

中国密码学会 2025 年密码测评学术会议

(CryptoTE 2025)第二轮通知暨会议日程安排

中国密码学会 2025 年密码测评学术会议定于 2025 年 9 月 13 日—14 日在上海市举行。本次会议由中国密码学会密码测评专业委员会主办，智巡密码（上海）检测技术有限公司和上海市商用密码行业协会共同承办。

会议以“数字时代密码全生命周期测评创新与融合”为主题，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共同交流、探讨密码算法、协议、产品和系统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。

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

智巡密码（上海）检测技术有限公司

上海市商用密码行业协会

三、协办单位

北京智芯微电子科技有限公司

豪符密码检测技术(成都)有限责任公司

四、时间地点

报到时间：2025 年 9 月 12 日 15:00—21:00

2025 年 9 月 13 日 08:00—09:00

会议时间：2025 年 9 月 13 日—9 月 14 日

报到地点：上海富悦大酒店一楼签到台（9 月 12 日）

上海富悦大酒店三楼签到台（9 月 13 日）

会议地点：上海富悦大酒店（茸悦路 208 弄（万达广场东侧）-东方
厅（2 号厅））

五、会议议程

2025 年 9 月 13 日（周六）		
时间	报告主题	演讲人
09:00-10:20	开幕式、领导致辞以及合影留念	
10:20-10:40	茶歇	
10:40-11:20	特邀报告：格密码学安全性分析——破解 200 维 SVP 挑战	西交利物浦大学数理学院 丁津泰
11:20-12:00	特邀报告：密码国际化检测认证的挑战，机遇和实践	华为技术有限公司 陈恺
12:00-14:00	午餐，休息	
14:00-14:30	主题报告：密码测评视角下的访问控制漏洞检测技术	复旦大学 张源
14:30-15:00	主题报告：SHA-3 杂凑算法标准安全性分析进展	中国科学院信息工程所 刘美成
15:00-15:30	主题报告：基于可搜索加密的动态用户授权方法研究与分析	西安电子科技大学 樊凯
15:30-16:00	茶歇	
16:00-16:30	主题报告：基于身份加密算法的密钥安全性分析	西安邮电大学 秦宝东
16:30-17:00	主题报告：New Collision Attacks on	华东师范大学 李迎新

	Round-Reduced SHA-512	
17:00-17:30	主题报告：针对 Sphinx+ (SLH-DSA) 后量子算法的故障攻击和防护方法	中国农业大学 李岩
2025 年 9 月 14 日（周日）		
时间	报告主题	演讲人
09:00-09:30	主题报告：探囊取物：基于遗传算法的侧信道碰撞攻击	武汉大学 欧长海
09:30-10:00	主题报告：人工智能赋能密码模块简单能量分析的全自动测评	北京理工大学 王安
10:00-10:30	主题报告：大语言模型驱动的侧信道攻击测试新范式	深圳市纽创信安科技开发有限公司 王宗岳
10:30-11:00	茶歇	
11:00-11:30	主题报告：基于量子效应的随机数发生器故障注入脆弱性评估	北京智芯微电子科技有限公司 刘辉志
11:30-12:00	主题报告：国内外安全芯片标准研究及检测实践	豪符密码检测技术（成都）有限责任公司 饶金涛
12:00-14:00	午餐，休息	
14:00-14:30	特邀报告：针对 ML-DSA (Dilithium) 拒绝采样的侧信道攻击	上海交通大学 郁昱
14:30-15:00	主题报告：商用密码算法上车政策标准研究与检测实践	中汽研软件测评（天津）有限公司 鲍越
15:00-15:30	茶歇	
15:30-16:00	主题报告：低空安全准入检测及黑飞识别接管技术	北京智慧云测设备技术有限公司 徐九八
16:00-16:30	主题报告：多模态大模型和多智能体背景下的安全问题分析	上海交通大学 王烁

16:30-17:00

闭幕式

六、会议注册与缴费

1. 注册费

学生及学生会会员 1580 元/人、密码学会会员 1680 元/人、非会员 1780 元/人。

2. 注册方式

通过中国密码学会会议注册系统在线报名。

网址：<https://cacrmeeting.cacrnet.org.cn/cms/CryptoTE2025/>

二维码：



点击链接或扫描上方二维码→参会注册→确认信息后提交订单→支付方式（在订单页面选择个人缴费、对公转账或现场缴费），注册缴费具体流程见学会网站《中国密码学会活动会议注册缴费流程(试行)》：

<https://www.cacrnet.org.cn/site/content/1619.html>，现场注册同上流程。

注：1. 如选择“对公转账”，工商银行将通过短信发送以 95588 开头的 19 位汇款账号，请提交财务对公汇款，备注密码测评 2025+姓名。

2. 增值税发票将统一发送到注册时登记的电子邮箱中。

七、会议住宿

大会统一安排参会人员富悦大酒店凭票用餐。

大会推荐入住以下酒店：

1) 上海富悦大酒店, 地址: 上海市松江区茸悦路 208 弄 (万达广场东侧), 酒店住宿价格 580 元/天 (含早), 住宿费自理, 订房联系人: 范丽娟, 联系电话: 18157311319。

2) 维也纳酒店(上海松江万达广富林路店), 地址: 上海市松江区中山街道广富林路 255 号 (距离会场 1.2km), 酒店住宿价格双床房 280 元/天 (含早), 豪华大床房 300 元/天 (含早), 住宿费自理, 订房联系人: 许雪艳, 联系电话: 18501713208。

3) 上海松江 m 美玥酒店, 地址: 上海市松江区广富林路 358 弄 (距离会场 0.85km), 酒店住宿价格 350 元/天 (含早), 住宿费自理, 订房联系人: 刘相成, 联系电话: 18736598066。

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。

八、联系方式

1. 会务联系人

吴老师 18289875451

田老师 13818599673

2. 财务联系人

梁老师: 010-59703687, 18600651587

米老师: 010-59703687, 13718641920

中国密码学会密码测评专业委员会

2025 年 8 月 25 日

