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

2015年第1期（总第1期）

目　录

实验室要闻

实验室举办分组密码暑期学校

信息工程研究所信息安全国家重点实验室于 2015 年 7 月 9 日至 7 月 20 日在北京怀柔区中国科学院大学雁栖湖校区国际会议中心举办了“分组密码”暑期学校。此次暑期学校以分组密码为主题，主要面向国内高等学校、科研机构和其它单位相关领域的研究生，邀请了包括中国科学院院士在内的国内著名专家学者，开设分组密码专业课程、前沿热点专题讲座，组织挑战性竞赛，旨在拓展学术视野，活跃学术思想，鼓励学术创新和加强学员之间的交流。

本次暑期学校以专题课程和讲座相结合，讲授的主要内容包括分组密码的综述、分组密码的设计思想与原理、分组密码的分析方法、分组密码的相关数学问题以及分组密码分析的相关计算方法等。本次暑期学校邀请到了李超教授、屈龙江教授、王美琴教授、陈少真教授、金晨辉教授、段明副教授、王鹏副研究员、张文涛副研究员、孙瑶副研究员、黄震宇副研究员、孙思维老师、崔霆老师、吴保峰老师、赵静远老师等多位国内外知名的学者做了专题讲座和报告，他们分别介绍了各自领域的国际最新进展及自身的研究工作，令学员受益匪浅。

本次暑期学校共招收 50 名学员（部分旁听生未计算在内），他们分别来自清华大学、上海交通大学、复旦大学、南开大学、中国科学技术大学、浙江大学、西安电子科技大学、山东大学、厦门大学、武汉大学、国防科技大学、解放军信息工程大学、中国科学院大学等国内著名高校和研究机构。在为期 11 天的学习中，学员相互交流，共同提高。在暑期学校结束之际，学员纷纷表示这是一次难得的学习机会，受益良多，希望下次还有更多类似的学习活动。

IEEE 期刊邀请操晓春研究员为编委（AE）

2015 年 7 月，信息安全国家重点实验室操晓春研究员被 IEEE Transaction on Image Processing（TIP）邀请为 Associate Editor，任期三年。

IEEE Transaction on Image Processing 是图像与信号处理领域国际顶级学术期刊，是中国计算机学会推荐的 A 类杂志 (CCF-A)，为 SCI 索引刊物，当前影响因子为 3.111。

天津大学国家保密学院参观实验室

2015 年 9 月 29 日下午，天津大学国家保密学院学生来实验室参观。各课题组代表在展室向来室学生展示了近期研究成果，并回答了学生提问。




科研进展

实验室两项算法研究成果被 IJCAI 2015 录用

人工智能国际联合大会（IJCAI）是 AAAI 协会两年一度的学术性会议，是世界顶级的人工智能会议之一，2015 年 7 月在阿根廷布宜诺斯艾利斯举办。信息安全国家重点实验室郭晓杰助理研究员完成的两项工作"Robust Subspace Segmentation by Simultaneously Learning Data Representations and Their Affinity Matrix" 以及 "Online Robust Low Rank Matrix Recovery" 被人工智能领域顶级会议人工智能国际联合大会 IJCAI 2015 录用。

大数据时代，对数据进行有效的分类及分析是一个重要且极具挑战性的问题。根据数据统计意义上的分布特性，子空间是最为流行的数据“容器”之一。虽然在过去的 10-20 年，大量的相关研究，特别是基于谱聚类方法的研究，获得一系列的进展，但始终围绕着数据表达的框架展开。"Robust Subspace Segmentation by Simultaneously Learning Data Representations and Their Affinity Matrix"这项工作试图突破这一框架，即同时学习数据表达和相似性矩阵。该项工作获得了 IJCAI 专家的一致认可，并被推荐为 20 分钟大会报告。

另一项工作"Online Robust Low Rank Matrix Recovery"提出了一种鲁棒的在线低秩矩阵恢复的算法。低秩矩阵数据在现实应用中广泛存在，例如人脸识别，视频监控，数据恢复等。该工作主要从两项指标上作出了改进：一、对数据噪音和破坏具有更强的鲁棒性； 二、对大数据而言，可通过轻便的在线方式对数据进行处理。该项工作在 IJCAI 大会上给出了 10 分钟大会报告。

实验室图像标注算法研究成果取得突破

IEEE Transaction on Image Processing 是多媒体内容安全和图像处理方向的顶级期刊之一，被中国计算机协会（CCF）评定等级为 A 类国际期刊。信息安全国家重点实验室张华助理研究员等人完成的关于图像语义标注的工作《SLED: Semantic Label Embedding Dictionary Representation for Multi-label Image Annotation》被录用并刊登在该期刊 2015 年第 9 期。

