CONFERENCE PROGRAM

ICICS 2025

2025 International Conference on INFORMATION AND COMMUNICATIONS SECURITY

Nanjing, China

October 29-31, 2025

CONFERENCE PROGRAM

ICICS 2025 Nanjing, China

2025 International Conference on

Information and Communications Security

October 29-31, 2025

Nanjing, China

Organized By

Photo live streaming /照片直播

TABLE OF CONTENT

Note

GENERAL INFORMATION

A Conference Venue


B Onsite Registration

Holiday Inn Nanjing Qinhuai South/南京上秦淮假日酒店
NO.21 Mozhou East Road, Jiangning District, Nanjing, JS, 211111, China
中国江苏省南京市江宁区秣周东路 21 号

Arrive at Registration desk→ Inform the staff of your paper name→ Sign-in→ Claim your conference kit.

C Devices Provided by the Organizer

Oral Session: Laptops (with MS-Office & Adobe Reader) / Projectors & Screen / Laser Sticks

D Materials Provided by the Presenter

Oral Session: Slides (pptx or pdf version). Format 16:9 is preferred.

E Duration of Each Presentation

Keynote Speech: 60min, including Q&A.

Oral Session: 20min, including Q&A.

F Notice

※ Please wear your delegate badge (name tag) for all the conference activities. Lending your participant card to others is not allowed.

※ Please take good care of your valuables at any time during the conference. The conference organizer does not assume any responsibility for the loss of personal belongings of the participants during conference day.

Contact us

E-mail: icics2025@gmail.com

WELCOME MESSAGE

On behalf of the conference committees, we warmly welcome you to the 2025 International Conference on Information and Communications Security (ICICS 2025), held in Nanjing, China from October 29 to 31, 2025, organized by Southeast University (China), Swinburne University of Technology (Australia) and University of Wollongong (Australia).

ICICS was initiated in 1997, this year marks the 27th anniversary of ICICS conference. The goal and feature of this conference is to bring together researchers and practioners from both academia and industry to discuss and exchange their experiences, lessons learned, and insights related to information and communications security.

The program this year was comprised of 3 keynote lectures and 18 oral sessions.

On behalf of all the conference committees, we feel deeply grateful to all that have contributed to make this event possible: authors who contributed papers, the session chairs and the diligent reviewers. Your high competence, enthusiasm, valuable time and expertise knowledge, enabled us to prepare this conference program smoothly. Special thanks are also extended to the conference administrative committee for their tireless efforts throughout the course of the conference.

We have an exciting program at this conference that will allow members to reflect upon and celebrate our past accomplishments, renew friendships and extend our networks, and jointly explore current and future research directions. We hope that you will have a productive and fun - filled time at this very special conference. We would like to thank all of the sponsoring organizations for providing their generous financial support. Lastly, we would like to thank all of the conference participants for their contributions which are the foundation of this conference. We welcome different opinions from all participants and look forward to the better development of ICICS in the coming years.

Wish you a very successful conference!

Best regards,

Conference Organizing Committee, ICICS 2025
Nanjing

CONFERENCE COMMITTEE

Steering Committee Chair

Jianying Zhou, Singapore University of Technology and Design, Singapore

Steering Committee Members

Robert Deng, Singapore Management University, Singapore

Dieter Gollmann, Hamburg University of Technology, Germany

Javier Lopez, University of Malaga, Spain

Qingni Shen, Peking University, China

Zhen Xu, Institute of Information Engineering, Chinese Academy of Sciences, China

General Co-chairs

Guang Cheng, Southeast University, China

Willy Susilo, University of Wollongong, Australia

Organization Chair

Liquan Chen, Southeast University, China

Registration Chair

Chao Sun, Southeast University, China

Publicity Co-chairs

Weizhi Meng, Lancaster University, UK

Yong Yu, Shaanxi Normal University, China

Publication Co-chairs

Ibrahim Khalil, The Royal Melbourne Institute of Technology, Australia

Viet Vo, Swinburne University of Technology, Australia

Web Chair

Ge Wu, Southeast University, China

Program Co-chairs

Jinguang Han, Southeast University, China

Yang Xiang, Swinburne University of Technology, Australia

Program Committees

Mujeeb Ahmed, Newcastle University, UK

Massimiliano Albanes, George Mason University, USA

Cristina Alcaraz, University of Malaga, Spain

Saed Alrabaee, United Arab Emirates University, UAE

Man Ho Au, Hong Kong Polytechnic University, China

Joonsang Baek, University of Wollongong, Australia

Guangdong Bai, University of Queensland, Australia

CONFERENCE COMMITTEE

Jin Wook Byun, Pyeongtaek University, South Korea
Di Cao, Swinburne University of Technology, Australia
Xiao Chen, University of Newcastle, Australia
Rongmao Chen, National University of Defense Technology, China
Xiaofeng Chen, Xidian University, China
Ting Chen, University of Electronic Science and Technology of China, China
Yuanmi Chen, Zhejiang Lab, China
Nathan Clarke, University of Plymouth, UK
Mauro Conti, University of Padua, Italy
Bruno Crispo, University of Trento, Italy
Shujie Cui, Monash University, Australia
Jingjing Deng, Durham University, UK
Changyu Dong, Guangzhou University, China
Carmen Fernandez-Gago, University of Malaga, Spain
Anmin Fu, Nanjing University of Science and Technology, China
Steven Furnell, University of Nottingham, UK
Fei Gao, Beijing Post and Telecommunications University, China
Dieter Gollmann, Hamburg University of Technology, Germany
Yong Guan, Iowa State University, USA
Shuai Hao, Old Dominion University, USA
Hongsheng Hu, University of Newcastle, Australia
Zhi Hu, Central South University, China
Qiong Huang, South China Agricultural University, China
Xinyi Huang, Jinan University, China
Pekaric Irdin, Universität Liechtenstein, Liechtenstein
Aditya Japa, Queen's University Belfast, UK
Peng Jiang, Beijing Institute of Technology, China
Jiaojiao Jiang, University of New South Wales, Australia
Christos Kalloniatis, University of the Aegean, Greece
Sokratis Katsikas, Norwegian University of Science and Technology, Norway
Georgios Kavallieratos, Norwegian University of Science and Technology, Norway
Hyoungshick Kim, Sungkyunkwan University, South Korea
Romain Laborde, Université Toulouse III – Paul Sabatier, France
Jianchang Lai, Southeast University, China
Guyue Li, Southeast University, China
Meng Li, Hefei University of Technology, China
Shancang Li, Cardiff University, UK
Shujun Li, Kent University, UK
Song Li, Nanjing University of Finance and Economics, China
Wanpeng Li, University of Aberdeen, UK
Fagen Li, University of Electronic Science and Technology of China, China
Xiaoguo Li, Chongqing University, China
Xin Liao, Hunan University, China

