CONFERENCE PROGRAM

ICICS 2026

28th International Conference on
INFORMATION AND COMMUNICATIONS SECURITY

Fukui, Japan
October 27–30, 2026

Program Co-Chairs: Mauro Conti and Chunhua Su

TABLE OF CONTENTS

Section	Contents
General information	Venue, format, timing and presentation instructions
Agenda overview	Four-day overview of shared events and rooms
Keynote speakers	Speakers, scheduled times and titles
In-person program	Hall AB and Room 603, 27–30 October
Online program	Online Room, evening/night windows
Poster gallery	17 posters; presented during coffee breaks

GENERAL INFORMATION

Conference dates	October 27–30, 2026
Venue	Senshu Building, Fukui, Japan (final room allocation to be confirmed)
Format	Two parallel in-person rooms (Hall AB and Room 603) plus one online room
Regular paper	15 minutes: 12-minute presentation + 3-minute Q&A
Short paper	12 minutes: 9-minute presentation + 2-minute Q&A + 1-minute changeover
Poster	Coffee Break & Poster Presentations during the morning and afternoon coffee breaks; online poster slots are 10 minutes (7-minute talk + 3-minute Q&A)
Online windows	Oct 27 13:00 and 21:00; Oct 28 13:00 and 22:42; Oct 29 13:00 and 22:00; Oct 30 09:45. One room, continuous sessions without breaks.
Important	On Oct 28–29 most online sessions run in the afternoon; the remaining evening sessions on Oct 27–28 may continue past midnight. All times are local Japan time (JST).

AGENDA OVERVIEW

Date	Shared events	Hall AB / Room 603	Online Room
Tue, Oct 27	09:00–09:20 ICICS 2026 General Co-Chairs' Welcome Address / ICICS 2026 PC Co-Chairs' Report; 09:20–10:00 Keynote 1; 12:40–13:20 Lunch; 18:00–20:00 welcome reception	10:15, 11:40, 13:20, 14:20, 16:00 regular sessions	13:00–18:30 and 21:00–22:12, 26 papers
Wed, Oct 28	12:00 excursion departure (Tojinbo); 13:00–16:45 NEXUS Workshop Session 1 (from 15:15 in Room 604); 13:10–13:50 Keynote 2 — Prof. Cong Wang	09:00, 10:25 regular; 11:15 short/regular	13:00–17:06 and 22:42–01:12, 27 papers
Thu, Oct 29	09:00 Keynote 3; 11:50–12:35 NEXUS Workshop Session 1 (cont.); 12:00 social event (Eiheiji Temple & Ichijodani Ruins); 13:00–17:00 NEXUS Workshop Session 2; 18:00 banquet (Rose Garden, Fukui City)	09:55 regular; 11:10 short/regular	13:00–16:45 and 22:00–22:45, 18 regular papers
Fri, Oct 30	15:50 closing (all in-person sessions end by 16:20)	09:00, 10:25 regular; 13:00, 14:08, 15:08 short	10:00–11:30 regular; 11:30–18:54 short; 19:00 online poster session (3 posters)

PAPER COUNTS

Category	Count
Regular papers	148
Short papers	69
Posters	17
In-person oral papers	103
Online oral papers	114
Total oral papers	217

KEYNOTE SPEAKERS

Time	Speaker	Title
Tue, Oct 27 09:20–10:00	Prof. Moti Yung	Security, Privacy, Society: Theory and Practice Supporting Concrete Problems
Wed, Oct 28 13:10–13:50	Prof. Cong Wang	AI x Cybersecurity: Navigating Challenges and Embracing Opportunities
Thu, Oct 29 09:00–09:40	Prof. Kwangjo Kim	Beyond Classical Cryptography: Neural Leakage, Post-Quantum Signatures, and the Security Frontier

KEYNOTE 1 — PROF. MOTI YUNG

Security, Privacy, Society: Theory and Practice Supporting Concrete Problems

Abstract. I will review the field of Applied Cryptography, explain how it differs from and relates to other fields, and discuss its ultimate goal: responsibly aiding society. Then I will cover how to seek innovation in this field, focusing mainly on lessons from various areas of cryptographic research. I will naturally exemplify this through some of my work. Primary attention will focus on the connections and transition of results among theory (math), practice (systems research), and concrete deployments (engineering). The presentation will be suitable for a general security research audience.

Bio. Moti Yung is a Distinguished Research Scientist with Google and a senior Research Faculty member at Columbia University. Previously he worked for IBM, SNAP, and Certco. He got his PhD in 1988 from Columbia University. Yung is a member of the US National Academy of Engineering, and the American Academy of Arts and Sciences. He is a fellow of ACM, IEEE, IACR, and EATCS. His recognitions include a number of awards, including the IEEE 2026 Innovation in Societal Infrastructure award, the IEEE-CS Computer Pioneer Award 2021, and the ACM-SIGSAC 2014 Outstanding Innovation award.

DAY 1 — Tuesday, October 27, 2026

IN-PERSON PROGRAM

08:30–09:00 Registration desk opens
10F / Hall AB foyer · Registration desk on the 10F, in front of Hall AB; open from 8:30 every day.

09:00–09:20 ICICS 2026 General Co-Chairs' Welcome Address / ICICS 2026 PC Co-Chairs' Report
Hall AB · Welcome address and program committee report.

09:20–10:00 Keynote 1 — Prof. Moti Yung: "Security, Privacy, Society: Theory and Practice Supporting Concrete Problems"
Hall AB · 40-minute keynote

Session 1: Cryptanalysis and Secure Computation — ON-SITE

Hall AB · Tuesday, October 27, 2026 | 10:15–11:00 · Session Chair: Prof. Atsuko Miyaji

10:15–10:30	Improving Small Private Exponent Attack on RSA: Making It Faster and More Practical	Jun Song, Jun Xu, Hao Jiang, Haomeng Xu and Lei Hu
10:30–10:45	On the Committing Security of Generic Compositions for Authenticated Encryption	Yan Jia, Xueqi Zhu, Peng Wang, Lei Hu and Gang Liu
10:45–11:00	AH-BKZ: A Lattice Reduction Algorithm with Asynchronous Hybrid Processing	Renya Hashimoto, Junji Shikata, Atsushi Takayasu and Yuntao Wang

Session 2: Ring Signatures and Post-Quantum Implementations — ON-SITE

Room 603 · Tuesday, October 27, 2026 | 10:45–11:15 · Session Chair: Prof. Jianying Zhou

10:45–11:00	A RISC-V Software Implementation and Instruction Set Extension for PERK	Yunfei Wang, Hao Cheng, Qi Tian, Weijia Wang and Long Chen
11:00–11:15	SoK: Ring Signatures from Symmetric-Key Primitives: A Systematisation and Research Agenda	Zhixuan Li, Joseph Liu, Tsz Hon Yuen and Xinyu Zhang

11:15–11:40 Coffee Break & Poster Presentations
Poster area · Poster presentations during the on-site break.

Session 3: Secure Multiparty Computation and Cryptographic Engineering — ON-SITE

Hall AB · Tuesday, October 27, 2026 | 11:40–12:40 · Session Chair: Prof. Kouichi Sakurai

11:40–11:55	A Holistic PS-PL-AIE Co-Design for ML-KEM and ML-DSA on Versal AI Platforms	Ningyue Zhang, Tengfei Wang, Chenghao Chen, Zixin He, Chi Zhang, Pei Cao and Dawu Gu
11:55–12:10	Secure Constant-Round Multi-Party Fair Exchange without Broadcast Channel	Yuhi Fujisaka, Takeshi Nakai and Koutarou Suzuki
12:10–12:25	Graph-based Asynchrony for Any Linear Verifiable Secret Sharing Scheme	Hugo Delavenne and Lola-Baie Mallordy
12:25–12:40	Prism: Scalable and Efficient High-Dimensional Fuzzy Private Set Intersection via Compact Mapping	Zhenyu Xiong, Kai Chen, Xingwei Ren, Yongqiang Li and Mingsheng Wang

Session 4: Digital Signatures and Signcryption

ON-SITE

Room 603 · Tuesday, October 27, 2026 | 11:40–12:25 · Session Chair: Prof. Atsuko Miyaji

11:40–11:55	Prefix Puncturable Signatures from Hierarchical Identity-Based Signatures	Masayuki Tezuka and Keisuke Tanaka
11:55–12:10	Efficient Dual-Side Online/Offline Heterogeneous Signcryption for Low-Altitude SAGINs	Zhe Xia, Jiale Shen and Yifei Wang
12:10–12:25	Batching Returns: Revamping Insecure Exponent-Inversion Ring Signatures	Sherman S. M. Chow

12:40–13:20 Lunch

Hall AB

Session 5: Blockchain Interoperability and Privacy-Preserving Collaboration

ON-SITE

Hall AB · Tuesday, October 27, 2026 | 13:20–14:05 · Session Chair: Prof. Kazumasa Omote

