



CSS2026

The 16th International Symposium on Cyberspace Safety and Security

Macau, China | August 3-5, 2026

Program Book





Content

Welcome Message from the General Chairs.....	1
Committee	3
Program Overview.....	6
Keynote	9
Paper Session.....	17
General Information	25
Conference Venue.....	25
About Macau.....	27
Other Information.....	29



Welcome Message from the General Chairs

On behalf of the Organizing Committee, it is our great pleasure to welcome you to the 16th International Symposium on Cyberspace Safety and Security (CSS 2026), held on August 3-5, 2026, at the Galaxy International Convention Center in Macau, China.

Since its first edition in Sydney in 2008, CSS has grown into one of the leading international forums dedicated to the safety and security of cyberspace. Previous editions have taken the symposium to Hangzhou, Xi'an, Copenhagen, Hainan, Guangzhou, Amalfi, Granada, New York, Paris, Zhangjiajie, Melbourne and Chengdu, and each has brought together researchers, practitioners and students who share a commitment to making our digital infrastructure more trustworthy. We are delighted that this year the community meets in Macau, a city where East and West have long met, exchanged and prospered.

Cyberspace is being reshaped at remarkable speed by large language models, generative content and increasingly autonomous agents. The technical program of CSS 2026 mirrors this shift. It covers LLM safety and jailbreak defence, machine unlearning, trustworthy and fair machine learning, AIGC and multimodal security, authentication and cryptographic protocols, vulnerability detection and network security, privacy-preserving learning, safety-critical and autonomous systems, and security for agentic and 6G networks. This year the symposium received 123 submissions from authors around the world. Following two rounds of rigorous peer review, in which every paper was assessed by multiple independent reviewers, 42 papers were accepted for presentation, giving an acceptance rate of 34.1%. The accepted work will appear in the conference proceedings published by Springer.

The program spans six keynote talks by distinguished scholars, twenty-one oral sessions running in three parallel tracks, and four poster sessions held alongside the coffee breaks. Beyond the technical sessions, we hope you will join us at the conference banquet at Macau Tower and at the technical visit on the final day, where the conversations begun in the lecture rooms can continue in a more relaxed setting.

A conference of this scale is the work of many hands. We thank all authors for entrusting us with their research, and the Program Chairs, Program Committee members and external reviewers for the care they brought to the review process. We are grateful to our keynote speakers for sharing their

insights, to the Steering Committee for its guidance, and to the Local, Publication and Workshop Chairs, the student volunteers and the staff of City University of Macau for the countless practical details that make an event like this possible. We also thank our supporting institutions and sponsors for their generous assistance.

We wish you a stimulating symposium, many productive new connections, and an enjoyable stay in Macau.

CSS 2026 General Chairs

Binxing Fang

Wanlei Zhou

Sheng Wen

Aniello Castiglione

Committee

Honorary Chairs

Jianfeng Ma	Xidian University, China
Wanlei Zhou	City University of Macau, China
Jin Li	Guangzhou University, China

General Chairs

Binxing Fang	Guangzhou University, China
Wanlei Zhou	City University of Macau, China
Sheng Wen	Swinburne University of Technology, Australia
Aniello Castiglione	University of Salerno, Italy

Program Chairs

Tianqing Zhu	City University of Macau, China
Lihua Yin	Guangzhou University, China
Chiara Pero	Link Campus University, Italy

Local Chairs

Wenjian Liu	City University of Macau, China
Zhe Sun	Guangzhou University, China
Minfeng Qi	City University of Macau, China

Publication Chairs

Lefeng Zhang	City University of Macau, China
--------------	---------------------------------

Workshop Chairs

Chi Liu	City University of Macau, China
---------	---------------------------------

Steering Committee Chair

Yang Xiang	Swinburne University of Technology, Australia
------------	---

Program Committee

Cristina Alcaraz	University of Malaga, Spain
Silvio Barra	University of Naples Federico II, Italy
Jianping Cai	City University of Macau, China
Changlu Chen	City University of Macau, China
Huajie Chen	Faculty of Data Science, City University of Macau, China
Huiqiang Chen	City University of Macau, China
Rongmao Chen	National University of Defense Technology, China
Ashutosh Dhar Dwivedi	Technical University of Denmark, Denmark
Wanxin Gao	City University of Macau, China
Dieter Gollmann	Hamburg University of Technology, Germany
Faqian Guan	City University of Macau, China
Fuchun Guo	University of Wollongong, Australia
Jinguang Han	Southeast University, China
Qiong Huang	South China Agricultural University, China
Fengshi Jing	City University of Macau, China
Xingfeng Li	City University of Macau, China
Jay Ligatti	University of South Florida, USA
Hengzhu Liu	City University of Macau, China
Shigang Liu	Swinburne University of Technology, Australia
Xu Ma	Qufu Normal University, China
Jianting Ning	Singapore Management University, Singapore
Claudia Peersman	University of Bristol, UK
Josef Pieprzyk	CSIRO's Data61, Australia
Laiqiao Qin	City University of Macau, China
Jun Shao	Zhejiang Gongshang University, China
Hui Sun	City University of Macau, China
Jing Sun	City University of Macau, China
Shi-Feng Sun	Shanghai Jiao Tong University, China
Zhiyuan Tan	Edinburgh Napier University, UK
Qiang Tang	Luxembourg Institute of Science and Technology, Luxembourg