随着移动互联网技术的发展，网络上存在着大量由用户上传的图像信息。用户上传信息的随意性使大量的图像信息不存在任何标注。如何有效地利用这些图像信息并挖掘出其中的有价值信息和危害信息是多媒体方向重要的研究问题。该篇论文通过利用语义标签之间的共存性和互斥性进行字典特征表示学习并且将该语义特征嵌入到图像特征表示中去，最后利用嵌入语义特征的图像特征表示进行图像标注。

实验室视频信息隐藏研究获得显著进展

2015 年，实验室在视频信息隐藏研究方面获得显著进展，在学术和应用方面取得取了一系列成果。

首先，在视频隐写防范方面，首次将自适应分析策略成功应用于隐写分析，从而显著提高了专用隐写分析特征的针对性和有效性。另外，基于改进的视频校准技术，提高了现有针对运动向量和帧内预测模式检测技术的有效性。相关论文发表在今年的 IEEE International Conference on Multimedia and Expo (ICME)、International Workshop on Digital-forensics and Watermarking (IWDW)、IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP)等多媒体信息安全领域重要国际学术会议上。

其次，在视频隐藏算法方面，就安全嵌入容量和嵌入策略等隐写核心问题进行了深入研究，首次提出了保持“局部最优性”的视频隐写方法，从而能够在很大程度上减轻传统视频隐写方法对压缩编码准则的扰动，提高抗检测能力。相关论文发表在今年的 IEEE Communications Letters、ACM Workshop on Information Hiding and Multimedia Security (ACM IH & MMSec)、Multimedia Tools and Applications、IEEE International Symposium on Cyberspace Safety and Security (CSS 2015)等多媒体信息安全领域重要国际刊物及学术会议上，博士生张凌宇等人完成的论文还获得 CSS 2015 最佳论文奖(IEEE Best Paper Award)。

另外，实验室今年基于视频相关研究成果申请国家专利 4 项，提交相关部门成果系统 2 套，并于重大线上系统得到应用。

国际交流与合作

澳大利亚麦考瑞大学 Vijay Varadharajan 教授访问实验室

2015 年 06 月 22 日至 07 月 14 日，应信息安全国家重点实验室邀请，澳大利亚麦考瑞大学 Vijay Varadharajan 教授来实验室进行访问交流。

来访期间，Vijay 教授做了题为 《Trust in Crypto Role-based Access Control for Secure Cloud Data Storage》和《Security as a Service Model for Cloud Environment》的学术报告。报告介绍了云计算环境下数据安全存储、安全访问的重要性，同时着重介绍了 Vijay 团队近年针对云存储与访问控制方面提出的基于角色的运算存储加密方案以及云环境下硬、软件可信模型等一系列最新研究成果。

Vijay 教授在访问期间与实验室科研人员就云计算安全、物联网安全以及移动互联网安全等研究方面的有关问题作了深入交流，并就双方进一步的科研合作进行了探讨。

意大利罗马第二大学 René Schoof 教授访问实验室

2015 年 7 月 15 日至 8 月 1 日，应信息安全国家重点实验室邀请，意大利罗马第二大学 René Schoof 教授来实验室进行学术访问和交流。

来访期间，Schoof 教授开设了题为《Arakelov Class Group and LLL》的系列学术讲座，分四次报告系统介绍了代数数域的 Arakelov 类群及其与理想格的联系，并重点介绍了与之相关的一些计算数论问题。近年来，作为后量子密码的候选者，格密码成为密码学领域的热门研究课题，特别是理想格成为构造全同态加密、多线性映射等密码方案的重要工具。Schoof 教授的讲座深入浅出地介绍了与理想格相关的深刻的现代数学理论及其本人的相关工作，吸引了实验室多名成员以及来自清华大学、中科院数学院等多家兄弟单位科研人员、研究生的参加，引起了听众浓厚的兴趣和热烈的讨论。

访问期间，Schoof 教授与实验室科研人员就格理论、计算数论等方面的相关问题进行了深入交流，并探讨了双方进一步研究中可以开展合作的研究课题。受南开大学扶磊教授邀请，Schoof 教授还于 7 月 26 日至 7 月 30 日顺访了南开大学陈省身数学研究所，并作了题为《Serre’s uniformity conjecture》的学术报告。

