

中国密码学会2023年密码测评学术会议 第二轮通知暨会议日程安排

中国密码学会2023年密码测评学术会议定于2023年11月11日至12日在广西南宁市举行。本次会议由中国密码学会密码测评专业委员会主办, 桂林电子科技大学计算机与信息安全学院、桂林电子科技大学密码学院、桂林电子科技大学南宁研究院承办。

会议围绕密码测评主题, 邀请了国内密码测评领域的专家学者、行业精英和在校师生做特邀报告和主题报告, 并共同交流、探讨密码测评方面的最新成果、学术热点、学术动态及发展趋势, 促进密码测评学术界和产业界的相互交流与合作。

我们诚挚邀请您莅临本次会议, 共同探讨密码测评领域的发展与前沿问题。现将会议有关事项通知如下:

一、主办单位

中国密码学会密码测评专业委员会

二、承办单位

桂林电子科技大学计算机与信息安全学院

桂林电子科技大学密码学院

桂林电子科技大学南宁研究院

三、时间、地点

报到时间: 2023年11月10日15:00-21:00

报到地点: 南宁市荔园山庄11号楼总台

会议时间: 2023年11月11日至12日

会议地点: 南宁市荔园山庄中心一楼多功能厅

四、会议日程

11月11日（星期六）	
时间	会议内容
09:00-10:00	领导致辞，合影留念
10:00-10:40	报告人：冯登国（中国科学院院士） 报告题目：从密码发展历程看密码学科知识体系
10:50-11:30	报告人：胡予濮（西安电子科技大学） 报告题目：GVW15 谓词加密方案的 P/poly 有效性的注解
11:30-12:10	报告人：张文政（中国电子科技集团公司） 报告题目：动态分组密码算法的一些思考
14:30-15:05	报告人：马原（中国科学院信息工程研究所） 报告题目：商用密码应用安全性评估技术进展与趋势
15:05-15:40	报告人：樊俊锋（深圳市纽创信安科技开发有限公司） 报告题目：国外测评体系的发展动态
15:40-16:15	报告人：张帆（浙江大学） 报告题目：针对 NTT 篡改旋转常数的新型故障攻击
16:25-17:00	报告人：林璟锵（中国科学技术大学） 报告题目：密码工程安全相关研究
17:00-17:35	报告人：刘志乐（杭州安恒信息技术股份有限公司） 报告题目：商用密码应用及测评实践
17:35-18:10	报告人：陈万钢（豪符密码检测技术（成都）有限责任公司） 报告题目：密码检测实践与探讨
11月12日（星期日）	
09:00-09:35	报告人：杨波（陕西师范大学） 报告题目：区块链中的隐私保护
09:35-10:10	报告人：肖秋林（国家密码管理局商用密码检测中心） 报告题目：V2X 证书认证系统测评方法研究
10:10-10:45	报告人：胡之斐（深圳鼎铨数字科技控股有限公司） 报告题目：5G 网络密码测评研究
10:55-11:30	报告人：王安（北京理工大学） 报告题目：SPA-GPT：基于强化学习的密码芯片全自动简单能量分析
11:30-12:05	报告人：牛超（蚂蚁技术研究院-密码学实验室） 报告题目：AES 密文到全同态密文的转换技术及安全性研究
14:30-15:05	报告人：程朝辉（深圳奥联信息安全技术有限公司） 报告题目：标识密码技术及安全性研究
15:05-15:40	报告人：韩玮（智巡密码（上海）检测技术有限公司） 报告题目：密码检测标准概要研究

15:40-16:15	报告人：崔永娜（国家密码管理局商用密码检测中心） 报告题目：密码服务平台测评方法研究
16:35-17:10	报告人：冯景亚（桂林电子科技大学） 报告题目：基于 SAT 的轻量级密码 S 盒新优化实现及测试
17:10-17:45	报告人：许壮（北京智芯微电子科技有限公司） 报告题目：经典模板攻击的改进方案探究
17:45-18:00	闭幕式

五、会议注册

通过中国密码学会会议注册系统在线报名，网址：
<http://cacr2023.cacrnnet.org.cn/fair/41>，点击链接—>在线报名—>
 确认信息后提交订单—>支付方式（银行转账或手机扫码均需选择“银
 行转账”）—>上传缴费凭证—>保存（报名成功）。

学生会员1580元，密码学会会员1680元/人，非会员1780元/人。

（1）通过网银转账、银行汇款或现场刷卡方式缴纳

户 名：中国密码学会

开户行：中国工商银行北京万寿路南口支行

账 号：0200 1864 1920 0001 727

（2）手机扫码支付



020086510117

中国密码学会

注 意：网银转账、银行汇款、手机扫码支付的汇款附言或“添加
 备注”中请注明“密码测评2023+姓名”。如多人缴费，请备注全部缴

费人员姓名，增值税普通发票为电子发票发送到邮箱，增值税专用发票为纸质发票。

六、食宿安排

大会推荐入住南宁荔园山庄，地址：广西南宁市青山路22号，酒店协议价(不含早)：大床房470元/天、双床房350元/天，住宿费自理。

酒店预订：会议报名成功后，请通过会议微信推送系统进行预定，网址：<https://h5.xunzhuang.net/h5/U140819VUP3R6>。

入住推荐酒店时需报会议名称才能享受此优惠价，酒店为会议预留房间有限，订满为止，如遇订满请自行预订周边宾馆、快捷酒店。大会统一安排参会人员在南宁荔园山庄凭票用餐（包括早、午和晚餐）。

七、联系人

1.会务联系人：武小年 13077658295 xnwu@guet.edu.cn

李灵琛 17877356228 lilincheng601@126.com

2.财务联系人：梁老师：010-59703687，18600651587

米老师：010-59703687，13718641920

3.酒店预订联系人：凌经理：18977160590

中国密码学会密码测评专业委员会

2023年11月02日