13:20–13:35	Extending Subsidy Bridge to Bidirectional Interoperability	Yifu Geng, Wei Huang, Bo Qin, Bohang Wei, Jian Liu, Xinyu Li and Wenchang Shi
13:35–13:50	Bitwork: Achieving Verifiable Adoption for Decentralized Collaboration	Wei Huang, Yifu Geng, Bo Qin, Qin Wang, Xinyu Li, Jiaqi Su and Na Luo
13:50–14:05	D-PayIns: Deployer-Led Insurance for Risky Smart Contract Services	Jiaqi Su, Xinyu Li, Na Luo, Kailun Song, Lan Luo, Jingxuan Cheng, Bo Qin and Wenchang Shi

Session 6: Zero-Knowledge Proofs, Signatures and Watermarking

ON-SITE

Room 603 · Tuesday, October 27, 2026 | 13:20–14:20 · Session Chair: Prof. Akihito Nakamura

13:20–13:35	DL-Based Ring Signatures Using Curve Trees: Sublinear Signing and Verification with Precomputed Tree	Keigo Hayakawa, Toru Nakanishi, Teruaki Kitasuka and Zhuotao Lian
13:35–13:50	Human-Extractable ZK Proofs of Knowledge: A Solution to Dark DAOs	Zeyuan Yin, Leiyuan Tian, Bingsheng Zhang and Kui Ren
13:50–14:05	Card-Based Zero-Knowledge Proof Protocol for Polyomino Tiling Puzzle	Koichi Koizumi, So Shibamiya, Eikoh Chida, Daichi Muro and Takaaki Mizuki
14:05–14:20	Embedding Watermarks in Diffusion Process for Model Intellectual Property Protection	Jijia Yang, Sen Peng and Xiaohua Jia

Session 7: Robust Learning, Model Protection and Verifiable Systems

ON-SITE

Hall AB · Tuesday, October 27, 2026 | 14:20–15:35 · Session Chair: Prof. Mauro Conti

14:20–14:35	On the Adversarial Robustness of Temporal Ethereum Malicious Activity Detection	Dong Wang, Bofeng Pan, Nian Li, Liyun Shao and Shasha Zhang
14:35–14:50	DiTMark: Secure Watermarking for Model Ownership in Diffusion Transformers	Nicholas Chivaran, Qi Li and Jianbing Ni
14:50–15:05	Decryption-as-Vote: Zero-Communication Reconstruction Latency via Hard-Coupled Threshold Encryption in BFT Consensus	Zhenyang Ding, Qianhong Wu, Minghang Li and Ziyu Zhao
15:05–15:20	VDR-Proof: State Attestation for Verifiable Data Registry through Distributed Users	Iifan Tyou, Haocheng Jiang, Shigenori Ohashi and Kanta Matsuura
15:20–15:35	Model-Space Reversal for Efficient Federated Agnostic Unlearning	Xiangyun Tang, Zuobin Ying, Zijie Pan, Yajie Wang, Liehuang Zhu, Wanlei Zhou and Jianfeng Ma

15:35–16:00 Coffee Break & Poster Presentations

Poster area · Poster presentations during the on-site break.

Session 8: Public-Key Cryptography and Secure Communication

ON-SITE

Hall AB · Tuesday, October 27, 2026 | 16:00–17:00 · Session Chair: Prof. Sherman S. M. Chow

16:00–16:15	TreeCast: Multi-Party Key Establishment Protocol for IoT Devices	Supriyo Banerjee and Sayon Duttagupta
16:15–16:30	Extended Withdrawable Signatures with Refined Security: Generic Constructions and Post-Quantum Instantiations	Madusha Chathurangi, Qinyi Li, Ernest Foo and Leo Yu Zhang
16:30–16:45	AnonyWing: Anonymous Message Delivery	Enyu Liu, Haobo Wang, Yuxuan Li and Zengpeng Li
16:45–17:00	Generic Construction of CCA-Secure PKE from Key-Insulated and Privacy-Preserving Signatures with Publicly Derived Public Key	Ryo Mizuno and Keita Emura

Session 9: Federated Learning: Attacks, Detection and Robust Aggregation

ON-SITE

Room 603 · Tuesday, October 27, 2026 | 16:00–16:30 · Session Chair: Dr. Bofeng Pan

16:00–16:15	APT-Oriented Steganographic Covert Channels in Federated Learning	Qingkui Zeng and Zhuotao Lian
16:15–16:30	FedGAR: Guardrailed RL Aggregation with Multi-View Evidence for Byzantine-Majority Federated Learning	Wenye Xing, Jiageng Chen, Yuanyuan He, Changrui Zheng and Yanyu Tong

18:00–20:00 Welcome reception

Hall AB

DAY 1 — Tuesday, October 27, 2026

ONLINE PROGRAM

Online Session 1: AI Security and Homomorphic Encryption

ONLINE

Online Room · Tuesday, October 27, 2026 | 13:00–14:00

13:00–13:15	A Lightweight and Comprehensive Robust Graph Structure Learning Method Chenyu Zhou, Hanjie Dong, Wei Huang, Yabin Peng and Kunlin Li
13:15–13:30	PixCrypt: Fast Fine-Grained FHE with Range-Aware Caching Chao Wang, Shubing Yang, Xiaoyan Sun, Yan Bai, Jun Dai and Dongfang Zhao
13:30–13:45	Functional Bootstrapping for Fully Homomorphic Encryption Over the Integers Haohao Jiang, Xiaoyi Wang, Min Zhang and Dengguo Feng
13:45–14:00	SHADE: A Symmetric-Homomorphic Adaptor for Duplex Evaluation over AES-Transciphered Circuits Yanhan Huang, Feng Qi, Xiaohong Li and Debiao He

Online Session 2: Cryptographic Protocols and Encrypted Search

ONLINE

Online Room · Tuesday, October 27, 2026 | 14:15–15:45

14:15–14:30	Scalable Method of Reachability Analysis for Quantum Cryptographic Protocols via Tensor Network Partitioning Mingyuan Pang, Juan Xu, Sunqi Cai, Yuanyuan Ma, Yanyang Shu and Jiawei Xu
14:30–14:45	Memory-Efficient Implementation of Scloud+ for Resource-Constrained Embedded Devices Xiaoqi Zhang, Lu Zhou and Hao Yang
14:45–15:00	Multi-party Computation over Finite Cyclic Groups with Friends and Foes Hikaru Tsuchida and Takashi Nishide
15:00–15:15	Private Set Union Aggregates via Functional Encryption Gao Liu, Yuchen Huang, Shengnan Zhao, Shan Jing, Zhenxiang Chen and Chuan Zhao
15:15–15:30	VMES-MC: A Lightweight Verifiable Multi-Owner Encrypted Search Scheme for Mobile Cloud Yang Yu, Fei Zhu, Minghao Yang, Xingpeng Zhang, Chunhua Ren and Bopeng Fang
15:30–15:45	Composable Aggregation of Schnorr Signatures via Transcript Rebinding Lingqing Zhao, Liping Wang and Yu Li

Online Session 3: Model Security and Website Fingerprinting

ONLINE

Online Room · Tuesday, October 27, 2026 | 15:45–17:00

15:45–16:00	MetaCorr: Robust Black-Box Model Ownership Verification via Meta-Optimized Corrective Fingerprints Yingying Sun, Chen Gu, Donghui Hu, Shenyuan Ren and Yaofei Wang
16:00–16:15	PRISM: Fusing Prediction-Inference Evidence for Test Selection in Deep Neural Networks Runze Yan, Benxiao Tang, Jianpeng Ke, Weixiang Ren and Aoshuang Ye
16:15–16:30	Learning from Ambiguity: Uncertainty-Aware Intervention for Multimodal Learning Baohua Wen, Zijie Pan, Jianhang Ji, Yani Wang and Zuobin Ying
16:30–16:45	DeepFinger: A Dynamic Fingerprinting Framework for Digital Rights Management in Model Distribution Linqi Li, Wei Wu, Youyang Qu, Cong Zuo, Lei Xu and Jianghua Liu
16:45–17:00	ALEM-WF: Adaptive Local Evidence Modeling for Robust Multi-Label Website Fingerprinting Jiaqi Feng, Peipei Fu, Haibo Xiao, Gaopeng Gou, Zhen Li, Gang Xiong, Lin Chen and Zhenzhen Li

