SKLOIS
信息安全国家重点实验室

信息安全国家重点实验室通讯

STATE KEY LABORATORY OF INFORMATION SECURITY

2016年第4期（总第6期）

信息安全国家重点实验室办公室
电话：+86-10-82546611
传真：+86-10-82546564
邮箱：sklois@iie.ac.cn
网站：http://www.sklois.cn

SKLOIS
信息安全国家重点实验室

摄影作品展

雨过天晴（作者：刘淼）

西山晚霞（作者：吕昌）

动与静（作者：陈恺）

日出（作者：陈宇）

轨道（作者：吕昌）

捕捉（作者：仝艳菲）

目　录

第十四届理论密码学会议在京召开

2016 年 10 月 31 日至 11 月 3 日，由国际密码研究学会（IACR）主办，中国科学院信息工程研究所信息安全国家重点实验室 (SKLOIS) 承办的“第十四届理论密码学会议”（TCC 2016-B）在北京友谊宾馆召开，来自美国、丹麦、瑞士、以色列、奥地利、波兰、比利时、印度等国家和地区的一百余名研究人员参加了此次会议。

大会为 Ueli Maurer (ETH)、Renato Renner (ETH) 和 Clemens Holenstein (ETH) 三人颁发了“Test of Time Award”奖项，以表彰其在 TCC 2004 会议上发表的题为“Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology”的文章对理论密码和应用密码体系做出的突出贡献。

本次会议共邀请到三位来自理论密码学领域国际著名学者作了精彩的特邀报告，引起了众多与会者的积极讨论。苏黎世联邦理工学院（ETH）的 Ueli Maurer 教授就不可分辨性概念作了题为“From Indifferentiability to Constructive Cryptography (and Back)”的特邀报告；哥伦比亚大学的 Allison Bishop 副教授在“Through the Looking Glass : What Cryptography Should Do for Alice”的特邀报告介绍了差分隐私；麻省理工大学 Srini Devadas 教授在特邀报告“Secure Hardware and Cryptography: Contrasts, Challenges and Opportunities”中提出了一个新颖的方法可以为云中计算提供强有力的安全保障。此外，四十五篇论文作者就理论密码基础、无条件安全、多方协议、委托和交互式证明、差别隐私、公钥加密、秘密共享、混淆和多线性映射、多方计算的轮复杂性和有效性、基于属性的加密方案、功能性加密等多个领域分别进行了学术报告。

在为期四天的会议中，与会者针对理论密码学的前沿热点问题进行了深刻的研讨交流。会议增强了理论密码学者之间的相互合作与交流，推动了理论密码学知识的传播与应用，大会取得圆满成功。

大会颁发“Test of Time Award”奖项

Ueli Maurer 教授作特邀报告

Allison Bishop 副教授作特邀报告

Srini Devadas 教授作特邀报告

第十二届信息安全与密码学国际会议在京召开

2016 年 11 月 4 日至 6 日，由信息安全国家重点实验室 (SKLOIS) 与中国密码学会 (CACR)、信息保障技术重点实验室联合主办的“第十二届信息安全与密码学国际会议”（INSCRYPT 2016）在北京友谊宾馆召开，来自美国、以色列、奥地利、波兰、比利时、印度等国家和地区百余名研究人员、学生参加了此次会议。

本次会议共邀请到三位来自信息安全、密码学领域国际著名的专家学者作了精彩的特邀报告，引起众多与会者的积极讨论。宾尼法西亚州立大学的 Adam Smith 副教授就数据挖掘中的保护隐私问题作了首场题为“Rigorous Foundations for Privacy in Statistical Databases”的特邀报告；哥伦比亚大学的 Moti Yung 教授在特邀报告“On Deploying Secure Computations Commercially”中提出了涉及商业应用“安全的对特定任务的多方计算协议”；比利时的荷语天主教鲁汶大学 Elena Andreeva 博士在特邀报告“Authenticated Encryption and the CAESAR Competition”中介绍了可认证加密方案。此外，四十篇论文作者就公钥加密系统、对称加密系统、基于格的同态加密系统、网络安全及其应用、云计算安全、混淆、抗泄露和抗量子攻击密码系统等多个领域分别进行了学术报告。

在为期三天的会议中，与会者针对信息安全与密码学领域现在的前沿热点问题进行了深刻的研讨交流。此次会议增强了国内信息安全与密码学领域与国际间的交流，推动了国内信息安全与密码学的进一步发展，会议取得圆满成功。

王小云教授为大会致辞

Moti Yung 教授作特邀报告

Adam Smith 副教授作特邀报告

Elena Andreeva 博士作特邀报告

2016(首届)中国隐私保护学术会议在京圆满召开

2016 年 11 月 7 日，由中国保密协会隐私保护专业委员会（以下简称“专委会”）主办，中国人民大学、中国科学院信息工程研究所联合承办的“2016（首届）中国隐私保护学术会议”，在中国人民大学召开，并获得圆满成功。

大会围绕数据隐私保护与安全等研究领域，邀请了国内外著名院士、学者等专家到会作了特邀报告及专题报告，共同探讨数据隐私保护发展现状，以及所面临的关键性挑战问题和研究方向。本次大会由中国人民大学教授、CCF 会士、隐私保护专业委会副主任委员孟小峰主持。

报告结束后，隐私保护专业委会主任委员林东岱研究员主持了隐私保护专委工作会议及发展研讨会议，主要讨论了专委会的年度工作计划、专委会组织架构的完善以及如何推动隐私保护事业的发展等事项。与会委员积极发言，提出了诸多宝贵意见。

