# 会议简介 壹

随着互联网的迅速发展，网络应用变得越来越广泛和深入，网络攻击手段与方式也层出不穷，更加精密和强大，网络与信息安全问题更加突出，形势日益严峻。习近平总书记在中央网络安全和信息化领导小组第一次会议中指出：“没有网络安全就没有国家安全，没有信息化就没有现代化。” 因此，网络安全和信息化已成为事关国家安全和国家发展的重大战略问题。无论在政府、工业界还是在学术界，网络空间安全等研究领域一直是大家关注的研究热点之一。

网络空间安全国际研讨会（International Workshop on Cyber Security）应时代发展而设立，关注网络空间安全领域的热点、前沿、重要学术问题。第一届会议于 2015 年在西安举办，后续会议在厦门、武汉、北京、广州、南京、天津、杭州等地举办。本次会议重回广州， 由中山大学承办、广东省信息安全技术重点实验室协办、广州信睿网络科技有限公司支持，邀请了十余位业内专家做特邀报告，报告内容涉及网络空间安全、密码学、数据安全、网络安全等多个方面，诚邀各位学者专家共聚羊城！

# 贰 委员会成员

## 大会主席

张方国

中山大学

## 程序委员会主席

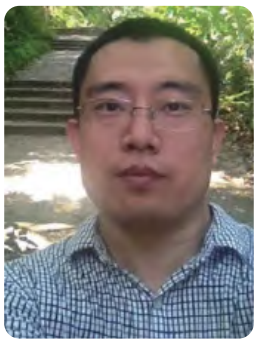
陈晓峰

西安电子科技大学

黄欣沂

暨南大学

## 组织委员会主席



田海博

中山大学

# 会议日程 叁

| 2025 年 5 月 16 日 | | | | |
|---|---|---|---|---|
| 时间 | 内容 | | 地点 | 主持人 |
| 12:00-21:00 | 参会人员注册 | | 酒店大堂 | |
| **2025 年 5 月 17 日** | | | | |
| 时间 | 内容 | | 地点 | 主持人 |
| 08:30-08:50 | 开幕式 | 领导致辞 | 丽晶殿 A 厅 | 张方国 |
| 08:50-09:00 | 参会代表合影 | | | |
| 09:00-09:40 | 特邀报告一 | 黄继武 教授　深圳北理莫斯科大学<br>题目：图像篡改定位模型的对抗 | 丽晶殿 A 厅 | 李进 |
| 09:40-10:20 | 特邀报告二 | 贾焰 教授　国防科技大学<br>题目：网络空间安全态势感知：技术、系统与应用 | | |
| 10:20-10:35 | 茶歇 | | | |
| 10:35-11:15 | 特邀报告三 | Prof. Willy Susilo　University of Wollongong<br>Title: Securing Databases in the Cloud: Threats and Challenges | 丽晶殿 A 厅 | 伍前红 |
| 11:15-11:55 | 特邀报告四 | 仲盛 教授　南京大学<br>题目：“还不从实招来？”——大模型越狱初探 | | |
| 11:55-14:00 | 午餐 | | 二楼丽廊咖啡厅 | |
| 14:00-14:40 | 特邀报告五 | 刘胜利 教授　上海交通大学<br>题目：口令认证密钥协商协议 | 丽晶殿 A 厅 | 沈剑 |
| 14:40-15:20 | 特邀报告六 | 高飞 教授　北京邮电大学<br>题目：从 Deutsch 算法到 Shor 算法 | | |
| 15:20-15:35 | 茶歇 | | | |
| 15:35-16:15 | 特邀报告七 | 朱天清 教授　澳門城市大學<br>题目：强化遗忘学习初探及应用 | 丽晶殿 A 厅 | 黄欣沂 |
| 16:15-16:55 | 特邀报告八 | Assoc Prof. Guo Jian　Nanyang Technological University<br>Title: An Update on Symmetric-Key Cryptology | | |

| | | | | |
|---|---|---|---|---|
| 16:55-17:35 | 特邀报告九 | 邓燚 教授　中国科学院大学<br>题目：Defining knowing, optimal extractors, and individual reductions | 丽晶殿 A 厅 | 黄欣沂 |
| 18:30-21:30 | 中式晚宴 | | 丽晶殿 A 厅 | |
| **2025 年 5 月 18 日** | | | | |
| 08:30-09:10 | 特邀报告十 | Prof. Yang Xiang　Swinburne University of Technology, Australia<br>Title: Securing AI Systems: from Development to Deployment | 丽晶殿 A 厅 | 张福泰 |
| 09:10-09:50 | 特邀报告十一 | Prof. Man Ho Allen Au　University of Hong Kong<br>Title: JesseQ: Efficient Zero-Knowledge Proofs for Circuits over Any Field | | |
| 09:50-10:05 | 茶歇 | | | |
| 10:05-10:45 | 特邀报告十二 | 张海滨 教授　浙江清华长三角研究院<br>题目：多模态大模型及其应用：数据层、模型层、应用层 | 丽晶殿 A 厅 | 汪定 |
| 10:45-11:25 | 特邀报告十三 | 路献辉 研究员　中国科学院信息工程研究所<br>题目：高效同态自举算法设计 | | |
| 11:25-12:05 | 特邀报告十四 | 陈荣茂 副研究员　国防科技大学<br>题目：抗量子密码算法的紧致归约技术 | | |
| 12:05-14:00 | 午餐 | | 二楼丽廊咖啡厅 | |