CONFERENCE COMMITTEE

Jingqiang Lin, University of Science and Technology of China, China
Zhen Ling, Southeast University, China
Antonio Lioy, Politecnico di Torino, Italy
Bo Liu, University of Technology Sydney, Australia
Jianghua Liu, Nanjing University of Science and Technology, China
Bo Luo, University of Kansas, USA
Yang Lu, Nanjing Normal University, China
Xiapu Luo, The Hong Kong Polytechnic University, China
Wanlun Ma, Swinburne University of Technology, Australia
Jean-Yves Marion, Université de Lorraine, France
Daisuke Mashima, Singapore University of Technology and Design, Singapore
Weizhi Meng, Lancaster University, UK
Sky Miao, University of Newcastle, Australia
Atsuko Miyaji, Osaka University, Japan
Di Wu, University of Southern Queensland, Australia
Siaw-Lynn Ng, Royal Holloway, University of London, UK
Jianting Ning, Wuhan University, China
Takashi Nishide, University of Tsukuba, Japan
Rolf Oppliger, eSECURITY Technologies, Switzerland
Michalis Pavlidis, University of Brighton, UK
Tran Viet Xuan Phuong, University of Arkansas at Little Rock, USA
Stjepan Picek, Radboud University, The Netherlands
Yanli Ren, Shanghai University, China
Na Ruan, Shanghai Jiao Tong University, China
Sumanta Sarkar, University of Essex, UK
Nitesh Saxena, Texas A&M University, USA
Savio Sciancalepore, Eindhoven University of Technology, The Netherlands
Sevil Sen, Hacettepe University, Turkey
Jun Shao, Zhejiang Gongshang University, China
Qingni Shen, Peking University, China
Yang Shi, Tongji University, China
Chunhua Su, The University of Aizu, Japan
Purui Su, Institute of Software, CAS, China
Willy Susilo, University of Wollongong, Australia
Azadeh Tabiban, University of Manitoba, Canada
Zhiyuan Tan, Edinburgh Napier University, UK
Qiang Tang, Luxembourg Institute of Science and Technology, Luxembourg
Yangguang Tian, University of Surrey, UK
Ding Wang, Nankai University, China
Huaqun Wang, Nanjing University of Posts and Telecommunications, China
Jianfeng Wang, Xidian University, China
Nan Wang, CSIRO's Data61, Australia
Wei Wang, Xi'an Jiaotong University, China

CONFERENCE COMMITTEE

Jinpeng Wei, University of North Carolina at Charlotte, USA
Qianhong Wu, Beihang University, China
Tong Wu, University of Science and Technology Beijing, China
Zhe Xia, Wuhan University of Technology, China
Hu Xiong, University of Electronic Science and Technology of China, China
Lizhi Xiong, Nanjing University of Information Science and Technology, China
Chungen Xu, Nanjing University of Science and Technology, China
Dongpeng Xu, University of New Hampshire, USA
Guangquan Xu, Tianjin University, China
Peng Xu, Huazhong University of Science and Technology, China
Zhen Xu, Institute of Information Engineering, CAS, China
Hailun Yan, University of Chinese Academy of Sciences, China
Guomin Yang, Singapore Management University, Singapore
Kang Yang, State Key Laboratory of Cryptology, China
Rupeng Yang, University of Wollongong, Australia
Zheng Yang, Southwest University, China
Wun-She Yap, Universiti Tunku Abdul Rahman, Malaysia
Xun Yi, RMIT University, Australia
Zuobin Ying, City University of Macau, China
Yachao Yuan, Soochow University, China
Yang Yu, Tsinghua University, China
Yong Yu, Shaanxi Normal University, China
Quan Yuan, Shandong University, China
Tsz Hon Yuen, Monash University, Australia
Thomas Zacharia, University of Glasgow, UK
Fangguo Zhang, Sun Yat-sen University, China
Futai Zhang, Fujian Normal University, China
Lei Zhang, East China Normal University, China
Leo Zhang, Griffith University, Australia
Mingwu Zhang, Hubei University of Technology, China
Rui Zhang, Institute of Information Engineering, CAS, China
Yuan Zhang, Nanjing University, China
Zhi Zhang, University of Western Australia, Australia
Zongyang Zhang, Beihang University, China
Yunlei Zhao, Fudan University, China
Liang Zhao, Sichuan University, China
Yongbin Zhou, Nanjing University of Science and Technology, China
Lu Zhou, Nanjing University of Aeronautics and Astronautics, China
Huiyu Zhou, University of Leicester, UK
Youwen Zhu, Nanjing University of Aeronautics and Astronautics, China
Sencun Zhu, Pennsylvania State University, USA
Xiaogang Zhu, University of Adelaide, Australia
Cong Zuo, Beijing Institute of Technology, China

AGENDA OVERVIEW

Holiday Inn Nanjing Qinhuai South 南京上秦淮假日酒店 NO.21 Mozhou East Road, Jiangning District, Nanjing, JS, 211111, China 中国江苏省南京市江宁区秣周东路 21 号	3F Qinhuai Amazing B/尚秦淮 B 厅 Ulake/悠湖厅	5F Upark/悠谷厅 Knowledge/智慧厅/

Session Time	Tuesday, October 28, 2025 | Registration	Venue
14:00-21:00	On-site Registration	1F Lobby <Holiday Inn Nanjing Qinhuai South/南京上秦淮假日酒店>

