中国密码学会2019年福建会员日活动通知

由中国密码学会组织工作委员会主办，莆田学院、应用数学福建省高校重点实验室联合承办的中国密码学会2019年福建会员日活动将于2019年12月21日在福建省莆田市举行。此次会员日活动旨在促进中国密码学会会员之间的交流，探讨密码前沿技术和密码创新发展，促进密码研究和应用。届时将邀请专家学者做密码学专题报告。现将活动有关事项通知如下：

一、主办单位：中国密码学会组织工作委员会

二、承办单位：莆田学院、应用数学福建省高校重点实验室

三、活动时间：2019 年 12 月 21 日

08:30~12:00 学术交流

14:00~17:00 会员（单位）交流

四、活动地点：莆田学院

五、特邀报告(报告简介见附件)

1、报告题目：密码学与区块链的相互推进

报告专家：来学嘉，中国密码学会理事，上海交通大学教授

2、报告题目：中国编码学历史和现状

报告专家：丁存生，香港科技大学教授

3、报告题目：量子密码简介

报告专家：高飞，中国密码学会组织工作委员会委员，北京邮电大学教授

六、会议费用：本次活动免收注册费。参会者食宿、交通费自理。

七、会议注册：各位参会人员请在2019年12月10日前填写参会回执。

八、会议报到酒店：海源国际大酒店（莆田市区）。

九、会务组联系方式：

总负责人：陈智雄，13515932597，ptczx@126.com；

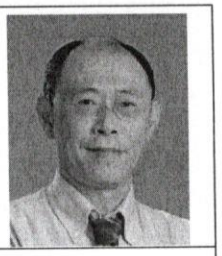
会议注册：吴晨煌，13599896761，ptuwch@163.com；

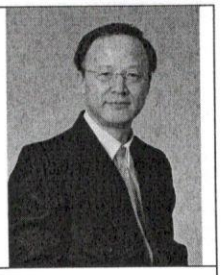
中国密码学会

2019 年 11 月 20 日

附件：

特邀报告简介

特邀报告 1	
报告专家	来学嘉教授，上海交通大学
报告题目	密码学与区块链的相互推进
报告摘要	随着比特币等数字货币的兴起，区块链成了一个热门课题。本报告介绍比特币系统如何使用密码算法实现了交易，记账，货币的发行与控制；讨论区块链技术对密码学的实质贡献：通过由区块链实现的可信第三方，完善了密码学的抗抵赖，抗捏造功能。从密码学角度探讨区块链的实际应用场景。
专家简介	来学嘉，1982 年获西北电讯工程学院学士学位，1984 年获应用数学硕士学位，1992 年获得瑞士苏黎世高工技术科学博士学位。现任上海交通大学教授、博导。从事密码学和信息安全工作 30 多年。设计了 IDEA 加密算法，被用于多个国际标准如 ISO,TLS,PGP 等。在密码分析中，提出差分，高阶差分，马尔科夫密码的概念，对 Hash 函数的研究成果得到国际上普遍应用。提出 DNA 公钥密码及离散对数的 DNA 算法。设计了 SM4，AES 的白盒密码实现。出版了《分组密码的设计和安全》专著并发表论文 100 多篇。曾任亚密指导委员会主席，亚密会，AsiaCCS 2012, ISC 等 10 个国际学术会议主席或程序委员会主席。期刊 JCST，JISE 编委。

特邀报告 2	
报告专家	丁存生教授，香港科技大学
报告题目	中国编码学历史与现状
报告摘要	编码学在密码学中有重要的应用。例如，线性码可以用来构造公钥密码体制，认证码和秘密共享体制。此外，MDS 码用于设计 AES 的一个建筑模块。目前基于编码的密码体制的研究是密码学的一个热点。编码学有 70 多年的历史。我国的编码学虽然起步较晚，但是近 15 年取得了长足进步。本报告的目的对中国的编码学历史和现状给国内密码学届同行做个简单介绍。希望能促进编码学和密码学研究人员的合作和交流。
专家简介	丁存生博士受教育于陕西师范大学物理系，西北电讯工程学院应用数学系，德国 Karlsruhe 大学计算机系，芬兰 Turku 大学数学系及 Turku 计算机科学中心。在新加坡国立大学计算机系任助理教授三年。从 2000 年至今在香港科技大学计算机科学及工程系任教。他于 1996 年任英国剑桥大学牛顿数学科学研究所研究员，2001 年任新加坡国立大学数学科学研究所高级研究员. 丁存生教授的科研方向包

	括密码学，信息安全，编码学，组合设计和有限几何。

特邀报告 3		
报告专家	高飞教授，北京邮电大学	
报告题目	量子密码简介	
报告摘要	随着人们计算能力的快速发展，特别是量子算法的提出，传统密码的安全性受到了严峻挑战。量子密码的安全性基于物理原理，与攻击者的计算能力无关，现在已经引起了广泛关注。量子力学的特有性质使得用户可以发现潜在的窃听行为，甚至允许用户使用不可信的设备来产生安全密钥。报告将从量子密码的研究背景开始，重点介绍 BB84 量子密钥分配（QKD）协议和设备无关协议的基本思想，以及其它量子密码协议的发展现状和实验进展。	
专家简介	高飞，北京邮电大学教授，中国密码学会组织工作委员会、青年工作委员会委员，中国电子学会量子信息分会委员会委员。2007 年毕业于北京邮电大学，获密码学博士学位。主要研究量子密码与量子算法，已在 PRL/PRA 等重要期刊发表论文 40 余篇，SCI 总他引 2600 余次，H 因子 36。2016 年入选青年长江学者。	