Wei Wan	City University of Macau, China
Chun Wang	City University of Macau, China
Minghao Wang	City University of Macau, China
Yunling Wang	Xi'an University of Posts and Telecommunications, China
Qianhong Wu	Beihang University, China
Gengshen Wu	City University of Macau, China
Shiqing Wu	City University of Macau, China
Zhe Xia	Wuhan University of Technology, China
Heng Xu	City University of Macau, China
Peng Xu	Huazhong University of Science and Technology, China
Wun-She Yap	Universiti Tunku Abdul Rahman, Malaysia
Dayong Ye	City University of Macau, China
Xingliang Yuan	Monash University, Australia
Bonan Zhang	City University of Macau, China
Xiaoyu Zhang	Xidian University, China
Xuyun Zhang	Macquarie University, Australia
Qi Zhong	City University of Macau, China
Shuai Zhou	City University of Macau, China
Congcong Zhu	City University of Macau, China
Xuhan Zuo	City University of Macau, China

Program Overview

CSS 2026 & FCS 2026 Program Overview		
Time	Room 24+25	Room 26
Day 1 Aug 3, 2026		
08:30-18:00	Registration	
09:10-09:30	Opening Ceremony	
09:30-10:00	Keynote 1 Robert Deng	
10:00-10:30	Coffee Break & Poster Session 1	
10:30-11:00	Keynote 2 Xiaosong Zhang	
11:00-11:30	Keynote 3 Aniello Castiglione	
11:30-13:00	CSS Oral Session 1	FCS Oral Session 1
13:00-14:00	Lunch	
14:00-15:30	CSS Oral Session 2	FCS Oral Session 2
15:30-16:00	Coffee Break & Poster Session 2	
16:00-18:00	CSS Oral Session 3	CCS Oral Session 4
Day 2 Aug 4, 2026		
08:30-18:00	Registration	
09:00-09:30	Keynote 4 Jianwei Liu	
09:30-10:00	Keynote 5 Shengke Zeng	
10:00-10:30	Coffee Break & Poster Session 3	
10:30-11:00	Keynote 6 Chiara Pero	
11:00-12:30	CSS Oral Session 5	FCS Oral Session 3
12:30-14:00	Lunch	
14:00-15:30	CSS Oral Session 6	FCS Oral Session 4
15:30-16:00	Coffee Break & Poster Session 4	
16:00-17:30	CSS Oral Session 7	CSS Oral Session 8 & ASR Session
18:30-21:00	Banquet @Lisboeta Macau	
Day 3 Aug 5, 2026		
08:00-12:00	Technical Visit & Cultural Tour	

CSS 2026 Program Overview

Day 1 Aug 3, 2026

08:30-18:00	Foyer	Registration
09:10-09:30	Room 24+25	Opening Ceremony
09:30-10:00	Room 24+25	Keynote 1 Robert Deng
10:00-10:30	Foyer	Coffee Break & Poster Session 1
10:30-11:00	Room 24+25	Keynote 2 Xiaosong Zhang
11:00-11:30	Room 24+25	Keynote 3 Aniello Castiglione
11:30-13:00	Room 24+25	CSS Oral Session 1: LLM Safety & Jailbreak Defense
13:00-14:00	Room 2+3	Lunch
14:00-15:30	Room 24+25	CSS Oral Session 2: Trustworthy & Fair Machine Learning
15:30-16:00	Foyer	Coffee Break & Poster Session 2
16:00-18:00	Room 24+25	CSS Oral Session 3: Machine Unlearning / Safety-Critical & Autonomous Systems
	Room 26	CSS Oral Session 4: Time-Series Anomaly Detection & Forecasting

Day 2 Aug 4, 2026

08:30-18:00	Foyer	Registration
09:00-09:30	Room 24+25	Keynote 4 Jianwei Liu
09:30-10:00	Room 24+25	Keynote 5 Shengke Zeng

10:00-10:30	Foyer	Coffee Break & Poster Session 3
10:30-11:00	Room 24+25	Keynote 6 Chiara Pero
11:00-12:30	Room 24+25	CSS Oral Session 5: AIGC & Multimodal Security
12:30-14:00	Room 2+3	Lunch
14:00-15:30	Room 24+25	CSS Oral Session 6: Authentication, Cryptography & Protocols
15:30-16:00	Foyer	Coffee Break & Poster Session 4
16:00-17:30	Room 24+25	CSS Oral Session 7: Vulnerability Detection & Network Security
	Room 26	CSS Oral Session 8: Privacy-Preserving Learning & Applications / ASR Session: Agentic & 6G Network Security
18:30-21:00	Lisboeta Macau	Banquet
Day 3 Aug 5, 2026		
08:00-12:00	Technical Visit & Cultural Tour	

Keynote

Keynote Speech 1:

Robert Deng, Singapore Management University

**Presentation Title:**

Post-Quantum Cryptography Migration: Securing Data and Protecting Privacy

Biography:

Robert Deng is Lee Kong Chian Chair Professor, Deputy Dean for Faculty & Research, School of Computing and Information Systems, Singapore Management University (SMU). His research interests are in the areas of data security and privacy, network and distributed system security, and applied cryptography. He received the Outstanding University Researcher Award from National University of Singapore, Lee Kuan Yew Fellowship for Research Excellence and Zhongni Distinguished Educator Award from SMU, Asia-Pacific Information Security Leadership Achievements and Community Service Star from International Information Systems Security Certification Consortium (ISC2), the Public Administration Medal (Silver) Singapore National Day Award. He is a Fellow of IEEE, AAIA, and Academy of Engineering Singapore.