Session Time	Wednesday, October 29, 2025 | Plenary Meeting & Oral Session	
09:00-09:15	*Host -Jinguang Han, Southeast University, China* *Opening Remark*	3F Qinhuai Amazing B 3 楼尚秦淮 B 厅
09:15-10:15	*Host - Yang Xiang, Swinburne University of Technology, Australia* *Keynote Speech I* Title: Device Awareness and User Privacy in the IoT Ecosystem **Gene Tsudik** (University of California, Irvine, USA)	
10:15-10:45	Coffee Break	
10:45-12:25	**Session 1:** Blockchain and Cryptocurrencies 1 Session chair: Xingye Lu, Hong Kong Polytechnic University, China	3F Qinhuai Amazing B 3 楼尚秦淮 B 厅
	Session 2: Access Control Session Chair: Mingwu Zhang, Hubei University of Technology, China	5F Knowledge/5 楼智慧厅
	Session 3: Traffic Classification Session Chair: Antonio Lioy, Politecnico di Torino, Italy	5F Upark /5 楼悠谷厅
12:25-14:00	Lunch <1F Peppers All Day Dining Restaurant/1 楼百香全日餐厅>	
14:00-15:40	**Session 4:** Crypto 1 Session Chair: Man Ho Au, Hong Kong Polytechnic University, China	5F Upark/5 楼悠谷厅
	Session 5: Anonymity and Privacy 1 Session Chair: Meng Li, Hefei University of Technology, China	5F Knowledge/5 楼智慧厅
	Session 6: Security and Privacy of AI 1 Session Chair: Yuan Zhang, Nanjing University, China	3F Ulake/3 楼悠湖厅
15:40-16:10	Coffee Break	
16:10-17:50	**Session 7:** Crypto 2 Session Chair: Hua Guo, Beihang University, China	5F Upark/5 楼悠谷厅
	Session 8: Anonymity and Privacy 2 Session Chair: Xiaofen Wang, University of Electronic Science and Technology of China	5F Knowledge/5 楼智慧厅
	Session 9: Security and Privacy of AI 2 Session Chair: Jianghua Liu, Nanjing University of Science and Technology, China	3F Ulake/3 楼悠湖厅
18:00-20:00	Dinner <1F Peppers All Day Dining Restaurant/1 楼百香全日餐厅>	

AGENDA OVERVIEW

Session Time	Thursday, October 30, 2025 | Plenary Meeting & Oral Session	
09:00-10:00	*Host - Jianying Zhou, Singapore University of Technology and Design, Singapore* *Keynote Speech II* Title: Cyber Ranges and Cyber-Physical Ranges: Progress, Potential, and Future Directions **Sokratis Katsikas** (Norwegian University of Science and Technology, Norway)	5F Upark/5 楼悠谷厅
10:00-10:30	Coffee Break	
10:30-12:10	**Session 10:** Machine Learning for Security Session Chair: Weizhi Meng, Lancaster University, UK	5F Upark/5 楼悠谷厅
	Session 11: System and Network Security Session Chair: Sokratis Katsikas, Norwegian University of Science and Technology, Norway	5F Knowledge/5 楼智慧厅
	Session 12: Vulnerability Analysis Session Chair: Tao Guo, Southeast University, China	3F Ulake/3 楼悠湖厅
12:25-14:00	Lunch <1F Peppers All Day Dining Restaurant/1 楼百香全日餐厅>	
14:00-17:30	**Steering Committee Meeting & Social Event (National Geopark of Mount Fang)**	
18:00-20:00	Banquet & Award Ceremony <3F Qinhuai Amazing B/3 楼尚秦淮 B 厅>	

Session Time	Friday, October 31, 2025 | Plenary Meeting & Oral Session	
09:00-10:00	*Host - Jinguang Han, Southeast University, China* Title: Post-Quantum Group-Oriented Anonymous Signatures from Symmetric Primitives **Liqun Chen** (University of Surrey, UK)	5F Upark/5 楼悠谷厅
10:00-10:30	Coffee Break	
10:30-12:10	**Session 13:** Blockchain and Cryptocurrencies 2 Session Chair: Yiwei Xu, Southeast University, China	5F Upark/5 楼悠谷厅
	Session 14: Post-Quantum Crypto Session Chair: Chao Sun, Southeast University, China	5F Knowledge/5 楼智慧厅
	Session 15: Attack and Defense 1 Session Chair: Yuanmi Chen, East China Normal University, China	3F Ulake/3 楼悠湖厅
12:10-14:00	Lunch <1F Peppers All Day Dining Restaurant/1 楼百香全日餐厅>	
14:00-16:00	**Session 16:** Crypto, Steganography and Watermarking Session Chair: Yang Shi, Tongji University, China	5F Upark/5 楼悠谷厅
	Session 17: Anomaly Detection Session Chair: Bruno Crispo, University of Trento, Italy	5F Knowledge/5 楼智慧厅
	Session 18: Attack and Defense 2 Session Chair: Jianchang Lai, Southeast University, China	3F Ulake/3 楼悠湖厅
16:00-16:30	Coffee Break	
16:30-17:00	**Closing Session**	5F Upark/5 楼悠谷厅
18:00-20:00	Dinner <1F Peppers All Day Dining Restaurant/1 楼百香全日餐厅>	

KEYNOTE SPEAKER

09:15-10:15 Wednesy, October 29,2025
3F Qinhuai Amazing B/3 楼尚秦淮 B 厅

Gene Tsudik

University of California, Irvine, USA

Speech Title: Device Awareness and User Privacy in the IoT Ecosystem

Biography: Gene Tsudik is a Distinguished Professor of Computer Science at the University of California, Irvine (UCI). He obtained his PhD in Computer Science from USC in 1991. Before coming to UCI in 2000, he was at IBM Zurich Research Laboratory (1991-1996) and USC/ISI (1996-2000). His research interests include many topics in security, privacy and applied cryptography. Gene Tsudik is a Fulbright Scholar, a fellow of ACM, IEEE, AAAS, and IFIP, as well as a foreign member of Academia Europaea. From 2009 to 2015 he served as Editor-in-Chief of ACM TOPS. He was the recipient of the 2017 ACM SIGSAC Outstanding Contribution Award, the 2020 IFIP Jean-Claude Laprie Award,the 2023 ACM SIGSAC Outstanding Innovation Award, the 2024 NDSS Test-of-Time Award, and a 2024 Guggenheim Fellowship. He authored the first rhyming crypto-poem published as a refereed paper.