美国克莱姆森大学 Shuhong Gao 教授访问实验室

2015 年 7 月 23 日至 8 月 2 日，应信息安全国家重点实验室邀请，美国克莱姆森大学 Shuhong Gao 教授来实验室进行合作研究

和学术交流。

来访期间，Shuhong Gao 教授做了题为《Expander graphs and linear codes》的学术报告。扩展图是一个重要概念，在数学和计算机科学中有广泛的应用。报告介绍了扩展图与可快速解码的线性码之间的联系，以及 Shuhong Gao 团队近期在此方面的一系列研究成果。在报告的最后，Shuhong Gao 教授给出了该领域的一些公开问题。

Gao 教授在访问期间与实验室科研人员就有限域上的置换多项式、主要部件的构造、利用代数方法进行密码分析等一些问题进行了深入交流，对部分问题展开合作研究，并就双方进一步的合作方向进行了探讨。

美国宾夕法尼亚州立大学 Dinghao Wu 教授访问实验室

2015 年 7 月 29 日至 2015 年 8 月 2 日，应信息安全国家重点实验室邀请，美国宾夕法尼亚州立大学 Dinghao Wu 教授来实验室进行学术交流。来访期间，吴教授做了题为《Towards Obfuscation-Resilient Software Plagiarism Detection》的学术报告，针对软件剽窃提出了一种检测方法，吸引了研究所数十名科研人员与研究生到会参加。吴教授在报告中提出了针对 PC 应用程序利用程序逻辑和最长 semantically-equivalent-basic-block 序列进行剽窃检测的方法，此方法可以检测部分程序剽窃，同时可以提供对 obfuscation resilience 的保障，并详细介绍了软件剽窃检测的最新研究成果。

吴教授访问期间，还与实验室科研人员就双方研究中的有关问题进行了学术交流，对双方进一步在科研项目中的合作研究进行了探讨。

澳大利亚新南威尔士大学 Jiankun Hu 教授访问实验室

2015 年 09 月 07 日至 09 月 21 日，应信息安全国家重点实验室邀请，澳大利亚新南威尔士大学 Jiankun Hu 教授来实验室进行学术访问和交流。

来访期间，Jiankun Hu 教授做了题为《A New Biocryptosystem-oriented Security Analysis Framework》的学术报告，介绍了基于机器学习理论的网络攻击检测的新方法，并着重介绍了生物密码系统安全分析的新理论以及多模态生物特征识别的性能上界。近年来，生物密码得到

越来越多的关注，但生物密码系统的安全性分析缺乏理论支撑，Jiankun Hu 教授的报告深入浅出地介绍了他们团队提出的基于熵和复杂性的生物密码系统安全分析理论。

Jiankun Hu 教授在访问期间与实验室科研人员就攻击检测、密文检索、生物密码生成算法等研究方面的有关问题进行了深入探讨，并就双方进一步的科研合作进行了交流。

荆继武研究员赴美国宾夕法尼亚州立大学开展学术交流访问

应美国宾夕法尼亚州立大学 LINOS 中心刘鹏教授邀请，实验室荆继武研究员于 2015 年 8 月 7 日—8 月 22 日到 LINOS 中心开展学术交流访问。美国宾西法尼亚州立大学 LIONS 中心是刘鹏教授创立的信息安全研究中心，是美国重要的信息安全技术研究中心之一。刘鹏教授与荆继武老师的研究团队保持着长期的密切合作研究关系。

访问期间，荆继武研究员与 LIONS 中心研究人员就网络安全技术、隐私保护技术、计算过程可信确保技术等具体研究内容开展了深入系统的交流。通过座谈和实地考察，进一步了解了双方的技术发展具体情况。此次交流访问进一步清晰了美国宾夕法尼亚大学 LIONS 中心与实验室开展学术研究合作的具体技术点，为进一步推动实验室学术水平提高起到了推动作用。

在访问期间，荆继武研究员受刘鹏教授邀请，一同参加了在华盛顿 DC 举办的 USENIX Security Symposium 2015。并团队在华盛顿 DC 附近研究机构开展交流合作的孙赫、管乐等同学进行了座谈，了解了他们的交流学习情况。其中，孙赫同学的最新研究成果，被信息安全界的顶级国际会议 ACM CCS 2015 录用，显示了我们开展国际交流合作的成果。

曹纭高级工程师赴意大利参加 IEEE ICME 2015 国际会议

2015 年 6 月 29 日至 7 月 3 日，实验室曹纭高级工程师赴意大利都灵参加了 2015 年多媒体与博览国际会议（2015 IEEE International Conference on Multimedia and Expo，简称 ICME）。ICME 是多媒体技术领域的旗舰会议之一，由 IEEE 下属的计算机学会、通信学会、信号处理学会和电路与系统学会等四大学术组织联合主办，每年举办一次。