# 特邀报告专家 肆

## 黄继武 教授　深圳北理莫斯科大学

**报告题目：图像篡改定位模型的对抗**

**个人简介：**黄继武，工学博士。深圳北理莫斯科大学教授、IEEE Fellow。广东省网络与信息安全产学研创新联盟理事长。获国家杰出青年科学基金。入选广东省特支计划杰出人才。分别毕业于西安电子科技大学（电子对抗专业，学士）、清华大学（通信与信息系统专业，硕士）、中国科学院自动化所（模式识别与智能系统专业，博士）。研究兴趣为多媒体取证与安全、信息隐藏。曾获国家自然科学二等奖（排名第二）、教育部自然科学一等奖（排名第一）、中国计算机学会自然科学一等奖（排名第一）、广东省教学成果一等奖（排名第一）。在本领域发表学术论文 350 多篇，google 引用 23000 多次，H-index 80。

**报告摘要：**

篡改图像因其视觉难以察觉给社会和公共安全带来了很大的安全隐患，篡改定位的目标是检测并定位篡改区域。AI 模型在给图像篡改定位提供强大工具的同时，其自身也存在脆弱性。攻击者可以利用这些脆弱性针对篡改定位模型进行对抗性攻击，以逃避篡改定位的检测。本报告围绕图像篡改定位任务，结合本实验室的相关工作，介绍了面向篡改定位任务的 AI 模型的对抗，包括图像篡改定位背景、图像篡改定位模型的攻击、图像篡改定位模型的防御。最后，讨论了这一领域所面临的挑战。

## 贾焰 教授　国防科技大学

**报告题目：网络空间安全态势感知：技术、系统与应用**

**个人简介：**贾焰博士，国防科大研究员，现任国家重大攻关项目负责人，工业控制系统信息安全技术国家工程研究中心首席，中国中文信息学会副理事长等职。主要研究方向为人工智能和大数据分析技术在网络空间安全领域中的应用；作为课题负责人承担和主持了国家级重大 / 重点项目 20 余项；获国家科技进步二等奖 5 项；发表进入 SCI 和 EI 检索的论文 320 余篇，出版专著 8 部，获得 100 余项发明专利；国际论坛 FFD、国际会议 IEEE DSC 和 CSE 等的主要发起人和负责人。

**报告摘要：**

报告从网络空间安全态势感知的概念和重要地位出发，首先给出了态势感知的三大应用需求：内容安全舆情事件态势感知，系统安全攻击事件态势感知，以及攻防对抗态势评估；其次给出针对该应用需求的三大挑战：准确、实时和全面；再次给出解决这些挑战的多维关联认知模型 MDATA 及其发展技术；最后给出相关理论和技术的应用和效果。

**Prof. Yang Xiang**
**Swinburne University of Technology, Australia**

**Title:** **Securing AI Systems: from Development to Deployment**

**Bio:**

Professor Yang Xiang received his PhD in Computer Science from Deakin University, Australia. He is currently a full professor and the Director of Digital Capability Research Platform, Swinburne University of Technology, Australia. In the past 20 years, he has been working in the broad area of Cybersecurity, which covers software, system, network, and application security. He has published more than 300 research papers in many international conferences and journals in Cybersecurity, such as ACM CCS, IEEE S&P, Usenix Security, NDSS, IEEE TDSC, and IEEE TIFS. He is the Editor-in-Chief of the SpringerBriefs on Cyber Security Systems and Networks. He serves as the Associate Editor of the ACM Computing Surveys. He served as the Associate Editor of IEEE Transactions on Dependable and Secure Computing, IEEE Internet of Things Journal, IEEE Transactions on Computers, and IEEE Transactions on Parallel and Distributed Systems. He is a current member of College of Experts (CoE) of the Australian Research Council (ARC). He is a Fellow of the IEEE.

**Abstract:**

The rapid advancement of artificial intelligence (AI) systems has led to their integration into a multitude of applications, necessitating innovative security measures to safeguard these systems throughout their lifecycle. AI models, while highly accurate, are inherently vulnerable to a variety of sophisticated attacks, posing significant risks to their security and trustworthiness. In this presentation, we will examine the comprehensive security challenges faced by AI systems from their development phase to deployment. We will delve into advanced defensive methods to detect and neutralize sophisticated attacks, which jeopardize the security and integrity of AI systems during development. We will explore the vulnerabilities of AI systems, highlighting the threats to AI model availability during deployment. Furthermore, we will dissect the accountability of AI code generators from both development and deployment perspectives, providing valuable insights into ensuring accountability throughout the AI system lifecycle.

