

2021 第十四届中国密码学会年会 议程

日期	时间	会议内容	主持人
12月3日	9:00-21:00	注册报到	
	18:00-18:30	中国密码学会 2021 年第五次党委会	安晓龙
	18:30-20:00	中国密码学会四届二次理事会	王小云
12月4日	7:30-8:30	注册报到	
	8:30-9:30	1. 国家密码管理局领导致辞 2. 贵州密码管理局领导致辞 3. 中国密码学会领导致辞 4. 贵州大学领导致辞 • 线下会议室：贵阳群升豪生大酒店百花厅 北京会场 • 线上会议室：直播	彭长根
		密码创新奖、学会奖和优博颁奖	安晓龙
		合影	
		特邀报告 线下会议室：贵阳群升豪生大酒店会议中心百花厅 北京会场 线上会议室：直播	
	9:30-10:10	报告题目：密码技术与区块链 报告人：王小云 清华大学 报告方式：线上	陈克非
	10:10-10:20	茶歇	
	10:20-11:10	报告题目：A Decade (or So) of Fully Homomorphic Encryption 报告人：Craig Gentry 报告方式：线上	陈克非
	11:10-12:00	报告题目：安全协议：理论与实践 报告人：冯登国 北京信息科学技术研究院 报告方式：线上	
	12:00-14:00	午餐（西餐厅）	
	14:00-15:00	报告题目：A New Theory of Adversarial Examples in Machine Learning 报告人：Adi Shamir 报告方式：线上	王小云
	15:00-15:50	报告题目：On deck functions 报告人：Joan Daemen 报告方式：线上	
	15:50-16:00	茶歇	
	16:00-16:50	报告题目：待定 报告人：翁健 暨南大学 报告方式：线下（贵阳会场）	吴文玲
	16:50-17:40	报告题目：Learning Parity with Noise: Constructions, Reductions, and Analyses 报告人：郁昱 上海交通大学 报告方式：线上	
	17:40-19:30	晚餐（特色餐厅）	
	20:00-21:30	自由论坛	高飞

日期	时间	会议内容	时间	会议内容
12月5日	08:30-11:50	优秀青年学者论坛	8:30-11:50	密码学前沿交叉论坛
	12:00-14:00	午餐（西餐厅）		
	14:00-17:30	论文报告论坛	14:00-17:30	密码产业技术论坛
	17:30-17:40	闭幕式 主持人：王小云 线下会议室：贵阳群升豪生大酒店会议中心百花厅 北京会场 线上会议室：直播		
12月6日	全天	会议疏散		

注：12月4日晚上自由论坛，欢迎全国密码领域的学者与工程技术人员自由报名交流最近个人研究、开发成果，交流疑惑或问题。报名信息小程序见会议手册附录。

分论坛议程

优秀青年学者论坛			
线下会议室：贵阳群升豪生大酒店会议中心百花厅 线上会议室：直播			
日期	时间	会议内容	主持人
12月5日	8:30-9:00	报告题目：基于SM9的功能型密码 报 告 人：黄欣沂 福建师范大学 报告方式：线上	谷大武
	9:00-9:30	报告题目：密钥封装机制：多用户安全性及紧致安全规约 报 告 人：韩帅 上海交通大学 报告方式：线上	
	9:30-10:00	报告题目：密码协议的博弈论分析与设计 报 告 人：田有亮 贵州大学 报告方式：线下（贵阳会场）	
	10:00-10:20	茶歇	
	10:20-10:50	报告题目：MITM Meets Guess-and-Determine: Further Improved Preimage Attacks against AES-like Hashing 报 告 人：史丹萍 中国科学院信息工程研究所 报告方式：线上	谷大武
	10:50-11:20	报告题目：基于格的高效公钥算法设计 报 告 人：张江 密码科学技术国家重点实验室 报告方式：线上	
	11:20-11:50	报告题目：云数据安全共享理论与方法研究 报 告 人：沈剑 南京信息工程大学 报告方式：线下（贵阳会场）	
	11:50-14:00	午餐（西餐厅）	

