HANDBOOK

THE 20th ACM ASIA CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY

Hanoi, Vietnam | 25-29 August 2025

ACM ASIACCS 2025

HANOI CITY

TIME ZONE: UTC/GMT +7

TELEPHONE COUNTRY CODE:

The Vietnam phone code is +84 and the area code for Hanoi is 24.

CLIMATE:

The average daytime temperature ranges from 26°C to 33°C (78.8°F to 91.4°F). Please note that sudden rain showers may occur in Hanoi.

EMERGENCIES:

Police: 113

Fire: 114

Ambulance – First Aid: 115

CURRENCY AND BANKING FACILITIES:

Vietnamese currency is Vietnamese Dong (VND). There are nine denominations of bills, ranging from VND 1,000 to VND 500,000.

Approximate exchange rate: 1US$»26,000VND and 1EUR»30,200VND. You can sometimes pay by US dollars or Euros in Vietnam (but it is not recommended). The widely accepted credit cards in Vietnam are Visa, MasterCard and American Express.

Foreign currency can be exchanged into VND at the airport or at any bank in the city. However, in general, under our regulations, you can hardly exchange from VND back to foreign currency, even at banks. Thus, please only exchange an amount enough for the duration of your stay.

For a small fee, obtaining cash with credit or debit cards is very easy from ATM cash machines, which are widely available at banks, hotels or on the street. Please be sure to follow the usual safety precautions and plan your withdrawals in advance.

ELECTRICITY:

The voltage and frequency are 220V, 50Hz. Plug types: A, C, F.

CROSSING THE STREETS:

Never run, go backward, or make any sudden movements. Walk slowly, and stop if you feel unsafe.

TAXIS

Taxi fares range from 12,000 to 18,000 VND per km (depending on car quality). Most taxis are safe, but on rare occasions you could get a fake taxi or a bad driver who might ask you to overpay. We recommend the following taxi brands:

* Mai Linh Taxi: (84 - 24) 38 333 333
* G7 Taxi: (84 - 24) 32 323 232
* Thanh Nga Taxi: (84 - 4) 38 215 215

GRAB AND XANH SM

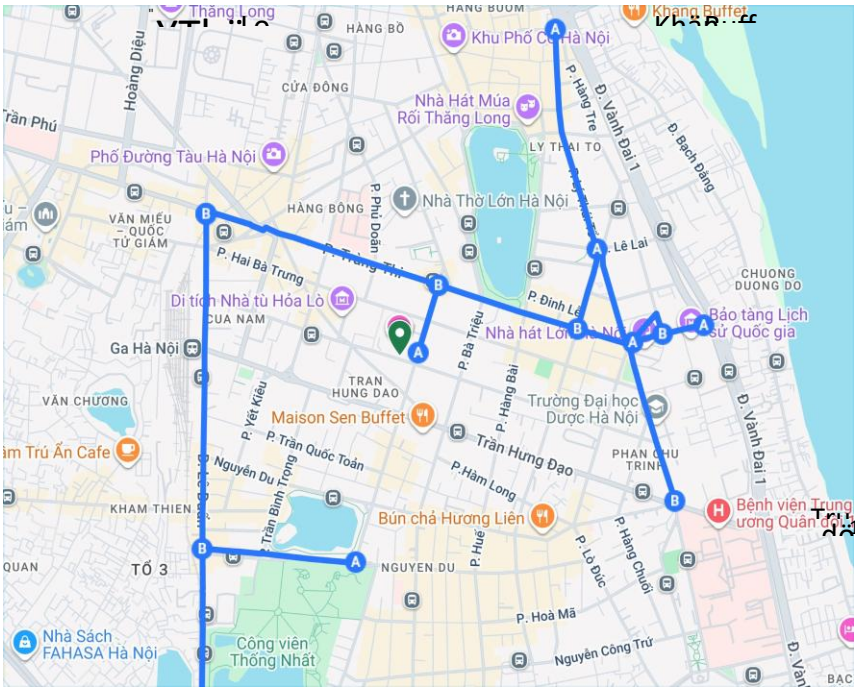
GRAB is available in Hanoi and most major cities across Vietnam. In Hanoi, one of the most popular choices is **XANH SM** - Vietnam's first all-electric taxi service.

PARADE REHEARSALS: TRAFFIC NOTICE

Vietnam will celebrate the 80th anniversary of its National Day on September 2, 2025. In preparation, military parade rehearsals will take place in Hanoi, requiring temporary road closures during the following times:

* **August 24, 5:00 PM – August 25, 3:00 AM**
* **August 27, 5:00 PM – August 28, 3:00 AM**
* **August 29, 6:00 PM – August 30, 3:00 PM**

During these times, vehicles will not be permitted on designated roads. However, buses and pedestrians will still have access, ensuring continued mobility**. Please note that these restrictions will NOT affect the conference**. Our team is dedicated to providing a smooth and enjoyable experience for all attendees.



Road Closure Map: 800-Meter Radius Around Meliá Hanoi.

In addition to being a time of celebration, this period offers a unique cultural experience. Guests may wish to observe parts of the parade rehearsals. If you are in Hanoi on September 2, you will also have the opportunity to witness the official parade and enjoy the spectacular National Day fireworks.

We appreciate your understanding and cooperation, and we look forward to welcoming you to Hanoi for a memorable and enriching conference experience.

AIRPORT TRANSFER

Noi Bai International Airport (HAN) is about 30 km north of the city center. Traveling from HAN to the city center is easy because there are plenty of transportation options.

Vietnam Airlines Shuttle Bus is a 16-seat minibus that departs according to Vietnam Airlines' flight schedule. However, departures from Noi Bai International Airport (HAN) to the city typically occur only when the bus is full, which may result in extended waiting times.