**Prof. Willy Susilo**
**University of Wollongong**

**Title:** **Securing Databases in the Cloud: Threats and Challenges**

## Bio:

Willy Susilo is a Distinguished Professor at the School of Computing and Information Technology, Faculty of Engineering and Information Sciences at the University of Wollongong (UOW), Australia.He holds the most prestigious Australian Laureate Fellowship awarded by the Australian Research Council. He is the director of Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, UOW.In 2024, he was awarded 2024 NSW Premier's Prizes for Science and Engineering due to his research work.He is an IEEE Fellow, an IET Fellow, an ACS Fellow, an AAIA Fellow and an AIIA Fellow. Previously, he was awarded the prestigious Australian Research Council Future Fellowship in 2009. He has published more than 500 papers in journals and conference proceedings in cryptography and network security. He is the Editor-in-Chief of the Information journal and a newly launched Pragmatic Cybersecurity journal, and the Special Content Editor of the Elsevier’ s Computer Standards and Interfaces. He is also serving as an Associate Editors in several international journals, including IEEE Transactions. He has also served as the program committee member of several international conferences.

## Abstract:

In the era of information technology, the demand for flexible and scalable data management has driven the widespread adoption of cloud-based database services. Outsourcing databases to the cloud allows organizations to reduce costs and enhance accessibility, but it also raises significant security concerns due to the potentially untrusted nature of third-party cloud providers. We give a simple review of a range of cryptographic techniques proposed to address these issues. Special attention is given to methods such as property preserving encryption and homomorphic encryption. Despite substantial progress, various inference attacks still exist. We conclude by identifying future challenges for developing more robust and efficient solutions for secure cloud database systems.

**仲盛 教授　南京大学**

**报告题目：“还不从实招来？”——大模型越狱初探**

**个人简介：**南京大学二级教授、软件学院院长。长江学者特聘教授，国家杰出青年科学基金获得者，万人计划科技创新领军人才，中国计算机学会会士、IEEE Fellow。南京大学学士、硕士，耶鲁大学博士。曾任教于纽约州立大学布法罗分校，获得美国国家科学基金会 CAREER Award，并提前晋升终身教职。现兼任中国计算机学会理事、ACM 南京分会主席，以及多家学术期刊编委。研究兴趣包括安全、隐私和经济激励。

**报告摘要：**

以 ChatGPT 为代表的大模型是当前人工智能的研究热点。大模型的管理者为大模型设置了诸多安全限制，以防其说出与非法活动相关的话，或者说出特别敏感、可能引起争议的话。然而，通过巧妙的引导完全有可能突破这些安全限制，这就是所谓的大模型越狱（LLM Jailbreak）。我们对此做了一些探索，取得了较好的越狱效果。

**刘胜利 特聘教授　上海交通大学**

**报告题目：口令认证密钥协商协议**

**个人简介：**刘胜利先后从西安电子科技大学和埃因霍芬理工大学获得学士、硕士和博士学位。2002 年加入上海交通大学，现任上海交大计算机系特聘教授。研究领域为公钥密码算法设计与证明、模糊提取器的设计与证明、认证性密钥协商协议等。

**报告摘要：**

本报告介绍口令密钥协商协议（PAKE）以及协议的 UC 安全，进一步讨论能够实现后量子 UC 安全的 PAKE 协议的新设计框架，并在新框架下介绍如何对多个 PAKE 协议进行融合，以提高其 UC 安全性。

## 陈荣茂 研究员　国防科技大学

**报告题目：抗量子密码算法的紧致归约技术**

**个人简介：** 陈荣茂，国防科技大学计算机学院研究员，博士生导师，主持和承担国家自然科学基金青年基金（B类）、重点项目和中国科协青托工程等项目，长期从事公钥密码理论与应用研究，在 Crypto、Asiacrypt、S&P、PKC、CHES 等发表多篇学术论文，指导学生获得中国密码学会优秀博士论文、湖南省优秀博士 / 硕士学位论文等，担任 IACR CiC/IEEE TDSC/JCST 编委以及 ASIACRYPT/ACM CCS/PKC 等国际会议程序委员会委员，入选特殊领域高层次人才工程。

**报告摘要：**

安全且高效的抗量子密码算法是现有公钥密码向后量子密码迁移面临的迫切需求。具备紧致安全的抗量子密码算法在同等安全级别下一般具有更好的实际部署性能，是抗量子密码算法设计所追求的一个重要目标，也是所面临的一大挑战。本报告将聚焦抗量子密钥封装机制 KEM 的紧致安全归约技术，重点介绍我们课题组关于 KEM 在 ROM 和 QROM 下的安全归约优化研究进展。

## 邓燚 教授　中国科学院大学

**报告题目：Defining knowing, optimal extractors, and individual reductions**

**个人简介：** 邓燚，中国科学院大学网络空间安全学院教授，中国科学院信息工程研究所研究员，博士生导师。主要从事理论密码学与计算复杂性的交叉领域研究，包括零知识证明，安全性归约技术，伪随机性及密码协议的轮 / 通信 / 计算复杂性等。曾获首届中国密码学会优秀青年奖，首届中国密码学会创新奖一等奖。