Abstract:

The rapid advancement of quantum computing poses a fundamental threat to today's public-key cryptography, making the transition to post-quantum cryptography (PQC) an urgent global priority. This talk begins with an overview of the quantum threat landscape, recent developments in PQC standardization, and the practical challenges of migrating existing systems to quantum-safe cryptography. The talk then explores how PQC serves not only as a replacement for classical public-key cryptography but also as a foundation for a new generation of secure data protection and privacy-preserving applications. Two recent research projects will be presented. KyberBridge extends the NIST-standardized ML-KEM (Kyber) to support efficient one-to-many encrypted data sharing through broadcast proxy re-encryption. Keyword PIR enables users to retrieve records using keyword queries without revealing their interests to the server, while achieving efficiency comparable to state-of-the-art quantum-safe index PIR. Together, these examples demonstrate how PQC can enable practical quantum-safe applications that extend well beyond secure communications.

Keynote Speech 2:**XiaoSong Zhang, University of Electronic Science and Technology of China****Presentation Title:**

Active Cybersecurity Models and Applications

Biography:

He is a professor and doctoral supervisor specializing in cybersecurity and network confrontation. He received his bachelor's degree from Shanghai Jiao Tong University and his master's and doctoral degrees from the University of Electronic Science and Technology of China. As a pioneering scholar in China's automated network confrontation research, he has focused on intelligent cybersecurity theories and technologies since 2004, mainly covering threat perception, detection defense, and traceability. He originally proposed the active cybersecurity SAPC model and established a scientific research paradigm for automated network confrontation, whose relevant achievements were selected as outstanding outcomes of the 13th Five-Year Plan National Natural Science Foundation Project. He has long presided over national key R&D programs and key National Natural Science Foundation projects, leading the development of a series of core cybersecurity platforms that have advanced the systematic and automated development of China's network security technologies. Academically, he has published 5 monographs, 2 translated works and 249 SCI/EI-indexed papers, and holds 63 authorized national invention patents. His original technological achievement, the domestic dedicated programming language and system for cybersecurity, was selected as one of the 2023 Top Ten Information and Communication Technological Advances and won the 2024 First Prize of China Institute of Communications Science and Technology Progress Award.

Abstract:

Network confrontation in non-cooperative computer systems represents the core challenge of modern cybersecurity. Traditional defense strategies, which depend on passive response mechanisms, struggle to address sophisticated and unknown network threats. To tackle this limitation, the active cybersecurity concept is proposed to upgrade defense capabilities through integrated technical and strategic defense systems. This concept treats attackers and defenders as rational decision-makers optimizing their respective benefits, and adopts game theory to analyze

their interactive behaviors and optimize confrontation strategies. On this basis, the SAPC active cybersecurity model is established to achieve integrated defense covering threat perception, analysis, tracing and response, with four core modules: intelligent perception, in-depth analysis, live visualization, and countermeasure. By modeling network confrontation as a dynamic game process, SAPC constructs a rigorous theoretical and practical cybersecurity framework. It realizes a paradigm shift from passive emergency response to active proactive confrontation, and promotes the innovative development of cybersecurity technologies with predictive, preventive and strategic defense capabilities.

Keynote Speech 3:

Aniello Castiglione, University of Salerno

**Presentation Title:**

Quantum Computing: Fact, Issues and Applications

Biography:

Aniello Castiglione received his PhD in Computer Science from the University of Salerno, Italy, where he currently serves as Associate Professor in the Department of Management & Innovation Systems. In 2021, he obtained the Italian National Scientific Qualification for the position of Full Professor in Computer Science. His scientific activity is marked by a strong international profile, with more than 300 publications in international journals and conference proceedings. His international collaboration network includes more than 95 co-authors affiliated with over 84 institutions across more than 25 countries. He has also contributed to the organization of approximately 300 international conferences, mainly as Program Chair and Technical Program Committee member. On the editorial side, he is currently Managing Editor and Editor-in-Chief for Special Issues of Elsevier's Image and Vision Computing. Until 2024, he served as Editor-in-Chief for Special Issues of the Journal of Ambient Intelligence and Humanized Computing, published by Springer. He has also been Managing Editor of two ISI-indexed international journals, reviewer for around 140 international scientific journals, Guest Editor of about 30 Special Issues, and member of more than 10 Editorial Boards of international journals, including IEEE Transactions on Sustainable Computing, IEEE Access, IET Image Processing, Journal of Ambient Intelligence and

Humanized Computing, Multimedia Tools and Applications, Cyber Security and Applications, IET Intelligent Transport Systems, Sustainability, Smart Cities, Future Internet, and Electronics. According to Web of Science Essential Science Indicators, two of his papers, published respectively in IEEE Transactions on Computers and Future Generation Computer Systems, were recognized as “Highly Cited Paper” and “Research Front paper”, placing them among the top 1% of worldwide publications in Computer Science in 2017 and 2022. Since 2019, he has consistently been included in Stanford University’s ranking of the world’s top 100,000 most influential scientists, based on Scopus data, in the areas of Artificial Intelligence & Image Processing and Networking & Telecommunications. Since 2022, he has also appeared in the Italian Computer Science Top Scientists ranking published by Research.com. His main research interests include Artificial Intelligence in Cyber Security, Information Forensics, Digital Forensics, Cloud Security and Privacy, Communication Networks, Post-Quantum Cryptography, Quantum Computing, Applied Cryptography, Steganography, and Sustainable Computing. He is a member of IEEE and ACM.

Abstract:

As the era of Noisy Intermediate-Scale Quantum (NISQ) technology advances, the risk of quantum-based attacks capable of breaking conventional encryption becomes increasingly realistic. This is particularly concerning for Blockchain and Trustworthy Systems, which depend heavily on cryptographic mechanisms to ensure full security. The emergence of quantum computing introduces serious challenges, as existing blockchain infrastructures rely on cryptographic algorithms that are susceptible to quantum breakthroughs. One of the most vulnerable algorithms is the widely adopted Elliptic Curve Digital Signature Algorithm (ECDSA), which experts warn could be compromised as early as 2027, according to the most optimistic forecasts. Furthermore, the shift to post-quantum cryptography raises critical questions about the associated costs, including energy consumption and the additional storage required to implement these new cryptographic methods. The tremendous computational power of quantum devices holds the potential to significantly contribute to building a more reliable and secure world. However, this power also brings the risk of exploitation, putting numerous systems in jeopardy. To safeguard the digital environment and ensure the privacy and security of people worldwide, implementing strict regulations and advanced quantum security techniques—such as Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and Quantum Random Number Generators (QRNG)—will be crucial.

