2019年物联网安全高峰论坛

程 序 册

主办单位：安徽省物联网安全技术工程实验室
安徽省计算机学会

承办单位：安徽大学计算机科学与技术学院

安徽 合肥

2019年11月13-14日

论坛背景

随着 5G 移动通信的全球商用部署，移动互联网及物联网业务呈指数式增长。5G 移动通信系统传输带宽更大且时延更低，以 5G、云计算、边缘计算、区块链、大数据等为代表的新一代信息技术正在全面融合于物联网中，加速推进云-边-端的智能融合，催生新型物联网系统架构。在新型物联网中，终端设备海量连接且类型混杂，网络形态更加异构多元，安全边界更加模糊，产生的数据将呈爆炸式增长，云-边-端协同的数据安全和隐私保护问题是亟需解决的关键问题之一。

2019 年物联网安全高峰论坛将邀请物联网与信息安全领域的国内顶级专家和学者，分享物联网与数据安全的学术成果，旨在为突破新型物联网安全的核心关键技术提供有益的思考和方向。

本次论坛汇聚了从事网络与信息安全理论及应用研究的科研人员，广泛开展学术交流，研究发展战略，共同促进相关理论、技术及应用的进一步发展。本次论坛有幸邀请到杨波教授（陕西师范大学）、徐宏力教授（中国科学技术大学）、陈晓峰教授（西安电子科技大学）、禹勇教授（陕西师范大学）、于佳教授（青岛大学）与会做数场特邀报告。

预祝本次论坛圆满成功！

2019 年“物联网安全高峰论坛”日程安排

会议时间：2019 年 11 月 13 日—11 月 14 日

会议地点：安徽大学磬苑校区行知楼负一层报告厅

安徽大学磬苑校区理工 D 楼 108 会议室

主办单位：安徽省物联网安全技术工程实验室

安徽省计算机学会

计算智能与信号处理教育部重点实验室

承办单位：安徽大学计算机科学与技术学院

会议日程：

<table>
<tr><td></td><td>时间</td><td colspan="2">议程</td><td>主持人</td></tr>
<tr><td>11 月 13 日
上午</td><td colspan="4">报 到 （安徽大学磬苑校区）</td></tr>
<tr><td rowspan="6">11 月 13 日
下午</td><td colspan="4">论坛专题报告（理工 D 楼 108 会议室）</td></tr>
<tr><td>时间</td><td>报告人</td><td>报告题目</td><td rowspan="5">仲 红
教授</td></tr>
<tr><td>14:00-14:40</td><td>杨波 教授
（陕西师范大学）</td><td>损耗陷门函数及应用</td></tr>
<tr><td>14:40-15:20</td><td>徐宏力 教授
（中国科学技术大学）</td><td>软件定义网络高效流表管理研究</td></tr>
<tr><td>15:20-15:40</td><td colspan="2">茶歇</td></tr>
<tr><td>15:40-16:20</td><td>陈晓峰 教授
（西安电子科技大学）</td><td>可搜索加密技术</td></tr>
<tr><td rowspan="4">11 月 14 日
上午</td><td colspan="4">论坛专题报告（理工 D 楼 108 会议室）</td></tr>
<tr><td>9:00-9:40</td><td>禹勇 教授
（陕西师范大学）</td><td>基于区块链的安全协议设计</td><td rowspan="2">陈志立
教授</td></tr>
<tr><td>9:40-10:20</td><td>于佳 教授
（青岛大学）</td><td>Towards Achieving Keyword Search over Dynamic Encrypted Cloud Data with Symmetric-Key based Verification</td></tr>
<tr><td>10:20-12:00</td><td colspan="3">自由讨论、实验室参观</td></tr>
</table>

论坛报告 1

题　目：损耗陷门函数及应用

报告人：杨波 教授（陕西师范大学）

摘要：损耗陷门函数是现代密码学中的重要工具，报告首先介绍损耗陷门函数的定义，然后介绍损耗陷门函数在 CCA 安全的公钥加密方案及不经意传输协议中的应用，最后介绍损耗陷门函数在抗泄漏密码学中的应用。