Online Session 4: Post-Quantum Implementations and Federated Learning Security

ONLINE

Online Room · Tuesday, October 27, 2026 | 17:00–18:30

17:00–17:15	Practical Private Set Union via Trusted Execution Environments Xiaotian Zhang, Shujie Cui, Tsz Hon Yuen and Man Ho Au
17:15–17:30	Optimized Implementation of Kyber on Resource-Constrained 8-bit AVR Microcontrollers Jingwen Lu, Lu Zhou, Sihan He, Zhe Liu and Liming Fang
17:30–17:45	A Compact Ring-LWR KEM over Power-of-Two Arithmetic with Efficient NTT-Based Multiplication Shijia Ye, Lu Zhou, Wen Zhang and Feng Zhang
17:45–18:00	Communication-Efficient and Privacy-Preserving Vertical Federated Learning via Dynamic Quantization Saifei Qu, Enting Guo, Hongyun Cai, Xiaoqian Chen and Shuai Shang
18:00–18:15	DynamicGater: Fine-Grained Recovery for Machine Unlearning via Dynamic Neuron Gating Xiaoqian Chen, Hongyun Cai, Shuai Shang, Saifei Qu and Enting Guo
18:15–18:30	FedMCE: Model Capacity Effect for Backdoor Detection in Federated Learning Xingyu Chen

Online Session 5: IoT, Networks and Post-Quantum Signatures

ONLINE

Online Room · Tuesday, October 27, 2026 | 21:00–22:12

21:00–21:15	Concurrent Signatures from Isogeny Assumptions Xuan Thanh Khuc, Willy Susilo, Dung Hoang Duong, Partha Sarathi Roy, Kazuhide Fukushima and Shinsaku Kiyomoto
21:15–21:30	IoTPrune: Causality-Guided Device-State Integrity Verification in Smart Homes Mahdieh Ghorbanian, Suryadipta Majumdar, Paria Shirani, Menan Ratnasabapathy and J. David Brown
21:30–21:45	SL-DNPR: A Protocol-Aware Open-Set Radio Frequency Fingerprint Identification Framework for WiFi Scenarios Shuzhen Sun, Yutong Li, Lishan Jin, Junbo Su, Jinhui Cao, Xiaoqiang Di and Hui Qi
21:45–22:00	CTD-Fed: A Conditional Tabular Diffusion Data Augmentation Method for Federated Intrusion Detection in Satellite Networks Qiaojun Qu, Xu Liu, Yu Wang, Chunbo Wang, Yuqing Pei and Hui Qi
22:00–22:12	Satellite Network Multicast Routing Method Based on Orbital Average Distance Clustering Dan Zhao, Guoying Zhang, Chunbo Wang, Ligang Cong and Hui Qi

DAY 2 — Wednesday, October 28, 2026

IN-PERSON PROGRAM

Session 10: Media Security and AI-Assisted Security Testing

ON-SITE

Hall AB · Wednesday, October 28, 2026 | 09:00–10:00 · Session Chair: Prof. Joseph Liu

09:00–09:15	Defending Against Audio Spoofing Attacks via Emotion-Aware Prototype Metric Learning Xiaokang Li, Yicheng Gong, Dinghao Zou and Jialan Chen
09:15–09:30	CRISP: Channel-Randomised Single-Image Steganography with Permutations Shahzad Ahmad and Stefan Rass
09:30–09:45	SCOUT: Structural Coverage-Guided Diffusion for Testing Deep Classifiers Shilin Zhang, Benxiao Tang, Jianpeng Ke, Aoshuang Ye, Yiru Zhao and Lei Zhao
09:45–10:00	WhalingX: A Concurrent Multi-Agent Penetration Testing Framework via BDI Cognition and Queuing Theory Zhengxi Shao, Chenfeng Nie, Junyou Zhang, Bohan Xue, Qiuliang Ye, Zi Liang, Jiafei Wu, Haoyi Yuan, Qipeng Xie, Brian C.W. Kei and Zhiquan Liu

Session 11: LLM and Multi-Agent Security

ON-SITE

Room 603 · Wednesday, October 28, 2026 | 09:00–10:00 · Session Chair: Dr. Ruiran Yu

09:00–09:15	MIST: Malicious In-Distribution Stealth Attack on LLMs via Benign Interspersion Yuxiang Chen, Zekai He and Haibo Hong
09:15–09:30	When Facts Mislead: Defeating Search-Augmented Multi-Agent Debate via Factual Persuasion Enhua Zhang and Yan Chang
09:30–09:45	SSIB: A Security-Centric Benchmark and Multi-Agent Framework for Detecting Stablecoin-Specific Vulnerabilities Jiahao He, Zhenwei Liu, Zhihui Zhou, Wenxuan Luo, Hao Song, Yang Liu, Zihao Li, Ting Chen and Jiachi Chen
09:45–10:00	Composable CVE-Component Catalogs for Open-Source LLM-Driven Cyber Range Generation with Two-Tier Verification Yu-Chih Wei, Jing-Ping Yu and Chien-Hung Chen

10:00–10:25 Coffee Break & Poster Presentations

Poster area · Poster presentations during the on-site break.

Session 13: Malware Analysis, Binary Understanding and Security Evaluation

ON-SITE

Room 603 · Wednesday, October 28, 2026 | 10:25–11:10 · Session Chair: Dr. Arash Mahboubi

10:25–10:40	Seeing Through Compression: Static Detection of Packed IoT Malware Po-Lin Lai, Tao Ban, Shin-Ming Cheng, Tomohiro Morikawa and Takeshi Takahashi
10:40–10:55	Rethinking Neural Decompilation: Candidate Selection as the Hidden Bottleneck Felix Mächtle, Gautham Sriram, Manjil Neupane, Nils Loose and Thomas Eisenbarth
10:55–11:10	Unveiling the Sentinels: Assessing AI Performance in Cybersecurity Peer Review Liang Niu, Nian Xue, Cheng Yuan, Liyuan Zhao, Christina Pöpper and Zhen Li

Session 12: Security Assessment and Software Vulnerability Analysis

ON-SITE

Hall AB · Wednesday, October 28, 2026 | 10:25–11:40 · Session Chair: Dr. Pengpeng Qiao

10:25–10:40	Towards Personalized Information Security Awareness: A User-, Risk- and Context-Based Framework Enhanced by Artificial Intelligence Aaron Kutzner, David Henkelmann and Kristin Weber
10:40–10:55	Semantic Capabilities and Limitations of Detection Rule Languages: A Systematization of Knowledge Rocio Senger, Tobias Fertig and Sebastian Biedermann
10:55–11:10	LAPSE: Guided Program-Slice Representations for Project-Level Vulnerability Triage Leon Gonzalez and Yinzhi Cao
11:10–11:25	Hidden Ciphers and Where to Find Them: Static Discovery and Assessment of Cryptographic Assets in Software Christian Näther and Eduard Hirsch
11:25–11:40	Enhancing Firmware Fuzzing Efficiency for Zephyr RTOS in LEO Satellite Operating Systems via Semantic Aware Interrupt Scheduling & Symbolic Pointer Probing Bai Chuen Hsiao and Yu Chih Wei

Session 14: Decentralized Learning, Identity and Searchable Encryption

ON-SITE

Room 603 · Wednesday, October 28, 2026 | 11:15–11:54 · Session Chair: Dr. Enting Guo

11:15–11:27	A Robust and Privacy-Preserving Blockchain-based Clustering Decentralized Federated Learning Framework Kien Tran, Khoi Bui, Khoa Nguyen and Thu Le
11:27–11:39	Public Key Authenticated Encryption with Keyword Search using Secure Hardware Tatsuya Suzuki and Kazumasa Omote
11:39–11:54	Ear-Acoustic Authentication: Binaural Robustness against Playback Attacks Tongxi Chen, Yanyu Lu, Yuxuan Ma, Weizhi Meng and Wenjuan Li

12:00–18:00 Excursion

Tojinbo · Buses depart 12:00; lunch and strolling at Tojinbo on your own (lunch at your own expense), then a visit to Oshima Island; return to Fukui Station by 18:00. No paper sessions after 12:00.

