

中国密码学会 2022 年密码测评学术会议 征文通知

由中国密码学会密码测评专业委员会主办，浙江大学网络空间安全学院承办的中国密码学会 2022 年密码测评学术会议（CryptoTE 2022）定于 2022 年 11 月 12 日至 2022 年 11 月 13 日在杭州举行（会议地点：浙江大学杭州国际科创中心会议大厅）。

会议旨在促进以密码为安全支撑的新网络安全的体系设计、环境构建和文明建设，促进数字化、网络化、智能化转型升级，推动“十四五”密码科技高质量发展。会议将聚焦新型密码分析测评学术交流、技术研究、应用推进和发展趋势，为“产”“学”“研”“用”“测”等方向的人才提供学术技术交流平台，共同探讨新时代密码分析测评技术的发展，推动密码与数字经济、新基建、新技术等领域的深度融合与发展。

本次会议拟邀请多名学术界、产业界和评测机构的知名专家做专题报告，并面向全国征集学术论文。征稿范围包括但不限于以下议题：

1、密码算法测评理论和技术：随机数发生器测评；新型密码算法的测评方法；基于人工智能的密码安全性分析方法和技术等。

2、密码产品测评方法和技术：密码芯片分析技术；密码模块安全性测评分析技术等。

3、隐私计算安全性分析方法：针对多方安全理论等实现的安全分析研究和技术等。

4、密码应用及系统的测评方法和技术：区块链、物联网、车联网、智慧城市、5G、智慧医疗等应用场景的密码安全要求和测评方法；工控网络安全测评技术和方法；密码系统中针对密码应用合规、正确、有效的自动化测评技术；密码系统健壮性测评方法和技术等。

5、新型密码组件技术：物理不可克隆函数（PUF）；白盒密码等。

6、密码实现的形式化分析和自动化验证技术：密码算法软件、硬件和系统等实现的形式化分析和自动化验证技术。

本次会议的投稿论文可以是已向其他学术期刊或会议投稿的论文成果，或新近发表的研究成果，论文不限长度。会议将编辑学术年会论文集（不正式出版，允许再投稿），并评选会议最佳论文、优秀论文，论文集根据作者意愿刊登全文或摘要。对于本次会议投稿论文，根据作者意愿推荐至密码学报、通信学报刊登，欢迎各位踊跃投稿！

投稿方式：投稿论文请以说明+附件形式 Email 投稿至 cryptote2022@163.com。邮件名称应写 CryptoTE 2022-投稿论文，邮件正文中请注明作者基本信息（隶属单位、职称、学历学位、研究兴趣）和文章联系人及联系方式，已在其他刊物或会议发表的论文请注明，并注明是否愿意在会议内部交流资料中刊登全文或摘要等。

截稿日期：2022 年 10 月 23 日

会议审稿通知：2022 年 10 月 29 日

论文定稿：2022 年 11 月 4 日

会议时间：2022 年 11 月 12 日至 2022 年 11 月 13 日

会议地点：杭州

论文联系人：王小航（15014182716）；沈浩颀（17321355766）；
杨 坤（15267427696）

E-mail:Cryptote2022@163.com

会议联系人：张 帆（13777356409）

E-mail:fanzhang@zju.edu.cn

中国密码学会密码测评专业委员会

2022 年 10 月 8 日

