Day 1 (Wednesday, October 29, 2025)			
09:00-09:15	**Opening Remark**		
09:15-10:15	**Keynote 1: 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 2: Access Control**	**Session 3: Traffic Classification**
	EquinoxBFT: BFT Consensus for Blockchain Emergency Governance *Jialiang Fan, Qianhong Wu, Minghang Li, Decun Luo, Qin Wang and Bo Qin* **fFuzz: A State-aware Function-level Fuzzing Framework for Smart Contract Vulnerabilities Detection** *Chang Li, Binqin Lu, Wenyang Zhang, Kaixuan Yang and Huijuan Zhu* **TraceBFT: Backtracking-based Pipelined Asynchronous BFT Consensus for High-Throughput Distributed Systems** *Haofeng Zhuang, Haifeng Qian, Junqing Gong and Zhili Chen*	**Circulation Control Model and Administration for Geospatial Data** *Heng Li, Fenghua Li, Yunchuan Guo, Lingcui Zhang, Xiao Wang and Ziyan Zhou* **Identifying Unusual Personal Data in Mobile Apps for Better Privacy Compliance Check** *Jiatao Cheng, Yuhong Nan, Xueqiang Wang, Zhefan Chen and Yuliang Zhang* **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*	**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* **SPTC: Signature-based Cross-protocol Encrypted Proxy Traffic Classification Approach** *Huajie Jia, Yige Chen and Zhengzhou Tang* **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*

	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* **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*	**DBG-LB: A Trustworthy and Efficient Framework for Data Sharing in the Internet of Vehicles** *Chaoyue Li, Yongming Zhang and Xiaolong Xu* **TetheGAN: A GAN-Based Synthetic Mobile Tethering Traffic Generating Framework** *Xuman Zhang, Guang Cheng and Li Deng*	**FlowGraphNet: Efficient Malicious Traffic Detection via Graph Construction** *Changsong Yang, Han Wang, Yueling Liu, Yong Ding, Hai Liang and Zhenyu Li* **RustGuard: Detecting Rust Data Leak Issues with Context-Sensitive Static Taint Analysis** *Shanlin Deng, Mingliang Liu, Si Wu and Baojian Hua*
12:25-14:00	**Lunch**		
14:00-15:40	**Session 4: Crypto 1**	**Session 5: Anonymity and Privacy 1**	**Session 6: Security and Privacy of AI 1**
	Multi-Signer Locally Verifiable Aggregate Signature from (Leveled) Multilinear Maps *Yuchen Yang, Jie Chen, Qiaohan Chu, Qiuyan Du and Luping Wang* **Conditional Attribute-based Encryption with Keyword Search for Pay-Per-Query Commercial Model** *Zerui Guo, Sha Ma and Qiong Huang*	**MagWatch: Exposing Privacy Risks in Smartwatches through Electromagnetic Signals** *Haowen Xu, Tianya Zhao, Xuyu Wang, Jun Dai and Xiaoyan Sun* **Privacy-preserving, Secure and Certificate-based Integrity Auditing for Cloud Storage** *Wenhao Wang, Yu Li, Yinxia Sun, Yuan Zhang and Sheng Zhong*	**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* **AFedGAN: Adaptive Federated Learning with Generative Adversarial Networks for Non-IID Data** *Xuyang Zhang, Hua Jin and Peiyuan Guo*

	Lightweight Transparent Zero-Knowledge Proofs for Cross-Domain Statements *Zhengzhou Tu, Min Xie, Junbin Fang, Yong Yu and Zoe L. Jiang* **Public Verifiable Server-Aided Revocable Attribute-Based Encryption** *Luqi Huang, Fuchun Guo, Willy Susilo and Yumei Li* **New First-Order Secure AES Implementation without Online Fresh Randomness Records** *Botao Liu and Ming Tang*	**Unbalanced Private Computation on Set Intersection with Reduced Computation and Communication** *Zelin Tang, Hua Guo, Yewei Guan and Kaijie Yang* **Artemis: Decentralized, Secure, and Efficient Safety Monitoring with Dynamic Trajectories** *Meng Li, Zhuangwei Li, Yifei Chen, Yan Qiao and Mauro Conti* **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*	**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* **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* **CascadeGen: A Hybrid GAN-Diffusion Framework for Controllable and Protocol-Compliant Synthetic Network Traffic Generation** *Qingyuan Yu, Chuping Yan and Xiaoying Liu*
15:40-16:10	**Coffee Break**		
16:10-17:50	**Session 7: Crypto 2**	**Session 8: Anonymity and Privacy 2**	**Session 9: Security and Privacy of AI 2**
	SM2-VBKE: Achieving Cryptographic Binding Between Verification Integrity and Key Generatio *Runze Zhao, Siqi Lu, Yongjuan Wang, Liujia Cai, Wenyi Chen and Fenghua Jiang*	**AnoST: An Anonymous Optimistic Verification System Based on Off-Chain State Transition** *Qiyuan Gao, Qianhong Wu, Junxiang Nong and Qi Liu*	**Efficient Semi-asynchronous Federated Learning with Guided Selective Participation and Adaptive Aggregation** *Chaoyun Wang, Kedong Yan and Chanying Huang*

