全应用领

资助信息：现代通信国家重点实验室基金资助项目 (No.9140C1106021006)

978-1-935068-09-9

域的密码服务器、中国人民银行 UKEY 系统等得到规范应用。

课程体系的建设坚持以人为本，以培养学生创新能力和实践技能为核心，将密码理论融会贯通应用于信息安全实践领域之中。坚持将学生对密码理论的学习与密码工程应用紧密结合，强调学生在应用中加深对相关理论的理解，注重培养学生发现问题、分析问题和解决问题的能力。通过 10 名研究生培养和两届学生的教学实践表明：教学效果良好，基本达到建设要求，但也存在课程体系不够顺畅、教材内容有待充实、实验教学相对薄弱、教学方法和评价体系有等完善等问题。

3. 教学改革思路

3.1 进一步理顺课程体系

密码技术作为军事和政治斗争的产物，伴随着信息化的发展，已经成为信息安全领域广泛应用，能够有效解决信息安全问题且不可替代的支撑性核心技术。利用密码系统提供的机密性、不可否认性、完整性和可认证性等密码技术来解决信息传输过程中可能出现的信息安全遭到破坏的情况，可有效防止网络中出现的信息窃取、信息篡改、信息抵赖和信息冒充等信息安全问题。

密码工程是以密码功能为基础，密码服务为核心，面向系统和应用提供加密、解密、签名、认证以及相应密码管理、安全防护等密码服务支持的工程应用系统。已建成的课程体系围绕密码工程应用，将抽象的理论转化为实际应用、将课程学习和课程设计紧密结合起来，综合培养学生学用结合、贴近实际任职需求的特点，解决了学生理论学习和工程应用需求相脱节的问题。新的课程体系将重点放在夯实学生的基础知识，拓宽其知识面，注重各门课程之间的衔接，保持知识体系的连贯性与继承性，兼顾学生面向职业生涯的可持续发展。因而新的课程体系建设将信息安全与研究专业的课程体系规划为密码理论课程体系与密码工程课程体系两个方面。图 1 展示了密码理论课程体系中各门课程之间的相互关系与作用。

在图 1 的密码理论课程体系框架中，规划了以数学为基础，结合信息科学与计算机科学的相关理论，支持密码理论的教学。形成以《密码编码学》、《密码分析学》和《公钥密码学》为主干的密码理论课程体系，为密码工程课程体系提供理论支持与指导。

密码工程课程体系框架如图 2 所示，该课程体系以计算机科学和电子工程等专业基础课为基础，支撑密码理论在密码工程中的具体应用，形成密码理论与工程相结合的信息安全应用、密码服务标准接口和密码设备原理与设计等特色鲜明的工程应用课程系统，通过对低层设备、驱动软件的屏蔽与封装，最终向用户提供标准统一的密码服务应用接口规范，支持本专业的学位论文、课程设计、毕业论文、各类学科竞赛和自主科研等实践教学环节，将密码理论与信息安全的实际应用有机接合，满足学生的任职需求和将来个人发展的需要。

