学会资讯
Learn information
学会动态
通知通告
图片新闻
会议报道
年会报道
在线咨询
学会章程
联系方式

第一届安全协议进展国际会议在北京成功召开

2014年9月28日至30日，由中国密码学会安全协议专业委员会主办，中国科学院信息安全国家重点实验室承办的“第一届安全协议进展国际会议”（2014 International Conference of Progress on Security Protocols，简称PSP国际会议）在北京成功召开。来自全国30余个研究机构的100余名科研人员参加了会议。

开幕式由程序委员会主席、安全协议专业委员会副主任委员、中国科学院信息工程研究所薛锐研究员主持，中国密码学会秘书长于艳萍和中国密码学会副理事长、第一届安全协议进展国际会议大会主席、中国密码学会安全协议专业委员会主任委员冯登国研究员分别向大会致辞，对会议的召开表示祝贺。

会议日程安排合理，交流气氛活跃，中国密码学会安全协议专业委员会的曾庆凯教授、李舟军教授、徐秋亮教授、李红达教授、邓燚研究员、朱岩教授、徐静研究员、苏璞睿研究员等委员到会参加研讨。 中国科学院信息工程研究所的邓燚研究员、中国科学院软件研究所的张振峰研究员和复旦大学的赵运磊教授分别做了题为“零知识证明-从基础到前沿” 、“匿名认证——大数据时代隐私保护的金钥匙”和“A New Family of Implicitly Authenticated Diffie-Hellman Protocols”的特邀报告。会议共征集到稿件15篇，经程序委员会评审后录用11篇。 8位国内专家学者及所作报告分别是：国防科技大学的李梦君副教授做了题为“mathRodin: An Event-B Refinement Tool Based on Mathematica”的报告；北京航空航天大学的姚燕青博士做了题为“Privacy and Imperfect Randomness” 的报告；山东大学的蒋翰副教授做了题为“Two-Way OT Protocol for sending garbage circuits in Cut-and-Choose Secure Two-Party Computation”的报告；解放军信息工程大学的李宏欣

做了题为 “UC 安全有限码长诱骗态协议研究”的报告;上海交通大学的宁建廷博士做了题为“Large Universe Ciphertext-Policy ABE with White-Box Traceability”的报告; 邢台学院的张江宵博士做了题为 “基于花费链最优匿名的等长可传递电子现金系统”的报告; 中国科学院大学的范丹博士做了题为 “An Adaptive Formal Modeling and Analysis Schema for Security Protocols”的报告; 解放军外国语学院的陆思奇做了题为 “安全协议形式化分析工具比较研究”的报告。此外, 报告期间与会人员就自己关心的问题与各报告人进行了深入的交流与讨论, 均表示获益良多。

此次研讨会为国内安全协议的研究人员提供了交流的平台，为提高我国安全协议的研究水平，促进国内该领域学者之间的学术交流与合作起到了积极的作用，取得了圆满成功。今后，将每年举办一次安全协议进展国际会议。