Vietjet Air Shuttle Bus schedule corresponds to the schedule of Vietjet Air flights arriving to and departing from HAN. If the bus passes your destination along the route, you can notify the bus driver to stop anywhere.

A taxi service is provided for all flights of the day, including weekends and holidays. Taxis at HAN are easy to find. They wait for passengers in front of the domestic and international arrivals halls. Taxi fares are calculated according to the meter for the departure from HAN to the city center and should be around 350,000 to 450,000 VND. The trip from Hanoi to the airport is often discounted by 30% compared to the charge calculated according to the meter.

There are 12 concessionaire taxi firms at HAN. Here are some popular taxi companies: **AIRPORT TAXI, NOIBAI TAXI, TAXI GROUP, TAXI MAI LINH, G7 TAXI** and **XANH SM AIRPORT TAXI**. Of these, **XANH SM AIRPORT TAXI** is the first electric taxi service in Vietnam, and you can book a trip via the **XANH SM** app, available on App Store and Google Play.

CONFERENCE INFORMATION

CONFERENCE VENUE

The conference will take place in Meliá Hanoi (Address: 44B Ly Thuong Kiet Street, Hanoi). Meliá Hanoi is a luxurious five-star hotel located in the heart of Hanoi, Vietnam, just minutes from the Old Quarter and major cultural landmarks.

REGISTRATION DESK OPENING TIME

Monday, 25 August 2025: 13:00 – 17:30
Tuesday, 26 August 2025: 7:45 – 17:30
Wednesday, 27 August 2025: 8:00 – 17:00

CONFERENCE OPENING

The opening ceremony starts at 9:00 and the first keynote speech commences at 9:30 on Wednesday, 27 August 2025 at the Grand Ballroom.

FUNCTION ROOMS

Level 1	Ballroom 1
	Ballroom 2
	Ballroom 3
	Function Room 1 + 2
Level 2	Function Room 3
	Function Room 6 + 7

REFRESHMENTS

Tea breaks are arranged in the foyer outside the meeting rooms. Buffet lunch is served at Mosaico Restaurant on the ground floor and Cham Restaurant on Level 1.

NAME BADGES

All participants will receive a name badge, which must be worn at all times while inside the conference venue.

SATCHELS

All participants will receive a conference satchel. Your satchel includes a souvenir from the organizers.

INTERNET ACCESS

Free Wi-Fi is available at the conference venue. The Wi-Fi network does not require any password.

INSTRUCTIONS FOR PRESENTING AUTHORS

All conference rooms are equipped with a projector, projector screen, speakers, and microphones. Supported display connector types include VGA and HDMI. USB Type-C to HDMI and VGA converters are also available at the conference venue.

Presentations at the Main Conference are allocated 12 minutes, followed by 3 minutes for Q&A. Presenters may use their own laptops or upload their presentation slides to the scheduled room computer well in advance of their session.

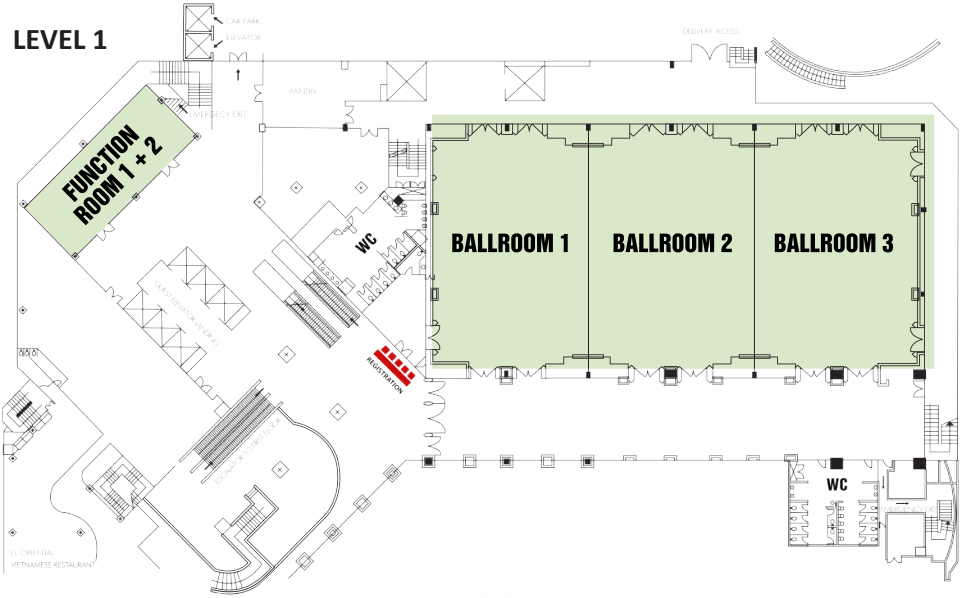
USEFUL CONTACT NUMBERS

Assoc. Prof. Tran Quang Duc (Local Organizing Co-Chair)
(+84) 916 192 156 (Mobile/WhatsApp)
Email: asiaccs25-contact@soict.hust.edu.vn

