全同态加密前沿学术论坛通知

中国密码学会密码算法专业委员会、中国密码学会青年工作委员会将于 2014 年 6 月 3-4 日在北京联合举办“全同态加密前沿学术论坛”。本次论坛由中国科学院软件研究所可信计算与信息保障实验室、重庆大学信息物理社会可信服务计算教育部重点实验室承办。

同态加密的思想是由密码学家 Rivset、Adleman 和 Dertouzos 提出来的，可解决数据和操作委托给第三方时的安全问题。全同态加密的构造问题困扰了人们 30 余年，直到 2009 年 Craig Gentry 设计了第一个全同态加密体制，在理论上解决了这一问题。全同态加密成为近年来密码研究热点之一。

本次论坛邀请了 IBM Watson 研究中心 Craig Gentry 研究员、ShaiHalevi 研究员、Cincinnati 大学 Jintai Ding 教授等人做主题报告。论坛旨在通过与全同态加密顶尖研究学者零距离接触，深入交流全同态加密和格密码的设计思想与最新进展，分析全同态加密研究面临的问题和技术挑战，探讨全同态加密的发展方向，促进全同态加密和格密码的研究与应用。

欢迎关注全同态加密和格密码研究与应用的有关人员参加此次论坛！

主办单位：中国密码学会密码算法专业委员会、青年工作委员会

承办单位：中国科学院软件研究所可信计算与信息保障实验室
重庆大学信息物理社会可信服务计算教育部重点实验室

会议时间：2014 年 6 月 3-4 日

会议地点：中国科学院软件研究所

会议注册：

1、参会人员请填写附件注册单，并于 5 月 25 日前发送至会议邮箱（tca-conferences@tca.iscas.ac.cn）。

2、参会人员须缴纳注册费： 600 元/人。

3、 注册费缴纳可以选择以下方式之一：

(1) 银行汇款（请在 5 月 25 日之前（含）汇出）。

开户名：中国科学院软件研究所

开户银行： 工商银行北京市分行海淀西区支行

帐号： 0200004509088122880

附言：同态加密前沿论坛+姓名

（2）现场缴费：会议首日 12：30 -- 14：00 在会场注册台缴纳现金或支票（限开户行在北京，勿折）。

如通过银行汇款，请将汇款凭证扫描件发送至会议邮箱，凭身份证可在会议报到当天领取注册费发票。现场缴费者可在会后两周内收到邮寄的注册费发票。会议对部分博士生免收注册费，如果需要请在返回注册单时申请。

会议住宿：本次会议不提供统一住宿，京外参会者请自行解决，也可联系北京物科宾馆或者莫泰 168 中关村店。

联 系 人：秦益，tca-conferences@tca.iscas.ac.cn，010-62661700

会议网址：http://tca.iscas.ac.cn

附：注册表和议程

中国密码学会密码算法专业委员会

中国密码学会青年工作委员会

2014 年 5 月 14 日

附件一:注册表

全动态加密前沿论坛注册表	
姓名	
所在单位	
联系电话	
邮箱	
注册方式	□ 银行汇款　　□ 现场缴费

附件二：“全同态加密前沿学术论坛”议程

日期	时间	内容
6 月 3 日	12:30-14:00	会议注册
	14:00-15:00	Craig Gentry（IBM Watson 研究中心） Constructions of Fully Homomorphic Encryption (I)
	15:00-15:20	茶歇
	15:20-16:20	Craig Gentry（IBM Watson 研究中心） Constructions of Fully Homomorphic Encryption (II)
	16:20-16:40	茶歇
	16:40-17:40	Craig Gentry（IBM Watson 研究中心） Constructions of Fully Homomorphic Encryption (III)
	18:00-19:30	晚餐
6 月 4 日	9:00-10:00	ShaiHalevi（IBM Watson 研究中心） Advances inFully Homomorphic Encryption (I)
	10:00-10:20	茶歇
	10:20-11:20	ShaiHalevi（IBM Watson 研究中心） Advances inFully Homomorphic Encryption (II)
	11:20-11:40	茶歇
	11:40-12:40	ShaiHalevi（IBM Watson 研究中心） Advances inFully Homomorphic Encryption (III)
	12:40-14:00	午餐
	14:00-15:00	Jintai Ding（Cincinnati 大学） Lattice-based Cryptography I
	15:00-15:20	茶歇
	15:20-16:20	Jintai Ding（Cincinnati 大学） Lattice-based Cryptography II
	16:20-16:40	茶歇
	16:40-17:40	Jintai Ding（Cincinnati 大学） Lattice-based Cryptography III
	18:00-19:00	晚餐