



学会资讯

Learn information

学会动态

通知公告

图片新闻

会议报道

年会报道

在线咨询

学会章程

联系方式

[首页](#)>>[学会资讯](#) >>[通知公告](#)

密码学高端系列培训之三——序列密码设计与分析培训通知

序列密码也称为流密码 (Stream Cipher)，它是对称密码的一种。序列密码算法具有实现简单、便于硬件实施、加解密处理速度快，是经典密码算法中最基本最重要的一种，是目前广泛使用的密码算法，应用在国防、金融、商务、办公自动化、日常生活等各个领域。

为了使我国密码学工作者、密码产品开发者了解序列密码研究和发展进展，中国密码学会将于11月28日—12月2日举办序列密码设计与分析培训班，邀请密码界知名学者：冯登国、Hongjun Wu、戚文峰、张斌、冯秀涛、田甜和樊俊锋等，讲解序列密码研究与应用的最新进展。内容包括序列密码理论、序列密码设计、序列密码分析和序列密码硬件实现技术与攻击等。培训将对序列密码基本知识到最新的研究热点进行透彻的讲解。

此次培训的目的是使得学员能够掌握序列密码的基础知识和理论，领会设计分析的基本手段，并最终将这些手段和知识应用到密码教学、学术研究和产品开发中，推动我国密码学研究在广度和深度两个方面的发展。本培训班的内容可以作为硕士研究生的一门专业课或者博士生的一门专业基础课。

培训的有关事项通知如下：

一、主办单位

中国密码学会
中国密码学会学术工作委员会

二、培训时间

2014年11月28日9:00-13:30报到，11月28日下午至12月2日正式培训

三、培训地点

北京电子科技学院电教楼电教3（北京丰台区富丰路7号）

四、培训对象

高等院校、科研院所密码和相关专业专家、学者、科技工作者，密码专业和信息安全专业在读博士生、研究生，从事密码产品开发和应用的企事业技术人员。

五、培训日程安排

日期 时间 培训内容 主讲者

11月28日 14:00-17:00 基于密码应用的序列理论 戚文峰
(信息工程大学)

11月29日 8:30-11:30

14:00-17:00 序列密码设计 Hongjun Wu
(Nanyang Technological University, Singapore)

11月30日 8:30-11:30

14:00-17:00 冯登国

(中科院软件所)

12月1日 8:30-11:30 序列密码分析 张 斌

(中科院软件所)

14:00-17:00 田 甜

(信息工程大学)

12月2日 8:30-11:30 冯秀涛

(中科院数学所)

14:00-17:00 序列密码的硬件实现技术及攻击 樊俊锋

(深圳市组创信安科技开发有限公司)

六、培训费用

密码学会已缴费会员2300元(学生) / 2800元(其它)

非密码学会会员3000元

备注: 培训费含培训期间餐费、资料费、讲课费等。

七、住宿费

住 宿: 推荐北京电子科技学院院内宾馆及附近酒店, 费用自理。

北京电子科技学院招待所, 协议价: 标准间160元/双人间或单人间 (可帮助预订)

汉庭酒店北京总部基地二店 (科丰桥西时代财富天地大厦西侧, 距学校800米), 联系电话: 010-63786767。

北京丞泰宾馆(北京市丰台区看丹路南开西里23号, 距学校200米), 联系电话: 010-63798678。

注: 汉庭酒店和北京丞泰宾馆, 请自行预订。

八、相关事项

1、培训回执请于2014年11月20日前, 发送至联系人邮箱: 409680030@qq.com, 学生请将学生证扫描发此邮箱。

2、请于11月30日前通过银行汇款方式缴纳培训费用。

汇款至: 户 名: 中国密码学会

账 号: 0200 1864 1920 0001 727

开户行: 中国工商银行北京公主坟支行

3、完成汇款后, 请将汇款凭证传真至010-59703688, 或发送到财务联系人电子邮箱(cacr02@cacrnet.org.cn), 注明人员和单位名称, 以便开发票和确认。

4、开车来的学员, 请在登记表中注明。

会务联系人: 党凡18810962909 409680030@qq.com

财务联系人: 刘洁010-59703688 13661388568 cacr02@cacrnet.org.cn

5、培训提供PPT资料U盘, 不提供文本教材。

附: 1、通知(报名回执、路线图)下载

2、带公章通知下载

中国密码学会

中国密码学会学术工作委员会

2014年10月26日