**报告摘要：**

传统上我们说一个机器 S 知道某个问题的答案，是指我们能够构造一个（依赖 S 的）新机器 R，它能将该答案输出来。本报告里我们考虑 R 的存在性（而非构造性），并证明对任意的 NP 实例的抽样机器，都存在一个几乎最有的证据（答案）抽取机器。我们将介绍如何在密码构造安全性归约中利用这一最优抽取器来解析敌手的结构特征，进而开发依赖具体敌手的（存在性的）个体化归约。结合知识加密这一新概念，我们突破了一系列基础性密码协议（包括零知识证明，不经意传输 / 安全两方计算，以及最近的不可延展承诺等）交互轮数的黑盒归约下界，给出了更低轮复杂度的相应协议构造。

**Assoc Prof. Guo Jian**
**Nanyang Technological University**

**Title: An Update on Symmetric-Key Cryptology**

## Bio:

Dr. Guo Jian obtained his PhD in cryptography from Nanyang Technological University in Singapore, under the supervision of Prof Wang Huaxiong in year 2011. He is currently a tenured Associate Professor with NTU. His major research interest is symmetric-key cryptography. He co-designed PHOTON --- one of the ISO standards of lightweight hash functions, CLOC and SILC authenticated ciphers --- one of the third-round candidates of the CAESAR competition, as well as LED --- one of the lightest block ciphers suitable for constrained hardware. He has done some intensive cryptanalysis against various cryptographic primitives including the latest NIST hash function standard SHA-3 and AES, on which he and his team won several awards. Among others, he published more than 50 papers in conferences/workshops under the International Association for Cryptologic Research (IACR). He is a founding co-chair of ASK — the Asian workshop on Symmetric-Key cryptography. He served as a Program Co-Chair of Asiacrypt 2023, the General (Co-)Chair of Asiacrypt 2021 and FSE 2013, a Program Committee Member of FSE, Asiacrypt, Eurocrypt, Crypto, and ACM CCS constantly. He is an elected director of IACR Board since 2022, a member of ASIACRYPT steering committee representing for Singapore since 2017, and a member of the Security and Privacy Standards Technical Committee in Singapore acting as delegate of the International Standardization ISO/IEC JTC 1/SC 27 since 2017. He also actively collaborates with industry in forms of being a consultant for multiple companies including Huawei, JD, and being the Principal Investigator for R&D projects with PayPal Inc. Within NTU, he also co-founded and has been a Director of the Master of Science in Cyber Security program. He also founds and leads the Cryptanalysis Taskforce research team since 2014.

## Abstract:

In this talk, we will provide a realistic summary of the recent developments of cryptanalysis methodologies, including those by automated tools, and machine learning. Through these, a projection of future developments in the next decade or two is provided.

**Prof. Man Ho Allen Au**
**University of Hong Kong**

**Title: JesseQ: Efficient Zero-Knowledge Proofs for Circuits over Any Field**

**Bio:**

Prof. Man Ho Allen Au is a Professor and Associate Head (Research and Development) in the Department of Computing at The Hong Kong Polytechnic University, and an Honorary Professor in the Department of Computer Science at the University of Hong Kong. He previously held faculty positions at the University of Hong Kong and the University of Wollongong. His research interests lie in information security, cryptography, blockchain technology, and their practical applications. Prof. Au has authored over 200 refereed papers in top-tier journals and conferences, including CRYPTO, ASIACRYPT, ACM CCS, NDSS, IEEE S&P, SIGMOD, SOSP, IEEE TIFS, and IEEE TDSC. His work has been recognized with several prestigious honors, including the 2024–25 Hong Kong Engineering Science and Technology (HKEST) Award, the 2023 BOCHK Science and Technology Innovation Prize (STIP) in FinTech, the 2009 PET runner-up award for outstanding research in privacy-enhancing technologies, and as a two-time winner of the ZPrize competition. He has served as general or program committee chair for numerous international conferences, such as ACM ASIACCS, RAID, SECURECOM, IEEE Blockchain, ISPEC, and PROVSEC. He currently serves as an Associate Editor for IEEE Transactions on Dependable and Secure Computing (TDSC) and the Journal of Information Security and Applications (JISA). In addition, Prof. Au is an Advisory Board member of ELSP Blockchain and a member of the CBDC Expert Group of the Hong Kong Monetary Authority.

**Abstract:**

Zero-knowledge proofs, a fundamental cryptographic primitive, enable one party to convince another of the validity of a statement without revealing any additional information. Recent advancements have highlighted VOLE-based protocols as a highly efficient approach for generating zero-knowledge proofs at scale, opening up new possibilities for real-time, privacy-preserving computation. In this talk, we introduce JesseQ, our latest zero-knowledge proof system built on Vector Oblivious Linear Evaluation (VOLE). JesseQ supports both arithmetic and Boolean circuits over any field and achieves high performance with minimal overhead. A key highlight of JesseQ is its ability to prove 9.2 trillion AND gates on a low-cost AWS instance for just $1, demonstrating exceptional scalability and cost-effectiveness. Finally, we discuss the practical applications of VOLE-based proofs in real-world scenarios such as zkTLS, verifiable computation, and private authentication.

