南京航空航天大學
NANJING UNIVERSITY OF AERONAUTICS AND ASTRONAUTICS

The 4th International Conference on Data Security and Privacy Protection

(DSPP 2026)

Program

November 06–08, 2026
Nanjing, China

Organizing Committee

Honorary Chairs

Elisa Bertino	Purdue University	USA
Moti Yung	Columbia University	USA

Technical Program Committee Chairs

Xingshuo Han	Nanjing University of Aeronautics and Astronautics	China
Guohua Tian	Xidian University	China
Tianwei Zhang	Nanyang Technological University	Singapore

General Chairs

Shengjun Huang	Nanjing University of Aeronautics and Astronautics	China
Man Ho Allen Au	The Hong Kong Polytechnic University	China

Steering Committee

Xiaofeng Chen	Xidian University	China
Xinyi Huang	Nanjing University of Aeronautics and Astronautics	China
Yang Xiang	Monash University	Australia

Organizing Chairs

Youwen Zhu	Nanjing University of Aeronautics and Astronautics	China
Rui Zhang	Nanjing University of Aeronautics and Astronautics	China
Qiao Xue	Nanjing University of Aeronautics and Astronautics	China

Xinlei He	Wuhan University	China

Publication Chair

Haoxiang Tian	Nanyang Technological University	Singapore

Publicity Chairs

Shengmin Xu	Fujian Normal University	China
Shaofeng Li	Southeast University	China
Kangjie Chen	Tianjin University	China
Haozhao Wang	Huazhong University of Science and Technology	China

Contact:

Xingshuo Han (韩星烁)：+86 13420839743

Sponsored by:

- Nanjing University of Aeronautics and Astronautics
- Collaborative Innovation Center of Novel Software Technology and Industrialization
- Springer

Program

November 6　Reception Hall, Lakehome Hotels and Resorts（丽湖雅致酒店）

15:00–21:00	**Registration**

November 7　Main Hall（主厅）, Lakehome Hotels and Resorts

08:00–21:00	**Registration**
08:20–08:40	**Opening Remarks**
08:40–09:20	**Keynote Talk 1（Chair：Xiaofeng Chen）** **Topic: Identify Without Seeing: Visual Privacy Protection for Trustworthy Face Recognition** **Xinbo Gao**
09:20–10:00	**Keynote Talk 2（Chair：Xiaofeng Chen）** **Topic: AI Across the Lifecycle: Security, Safety, and Accountability** **Yang Xiang**
10:00–10:20	**Coffee Break**
10:20–11:00	**Keynote Talk 3（Chair：Xinlei He）** **Topic: Secure and Trustworthy Technologies for Intelligent Model Training and Inference** **Meng Shen**
11:00–11:40	**Keynote Talk 4（Chair：Xinlei He）** **Topic: Research on Password Guessing with Side-Channel Information** **Ding Wang**
11:40–14:00	**Lunch**
14:00–14:40	**Keynote Talk 5 （Chair: Jinguang Han）** **Topic: Fully Homomorphic Encryption for Privacy-Preserving AI** **Huaxiong Wang**

14:40–15:20	**Keynote Talk 6（Chair：Jinguang Han）** **Topic: Physical AI Security: Challenges and Practices** **Xiaoyu Ji**
15:20–16:00	**Keynote Talk 7（Chair：Jinguang Han）** **Topic: Data Security Protection Technologies for Commercial Spaceflight** **Qidi You**
16:00–16:20	**Coffee Break**
16:20–17:00	**Keynote Talk 8（Chair：Shengmin Xu）** **Topic: Building Efficient LLM Agents for Penetration Testing** **Gelei Deng**
17:00–17:40	**Keynote Talk 9（Chair：Shengmin Xu）** **Topic: Dynamic Pattern Discovery in Time-Series Data Security: A Kernel Self-Representation Learning Perspective** **Kunpeng Xu**
18:15–21:00	**Banquet**

November 8　Tangshan Lukou (汤山禄口) Hall, Lakehome Hotels and Resorts

08:30–09:10	**Opening Remarks**	
	Session 1: AI and System Security **Tencent Meeting: 864-540-436** **Chair: Qiao Xue**	
09:10–09:25	**BitTrace: Black-Box Multi-Bit Watermarking for Client Attribution of LLM Copies**	Hao Xia, Aoting Hu, Haoran Ou, Hao Wang, Xinwei Zhang
09:25–09:40	**Erasing Watermarks Resistant to Model Extraction in Neural Networks**	Ruigang Liang, Peizhuo Lv, Pan Li, Hualong Ma, Yuan Gao, Tao Chen, Yuxuan Chen
09:40–09:55	**HierAudioWM: Hierarchical Dual Watermarking for Speech Synthesis Attribution**	Jie Zhou, Jinhua Ma, Wenqi Li, Shen Lin, Jiayin Li, Yongcheng Song, Shengmin Xu
09:55–10:10	**Causality-Driven Physical Attacks against VLM-based Embodied Agents**	Dongdong An, Lei Liu, Zheng Wei, Letian Fang, Shuo Zhang, Wenbing Tang
10:10–10:25	**Class-Generalizable Few-Shot Anomaly Detection via Feature Adaptation and Region Guidance**	Yuting Xue, Jiayin Li, Li Xu, Yuanfei Dai