中国保密协会副秘书长王炎冰、中国保密协会隐私保护专业委员会主任委员林东岱、副主任委员杜跃进、孟小峰、秘书长薛锐，以及专委会其他委员和来自各企事业、研究单位、高校的专家、学者逾 150 人参加了本次大会。

隐私保护专业委会主任委员林东岱研究员主持隐私保护专委工作会议及发展研讨会议

SKLOIS-USITO 安全技术国际研讨会在京举行

2016年12月13日下午，由信息安全国家重点实验室(SKLOIS)与美国信息技术产业理事会(ITI)共同主办、美国信息产业机构北京办事处（USITO）协办的 SKLOIS-USITO 安全技术国际研讨会在北京举行。信息安全国家重点实验室和全球信息技术通信行业安全技术专家团共计三十余位专家出席了研讨会。

此次研讨会由 USITO 总裁缪万德主持，SKLOIS 主任林东岱研究员与 ITI 高级副总裁 Josh Kallmer 为研讨会致辞。随后，大会邀请中美双方的七位专家代表作了精彩演讲。伦敦帝国学院 Michael Huth 教授作了题为《优化区块链》的演讲，对区块链优化技术，特别是对区块链治理技术的研究进展进行了介绍。实验室张文涛副研究员题为《轻量级密码算法 RECTANGLE 简介》的演讲对轻量化密码方案 RECTANGLE 进行了简要分析。

SKLOIS 主任林东岱为研讨会致辞

实验室陈恺研究员作了题为《软件同源性分析与恶意代码检测》的演讲，介绍了当前在软件同源性分析方面的工作进展，以及对智能手机应用程序恶意代码检测方面的工作，并探讨了该工作的研究意义与商业价值。ITI 高级副总裁 Josh Kallmer 题为《NIST 加密标准开发过程的最新进展》的演讲就 NIST 密码标准与指南的制定进行了详细阐述。英特尔公司信任与安全部门总监 Claire Vishik 博士在演讲《区块链金融领域以外的应用》中介绍了区块链技术在金融领域以外，如电子政务、物联网等领域的应用。实验室卿斯汉研究员的演讲《云计算安全标准探讨》介绍了当前国内外云计算安全标准制定的进展以及标准制定中存在的不足。北京安博通科技股份有限公司技术总监李远题为《安全能力可视化与虚拟调度》的演讲对安全能力可视化与虚拟调度的应用进行了介绍。

交流讨论

实验室陈恺研究员作演讲

实验室张文涛副研究员作演讲

此外，双方还就区块链技术安全标准制定进展、美国密码标准制定依据和密码安全产品的出口政策限制等议题进行了深入的交流和讨论。

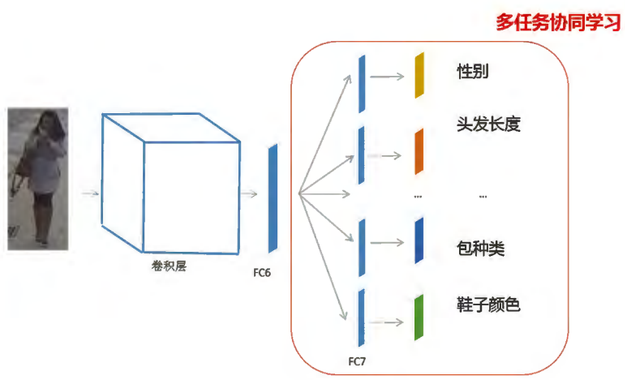
实验室 S-LAB 团队获 2016CCF 大数据与计算智能大赛综合特等奖

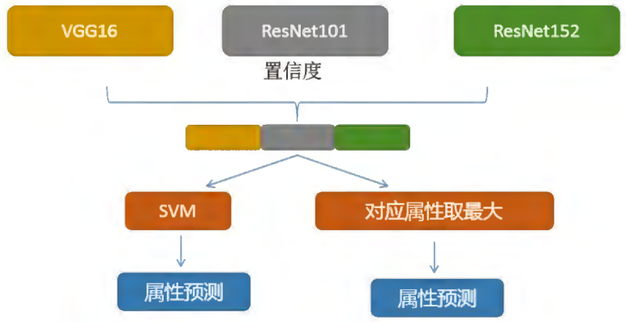
（任广辉）

2016 年 12 月 25 日，实验室刘偲副研究员带领的 S-LAB 团队在“2016CCF 大数据与计算智能大赛”中击败四百余支参赛队伍，获得“监控场景下的行人精细化识别”赛题的企业单项一等奖，并在最后特等奖的激烈角逐中，凭借创新的算法思路及广阔的应用前景，从来自北大、国科大等知名高校、企业的十一支单项冠军队伍中脱颖而出，最终夺得此次大赛的终极奖项——CCF 综合特等奖。

刘偲团队在计算机视觉领域有着深厚的技术积累，本次大赛中“监控场景下的行人精细化识别”赛题正切合团队的研究方向。赛题主要包括行人的六种部件检测及十种属性分类两大任务，存在着光照情况复杂、清晰度差、行人姿态多样等难点，同时监控场景这一实际应用环境又对实时性提出了较高要求，赛题难度较大。

在分类任务中，团队考虑到行人性别、头发长短，以及上下衣着等属性间的相关性，采用多任务协同学习的框架，这种框架既考虑到了不同属性的上下文相互关系，也能够仅通过一个模型预测出总共的十种属性，较为快速便捷。





在这一框架下，团队尝试了包括 VGG 及 ResNet 在内的多种单一的模型，并完成了大量实验以选取最优模型，同时在性能较好的三种模型（VGG19/ResNet101/ResNet152）的基础上尝试支持向量机以及最大响应等多种融合策略，综合考虑精度、速度，最终选择了采用最大响应的融合策略。