NEXUS Japan-Singapore Workshop on Trustworthy Multimodal AI (Day 1)

ON-SITE

Hall AB · Wednesday, October 28, 2026 | 13:00–16:45 · Session Chair: TBA

13:00–13:05	Opening remarks · Greetings Yang Cao (Science Tokyo) Draft workshop program — subject to change
13:05–13:10	Introduction of the NEXUS program Takafumi Sasaki (JST)
13:10–13:50	Keynote (ICICS 2026 Keynote 2): AI x Cybersecurity: Navigating Challenges and Embracing Opportunities Prof. Cong Wang
13:50–14:30	Invited Talk 1 (online): Trustworthy Multimodal AI in Health: From Data Foundations to Clinical Deployment Prof. Syed Ahmad Chan Bukhari (St. John's University)
14:30–14:45	Performance of Multi-agent Framework on Multimodality Brain MRI Report Generation Ahmed Elboardy (University of Hyogo)
14:45–15:00	Cross-Planar Consistency for Trustworthy Volumetric Medical Image Segmentation Mina Yousef (University of Hyogo)
15:00–15:15	Coffee Break
15:15–15:55	Invited Talk 2 (online): AI for Cyber Offense and Defense: From Exploitation to Security Operations Naoto Yanai (Panasonic Holdings Corporation)

15:55–16:10	Expert-Aware Adversarial Self-Play for Safety Alignment of Mixture-of-Experts Language Models Ryoki Sato (Science Tokyo)
16:10–16:25	Reliable and Capable Computer-Using Agent Fuyao Zhang (NTU)
16:25–16:40	Inference-Time Intervention for Safe and Controllable AI Yiyang Duan (NTU)
16:40–16:45	Closing of Session 1 (continues Oct 29, 11:50, Hall AB) Bryan Lim

DAY 2 — Wednesday, October 28, 2026

ONLINE PROGRAM

Online Session 8: Multimodal Learning, LLM Safety and Threat Intelligence

ONLINE

Online Room · Wednesday, October 28, 2026 | 16:54–16:54

16:54–17:06	DGIML: A Decentralized Identity and Game-Theoretic Incentive Mechanism for LLM Collaboration Wusong Lan, Zuobin Ying, Jianping Cai and Jinbo Xiong
15:15–15:30	Few-Shot Stroke-Width Imitation for Offline Handwriting Rendering in Trajectory-Based Synthesis Jihan Liu, Wenping Yu, Yu Zhao, Xuan Wei, Yuhao Bai, Shanshan Tang and Haiyan Wang
15:30–15:45	EvoJudge: Confidence-Aware Rule Evolution for LLM Safety Auditing Yanqing Li, Jiangtao Wang, Qing Zhang, Gang Xu and Yueling Zhang
15:45–16:00	Patching the Ground: Representation-and-Generation Attacks on Dangerous-Object Grounding in MLLMs Jiachun Li, Jianjun Huang, Wei You and Bin Liang
16:00–16:15	LLM-ETKG: Event-Centric and Evidence-Grounded Knowledge Graph Construction for Cyber Threat Intelligence Zerun Wang, Yongxing Du, Lingfang Li, Weijian Hu, Heng Pan and Jiayu Wang
16:15–16:27	Implicit Consensus-based Steganography for Multimodal Data Hiding Qi Song, Ziyuan Luo and Renjie Wan
16:27–16:42	BinCryptID: Semantic-Structural Identification of Cryptographic Functions in Stripped Binaries Long Zhao, Jingdian Ming, Dandan Xu, Yongbin Zhou and Jian Weng
16:42–16:54	Enhancing Post-Inversion Detection of Tree-Ring Watermarks under Image Distortions Saige Sun, Ruiqiang Ma, Jerry Yongsheng Jiang, Jinyang Han, Haoran Yang and Yanan Guo

Online Session 6: Adversarial Attacks and Blockchain Security

ONLINE

Online Room · Wednesday, October 28, 2026 | 13:00–14:15

13:00–13:15	ColorFool: Three Color Elements to Fool Deepfake Detectors Jianpeng Ke, Yulin Liu, Chuyi Tian, Wenqi Wang and Aoshuang Ye
13:15–13:30	PointCBA-TGRP: Clean-Label Backdoor Trigger Generation for Point Cloud via Regular Octahedron Partitioning Mengyao Xu, Wei Li and Wuyong Tao
13:30–13:45	TIE: A Temporal Inconsistency Exploitation Threat Class for Cross-Chain Bridges Ryuto Kitajima and Kouichi Sakurai
13:45–14:00	LoCal: Localized Challenge Resolution via Off-Chain Dispute Localization and Escalating Stakes Ziyu Zhao, Qiyuan Gao, Qi Liu and Qianhong Wu
14:00–14:15	A Formal Semantics of Ownership for Multi-Chain NFT Systems Ryuto Kitajima and Kouichi Sakurai

Online Session 7: Federated Learning: Privacy and Robustness

ONLINE

Online Room · Wednesday, October 28, 2026 | 14:15–15:15

14:15–14:30	Detecting the Unseen: Privacy-Aware Federated IoT Botnet Traffic Analysis Yujin Tian, Lihua Yin, Weizhe Chen, Weida Chen, Yang Cao and Dexin Zhu
14:30–14:45	FedDualAdapt: Adaptive Dual-Stage Personalized Federated Learning with Prototype-Guided Feature Calibration for IoMT Attack Detection Xian-Xian Liu
14:45–15:00	DMM: Dynamic Moment Matching for Stealthy Fake-Gradient Defense in Vertical Federated Learning Qiheng Cheng, Shuai Shang, Xiuheng Liao, Fuwei Zhang, Pinle Qin and Hong Zhao
15:00–15:15	Adaptive Privacy-Preserving Federated Learning with Hierarchical Aggregation for Resource-Constrained Consumer Electronics Shishu Chen, Huachang Su, Yuzhou Liu, Shan Ji and Yanbin Li

Online Session 9: Secure AI Agents and LLM Systems

ONLINE

Online Room · Wednesday, October 28, 2026 | 22:42–23:27

22:42–22:57	Cat-and-Mouse Game: AI Agents for URL Merging of Magnet Link Search Websites Yaqin Fan, Songtao Ye and Jianhao Wei
22:57–23:12	Structured Decomposition for Reliable LLM-Generated Access Control Policies Vatsal Gupta and Darshan Darshan Tumkur Sreenivasamurthy
23:12–23:27	PriMedLLM: A TEE-Based Secure Mediation Framework for Privacy-Preserving LLM Training and Inference Lei Zhang, Jiachun Liao, Sunan Kan, Jiafeng Fan and Wei Dong

Online Session 10: Intrusion Detection and Threat Intelligence

ONLINE

Online Room · Wednesday, October 28, 2026 | 23:27–00:27 (+1)

23:27–23:42	FRIME-TCN: A Feature-Adaptive RIME Optimization Framework for Efficient Network Intrusion Detection Hongxin Zhao, Shiao Mi, Jinping Cao, Xin Liu, Shuai Zhang and Yiying Zhang
23:42–23:57	OP-UMKL: Ordinality-Preserving Unsupervised Multi-Kernel Learning for Provenance-Graph-based APT Detection Hong Mou, Cong Wang, Guohua Xin, Tuoyu Chen and Guangquan Xu
23:57–00:12 (+1)	GraceTI: A Graph Relation-Aware Contrastive Embedding Method for Threat Intelligence Haiyan Wang, Shanshan Tang, Wenying Feng, Huchen Zhou, Shizhu Li, Xiangyu Song and Zhaoquan Gu
00:12 (+1)–00:27 (+1)	Lightweight IoT Malware Detection via Adaptive Federated Aggregation and Transformer Distillation for Network Traffic Lihong Yan, Shuhui Zhang, Lianhai Wang, Shujiang Xu, Yanling Zhao and Xiaoming Wu

Online Session 11: Malware Detection and Credential Security

ONLINE

Online Room · Wednesday, October 28, 2026 | 00:27 (+1)–01:12 (+1)

00:27 (+1)–00:42 (+1)	RL-ChainGuard: Reinforcement Learning-based Evidence Chain Selection for Explainable Malware Detection Lei Wang, Xizheng Pan, Fenglin Bi and Fei Wu
00:42 (+1)–00:57 (+1)	An Empirical Measurement Study of Authentication Mechanisms in Cloud-Based Password Managers Yanduo Fu, Qingxuan Wang and Ding Wang
00:57 (+1)–01:12 (+1)	When Secrets Get Committed: The role of code platforms in avoiding secret leakage Ruining Yang, Billy Tsouvalas and Nick Nikiforakis

DAY 3 — Thursday, October 29, 2026

IN-PERSON PROGRAM

09:00–09:40 Keynote 3 — Prof. Kwangjo Kim: “Beyond Classical Cryptography: Neural Leakage, Post-Quantum Signatures, and the Security Frontier”
Hall AB · 40-minute keynote

Session 15: Privacy-Preserving Authentication and System Threat Analysis

ON-SITE

Hall AB · Thursday, October 29, 2026 | 09:55–10:40 · Session Chair: Dr. Hong Zhao

09:55–10:10	PrivEscope: Systematic Detection of Privilege Escalation Paths in Database Management Systems	Wai Kin Wong, Shuai Wang, Xincheng Yan and Tian Tian
10:10–10:25	Beyond Isolated Phishing Emails: Discovering Hidden Campaign Relationships with MCDA	Elyssa Boulila, Marc Dacier, Siva Prem Vengadessa Peroumal, Nicolas Veys and Simone Aonzo
10:40–10:55	FBAN: A Fully Homomorphic Encryption Compatible Bottleneck Attention Network for Privacy-Preserving Behavioral Authentication	Jichao Xiong, Atsuko Miyaji and Jiageng Chen
10:25–10:40	Security Weaknesses and Privacy Leakage in Mini-apps: An Analysis Based on Structural, Behavioral, and Indicators	Pinghai Yuan, Hao Jiang, Zhixiang Lu, Jie Sun and Fulong Chen

Session 16: Cryptographic Implementations, Cloud and Application Security

ON-SITE

Room 603 · Thursday, October 29, 2026 | 09:55–10:40 · Session Chair: Dr. Enting Guo

09:55–10:10	Efficient Constant-Time Traversal of Isogeny22Chain in SQIsign via Montgomery Arithmetic	Mohamed Bourefis and Atsuko Miyaji
10:10–10:25	Nephology: Characterizing the Security of Base Images across Cloud Providers	Narong Chaiwut and Nick Nikiforakis
10:25–10:40	HostCFI: Host-Side Control-Flow Integrity for Unmodified Guest Kernels in Cloud Environments	Pinghai Yuan, Hao Jiang, Wenjie Li, Fulong Chen and Zhenjiang Qian

10:55–11:10 Coffee Break & Poster Presentations
Poster area · Poster presentations during the on-site break.

