

关于举办“密码学高端系列培训之九——

密码算法设计与分析高端培训”的通知

密码算法是保障通信和数据安全的核心，多样化的密码应用环境和新兴密码分析技术的发展对密码算法的设计与分析提出了新的要求。为进一步提高我国研究人员在密码算法设计和分析领域的研究水平，促进密码人才的成长与进步，中国密码学会决定举办“密码学高端系列培训之九——密码算法设计与分析高端培训”。

本次培训由王丽萍、孙兵、张江、潘彦斌、孙思维、崔霆、薛海洋等优秀专家学者组成授课团队，围绕全国密码算法竞赛中的若干算法讲授分组密码和后量子公钥密码的主要设计理论和分析技术。课程设置涵盖分组密码的设计原理、典型分析方法与应用、自动化分析技术，基于格的公钥密码、数字签名和密码协议设计与分析，基于编码的密码算法设计与分析，基于椭圆曲线同源的密码协议设计与分析等。

本次培训目的是使学员能够了解分组密码和后量子公钥密码相关领域的基础理论、分析技术和最新进展，推动我国密码算法设计与分析基础研究和密码应用方面的发展。培训班的内容可以作为研究生的一门专业基础课，培训结束，可提供相应学习证明。

一、培训对象

高等院校、科研院所等密码相关专业的科技工作者，密码学及网络空间安全等专业在读硕士生、博士生，以及从事信息安全产品开发和应用的企事业单位工程技术人员。

二、培训时间

签到时间：8月16日 14:00—21:00

培训时间：8月17日 9:00至8月20日 18:00

三、培训地点

北京铁道大厦 三层多功能 B

四、培训费用

学生 2800 元、密码学会会员 3200 元、非会员 3400 元
(含培训资料费、培训期间午晚自助餐费)

五、住宿安排

1. 推荐北京铁道大厦(北京市海淀区北蜂窝 102 号)

酒店协议价: 大床房/标间: 515 元/间(含单早)、550 元/间(含双早), 住宿费用自理。

注: 酒店预订需提前报学会, 经确认后个人可直接联系宾馆入驻。酒店为学会预留房间有限, 订满为止。

2. 学员也可自行预定培训地点周边的其它宾馆、快捷酒店。

六、培训交费

请通过银行汇款或现场刷卡交纳培训费用

户 名: 中国密码学会

账 号: 0200 1864 1920 0001 727

开户行: 中国工商银行北京万寿路南口支行

注: 学会将根据交费顺序安排听课座次

七、相关事项

1. 报名培训的回执请于 2021 年 8 月 10 日前, 发送至联系人邮箱: gdp@cacrn.net.org.cn, 学生请将学生证扫描发此邮箱。

2. 会务联系人: 汤老师 010-59703621

财务联系人: 米老师、梁老师 010-59703687

附件: 1. 密码算法设计与分析高端培训报名回执表

2. 密码算法设计与分析高端培训日程安排

