基于 SPOC 和翻转课堂的现代密码学课程改革总结与分析

张宁，谭示崇，傅晓彤，杜小刚，李晖

（西安电子科技大学网络与信息安全学院，陕西 西安 710071）

摘　要：针对 2015-2018 年西安电子科技大学现代密码学课程改革的经历，分析总结了 MOOC、SPOC、翻转教学在现代密码学课程上的实践与效果，同时以编程马拉松式的实验和传统实验两种形式作为现代密码学课程的配套实验，介绍了课程实验的实施情况，总结了课程改革的经验和教训，给出了可推广的“互联网+”式现代密码学本科教学创新模式。

关键词：现代密码学；本科教学；课程改革；翻转课堂；互联网+

中图分类号：G643.0

文献标识码：A

doi: 10.11959/j.issn.2096−109x.2019029

Summary and study on the curriculum reform of modern cryptography based on SPOC and flip classroom

ZHANG Ning, TAN Shichong, FU Xiaotong, DU Xiaogang, LI Hui

School of Cyber Engineering, Xidian University, Xi’an 710071, China

Abstract: Based on the teaching practice of modern cryptography curriculum reform in xidian university from 2015 to 2018, the practice and effect of MOOC, SPOC and flip classroom in modern cryptography were analyzed. The implementation and reform of the lab course were summarized based on the experiments with programming marathon and traditional lab course. The accomplishments and lessons of the curriculum reform were summarized and some suggestions of innovative modern cryptography education for undergraduate in the mode of “Internet +” were provided.

Key words: modern cryptography, undergraduate education, curriculum reform, flipped classroom, Internet+

1　引言

2015 年 7 月，国务院学位委员会学科评议组评议，报国务院学位委员会批准，国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科，学科代码为“0839”，授予

收稿日期：2019−04−12 ；**修回日期：**2019−05−27

通信作者：张宁，znlady@163.com

基金项目：中央网信办网络安全人才培养试点基地建设项目

Foundation Item: Project of Cyber Security Talent Cultivation Base by Office of Central Leading Group for Cyberspace Affairs

论文引用格式：张宁, 谭示崇, 傅晓彤, 等. 基于 SPOC 和翻转课堂的现代密码学课程改革总结与分析[J]. 网络与信息安全学报, 2019, 5(3): 89-95.

ZHANG N, TAN S C, FU X T, et al. Summary and study on the curriculum reform of modern cryptography based on SPOC and flip classroom[J]. Chinese Journal of Network and Information Security, 2019,5(3): 89-95.

“工学”学位。西安电子科技大学于 2014 年 12 月 30 日成立网络与信息安全学院，整合本校密码学、信息安全、计算机安全等相关专业的力量，成为首批获批网络空间安全一级学科的学校，同时作为中央网信办网络安全人才培养示范基地，实行了一系列教学改革创新。

大规模在线开放课程（MOOC，massive open online course）是基于课程与教学论及网络和移动智能技术发展起来的新兴在线课程形式。2012 年，“MOOC 元年”开启之后，MOOC 迅速在全球升温，平台建设风起云涌。Udacity、Coursera、edX 等国际 MOOC 平台，以及中国国内爱课程、中国大学 MOOC、学堂在线等 MOOC 平台开始越来越多地出现在教师与学生的视线中。但 MOOC 课程的低完成率，缺少师生互动等问题随着 MOOC 的流行凸显出来，后 MOOC 时代引起了另一类教学，SPOC（small private online course），按照字面意义理解为“小规模限制性在线课程”。“Small”是指学生规模一般在几十人到几百人；“Private”是指对学生设置限制性准入条件，达到要求的申请者才能被纳入 SPOC 课程。教育界普遍认为，SPOC 可以弥补 MOOC 的不足，同时享受 MOOC 带来的便利[1]。同时翻转课堂“Flipped Class”开始进入课堂，这种教学形式下，课堂和老师的角色发生了变化，老师更多的责任是理解学生的问题和引导学生运用知识。随着“互联网+”开始进入教育，技术对教育的支持让学生可以完全沉浸在教学环境中，感觉不到技术的存在但在充分利用了技术，一场以技术转移为核心的教育变革在悄然进行，最终回归到提升教与学的质量。

1.1　课程背景分析

现代密码学是信息安全类专业一门重要的专业课。这门课程涉及离散数学、数论、基础代数、概率论、计算复杂性等数学专业，同时注重信息论、形式化逻辑、计算机编程等知识，既有理论，也有大量的实践学习。笔者所在的教学团队常年从事现代密码学教学工作，传统的现代密码学课程改革只是在原有的基础上进行适当的补充、小范围修改更新，但却一直未能推陈出新。如今，MOOC、翻转课堂、SPOC 等概念已经大范围进入中国的高校，在西安电子科技大学网络与信息安全学院的支持下，我们所在教学团队以 MOOC、SPOC、翻转课堂为基础，于 2015 年开始尝试全新的现代密码学教学模式。