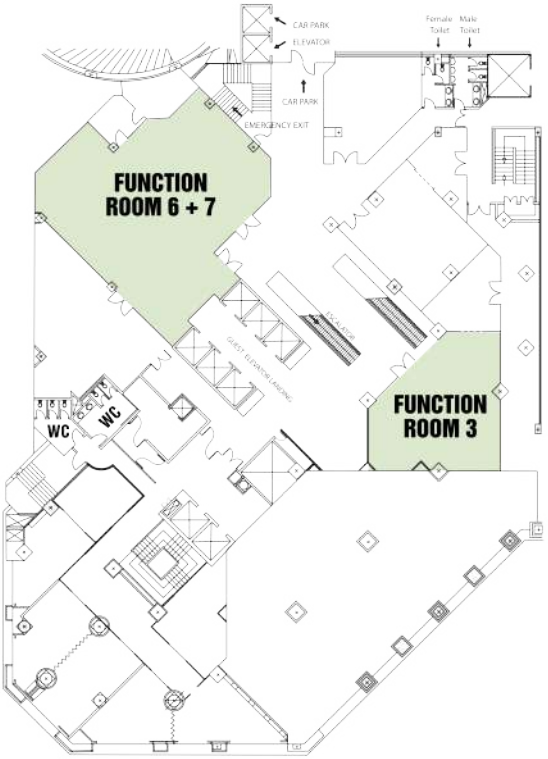
Ms. Vicky (Secretary)
(+84) 913 631 936 (Mobile/WhatsApp)
Email: vicky@hoabinhtourist.com

CONFERENCE LAYOUT

LEVEL 1



LEVEL 2



SOCIAL FUNCTIONS

TOUR OF THE TEMPLE OF LITERATURE

Address: 58 Quoc Tu Giam, Dong Da, Ha Noi

Date & Time: 25 August 2025, 14:00 – 16:00 (ICT)

Bus pickup time at hotel: 14:00 (ICT)

Ticket: Entrance tickets will be provided upon registration.

WELCOME RECEPTION

Venue: Nang Song Hong

Address: 306A Phu Vien, Bo De, Long Bien, Hanoi, Vietnam

Date & Time: 26 August 2025, 18:00 – 21:00 (ICT)

Bus pickup time at hotel: 18:00 (ICT)

Bus pickup time at Nang Song Hong (return): 21:00 (ICT)

Ticket: Entrance tickets will be provided upon registration.

SOCIAL EVENT

Venue: Bat Trang Pottery Museum

Address: Center of Vietnamese Craft Village Quintessence, Bat Trang Pottery Village, Gia Lam District, Hanoi, Vietnam

Date & Time: 28 August 2025, 14:00 – 17:30 (ICT)

Bus pickup time at hotel: 14:00 (ICT)

Ticket: Entrance tickets will be provided upon registration.

CONFERENCE BANQUET

The Gala Dinner commences at **19:00 (ICT)** on Thursday, 28 August 2025 in the Grand Ballroom.

Parallel activities at the dinner: 20th anniversary celebration of ACM AsiaCCS, award ceremony, Test-of-time award presentation, and announcement of ACM AsiaCCS 2026

ASIACCS MEETUP

Venue: Function Room 3, Level 2, Meliá Hanoi

Date & Time: 26 August 2025, 14:00 – 17:30 (ICT)

SPONSOR EVENT

All interested researchers and academics attending ACM ASIACCS 2025 are warmly invited to an interaction session with the Infocomm Technology Cluster (Department) leadership team of the Singapore Institute of Technology (SIT) to discover the potential collaboration and career opportunities.

Venue: Function Room 4, Level 2, Meliá Hanoi

Date & Time: 27 & 28 August 2025, 9:00 – 17:00 (ICT)

PROGRAM AT A GLANCE

DAY 1 (MONDAY, 25 AUGUST 2025)						
13:00-17:30	Registration					
14:00-16:00	**Temple of Literature Tour**, capped at 135 persons					
DAY 2 (TUESDAY, 26 AUGUST 2025)						
	Ballroom 1	**Ballroom 2**	**Function Room 6+7**	**Function Room 1+2**	**Ballroom 3**	**Function Room 3**
07:45-17:30	Registration					
08:30-10:20	Workshop **CPSS**	Workshop **BSCI**	Workshop **WDC**	Workshop **FL-AsiaCCS'25**	Workshop **APKC**	Workshop **SCID**
10:20-10:40	Tea Break					
10:40-12:30	Workshop **CPSS**	Workshop **BSCI**	Workshop **WDC**	Workshop **FL-AsiaCCS'25**	Workshop **APKC**	Workshop **SCID**
12:30-14:00	Lunch					
14:00-15:40	Workshop **CPSS**	Workshop **BSCI**	Workshop **WDC**	Workshop **LM-SHIELD**	Workshop **SecTL**	AsiaCCS Meetup
15:40-16:00	Tea Break					
16:00-17:30	Workshop **CPSS**	Workshop **BSCI**	Workshop **WDC**	Workshop **LM-SHIELD**	Workshop **SecTL**	AsiaCCS Meetup
18:00-21:00	**Welcome Reception** (**Nang Song Hong**)					

DAY 3 (WEDNESDAY, 27 AUGUST 2025)			
	Ballroom 1	**Ballroom 2**	**Ballroom 3**
08:00-17:00	Registration		
09:00-09:30	**Opening Remark**		
09:30-10:30	**Keynote 1: Wenyuan Xu (Zhejiang University)** The Double-Edged Sword of Facial and Voice Recognition: Analyzing Risks and Solutions		
10:30-11:00	Tea Break		
11:00-12:30	Session 1: **Homomorphic Encryption and Zero knowledge**	Session 2: **LLM for Security**	Session 3: **Hardware Security**
12:30-14:00	Lunch		
14:00-17:00	**Poster Session**		
14:00-15:30	Session 4: **Multi-party Computation**	Session 5: **ML Security**	Session 6: **Fault Injection and Side Channels**
15:30-16:00	Tea Break		
16:00-17:00	Session 7: **Applied Crypto**	Session 8: **IoT Security**	Session 9: **Blockchain 1**
17:30-20:30	**Steering Committee Meeting**		