Keynote Speech 4:**Jianwei Liu, Beihang University****Presentation Title:**

AI-Empowered Security for 6G Networks

Biography:

Jianwei Liu is a Professor and Ph.D. supervisor at Beihang University, and the founding Dean of its School of Cyber Science and Technology. He is a National Distinguished Teaching Professor and a recipient of the Special Government Allowance of the State Council of China.

He currently serves as a member of the Discipline Appraisal Group of the Academic Degrees Committee of the State Council, Vice Chair of the Ministry of Education Steering Committee for Cyberspace Security Education, and a member of the National Steering Committee for Professional Degree Graduate Education in Cryptography. He is a Standing Council Member of the Chinese Association for Cryptologic Research, and a Standing Council Member and Chair of the Publication Committee of the Cyber Security Association of China. He is Executive Associate Editor-in-Chief of the Journal of Cyberspace Security Science and Associate Editor-in-Chief of the Chinese Journal of Network and Information Security. He has served as chief editor of 16 textbooks, and has authored 7 monographs and translated 1 book. His honors include the National Distinguished Teaching Professor award, the National Cyber Security Outstanding Teacher Award, the Baosteel Outstanding Teacher Special Prize, the Beijing Distinguished Teaching Professor Award, and the Beijing Outstanding Teacher Award.

Abstract:

The sixth generation of mobile communications (6G), envisioned as an intelligently connected world spanning land, sea, air and space, will deliver terabit-per-second data rates, sub-millisecond latency and ultra-high reliability for a vast range of applications. However, the heterogeneous interconnection and ubiquitous connectivity of 6G raise severe security challenges: unified management is hard to guarantee, massive numbers of devices are hard to control, and network

trust is hard to establish. Artificial intelligence (AI), with its capabilities in learning, knowledge reasoning, and perception-driven decision making, breaks through the limits of human expertise. With an AI engine at its core, deep collaboration across security layers, and closed-loop feedback for adaptive learning, an AI-empowered 6G security architecture can make endogenous security in 6G networks a reality.

This talk focuses on the emerging requirements and unique challenges of 6G network security and proposes a deeply integrated, AI-empowered security architecture. It elaborates on the core enabling role of AI in protecting the physical layer, the network layer and the service layer of 6G, and identifies the specific points at which AI can empower each layer. It further reviews frontier research topics and key technologies in AI-empowered 6G security, and outlines promising directions for future work, aiming to provide both theoretical reference and practical guidance for advancing endogenous security in 6G.

Keynote Speech 5:

Shengke Zeng, Xihua University

**Presentation Title:**

Encrypted Data Deduplication: Rebuilding Trust Models for Cloud Storage Optimization

Biography:

Candidate for Academic and Technical Leaders of Sichuan Province, and recipient of Xihua University's "My Favorite Teacher" title. She has worked as a research assistant and visiting scholar at Curtin University (Australia), University of Waterloo (Canada) and University of Wollongong (Australia). Currently, she serves as a Standing Committee Member of the Professional Committee on Big Data Security and Privacy Computing of the Chinese Information Processing Society of China. Focusing on the research of cryptography and information security, she has presided over 8 national and provincial-level scientific research projects on privacy protection in vehicular ad-hoc networks and data security in industrial internet. As the first (corresponding) author, she has published more than 40 papers in journals and conferences including IEEE TDSC/TSC, IEEE ICC, JIII, The Computer Journal and TCS. She has presided over the

construction of provincial first-class undergraduate courses, provincial advanced courses and provincial high-quality postgraduate teaching resources, and won the second prize of teaching achievement, the third prize of the Outstanding Talent and Educator Challenge of China Chengdu International Software Design and Application Competition as the first achiever. She also guided the postgraduate work "Pioneer of Secure Exchange and Sharing of Encrypted Data in Cloud Computing" to win the provincial silver award in the "Internet+" competition.

Abstract:

Cloud storage faces problems such as large data scale, high redundancy and strong privacy requirements. Driven by encrypted data deduplication, optimizing encrypted data storage is an important approach to rebuild the trust model of cloud storage. Currently, there are bottlenecks in encrypted data deduplication technology regarding guess attacks, deduplication efficiency and cross-data type deduplication, which cannot meet the requirements of efficient and secure storage of large-scale data.

This presentation is based on the balance between storage efficiency and privacy protection in a non-trusted execution environment. It focuses on the technical limitations of encrypted data deduplication and storage optimization requirements to realize the optimization of storage space efficiency and privacy. It focuses on introducing technologies such as batch secure deduplication, fuzzy deduplication, color-aware deduplication and hierarchical deduplication. We also discuss the future research feasibility of encrypted data deduplication in visual data deduplication, entropy based similarity check and AI integrated deduplication technology.

