2014年密码算法前沿论坛在北京举办

2014年08月01日

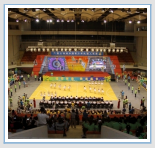
6月21－22日，由中国密码学会密码算法专业委员会主办，中国科学院软件研究所可信计算与信息保障实验室承办的2014年密码算法前沿论坛在北京举行。此次论坛围绕认证加密、格密码、密码分析、密码函数等主题，邀请了11位专家、学者作特邀报告。来自全国各地约150位密码学领域的科研工作者、工程技术人员、以及在校研究生参加论坛。

中国密码学会密码算法专业委员会主任吴文玲、中国科学院软件研究所研究员张振峰、新加坡南洋理工大学教授伍宏军、国防科技大学教授李超、西安电子科技大学教授胡予濮分别主持了各主题的研讨。

西安电子科技大学教授胡予濮作了题为《Non-spherical Gaussian: Revisiting MP12 Trapdoors》的特邀报告，从研究背景、MP12陷门、非球的基本高斯采样、改进的高斯采样、非球高斯变量五个方面进行了详细介绍。中国科学院系统科学研究所潘彦斌博士作了题为《A Three-Level Sieve Algorithm for the Shortest Vector Problem》的报告，围绕最短向量问题介绍了格、格密码与三层筛法的相关知识。新加坡南洋理工大学教授伍宏军作了题为《Designing Authenticated Ciphers in Four Different Approaches》的特邀报告，报告针对认证加密算法的设计方式，从软硬件效率两个方面，以AEGIS、MORUS、JAMBU、ACORN等算法与模式为例进行了详细介绍。伍宏军教授总结分析了认证加密算法的设计方式和研究热点，进一步明确了该领域的研究思路和发展方向。新加坡南洋理工大学的王磊博士作了题为《SHELL Authenticated Encryption》的特邀报告，围绕CAESAR候选算法SHELL的特点、设计准则、优缺点等方面展开，详细介绍了SHELL的相关知识，为认证加密算法的设计与分析提供了新思路。中国科学院软件研究所张斌研究员作了题为《Sabiler Stream Cipher with Authentication》的特邀报告，围绕算法特点、安全性目标、安全性分析、设计准则等方面详细介绍了CAESAR候选算法Sablier，对认证加密算法的下一步研究起到了引导和启发的作用。中国科学院信息工程研究所王鹏副教授作了题为《认证加密的设计模式》的特邀报告，进一步介绍了认证加密的几类设计模式。王鹏副教授生动形象地阐述了认证与加密的关系，以PAES与PANDA为例，总结分析了目前认证加密的设计模式与新的设计方法，并对未来的研究做出了展望与探讨。中国科学院软件研究所张立廷副研究员作了题为《iFeed Authenticated Encryption》的特邀报告，围绕CAESAR候选算法iFeed，从设计背景、结构、特点、安全性证明、压缩函数等方面对iFeed进行了详细的介绍，为认证加密模式的设计与分析提供了新的思路。山东大学王美琴教授作了题为《On the (In) Equivalence of Impossible Differential and Zero Correlation Distinguishers for Feistel- and Skipjack-type Ciphers》的特邀报告。报告围绕不可能差分与零和区分器的等价性，从Feistel类密码算法与Skipjack类密码算法两个方面进行了详细介绍。国防科技大学李超教授作了题为《New Results On the 2-adic Complexity of Binary Sequences》的特邀报告。报告主要介绍了二元序列研究的新成果，以及一些待解决的问题。桂林电子科技大学的韦永壮教授作了题为《密码函数新设计方法及其安全性指标分析》的特邀报告。报告围绕布尔函数常见的安全性度量指标、最新设计进展、一类密码函数的安全性新分析、密码函数构造中的一些新问题，以及M-M函数性质在分组密码分析中的应用五个方面进行了介绍。国民技术的王宇

要闻

第十四届青少年机器人竞赛闭幕式暨…



7月18日，第十四届中国青少年机器人竞赛闭幕式暨颁奖典礼在新疆维吾尔自…

详细>>

- 江苏泰州科普志愿者管理进入数字时代
- 束为调研黑龙江省科技馆体系建设工作
- “公众喜爱的科普作品”推介活动启动

工作动态

- 全国首家省级农技协与银行签订合作框…
- 第二十一届全国科普理论研讨会在哈尔…
- 中国科普研究所2014肇东科技夏令…
- 中学生英才计划2014年数学论坛在…
- 中国科协学术与学会工作专委会赴四川…
- 2014年全国农村妇女科学素质网络…
- 宋南平赴河北承德考察农技协和农业基…
- 2014年青少年高校科学营陕西分营…

全国学会

- 中国密码学会安全协议专业委员会成立
- 2014年密码算法前沿论坛在北京举…
- 2014全国图书馆未成年人服务提升…
- 中国图书馆学会组织新型城镇化与图书…
- 第五届中国技术未来分析论坛召开
- 2014中瑞绿色经济与企业可持续发…
- 可持续发展研究会人居环境专委会办中…
- 中国图书馆学会2014年秘书长联席…
- 韩布新当选国际应用心理学协会秘书长
- 第八届中国肿瘤内科大会在北京召开

地方科协

- 青海西宁市、浦东新区科技社团组织开…
- 青海省西宁老科协召开第八次会员代表…
- 北京天文学会举办第六届天文科普教育…
- 第十四届全国有机电化学与工业学术会…
- 福建省科协开设“科普之窗”栏目正式…
- 第十三届海峡两岸大学生辩论赛在福州…
- 山东日照组织“家园暑期行”科普大篷…
- 广东省科协“海智计划”工作座谈会召…
- 广东省惠州市惠阳区科协多措并举开展…
- 江苏省13市科协领导聚南京共话发展…

基层建设

- 汽车行业科协创新方法培训班在吉林举…
- 贵州省金沙县开展“农村科普大讲堂”…

建博士作了题为《面向金融、支付领域的芯片安全性分析技术》的特邀报告。报告围绕金融、支付领域的安全芯片展开，分别介绍了安全芯片所遭受的安全威胁、芯片安全性评估中的关键分析技术、芯片的安全性防护方法等内容。

大会加强了密码算法研究者相互间的理解和交流，开阔了科研思维，促进了我国密码算法领域学术水平的进一步提高。

中国密码学会供稿

责任编辑：董艳苹

- 黑龙江安达市科协加大对无公害蔬菜种…
- 山东省滕州市科普电影放映月活动进社…
- 国华台电科协力促公司可持续发展
- 江苏省大丰市召开企业科协成立现场观…
- 黑龙江省科协深入企业调研
- 贵州省金沙县以“公司-协会-基地-…