	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* **Zero-Knowledge Protocols with PVC Security: Striking the Balance between Security and Efficiency** *Yi Liu, Yipeng Song, Anjia Yang and Junzuo Lai* **Attribute-Based Adaptor Signature and Application in Control-based Atomic Swap** *Tianyuan Fan, Gang Shen, Yuzhu Wang, Yuntao Wang and Mingwu Zhang* **A Versatile Decentralized Attribute Based Signature Scheme for IoT** *Dazhi Xu, Yuejun Liu, Jiabei Wang, Yiwen Gao and Yongbin Zhou*	**Privacy-Preserving K-hop Shortest Path Query on Encrypted Graphs Based on Graph Pruning** *Ya Gao, Chao Mu, Ming Yang and Xiaoming Wu* **TA-PDC: Provable Data Contribution with Traceable Anonymous for Group Transactions** *Xiaocong Lin, Weijing You, Chenchen Wu, Wenmao Liu and Qi Gu* **Fine-filter: An Effective Defense against Poisoning Attacks on Frequency Estimation under LDP** *Yuxia Zhou, Qiao Xue and Youwen Zhu* **BioVite: Efficient and Compact Privacy-Preserving Biometric Verification via Fully Homomorphic Encryption**. *Pengfei Zeng, Han Xia and Mingsheng Wang*	**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* **Hierarchical Recovery of Convolutional Neural Networks via Self-Embedding Watermarking** *Yawen Huang and Huaicong Zhan* **Personalized Federated Learning Algorithm Based on User Grouping and Group Signature** *Hao Lin, Xiaoming Hu, Shuangjie Bai and Yan Liu* **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*
18:00-20:00	**Dinner**		

Day 2 (Tuesday, October, 30, 2025)			
9:00-10:00	**Keynote 2: Cyber Ranges and Cyber-Physical Ranges: Progress, Potential, and Future Directions** *Sokratis Katsikas (Norwegian University of Science and Technology, Norway)*		
10:00-10:30	**Coffee Break**		
10:30-12:10	**Session 10: Machine Learning for Security**	**Session 11 : System and Network Security**	**Session 12: Vulnerability Analysis**
	SPCD: A Shot-Based Partial Copy Detection Method *Yuhan Tao and Danwei Chen* **Bayesian-Adaptive Graph Neural Network for Anomaly Detection (BAGNN).** *Yong Ding, Chi Zhang, Shijie Tang, Changsong Yang and Hai Liang* **UzPhishNet Model for Phishing Detection** *Bektemir Saydiev, Xiaohui Cui and Umer Zukaib*	**Batch-oriented Element-wise Approximate Activation for Privacy Preserving Neural Networks** *Peng Zhang, Ao Duan, Xianglu Zou and Dongyan Qiu* **Social-Aware and Quality-Driven Incentives for Mobile Crowd-Sensing with Two-Stage Game** *Jun Tao and Hao Zou* **A Distributed Privacy Protection Method for Crowd Sensing Based on Trust Evaluation** *Hai Liu, Maoze Tian, Yadong Peng and Hongye Peng*	**Towards Efficient C/C++ Vulnerability Impact Assessment in Package Management Systems** *Zibo Wang, Xiangkun Jia, Jia Yan, Yi Yang, Huafeng Huang and Purui Su* **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* **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*

	CyberNER-LLM: Cyber Threat Intelligence Named Entity Recognition With Large Language Model *Xinzheng Liu, Wangqun Lin and Zhaoyun Ding* **Provenance-Based Intrusion Detection via Multi-Scale Graph Representation Learning** *Xuebo Qiu, Mingqi Lv, Tieming Chen, Tiantian Zhu and Qijie Song*	**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* **Bridging the Interoperability Gaps Among Trusted Architectures in MCUs** *Sandro Pinto, Lu´ıs Cunha, Daniel Oliveira, Michele Grisafi, Emanuele Beozzo and Bruno Crispo*	**KVT-Payload: Knowledge Graph-Enhanced Hierarchical Vulnerability Traffic Payload Generation** *Faqi Zhao, Rong Shi, Guoqiao Zhou, Wen Wang and Feng Liu* **Construction and Application of Vulnerability Intelligence Ontology under Vulnerability Management Perspective** *Guangxiang Dai, Peng Wang and Duohe Ma*
12:10-14:00	**Lunch**		
14:00-17:30	**Steering Committee Meeting & Social Event**		
18:00-20:00	**Banquet & Award Ceremony**		