Keynote Speech 6:**Chiara Pero, Link Campus University****Presentation Title:**

PQ-FLCom: Post-quantum secure communication for industrial federated learning

Biography:

Chiara Pero received the B.Sc. and M.Sc. degrees in Computer Science

from the University of Salerno, Italy, in 2016 and 2018, respectively. She earned the Ph.D. degree in Computer Science from the same university in 2023, graduating with the highest distinction (“Excellent”) with a dissertation entitled “Behavioral Biometrics in the Era of Artificial Intelligence”. She is currently with Link Campus University, Rome, Italy. She holds the Italian National Scientific Qualification (ASN) for Associate Professor in Computer Science (Competition Sector 01/B1). She has authored more than 50 peer-reviewed journal and conference publications, which have received over 600 citations. She serves as Associate Editor for several international journals and as Guest Editor for numerous Special Issues and scientific workshops. She is a member of the Biometrics and Image Processing Laboratory (BIPLab), the Context Aware Security Analytics Laboratory (CASALab), and the Computer Graphics Laboratory (CGLab). She is also an IEEE Member and a member of the Italian Association for Research in Computer Vision, Pattern Recognition, and Machine Learning (CVPL). Her research interests include computer vision, pattern recognition, deep learning, biometrics, and trustworthy artificial intelligence, with recent research focusing on the integration of post-quantum cryptography into intelligent systems.

Abstract:

Federated Learning (FL) has become a key paradigm for enabling collaborative artificial intelligence in Industry 4.0 by allowing distributed devices to train shared models without exchanging sensitive data. Despite its privacy advantages, the continuous exchange of model updates exposes FL to communication-level threats such as eavesdropping, model poisoning, and man-in-the-middle attacks. Furthermore, the emergence of quantum computing poses a significant challenge to the classical cryptographic mechanisms currently protecting these communications. PQ-FLCom is a modular communication framework that integrates NIST-standardized post-quantum cryptographic primitives into industrial federated learning systems. Its multi-level security architecture provides configurable protection for confidentiality, integrity, and authenticity while preserving the efficiency required by Industrial Internet of Things (IIoT) applications. Experimental results demonstrate the framework's robustness against communication-level attacks and evaluate the computational overhead introduced by post-quantum cryptography, showing that strong quantum-resistant security can be achieved without compromising the practicality and scalability of distributed learning systems.

Paper Session

CSS Oral Session 1: LLM Safety & Jailbreak Defense

Day 1 Aug 3, 2026 11:30-13:00 | Room 24+25

#32	<i>The TDIS Framework: Automated Synthesis of Adversarial Descriptions to Jailbreak LLM Tool Use</i> Xu Xin
#68	<i>Visual Feedback-Based Prompt Pollution Attack on Large Language Model-Driven Intelligent Systems: A Case Study with Smart Car Platform</i> Junrui Li, Heng Xu and Jie Xi
#70	<i>A Safety-Enhanced Retrieval-Augmented Generation Framework with Risk-Aware Retrieval and Lightweight Validation</i> Kaijie Ma
#85	<i>Graded Detection Against Multi-Turn Jailbreak Attacks</i> Zonglin Zhu, Qiming Wang and Chunxiao Zhang
#95	<i>TrustScore: Risk-Aware Framework for LLM Hallucination Detection</i> 一和 赵 and Cong Cong Zhu
#99	<i>A White-Box Jailbreak Defense Method for LLMs Based on Semantic Probe Conflict</i> Xiang Zhou, Shuai Zhou and Mingyu Zhu

CSS Oral Session 2: Trustworthy & Fair Machine Learning

Day 1 Aug 3, 2026 14:00-15:30 | Room 24+25

#8	<i>Bias-Corrected Momentum and Dynamic Step Bounding for Transferable Re-ID Attacks</i> Hailin Yang and Huajie Chen
#22	<i>Adversarially Consistent Representation Learning: A Unified Regularization Framework for Robust Deep Models</i> Xiang Zhang, Feng Wang, Qingxuan Luo, Xinghua Li, Wenqi Duan and Yuantao Wang
#43	<i>SHRED: Unified Adaptive Subspace Purification Defense Against Deep Hashing Backdoor Attacks</i> Leyang Zhang and Qi Zhong
#45	<i>MaxSim Hijack: Poisoning Multimodal RAG with Token-Aligned Patch Allocation</i> Weicheng Xing, Mengyang Wu, Jenny Wang, Jacko Feng and Bo Liu
#47	<i>A Game-Theoretic Defense against Membership Inference Attacks</i> Guangkai Jiang and Yuchen Shi
#61	<i>Fair Learning without Semantic Demographic Attributes via Curvature-Based Optimization</i> Zihou Zhao, Huiqiang Chen and Tianqing Zhu

CSS Oral Session 3: Machine Unlearning / Safety-Critical & Autonomous Systems

Day 1 Aug 3, 2026 16:00-18:00 | Room 24+25

#10	<i>GAU: A Data-free Black-box Adversarial Unlearning Framework via Generative Model</i> Mingze Sun, Hui Sun, Yubo Wang and Dong Xu
#13	<i>Design and Implementation of a Lightweight Model Federated Unlearning Framework for Resource-Constrained Edge Devices</i> Ming Zhang and Minghao Wang
#27	<i>Dual-Channel Fine-Grained Reinforcement Unlearning: Integrating Reward Shaping and State Perturbation for Selective Forgetting</i> Xinbo Fu and Lefeng Zhang
#44	<i>Dual-SU: Sequential Unlearning via Influence Localization and Representation Perturbation</i> Xun Zhang, Hengzhu Liu, Haoyuan Chen, Wenbin Shen and Qiyu Chen
#2	<i>Decentralized Multi-UAV Coordination for Robust Scheduling in Dynamic Environments</i> Xuanyi Qi, Huinan Zhang, Kai Li, Tiansi Li and Hongyi Liu
#11	<i>LLM-Driven Formal Verification for Safety-Critical Railway Control Systems</i> Hongxue Chen, Tianjian Liu, Yiwen Xia and Pengrui Liu
#23	<i>Safety Modeling and Verification of Perception-Enhanced Autonomous Train Control Systems Using Timed Automata</i> Qiang Li and Sheng Wen
#46	<i>KQHA: An Adaptive Dynamic Auto-Scaling Controller</i> Xi Luo, Baoru Li, Lihua Yin, Haoqin Chen, Yingkai Fan and Naqin Zhou