在部件检测任务中，团队在 SSD512 算法的基础上，创新性地采用了基于位置先验的局部检测模型，提出了 SSD512-Half 的方法，即裁剪半身图像送入模型网络进行检测，这样头、帽子、鞋等相对较小部件的检测精度有了较大提升。

此外团队还创新性地协同处理分类及检测，在不影响检测速度，同时又能明显提升精度这一前提下，进行了以下三个方案的改进：

1. 检测改进分类性能

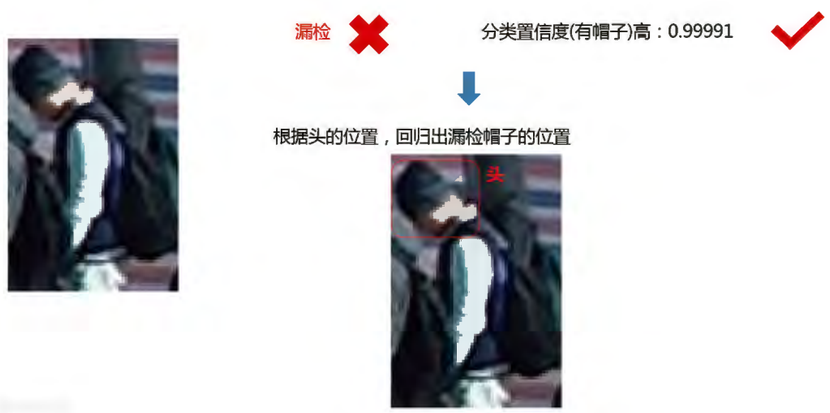
在某些情况下，属性分类可能将部件的颜色种类均预测为无，且置信度较低，但检测模型判断有部件存在，且置信度较高，此时把非类模型预测的置信度第二高的属性作为分类结果，这样即通过检测结果对分类进行了改进。

3. 分类协助去除虚警

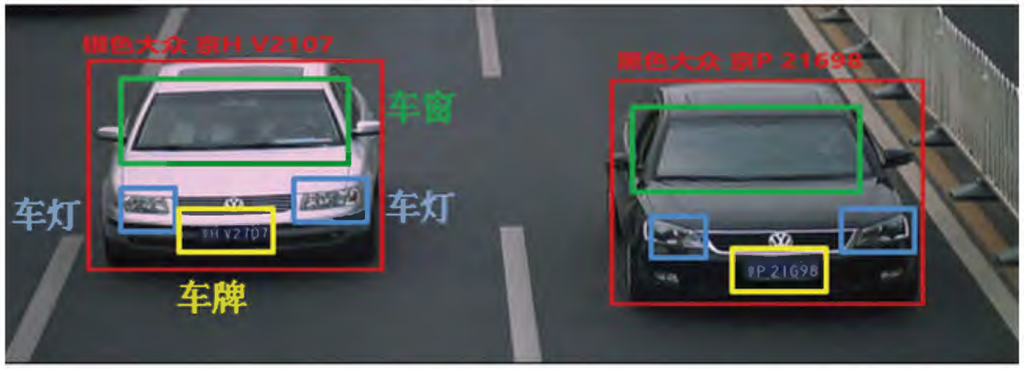
由于图像模糊、部件较小、错误样本与正确样本相似度高等原因，检测模型会误将部分错误的结果判断为正确，这部分错误样本的置信度高于检测阈值，被称为“虚警”。而在分类模型中，检测模型输出的虚警因其确实不存在具体部件，常常会得到一个较低的“有部件”的置信度，通过分类、检测的综合衡量，就可以去除部分虚警，以提高整体精度。

3. 分类协助减少漏检

由于同样的原因，除虚警外，检测模型还存在漏检这一问题，如对有帽子的图片，因检测框置信度较低而未能检测出帽子。同样通过分类模型，对在分类模型中“有帽子”的置信度较高但未能检测出帽子的样本，通过头的位置，回归出帽子的位置，便可减少漏检的情况。



在进行多种创新改进提升精度的同时，团队也兼顾了实时性需求，以便在实际场景中应用，并完成了demo制作。此外 ,这一方案的技术经过改造 ,可应用于更多场景 ,如车辆的精细化识别 ,即对车辆的品牌、型号、颜色、车牌号等属性进行识别，同时对车辆的各个部件位置进行检测，可应用于道桥卡口、收费站、机场车站等车流密集的重点场所，也可用于城市安防的日常监控，具有广阔的产业化前景。