1.2　学生背景分析

本次教学改革的教学对象是我校信息安全实验班，该班的学生是在全校范围内根据学生基础、兴趣选拔的，由 40 名对信息安全有浓厚兴趣、具有扎实的数理基础和较强的编程能力的学生组成。如果学生水平差别符合正态分布，那么授课教师一般选择中间的大多数学生为重点照顾对象，对于最优秀和最差的学生的照顾程度小一些，这样会增加提升教学质量的难度。此实验班的学生水平差异比普通班小，可以更容易地取得良好的授课效果，这 40 名同学构成的小班，也给课堂创新和翻转课堂的实施提供了基础。

2　课程改革

2.1　课程资源准备与 SPOC

现代密码学课程开设在每年的秋季学期，暑假前，搜集整理并制作所需的课程资料发给学生，其中教材和实验资源都是全球顶尖水平的密码学课程资源，除了教材书籍，还有相应的视频资源[2]，为了方便学生学习，我们组织人力进行了课程视频的翻译。本课程注重实践，实验资源采用了 2014 年 Blackhat[3]大会上提出的实践类密码题目以及 MTC3[4]上的部分题目，另外也整合了欧拉计划[5]中一些基础的数学题目，所有的资源以微信推送[6]的方式在假期发给学生。

每年暑假，Coursera 上斯坦福大学 Dan Boneh

教授的 Cryptography I 开课（目前的情况是 3 个月开一次课），要求学生一起注册这个课程，如图 1 所示。本课程包含密码学的讲义、视频讲授、章节测试题，为期 6 周，让学生充分利用暑假和开学后的一段时间，以在线看视频自学、每周做完相应的章节测试题的方式自主学习。事实上，同学们非常认真负责地对待这项任务，暑假以及开学后几乎每天都会在线上交流工具中提出和讨论各种各样的问题，其中一些问题还相当具有代表性。

图 1　Coursera 的密码学课程

2.2　翻转课堂

2.2.1　课堂安排

秋季开学后，本着学生“自主学习，自我管理”的翻转课堂指导思想，把全班 40 名学生分成 4~6 个学习小组，每周由课代表和老师分配安排相应的任务到各个小组，再由各组组长对组员进行任务调配。任务内容主要就是对于 Coursera 上在线学习的斯坦福大学密码课程的再现和深入。在上课时间的安排上，笔者每次利用两大节课的时间进行现代密码学的课堂教学。典型的课堂流程如表 1 所示。

课堂报告和总结点评会进行 4~6 次，完整的一个课堂流程是 200 min。

课堂上，经过充分准备的学生上讲台按自己的理解对课程内容进行讲解，任课教师和助教坐在下面和其余同学一起听课，随时提出一些相关问题的补充和见解，课堂上有激烈的讨论，有现场运行程序验证算法，也有现场问答环节，课堂上充分利用手机和计算机，教师会准备即时的问题和测验发上线。同学们在这种新颖、互动的课堂上，充分体验到了自主学习的乐趣和责任，同时又将心比心地体会到在上面讲课的同学所准备内容的来之不易，本着尊重他人也尊重自己的态度，更加认真地投入课堂中，从而达到全员参与、全体互动的效果，在一定程度上解决了大学课堂中普遍的“老师讲，学生走神”的现象。

课下，在学生完成在线题目后，课程组给出一些附加题目，学生完成的水平和质量远远超出预期，对于知识的理解可通过多种练习积累起来。我们利用 QQ、微信（设置了课程微信公众号）、邮件等一切资源，督促鼓励学生按期完成课程学习，鼓励学生互相交流，保证每一个学生都能完成相应的课程要求。

2.2.2　在线作业和评价体系

斯坦福大学 Dan Boneh 教授的密码学课程是公认的“课程内容难，听课要基础，作业充满挑战性”。该课程的每一部分内容讲授结束后，对应的在线作业要求在某个时间之前完成，如果不按时提交作业答案，成绩将会受到极大的影响，关系到是否能够取得结课证书。课程作业不考察记

表 1　典型的课堂流程

课堂流程	学生任务	教师工作	时长	形式与媒介	优势和特点
课前测	在线答题	准备题目	20 min	问卷星或雨课堂	即时出成绩
课堂报告	按要求报告	听，穿插问题	15 min	PPT、板书等	问题及时出现
总结点评	听	串讲	5 min	PPT、板书等	总结性质
课后测	纸笔题	随时答疑	30 min	纸笔分组讨论研究	分组讨论出结果
课后测答案解析	讲题	纠错答疑	10 min	投屏或 PPT 板书	开放式