Abstract: As many types of IoT devices worm their way into numerous settings in our daily lives, awareness of their presence and functionality becomes a source of major concern. Hidden IoT devices can snoop (via sensing) on unsuspecting nearby users, and impact the environment where unaware users are present, via actuation. This prompts, respectively, privacy and security/safety issues. The dangers of hidden IoT devices have been recognized and prior research suggested some means of mitigation, mostly based on traffic analysis or using specialized hardware to uncover devices. While such approaches are partially effective, there is currently no comprehensive approach to IoT device transparency. Prompted in part by recent privacy regulations (GDPR and CCPA), this work constructs a privacy-agile Root-of-Trust architecture for IoT devices called PAISA: Privacy-Agile IoT Sensing and Actuation. It guarantees timely and secure announcements of nearby IoT devices' presence and capabilities. PAISA has two components: one on the IoT device that guarantees periodic announcements of its presence even if all device software is compromised, and the other on the user device, which captures and processes announcements. PAISA requires no hardware modifications; it uses a popular off-the-shelf Trusted Execution Environment (TEE) – ARM TrustZone. A follow-on work, DB-PAISA, complements PAISA by offering request-based discovery of IoT devices via BlueTooth. To demonstrate viability, both PAISA and DB-PAISA are available as open-source prototypes. We also address their security properties and performance factors.

KEYNOTE SPEAKER

09:00-10:00 Thursday, October 30, 2025
5F Upark/5 楼悠谷厅

Sokratis Katsikas

Norwegian University of Science and Technology, Norway

Speech Title: Cyber Ranges and Cyber-Physical Ranges: Progress, Potential, and Future Directions

Biography: Sokratis K. Katsikas was born in Athens, Greece, in 1960. He is the Director of the Norwegian Centre for Cybersecurity in Critical Sectors and Professor with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology. He is also Professor Emeritus of the Department of Digital Systems, University of Piraeus, Greece, and Member of the Board of the University of Patras, Greece. In 2019 he was awarded a Doctorate Honoris Causa from the Department of Production and Management Engineering, Democritus University of Thrace, Greece. In May-June 2023 he served as Minister of Digital Governance in the interim (caretaking) government of the Hellenic Republic. Among others, he has been the Rector of the Open University of Cyprus; the Rector and Vice-Rector of the University of the Aegean, Greece; President of the National Education Council of Greece; State Secretary of Telecommunications and Posts of the Hellenic Republic; Member of the Board of the Hellenic Authority for Communication Security and Privacy (ADAE); and Member of the Board of the Hellenic Authority for Higher Education (HAHE). In 2023 and in 2024 he was listed in the Stanford University list of the top 2% most cited scientists worldwide and in 2024 he was listed in the ScholarGPS Top Scholars list of the top 0.5% of all scholars worldwide. In 2025 he received the IEEE SMC TC on Homeland Security Research and Innovation Award. He has authored or co-authored more than 300 journal papers, book chapters and conference proceedings papers. He is serving on the editorial board of several scientific journals, he has co-authored/edited 52 books and conference proceedings and has served on/chaired the technical programme committee of more than 1000 international scientific conferences. He is a member of the Steering Committee of the ESORICS Conference (chair 2017-2023) and of several other international conferences and he is the Editor-in-Chief of the International Journal of Information Security (Springer).

Abstract: A Cyber Range (CR) serves as a specialized environment designed to provide dedicated testbeds and infrastructures for executing immersive training scenarios. Its primary goal is to enhance cybersecurity knowledge among security practitioners and awareness among non-security professionals and the public, while offering a hands-on learning experience for trainees. Over time, CRs have become an indispensable tool, offering a multifaceted approach to strengthening cybersecurity postures. On the other hand, Cyber-Physical Systems (CPSs) are advanced, intelligent systems that integrate physical processes with computational elements. These encompass diverse applications such as smart grids, autonomous vehicles, medical devices, process control systems, and autopilot avionics. As a fundamental pillar of Industry 4.0, CPSs drive the convergence of formerly distinct operational technology and modern information systems. Within this evolving technological landscape, Cyber-Physical Ranges (C-PRs) have emerged as an innovative and cost-effective solution that enable researchers and practitioners to explore vulnerabilities and devise robust defense mechanisms—without compromising real-world systems. This talk will first introduce a comprehensive taxonomy of CR systems, followed by an analysis of existing literature focusing on architecture, scenario development, capabilities, roles, tools, and evaluation criteria. Subsequently, we will present a fine-grained reference architecture for CRs, built upon a rigorous three-step methodology. Additionally, we will propose an evaluation framework that quantifies the alignment of a CR with state-of-the-art practices, offering a standardized method to identify optimal components for implementing the structural, functional, and informational facets of a CR. Finally, we will explore the latest advancements in C-PRs through real-world case studies, uncovering the challenges associated with designing, deploying, and managing these environments. We will also discuss their seamless integration with emerging technologies, illustrating their pivotal role in the future of cybersecurity research and innovation.

KEYNOTE SPEAKER

09:00-10:00 Friday 31, 2025
5F Upark/5 楼悠谷厅

Liqun Chen

University of Surrey, UK

Speech Title: Post-Quantum Group-Oriented Anonymous Signatures from Symmetric Primitives

Biography: Liqun Chen is a Professor in Secure Systems at the University of Surrey. Before taking up this position in 2016, she was a principal research scientist at Hewlett-Packard Laboratories in Bristol, UK. Her 19 years working for the company led to 79 granted US patents. She developed several cryptographic schemes that were adopted by international standards bodies, such as ISO/IEC, IEEE and TCG (Trusted Computing Group). Notably, she co-designed several cryptographic algorithms, including direct anonymous attestation, which are used in the Trusted Platform Module (TPM). She was the technical leader and principal investigator in the EU H2020 FutureTPM project, which identified and developed algorithms for a TPM that would be secure against quantum computer attacks. Additionally, she has served as a principal investigator in six other EU Horizon projects that utilise post-quantum cryptography, trusted computing and distributed ledger technologies to achieve security, privacy and trust in real-world applications. She has acted as an editor or co-editor for 11 ISO/IEC documents and assisted with TCG's TPM specifications. Her current research interests include applied cryptography, post-quantum cryptography, trusted computing, and security standardisation.