报告人简介：陕西师范大学计算机科学学院二级教授、博士生导师，陕西省百人计划特聘教授，中国密码学会理事，中国密码学会密码算法专业委员会委员，《密码学报》编委。

1986 年获北京大学数学系学士学位，1993 年获西安电子科技大学计算机系计算机软件硕士学位，1999 年获西安电子科技大学通信工程学院密码学博士学位。1986 年至 2005 年在西安电子科技大学工作，2005 年至 2011 年在华南农业大学信息学院、软件学院工作，任院长。2011 年起在陕西师范大学计算机科学学院工作。

已主持国家重点研发项目、国家自然科学基金、“863”计划、国家密码发展基金等项目 20 余项。发表学术论文 200 余篇，其中被三大检索收录 100 余篇，出版学术著作及教材 6 部。

论坛报告 2

题　目：软件定义网络高效流表管理研究

报告人：徐宏力 教授（中国科学技术大学）

摘要：软件定义网络（Software Defined Network，SDN）控制平面通过流表的操作实现对数据平面的集中式管理。然而，SDN 交换机流表大小有限，对系统可扩展性提出了严峻挑战。为此，我们面向不同的网络场景设计了不同的流表管理方案，从而解决 SDN 可扩展性问题。针对网络流动态场景，结合传统的分布式路由和 SDN 集中式控制机制，设计了一种基于混合交换的流表部署方案（Infocom17，TON18）；针对大规模网络场景，提出了结合组表与流表的默认路径部署机制（ICNP17. TON18）；针对 Middlebox 网络场景，设计了基于标签和默认路径的 SAFE-ME 架构（ICNP19）。小规模的测试床验证以及大规模的仿真实验均表明我们提出的方案相比现有算法可以极大地提高网络可扩展性。

报告人简介：徐宏力，男，特任教授，博士生导师，国家优青基金获得者，现任中国科学技术大学计算机科学与技术学院党委书记。2002 获中科大计算机科学与技术学士学位，2007 年获中科大计算机软件与理论专业博士学位，2018 年在美国佛罗里达大学访问研究。主要研究方向为软件定义网络、边缘计算和物联网等。近年来，作为负责人主持了国家基金委优青/面上/青年基金（共 4 项）、博士后特别资助及博士后基金（一等）等项目。作为第一/通信作者在 IEEE/ACM Trans.及 CCF A 类会议发表论文 20 余篇，获授权专利 30 多项。获得过省科技进步二等奖及 ICNP、CWSN 等会议的最佳论文奖或提名。

论坛报告 3

题　目：可搜索加密技术

报告人：陈晓峰 教授（西安电子科技大学）

摘要: 近年来越来越多的用户选择将自己的数据存储到云服务器上，从而享受云存储带来的便利，减轻本地存储管理成本和维护负担。而使用云存储服务，用户会失去对数据的直接控制，数据可能会遭受恶意敌手的攻击窃取。为了保护数据的安全性，用户在外包数据之前往往会对数据进行加密，这对实现数据搜索功能带来了困难。使用可搜索加密技术，用户可以根据查询的关键词陷门，提取出感兴趣的密文文件。本报告主要讲述云环境下可搜索加密协议的研究与进展。

报告人简介：陈晓峰，教授，国家万人计划科技创新领军人才，教育部青年长江学者，互联网基金会网络安全优秀教师。主要研究领域为密码学和云计算安全，已在重要国际会议和期刊发表学术论文 100 余篇，包括 IEEE trans. 系列期刊论文 30 多篇；主持和完成国家自然科学基金等 10 多项科研项目；担任 IEEE TDSC 等著名国际期刊的编辑，AisaCCS 2016、NSS 2014 等多个国际会议的大会主席。获 2016 年度中国密码学会密码创新奖和陕西省青年科技奖。

论坛报告 4

题目：基于区块链的安全协议设计

报告人：禹勇 教授（陕西师范大学）

摘要：区块链技术被认为是 21 世纪最具革命性的技术之一，受到学术界和工业界的广泛关注。区块链作为一种技术创新，为许多行业带来了新的范例。区块链由于其众多优点而具有许多潜在的应用，本报告首先介绍区块链的基础知识及工作原理，然后介绍区块链在多种场景下的应用，包括去中心化的电子投票、去中心化外包存储、可监管密码货币等。