本次会议实验室有一篇题为《An Adaptive Detecting Strategy Against Motion Vector-Based Steganography》的论文被接收。该论文提供了一种内容自适应的视频隐写分析策略，解决了载体嵌入容量不均导致的分析特征有效性下降问题。该策略基于定义的“帧动态度”和“可疑运动矢量”，首先将待测视频序列按时序划分成变长检测区间，进而对区间内的可疑区域进行定位，从而能够显著提高提取特征的针对性和有效性。曹纭高级工程师在会议期间对该项技术以及课题组近年来在视频隐写与分析领域取得的其他系列成果进行了介绍，并与与会专家进行了深入的交流。

陈恺副研究员赴美国参加 USENIX Security 2015 国际会议

2015 年 8 月 12 日至 8 月 14 日，信息安全国家重点实验室陈恺研究员赴美国华盛顿参加 2015 年著名信息安全会议 USENIX Security 2015 并做大会报告。USENIX Security 是信息安全领域“四大”顶级会议之一（CCF-A 类），所刊载的论文往往代表着国际信息安全领域的最新研究方向，每年举办一次。

实验室文章《Finding Unknown Malice in 10 Seconds: Mass Vetting for New Threats at the Google-Play Scale》被本次会议接收。文章提出了一种快速高效的移动应用未知（行为）恶意代码检测方法，该方法在软件同源性基础上对 Android 软件进行“同源”与“非同源”分类，并进行函数级和视图级别的相关性分析，从而快速定位恶意代码。陈恺及其团队利用该方法已实现了对 33 个 Android 软件市场、120 万个 Android 应用的检测分析，发现共计 12 万恶意软件(至少 2000 个软件被下载 50000 次以上，影响 1 亿以上用户)。该方法对一个软件应用检测时间仅需不到 10 秒，在相关领域产生了很大的影响。

这是中国科学院首次在该顶级学术会议上发表论文。会议期间，陈恺副研究员对该项技术及课题组近年来在移动终端安全领域取得的系列成果进行了介绍，并同与会专家进行深入交流，取得了很好的效果。

张锐研究员、王伟博士参加 ESORICS 2015 国际会议

2015 年 9 月 21 日至 9 月 25 日，信息安全国家重点实验室张锐研究员、王伟博士赴奥地利参加了第 20 届欧洲计算机安全研究大会（European Symposium on Research in Computer Security 2015，简称 ESORICS 2015）。

ESORICS 2015 欧洲计算机安全研究大会是国际计算机安全技术学术与科技交流的重要平台，每一年举办一次，是计算机学会（CCF）网络与信息安全方向 B 类中排名前三的著名国际会议。本次大会一共收到 293 篇投稿，录用了 59 篇论文做大会报告，录取率为 20%。

实验室文章《Updatable Hash Proof System and Its Applications》和《vBox: Proactively Establishing Secure Channels between Wireless Devices without Prior Knowledge》被本次会议接收。《Updatable Hash Proof System and Its Applications》论文提出了连续泄露模型下构造公钥加密方案较为一般的方法，其优点是只需要将既存文献中用来构造非连续有限泄露安全的众所周知的哈希证明系统（Hash Proof System，简称 HPS）做一些“自然的扩展”，原来基于 HPS 构造的非泄露容忍安全的公钥加密构造方法不用任何改变，就可用来构造连续泄露模型下的公钥加密方案。论文还给出了基于不同假设的多种具体实现方法，这些大大提高了已知方案的效率。《vBox: Proactively Establishing Secure Channels between Wireless Devices without Prior Knowledge》创造性地提出和实现了一种利用无线信号传播特征在无线设备之间创建安全信道的方法，相比于现有工作具有更高的易用性和执行效率。

会议期间，张锐研究员和王伟博士应邀就论文作学术报告并回答了相关学术问题，并在会后与来自法国、新加坡、香港等地的研究者进行了广泛的讨论。张锐研究员还对课题组近年来在泄露容忍密码学领域取得的系列成果进行了介绍。此次参会不仅加强了与国际著名学术机构与学术同行之间的学术交流，还促进了我们对最新学术前沿动态与趋势的了解。

