附件2

密码算法设计与分析高端培训日程安排

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 日 期 | 时 间 | 培训内容 | 主讲者 | 主持人 |
| 8月16日 | 14:00-21:00 | 学员报到 |
| 8月17日 | 8:20-8:30 | 开班仪式 | 待 定 | 待定 |
| 8:30-12:00 | 分组密码的基本设计原理及实例 | 崔 霆 |
| 14:30-18:00 | 基于格的加密算法：设计与分析 | 潘彦斌 |
| 8月18日 | 8:30-12:00 | 分组密码的典型分析方法及其应用（一）：差分密码分析、线性密码分析 | 孙 兵 | 待定 |
| 14:30-18:00 | 基于格的数字签名算法和密钥交换协议：设计与分析 | 张 江 |
| 8月19日 | 8:30-12:00 | 分组密码的典型分析方法及其应用（二）：不可能差分分析、积分攻击、零相关线性分析等 | 孙 兵 | 待定 |
| 14:30-18:00 | 基于编码的加密算法：设计与分析 | 王丽萍 |
| 8月20日 | 8:30-12:00 | 分组密码算法自动化设计分析理论与方法 | 孙思维 | 待定 |
| 14:30-18:00 | 基于椭圆曲线同源问题的密钥交换协议：设计与分析 | 薛海洋 |

注:（1）本次培训的讲授内容是2019年中国密码学会密码算法竞赛中若干算法的设计原理和部分分析方法。

（2）每天上午讲授分组密码，下午讲授公钥密码。其中上午10:00-10:15和下午16:00-16:15为茶歇时间，上午11:45-12::00和下午17:45-18:00为答疑时间。