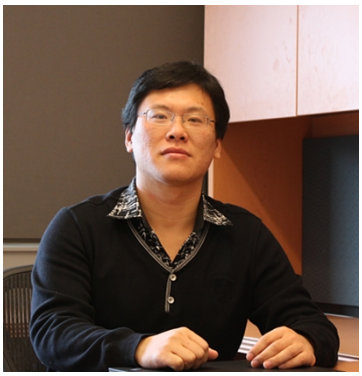
报告人简介：禹 勇 教授，博士生导师，陕西省百人计划特聘教授，中国密码学会高级会员，中国密码学会青年工作委员会委员，中国密码学会协议专业委员会委员，中国密码学教育与科普委员会委员，中国中文信息学会大数据安全与隐私保护专委会委员，Soft Computing 和网络与信息安全学报编委。2008 年获西安电子科技大学密码学博士学位。曾在电子科技大学、澳大利亚 Wollongong 大学工作。主要研究方向为公钥密码理论及应用、区块链与密码货币、云计算安全、大数据安全与隐私保护。在 IEEE Trans on Information Forensics and Security, IEEE Trans on Dependable and Secure Computing, IEEE Trans on Parallel and Distributed System， IEEE Trans on Service Computing， IEEE Trans on Industrial Informatics, IEEE Communications Magazine, IEEE Wireless Communications，IEEE Network, IEEE IoT Journal 等国内外期刊录用\发表学术论文 100 余篇。网络空间安全重点研发计划子课题负责人，主持国家自然科学基金面上项目、青年基金项目和国际合作项目 4 项。国际会议 FCS2019, ProvSec 2017, CS 2015，LSNS 2014 等大会主席，30 多个国内外期刊和学术会议审稿人。

论坛报告 5

题　　目：Towards Achieving Keyword Search over Dynamic Encrypted Cloud Data with Symmetric-Key based Verification

报告人：于佳　教授（青岛大学）

摘要：云计算已经成为重要的信息技术设施，支撑国家各个重大行业，提供智慧大脑功能。传统的网络安全问题在云计算中依然存在，因云计算体系结构变化导致其面临更加严峻的安全挑战。针对云计算安全需求，探讨云端程序逻辑机密性、执行过程完整性、运算结果完备性等安全保障机制；针对云数据安全，探讨云端数据加密、密文操作、多域数据受控共享等安全机制。



报告人简介：于佳，博士，教授，博士生导师，青岛大学计算机科学技术学院副院长，网络空间安全研究所所长，大数据技术与智慧城市研究院常务副院长，青岛大学信息安全方向学术带头人、网络空间安全学科负责人。研究兴趣：密码学理论及应用、云计算安全、大数据安全、无线网络安全。现为中国密码学会学术工作委员会委员、中国密码学会高级会员、中国计算机学会高级会员、山东省计算机学会理事、青岛市大数据发展促进会副理事长、青岛市计算机学会网络与信息安全专委会主任。近年来主持国家自然科学基金项目 3 项、国家密码发展基金 2 项，承担其他各类科研项目 20 余项。在《IEEE Transactions on Information Forensics and Security》、《IEEE Transactions on Dependable and Secure Computing》、《IEEE Transactions on Services Computing》等期刊和会议上发表 SCI/EI 收录的学术论文 120 余篇, 授权美国发明专利 2 项、中国发明专利 10 项。获第八届青岛市青年科技奖，山东省高校优秀科研成果一等奖等奖项。

会议地点

安徽省合肥市经开区九龙路 111 号，安徽大学磬苑校区理工 D 楼 108 会议室。

★ 会议地址

住宿地点

酒店名称：翡翠湖迎宾馆

地址：合肥市蜀山区容成路 1 号（近安徽大学磐苑校区）

会务联系人

137-2103-2191（崔杰）　　**153-9509-0670**（许艳）