Session 17: Cryptanalysis and Machine Learning Security

ON-SITE

Hall AB · Thursday, October 29, 2026 | 11:10–11:49 · Session Chair: Prof. Yang Cao

11:10–11:22	Revisited Distinguishers for Stream Cipher ChaCha	Yurie Okada and Atsuko Miyaji
11:22–11:34	Toward Efficient Long-Term Poisoning Defense in Federated Learning Using Conditional Variational Autoencoder	Chun-I Fan, Yan-Lin Huang and Ming-Feng Tsai
11:34–11:49	Artistic Adversarial Examples: Graffiti-Based Adversarial Attacks on Traffic Sign Recognition	Zhenghao Michele Zhuge, Go Tsuruoka, Zhihe Zhang, Stefano Longari, Lachlan Moore, Stefano Zanero and Tatsuya Mori

Session 18: Digital Signatures: Foundations and Implementation Security

ON-SITE

Room 603 · Thursday, October 29, 2026 | 11:10–11:34 · Session Chair: Prof. Kazumasa Omote

11:10–11:22	Implementation Pitfalls of Vinegar Randomness in UOV Signatures: Leakage Amplification and Verifiability Limits	Zhanlin Wang and Zhiwei Wang
11:22–11:34	Digital Signatures in the Standard Model from Linear Hash Functions	Kodai Hayashida and Atsuko Miyaji

NEXUS Japan-Singapore Workshop on Trustworthy Multimodal AI (Session 1 continued)

ON-SITE

Hall AB · Thursday, October 29, 2026 | 11:50–12:35 · Session Chair: TBA

11:50–12:05	Measuring and Mitigating Contextual Memory Leakage in Multi-agent System Hengyu Wu (Science Tokyo)
12:05–12:20	Auditing and Understanding Safety and Robustness in Multimodal LLMs Zherui Li (NTU)
12:20–12:35	Scaling Deepfake Detection: From Benchmarking to Agentic Intelligence Xinyu Yan (NTU)

12:00–18:00 Social event

Eiheiji & Ichijodani · Buses depart 12:00 (bento lunch on board); Eiheiji Temple and Ichijodani Asakura Clan Ruins; buses arrive at the banquet venue by 18:00. No paper sessions after 12:00.

NEXUS Japan-Singapore Workshop on Trustworthy Multimodal AI (Day 2)

ON-SITE

Hall AB · Thursday, October 29, 2026 | 13:00–17:00 · Session Chair: TBA

13:00–13:05	Opening Yang Cao Draft workshop program — subject to change
13:05–13:10	Greetings Prof. Tomohiro Shibata (NEXUS Program Officer)
13:10–13:25	PI Talk: Project overview and progress Yang Cao (Science Tokyo)
13:25–13:40	PI Talk: Towards AI Co-Scientists: From Knowledge Analysis to Scientific Discovery Bryan Lim (NTU)
13:40–13:55	PI Talk: Trustworthy AI in the Era of Foundation Models Prof. Chunhua Su (University of Aizu)
13:55–14:10	PI Talk: From Foundation Models to Agentic AI: Advancing Trustworthy Medical Intelligence Essam Rashed (University of Hyogo)
14:10–14:30	Research talk: Federated LoRA under Heterogeneous Ranks Pengpeng Qiao (Science Tokyo)
14:30–14:45	Are Active GIAs Really Easy to Detect? Stealthy GIAs via Linear Leakage Layer Manipulation Tomoyuki Shiroyama (Science Tokyo)
14:45–15:00	Security and Privacy in Federated Learning Zhiwei Si (University of Aizu)
15:00–15:15	Coffee Break
15:15–15:30	Federated Continual Intelligence at the Edge Xiuheng Liao (University of Aizu)
15:30–15:45	Communication-Efficient Federated Class-Incremental Intrusion Detection for Edge IoT Networks Ziang Wu (University of Aizu)
15:45–16:00	Cost-Aware Confidence-Gated Two-Stage Network Intrusion Detection under a Cross-File Cross-Class Stress Test Jiaming Zhang (University of Aizu)
16:00–16:15	Hardening Project 2026 “Agentic Collapse”: After-Action Review, What We Learned the Hard Way Timoté Moreaux (University of Aizu)
16:15–16:55	Panel Discussion: Trustworthy Multimodal AI from the Edge to Agents: Open Challenges and the Road Ahead Moderator: Yang Cao (Science Tokyo) · Panelists: Tomohiro Shibata (NEXUS Program Officer), Bryan Lim (NTU), Chunhua Su (University of Aizu), Essam Rashed (University of Hyogo)

16:55–17:00	Closing Yang Cao

18:00–20:00 Conference Banquet

Rose Garden · Rose Garden (Takagi, Fukui City). Reception from 17:30, dinner 18:00-20:00; buses return to Fukui Station around 20:30.

DAY 3 — Thursday, October 29, 2026

ONLINE PROGRAM

Online Session 14: Network Intrusion Detection I

ONLINE

Online Room · Thursday, October 29, 2026 | 16:30–16:30

16:30–16:45	Cross-ISA Heterogeneous Component Generation and Endogenous Security Enhancement via Code Segmented Compilation Dalong Zhang, Zhenjiang Liang and Yan Cao
15:30–15:45	Few-Shot Class-Incremental Learning for Encrypted Network Intrusion Detection Shangming Liu, Weihong Han and Shuyuan Jin
15:45–16:00	P4-AutoGuard: Scalable DDoS Detection and Mitigation with Aggregate Traffic Features in Programmable Data Planes Jiayu Wang, Lingfang Li, Heng Pan, Weijian Hu and Zerun Wang
16:00–16:15	S3L-IDS: Enabling Efficient Large-Scale Network Intrusion Detection via Sketch And Self-Supervised Learning Jiqiang Xia, Jianjin Zhao, Qi Zhan, Zihao Wang, Le Tian and Yuxiang Hu
16:15–16:30	T-MTAD: A Lightweight Multiscale Time-Series Framework with Causal Attention for Network Traffic Anomaly Detection Yu Gong, Min Li, Jia Sun, Hu Xiong and Kuo-Hui Yeh

Online Session 12: Software Vulnerability Detection and Fuzzing

ONLINE

Online Room · Thursday, October 29, 2026 | 13:00–14:30

13:00–13:15	Small Models, Big Variances: Unveiling the Impact of Execution Environments on SLMs' Security Zijun Li, Tengfei Tu, Yuxin Lian, Zicheng Kong, Yiling Zhou, Aofan Liu and Wenmin Li
13:15–13:30	LAVD: Cross-Project Vulnerability Detection via Layer-Fading and Logical Alignment Huiming Zhuo and Xia Li
13:30–13:45	Exploring Function-Level Vulnerability Detection with Vulnerability Intelligence-Enhanced LLMs Guangxiang Dai, Peng Wang, Duohe Ma, Qiru Pan, Yaqin Zhang and Kai Chen
13:45–14:00	Edge-Aware Heterogeneous Graph Transformer for Source Code Vulnerability Detection Qiaoguo Zhang and Fuyong Zhang
14:00–14:15	Toward Comprehensive Cryptographic API Misuse Detection: Fine-tuning Discriminative LLMs on Sliced Code Snippets Hao Wang, Jingdian Ming, Yuejun Liu, Dandan Xu, Yiwen Gao and Yongbin Zhou
14:15–14:30	DUFuzz: Define-Use Chain Guided Fuzzing for RESTful API Vulnerability Discovery Ziben Jin, Libo Chen, Qinsheng Hou and Zhi Xue