Abstract: Group-oriented anonymous digital signatures, including group signatures, direct anonymous attestation (DAA) and enhanced privacy ID (EPID), have become important cryptographic primitives in information and communications security. Schemes using RSA and elliptic curve cryptography have been integrated into real-world applications and international standards. However, these standardised schemes are insecure against quantum attackers. Research into post-quantum (PQ) anonymous signatures has led to several schemes across various PQ cryptographic families. In this talk, we will focus on designing anonymous signature schemes based on symmetric techniques. For instance, we utilise a hash-based signature as a group membership credential. An anonymous signature is a non-interactive zero-knowledge proof of such a credential. We will also discuss robust design, strong security properties and efficient performance, particularly in relation to accommodating large group sizes, which is essential for rapidly developing applications.

SESSION 1

Session 1: Blockchain and Cryptocurrencies 1 Session Chair: Xingye Lu, Hong Kong Polytechnic University, China	**10:45-12:25** **Wednesday, Oct 29, 2025** 3F Qinhuai Amazing B/3 楼尚秦淮 B 厅

Time	Speech Title & Authors
10:45-11:05	**EquinoxBFT: BFT Consensus for Blockchain Emergency Governance** Jialiang Fan, Qianhong Wu, Minghang Li, Decun Luo, Qin Wang and Bo Qin
11:05-11:25	**fFuzz: A State-aware Function-level Fuzzing Framework for Smart Contract Vulnerabilities Detection** Chang Li, Binqin Lu, Wenyang Zhang, Kaixuan Yang and Huijuan Zhu
11:25-11:45	**TraceBFT: Backtracking-based Pipelined Asynchronous BFT Consensus for High-Throughput Distributed Systems** Haofeng Zhuang, Haifeng Qian, Junqing Gong and Zhili Chen
11:45-12:05	**RADIAL: Robust Adversarial Discrepancy-aware Framework for Early Detection of Illicit Cryptocurrency Accounts** Victor Kombou, Qi Xia, Jianbin Gao, Hu Xia, Brinda Leaticia Kuiche Sop and Leoba Jonathan Anto
12:05-12:25	**BR-CPPFL: A Blockchain-based Robust Clustered Privacy-preserving Federated Learning System** Yuantong Li, Xiaofen Wang, Ke Zhang, Bo Zhang, Lei Zhang, Xiaosong Ding and Qing Xu

SESSION 2

Session 2: Access Control Session Chair: Mingwu Zhang, Hubei University of Technology, China	**10:45-12:25** **Wednesday, Oct 29, 2025** 5F Knowledge/5 楼智慧厅

Time	Speech Title & Authors
10:45-11:05	**Circulation Control Model and Administration for Geospatial Data** Heng Li, Fenghua Li, Yunchuan Guo, Lingcui Zhang, Xiao Wang and Ziyan Zhou
11:05-11:25	**Identifying Unusual Personal Data in Mobile Apps for Better Privacy Compliance Check** Jiatao Cheng, Yuhong Nan, Xueqiang Wang, Zhefan Chen and Yuliang Zhang
11:25-11:45	**Why Biting the Bait? Understanding Bait and Switch UI Dark Patterns in Mobile Apps** Yixi Lin, Yue Xu, Zitong Yao, Yuhong Nan, Queping Kong and Xueqiang Wang
11:45-12:05	**DBG-LB: A Trustworthy and Efficient Framework for Data Sharing in the Internet of Vehicles** Chaoyue Li, Yongming Zhang and Xiaolong Xu
12:05-12:25	**TetheGAN: A GAN-Based Synthetic Mobile Tethering Traffic Generating Framework** Xuman Zhang, Guang Cheng and Li Deng

SESSION 3

Session 3: Traffic Classification Session Chair: Antonio Lioy, Politecnico di Torino, Italy	**10:45-12:25** **Wednesday, Oct 29, 2025** 5F Upark/5 楼悠谷厅

Time	Speech Title & Authors
10:45-11:05	**FCAL: An Asynchronous Federated Contrastive Semi-Supervised Learning Approach for Network Traffic Classification** Yu Yan, Qingjun Yuan, Weina Niu, Xiangyu Wang, Yanbei Zhu and Yongjuan Wang
11:05-11:25	**SPTC: Signature-based Cross-protocol Encrypted Proxy Traffic Classification Approach** Huajie Jia, Yige Chen and Zhengzhou Tang
11:25-11:45	**Multi-modal Datagram Representation with Spatial-Temporal State Space Models and Inter-flow Contrastive Learning for Encrypted Traffic Classification** Xianwen Deng, Ruijie Zhao, Mingwei Zhan, Shaoqian Wu, Yijun Wang and Zhi Xue
11:45-12:05	**FlowGraphNet: Efficient Malicious Traffic Detection via Graph Construction** Changsong Yang, Han Wang, Yueling Liu, Yong Ding, Hai Liang and Zhenyu Li
12:05-12:25	**RustGuard: Detecting Rust Data Leak Issues with Context-Sensitive Static Taint Analysis** Shanlin Deng, Mingliang Liu, Si Wu and Baojian Hua

SESSION 4

Session 4: Crypto 1 Session Chair: Man Ho Au, Hong Kong Polytechnic University, China	**14:00-15:40** **Wednesday, Oct 29, 2025** 5F Upark/5 楼悠谷厅

Time	Speech Title & Authors
14:00-14:20	**Multi-Signer Locally Verifiable Aggregate Signature from (Leveled) Multilinear Maps** Yuchen Yang, Jie Chen, Qiaohan Chu, Qiuyan Du and Luping Wang
14:20-14:40	**Conditional Attribute-based Encryption with Keyword Search for Pay-Per-Query Commercial Model** Zerui Guo, Sha Ma and Qiong Huang
14:40-15:00	**Lightweight Transparent Zero-Knowledge Proofs for Cross-Domain Statements** Zhengzhou Tu, Min Xie, Junbin Fang, Yong Yu and Zoe L. Jiang
15:00-15:20	**Public Verifiable Server-Aided Revocable Attribute-Based Encryption** Luqi Huang, Fuchun Guo, Willy Susilo and Yumei Li
15:20-15:40	**New First-Order Secure AES Implementation without Online Fresh Randomness Records** Botao Liu and Ming Tang

SESSION 5

Session 5: Anonymity and Privacy 1 Session Chair: Meng Li, Hefei University of Technology, China	**14:00-15:40** **Wednesday, Oct 29, 2025** 5F Knowledge/5 楼智慧厅