获奖情况

许倩倩助理研究员喜获中国人工智能学会优秀博士学位论文奖

2015 年度中国人工智能学会优秀博士学位论文颁奖典礼于 8 月 14 日在上海长荣桂冠酒店举行，信息安全国家重点实验室许倩倩助理研究员的博士学位论文《基于几何拓扑和心理学准则的图像、视频质量评价方法研究》获得优秀博士学位论文奖。该论文针对多媒体质量评价中主客观一致性欠佳的问题，提出以心理学准则、组合 Hodge 理论及随机图为核心的评价体系，降低了采样复杂性的同时提升了评价的准确性。

本次共评选出 8 篇学会优秀博士学位论文以及 3 篇提名论文，许倩倩助理研究员是获此殊荣的唯一女性科研工作者。

许倩倩在颁奖典礼领奖（左三）

实验室论文获 IEEETRUSTCOM 2015“Best Paper Award”

在 2015 年 8 月 20-22 日于芬兰赫尔辛基市举办的 The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications（IEEE TRUSTCOM-15）会议上，信息安全国家重点实验室博士研究生王彦超等人完成的论文“Achieving Lightweight and Secure Access Control in Multi-Authority Cloud”获得 IEEE TRUSTCOM 2015“Best Paper Award”。

IEEE TRUSTCOM 会议作为由 IEEE 主办的年度系列会议之一，自 1998 年已成功举办 14 届。会议以可信网络与通信，计算与通信系统中可信计算、网络安全与隐私保护为主要研讨题目进行研讨交流，是该领域内重要的国际会议之一。

实验室论文获 CSS 2015“IEEE Best Paper Award”

在 2015 年 8 月 24-26 日于美国纽约市举行的 7th IEEE International Symposium on Cyberspace Safety and Security（CSS 2015）会议上，信息安全国家重点实验室博士生张凌宇等人完成的论文“A Practical Method to Determine Achievable Rates for Secure Steganography”获得“IEEE Best Paper Award”。CSS 会议已经在法国巴黎、中国张家界、澳大利亚墨尔本、意大利米兰、中国成都、澳大利亚悉尼、美国纽约市成功举办了 7 届，已经在网络空间安全领域受到重要关注。

以上论文解决的主要问题是，在基于信息隐藏的保密通信中，如何针对给定载体图像内容的不同智能地确定信息隐藏的安全嵌入率，确保载密后的图像难以被检测。该论文提出了一种基于非线性回归的方法，它能够通过机器学习在被检测率和嵌入率之间形成映射关系。分析和实验说明，该方法能够很好地指导对安全嵌入率的动态确定，提高了信息隐藏保密通信的隐蔽性。

党群园地

实验室举办“科研过程中的文献资源与服务利用”讲座

为帮助科研人员和学生更有效地利用文献资源与服务，助力科研工作，9 月 30 日下午，信息安全国家重点实验室邀请中科院文献情报中心学科馆员李海英老师来室举办了题为“科研过程中的文献资源与服务利用”的主题讲座。

讲座中，李海英老师首先介绍了中科院及信工所可用的文献资源以及文献情报中心提供的服务，随后介绍了信息检索与分析方法，最后对文献管理软件 Endnote 的使用进行了演示。

此次讲座使科研人员和学生对中科院及信工所拥有的图书和信息资源有了系统认识，对中科院文献情报中心提供的相关服务有了一定了解，对新入室职工和学生尽快掌握中科院的文献资源与服务利用方法，便利今后的学习和科研工作有着积极的引导作用。

信工所第三党总支举办“职工科技合作素养与礼仪培训”

在当前全国深入开展“三严三实”学习教育活动的形势下，为响应党中央号召，更好地在三室开展“三严三实”学习教育活动，进一步加强三室党总支的作风建设，第三研究室党总支（简称，三室党总支）于 2015 年 9 月 29 日组织开展了《职工科技养与礼仪培训》活动。活动主要围绕三个主题进行：（1）践行“严以修身、严以律己”的作风建设要求；（2）在工作中建立有效的科研合作和沟通机制，营造风清气正、务实实干的良好环境，提升科研团队的整体素质和形象；（3）规范工作作风，进一步加强党员干部的服务意识，培养更好的行为规范和道德素养。

活动历时 3 小时，邀请的张会英老师从优雅仪表形貌，优雅仪态、举止，接待礼仪规范，职业素养等方面进行了生动、详细的介绍。培训现场气氛活跃，互动良好，大家在高涨的学习氛围中掌握了许多实用性强的社交礼仪知识，同时也加强了了解与沟通。

SKLOIS
信息安全国家重点实验室

电话：+86-10-82546611
传真：+86-10-82546564
邮箱：sklois@iie.ac.cn
网站：http://www.sklois.cn