忆性的知识，侧重考查学习者对知识的理解、掌握和应用，作业充满挑战性，可以很好地考查学生是否真的理解了密码学的概念和基础理论。目前，四届共计 120 名学生全部修完了在线课程，拿到了 Dan Boneh 教授签名的课程声明，顺利完成了全球最优秀的密码学课程的学习。

2.2.3 课堂上问题解决

翻转课堂旨在充分调动课堂中每一个人的积极性，不仅教师在讲台前讲课，更提倡学生准备内容，自己也当一回“教师”。但是，学生毕竟刚开始学习现代密码学这门课，在讲解相关章节时，在讲解的深度和广度上，有一定的不足之处。要求任课教师熟练应用教学策略，充分准备预案，妥善实施。在学生讲解的时候，任课教师会根据具体情况做相应的补充，其余同学可以随时在课堂上提问，但提问往往很踊跃，需要教师合理安排，及时解决课堂出现的各种问题。同时，为了充分帮助学生理解课堂内容，在课堂上会随时给出新的题目，这些题目的形式多种多样，包括提前准备的纸笔考试，利用问卷星、雨课堂等在线工具做的课堂问答，QQ 群中直接发出题目的电子版，课堂上直接利用 PPT 给出题目等多种形式，保证学生在这 3 个小时的时间内全身心投入。

2.2.4 课堂测验

课堂测验分为课前测和课后测。课前测约 10 道题，为填空选择题（客观题），通过在线答题，即时出成绩，准时在课程开始时计时，有效避免迟到，教师提前设置好，自动出题和判卷，允许现场学习，题目 40%是对以前课程的复习，60%是对本次课程预习的考察，也会引出本节课程的主要讨论内容，课前测的题目一般在课程讲解的过程中会出现，随时给出答案和讲解。课后测约 5 道题，为简答题和计算题（开放式主观题），紧扣本节课的课程内容，要求小组讨论给出正确答案。课前测可以有效检验课程预习效果，让学生带着问题进入课堂；课后测是以问题为导向，让学生对本节课的内容进行总结归纳，进行更深入的思考，所有的测试都只规定时间，可以讨论或现场学习，唯一的目的是服务课堂，提高学习效果。

通过以上翻转课堂的实施，笔者深刻体会到，在 SPOC 翻转课堂中，教师的主要任务是构建学生自主学习的环境，需要大量的课前准备。教师考虑的问题从传统的按照教学大纲如何保证完成教学任务转变为如何引导学生开展个性化学习、如何将技术融入师资、如何重塑教师角色，对教师的要求很高。

2.3 实验课的探索与实践

2.3.1 编程马拉松

在 2013 级和 2014 级现代密码学实验中，我们采用编程马拉松式的实验过程。

前期准备工作主要包括实验题目的确定，代码提交平台的选择和熟悉以及完整详细的实施方案。此外，参加编程马拉松实验的学生以团队的形式参加，所以要提前进行人员的分组，还有实验场地的布置、消耗物资的备办以及对实验细则的制定等。除此之外，需要至少 5 名志愿者，负责代码验证、现场软硬件维护等，学院实验教学中心保障各种硬件需求。

实验当天每组学生根据实际情况分工合作攻克 20~40 道题目，这些题目均为国外知名的密码学挑战，内容涉及现代密码学的经典算法和应用，题目难、中、易分布为 3:4:3，其中，30%的题目具有相当大的难度。在场的评判小组实时根据各组代码提交情况进行评判并做出回应，如果答对一道题则在该组记分牌上打钩表示通过。现场有任课教师和多位研究生助教，随时帮助同学们理解题意，解决各种问题，持续两天一夜。最后各个团队分别提交各自的实验报告，我们组织专家组听取各个团队的实验汇报指导点评，给出针对

性的意见和建议。经过 2 个小时的汇报和评议，最终决定以答题数量最多、代码质量和报告质量最优的团队为优胜团队。

编程马拉松的形式较传统实验更有挑战性，能给同学们留下深刻的印象，在实验过程中学生能够以团队形式投入、分工合作。这种形式的实验对题目质量要求高，事先课程组将所有的题目验证核对，所需教学资源（包括资金人力）也较多。