团队合影

原创诗歌作品欣赏

网安歌

作者：路献辉

波诡云谲互联网，攻守绝技胸中藏。

直面燃眉心腹患，带头攻关大旗扛。

西山赏花

作者：刘亚敏

半坡红欲放，几树粉初裁。

莫问花名类，春风尽使开。

科普园地

网络安全态势感知技术

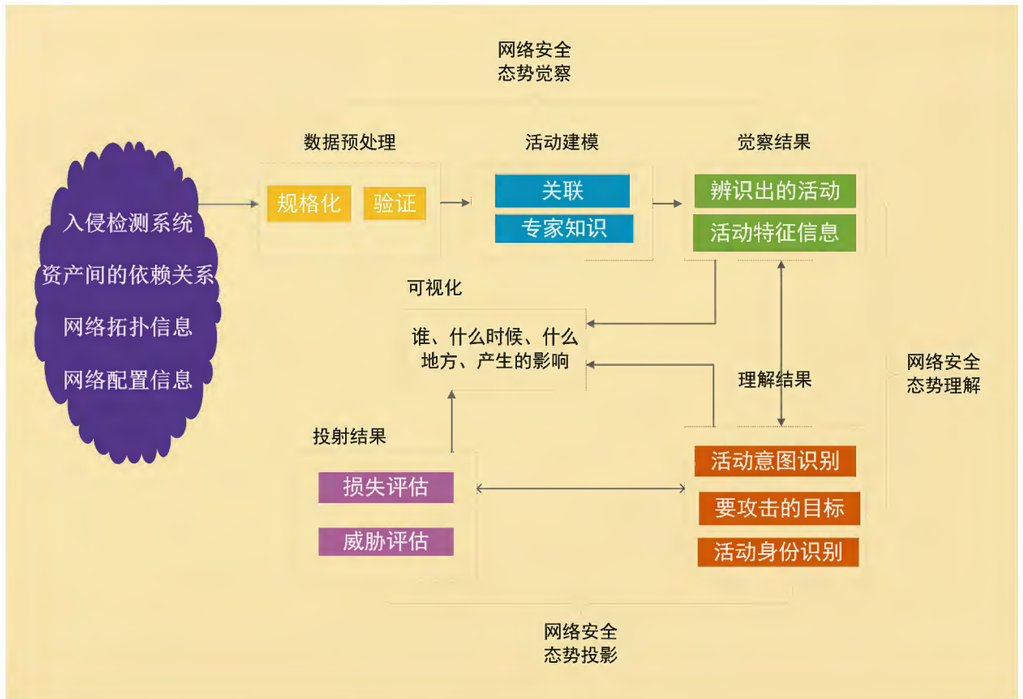
（许玥）

互联网基础设施的不断发展和新应用的不断涌现使得网络规模逐渐增大，拓扑结构日益复杂，网络安全管理的难度不断增加。为了应对日益复杂、隐蔽的网络威胁，各种检测技术相继出现，如：脆弱性检测技术，恶意代码检测技术、入侵检测技术等。这些技术试图从不同的角度发现网络中可能存在的安全问题，但在实时、全面地寻找出网络系统中存在的真实威胁方面不够理想和有效，限制了网络安全管理员做出最佳响应决策的能力。近年来，网络安全态势感知的概念逐渐引起研究人员的兴趣，希望利用其从大量、存在噪声的数据中辨识出网络中的攻击活动，宏观地把握整个网络的安全状况，并合理有效地进行响应，以尽可能降低因攻击造成的损失。这对于提高网络系统的监控能力和应急响应能力具有积极的作用。

态势感知是指在一定的时间和空间范围内，提取系统中的要素，理解这些要素的含义，并且预测其可能的效果。它是一个认知过程，通过使用过去的经验和知识，识别、分析和理解当前的系统状况。分析人员对当前的态势进行感知，更新“状态知识”，然后再进行感知以致构成一个循环的映射过程。这个映射过程不是简单的数据变换而是一种语义提取。因此感知的过程表现为不断地作认知映射以获取更多更详细的语义。态势感知是一个动态变化的过程，不同的人由于经验、知识等不同，得到的态势感知不尽相同。

态势感知最早来源于美国军方在军事对抗中的研究。在军事术语中，态势感知的目标是使指挥官了解双方的情况，包括敌我的所在位置、当前状态和作战能力，以便能做出快速而正确的决策，达到知己知彼，百战不殆的目的。

网络安全态势感知（Network Security Situation Awareness，简称 NSSA）是态势感知方法在网络安全领域的应用。它是对网络系统安全状态的认知过程，包括对从系统中测量到的原始数据逐步进行融合处理和实现对系统的背景状态及活动语义的提取，识别出存在的各类网络活动以及其中异常活动的意图，从而获得据此表征的网络安全态势和该态势对网络系统正常行为影响的了解。它能够实现对网络中各种活动的行为辨识、意图理解和影响评估，以支持合理的安全响应决策，是对网络的安全性进行定量分析的一种手段。网络安全管理系统可以借助其宏观把握整个网络的安全状况，分析攻击者的意图，为管理决策提供重要的依据。



图：网络安全态势感知模型

目前网络安全态势感知的研究是一个正处于发展中的课题，大部分研究都集中在重构攻击活动方面，基本都是网络入侵检测领域研究的延伸，已有很好的基础但也有很多问题需要研究和解决。另一方面，包括网络测量、网络流量行为学、网络管理技术、大数据处理技术、流式数据处理技术、可视化技术在内的其它相关领域的发展也为网络安全态势感知的研究提供了积极的支持。尽管网络安全态势感知的研究仍处于初级阶段，随着各种相关技术和研究的不断完善，网络安全态势感知技术将走向成熟和实用，为保障网络的安全起到越来越重要的作用。

中国科学院大学网络空间安全学院成立

（文章来源：中国科学报 2016 年 12 月 15 日）

12 月 12 日下午，中国科学院大学网络空间安全学院召开成立大会。中科院院长、党组书记白春礼，中科院副院长、中国科学院大学校长丁仲礼，国家自然科学基金委副主任高文等出席会议。

由于网络空间已成为继陆、海、空、天之外的第五疆域，网络空间安全也成为保护网络疆域、治理网络秩序、维护国家和人民利益的重要领域。为满足我国网络空间安全事业发展的人才需求，2015 年 6 月，国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科，这是推动我国网络空间安全发展的重要举措。同年 12 月，中国科学院大学成为国内首批获准建设“网络空间安全”一级学科的大学之一。

此后，由中科院信息工程研究所牵头，中科院计算技术研究所、数学与系统科学研究院、声学研究所、计算机网络信息中心、自动化研究所等单位以及国家有关部委共同组建了网络空间安全学院。该学院将面向国家网络空间安全战略需求，面向国际科技前沿，以中国科学院大学为核心，研究所深度参与，形成科研与教育融合、多学科交叉的培养体系。中国科学院大学网络空间安全学院首批招生 244 人。