Day 3 (Friday, October 31, 2025)			
9:00-10:00	**Keynote 3 Post-Quantum Group-Oriented Anonymous Signatures from Symmetric Primitives** *Liqun Chen (University of Surrey, UK)*		
10:00-10:30	**Coffee Break**		
10:30-12:10	**Session 13: Blockchain and Cryptocurrencies 2**	**Session 14: Post-Quantum Crypto**	**Session 15: Attack and Defense 1**
	Enhancing Private Signing Key Protection in Digital Currency Transactions Using Obfuscation *Yang Shi, Jintao Xie, Minyu Teng, Guanxu Liu, Linhai Guo and Jiangfeng Li* **AnsBridge: Towards Secure Cross-Chain Interoperability via Anonymous and Verifiable Validators** *Mingming Huang, Xiaodan Zhang, Wei Mi, Huimei Liao and Yi Sun* **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*	**Compact Adaptively Secure Identity-Based Encryption from Middle-Product Learning with Errors** *Jingjing Fan, Xingye Lu, Man Ho Au and Siu Ming Yiu* **Turtle Wins Rabbit Again: Faster Modulus Reduction for RNS-CKKS** *Lianglin Yan, Pengfei Zeng and Mingsheng Wang* **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*	**Domain Adaptation for Cross-Device Profiled ML Side-Channel Attacks** *Ian Garrett and Ryan Gerdes* **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* **Full-phase Distributed Quantum Impossible Differential Cryptanalysis** *Kun Zhang, Tao Shang, Yuanjing Zhang and Jianwei Liu* **ProverNG: Efficient Verification of Compositional Masking for Cryptosystem's Side-Channel Security**

	R1-MFSol: a Smart Contract Vulnerability Detection Model Based on LLM and Multi-modal Feature Fusion *Huibo Yang, Zhize Hao and Tao Liu* **No Place to Hide: An Efficient and Accurate Backdoor Detection Tool for Ethereum ERC-20 Smart Contracts** *Shouchen Zhou, Lu Zhou and Yu Tao*	**PolarKyber: Polished Kyber with Smaller Ciphertexts, Greater Security Redundancy, and Lower Decryption Failure Rate** *Chen An, Ziyao Liu, Xianhui Lu and Jingnan He* **Lion: A New Ring Signature Construction from Lattice Gadget** *Yanting Li, Pingbin Luo, Xinjian Chen and Qiong Huang*	*Yiming Yang, Feng Zhou, Yuanyuan Wang, Hua Chen, Limin Fan and An Wang* **SADGA: A Self Attention GAN-Based Adversarial DGA with High Anti-Detection Ability** *Jiang Luo, Shaohua Qin and Zhe Wang*
12:10-14:00	**Lunch**		
14:00-16:00	**Session 16: Crypto, Steganography and Watermarking**	**Session 17: Anomaly Detection**	**Session 18: Attack and Defense 2**
	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* **MDKG: Module-lattice-based Distributed Key Generation** *Ye Bai, Debiao He, Zhichao Yang, Min Luo and Cong Peng*	**Speaker Inference Detection Using Only Text** *Ruoxi Cheng, Yizhong Ding, Shaowei Yuan and Zhiqiang Wang* **DTGAN: Diverse-Task Generative Adversarial Networks for Intrusion Detection Systems Against Adversarial Examples** *Yiyang Wang, Wuxia Bai and Kai Chen*	**POWERPOLY: Multilingual Program Analysis with the Aid of Web Assembly** *Zhuochen Jiang and Baojian Hua* **Not only spatial, but also spectral: Unnoticeable backdoor attack on 3D point clouds** *Yongzhen Jiang, Haoran Li, Hongjia Liu, Jiageng Pan and Jian Xu*

	Towards High-Capacity Provably Secure Steganography via Cascade Sampling *Meiyang Lv, Haocheng Fu, Xiaowei Yi, Hongxian Huang, Yun Cao and Changjun Liu* **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* **Robust Reversible Watermarking for 3D Models Based on Auto Diffusion Function** *Zixing Lin, Yaolong Song and Rui Li*	**ConComFND: Leveraging Content and Comment Information for Enhanced Fake News Detection** *Huan Zhang, Chanying Huang, Kedong Yan and Shan Xiao* **Transferable Adversarial Attacks in Object Detection: Leveraging Ensemble Features and Gradient Variance Minimization** *Zhitong Lu, Zhen Xu, Qian Yang and Kai Chen* **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*	**Permutation-Based Cryptanalysis of the SCARF Block Cipher and Its Randomness Evaluation** *Qi Li, Wenying Zhang and Xiaomeng Sun* **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* **Security Vulnerabilities in AI-Generated Code: A Large-Scale Analysis of Public GitHub Repositories** *Maximilian Schreiber and Pascal Tippe* **FluxSketch: A Sketch-based Solution for Long-Term Fluctuating Key Flow Detection** *Jun Xu, Guoju Gao, Yu-E Sun, He Huang and Yang Du*
16:00-16:30	**Coffee Break**		
16:30-17:00	**Closing Session**		
18:00-20:00	**Dinner**		