CSS Oral Session 4: Time-Series Anomaly Detection & Forecasting

Day 1 Aug 3, 2026 16:00-18:00 | Room 26

#29	<i>SMA-AD: Self-Supervised Margin-Aware Multivariate Time Series Anomaly Detection</i> Fangzhe Zhang, Hao Zhang, Rui Wang, Fuhui Zhao, Mai Ye, Yourong Li and Hongyi Liu
#30	<i>SemDC: A Semi-supervised Anomaly Detection Approach for Time Series with Redundant Variates via Dimension Complement</i> Yingxian Chang, Xin Liu, Donglan Liu, Fuhui Zhao, Fangzhe Zhang and Hongyi Liu
#49	<i>VAAD: A Variate-Aware Method for Multivariate Time-Series Anomaly Detection</i> Shanjie Xu, Jingyu Wang, Xin Liu, Yuhui Jin, Honglei Yao and Hongyi Liu
#51	<i>Federated Learning-Based Multi-Source Time Series Fusion for Forecasting</i> Guidong Zhang, Mai Ye, Xin Liu, Donglan Liu, Hao Yu, Bing Su and Hongyi Liu
#62	<i>LitePriv: A Lightweight On-chip Real-Time Privacy Protection Method for IoT Time Series</i> Yizhao Zhou, Xinyu Chen, Li Kuang, Jia-Nan Liu, Fengjun Xiao, Lijian Mao, Bangjie Tang, Heng Jin and Yingjie Xia

CSS Oral Session 5: AIGC & Multimodal Security

Day 2 Aug 4, 2026 11:00-12:30| Room 24+25

#15	<i>Beyond Explicit Decoding: An Implicit Tracing Framework Based on TS-Mark Watermarks and GTD-Net Tracer Datasets</i> Yufeng Pan, Yonghai Wang and Gengshen Wu
#33	<i>DSER: Generative Image Detection Based on Dual-Space Reconstruction Error</i> Xu Xin
#41	<i>TL-FSGW: A Hybrid Text Watermarking Framework for Large Language Models with Frame Synchronization and Adaptive Skipping</i> Haoyuan Huang
#50	<i>SafeRendering: Harnessing Attention for Prohibited Concept Removal Autoregressive Models</i> Sihui Wu and Yilin Yang
#60	<i>On the Vulnerability of Cross-Modal Symmetry in Multimodal AIGC Systems</i> Jin Wei, Siyu Zhang, Yuchang Mo, Yunfei Li and Mirlan Chynybaev
#77	<i>A Transformer-Based Multi-Modal Feature Fusion Enhanced DenseNet for Medical Image Classification</i> Honggang Wei, Chuanhao Jing and Yu Fu

CSS Oral Session 6: Authentication, Cryptography & Protocols

Day 2 Aug 4, 2026 14:00-15:30| Room 24+25

#3	<i>A Lightweight Anonymous Authentication and Key Agreement Protocol for Wearable Devices Using PUF</i> Fangchen Xu, Juncheng Tong, Huijie Yang, Xinyu Li and Quanrun Li
#31	<i>Information-Limited Login Oracles: Reducing Feedback Leakage for Online Password Guessing</i> William Mengyang Wu, Weicheng Xing, Xuhan Zuo, Minghao Wang and Tianqing Zhu
#93	<i>SAML: A Secure Anti-Money Laundering Scheme with Multi-Client Functional Encryption</i> Peng Yu, Yuzhu Wang, Yu Chen, Qing Ye and Mingwu Zhang
#107	<i>The Light at the End of the (TLS) Tunnel: Dynamic Cryptographic and Protocol-Downgrade Analysis of Web Traffic</i> Aniello Castiglione, Davide De Angelis, Alessia Maffei, Alberto Moccardi, Chiara Pero and Zhiyuan Tan
#113	<i>Combating Visual Disinformation: A Post-Quantum Cryptographic Framework for Image and Metadata Integrity</i> Aniello Castiglione, Jacopo Gennaro Esposito, Vincenzo Loia, Michele Nappi, Chiara Pero and Florin Pop
#123	<i>A Secure and Lightweight Authentication and Key Agreement Protocol Against Ephemeral Secret Leakage Attacks for the Internet of Drones</i> Sijia Li, Jianwei Liu, Hua Guo and Haojia Qi

CSS Oral Session 7: Vulnerability Detection & Network Security

Day 2 Aug 4, 2026 16:00-17:30| Room 24+25

#9	<i>MA-HGAT: Multi-Agent Heterogeneous Graph Attention Network for Smart Contract Logical Vulnerability Detection</i> Jialin Li, Minfeng Qi, Lefeng Zhang, Yaxuan Xiong, Zhe Sun and Tianqing Zhu
#14	<i>Add character noise to the network side channel</i> Liu Yunqiang
#65	<i>Certificateless Privacy-Preserving Integrity Auditing and Sanitizable Data Sharing for Cloud-Based Electronic Medical Records</i> Lingzhu Li, Xiaoying Jia, Cong Peng and Zhiyan Xu
#82	<i>Cyber Insurance Forensics and Attribution in the Encrypted Ecosystem: A GNN-based Non-decrypting Traffic Analysis Approach</i> Qiang Li, Rongqi Jing and Qianwen Sun
#83	<i>ArchVul: Architecture-Aware Hybrid RAG for Vulnerability Detection in Enterprise Java</i> Xiaowei Zhang, Shigang Liu, Jun Zhang and Yang Xiang
#118	<i>SoK: Application-Layer Denial-of-Service in OCPP-Based EV Charging: Denial Pathways, Observability Regimes, and Evidence Gaps</i> Amarjot Singh Atwal, Yang Xiang, Prem Prakash Jayaraman and Xiaoning Du