## 高飞 教授　北京邮电大学

## 报告题目：从 Deutsch 算法到 Shor 算法

**个人简介:** 高飞，男，北京邮电大学教授，国家级青年人才，中国密码学会常务理事、青年工作委员会主任委员，中国计算机学会量子计算专业委员会常务委员，中国电子学会网络空间安全专家委员会委员。主要研究量子密码、量子算法和相关量子信息问题，已在 PRL/PRA、TKDE、TC、JSAC 等重要期刊发表论文 150 余篇，SCI 总引用 7000 余次，H 因子 51。近五年连续入选斯坦福大学“全球前 2% 科学家榜单”、爱思唯尔中国高被引学者。

### 报告摘要：

Shor 算法可以在多项式时间内解决整数分解问题，对量子计算和密码学的发展带来了深刻的影响。Shor 算法的步骤非常简单，但理解其中的道理却并非易事。当前教科书中多从相位估计的角度来介绍 Shor 算法，给该算法的理解带来了很多神秘色彩。本报告从量子操作的并行计算能力开始，以求函数的某个整体性质为主线，逐步介绍 Deutsch 算法、BV 算法、Simon 算法、求周期算法，并尝试理解出现周期的深层次原因。以上内容可以看作是对 Shor 算法的一种不同角度的理解方式。

## 张海滨 教授　浙江清华长三角研究院

## 报告题目：多模态大模型及其应用：数据层、模型层、应用层

**个人简介:** 张海滨，加州大学戴维斯分校博士，清华长三角研究院信息技术研究所所长、通用与具身智能研究中心主任、浙江省欧美同学会理事。主持国家重点研发计划项目、人社部高层次留学回国人才项目、国家自然基金委项目、美国自然基金委项目等。聚焦人工智能、区块链、隐私计算、操作系统等关键领域，在 S&P、CCS、Usenix Security、Asiacrypt、EuroSys、PODC 等发表顶会论文 40 多篇。参与设计并实现多个大型分布式系统与人工智能平台，包括 BChain、迪诺链、大圣（Dashing）、天枢可信数据空间、天问人工智能平台、瑶光大语言模型、人工智能测试 - 评估 - 防御平台、天玑隐私计算平台、中国电信可信数据原子能力平台等。成果广泛应用在工业界，包括多边央行货币桥、亚洲数字支付、国际清算银行、世界最大开源区块链 Hyperledger、柬埔寨央行、印尼央行、越南央行、先正达 MAP Beside、Norton Zone、苹果 iMessage、WhatsApp 等。

### 报告摘要：

尽管大模型的发展迅猛，真正赋能工业生产和智能制造的应用仍显稀少。如何发挥大模型的能力改善现有工业产业的格局是当前科技与生产领域中最重要的问题之一。本报告将介绍大模型的发展历史、现状与创新应用，以及可信大模型的一些进展。

**路献辉 研究员　中国科学院信息工程研究所**

**报告题目：高效同态自举算法设计**

**个人简介：**路献辉，中科院信息工程研究所研究员，网络空间安全防御全国重点实验室副主任，2009 年于西南交通大学获得信息安全专业博士学位，2009-2012 年进入中科院信息安全国家重点实验室从事博士后研究，2012 年进入中科院信工所。主要研究兴趣包括可证明安全理论、抗量子密码、全同态密码、物理层密码，担任国际标准化组织 ISO/IEC 密码工作组专家，参与抗量子密码和全同态密码领域的国际标准化工作。

**报告摘要：**

全同态加密是数据隐私保护的主要技术之一，目前面临的主要技术挑战包括密文膨胀和计算效率低，其中自举操作是全同态加密最耗时的操作之一，近年来取得了快速发展，自举性能不断提升。本报告介绍自举算法的主流设计思路、关键加速技术和目前最新进展情况。

# 伍 特邀嘉宾

张福泰
福建师范大学

李进
广州大学

操晓春
中山大学

何德彪
武汉大学

刘哲理
南开大学

沈剑
浙江理工大学

伍前红
北京航空航天大学


禹勇
陕西师范大学

汪定
南开大学

郑子彬
中山大学

# 主办单位简介 陆

## 中山大学计算机学院

中山大学计算机学院位于广州校区东校园（广州大学城），前身是 1979 年教育部批复设立的计算机科学系。经过 40 余年的建设，学院在学科建设、人才培养、科学研究、师资队伍等方面均取得了显著成绩。学院全面贯彻落实党的教育方针，以党建为引领，以“四个面向”为指导思想，以筑牢学科基础、聚焦战略前沿、推进产学研用作为办院方针，践行“理工结合、学科交叉”，重点发展高性能计算、体系结构与存储、人工智能与无人系统、大数据分析处理、新型网络与分布式系统、云计算与边缘计算、工程计算软件、芯片设计与 EDA 软件、量子计算与新型计算、计算机理论、网络与信息安全、区块链、计算数学等研究方向。聚焦“卡脖子”问题和关键领域，提升学院承担国家重大战略任务的能力，为创新型国家贡献力量。