丁仲礼在会上指出，2016 年是我国“十三五”规划的开端之年，也是中科院深入实施“率先行动计划”，促进“科教融合”的关键之年。中国科学院大学研究制定了《“十三五”发展规划纲要》，树立了建设世界一流大学和一流学科的宏伟目标。网络空间安全学院的成立，正是为实现这一目标而作出的重要举措。

中国科学院大学网络空间安全学院院长孟丹在大会发言中强调，培养网络空间安全人才的工作已经刻不容缓。在相关单位的共同努力下，今年 6 月网络空间安全学院就落实了组织架构和人员配置。在充分参考相关学科和国外教学经验的基础上，对学院的本科课程和研究生课程进行了规划，并充分发挥科学院综合优势构建了产学研用一体化的人才培养模式。9 月，网络空间安全学院的第一届研究生已经入学。

孟丹表示，学院将按照习近平总书记建设一流网络空间安全学院的指示要求，努力做到四个一流：拥有世界一流的师资队伍、拥有世界一流的创新土壤、产出世界一流的科研成果、产出世界一流的高端专业人才，造就网络空间安全科技领域“中国的领导者、世界的引领者”。

丁仲礼表示，今后，中国科学院大学网络空间安全学院将继续发挥“科教融合”的特有优势，力争在国内网络空间安全领域占据领先地位，并成为国际知名的网络空间安全科研、教学一体化人才培养基地。

我国网络空间防御技术取得重大突破 将改变网络安全游戏规则

（文章来源：新华社 2016 年 11 月 14 日）

经科技部授权上海市科学技术委员会组织的测试评估，由解放军信息工程大学、复旦大学、浙江大学和中国科学院信息工程研究所等科研团队联合承担的国家“863 计划“重点项目研究成果“网络空间拟态防御理论及核心方法“近期通过验证，测评结果与理论预期完全吻合。这标志着我国在网络防御领域取得重大理论和方法创新，将打破网络空间“易攻难守”的战略格局，改变网络安全游戏规则。

拟态，是指一种生物模拟另一种生物或环境的现象。2008 年，中国工程院院士邬江兴从条纹章鱼能模仿十几种海洋生物的形态和行为中受到启发，提出了研发拟态计算机的构想。在科技部和上海市的共同支持下，拟态计算原理样机研制成功并入选“2013 年度中国十大科技进展”。在此基础上，研发团队针对网络空间不确定性威胁等重大安全问题，开展基于拟态伪装的主动防御理论研究并取得重大突破，所提出的“动态异构冗余体制架构”，能够将基于未知漏洞后门的不确定性威胁或已知的未知风险变为极小概率事件。

2016 年 1 月起，由国内 9 家权威评测机构组成的联合测试验证团队，对拟态防御原理验证系统进行了为期 6 个月的验证测试，先后有 21 名院士和 110 余名专家参与不同阶段的测评工作。测评专家委员会发布的《拟态防御原理验证系统测评意见》认为：拟态防御机制能够独立且有效地应对或抵御基于漏洞、后门等已知风险或不确定威胁。受测系统达到拟态防御理论预期，并使利用“有毒带菌”构件实现可管可控的信息系统成为可能，对基于“后门工程和隐匿漏洞”的“卖方市场”攻势战略具有颠覆性意义。

邬江兴介绍说，我国是遭受网络攻击最严重的国家之一。据国家互联网应急中心数据显示，仅 2015 年的抽样监测，我国有 1978 万余台主机被 10．5 万余个木马和僵尸网络控制端控制。由于现有的网络防御体制采用的是“后天获得性免疫”机制，先“亡了羊”，才能通过打补丁、封门堵漏来“补牢”，对于不能感知和认知的网络攻击几乎不设防，而拟态防御理论与方法能够有效应对这些问题。

邬江兴还表示，网络空间拟态防御理论与方法是全人类的共同财富，中国科学家愿意将这一技术与世界分享，为构建网络空间命运共同体作出贡献。

特朗普领导下的白宫： 网络武器开发将是一项“头等大事”

（文章来源：E 安全 2017 年 1 月 22 日）

根据白宫网站最新公布的信息，美国新任总统特朗普优先考虑“进攻性网络能力的开发”，通过向美国网络司令部提供新的资源以“维护美利坚合众国国家的安全机密与各类系统。”

就在本周，白宫官网 whitehouse.gov 已经开始进行针对新一任美国总统就职仪式的相关准备。该网站现在提供一系列新的在线内容与特朗普的重点政策信息——其中包括建立军队、拉拢更多就业机会回到美国以及制定对美国更为有利的贸易协议等等。

白宫网站指出，“网络战是一类新兴战场，我们必须采取一切措施以保护我们的国家安全机密及各类系统。我们将优先通过网络司令部开发防御与进攻性网络能力，同时招募最出色且最睿智的美国人才以服务于这一关键性领域。”

这已经不是特朗普总统第一次公开呼吁提升美国的网络攻击能力。

特朗普曾在去年 10 月 3 日一次面向美国退役军人的演讲中表示，“我将确保我们的军队拥有世界上最强大的网络进攻与防御能力。以今天为起点，我们将重拾这一长久以来遭受忽视的国家层面决议，讨论如何……发展必要的网络攻击战略，从而在二十一世纪取得关键性安全优势。”

特朗普在支持美国网络武器发展方面的具体计划目前尚不明确。在白宫的外交政策页面中，可以看到特朗普当局将“参与到网络战当中，旨在破坏并阻止恐怖分子借此进行的宣传与招募活动。”在竞选期间，他还批评称美国在发动网络战的能力方面不及其它国家。