DAY 4 (THURSDAY, 28 AUGUST 2025)			
	Ballroom 1	**Ballroom 2**	**Ballroom 3**
09:00-10:30	Session 10: **Post-Quantum**	Session 11: **ML Applications to Security**	Session 12: **Privacy 1**
10:30-11:00	Tea Break		
11:00-12:00	**Keynote 2: Yier Jin (Huawei)** virtCCA and CoDA: An Industrial Practice in Advancing AI Confidential Computing on ARM Platforms		
12:00-14:00	Lunch		
14:00-17:30	**Social Event (Bat Trang Pottery Museum)**		
19:00-22:00	**Conference Dinner, Award Ceremony, Test-of-time Award Presentation, and Announcement of AsiaCCS 2026 (Conference Hotel)**		
DAY 5 (FRIDAY, 29 AUGUST 2025)			
	Ballroom 1	**Ballroom 2**	**Ballroom 3**
09:00-10:00	**Keynote 3: Moti Yung (Google/Columbia University)** Malicious Cryptography: Repurposing Cryptographic Mechanisms for Unintended Tasks		
10:00-10:30	Tea Break		
10:30-12:00	Session 13: **Privacy 2**	Session 14: **Software and OS Security**	Session 15: **Web Security**
12:00-13:30	Lunch		
13:30-15:00	Session 16: **Usable Security and Privacy**	Session 17: **Binary Security**	Session 18: **Network Security**
15:00-15:30	Tea Break		
15:30-16:30	Session 19: **CPS Security**	Session 20: **Blockchain 2**	Session 21: **Blockchain 3**
16:30-17:00	**Closing Remark**		

FULL PROGRAM (MAIN CONFERENCE)

DAY 3 (WEDNESDAY, 27 AUGUST 2025)

	Ballroom 1	Ballroom 2	Ballroom 3
08:00-17:00	Registration		
09:00-09:30	**Opening Remark**		
09:30-10:30	**Keynote 1: Wenyuan Xu (Zhejiang University)** The Double-Edged Sword of Facial and Voice Recognition: Analyzing Risks and Solutions		
10:30-11:00	Tea Break		
11:00-12:30	Session 1: **Homomorphic Encryption and Zero knowledge** *Session Chair: Jacob Imola*	Session 2: **LLM for Security** *Session Chair: Thi-Thu-Huong Le*	Session 3: **Hardware Security** *Session Chair: Patrick Schaumont*
	Optimized Composite Polynomials in CKKS Bootstrapping *Seonhong Min, Joon-Woo Lee, Yongsoo Song* **An Efficient Circuit Synthesis Framework for TFHE via Convex Sub-graph Optimization** *Animesh Singh, Ayantika Chatterjee, Anupam Chattopadhyay, Debdeep Mukhopadhyay*	**Perses: Unlocking Privilege Escalation for Small LLMs via Extensible Heterogeneity** *Dominik M. Weber, Ioannis Tzachristas, Aifen Sui* **Generalized Adversarial Code-Suggestions: Exploiting Contexts of LLM-based Code-Completion** *Karl Rubel, Maximilian Noppel, Christian Wressnegger*	**N-Tracer: A Trace Driven Attack on NoC-Based MPSoC Architecture** *Dipesh, Urbi Chatterjee* **FP-Rowhammer: DRAM-Based Device Fingerprinting** *Hari Venugopalan, Kaustav Goswami, Zainul Din, Jason Lowe-Power, Samuel T. King, Zubair Shafiq* **ProbeShooter: A New Practical Approach for Probe Aiming** *Daehyeon Bae, Sujin Park, Minsig Choi, Young-Giu Jeong, Changmin Jeong, Heeseok Kim, Seokhie Hong*

	A Novel Asymmetric BSGS Polynomial Evaluation Algorithm under Homomorphic Encryption *Qingfeng Wang, Li-Ping Wang* **Efficient Updatable Private Information Retrieval From Simulatable Homomorphic Ciphertexts** *Haibo Tian, Yini Lin* **Key Extension: Multi-Key FHE Utilizing LWR** *Mansi Goyal, Aditi Kar Gangopadhyay* **DUPLEX: Scalable Zero-Knowledge Lookup Arguments over RSA Group** *Semin Han, Geonho Yoon, Hyunok Oh, Jihye Kim*	**Comprehensive Evaluation of Cloaking Backdoor Attacks on Object Detector in Real-World** *Hua Ma, Alsharif Abuadbba, Yansong Gao, Hyoungshick Kim, Surya Nepal* **SAFE: A Novel Approach For Software Vulnerability Detection from Enhancing The Capability of Large Language Models** *Van Nguyen, Surya Nepal, Xingliang Yuan, Tingmin Wu, Carsten Rudolph* **Sounds Vishy: Automating Vishing Attacks with AI-Powered Systems** *João Figueiredo, Afonso Carvalho, Daniel Castro, Daniel Gonçalves, Nuno Santos* **SoK: The Privacy Paradox of Large Language Models: Advancements, Privacy Risks, and Mitigation** *Yashothara Shanmugarasa, Ming Ding, Chamikara Mahawaga Arachchige, Thierry Rakotoarivelo*	**GAE4HT: Detecting Hardware Trojans with Graph Autoencoder-Trained on Golden Model Data Flow Graphs** *Daehyeon Lee, Junghee Lee* **Monocle: Transient Execution Proof Memory Views for Runtime Compiled Code** *Matteo Oldani, William Blair, Shweta Shinde, Matthias Neugschwandtner* **Okapi: Efficiently Safeguarding Speculative Data Accesses in Sandboxed Environments** *Philipp Schmitz, Tobias Jauch, Alex Wezel, Mohammad Rahmani Fadiheh, Thore Tiemann, Jonah Heller, Thomas Eisenbarth, Dominik Stoffel, Wolfgang Kunz*
12:30-14:00	Lunch		
14:00-17:00	**Poster Session**		

POSTER:Stealthy SWAP-Based Side-Channel Attack on Multi-Tenant Quantum Cloud Systems
Wei Jie Bryan Lee, Siyi Wang, Suman Dutta, Walid El Maouaki, Anupam Chattopadhyay