学院建有国家超级计算广州中心、国家数字家庭工程技术研究中心、2011 高性能计算协同创新中心、教育部超算工程软件工程研究中心、教育部机器智能与先进计算重点实验室、广东省大数据分析与处理重点实验室、广东省计算科学重点实验室、广东省信息安全重点实验室、大数据分析与应用、大数据系统软件国家工程实验室（分中心）、信息技术国家级实验教学示范中心等 7 个国家级和 8 个省部级一流科研平台。

学院拥有一支实力雄厚的师资队伍，包括国家级重点领域创新团队、国家重点研发计划专项专家、教育部国家级高层次人才、国家高层次领军人才、国家百千万人才工程、国家自然科学基金杰出青年基金、优秀青年基金等项目获得者、国家高层次人才特殊支持计划、“全国三八红旗手”、“全国三八红旗手标兵”、各类省部级优秀人才、以及获得国家科技进步特等奖、一、二等奖及省部级奖励的研究队伍。近五年来，学院获国家、省部级和国家一级学会科技奖励 10 多项，获批国家重点研发项目及课题近 20 项、国家自然基金项目过百项、国防重点项目、省级重大科技与重点研发、及国家级和省级创新团队多项，年度科研经费过亿元；以第一单位发表中国计算机学会 CCF A 类和中科院一区期刊会议论文 300 多篇。 学院学科基础积淀深厚，在 USNews、ARWU、ESI 等主流世界排行榜中均位居全球前 100 名。近五年学院在人工智能的 AI Rankings 和 CS Rankings 排名均位于世界前 50 名左右（第 33 名）。在 AI 应用最广泛的计算机视觉方向在 AI Rankings 和 CS Ranking 排名均位于世界前 10 名 。

学院具有本 - 硕 - 博完整的人才培养体系，坚持立德树人根本任务，为党育人、为国育才，

入选首批国家级一流本科专业建设点，结合新工科培育人才，获得广东省教学成果一等奖。研制了世界上规模最大的超算教育实践在线平台“超算习堂”，服务用户 1.3 万人以上，用户分布在全国 1000 余家单位，访问量超过 1600 万人次，提供 100 余门课程实践。针对国家急需的“卡脖子”关键技术人才培养，学院大力加强计算机教育改革力度，设立强化计算机系统结构和超算工程软件方向人才培养的“冯 . 诺依曼”实验班，配备优秀专任教师，配置优势资源，培养高素质计算机类人才。

学院积极开展对外学术交流与合作，已经与美国、德国、新加坡等国家以及港澳台地区的众多著名学府、学术机构和学者建立了广泛的学术交流关系，积极推动学科建设、人才培养、科学研究等方面稳步前进。

计算机学院将抓住机遇、迎接挑战、努力突破，以只争朝夕，不负韶华的时代责任感，为国家培养高素质的计算机人才而努力奋斗，为学校扎根中国大地建设世界一流大学贡献力量！

## 广东省信息安全技术重点实验室

广东省信息安全技术重点实验室于 2004 年经广东省科技厅批准建立，依托中山大学计算机学院和网络空间安全学院共建，是广东省信息安全领域创建最早的研究机构之一。目前，实验室拥有总面积达 3000 平方米的科研场地，聚集了高水平研究人员 38 人。经过多年的发展与积累，近年实验室在省科技厅组织的广东省重点实验室评估中分别获得良好和优秀的好成绩。

- 实验室主任：张方国教授
- 实验室副主任：操晓春教授 康显桂教授 谢晓华教授
- 学术委员会主任：黄继武教授

实验室的发展定位：瞄准国际信息安全学科发展前沿，以信息安全技术基础研究为主，坚持理论与应用并重，密切结合广东省信息安全战略需求，进行前沿性和前瞻性科学研究，逐步发展成为代表广东省、具有国内影响力的研究平台。

实验室主要研究方向：

- 多媒体信息安全技术
- 密码技术与应用
- 人工智能安全及应用
- 网络安全技术

近五年实验室分别获得教育部优秀成果奖一等奖 1 项、二等奖 2 项；广东省科学技术奖一等奖 2 项、二等奖 3 项；国家一级学会奖一等奖 3 项。发表论文 322 篇（中科院大类一区 56 篇，CCF A 类 70 篇，CCF B 类 68 篇）；出版著作 9 部（包括：英文专著 2 部，译著 2 部，国内专著 2 部，教材 1 部）；发明专利授权 347 项（国家专利 3 项，专利转让 20 项）；