Time	Speech Title & Authors
14:00-14:20	**MagWatch: Exposing Privacy Risks in Smartwatches through Electromagnetic Signals** Haowen Xu, Tianya Zhao, Xuyu Wang, Jun Dai and Xiaoyan Sun
14:20-14:40	**Privacy-preserving, Secure and Certificate-based Integrity Auditing for Cloud Storage** Wenhao Wang, Yu Li, Yinxia Sun, Yuan Zhang and Sheng Zhong
14:40-15:00	**Unbalanced Private Computation on Set Intersection with Reduced Computation and Communication** Zelin Tang, Hua Guo, Yewei Guan and Kaijie Yang
15:00-15:20	**Artemis: Decentralized, Secure, and Efficient Safety Monitoring with Dynamic Trajectories** Meng Li, Zhuangwei Li, Yifei Chen, Yan Qiao and Mauro Conti
15:20-15:40	**Privacy-preserving Framework for k-modes Clustering Based on Personalized Local Differential Privacy** Yuling Luo, Zhangrui Wang, Xue Ouyang, Siyuan Zu, Qiang Fu, Sheng Qin and Junxiu Liu

SESSION 6

Session 6: Security and Privacy of AI 1 Session Chair: Yuan Zhang, Nanjing University, China	**14:00-15:40** **Wednesday, Oct 29, 2025** 3F Ulake/3 楼悠湖厅

Time	Speech Title & Authors
14:00-14:20	**A Dropout-Resilient and Privacy-Preserving Framework for Federated Learning via Lightweight Masking** Yufeng Jiang, Jianghua Liu, Chenhao Xu, Cong Zuo, Lei Xu and Jian Lei
14:20-14:40	**AFedGAN: Adaptive Federated Learning with Generative Adversarial Networks for Non-IID Data** Xuyang Zhang, Hua Jin and Peiyuan Guo
14:40-15:00	**OTTER: Optimized Training with Trustworthy Enhanced Replication via Diffusion and Federated VMUNet for Privacy-Aware Medical Segmentation** Haocheng Kan, Yuesheng Zhu, Guibo Luo and Hanwen Zhang
15:00-15:20	**EAGLE: Ensemble Adaptive Graph Learning for Enhanced Ethereum Fraud Detection** Stephane Richard Befoum, Jianbin Gao, Qi Xia, Victor Kombou, Benjamin Fabien Eyezo'O and Rossini Mulenga Mukupa
15:20-15:40	**CascadeGen: A Hybrid GAN-Diffusion Framework for Controllable and Protocol-Compliant Synthetic Network Traffic Generation** Qingyuan Yu, Chuping Yan and Xiaoying Liu

SESSION 7

Session 7: Crypto 2 Session Chair: Hua Guo, Beihang University, China	**16:10-17:50** **Wednesday, Oct 29, 2025** 5F Upark/5 楼悠谷厅

Time	Speech Title & Authors
16:10-16:30	**SM2-VBKE: Achieving Cryptographic Binding Between Verification Integrity and Key Generatio** Runze Zhao, Siqi Lu, Yongjuan Wang, Liujia Cai, Wenyi Chen and Fenghua Jiang
16:30-16:50	**Certificate-Based Quasi-Linearly Homomorphic Signatures: Definition, Construction, and Application to Data Integrity Auditing** Jintao Cai, Futai Zhang, Wenjie Yang, Shaojun Yang, Yichi Huang, Rongmao Chen and Willy Susilo
16:50-17:10	**Zero-Knowledge Protocols with PVC Security: Striking the Balance between Security and Efficiency** Yi Liu, Yipeng Song, Anjia Yang and Junzuo Lai
17:10-17:30	**Attribute-Based Adaptor Signature and Application in Control-based Atomic Swap** Tianyuan Fan, Gang Shen, Yuzhu Wang, Yuntao Wang and Mingwu Zhang
17:30-17:50	**A Versatile Decentralized Attribute Based Signature Scheme for IoT** Dazhi Xu, Yuejun Liu, Jiabei Wang, Yiwen Gao and Yongbin Zhou

SESSION 8

Session 8: Anonymity and Privacy 2 Session Chair: Xiaofen Wang, University of Electronic Science and Technology of China	**16:10-17:50** **Wednesday, Oct 29, 2025** 5F Knowledge/5 楼智慧厅

Time	Speech Title & Authors
16:10-16:30	**AnoST: An Anonymous Optimistic Verification System Based on Off-Chain State Transition** Qiyuan Gao, Qianhong Wu, Junxiang Nong and Qi Liu
16:30-16:50	**Privacy-Preserving K-hop Shortest Path Query on Encrypted Graphs Based on Graph Pruning** Ya Gao, Chao Mu, Ming Yang and Xiaoming Wu
16:50-17:10	**TA-PDC: Provable Data Contribution with Traceable Anonymous for Group Transactions** Xiaocong Lin, Weijing You, Chenchen Wu, Wenmao Liu and Qi Gu
17:10-17:30	**Fine-filter: An Effective Defense against Poisoning Attacks on Frequency Estimation under LDP** Yuxia Zhou, Qiao Xue and Youwen Zhu
17:30-17:50	**BioVite: Efficient and Compact Privacy-Preserving Biometric Verification via Fully Homomorphic Encryption.** Pengfei Zeng, Han Xia and Mingsheng Wang

SESSION 9

Session 9: Security and Privacy of AI 2 Session Chair: Jianghua Liu, Nanjing University of Science and Technology, China	**16:10-17:50** **Wednesday, Oct 29, 2025** 5F Ulake/5 楼悠湖厅

Time	Speech Title & Authors
16:10-16:30	**Efficient Semi-asynchronous Federated Learning with Guided Selective Participation and Adaptive Aggregation** Chaoyun Wang, Kedong Yan and Chanying Huang
16:30-16:50	**Improving Byzantine-resilience in Federated Learning via Diverse Aggregation and Adaptive Variance Reduction** Xiuhua Wang, Shikang Li, Fengrui Fan, Shuai Wang, Yiwei Li and Yu Zheng
16:50-17:10	**Hierarchical Recovery of Convolutional Neural Networks via Self-Embedding Watermarking** Yawen Huang and Huaicong Zhan
17:10-17:30	**Personalized Federated Learning Algorithm Based on User Grouping and Group Signature** Hao Lin, Xiaoming Hu, Shuangjie Bai and Yan Liu
17:30-17:50	**Secure Guard: A Semantic-Based Jailbreak Prompt Detection Framework for Protecting Large Language Models** Sixin Fang, Ke Cheng, Jixin Zhang, Zheng Qin and Mingwu Zhang