经过了两年的实验，第一年效果还好，在全院学生中引起了一波学习密码学编程的风气，但第二年，下一届的学生已经听说了这种方式，甚至提前“抱好大腿”，准备“划水”。另外还存在“题目老化”的情况，因为教师要求学生将题解上传到 Github 和 Coding 这样的代码托管平台方便团组合作，于是往届同学会很方便地分享题解给应届同学，因为是代码，即便我们在准备题目时改变参数，仍然很难保持题目的“新鲜感”。“资源不足”也是一个重要的问题，在编程马拉松阶段至少需要 10 名学生志愿者、5 名教师，不少于 100 m^2 的场地，还需要准备三餐以及暖气（适逢本地最冷的时间段）。基于以上种种原因，2018 年经过研究回归到传统的实验模式。

2.3.2　传统实验

2018 年教学组在以往的基础上，从题库中选备 16 道题目，以单独验收的方式进行。

实验课在现代密码学课程大纲中占 16 课时，实验课前通过网络公布实验题目，请同学们单独做题。与讲授课程同步，我们安排 8 次实验，每次实验题目是与当前课程相关的 2 个题目，每次实验 3 个小时，在这 3 个小时内，验收 40 名同学的代码和运行结果。每位同学约有 5 min 时间演示，保证每个同学完成每道题目，每次通过学生的完成情况和实验报告给出实验分数。

目前题库约有 100 道题目，可以通过改动参数、自由组合的方式进行扩展，至少 4 年内不会出现重复，学生单独完成题目并撰写实验报告，有效避免“打酱油”和“题目老化”的情况，也能和课程同步，检验巩固学习效果。另外，扩展性比较强，可以扩展到大班授课的情况，实验老师随课程人数线性增加，如 40 名同学需要 1 位实验老师，80 名同学 2 位实验老师。

2.4　评价体制

2.4.1　课程评分机制

区别于传统的一考定成绩，此次课程改革采用了多元的评价体制，学生的成绩由 4 部分构成，如图 2 所示。① 课堂成绩是指在线课程学习的完成情况，SOA（statement of accomplishment）是 Coursera 颁发的完成课程后的证明，课堂上做报告可以至少保证一个同学 2 次报告。② 作业是指课堂上给出的现场作业，同时也是保证到课率的方法，另外给出了一种全新的作业——出题，通过让学生自己出题来查缺补漏。③ 期末考试占 20%，期末考试使用了全新的考试平台，进行在线考试，题库由从学生出的题目中选出来的一部分和课程组准备的题目构成，保证每个学生拿到的套题都是不一样的。④ 附加分，在课程进行过程中，也给出了一些很有挑战性的课题，有不少同学对这些题目进行了深入研究，依次给出附加分。

现代密码学成绩构成

一　课堂成绩 40%

1　SOA 20% distinction 20, 合格 15

2　课堂报告 20%　3 次或以上 20，2 次 15（最后不够两次者请补笔记）

二　作业 40%

5 次 Quiz+final 题目取最高 4 次，每次 10 分（1019, 1102, 1109, 1116, 1123）

三　期末考试 20%

四　附加分

附加的题目，其他报告酌情加分

五　实验成绩另计

图 2　Coursera 的密码学课程

2.4.2 问卷调查

在课程进行的过程中，课程组召开过多次教学研讨会，引起了学校高教研究所的重视，高教研究所的教师帮助我们设计问卷调查，经历了严格的问卷设计、预问卷等环节，面向第一届 40 名学生进行调查，经过对问卷分析统计，对此次现代密码学教学改革给出了比较正面的评价[7]。同时，学生也给出了一些意见，如课堂时间较少、作业题目缺少梯度、考试平台设计的 bug 等问题。在此后的两届中，我们对问卷进行了微调，每次课程结束都发放问卷，根据问卷结果对课堂和实验体系进行修正，对课程安排进行循环优化。

2.4.3 与传统课堂的区别

课程结束后课程组从学生和教师的反应两个维度分析了基于翻转课堂和传统课堂的区别，如表 2 和表 3 所示。

通过 3 年的跟踪分析发现，基于翻转课堂进行密码学教学的同学较传统课堂教授的学生能更加积极主动地分析密码学应用中的问题，而不是单纯地使用密码学，具备更强的批判性思维，在工作中能更主动地应用密码学知识解决实际问题，更乐于从实用的角度研究密码学。

在翻转课堂教学中，教师从知识传授者向学习活动的设计者、学习资源的研发者、学习过程的促进者转变，对教师有更高的要求，注重教师以往的课堂经验。随着题库和课堂经验的丰富，在一轮一轮的迭代中，教师课堂准备的工作量逐渐减小，但随着密码学新技术的发展，课堂内容需要更新迭代，总体而言，教师的工作量相较传统教学更多，但是课堂获得的成就感也更多。