Online Session 13: Wireless, Vehicular and Traffic Security

ONLINE

Online Room · Thursday, October 29, 2026 | 14:30–15:30

14:30–14:45	Real-World Assessment of EXP3-MA-Based Random Access in Wireless IoT Networks Yu Zhao, Yuru Zhai, Wenping Yu, Juan Zhao, Haiyan Wang and Yuhao Bai
14:45–15:00	Dual-Domain Transformer with Physics-to-Security Transfer Learning for ADS-B Anomaly Detection Hongyu Yang, Qikang Feng and Ziwen Zhao
15:00–15:15	Hierarchical Website Fingerprinting: Incorporating Multi-Page Traffic Features via Cross-Attention and Evidential Fusion Fangzhe Li, Lizhi Peng and Bo Yang
15:15–15:30	MultiView-EF: Bounded Cross-View Evidence for ETSI-Compliant V2X Misbehaviour Reporting Yanping Wei, Tong Jin and Gongxuan Zhang

Online Session 15: Network Intrusion Detection II and Screening Security

ONLINE

Online Room · Thursday, October 29, 2026 | 22:00–22:45

22:00–22:15	Dual-Branch Encoding for Network Intrusion Detection Xuefei Cao, Yue Wang, Yan Xue, Jinqi Chen and Linyan Shi
22:15–22:30	SFDNet: Structure-Feature Decoupling for Robust Encrypted Malicious Traffic Detection under Network Perturbations Xueying Zhao, Shuhao Li, Tao Yin, Yu Wang, Chen Yang, Peishuai Sun and Ziyang Li
22:30–22:45	Crafted Innocence: A Stigmatization Threat Model for Watchlist Screening and Its Defenses Ruohan Gao and Haixuan Yan

DAY 4 — Friday, October 30, 2026

IN-PERSON PROGRAM

Session 19: Cloud, IoT and Cyber-Physical System Security

ON-SITE

Hall AB · Friday, October 30, 2026 | 09:00–09:45 · Session Chair: Dr. Hong Zhao

09:00–09:15	Reliability Analysis for Multi-Cloud Auditing Systems	Simmel Yan, Yongxia Sun and Gang Wang
09:15–09:30	When Side Channels Meet Covert Channels: A Practical Fully Sensor-Driven Attack Chain	Ye Wang, Yuying Li, Bo Luo and Fengjun Li
09:30–09:45	Digital Twin Degradation: Detecting Cyber–Physical Attacks via Temporal Inconsistencies	Konstantinos E Kampourakis, Vasileios Gkioulos and Sokratis Katsikas

Session 20: IoT Security: Detection, Firmware and Data Privacy

ON-SITE

Room 603 · Friday, October 30, 2026 | 09:00–09:45 · Session Chair: Prof. Chunhua Su

09:00–09:15	PowerTrace-IoT: An Empirical Power-Consumption Dataset for Physical-Layer Attack Detection in Distributed IoT Sensor Networks	Hugo Bourreau, Fabien Dagnat, Marc-Oliver Pahl, Fehmi Jaafar and Kévin Bouchard
09:15–09:30	A Privacy-Preserving Data Sharing Framework for Consumer-Centric Digital Twin in Healthcare 5.0	Lin-Fa Lee, Yi-Yu Chang, Wei-Bin Lee and Kuo-Hui Yeh
09:30–09:45	Robust Stealthy Attacks Detection in IoT Through Dynamic Masking-Based Autoencoder	Subir Halder, Amrita Ghosal, Stefano Chessa and Donna O'Shea

10:00–10:25 Coffee Break & Poster Presentations

Poster area · Poster presentations during the on-site break.

Session 21: Network Security and Privacy-Preserving Data Analysis

ON-SITE

Hall AB · Friday, October 30, 2026 | 10:25–12:19 · Session Chair: Dr. Qingkui Zeng

10:25–10:40	Benign Activity Filter: A Benign Activity Extraction Method for Efficient Provenance-based Log Analysis	Ryo Niwase, Taishin Saito, Kuniyasu Suzaki and Masaki Hashimoto
10:40–10:55	Dynamic Deep Packet Inspection for Secure Middlebox on Encrypted Traffic with Forward Privacy	Mingwu Zhang, Chenguang Liu, Yudi Zhang and Tianqing Zhu
10:55–11:10	MC2Net: Mutation-Decision-Level Credit Learning for Stateful Network Protocol Fuzzing	Zhaohui Liu, Wenchen Liao, Haocheng Yang and Shiyi Zhou
11:10–11:25	SSAFI: Sorting-Based Score Anonymization Against Feature Inference in Vertical Federated Learning	Xingpeng Ren, Hong Zhao, Shuai Shang, Xiaolin Liu, Zeyu Li and Xu Yang
11:25–11:40	Reducing Privacy Overhead in Accuracy-First Differentially Private Fine-Tuning of LLMs	Tomoyasu Okada and Yang Cao
11:40–11:55	Data Poisoning Attacks to Local Differential Privacy for Triangle Counts	Wen Xu, Zhirun Zheng, Pengpeng Qiao, Yang Cao, Mianxiong Dong and Kaoru Ota
11:55–12:07	Cost-Aware Confidence-Gated Two-Stage Network Intrusion Detection under a Cross-File Cross-Class Stress Test	Jiaming Zhang, Huishan Lai, Runtong He, Jingxue Chen and Chunhua Su
12:07–12:19	Dual-View Semantic-Structural Learning for IoT device Firmware Vulnerability Detection	Hao Liu, Liquan Chen, Suhui Liu and Gerhard Hancke

Session 22: Privacy Protection and Side-Channel Countermeasures

ON-SITE

Room 603 · Friday, October 30, 2026 | 10:25–11:55 · Session Chair: Dr. Xiuheng Liao

10:25–10:40	Privacy Preserving Multidimensional Medical Data Collection With Efficient Fixed Length Encoding Juhao Wang, Fei Zhou and Jingcheng Song
11:55–12:10	Visibility Does Not Equal Effective Privacy Notice: Rethinking LED Notice on AI Glasses Tongxi Chen, Yanyu Lu, Shengqi Qiu and Weizhi Meng
10:40–10:55	Leakage-Free Dissemination of Authenticated Graph-Structured Data Shuang Chen, Aoshuang Ye, Fei Zhu, Jinhua Ma and Xu Yang
10:55–11:10	PIPE-SCD: Pipeline-Aware Side-Channel Disassembly of Multi-Instruction Power Traces Xinghao Wang, Pei Cao, Chi Zhang, Dawu Gu and Juncheng Ji
11:10–11:25	HLS/RTL Hybrid Design for Power Side-channel Secure Cipher Circuits Mingyu Yang, Jingyu Zheng and Yuko Hara
11:25–11:40	Acoustic Side-Channel Attack on Smartphone via Cross-Sensor Fusion Diba Afroze, Amirhossein Jamarani, Yazhou Tu and Xiali Hei
11:40–11:55	Toward Secure Compilation: Leakage Detection for Masked Implementations in Jasmin Nicolai Schmitt, Sven Wroblewski, Fabio Campos and Andreas Heinemann

12:20–13:00 Lunch
Hall AB

Session 23: Secure Computation and Collaborative Security

ON-SITE

Hall AB · Friday, October 30, 2026 | 13:00–13:48 · Session Chair: Prof. Chi Wan Sung

13:00–13:12	CANCEL: Collaborative and Adaptive Intrusion Detection in Autonomous Connected Vehicles Tannishtha Devgun, Gulshan Kumar and Mauro Conti
13:12–13:24	Efficient Private Set Intersection and Searchable Encryption using Homomorphic Bloom Filters Anil Kumar Pradhan, Killari Nandini, Harsh Kasyap and Sayantan Mukherjee
13:24–13:36	A Lean Formalization of Perfect Secret Sharing and Secure Distributed Matrix Multiplication Kenneth Shum and Chi Wan Sung
13:36–13:48	Fast MPC Framework under Shamir’s Secret Sharing with Malicious Security and Two-Thirds Honest Majority Hanchao Ku, Hikaru Tsuchida, Mingwu Zhang and Takashi Nishide

Session 24: Encryption, Signatures and Anonymous Protocols

ON-SITE

Room 603 · Friday, October 30, 2026 | 13:00–13:48 · Session Chair: Dr. Zhuotao Lian

13:00–13:12	HiFile-ABE: An Efficient Hierarchical File Encryption Scheme for Cloud Computing Haiyan Wang, Yuan Li, Shanshan Tang, Bo Qu, Cui Luo and Zhaoquan Gu
13:12–13:24	On Publicly Verifiable Tokens in Group Signatures with Message-Dependent Opening Takuma Watanabe and Keita Emura
13:24–13:36	DASTE: Decentralized Ad-Hoc Access-Structured Threshold Encryption with Dynamic Policy Evolution Anil Kumar Pradhan and Abhraneel Dutta
13:36–13:48	What Anonymous Public Announcements Can Do Thomas Ågotnes, Rustam Galimullin and Ken Satoh

13:48–14:08 Coffee Break & Poster Presentations
Poster area · Poster presentations during the on-site break.