SESSION 10

Session 10: Machine Learning for Security Session Chair: Weizhi Meng, Lancaster University, UK	**10:30-12:10** **Tuesday, Oct 30, 2025** 5F Upark/5 楼悠谷厅

Time	Speech Title & Authors
10:30-10:50	**SPCD: A Shot-Based Partial Copy Detection Method** Yuhan Tao and Danwei Chen
10:50-11:10	**Bayesian-Adaptive Graph Neural Network for Anomaly Detection (BAGNN).** Yong Ding, Chi Zhang, Shijie Tang, Changsong Yang and Hai Liang
11:10-11:30	**UzPhishNet Model for Phishing Detection** Bektemir Saydiev, Xiaohui Cui and Umer Zukaib
11:30-11:50	**CyberNER-LLM: Cyber Threat Intelligence Named Entity Recognition With Large Language Model** Xinzheng Liu, Wangqun Lin and Zhaoyun Ding
11:50-12:10	**Provenance-Based Intrusion Detection via Multi-Scale Graph Representation Learning** Xuebo Qiu, Mingqi Lv, Tieming Chen, Tiantian Zhu and Qijie Song

SESSION 11

Session 11: System and Network Security Session Chair: Sokratis Katsikas, Norwegian University of Science and Technology, Norway	**10:30-12:10** **Tuesday, Oct 30, 2025** 5F Knowledge/5 楼智慧厅

Time	Speech Title & Authors
10:30-10:50	**Batch-oriented Element-wise Approximate Activation for Privacy Preserving Neural Networks** Peng Zhang, Ao Duan, Xianglu Zou and Dongyan Qiu
10:50-11:10	**Social-Aware and Quality-Driven Incentives for Mobile Crowd-Sensing with Two-Stage Game** Jun Tao and Hao Zou
11:10-11:30	**A Distributed Privacy Protection Method for Crowd Sensing Based on Trust Evaluation** Hai Liu, Maoze Tian, Yadong Peng and Hongye Peng
11:30-11:50	**Actions Speak Louder Than Words: Evidence-Based Trust Level Evaluation in Multi-Agent Systems** Nikolaos Fotos, Koffi Ismael Ouattara, Dimitrios S. Karas, Ioannis Krontiris, Weizhi Meng and Thanassis Giannetsos
11:50-12:10	**Bridging the Interoperability Gaps Among Trusted Architectures in MCUs** Sandro Pinto, Lu´ıs Cunha, Daniel Oliveira, Michele Grisafi, Emanuele Beozzo and Bruno Crispo

SESSION 12

Session 12: Vulnerability Analysis Session Chair: Tao Guo, Southeast University, China	**10:30-12:10** **Tuesday, Oct 30, 2025** 3F Ulack/3 楼悠湖厅

Time	Speech Title & Authors
10:30-10:50	**Towards Efficient C/C++ Vulnerability Impact Assessment in Package Management Systems** Zibo Wang, Xiangkun Jia, Jia Yan, Yi Yang, Huafeng Huang and Purui Su
10:50-11:10	**AugGP-VD: A smart contract vulnerability detection approach based on augmented graph convolutional networks and pooling** Nianlu Liu, Linlin Zhang, Wenbo Fang and Kai Zhao
11:10-11:30	**VULDA: Source Code Vulnerability Detection via Local Dependency Context Aggregation on Vulnerability-aware Code Mapping Graph** Tao Peng, Ling Gui, Lijun Cai, Junwei Tang, Aoshuang Ye and Fei Zhu
11:30-11:50	**KVT-Payload: Knowledge Graph-Enhanced Hierarchical Vulnerability Traffic Payload Generation** Faqi Zhao, Rong Shi, Guoqiao Zhou, Wen Wang and Feng Liu
11:50-12:10	**Construction and Application of Vulnerability Intelligence Ontology under Vulnerability Management Perspective** Guangxiang Dai, Peng Wang and Duohe Ma

SESSION 13

Session 13: Blockchain and Cryptocurrencies 2 Session Chair: Yiwei Xu, Southeast University, China	**10:30-12:10** **Friday, Oct 31, 2025** 5F Upark/5 楼悠谷厅

Time	Speech Title & Authors
10:30-10:50	**Enhancing Private Signing Key Protection in Digital Currency Transactions Using Obfuscation** Yang Shi, Jintao Xie, Minyu Teng, Guanxu Liu, Linhai Guo and Jiangfeng Li
10:50-11:10	**AnsBridge: Towards Secure Cross-Chain Interoperability via Anonymous and Verifiable Validators** Mingming Huang, Xiaodan Zhang, Wei Mi, Huimei Liao and Yi Sun
11:10-11:30	**TrustBlink: A zkSNARK-Powered On-Demand Relay for PoW Cross-Chain Verification With Low Cost** Bohang Wei, Yang Yang, Shihong Xiong, Minghang Li, Qianhong Wu and Bo Qin
11:30-11:50	**R1-MFSol: a Smart Contract Vulnerability Detection Model Based on LLM and Multi-modal Feature Fusion** Huibo Yang, Zhize Hao and Tao Liu
11:50-12:10	**No Place to Hide: An Efficient and Accurate Backdoor Detection Tool for Ethereum ERC-20 Smart Contracts** Shouchen Zhou, Lu Zhou and Yu Tao

SESSION 14

Session 14: Post-Quantum Crypto Session Chair: Chao Sun, Southeast University, China	**10:30-12:10** **Friday, Oct 31, 2025** 5F Knowledge/5 楼智慧厅