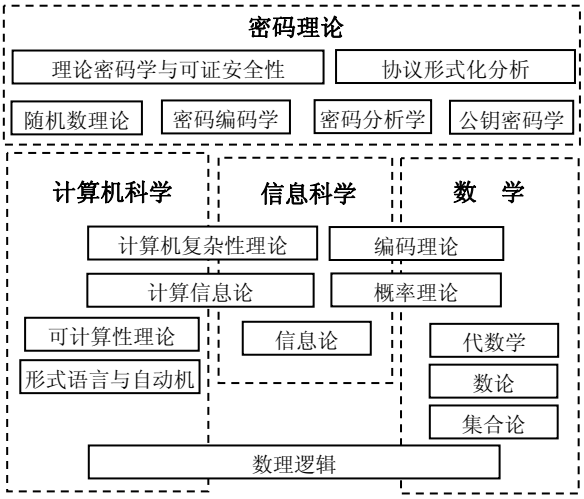

Figure 1. Curriculum system frame of cryptographic theory

图 1. 密码理论课程体系框架

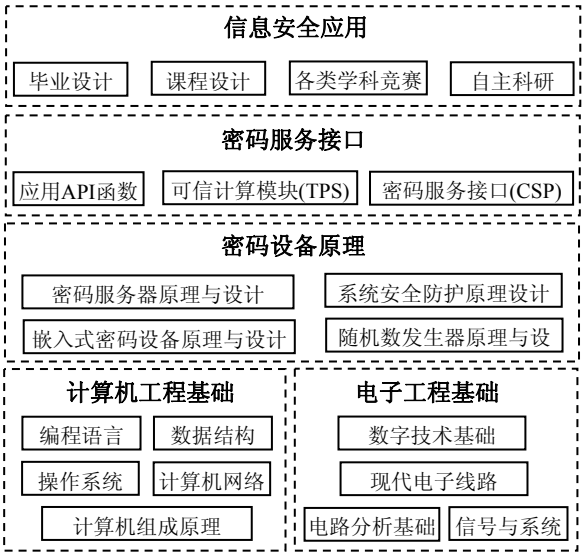

Figure 2. Curriculum system frame of cryptographic engineering

图 2. 密码工程课程体系框架

原有课程体系在课程设置上偏重硬件原理与密码实现教学，对密码工程体系、信息安全应用体系的讲解过于简单。教学改革本着“体系牵引、宏观把握”的思路进一步论证原有课程设置的合理性，在此基础上调整课程设置，明确各课程之间的相互衔接关系，达到密码理论和密码工程应用相互支撑，密码工程应用巩固和拓展密码理论的教学目的。同时，学生可根据自己的职业规划，在侧重于偏向密码理论研究、密码工程应用实践和两者兼顾等三个方面上，选择自己感兴趣的课程进行学习研究，拓展学生获取知识的自主性和独立性。

3.2. 补充与完善教学内容

密码工程应用是以密码设备提供高性能密码功能为基础，密码调度和管理、密码接口管理与服务为核心，密码应用和安全服务为目标的工程应用体系。密码工程应用课程体系建设围绕密码设备、密码服务和上层应用的理论与实践相结合，课程教学和课程设计相统一的密码服务体系为核心展开相关教学工作，本着理论与实践相结合原则，将密码算法软硬件高效实现、密码系统设计、密码调度管理、密码 SoC 芯片及片上操作系统、接口和密码服务等密码应用接合起来形成一个有机完整的密码应用体系，为信息系统提供安全服务。

新的课程体系应进一步贴合未来信息系统安全的需求，从系统与应用的角度对已编写的教材进行修订和补充，将密码理论与密码工程应用的最新成果纳入教学内容，结合信息系统安全应用实际，完成相关电子教材、密码工程应用案例等科技资料的收集与整理工作，组织力量自编一套能与教学内容相配套，并能体现创新精神和我院专业特色的多媒体网络课件，且使每个授课教员均能熟练掌握、独立操作，能在授课过程中灵活运用。每年跟踪密码学学科和信息安全应用研究方向的最新成果，并制作相应的多媒体课件应用于教学实践中。

充分发挥网络平台的优势，分类收集与发布相关国际会议和密码学年会的优秀论文，构建密码理论与工程应用的电子科技文献库，并将已完成的科研项目资料整理充实后，在网站上发布，并指出继续研究、探讨与优化的方向，给学生提供密码工程应用的实际案例，使有兴趣的学生能尽快找到科研实践的切入点。

3.3. 构建新的实验教学体系

研究相关实验与理论教学的相互关系，不断丰富实验和课程设计内容，构建密码理论工程应用的实践教学体系，组建密码工程应用实验室。

根据密码工程应用方向承担的实践教学任务情况，依据信息研究与安全、电子工程本科和密码学研究生培养方案及相关课程标准要求，密码工程应用实验室拟建成一个集密码嵌入式系统设计、密码 SoC 芯片集成、密码服务与接口设计教学与科研于一体的综合实验环境，为受训学生的课程设计、实验教学与毕业设计，密码系统设计与分析方向研究生教学和学位论文提供基础支撑。涵盖密码工程应用方向的教学与实验任务，主要开展密码芯片系统集成、密码嵌入式系统设计和密码服务与接口设计等三类实验教学和研究生学位论文研究，满足专业基础课和专业课程的教学要求，培养学生将密码理论应用于密码工程实践的能力。