POSTER:TYPOSQUATTING ATTACKS ON THE RUST ECOSYSTEM
Thanh-Cong Nguyen, Minh-Khanh Vu, Duc-Ly Vu

POSTER:Dissappearing Ink: How Partial Model Extraction Erases Watermarks
Venkata Sai Pranav Bachina, Ankit Gangwal

POSTER:Transparent Temporally-Specialized System Call Filters
Matthew Rossi, Michele Beretta, Dario Facchinetti, Stefano Paraboschi

POSTER:Policy-driven security-aware scheduling in Kubernetes
Matthew Rossi, Michele Beretta, Dario Facchinetti, Stefano Paraboschi

POSTER:An Empirical Study of Smart Contract Patching Practices in the Wild
Taeyoung Kim, Gilhee Lee, Hyoungshick Kim

POSTER:Automating ICS Malware Analysis with MITRE ATT&CK
Fatih Kurt, Neetesh Saxena, Vijay Kumar, George Theodorakopoulos

POSTER:When Models Speak Too Much: Privacy Leakage on Large Language Models
MingJun Zhang, Mahrokh Abdollahi, Thilina Ranbaduge, Ming Ding

POSTER:Investigating Transferability of Adversarial Examples in Model Merging
Ankit Gangwal, Aaryan Ajay Sharma

POSTER:Multimodal Graph Networks for Systematic Generalization in Code Clone Detection
Cuong Dao, Van Tong, Hai Anh Tran, Duc Tran, Giang Nguyen

POSTER:SuriCap – A Measurement Platform to Study and Evaluate Intrusion Detection Rule Engineering
Koen Teuwen, Emmanuele Zambon, Luca Allodi

14:00-15:30	Session 4: **Multi-party Computation** *Session Chair: Aydin Abadi*	Session 5: **ML Security** *Session Chair: Balázs Pejó*	Session 6: **Fault Injection and Side Channels** *Session Chair: Miroslaw Kutylowski*
	Pay What You Spend! Privacy-Aware Real-Time Pricing with High Precision IEEE 754 Floating Point Division *Soumyadyuti Ghosh, Boyapally Harishma, Ajith Suresh, Arpita Patra, Soumyajit Dey, Debdeep Mukhopadhyay* **Efficient Private Set Intersection by Utilizing Oblivious Transfer Extension** *Mingli Wu, Tsz Hon Yuen, Siu-Ming Yiu* **SEEC: Memory Safety Meets Efficiency in Secure Two-Party Computation** *Henri Dohmen, Robin William Hundt, Nora Khayata, Thomas Schneider* **Fair Server-Aided Multiparty Private Set Intersection from OKVS and OPRF** *Fei Xiao, Chunyang Lv, Jianfeng Wang* **Concretely Efficient Private Set Union via Circuit-Based PSI** *Gowri R Chandran, Thomas Schneider, Maximilian Stillger, Christian Weinert*	**ChainMarks: Securing DNN Watermark with Cryptographic Chain** *Brian Choi, Shu Wang, Isabelle Choi, Kun Sun* **Toward Malicious Clients Detection in Federated Learning** *Zhihao Dou, Jiaqi Wang, Wei Sun, Zhuqing Liu, Minghong Fang* **Nosy Layers, Noisy Fixes: Tackling DRAs in Federated Learning Systems using Explainable AI** *Meghali Nandi, Arash Shaghaghi, Nazatul Haque Sultan, Gustavo Batista, Raymond K. Zhao, Sanjay Jha* **When Better Features Mean Greater Risks: The Performance-Privacy Trade-Off in Contrastive Learning** *Ruining Sun, Hongsheng Hu, Wei Luo, Zhaoxi Zhang, Yanjun Zhang, Haizhuan Yuan, Leo Yu Zhang*	**FAULT+PROBE: A Generic Rowhammer-based Bit Recovery Attack** *Kemal Derya, M. Caner Tol, Berk Sunar* **Three Glitches to Rule One Car: Fault Injection Attacks on a Connected EV** *Niclas Kühnapfel, Christian Werling, Hans Niklas Jacob, Jean-Pierre Seifert* **AVXProbe: Enhancing Website Fingerprinting with Side-Channel-Assisted Kernel-Level Traces** *Suryeon Kim, Seung Ho Na, Jaehan Kim, Seungwon Shin, Hyunwoo Choi* **BranchGauge: Modeling and Quantifying Side-Channel Leakage in Randomization-Based Secure Branch Predictors** *Quancheng Wang, Ming Tang, Ke Xu, Han Wang* **Telescope: Top-Down Hierarchical Pre-silicon Side-channel Leakage Assessment in System-on-Chip Design** *Zhenyuan Liu, Andrew Malnicof, Arna Roy, Patrick Schaumont*