特朗普在去年 3 月接受《纽约时报》采访时指出，“首先，我们的网络已经严重过时。我们曾经是积极进行创造的群体，但现在我们已经落后于时代。大家可以选择拒绝，可以坐视美国缺乏强大网络能力的现状。但我认为我们不会作出这样的选择。我认为我们的网络先进程度已经不及其它国家。”

在去年 12 月末，特朗普任命前小布什总统国家安全副顾问托马斯•博塞特（Thomas Bossert）作为其国家安全顾问。在小布什政府供职期间，博塞特曾担任白宫基础设施保护政策主任一职——此领导职位负责帮助联邦政府内各组织机构对美国关键性基础设施（包括各主要交通及通信系统）加以保护。

目前，博塞特作为特朗普总统的最高级顾问负责处理网络安全相关事务。

拍照别再用剪刀手了！
因为你的指纹可能已经被盗

（文章来源： 爱活网 2017 年 01 月 16 日）

科技越来越发达，人们对信息安全也就越来越重视，因此现在许多电子设备上指纹解锁的应用变得很普遍。但是指纹解锁就真的那么安全么？千万别在傻乎乎的以为要获取指纹得经过很复杂的技术，据日本《产经新闻》报道，现在通过照片这种媒介你的指纹也有被盗的风险。

报道指出，根据日本国立情报研究所的研究显示，以现有的技术，只要是距离相机 3 米内摆出胜利手势也就是我们俗称的剪刀手，来拍照，就可以从照片中读出被摄者的指纹。而现在很多人都是 1 米范围的自拍照，如果不对图片加以压缩处理就直接发朋友圈什么的话，那更是增加了指纹被盗的机率。

与此同时，国立情报研究所还指出处了指纹外，面部以及虹膜认证也广泛应用于各个领域，原来这些信息属于＂个人生物特征＂看似很难复制，也一度被认为是最安全的认证方式。但目前既然已经能够通过照片这种媒介来盗取指纹了，那像面部虹膜这些其他生物信息也不会万无一失的。更何况 我们现在追求的都是高像素高画质的相机镜头，细思恐极……

而目前，国立情报研究所已经开发出一种具有特殊花纹的透明薄膜，除了可以隐藏指纹外同时也不影响指纹解锁的使用，最厉害的是，在你拍照使用剪刀手的时候，它还能将你的指纹伪装成别的指纹，保护你的指纹信息不会轻易泄露。要不然你就后期一下或者别用太高清的相机镜头了吧！

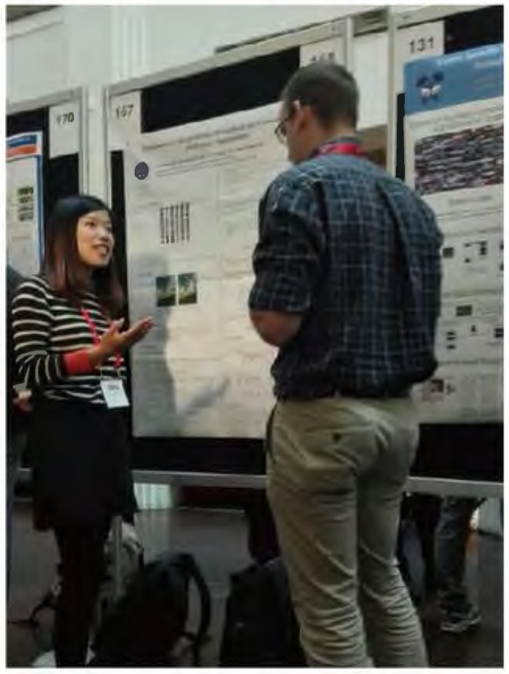
实验室最新研究成果被
ACM Multimedia 2016 录用

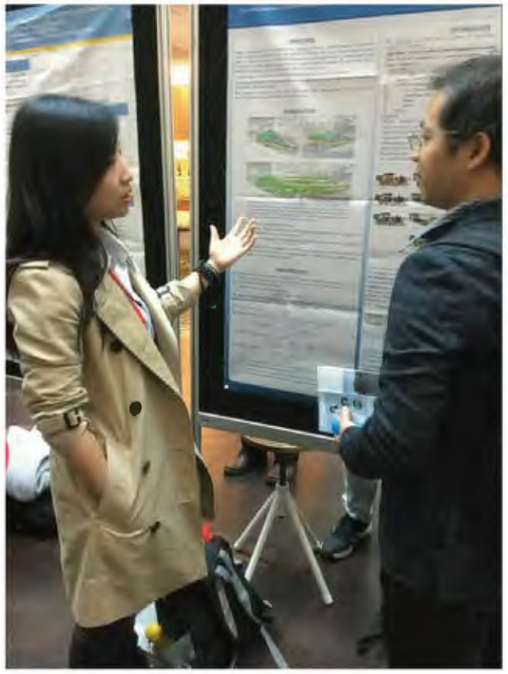
2016 年 10 月 14 日至 10 月 20 日，信息安全国家重点实验室王蕊副研究员、许倩倩副研究员赴荷兰阿姆斯特丹参加国际多媒体大会（ACM conference on Multimedia, 简称 ACM MM）。

ACM MM 创办于 1993 年，是由 ACM SIGMM 专委会组织的、多媒体领域具有最高学术地位的国际性学术会议。目前在中国计算机学会推荐国际学术会议的排名中，ACM MM 为人工智能领域的 CCF A 类会议。