Session 25: Zero-Knowledge Proofs and Adversarial Machine Learning

ON-SITE

Hall AB · Friday, October 30, 2026 | 14:08–14:56 · Session Chair: Dr. Harsh Kasyap

14:08–14:20	Card-Based Zero-Knowledge Proofs for Necklace Splitting Problem	Shota Ikeda and Kazumasa Shinagawa
14:20–14:32	Targeted Semantic Subspace Perturbation Against Model Inversion Attacks	Peiyao Yuan, Laiwen Yan, Qizhi Zhang, Yiru Zhao and Lei Zhao
14:32–14:44	CVAE-ECA: A Stealthy Backdoor Attack against Speech Classification via Emotion Conversion	Yueming Huang, Wenhan Yao, Weiping Wen and Xiarun Chen
14:44–14:56	Toward Robust Fingerprint Recognition: An Anchor-Guided Pre-emptive Protection Method Based on Forced Breeding Evolution	Yu-An Chen, Yen-Chia Kuo, Hsin-Hung Cho, Chi-Yuan Chen, Jiang-Yi Zeng, Fan-Hsun Tseng and Yeon Lee

Session 26: Authentication, Firmware and AI-Assisted Security

ON-SITE

Room 603 · Friday, October 30, 2026 | 14:08–14:56 · Session Chair: Dr. Gulshan Kumar

14:08–14:20	VeinoCert: Binding an Object to an Owner	Serge Vaudenay
14:32–14:44	SimulAPT: LLM-Driven Reconstruction and Simulation of APT Campaigns	Yeali Sun, Weihsiang Shih and Meng Chang Chen
14:44–14:56	VERDE: Semantic-Aware Weight Adaptation via Large Language Models for Green AI Orchestration	Yi Wu, Ruiran Yu, Yiyang Ye, Xianlong Hu and Yuanyi Jiang

Session 27: Malware Detection and Secure Distributed Networks

ON-SITE

Hall AB · Friday, October 30, 2026 | 15:08–15:44 · Session Chair: Dr. Hong Zhao

15:08–15:20	URAD:Unsupervised Ransomware Anomaly Detection Using LSTM-VAE and Bahdanau Attention	Arash Mahboubi, Keyvan Ansari and Seyit Camtepe
15:20–15:32	Loom: A Balanced String-Based Transformer for Android Malware Detection	Hantang Zhang, Mojtaba Eshghie, Bruno Kreyssig, Tommy Löfstedt and Alexandre Bartel
15:32–15:44	SPARTA – Soft-Proximal Adaptive Robust Trustworthy Aggregator for Decentralized Federated Learning under Label Skew and Byzantine Threats	Lam Tran, Hai Lam Duong, Tuan Kiet Phan and Thao Nguyen-Thi-Ai

Session 28: Networked Systems and Cryptographic API Security

ON-SITE

Room 603 · Friday, October 30, 2026 | 15:08–15:44 · Session Chair: Prof. Mauro Conti

15:08–15:20	A Security Analysis and Lightweight Hybrid IDS for the CubeSat Space Protocol over CAN	Giulia Cornetta, Daniele Mammone, Davide Avanzi, Mariagrazia Bibiano, Stefano Zanero, Michele Carminati and Stefano Longari
15:20–15:32	Synchronized Process-Network Datasets for Wireless Attacks in SDN-Enabled Industrial Control Systems	Muhammed Adekunle Azeez and Stefan Katzenbeisser
15:32–15:44	Fusing Code Semantics and Dynamic Execution Traces: A Multi-Modal Framework for Detecting Cryptographic API Misuse	Wentao Zhou, Shijie Jia, Yingjiao Niu and Daren Zha

15:50–16:20 Awards and closing ceremony

Hall AB

DAY 4 — Friday, October 30, 2026

ONLINE PROGRAM

Online Session 22: Encrypted Traffic Analysis and Intrusion Detection

ONLINE

Online Room · Friday, October 30, 2026 | 17:42–17:42

17:42–17:54	FSPANN: Forward-Secure and Privacy-Preserving ANN Search with Routing-Ciphertext Orthogonality Mehran Mehran, Yanguo Peng, Cong Cao and Zhen Lv
16:54–17:06	Beyond Isotropic Aggregation: Residual Graph Attention for Provenance-based Threat Detection Xinyu Xu, Yongzhong Huang and Guige Ouyang
17:06–17:18	Cross-Domain Encrypted Traffic Attack Detection with Feature Alignment under Few-Shot Settings Yuehan Zhang, Lyucheng Qian, Xibei Zou, Xingyi Li, Yunzhuo Wang, Yuchen Wu, Jingyu Hu and Haizhou Wang
17:18–17:30	Cross-domain Direction-aware Encrypted Traffic Analysis Based on Local Deviation Yixiang Lu
17:30–17:42	An Empirical Study of Cross-Domain Generalization in Network Intrusion Detection Shanshan Tang, Haiyan Wang, Rui Zong, Fucai Luo, Bo Qu and Zhaoquan Gu

Online Session 16: Privacy, Side-Channel Analysis and Trusted Systems

ONLINE

Online Room · Friday, October 30, 2026 | 10:00–11:30 · Session Chair: Dr. Zhe Yang

10:00–10:15	ConsistencyGuard: A Post-hoc Defense Against Poisoning in Frequent Itemset Mining under Local Differential Privacy Lele Yu, Yuxing Wei, Xuan Lei, Yuanjun Xia and Yining Liu
10:15–10:30	Liquid Neural Network in Far-Field EM Side-Channel Attack Zirun Wang, Caijian Luo, Huanyu Wang and Junnian Wang
10:30–10:45	CPNN: A Power Side-Channel Information-Assisted Modeling Attack Method on Arbiter-Based PUFs Hui Liu and Jiqiang Lu
10:45–11:00	Rank-Based Distribution Reshaping for Robust EM/Power Fusion in Side-Channel Analysis across Sampling Rates Linfeng Wang, Jiacheng Song, Xiaoran Huang, Wei Cheng, Jingdian Ming and Yongbin Zhou
11:00–11:15	RouterWhisper: Acoustic Side-Channel Inference of Smartphone Activities via Wi-Fi Router Power Adapters Yuwen Feng, Junchen Meng, Yuejia Hong, Yuxuan Yang, Xiaoli Zhang, Huaiyu Zhu and Zhe Yang
11:15–11:30	Building the Truman Show: A TrustZone-Based Framework for Lightweight Out-of-band Kernel Security Monitoring Zhenling Duan, Pan Dong, Renshuang Jiang, Xiaoxiang Fang and Bao Li

Online Session 17: Decentralized Systems, Cryptanalysis and Federated Privacy

ONLINE

Online Room · Friday, October 30, 2026 | 11:30–12:30

11:30–11:42	dcChecker: Efffcient Deterministic and Continuous Checking for Critical Data Integrity in Decentralized Storage Huyi Chen, Caimei Zuo, Bo Meng, Dejun Wang and Jianhao Zhu
11:42–11:54	An Anti-Collusion Incentive Mechanism Based on Reverse Auction for Crowdsensing Services Hai Liu, Yadong Peng and Nana Zhou
11:54–12:06	Impossible Differential Cryptanalysis of the SPARX-128 Block Cipher Xiao Zhang and Jiqiang Lu
12:06–12:18	DP-RADAR: Byzantine-Robust Federated Learning with Adaptive Privacy Budgeting Xingyu Chen
12:18–12:30	VIB-Distill: Label Privacy Protection in Vertical Federated Learning via Variational Bottleneck Compression and Knowledge Distillation Yang Tan

Online Session 18: Private Set Operations, Oblivious Data Structures and FHE

ONLINE

Online Room · Friday, October 30, 2026 | 12:30–13:30

12:30–12:42	Fast UpPSI: Block-Local Synchronization for Candidate Generation in Dynamic PSI Jiaqi Chen, Ou Ruan, Panpan Guo and Yiwei Li
12:42–12:54	Beyond Static Retrieval: A Dynamic Double Oblivious Map via B+ Tree for Secure Enclaves Tianhuo Bao, Jialin Chi, Min Zhang, Axin Wu, Chenyang Wang and Dengguo Feng
12:54–13:06	Forward-Private Updatable Private Set Intersection via Epoch-Based CryptoTree Evolution Yang Shi, Lei Shi, Chengming Liu, Mengyang He and Huijuan Lian
13:06–13:18	DO-EHash: Double Oblivious Extendible Hashing for Secure Keyword Search Using Trusted Execution Environments Chenyang Wang, Tianhuo Bao, Guizhou Liang, Jialin Chi, Min Zhang and Dengguo Feng
13:18–13:30	Client-Aided Hybrid FHE for BERT Attention: A CKKS-to-TFHE Transcoding Approach Asuman Dumlu and Bayram Ali Ersoy