	Prior-Based Label Differential Privacy via Secure Two-Party Computation *Amit Agarwal, Stanislav Peceny, Mariana Raykova, Phillipp Schoppmann, Karn Seth*	**Unraveling Elevated Data Leakage in Split Learning for Fine-Tuning Stable Diffusion Models** *Fei Wang, Yan Zhu, Baochun Li* **Transferable Adversarial Examples with Bayesian Approach** *Mingyuan Fan, Cen Chen, Wenmeng Zhou, Yinggui Wang*	**EXAM: Exploiting Exclusive System-Level Cache in Apple M-Series SoCs for Enhanced Cache Occupancy Attacks** *Tianhong Xu, Aidong Adam Ding, Yunsi Fei*
15:30-16:00		Tea Break	
16:00-17:00	Session 7: **Applied Crypto** *Session Chair: Aditi Gangopadhyay*	Session 8: **IoT Security** *Session Chair: Denis Donadel*	Session 9: **Blockchain 1** *Session Chair: Ngoc Khanh Nguyen*
	A Cryptographic Analysis of Google's PSP and Falcon Channel Protocols *Marc Fischlin, Sascha Hoffmann, Leonhard Ruppel, Gözde Saçıak, Tobias Schnitzler, Christian Schwarz, Maximilian Stillger* **Rejection Sampling for Covert Information Channel: Symmetric Power-Of-2-Choices** *Dominik Bojko, Jacek Cichoń, Mirosław Kutyłowski, Oliwer Sobolewski* **LogaLookup: Efficient Multivariate Lookup Argument for Accelerated Proof Generation** *Dien H. A. Tran, Tam N. B. Nguyen, Nhien-An Le-Khac, Thuc D. Nguyen*	**NoBU: An effective and viable cyber-physical solution to thwart BadUSB attacks** *Andrea Ciccotelli, Maurantonio Caprolu, Roberto Di Pietro* **Your Control Host Intrusion Left Some Physical Breadcrumbs: Physical Evidence-Guided Post-Mortem Triage of SCADA Attacks** *Moses Ike, Keaton Sadoski, Romuald Valme, Burak Sahin, Saman Zonouz, Wenke Lee*	**Fast SNARK-based Non-Interactive Distributed Verifiable Random Function with Ethereum Compatibility** *Jia Liu, Mark Manulis* **VeRange: Verification-efficient Zero-knowledge Range Arguments with Transparent Setup for Blockchain Applications and More** *Yue Zhou, Sid Chi-Kin Chau* **Scalable Time-Lock Puzzle** *Aydin Abadi, Dan Ristea, Artem Grigor, Steven Murdoch*

	Post-Compromise Security with Application-Level Key-Controls – with a comprehensive study of the 5G AKMA protocol *Ioana Boureanu, Cristina Onete, Stephan Wesemeyer, Léo Robert, Rhys Miller, Pascal Lafourcade, Fortunat Rajaona*	**Bits and Pieces: Piecing Together Factors of IoT Vulnerability Exploitation** *Arwa Abdulkarim Al Alsadi, Mathew Vermeer, Takayuki Sasaki, Katsunari Yoshioka, Michel Van Eeten, Carlos Gañán* **AuthentiSafe: Lightweight and Future-Proof Device-to-Device Authentication for IoT** *Lukas Petzi, Torsten Krauß, Alexandra Dmitrienko, Gene Tsudik*	**BIP32-Compatible Threshold Wallets** *Poulami Das, Andreas Erwig, Sebastian Faust, Philipp-Florens Lehwalder, Julian Loss, Ziyan Qu, Siavash Riahi*
17:30-20:30	**Steering Committee Meeting**		
DAY 4 (THURSDAY, 28 AUGUST 2025)			
	Ballroom 1	**Ballroom 2**	**Ballroom 3**
09:00-10:30	Session 10: **Post-Quantum** *Session Chair: William Blair*	Session 11: **ML Applications to Security** *Session Chair: Van Nguyen*	Session 12: **Privacy 1** *Session Chair: Nazatul Sultan*
	An Optimized Instantiation of Post-Quantum MQTT protocol on 8-bit AVR Sensor Nodes *YoungBeom Kim, Seog Chung Seo* **Quantum-safe Signatureless DNSSEC** *Aditya Singh Rawat, Mahabir Prasad Jhanwar*	**Glitch in Time: Exploiting Temporal Misalignment of IMU For Eavesdropping** *Ahmed Najeeb, Abdul Rafay, Muhammad Hamad Alizai, Naveed Anwar Bhatti*	**Enhancing Search Privacy on Tor: Advanced Deep Keyword Fingerprinting Attacks and BurstGuard Defense** *Haeseung Jeon, Chaiwon Hwang, Jiwoo Hong, Hosung Kang, Nate Mathews, Goun Kim, Se Eun Oh*

Ring-LWR based Commitments and ZK-PoKs with Application to Verifiable Quantum-Safe Searchable Symmetric Encryption
Debadrita Talapatra, Nimish Mishra, DebdeepMukhopadhyay

Practical Deniable Post-Quantum X3DH: A Lightweight Split-KEM for K-Waay
Guilhem Niot

A Quantum-Secure Framework for IoD: Strengthening Authentication and Key-Establishment
Salman Shamshad, SANA BELGUITH, ALMA ORACEVIC

poqeth: Efficient, post-quantum signature verification on Ethereum
Ruslan Kysil, István András Seres, Péter Kutas, Nándor Kelecsényi

Eradicating the Unseen: Detecting, Exploiting, and Remediating a Path Traversal Vulnerability across GitHub
Jafar Akhoundali, Hamidreza Hamidi, Kristian Rietveld, Olga Gadyatskaya

PITCH: AI-assisted Tagging of Deepfake Audio Calls using Challenge-Response
Govind Mittal, Arthur Jakobsson, Kelly Marshall, Chinmay Hegde, Nasir Memon

Minerva: A File-Based Ransomware Detector
Dorjan Hitaj, Giulio Pagnotta, Fabio De Gaspari, Lorenzo De Carli, Luigi Mancini

Evaluating Robustness of Reference-based Phishing Detectors
Eunjin Roh, Sungwoo Jeon, Sooel Son, Sanghyun Hong

PentestAgent: Incorporating LLM Agents to Automated Penetration Testing
Xiangmin Shen, Lingzhi Wang, Zhenyuan Li, Yan Chen, Wencheng Zhao, Dawei Sun, Jiashui Wang, Wei Ruan

Robust Locally Differentially Private Graph Analysis
Amrita Roy Chowdhury, Jacob Imola, Kamalika Chaudhuri