CSS Oral Session 8: Privacy-Preserving Learning & Applications

/ ASR Session: Agentic & 6G Network Security

Day 2 Aug 4, 2026 16:00-17:30| Room 26

#21	<i>Hadoop MapReduce-based “People You May Know” Friend Recommendation</i> Zi Xie
#36	<i>SMART: SMT-Augmented Multi-Agent Reasoning for Travel</i> Wang Yixiang and Zhu Congcong
#69	<i>A Privacy-by-Design Heterogeneous Graph Reasoning for Cross-Entity Stance Inference</i> Zehan Li, Xuemeng Zhai, Hangyu Hu, Jiandong Liang and Guangmin Hu
#78	<i>Multi-Source Representation Learning for Federated and Privacy-Preserving Emotion Recognition</i> Qinyuan Wang, Ming Liu, Kewen Liao, Guangyan Huang, Y. Neil Qu, Bruce Gu and Longxiang Gao

ASR Session: Agentic & 6G Network Security

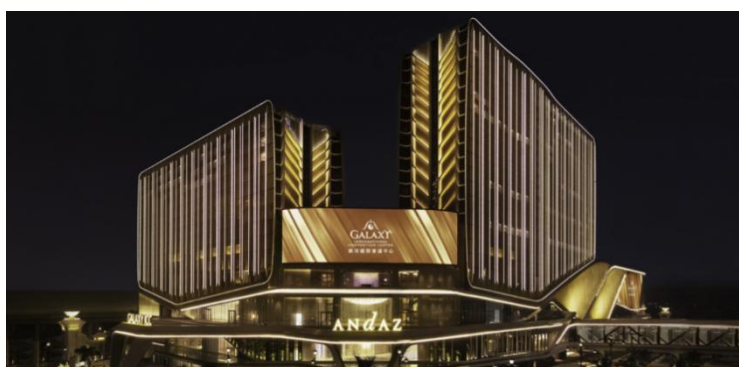
#71	<i>Agent Card Module Security Analysis and Vulnerability Discovery: A Review of A2A Protocol Security Research</i> Wang Yian, Liu Zhen and Wang Yajie
#92	<i>Distributed Aol-aware AI-driven Anomaly Detection for Secure Service Function Chains in 6G Networks</i> Wenjun Huang, Zixiao Kong, Yingtian Sun and Rui Huang

General Information

Conference Venue

Galaxy International Convention Center (GICC)

Address: Galaxy Macau™, Estrada da Baia de Nossa Senhora da Esperanca, s/n, Cotai, Macau



Galaxy International Convention Center (GICC) is the latest addition to Galaxy Entertainment Group's ever-expanding integrated resort precinct and will usher in a new era for the MICE industry in Macau.

GICC — Asia's most iconic and advanced MICE destination — is a world-class event venue featuring 40,000 sqm of total flexible MICE space that can cater for up to 8,500 banquet guests, or cocktail parties for as many as 16,000 guests. The 10,000-sqm pillar-less exhibition hall located on the ground floor, can accommodate up to 7,000 delegates. The exhibition hall is also perfectly suited for banquets of approximately 6,500 guests or cocktail parties for 8,500 guests.

Conveniently located within GICC, the 16,000-seat Galaxy Arena is the largest indoor arena in Macau and where spectacular events come to life - from world concert tours to thrilling fight nights, every guest at Galaxy Arena will enjoy 360°unobstructed views and high quality surround sound while high definition broadcasting will bring the event to every corner of the arena.

SECOND FLOOR



Galaxy Shuttle Buses:

Galaxy shuttle buses are complimentary between key entry ports and their properties, detailed schedule is below.

<u>Border Gate</u>	To Galaxy Macau	09:00 ~ 23:30	<u>Taipa Ferry Terminal</u>	To Galaxy Macau	09:00 ~ 23:00
	From Galaxy Macau	09:00 ~ 23:30		From Galaxy Macau	09:15 ~ 23:15
	Average 5 - 15 minutes (Around 25 minutes drive)			Average 15-40 minutes (Around 20 minutes drive)	
	Border Gate → Diamond Lobby# → Border Gate			Taipa Ferry Terminal* → Crystal Lobby# → Taipa Ferry Terminal*	
<u>Macau International Airport</u>	To Galaxy Macau	10:00 ~ 21:00	<u>Hengqin Port</u>	To Galaxy Macau	09:00 ~ 22:00
	From Galaxy Macau	10:15 ~ 20:45		From Galaxy Macau	09:15 ~ 21:45
	Average 35 minutes (Around 20 minutes drive)			Average 5 ~ 10 minutes, Non-Peak Hours (17:00-22:00) 30 minutes (Around 10 minutes drive)	
	Macau International Airport → Crystal Lobby# → Macau International Airport			Hengqin Port → Crystal Lobby# → Hengqin Port	
<u>Andaz Macau</u>	To Galaxy Macau	09:00 ~ 02:00	<u>Hong Kong Zhuhai Macau Bridge To Galaxy Macau</u>	To Galaxy Macau	10:00 ~ 23:00
	From Galaxy Macau	09:00 ~ 02:00		From Galaxy Macau	10:00 ~ 23:00
	Average 5-10 minutes (Around 10 minutes drive)			Average 10 ~ 25 minutes (Around 25 minutes drive)	
	Andaz Macau → Crystal Lobby → Andaz Macau			Hong Kong Zhuhai Macau Bridge → Diamond Lobby → Hong Kong Zhuhai Macau Bridge	
<u>StarWorld Hotel/Border Gate</u>	To StarWorld Hotel	09:00 ~ 23:30	<u>StarWorld Hotel / Macau Ferry Terminal</u>	To Galaxy Macau	09:30-22:00
	From StarWorld Hotel	09:00 ~ 23:30		From Galaxy Macau	09:30-22:00
	Average 10-15 minutes			Average 10-20 minutes (Around 35 minutes drive)	
	Border Gate → StarWorld Hotel → Border Gate			Crystal Lobby → StarWorld Hotel → Macau Ferry Terminal → StarWorld Hotel → Crystal Lobby	