Online Session 19: Signatures, Zero-Knowledge Proofs and Secure AI Applications

ONLINE

Online Room · Friday, October 30, 2026 | 13:30–14:42

13:30–13:42	PS-SM9: A Proxy Multi-Signature Scheme with Selective Local Verification based on SM9 Xiaotong Ma and Limin Ma
13:42–13:54	Card-Based Zero-Knowledge Proof for Yajisan-Kazusan and Yajilin Rikuto Noda, Chuzo Iwamoto and Kouichi Sakurai
13:54–14:06	BLM-PFP: A Trustworthy Biomedical Knowledge-Guided Multimodal Fusion Model for Security-Sensitive Protein Function Prediction Yuyin Ma, Yue Hu, Chaolin Song, Yijun Lu, Zheng Lin, Pengpeng Qiao and Jiale Shu
14:06–14:18	Expose-then-Use: Multi-Label Medical Model Extraction via Victim-Induced Label Structure Chuyang Ma, Yali Liu and Jianting Ning
14:18–14:30	Learning Human-Computable Passwords: What Makes Them Hard (or Easy) for Neural Models? Shohei Ogawa, Yuto Ikeda and Kouichi Sakurai
14:30–14:42	Quantum Origami Access Control: Authorization as Structural Compatibility in Quantum Systems Gabriela Mogos and Ho-Pun Lam

Online Session 20: IoT Protection and LLM-Assisted Security

ONLINE

Online Room · Friday, October 30, 2026 | 14:42–15:54 · Session Chair: Prof. Li Wang

14:42–14:54	CANederlo: A Lightweight Safety-Aware Anomaly Detection System for CAN Vehicle Networks Umberto Bellini, Davide Compar and Bruno Crispo
14:54–15:06	TIEE Role Inversion for Sensitive Data Protection in Smart Home Hubs Krishnava Ghosh, Samyak Khare and Anubhav Goyal
15:06–15:18	TraceShield: Boundary-Aware Semantic Auditing and Risk-Graph Analysis for Secure LLM Agent Tool Chains Shiheng Guo, Mingyi Liu, Xueyang Wang, Ruiqing Huang, Xuan Kan and Zhiyang Fang
15:18–15:30	NANOZK: Privacy-Preserving Verifiable Inference for Large Language Models via Layerwise Zero-Knowledge Proofs Zhaohui Wang
15:30–15:42	VulnPilot: A Multi-Agent LLM Framework for Automated Penetration Testing Xi Zhang and Bailin Xie
15:42–15:54	CIPHERNOVA: A Test Feedback-Driven and Hierarchical LLM-Prompt-Based Approach for Cryptographic Code Generation Jiayi He and Xiao Lan

Online Session 21: AI-Assisted Threat Detection and Malware Analysis

ONLINE

Online Room · Friday, October 30, 2026 | 15:54–16:54

15:54–16:06	Agent-based HTTP Alert Judgment System: Integrating Reinforcement Learning and Multi-Agent Collaboration Yicheng Pan, Xu Zhou and Kejiang Ye
16:06–16:18	BinSpeed: Efficient Semantic Binary Similarity Analysis with N-Gram Basic-Block Sequences Li Wang, Lin Deng and Weifeng Xu
16:18–16:30	KAN-Det: Generalizable Hybrid Malware Detection with Kolmogorov-Arnold Networks Rama Satya Chittala and Raghu Kishore N
16:30–16:42	CLEAR: Cross-path Large-kernel Embedding and Adaptive Refinement Kefei Wu, Siyu Xiong, Shichao Gao, Ziyi Jiang, Lin Li and Qingyan Li
16:42–16:54	Beyond Semantic Drift: High-Fidelity Byte-Level Malware Attribution via Structure-Aware MIL Wenzhou Zhao, Bocheng Zhang, Yuhang Chen and Lei Zhang

Online Session 23: Vulnerability Assessment, Fuzzing and Application Security

ONLINE

Online Room · Friday, October 30, 2026 | 17:54–18:54

17:54–18:06	Quantifying Network-Visible Exposure and Vulnerability-Risk Reduction Through Reconnaissance-Driven Hardening in a Controlled Virtual Testbed Mohammed F. Suleiman and Ajoze Abdulraheem Zubair
18:06–18:18	SFGFuzz: Field-Sensitivity-Guided Fuzzing for Vulnerability-Candidate Mining in Modbus TCP Jianpo Li, Yinqi Wang, Wei Wang, Li Cong and Yuehua Yang
18:18–18:30	Automated Protocol Fuzzing: Are We There Yet? Jiemin Wan, Le Yu, Zhijin Chen and Guozi Sun
18:30–18:42	DiffScope: Auditing Functionality-Level Data Over-Collection in Mobile Apps via Cross-Platform Differential Analysis Jiangrong Wu, Yuming Xiao, Mengyi Long and Yuhong Nan
18:42–18:54	When Packages Lie: Mitigating Package Hallucinations with a Sufficient Context RAG Framework Duhyeon Baek and Jiwon Yoon

Online Poster Session

ONLINE

Online Room · Friday, October 30, 2026 | 19:00–19:30

19:00–19:10	LABA: A Query-Efficient Black-Box Textual Attack via Adaptive N-ary Search and LLM-Guided Substitution Mingsheng Cao, Lihong Wang, Jun Wang, Jiuzhou Chen, Yin Zhang, Yulin Huang, Yi Ding and Qing Ma 7-minute oral presentation + 3-minute Q&A; (poster presented online)
19:10–19:20	Privacy-Preserving and Verifiable Dynamic Billing for Edge--Cloud Collaboration Jianfeng Zhao and Liu Lixin 7-minute oral presentation + 3-minute Q&A; (poster presented online)
19:20–19:30	Operationalizing Stateful Hash-Based Signatures for VPN Authentication Daniel Herzinger, Linus Heise, Christian Näther and Daniel Loebenberger 7-minute oral presentation + 3-minute Q&A; (poster presented online)

POSTER GALLERY

Poster presentations take place during the morning and afternoon coffee breaks shown in the daily program. Posters presented online appear in the Online Poster Session (Fri, Oct 30, from 19:00).

Poster title	Authors
Threshold Blind Identity-Based Encryption with Certified Identities	Wei-Cheng Pan, Ting-Yu Wang and Zi-Yuan Liu
Exploring Connectionless MQTT to Achieve End-to-End Security and High Performance	Hung-Yu Chien
Security Analysis on a Secure Medical Data Sharing System in Digital Twin Environments	Mizuki Hayashi and Keita Emura
Blind Revocable Identity-Based Encryption with Certified Identities	Jia-Sin Yang, Cheng-Wei Liao and Zi-Yuan Liu
Why Do Vulnerability Scanners Disagree? Statistical Evidence and Scenario-Based Selection Guidance for Nessus and Rapid7	Chewei Li
Defending LLMs Against Non-Natural Language Obfuscated Attacks	Huynh Phuong Thanh Nguyen and Razvan Beuran
A Cuckoo-Filter-Based Local Differential Privacy Scheme for Multi-Task F-MCS	Wang Xiaodi, Yunwei Dong Yunwei, Wei Yuxing Wei and Liu Yining Liu
Operationalizing Stateful Hash-Based Signatures for VPN Authentication	Daniel Herzinger, Linus Heise, Christian Näther and Daniel Loebenberger
From Leakage Detection to Leakage-Aware Compilation of Masked Implementations in Jasmin	Nicolai Schmitt and Sven Wroblewski
Privacy-Preserving and Verifiable Dynamic Billing for Edge--Cloud Collaboration	Jianfeng Zhao and Liu Lixin
When Differential Privacy Reshapes Robust Aggregation: Signal Degradation and Adaptive Aggregation for Federated Intrusion Detection	Xitong Wang, Yining Liu and Wei Yuxing
Multi-Key Homomorphic Encryption-Based TTP-Free Privacy-Preserving Federated Learning Framework	Fumiya Inoue and Yuntao Wang
LABA: A Query-Efficient Black-Box Textual Attack via Adaptive N-ary Search and LLM-Guided Substitution	Mingsheng Cao, Lihong Wang, Jun Wang, Jiuzhou Chen, Yin Zhang, Yulin Huang, Yi Ding and Qing Ma
AutoWebExplorer: A Code-Orchestrated LLM Agent for Web Attack Surface Exploration	Hong Zhao, Kaixin Han, Zhijian Liang and Pinle Qin
Towards an IoIV Classification Framework for Post-Quantum Cryptographic Implementation Vulnerabilities	Vincent Tan, Amal Raj, Jonathan Pan and Vivek Balachandran
Poisoning Attacks to Local Differential Privacy Protocols for Dynamic Graphs	Shang Liu, Yuhan Bao and Guan Yuan
Multi-Objective Fine-Tuning for Secure Code Generation: A Comparative Study of LoRA and Prefix-Tuning Methods	Wakato Maeda, Nikolay Matyunin and Ali Raza