实验内容由密码芯片系统集成实验、密码嵌入式系统设计实验、密码服务与接口设计实验三大部分组成。购置嵌入式开发系统、嵌入式操作系统及测试开发环境、嵌入式 EDA 开发工具、FPGA 实验系统、密码应用实验系统、工作站、示波器等相关仪器设备，构成集软硬件于一体的密码应用实验教学平台。

3.4. 开展教学方法研究

以密码理论工程应用教学实践为牵引，进行研讨式教学方法探索，摸索出一套适合本课程体系的教学方法。组织力量集体攻关备好每一堂课，根据授课内容的不同，利用多媒体技术，将重点和难点问题转化为学生喜闻乐见的图形、图像、动画、文本与声音等，使学生在愉快的多媒体环境中掌握授课内容，并增加相关信息的获取，提高学习效率。注意引入启发式、研讨式等教学方法，以调动学生学习的积极性。

培养一支层次分布合理，业务水平较高的师资队伍，使教师在教学过程中的主导性能得以充分发挥。指导学生参与教研室科研工作和各类学科竞赛，把理论知识的讲授与工程实践的技能培养紧密结合，着力培养学生独立分析问题和自主创新的能力。

探索课堂教学和实验教学成绩评价体系，鼓励学生敢于创新和自主钻研的学习积极性，把实验结果正确与学生真正弄懂实验原理的考查结合起来，让学生讲解实验过程，遇到的问题与解决的方法，以及在实验验收过程的随机问题回答等统一考虑，综合评定实

978-1-935068-09-9 © 2010 SciRes.

验成绩。将课堂教学的成绩评定与学生的平时作业与学习情况、课程小论文、课程专题讨论、独立作业和最终考试有机结合起来，形成多种课程结课考核方式和评价体系，培养学生将所学知识融会贯通、随机应变、沉着冷静地解决实际问题的能力。

4. 结束语

本项目教学改革研究思路在学院各级组织的支持与配合下正在稳步向前推进中，部分思想已应用于具体的教学实践，有些环节将在反复论证和教学实践中不断修正与完善。欢迎各位专家和朋友们提出宝贵意见，以便我们的教学改革更加贴合社会对信息研究与安全专业学生的理论知识体系与工程实践能力的培养要求。

致　谢

该课题是在密码工程应用方向课程体系建设基础上进行的，教研室全体同仁为密码工程应用方向的课程体系建设付出了辛勤的劳动，本课题也得到了业务部门的支持和部分专家、教授的指导，在此，向所有对本课题给予指导、支持与帮助的专家、教授和同事们表示衷心的感谢和崇高的敬意。

References (参考文献)

[1] Michael Prosser，Keith Trigwell. Understanding Learning and teacher The Experience in Higher Education[M]. Peking University Press, 2008

[2] WANG Xin-chang. Constructing Multinedia Teaching Resources System of *Information Security Techniques*[J]. Journal of Institute of Electronic Technology，2007，19（1），P3-5(Ch)
王新昌，《信息安全技术》课程多媒体教学资源系统的构建[J]，电子技术学院学报，2007, 19(1)，P3-5.

[3] ZHANG Lu-guo，Application of Multimedia Technology in Teaching the Course of Date Encryption Standard[J]，Journal of Institute of Electronic Technology，2007，19（1），P1-2，P31(Ch)
张鲁国，多媒体技术在数据加密标准课中的应用[J]，电子技术学院学报，2007, 19(1)，P1-2，P31.

[4] LI Zheng，ZHANG Lu-guo，Foundations of Cryptographic Engineering[M] ， Institute of Electronic Technology, Information Engineering University，2008
李峥，张鲁国，密码工程基础[M]，信息工程大学电子技术学教材，2008.