PSP: A Privacy-Preserving Self-certify Pseudonym Protocol for V2X
Xuyuan Cai, SONG Rui, Bin Xie, Qingjun Xiao, Bin Xiao

Unveiling Privacy Risks in Quantum Optimization Services
Mateusz Leśniak, Michał Wroński, Ewa Syta, Mirosław Kutyłowski

QUIC-Exfiltration: Exploiting QUIC's Server Preferred Address Feature to Perform Data Exfiltration Attacks
Thomas Grübl, Weijie Niu, Jan von der Assen, Burkhard Stiller

ClearMask: Noise-Free and Naturalness-Preserving Protection Against Voice Deepfake Attacks
Yuanda Wang, Bocheng Chen, Hanqing Guo, Guangjing Wang, Weikang Ding, Qiben Yan

10:30-11:00	Tea Break		
11:00-12:00	**Keynote 2: Yier Jin (Huawei)** virtCCA and CoDA: An Industrial Practice in Advancing AI Confidential Computing on ARM Platforms		
12:00-14:00	Lunch		
14:00-17:30	**Social Event (Bat Trang Pottery Museum)**		
19:00-22:00	**Conference Dinner, Award Ceremony, Test-of-time Award Presentation, and Announcement of AsiaCCS 2026 (Conference Hotel)**		
DAY 5 (FRIDAY, 29 AUGUST 2025)			
	Ballroom 1	**Ballroom 2**	**Ballroom 3**
09:00-10:00	**Keynote 3: Moti Yung (Google/Columbia University)** Malicious Cryptography: Repurposing Cryptographic Mechanisms for Unintended Tasks		
10:00-10:30	Tea Break		
10:30-12:00	Session 13: **Privacy 2** *Session Chair: Ioana Boureanu*	Session 14: **Software and OS Security** *Session Chair: Lorenzo De Carli*	Session 15: **Web Security** *Session Chair: Giovanni Apruzzese*
	Slice it up: Unmasking User Identities in Smartwatch Health Data *Lucas Lange, Tobias Schreieder, Victor Christen, Erhard Rahm* **Secure Steganography Based on Chaos-Aided Quantization Index Modulation** *Xinquan Xu, Ling Liu, Shanxiang Lyu, Lip Yee Por*	**Can You Run My Code? A Close Look at Process Injection in Windows Malware** *Giorgia Di Pietro, Daniele Cono D'Elia, Leonardo Querzoni* **CryptoGuard: Lightweight Hybrid Detection and Response to Host-based Cryptojackers in Linux Cloud Environments** *Gyeonghoon Park, Jaehan Kim, Jinu Choi, Jinwoo Kim*	**Open Access Alert: Studying the Privacy Risks in Android WebView's Web Permission Enforcement** *Trung Tin Nguyen, Ben Stock* **TrustyMon: Practical Detection of DOM-based Cross-Site Scripting Attacks Using Trusted Types** *Sunnyeo Park, Jihwan Kim, Seongho Keum, Hyunjoon Lee, Sooel Son*

	App-solutely Modded: Surveying Modded App Market Operators and Original App Developers *Luis A. Saavedra, Hridoy S. Dutta, Alastair Beresford, Alice Hutchings* **Proxies as Sensors: Measuring Censorship of Refraction Networking in Iran** *Abdulrahman Alaraj, Eric Wustrow* **Virtual End-to-End Encryption: Analysis of the Doctolib Protocol** *Dennis Dayanikli, Laura Holz, Anja Lehmann* **Towards Usability of Data with Privacy: A Unified Framework for Privacy-Preserving Data Sharing with High Utility** *M.A.P. Chamikara, Seung Ick Jang, Ian Oppermann, Dongxi Liu, Musotto Roberto, Sushmita Ruj, Arindam Pal, Meisam Mohammady, Seyit Camtepe, Sylvia Young, Chris Dorrian, Nasir David*	**Vulnerable Intel GPU Context: Prohibit Complete Context Restore by Modifying Kernel Driver** *Wonseok Choi, Youngjoo Shin* **Starmie: Breaking Intel SGX Enclaves with Malicious Exceptions & Signals** *Supraja Sridhara, Andrin Bertschi, Benedict Schlüter, Shweta Shinde* **SoK: A Literature and Engineering Review of Regular Expression Denial of Service (ReDoS)** *Masudul Hasan Masud Bhuiyan, Berk Çakar, Ethan H Burmane, James C Davis, Cristian-Alexandru Staicu* **Systematic Analysis of Kernel Security Performance and Energy Costs** *Fabian Rauscher, Daniel Gruss, Benedict Herzog, Timo Hönig*	**ProwseBox: A Framework for the Analysis of the Web at Scale** *Dolière Francis Somé* **BISON: Blind Identification with Stateless scOped pseudoNyms** *Jakob Heher, Stefan More, Lena Heimberger* **Protocols and Formal Models for Delegated Authorisation with Server-Side Secrecy** *Jean Snyman, Chris Culnane, Ioana Boureanu, Gerault David* **OblivCDN: A Practical Privacy-preserving CDN with Oblivious Content Access** *Viet Vo, Shangqi Lai, Xingliang Yuan, Surya Nepal, Qi Li*
12:00-13:30	Lunch		