引进和培养杰青等人才 27 名，包括：国务院特殊津贴获得者 1 名、国家杰青 1 名、长江学者 1 名、国家万人 1 名、国家优青 4 名、国家创新团队核心成员 1 名，广东省特支计划“杰出人才”1 名，省杰青 4 名，省特支计划 5 名，珠江新星 3 名，中国高被引学者 5 名。

实验室围绕信息安全领域国家和广东省重大需求，积极承担省部级及以上项目 267 项，科研经费 1.3 亿元。包括：国家重点研发计划 9 项（课题 6 项，任务 3 项）；国家自然科学基金项目 12 项（国家杰青 1 项，国家优青 1 项，联合基金 2 项，面上 5 项，青年 3 项）；国家军工项目 13 项；省部级 16 项，其中省卓越青年团队 1 项，省青年提升项目 1 项，省自然 4 项。通过项目研究为国家和广东省信息安全领域的研究和发展贡献自己的力量。


# 柒 参会指南

## 会议地点和住宿信息

CS2025 将会在广州中国大酒店举行。中国大酒店坐落在繁华的城市商业中心流花区商圈，地址是广州市越秀区流花路 122 号。交通极其便利，紧邻地铁二号线越秀公园站出口，机场快线五号线在酒店门口设上下站点，行程约为 45 分钟，距离广州火车站 1.5 公里，乘坐出租车约 5 分钟；至越秀公园、流花湖公园，步行约 15 分钟。

- 房间价格：大床房 550 元 / 间 / 天 / 单早，双床房：650 元 / 间 / 天 / 双早（协议价，需要在注册时明确住宿需求）
- 酒店电话 : 020-8666 6888
- 酒店网站 : https://chinahotelgz.com/zh-hans/

中国大酒店附近有许多其它酒店，例如锦洲大酒店，宜必思酒店等，请参会代表自行选择预定。

## 温馨提示

- 会议期间请将手机设置为静音或震动，请勿在会场内接打电话或大声喧哗。
- 会议期间请妥善保管好个人贵重物品。
- 参会者须在大会期间全程佩戴相关证件出入会场。

## 会务组联系方式

田海博　电话号码：15913189163

会务邮箱：cs2025gz@163.com

# 赞助商（纽创信安）

## 纽创信安公司简介

深圳市纽创信安科技开发有限公司 ( 简称“纽创信安”或“OSR”) 成立于 2014 年，总部位于深圳，在北京、上海、苏州设有分 / 子公司。公司专注于新一代密码关键技术的创新突破与核心产品研发，为云计算、数据要素以及网络安全领域提供创新的商用密码产品和解决方案，致力于成为全球领先的密码服务商。

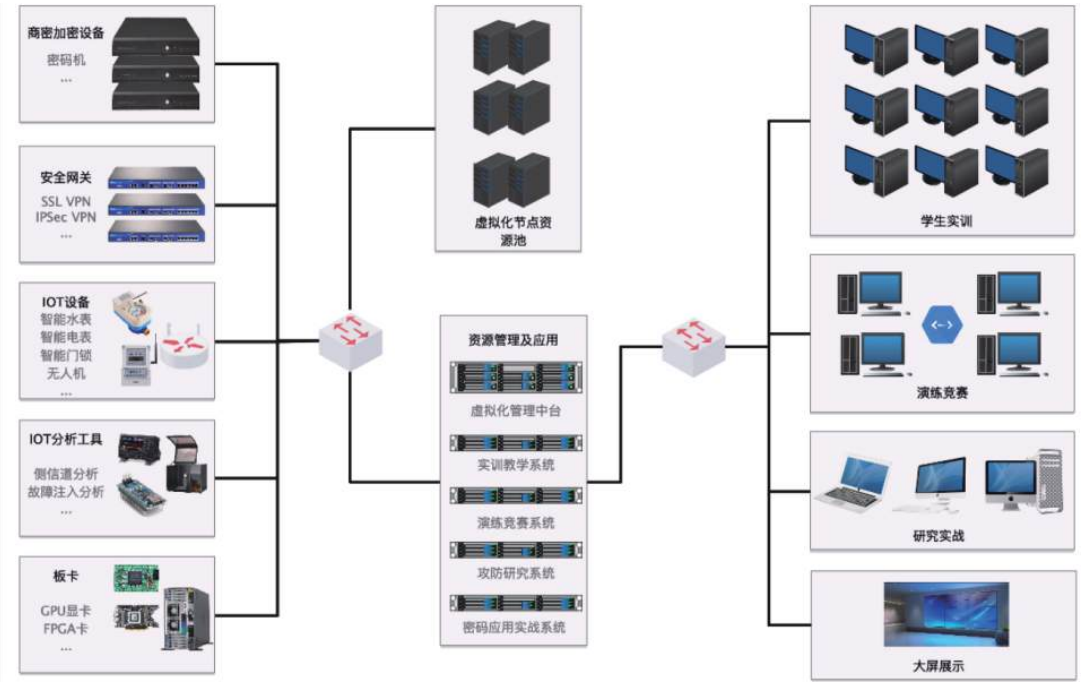
纽创信安是国家高新技术企业和国家专精特新小巨人企业，通过了 IS09001 质量管理体系认证、ISO20000 信息技术服务管理体系认证、ISO27001 信息安全管理体系认证，具备 CCRC 信息系统安全集成三级服务资质，CESSCN 安全设计与集成能力一级资质，同时通过 IS026262:2018 功安全 ASIL-D 流程认证和 ASIL-B 产品认证，具备信息安全和功能安全双重标准的产品研发交付能力。公司注重研发投入和技术创新，业务覆盖从 " 芯 " 到“云”的密码应用场景，提供的产品和服务包括高安全高性能密码算法 IP、片内安全子系统 eHSM、芯片安全检测设备、高安全国密产品、密码态势感知平台和密码靶场等，目前已获得 19 张密码型号证书，其中信创安全三级密码卡和密码态势感知平台均为国内首创。