信息安全国家重点实验室共有两篇文章被本次大会录用。长文《Parsimonious Mixed-Effects HodgeRank for Crowdsourced Preference Aggregation》通过 Mixed-Effects HodgeRank 模型对网络众包下用户的行为进行挖掘，从而为用户提供更加精准的喜好估计函数。求解过程中采用 Linearized Bregman Interations 方法，具有简单、速度快、偏差小、适用于大数据等优势。该项工作获得了 ACM MM 评审专家的一致认可，被邀请做 22.5 分钟的大会报告，并进行了海报展示。短文《MatchDR: Image Correspondence by Leveraging Distance Ratio Constraint》针对共享语义标签图像匹配困难的问题，采用优化距离比约束的思路进行图像匹配。提出图像匹配的排列模型，并采用基于梯度导向的模拟退火算法进行鲁棒的离散优化，有效降低了复杂图像的匹配错误率。

会议期间，王蕊副研究员和许倩倩副研究员还对实验室近年来取得的一系列研究成果进行了介绍，并同与会专家进行了深入交流。





许倩倩副研究员、王蕊副研究员向与会人员介绍实验室成果

实验室人员参加 2016 年亚洲对称密码学研讨会

2016 年 9 月 27 日至 10 月 1 日，实验室张文涛副研究员、刘美成副研究员、孙思维副研究员和宋凌助理研究员赴日本名古屋参加了 2016 年亚洲对称密码学研讨会。

亚洲对称密码研讨会（Asian Workshop on Symmetric Key Cryptography，简称 ASK）是对称密码学领域非常具有影响力的重要国际会议，每年举办一次，此次会议由日本名古屋大学（Nagoya University）主办，会议的主题是对称密码学研究进展研讨与合作交流。研讨会日程主要分为邀请报告和分组讨论两个部分。本次会议邀请报告主讲人主要包括 Florian Mendel, Atul Luykx, Lei Wang, Mridul Nandi, Jooyoung Lee, Ivica Nikolić, Meicheng Liu, Thomas Peyrin, Subhadeep Banik, Yosuke Todo, Shoichi Hirose, Damian Vizár 等，参会人员按照对称密码算法设计、分析与可证明安全等研究方向分为七个大组进行学术讨论与合作研究。

研讨会上，实验室刘美成副研究员作了题为“Algebraic Cryptanalysis of Round-Reduced Keccak”的邀请报告，该报告主要探讨了杂凑函数 Keccak 的代数密码分析技术及最新研究进展。与此同时，实验室张文涛副研究员、刘美成副研究员、孙思维副研究员和宋凌助理研究员参与了对称密码分析的分组讨论，同其他参会人员深入地进行了学术探讨，受益颇多，并为后续合作研究建立了基础。

全体与会人员合影

实验室人员参加第 22 届亚洲密码学年会

2016 年 12 月 3 日至 2016 年 12 月 9 日，信息安全国家重点实验室刘美成副研究员、向泽军博士生和朱双怡博士生赴越南河内参加了 2016 年亚洲密码学年会（22nd Annual International Conference on the Theory and Applications of Cryptology and Information Security，简 称 Asiacrypt 2016）。Asiacrypt 是由国际密码协会（IACR）举办的密码学领域三大旗舰会议之一，中国计算机学会（CCF）将其列为信息安全方向 B 类会议，中国密码学会推荐列会议表中将其归为 A 类会议。Asiacrypt 每年举办一次，Asiacrypt 2016 在越南河内举办。此次会议共收到投稿 240 篇，录用 67 篇，其中实验室有 4 篇论文被录用，刷新了会议举办以来大陆同一单位录用论文数的记录。

12 月 5 日，实验室刘美成副研究员在大会上作了题为《Linear Structures: Applications to Cryptanalysis of Round-Reduced Keccak》的报告。该报告论文是由实验室刘美成副研究员、宋凌助理研究员以及新加坡南洋理工大学郭建博士合作完成的。它通过引入线性结构来线性化至多 3 轮的 Keccak-f 置换，并以此提高 Keccak 关于 Zero-sum 区分器和原像攻击的结果，相关结果达到了国际领先水平。

12 月 5 日，实验室博士生朱双怡在大会作了题为《More powerful and reliable second-level statistical randomness tests for the NIST SP800-22》的报告。该报告论文是由实验室朱双怡博士生和马原助理研究员、林璟锵研究员、荆继武研究员以及庄家硕士合作完成的。它研究了应用最为广泛的 NIST 随机数统计检测标准 SP800-22，发现了 P-value 在二级检测中的不足，并提出了新的 Q-value 进行替代，提升了该检测的能力。

12 月 7 日，实验室博士生向泽军在大会上作了题为《Applying MILP Method to Searching Integral Distinguishers Based on Division Property for 6 Lightweight Block Ciphers》的报告。该报告论文是由实验室向泽军博士生、张文涛副研究员、包珍珍博士和林东岱研究员合作完成的。它首次将混合整数线性规划（Mixed Integral Linear Programming, MILP）的方法引入到搜索基于比特可分性的积分区分器中，解决了原有搜索算法的计算和存储复杂度随着分组密码的分组大小呈指数增长的问题，成功将搜索算法的复杂度控制在实际范围中。

实验室赵静远助理研究员与新加坡南洋理工郭建博士、上海交通大学王磊研究员、谷大武教授以及山东大学张国艳老师合作的《How to Build Fully Secure Tweakable Blockcipher from Classical Blockcipher》证明了 FSE 2015 上提出的一个可调控分组密码方案存在安全性问题，并且给出了一种安全的可调控分组密码构造方案。12 月 7 日，上海交通大学王磊研究员在大会上做了论文的报告。