13:30-15:00	Session 16: **Usable Security and Privacy** *Session Chair: Gabriele Oligeri*	Session 17: **Binary Security** *Session Chair: Qiang Liu*	Session 18: **Network Security** *Session Chair: Arash Shaghaghi*
	NailKey: Mutable Biometric Using Fingernails *Yihong Hang, Zhice Yang* **Different Seas, Different Phishes: Large-Scale Analysis of Phishing Simulations Across Different Industries** *Oskar Braun, Jan Hörnemann, Norbert Pohlmann, Tobias Urban, Matteo Grosse-Kampmann* **Can Small-scale Evaluation Reflect Real Ability? A Performance Study of Emerging Biometric Authentication** *Hangcheng Cao, Guowen Xu, Wenbin Huang, Hongwei Li* **The Impact of Emerging Phishing Threats: Assessing Quishing and LLM-generated Phishing Emails against Organizations** *Marie Weinz, Nicola Zannone, Luca Allodi, Giovanni Apruzzese*	**Breaking Bad: How Compilers Break Constant-Time Implementations** *Moritz Schneider, Daniele Lain, Ivan Puddu, Nicolas Dutly, Srdjan Capkun* **An Empirical Study of C Decompilers: Performance Metrics and Error Taxonomy** *Melih Sirlanci, Carter Yagemann, Zhiqiang Lin* **Enhancing Binary Code Similarity Analysis for Software Updates: A Contextual Diffing Framework** *August See, Moritz Mönnich, Mathias Fischer* **Evaluating Disassembly Errors With Only Binaries** *Lambang Akbar Wijayadi, Yuancheng Jiang, Roland Yap, Zhenkai Liang, Zhuohao Liu*	**OMALDA5G: Online Malware Detection and Attribution in 5G Networks using Compound Paths** *Zhixin Wen, Guanhua Yan* **Ruling the Unruly: Network Intrusion Detection Rule Design Principles for Specificity and Coverage to Decrease Unnecessary Workload in SOCs** *Koen T. W. Teuwen, Tom Mulders, Emmanuele Zambon, Luca Allodi* **SigN: SIMBox Activity Detection Through Latency Anomalies at the Cellular Edge** *Kouam Djuigne, Aline Carneiro Viana, Philippe Martins, Cédric Adjih, Alain Tchana* **An Automated Blackbox Noncompliance Checker for QUIC Server Implementations** *Kian Kai Ang, Guy Farrelly, Cheryl Pope, Damith C. Ranasinghe*

	PRISM: To Fortify Widget Based User-App Data Exchanges Using Android Virtualization Framework *YingTat Ng, Zhe Chen, Haiqing Qiu, Xuhua Ding* **On the Account Security Risks Posed by Password Strength Meters** *Ming Xu, Weili Han,Jitao Yu, Jing Liu, Xinyi Zhang, Yun Lin, Jin Song Dong*	**Enabling Microarchitectural Agility: Taking ML-KEM & ML-DSA from Cortex-M4 to M7 with SLOTHY** *Amin Abdulrahman, Matthias J. Kannwischer, Thing-Han Lim* **REFLECTA: Reflection-based Scalable and Semantic Scripting Language Fuzzing** *Chibin Zhang, Gwangmu Lee, Qiang Liu, Mathias Payer*	**Formal Analysis of SDNsec: Attacks and Corrections for Payload, Route Integrity and Accountability** *Ayoub Ben Hassen, Pascal Lafourcade, Dhekra Mahmoud, Maxime Puys* **Learning to Identify Conflicts in RPKI** *Haya Schulmann, Shujie Zhao*
15:00-15:30		Tea Break	
15:30-16:30	Session 19: **CPS Security** *Session Chair: Awais Yousaf*	Session 20: **Blockchain 2** *Session Chair: István András Seres*	Session 21: **Blockchain 3** *Session Chair: Roopa Vishwanathan*
	Runtime Stealthy Perception Attacks against DNN-based Adaptive Cruise Control Systems *Xugui Zhou, Anqi Chen, Maxfield Kouzel, Haotian Ren, Morgan McCarty, Cristina Nita-Rotaru, Homa Alemzadeh* **Adversarial Fog: Exploiting the Vulnerabilities of LiDAR Point Cloud Preprocessing Filters** *Yuna Tanaka, Kazuki Nomoto, Ryunosuke Kobayashi, Go Tsuruoka, Tatsuya Mori*	**FIRST: FrontrunnIng Resistant Smart ConTracts** *Emrah Sariboz, Gaurav Panwar, Roopa Vishwanathan, Satyajayant Misra* **Mining Attack with Zero Knowledge in the Blockchain** *Yu Jiaping, Gao Shang, Song Rui, Zhiping Cai, Xiao Bin*	**An Empirical Study on Cross-chain Transactions: Costs, Inconsistencies, and Activities** *Kailun Yan, Bo Lu, Pranav Agrawal, Jiasun Li, Wenrui Diao, Xiaokuan Zhang* **AWOSE: Probabilistic State Model for Consensus Algorithms Fuzzing Frameworks** *Tannishtha Devgun, Gulshan Kumar, Rahul Saha, Alessandro Brighente, Mauro Conti*

	From Transients to Flips: Hardware-level Bit Manipulation of In-Vehicle Serial Communication *Abdullah Zubair Mohammed, Ryan Gerdes* **Preventing Radio Fingerprinting through Friendly Jamming** *Muhammad Irfan, Savio Sciancalepore, Gabriele Oligeri*	**Infiltrated Selfish Mining: Think Win-Win to Escape Dilemmas** *Xuelian Cao, Zheng Yang, Tao Xiang, Jianting Ning, Yuhan Liu, Zhiming Liu, Jianying Zhou* **BRC20 Snipping Attack** *Minfeng Qi, Qin Wang, Ningran Li, Shiping Chen, Tianqing Zhu*	**DTL: Data Tumbling Layer A Composable Unlinkability for Smart Contracts** *Mohsen Minaei, Pedro Moreno-Sanchez, Zhiyong Fang, Srinivasan Raghuraman, Navid Alamati, Panagiotis Chatzigiannis, Ranjit Kumaresan, Duc Le* **Pace: Privacy-preserving and Atomic Cross-chain Swaps for Cryptocurrency Exchanges** *Jianhuan Wang, Bin Xiao*
16:30-17:00	**Closing Remark**		