Time	Speech Title & Authors
10:30-10:50	**Compact Adaptively Secure Identity-Based Encryption from Middle-Product Learning with Errors** Jingjing Fan, Xingye Lu, Man Ho Au and Siu Ming Yiu
10:50-11:10	**Turtle Wins Rabbit Again: Faster Modulus Reduction for RNS-CKKS** Lianglin Yan, Pengfei Zeng and Mingsheng Wang
11:10-11:30	**A BGV-subroutinted CKKS Bootstrapping Algorithm without Sine Approximation** Jingjing Fan, Chi Zhang, Zejiu Tan, Zoe Lin Jiang, Man Ho Au and Siu Ming Yiu
11:30-11:50	**PolarKyber: Polished Kyber with Smaller Ciphertexts, Greater Security Redundancy, and Lower Decryption Failure Rate** Chen An, Ziyao Liu, Xianhui Lu and Jingnan He
11:50-12:10	**Lion: A New Ring Signature Construction from Lattice Gadget** Yanting Li, Pingbin Luo, Xinjian Chen and Qiong Huang

SESSION 15

Session 15: Attack and Defense 1 Session Chair: Yuanmi Chen, East China Normal University, China	**10:30-12:10** **Friday, Oct 31, 2025** 3F Ulake/3 楼悠湖厅

Time	Speech Title & Authors
10:30-10:50	**Domain Adaptation for Cross-Device Profiled ML Side-Channel Attacks** Ian Garrett and Ryan Gerdes
10:50-11:10	**Find the Clasp of the Chain: Efficiently Locating Cryptographic Procedures in SoC Secure Boot by Semi-automated Side-Channel Analysis 20** Shipei Qu, Yuxuan Wang, Jintong Yu, Cheng Hong, Chi Zhang and Dawu Gu
11:10-11:30	**Full-phase Distributed Quantum Impossible Differential Cryptanalysis** Kun Zhang, Tao Shang, Yuanjing Zhang and Jianwei Liu
11:30-11:50	**ProverNG: Efficient Verification of Compositional Masking for Cryptosystem's Side-Channel Security** Yiming Yang, Feng Zhou, Yuanyuan Wang, Hua Chen, Limin Fan and An Wang
11:50-12:10	**SADGA: A Self Attention GAN-Based Adversarial DGA with High Anti-Detection Ability** Jiang Luo, Shaohua Qin and Zhe Wang

SESSION 16

Session 16: Crypto, Steganography and Watermarking Session Chair: Yang Shi, Tongji University, China	**14:00-15:40** **Friday, Oct 31, 2025** 5F Upark/5 楼悠谷厅

Time	Speech Title & Authors
14:00-14:20	**Cross-Domain Lattice-based DAA Scheme with Shared Private-Key for Internet of Things System** Minzhi Liang, Liquan Chen, Yinghua Jiang, Xuyan Min, Jin Qian and Jun Luo
14:20-14:40	**MDKG: Module-lattice-based Distributed Key Generation** Ye Bai, Debiao He, Zhichao Yang, Min Luo and Cong Peng
14:40-15:00	**Towards High-Capacity Provably Secure Steganography via Cascade Sampling** Meiyang Lv, Haocheng Fu, Xiaowei Yi, Hongxian Huang, Yun Cao and Changjun Liu
15:00-15:20	**When There Is No Decoder: Removing Watermarks from Stable Diffusion Models in a No-box Setting** Xiaodong Wu, Tianyi Tang, Xiangman Li, Jianbing Ni and Yong Yu
15:20-15:40	**Robust Reversible Watermarking for 3D Models Based on Auto Diffusion** Function Zixing Lin, Yaolong Song and Rui Li

SESSION 17

Session 17: Anomaly Detection Session Chair: Bruno Crispo, University of Trento, Italy	**14:00-15:40** **Friday, Oct 31, 2025** 5F Knowledge/5 楼智慧厅

Time	Speech Title & Authors
14:00-14:20	**Speaker Inference Detection Using Only Text** Ruoxi Cheng, Yizhong Ding, Shaowei Yuan and Zhiqiang Wang
14:20-14:40	**DTGAN: Diverse-Task Generative Adversarial Networks for Intrusion Detection Systems Against Adversarial Examples** Yiyang Wang, Wuxia Bai and Kai Chen
14:40-15:00	**ConComFND: Leveraging Content and Comment Information for Enhanced Fake News Detection** Huan Zhang, Chanying Huang, Kedong Yan and Shan Xiao
15:00-15:20	**Transferable Adversarial Attacks in Object Detection: Leveraging Ensemble Features and Gradient Variance Minimization** Zhitong Lu, Zhen Xu, Qian Yang and Kai Chen
15:20-15:40	**VAE-BiLSTM: A Hybrid Model for DeFi Anomaly Detection Combining VAE and BiLSTM** Shujiang Xu, Xiaomin Luo, Lianhai Wang, Miodrag Mihaljevi´e, Shuhui Zhang, Wei Shao and Qizheng Wang

SESSION 18

Session 18: Attack and Defense 2 Session Chair: Jianchang Lai, Southeast University, China	**14:00-16:00** **Friday, Oct 31, 2025** 3F Ulake/3 楼悠湖厅

Time	Speech Title & Authors
14:00-14:20	**POWERPOLY: Multilingual Program Analysis with the Aid of Web Assembly** Zhuochen Jiang and Baojian Hua
14:20-14:40	**Not only spatial, but also spectral: Unnoticeable backdoor attack on 3D point clouds** Yongzhen Jiang, Haoran Li, Hongjia Liu, Jiageng Pan and Jian Xu
14:40-15:00	**Permutation-Based Cryptanalysis of the SCARF Block Cipher and Its Randomness Evaluation** Qi Li, Wenying Zhang and Xiaomeng Sun
15:00-15:20	**Secure and Scalable TLB Partitioning Against Timing Side-Channel Attacks** Tianyi Huang, Xiaolin Zhang, Kailun Qin, Boshi Yuan, Chenghao Chen, Yipeng Shi, Chi Zhang and Dawu Gu
15:20-15:40	**Security Vulnerabilities in AI-Generated Code: A Large-Scale Analysis of Public GitHub Repositories** Maximilian Schreiber and Pascal Tippe
15:40-16:00	**FluxSketch: A Sketch-based Solution for Long-Term Fluctuating Key Flow Detection** Jun Xu, Guoju Gao, Yu-E Sun, He Huang and Yang Du

NOTE

Organized by

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

江苏省网络空间安全学会
Jiangsu Cyber Security Association

江苏省计算机学会
JIANGSU COMPUTER SOCIETY

Springer