3 结束语

我们在本校信息安全专业实验班的“代密码学”课堂上采用翻转课堂模式教学，充分利用优质在线教学资源，极大地调动了学生的学习积极性，将传统的学生被动接受知识转变为学生主动获取知识，让学生成为课堂的主角。同时改革配

表 2　传统教学和基于翻转课堂教学中学生的区别

	传统教学	基于翻转课堂的教学
课前预习	很少，基本不看	大量，需要完成课前作业
课堂角色	听课者，被动接受	演讲者与参与者，主动学习
理论知识	老师讲什么听什么，重在记忆和了解	自主进行理论知识的引入，推导，知识体系的脉络
课程重点内容	理论知识的理解和识记	理论知识的理解和识记，动手实践，现有密码体制的应用
动手能力	少量实验，重在实现密码算法	大量实验，重在理解和更正密码学应用的错误和疏漏
课后复习与巩固	以理论考试为目的，重在记忆，有往年题目蓝本	以发现问题为目的，自己探索可能出现的密码学应用错误，考试重在理解

表 3　传统教学和基于翻转课堂教学中教师的区别

	传统教学	基于翻转课堂的教学
目标	完成教学大纲所规定的教学任务	构建学生自主学习力的线上和线下教室
备课工作	课堂教学内容、课后作业、批改课后作业	课堂教学内容与可能出现的所有问题，课上各种测试，包括测试系统与测试内容课后反馈
课堂角色	以教师为中心的讲授者	以学生为中心的组织者
教学行为	更新教学内容，丰富教学方法	教学环境分析、课程分析、学生分析、课程评估
要解决的问题	如何保证完成教学任务	如何引导学生开展个性化学习、如何将技术融入师资、如何重塑教师角色

套实验课程，通过实践获得了一套可以推广的教学方法和模式。目前，此教学模式在实验班学生中取得了较好的教学效果。整合了教学资源，包括立体化的教材资源、题目资源，除了传统的问答题目，不管是作业还是考试，都加入了编程题目，学生得以把学到的知识学以致用，通过实际操作真切感受来自密码学的魅力以及现实世界中密码学存在的诸多不足之处，也进一步激发了学生此后对密码学进行深入研究的热情和动力。这一套方法对于其他课程而言，可以结合各自课程的特点，在“互联网+”的形式下，开展课堂创新，改革教学方式方法，提高教学的质量与品质。

参考文献：

[1] 康叶钦. 在线教育的“后MOOC”—SPOC解析[J]. 清华大学教育研究, 2014, 35(1): 85-93.
KANG Y Q. An analysis on SPOC: post-MOOC era of online education[J]. Tsinghua Journal of Education , 2014, 35(1): 85-93.

[2] Coursera. Dan boneh cryptography I [EB/OL]. https://class.coursera.org/crypto-014

[3] [EB/OL]. http://www.cryptopals.com/.

[4] [EB/OL]. https://www.mysterytwisterc3.org/.

[5] [EB/OL]. https://projecteuler.net/.

[6] [EB/OL]. https://mp.weixin.qq.com/s?__ biz= MzAxODUwMz YwNQ==&mid=400726644&idx=1&sn=8988a0725d0b0ec1cdc85a1dd629f392&mpshare=1&scene=1&srcid=02185U2abW3BD4ihA2HR5HqM#rd.

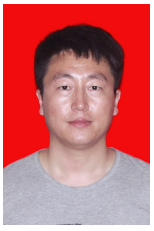
[7] 李瑾, 张宁, 云霄. 新工科背景下工科生自主学习力的深度构建[J]. 高等工程教育研究,2018,(5): 71-77.
LI J, ZHANG N, YUN X. The construction of engineering students' self-regulatedlearning in the background of emerging engineering[J]. Research in Higher Education of Engineering, 2018,(5): 71-77.

[作者简介]

张宁（1979− ），女，陕西宝鸡人，博士，西安电子科技大学副教授，主要研究方向为公钥密码学、应用密码学、无线物理层安全、信息安全法。

谭示崇（1979− ），男，广西贵港人，博士，西安电子科技大学副教授，主要研究方向为云计算安全、区块链技术。

傅晓彤（1977− ），女，陕西西安人，博士，西安电子科技大学副教授，主要研究方向为公钥密码学及其应用。



杜小刚（1989− ），男，甘肃秦安人，硕士，西安电子科技大学工程师，主要研究方向为数据压缩与存储、信息安全。

李晖（1968− ），男，河南灵宝人，博士，西安电子科技大学教授、博士生导师，主要研究方向为密码学、无线网络安全、云计算安全、信息论与编码理论。