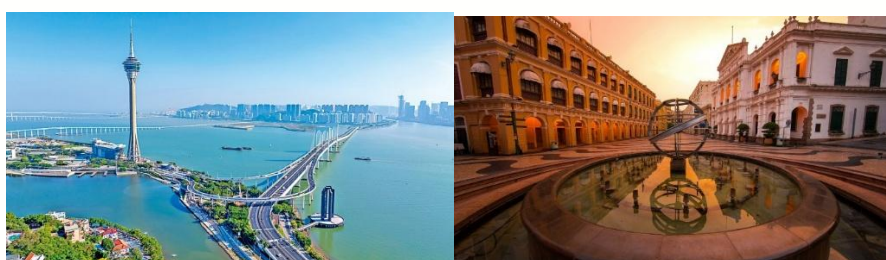
About Macau

Macao - located on the western bank of the Pearl River Delta in southern Guangdong Province, People's Republic of China - adjoins the Mainland city of Zhuhai and lies some 60 kilometres to the west of Hong Kong. Macao comprises Macao Peninsula, Taipa and Coloane. Macao Peninsula is the hub of the territory and is connected to Taipa by three bridges. Several large international hotel resorts - with new supporting infrastructure - are located on the reclaimed land between Taipa and Coloane in the newly developed district known as Cotai.

The Portuguese arrived and settled in Macao in the mid 16th Century. Thus, the city's architecture, art, religion, traditions, food and community reflect the integration of Chinese, Western and Portuguese cultures. Macao became a Special Administrative Region of the People's Republic of China on 20th December 1999 and exercises a high degree of autonomy under the principle of "One country, two systems". The SAR is growing in size with more buildings on reclaimed land, and in the number and diversity of its attractions. In 2005, The Historic Centre of Macao was inscribed on the UNESCO World Heritage List as a result of its unique historical and cultural landscape. Macao is currently positioning itself as the World Centre of Tourism and Leisure as it develops into a quality international tourist destination.

Macao is eight hours ahead of Greenwich Mean Time. Chinese and Portuguese are the official languages, Cantonese being most widely spoken. The official languages are used in government departments in all official documents and communications. English is generally used in trade, tourism and commerce.

For more information about Macao and sightseeing tours in this fantastic place, please view <https://www.macaotourism.gov.mo/en/>.



Local Public Bus

You can download the following local APP to check Macau bus schedule. Here is the link and QR code: <https://www.dsat.gov.mo/dsat/index.aspx>



Taxi

If you need to call taxi, please download MaasPlus APP for local on-call taxi. Macau is a popular tourist destination, you are strongly recommended to reserve a taxi ahead of schedule. Here is the link for downloading the Taxi APP:

<https://www.maasplus.com/file-api/maasplus/comm/app/version/download.html>

Other Information

Entry Permit

Please ensure that you have a valid Exit-Entry Permit for Travelling to and from Hong Kong and Macao (港澳通行证) if you are a Chinese Citizen, or Passport if you are a foreign citizen, and the appropriate endorsements to attend the conference smoothly. Upon entry into Macau, travelers will be issued an entry declaration/permission to stay (as shown in the white slip below). Please keep it properly during your hotel check-in and stay in Macau.

澳門特別行政區 REGIÃO ADMINISTRATIVA ESPECIAL DE MACAU MACAO SPECIAL ADMINISTRATIVE REGION 治安警察局 CORPO DE POLÍCIA DE SEGURANÇA PÚBLICA PUBLIC SECURITY POLICE FORCE	逗留許可 AUTORIZAÇÃO DE PERMANÊNCIA AUTHORIZATION TO STAY 入境目的(旅遊或等同旅遊) FINALIDADE DA ENTRADA (TURISMO OU EQUIVALENTE) PURPOSE OF ENTRY (TOURISM OR EQUIVALENTS)
姓名 Name CHAN DAI MAN 證件號碼 N.º do Documento Document No. 123456(-) 入境日期 Data de Entrada Date of Entry 15-11-2021 (08) 批准逗留至: (日-月-年) Autorizado a Permanecer até (dd-mm-aaaa) Permitted to Remain until (dd-mm-yyyy) 22-11-2021	 持證人禁止從事 與入境目的不符的活動 Ao titular desta autorização é interdito o exercício de actividades que não está conforme a finalidade da entrada. The holder is prohibited from in activities that are inconsistent with the purpose of entry.

Important contact number:

Tourism Hotline: +853 28 333 000 (Cantonese, Mandarin, English, Portuguese and Japanese)

Emergency Numbers

Emergency: 999 / 110 / 112

Hospital Centre S. Januário: +853 2831 3731

Kiang Wu Hospital: +853 2837 1333

University Hospital: +853 2882 1838

Organizers:



MACETS
澳門會展旅遊業協會



澳門城市大學
Universidade da Cidade de Macau
City University of Macau



广州大学
GUANGZHOU UNIVERSITY