密码学前沿交叉论坛

线下会议室：贵阳群升豪生大酒店会议中心西江厅

线上会议室：直播

日期	时间	会议内容	主持人
12月5日	8:30-9:00	报告题目：人工智能安全中的密码学 报 告 人：仲盛 南京大学 报告方式：线上	徐茂智
	9:00-9:30	报告题目：待定 报 告 人：郑志彬 华为 报告方式：线上	
	9:30-10:00	报告题目：新型电力系统大数据安全探讨 报 告 人：李智虎 电科院 报告方式：线上	
	10:00-10:20	茶歇	
	10:20-10:50	报告题目：密码与芯片 报 告 人：刘雷波 清华大学 报告方式：线下（贵阳会场）	徐茂智
	10:50-11:20	报告题目：SecureNLP：具有隐私保护的多方自然语言处理系统 报 告 人：何德彪 武汉大学 报告方式：线下（贵阳会场）	
	11:20-11:50	报告题目：待定 报 告 人：矩阵元技术有限公司 报告方式：线上	
	11:50-14:00	午餐（西餐厅）	

论文报告论坛

线下会议室：贵阳群升豪生大酒店会议中心百花厅

线上会议室：直播

日期	时间	会议内容	主持人
12 月 5 日	14:00-14:20	报告题目：RCCA安全公钥加密方案的匿名性研究 报 告 人：王毅 国防科技大学 报告方式：线上	戚文峰
	14:20-14:40	报告题目：Half-Gates电路混淆方案实际安全性：攻击与改进 报 告 人：郭淳 山东大学 报告方式：线上	
	14:40-15:00	报告题目：Fine-Grained Secure Attribute-Based Encryption 报 告 人：王煜宇 电子科技大学 报告方式：线上	
	15:00-15:20	报告题目：Meet-in-the-Middle Attacks Revisited: Key-recovery, Collision, and Preimage Attacks 报 告 人：董晓阳 清华大学 报告方式：线上	
	15:20-15:30	茶歇	
	15:30-15:50	报告题目：New Lattice Two-Stage Sampling Technique and its Applications to Functional Encryption Stronger Security and Smaller Ciphertexts 报 告 人：来齐齐 陕西师范大学 报告方式：线上	
	15:50-16:10	报告题目：Differential-Linear Cryptanalysis from an Algebraic Perspective 报 告 人：刘美成 中国科学院信息工程研究所 报告方式：线上	

16:10-16:30	报告题目： 定向口令猜测 报 告 人： 汪定 南开大学 报告方式： 线上	戚文峰
16:30-16:50	报告题目： Towards lightweight, privacy-preserving cooperative object classification and detection for CAV 报 告 人： 熊金波 福建师范大学 报告方式： 线下（贵阳会场）	
16:50-17:10	报告题目： Cloud-Aided Scalable Revocable Identity-Based Encryption with Ciphertext Update from Lattices 报 告 人： 张彦华 郑州轻工业大学 报告方式： 线上	
17:10-17:30	报告题目： 国际三大密码会议的知识图谱构建 报 告 人： 焦小彤 中国科学院大学 报告方式： 线上	

密码产业技术论坛

线下会议室：贵阳群升豪生大酒店会议中心西江厅
 线上会议室：直播

日期	时间	会议内容	主持人
12月5日	14:00-14:30	报告题目：量子计算在密码分析中的应用 报 告 人：高飞 北京邮电大学 报告方式：线上	彭长根
	14:30-14:50	报告题目：待定 报 告 人：兴唐 报告方式：线上	
	14:50-15:10	报告题目：密码学与云计算技术应用实践 报 告 人：王勇 西安得安信息技术有限公司 报告方式：线上	
	15:10-15:30	茶歇	
	15:30-16:00	报告题目：视觉情报挖掘 报 告 人：操晓春 中山大学 报告方式：线上	彭长根
	16:20-16:50	报告题目：云计算与数据安全 报 告 人：沈玉龙 西安电子科技大学 报告方式：线下（贵阳会场）	
	16:50-17:10	报告题目：新一代云密码服务方案和应用实践 报 告 人：朱家雄 江南天安 报告方式：线上	
	17:10-17:30	报告题目：待定 报 告 人：卫士通 报告方式：线上	



线上直播二维码



自由论坛报名信息采集小程序