

中国密码学会 2023 年安全协议进展国际会议 第二轮通知暨“密码协议实践与挑战”专题 交流报告征集

为促进国内外安全协议领域专家学者的交流与合作，由中国密码学会安全协议专业委员会主办，海南大学网络空间安全学院（密码学院）承办的中国密码学会 2023 年安全协议进展国际会议(PSP2023)将于 9 月 23 日-24 日在海南省海口市举行。会议旨在共同交流、探讨安全协议研究领域最新成果和发展趋势，提高学术研究水平并促进学术界与产业界的相互了解与合作。会议邀请了多名国内外从事相关研究的专家学者做专题报告（见会议日程），涵盖密码协议基础理论、安全多方计算、抗量子密码等内容。

为充分发挥中国密码学会安全协议专业委员会的桥梁纽带作用，加强密码协议学术界和产业界交流，促进产学研用融合发展，本次会议拟增设“密码协议实践与挑战”专题，邀请产业界知名专家共同探讨密码协议应用实践中的最新进展和存在的问题。请有意向在会议上交流发言的企业专家将交流题目简介和报告人信息于 9 月 16 日 24:00 前发送至邮箱 sklc@sklc.org，会议组委会将视情况确定最终交流形式。

我们诚挚邀请您莅临本次会议，共同探讨安全协议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

中国密码学会安全协议专业委员会

二、承办单位

海南大学网络空间安全学院（密码学院）

三、时间地点

报到时间：2023 年 9 月 22 日 15:00-21:00

报到地点：海南大学国际学术交流中心酒店

会议时间：2023 年 9 月 23 日-24 日

会议地点：海南大学国际学术交流中心

四、会议日程

9 月 23 日（周六）	
时 间	内 容
9:00-9:30	领导致辞&合影留念
9:30-10:20	报告人：刘胜利（上海交通大学） 报告题目：基于哈希证明系统的公钥密码构造及其紧致安全
10:40-11:30	报告人：喻杨（清华大学） 报告题目：基于格陷门的数字签名
14:00-14:50	报告人：郁昱（上海交通大学） 报告题目：最优编码的（基于哈希）后量子数字签名算法设计
14:50-15:40	报告人：赖俊祚（暨南大学） 报告题目：Robust Publicly Verifiable Covert Security: Limited Information Leakage and Guaranteed Correctness with Low Overhead

16:00-16:50	报告人：薛海洋（香港理工大学） 报告题目：门限 ECDSA 数字签名的发展与现状
9 月 24 日（周日）	
8:40-9:30	报告人：刘天任（北京大学） 报告题目：如何混淆代数电路
9:30-10:20	报告人：张秉晟（浙江大学） 报告题目：Endemic Oblivious Transfer via Random Oracles, Revisited
10:40-11:30	报告人：张亮（海南大学） 报告题目：基于属性密码的分布式安全协议研究
14:00-16:00	密码协议实践与挑战专题论坛
会议结束	

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：
<https://cacr2023.cacrnet.org.cn/fair/38>，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）

缴费：学生及密码学会会员 1800 元/人，非会员 2000 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“安全协议+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、会议住宿

1. 会议统一安排在海南大学国际学术交流中心用午餐及晚餐，推荐海南大学国际学术交流中心酒店住宿，根据您提供的注册信息会务组代为预订海南大学国际学术交流中心酒店的住宿房间，住宿费自理。

会议期间国际合作交流中心酒店协议价：标准间 350 元/天（含双早餐）、大床房 350 元/天（含早餐）

2. 会议报名成功后即可在会议系统进行酒店预订，网址：<https://cacr2023m.cacrnet.org.cn/hotel-list.html?id=38>。

注意：会议报名成功才能预订推荐酒店，享受优惠价。酒店为会议预留房间有限，订满为止。如预订周边宾馆、快捷酒店等，请自行预订。

七、联系方式

1、会务联系人:

马老师: 13368946867, hdmjq@hainanu.edu.cn

2、财务联系人:

梁老师: 010-59703687, 18600651587

米老师: 010-59703687, 13718641920



中国密码学会安全协议专业委员会

2023年9月12日