计 算 机 学 院

庆祝建校 110 周年系列学术报告

报告题目：恶意网络环境下区块链共识协议的设计

报 告 人：徐静，研究员、博导，中科院软件所

时　　间： 2019.5.28 上午 10:00

地　　点：计算机楼 B518

个人简介：

徐静，中国科学院软件研究所研究员、博导，中国密码学会安全协议专业委员会委员，长期从事应用密码学与安全协议研究。曾主持国家自然科学基金、国家科技支撑项目课题、国家信息安全战略研究与标准制定专项、国家密码发展基金等项目，在 IEEE S&P (Oakland)、IEEE Trans. TDSC 等国际重要会议和 CCF A 类刊物上发表论文 50 余篇，出版著作和译著 2 部，起草国家标准 2 项。传输层安全标准 TLS

的分析工作被互联网工程任务组 IETF 在标准中引用，以论证其下一代 TLS 标准的安全性。近年来专注于区块链密码研究，曾在美国康奈尔大学数字货币研究中心 IC3 访学一年。

报告摘要：区块链是随着比特币等数字加密货币的日益普及而逐渐兴起的一种全新的去中心化基础架构与分布式计算范式。共识协议解决了区块链如何在分布式场景下达成一致性的问题，是区块链的核心基础。本报告首先介绍区块链的基本安全性质，然后介绍两种典型的区块链共识协议—基于工作量证明的共识协议和基于权益证明的共识协议，最后介绍我们在恶意网络环境下区块链共识协议设计方面的研究进展。

欢迎广大师生参加！