10:25–10:45	**Coffee Break**	
10:45–11:00	**Unsupervised Machine Learning Methods for Static Gesture-based Authentication on Mobile Devices**	Maria Kazachuk, Mikhail Petrovskiy, Igor Mashechkin, Oleg Chikin
11:00–11:15	**Forgetting Beyond the Requested Scope: Targeted Over-Unlearning Attacks on CLIP**	Feng Li, Jinhua Ma, Xianxin Zhao, Shen Lin, Jiayin Li, Shengmin Xu
11:15–11:30	**GridFusion-IDS: Architecture and Design of a Heterogeneous Data Fusion Framework for Smart Grid Cyber-Physical Intrusion Detection**	Weiliang Li, Jiufeng Pang, Rui Shi, Yahao Zhang, Jing Li, Jingchu Wang
11:30–11:45	**Benchmarking Heterogeneous Cyber-Physical Features for Three-Class Smart Grid Event Classification on the MSU-ORNL Dataset**	Jiufeng Pang, Weiliang Li, Rui Shi, Qi Guo, Zhou Yuan, Yating Gao
11:45–12:00	**EL3Fuzz: Fuzzing Binary Secure Monitor Firmware via SMC Interface Recovery**	Lening Xu, Hao Han
	Lunch	

November 8　Dongshan Moling (东山秣陵) Hall, Lakehome Hotels and Resorts

08:30–09:10	**Opening Remarks**	
	Session 2: Privacy Protection and Data Security **Tencent Meeting: 248-673-100** **Chair: Rui Zhang**	
09:10–09:25	**Practical Privacy-Preserving Genomic Pattern Matching in Digital Biobanks**	Yizhen Wu, Willy Susilo, Nan Li, Yudi Zhang
09:25–09:40	**HDW-Based Group Covert Communication on Blockchain**	Yongjie Wu, Haibo Tian
09:40–09:55	**SecKnee: Secure Parameter Selection for Privacy-Preserving DBSCAN**	Xuyan Chen, Renwan Bi, Yuanyuan Zhang, Jiayi Huang, Jinbo Xiong
09:55–10:10	**BLADE: A Blockchain-Coordinated Dual-Server Secure Aggregation Protocol with Linear Auditing for Federated Learning**	Zunyu Ding, Huijie Yang, Tianpei Lu, Wenying Zheng

10:10–10:25	**Cross-Stage Optimization for Secure Multi-Party Learning with Differential Privacy**	Xujie Li, Jun Ye
10:25–10:45	**Coffee Break**	
10:45–11:00	**FastBatchPIR: Towards Efficient Online Query Processing in Batch Private Information Retrieval**	Zhihong Liu, Haibo Tian
11:00–11:15	**Data Poisoning Attacks and Defenses for Frequency Estimation under Personalized Local Differential Privacy**	Liu Guanjie, Zheng Jiping
11:15–11:30	**Road-Segment Metric Privacy Against Trajectory Linkage in Vehicular Event Publishing**	Haokun Zhang, Huamao Xie, Haojun Fu
11:30–11:45	**Don't Show What They Can't See: Authorization-First Schema Context for Secure Text-to-SQL**	Jianan Jiang, Yu Wang
11:45–12:00	**ForkSeal: Crash-Consistent Private Authorization for Checkpointable AI Agents**	Ping Wang, Mengxin Lv
	Lunch	

November 8　Guli Hushun (谷里湖熟) Hall, Lakehome Hotels and Resorts

08:30–09:10	**Opening Remarks**	
	Session 3: Cryptographic Schemes and Protocols **Tencent Meeting: 776-338-364** **Chair: Xingshuo Han**	
09:10–09:25	**Verifiable and Revocable Data Capsule for Controllable Group Data Sharing in Cloud Computing**	Meixia Miao, Zhengmao Chen, Peihong Qiang, Jianghong Wei, Guohua Tian
09:25–09:40	**Redactable Blockchain from Distributed and Revocable Policy-Based Chameleon Hash**	Yanqi Zhao, Teng Zhang, Xiaoyi Yang, Jiaqi Guo, Yangguang Tian, Yong Yu, Baodong Qin
09:40–09:55	**PUF-Based Authenticated Key Exchange with Fast Handover for the Internet of Drones**	Yao Hongbo, Liu Jiahao, Su Jinshu
09:55–10:10	**SM9-Based One-Round Tripartite Key Agreement with Session Binding and Conditional Forward Secrecy**	Xiaohu Liu, Mengqi Feng

10:10–10:25	**SM9 Identity-Bound Multi-Holder Anonymous Credentials**	Kuan Liu, Jianting Ning, Lefeng Zhang, Zuobin Ying, Zongyang Zhang
10:25–10:45	**Coffee Break**	
10:45–11:00	**A Verifiable and Redactable Blockchain with Traceability and Error Correction**	Meixia Miao, Panpan Liu, Siqi Zhao, Jianghong Wei, Guohua Tian
11:00–11:15	**A New Code-Based Signcryption Scheme**	Kuojie Xiao, Fangguo Zhang, Yang Yang
11:15–11:30	**k-out-of-n Σ-Protocol for ISIS Problem**	Qi Li, Shaojun Yang
11:30–11:45	**Toward Quantum Advantage in Learning Parities with Structured Noise via Lower Bound Optimization of the Condition Number**	Yusen Han, Xuelian Li, Juntao Gao, Bo Song
	Lunch	

Sponsored by:

- Nanjing University of Aeronautics and Astronautics
- Collaborative Innovation Center of Novel Software Technology and Industrialization
- Springer