纽创信安拥有深厚的技术积淀和产学研融合基础，与清华大学、浙江大学、鲁汶大学等国内外知名高校开展了产学研转化合作，在密码算法设计分析、密码芯片设计实现、密码算法快速实现、同态密码等领域处于国际领先水平。公司是全国信息安全标准化技术委员会、工业和信息化部密码应用推进标准工作组成员单位，牵头和参与制定了多项密码领域国家标准或行业标准。

“纽”即纽带，“创”即创新，纽创信安坚持做好科学、技术与产业的安全纽带，围绕科技进步、产业发展、用户需求做好密码技术创新融合，为用户提供实用好用管用的密码产品与服务，为我国的网络空间安全事业贡献自己的力量！

## VCCTS 密码学科教学平台

纽创信安的 VCCTS，基于虚拟化技术、云计算资源调度技术和通讯总线技术，通过硬件设备接入和软件仿真的方式，为学员提供符合真实应用场量的密码综合实验环境。平台内容包括数百个密码教学实验，涵盖了密码算法实现与验证、密码协议实现与验证、密码芯片设计与分析、密码工程实践和商密应用场景与评估等方面。VCCTS 适用于高校学生教学、个人技能培训和企业员工提升等多个场景。




- 教学资源：200+ 教学实验，算法、芯片、产品、场景等全栈密码技能实践实验覆盖，紧扣密码科学与技术课程大纲
- 培养形式：线上虚拟化实训实验与线下实训实践操作相结合，有效衔接密码人才培养和市场需求
- 教学闭环：“备”、“教”、“练”、“训”、“考”教学实训全流程服务
- 动态扩展：教学和实训内容持续更新，平台接口开放，支持教师自定义及实验内容定制

平台已经具备 10 余门的密码专业相关课程，涵盖教学大纲、教学 PPT、参考试题、考试试卷等教学资料，可快速完成课程资源建设，助力密码专业教学活动快速开展。

产业经验赋能人才培养，专注密码专业实验室建设。密码技术教科研平台成熟可靠，已交付多所高校密码专业建设项目。平台覆盖密码相关的密码算法 / 协议、密码芯片设计 / 评估、密码产品开发 / 应用、密码工程综合实践等。

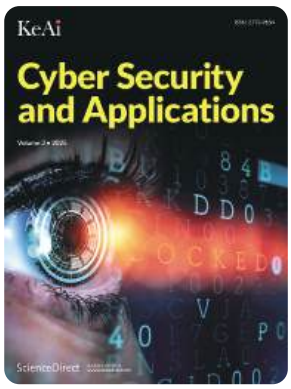
纽创信安
Open Security Research

# 赞助商（科爱）

## Cyber Security and Applications

To defend against various cyber-attacks, the companies and organizations should have right policies and procedures in place. Moreover, it is essential to develop new quantum-safe encryption algorithms and modern tools which can withstand from quantum computer-based attacks. This Cyber Security and Applications (CSA) journal focuses on cyber breaches, cyber-attacks, quantum computing based encryption and decryption techniques and cyber defense tools for improving level of cyber security.

In addition to this, CSA also welcomes the researchers to submit the papers related to advance methods and tools for improving the cyber security in the field of Information and Communication Technology (ICT). Therefore, the CSA journal seeks innovative papers in the field of cyber security. CSA also accepts the substantially extended version of the conference papers in the field of cyber security.




Editor-in-Chief
Prof. Jian Shen

Topics of interest include but are not limited to the following:

- Cyber attacks
- Software and Hardware Security
- Security issues in Intelligent Transportation Systems (ITS)
- Machine learning mechanisms for cyber security
- Key generation and key distribution schemes
- Modern tools for improving cyber security
- Emerging trends in cyber security
- Authenticated Key Agreement Protocols
- Cyber security in Internet of Things (IoT)
- Cyber security in Cloud
- Quantum-safe encryption algorithms
- Quantum-safe digital signature schemes
- Quantum-safe key management mechanisms

收录情况：DOAJ, Scopus, DBLP, EBSCOhost

期刊主页：https://www.keaipublishing.com/csa

KeAi
CHINESE ROOTS
GLOBAL IMPACT

# 会议记录页