清华大学高等研究院

Institute for Advanced Study, Tsinghua University

密码学学术报告 Cryptology Seminars

Title: 密码安全的新方向

Speaker: 曹珍富 （华东师范大学特聘教授）

Time: 9:30am, Friday, June 5, 2015

Venue: Conference Hall 322, Science Building, Tsinghua University

报告摘要:

随着移动互联网、下一代互联网、物联网、云计算、命名数据网、大数据等为代表的新型网络形态及网络服务的兴起，安全需求方式已经由通信双方都是单用户向至少有一方是多用户的方式转变。本报告论述了密码安全是网络安全核心发展方向，阐述了“应用需求”是密码安全研究的出发点。依据“应用需求”，密码安全由传统的仅考虑信道安全向“信道安全+”方向发展，说明了涉及“多方”的密码安全产生的特点，说明云计算、未来网络、大数据等应用模式对现代密码学提出了新的要求，产生了新的密码学原语和新的安全性模型。在此基础上，本报告介绍了这些密码学原语的主要进展，重点介绍了可追踪、可撤销、多权威机构、有界密文政策的属性基加密（ABE）问题和与位置相关的区间加密问题的研究和解决情况。最后，介绍了这些成果的应用，包括这些密码学原语的芯片研制、芯片应用，重点介绍了加密数据访问控制类应用和基于生物信息的身份鉴别类应用。

报告人简介:

曹珍富，国家杰出青年基金获得者，享受国务院特殊津贴。现任华东师范大学特聘教授，第十二届上海市政协常委。作为第一完成人或独立完成人获得教育部自然科学一等奖等省部级奖7项。从1981年开始发表学术论文以来，已在各种学术期刊、会议上发表400余篇高质量学术论文，SCI检索150余篇，EI检索260余篇，引用超过6000次，出版专著7部（包括1部CRC出版的英文专著）、主编（或副主编）全国教材两部，先后担任SCI国际期刊Computers & Security 、Fundamenta Informaticae、Peer-to-Peer Networking and Applications、Security and Communication Networks、IEEE Transactions on Parallel and Distributed Systems和Wireless Communications and Mobile Computing等的副主编、编委或客座编辑。主持完成国家或省部级科研项目50余项，包括国家自然科学基金A3前瞻计划项目、重点项目、杰出青年基金项目等重要科研项目。在高校执教30余年里，为国家有关部门科研人员、中科院和众多高校作邀请报告100余次，参与制定相关国家标准10余项，历任国家自然科学基金专家评审组成员、国家自然科学奖评委、中国科学院杰出成就奖评委、国家重点实验室评估专家等。