此次会议吸引了来自全世界的三百多名密码学者参会，各参会者在会议期间进行了深入交流，极大促进了国际密码学的发展与进步。

1 2
3

1、实验室刘美成副研究员在大会上作报告
2、实验室博士生朱双怡在大会上作报告
3、实验室博士生向泽军在大会上作报告

实验室 4 位科研人员入选 2017 年度中科院青年创新促进会会员

近日，中国科学院人事局公布了2017年度“青年创新促进会”会员名单，信息安全国家重点实验室查达仁、陈宇、刘宗斌、孙思维等 4 名青年科研人员入选。

中国科学院青年创新促进会成立于 2011 年，旨在对全院 35 岁以下的优秀青年科技人才进行综合培养的创新举措，目的是造就新一代学术技术带头人。中国科学院青年创新促进会会员任期 4 年，信息安全国家重点实验室现有青年创新促进会会员 8 名。

实验室人员获 IWSEC 2016 国际会议最佳论文奖

2016 年 9 月 12 日至 9 月 14 日，第十一届 IWSEC 国际会议在日本东京召开，信息安全国家重点实验室王蕊副研究员指导学生林子敏发表的会议论 文“Analyzing Android Repackaged Malware by Decoupling Their Event Behaviors”获得最佳论文奖。

该论文针对 Android 重打包恶意软件问题，提出了一种新的动态行为分析检测方法，通过解析恶意软件代码执行逻辑，利用少量样本，准确定位重打包恶意软件载荷行为。


CSEC in IPSJ
IWSEC2016 in Tokyo
ISEC of ESS in IEICE
Certificate of Best Paper Award
At the 11th International Workshop on Security (IWSEC 2016) which took place between September 12-14, 2016 in Tokyo, Japan:
the Best Paper Award was awarded to
Zimin Lin, Rui Wang, Xiaoqi Jia, Shengzhi Zhang, and Chuankun Wu
for the contribution
"Analyzing Android Repackaged Malware by Decoupling Their Event Behaviors"
Masahiro Mambo and Satoru Torii, IWSEC2016 General Co-Chairs
Kazuto Ogawa and Katsunari Yoshioka, IWSEC2016 Program Co-Chairs

赵险峰研究员、博士研究生马晖获 2016 年度朱李月华优秀教师奖、中国科学院院长优秀奖

近日，中国科学院公布 2016 年度各类奖学金、奖教金评审结果。信息安全国家重点实验室赵险峰研究员荣获 2016 年度朱李月华优秀教师奖，博士研究生生马晖荣获中国科学院院长优秀奖。

赵险峰，研究员，博士生导师。

主要研究方向为多媒体安全、信息隐藏与隐蔽通信、大数据分析与事件检测。任 International J. Digital Crime and Forensics 副编辑与多个国内外会议的程序委员会委员或组委会主席，任“中国电子学会计算机取证专委会”、“中国电子学会通信与信息安全专委会”与“中国保密协会隐私保护专委会”委员。

曾承担国家自然科学基金、863 计划、中科院战略先导专项、部委信息安全专项等任务 40 余项，在 IEEE Trans. Infor. Forensics and Security、IET Infor. Security、ACM IH & MMSEC 等本领域重要刊物和会议上发表论文 120 余篇，获得与申请专利 23 项，主要提出了增强信息隐藏安全、提高相关检测性能的多种方法，主持研制了多个系统并获得重要应用。参与撰写专著与教材 5 部，在中国科学院大学开设“信息隐藏”与“网络与信息安全系列讲座”课程。

马晖，在读博士研究生，师从张锐研究员。

主要研究领域为应用密码学和云计算数据安全。曾获国家奖学金、中国科学院大学院长奖学金、中国科学院信息工程研究所所长优秀奖、信息安全国家重点实验室研究生奖学金、信息安全国家重点实验室优秀论文一等奖。目前，已正式接收和发表论文共 6 篇，包括 CCF 网络与信息安全方向 A 类期刊 3 篇，CCF B 类期刊 2 篇（含 1 篇条件接收）。

所取得的主要成果有：针对移动终端，首次提出一种高效灵活的云存储可靠性检验机制，大幅提高方案的效率；首次提出全外包的属性加密方案，用户在密钥生成、加密和解密操作时仅分别需要 1 次模指数运算，大幅提高属性加密方案的效率；针对外包解密的属性加密方案，提出两种更加高效的可验证机制，首次提出可开脱性的定义并给出具体构造和安全证明，大幅提高属性加密方案的实用性。主要成果被 IEEE Transactions on Dependable and Secure Computing、IEEE Transactions on Information Forensics and Security 等国际顶级刊物接收。

《信息安全国家重点实验室通讯》征稿启事

为推进实验室科研工作，营造浓郁的学术氛围，加强实验室文化建设，为广大职工、学生提供一个展示自身才华的舞台，在实验室领导的指导和大力支持下，在全体职工、学生的积极配合和参与下《信息安全国家重点实验室通讯》于 2015 年 11 月正式和大家见面了。现实验室面向全体职工、学生征稿，具体信息如下：

征稿内容需与实验室建设相关或展现实验室职工、学生风采（比如实验室要闻、科研进展、交流与合作、荣誉、文化生活等）；此外，近期行业快讯、科普文章、学术研究成果、战略研究报告、综述文章等相关稿件均可。

稿件要求信息真实、可靠；图文并茂；一般不超过 1000 字。

投稿请发送邮件至 sklois@iie.ac.cn，邮件主题请注明“实验室通讯投稿”。本征稿启事常年有效。

望大家踊跃投稿，拿起笔，描绘事业的点和线，抒写生活的酸与甜，在实验室科研、学习的征途中留下坚实而清晰的足印！

信息安全国家重点实验室办公室

2016 年 1 月